

## CIS Google Cloud Platform Foundation Benchmark

v1.3.0 - 03-31-2022



## **Terms of Use**

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

#### Table of Contents

Րerms of Use	1
Dverview	8
Intended Audience	8
Consensus Guidance	8
Typographical Conventions	9
Assessment Status	9
Profile Definitions	10
Acknowledgements	11
Recommendations	13
1 Identity and Access Management	13
1.1 Ensure that Corporate Login Credentials are Used (Manual)	14
1.2 Ensure that Multi-Factor Authentication is 'Enabled' for All Non-Service Accounts (Manual)	16
1.3 Ensure that Security Key Enforcement is Enabled for All Admin Accounts (Manual)	18
1.4 Ensure That There Are Only GCP-Managed Service Account Keys for Each Service Account (Automated)	20
1.5 Ensure That Service Account Has No Admin Privileges (Automated)	23
1.6 Ensure That IAM Users Are Not Assigned the Service Account User or Servic Account Token Creator Roles at Project Level (Automated)	е 27
1.7 Ensure User-Managed/External Keys for Service Accounts Are Rotated Ever 90 Days or Fewer (Automated)	у 31
1.8 Ensure That Separation of Duties Is Enforced While Assigning Service Accou Related Roles to Users (Automated)	ınt 34
1.9 Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible (Automated)	37
1.10 Ensure KMS Encryption Keys Are Rotated Within a Period of 90 Days (Automated)	40
1.11 Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users (Automated)	i 43
1.12 Ensure API Keys Are Not Created for a Project (Manual)	46

	1.13 Ensure API Keys Are Restricted To Use by Only Specified Hosts and Apps (Manual)	48
	1.14 Ensure API Keys Are Restricted to Only APIs That Application Needs Access (Manual)	; 50
	1.15 Ensure API Keys Are Rotated Every 90 Days (Manual)	52
	1.16 Ensure Essential Contacts is Configured for Organization (Automated)	54
	1.17 Ensure that Dataproc Cluster is encrypted using Customer-Managed Encryption Key (Automated)	57
	1.18 Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager (Manual)	y 61
2 Logg	ing and Monitoring	66
	2.1 Ensure That Cloud Audit Logging Is Configured Properly Across All Services and All Users From a Project (Automated)	67
	2.2 Ensure That Sinks Are Configured for All Log Entries (Automated)	71
	2.3 Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock (Automated)	74
	2.4 Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes (Automated)	77
	2.5 Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes (Automated)	82
	2.6 Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes (Automated)	86
	2.7 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes (Automated)	90
	2.8 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes (Automated)	94
	2.9 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes (Automated)	98
	2.10 Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes (Automated)10	02
	2.11 Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes (Automated)10	06
	2.12 Ensure That Cloud DNS Logging Is Enabled for All VPC Networks (Automated)12	10

2.13 Ensure Cloud Asset Inventory Is Enabled (Automated)113
2.14 Ensure 'Access Transparency' is 'Enabled' (Manual)116
2.15 Ensure 'Access Approval' is 'Enabled' (Automated)119
3 Networking
3.1 Ensure That the Default Network Does Not Exist in a Project (Automated)124
3.2 Ensure Legacy Networks Do Not Exist for Older Projects (Automated)127
3.3 Ensure That DNSSEC Is Enabled for Cloud DNS (Automated)129
3.4 Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC (Manual)
3.5 Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC (Manual)
3.6 Ensure That SSH Access Is Restricted From the Internet (Automated)137
3.7 Ensure That RDP Access Is Restricted From the Internet (Automated)140
3.8 Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network (Automated)143
3.9 Ensure No HTTPS or SSL Proxy Load Balancers Permit SSL Policies With Weak Cipher Suites (Manual)147
3.10 Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed' (Manual)151
4 Virtual Machines
4.1 Ensure That Instances Are Not Configured To Use the Default Service Account (Automated)155
4.2 Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs (Automated)
4.3 Ensure "Block Project-Wide SSH Keys" Is Enabled for VM Instances (Automated)161
4.4 Ensure Oslogin Is Enabled for a Project (Automated)
4.5 Ensure 'Enable Connecting to Serial Ports' Is Not Enabled for VM Instance (Automated)167
4.6 Ensure That IP Forwarding Is Not Enabled on Instances (Automated)170
4.7 Ensure VM Disks for Critical VMs Are Encrypted With Customer-Supplied Encryption Keys (CSEK) (Automated)173

	4.8 Ensure Compute Instances Are Launched With Shielded VM Enabled (Automated)
	4.9 Ensure That Compute Instances Do Not Have Public IP Addresses (Automated)
	4.10 Ensure That App Engine Applications Enforce HTTPS Connections (Manual) 
	4.11 Ensure That Compute Instances Have Confidential Computing Enabled (Automated)
	4.12 Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects (Manual)
5 Stor	age197
	5.1 Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible (Automated)
	5.2 Ensure That Cloud Storage Buckets Have Uniform Bucket-Level Access Enabled (Automated)201
6 Clou	d SQL Database Services204
6.1	MySQL Database
	6.1.1 Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges (Manual)206
	6.1.2 Ensure 'Skip_show_database' Database Flag for Cloud SQL MySQL Instance Is Set to 'On' (Automated)
	6.1.3 Ensure That the 'Local_infile' Database Flag for a Cloud SQL MySQL Instance Is Set to 'Off' (Automated)212
6.2	PostgreSQL Database215
	6.2.1 Ensure 'Log_error_verbosity' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'DEFAULT' or Stricter (Manual)216
	6.2.2 Ensure That the 'Log_connections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' (Automated)
	6.2.3 Ensure That the 'Log_disconnections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' (Automated)222
	6.2.4 Ensure 'Log_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately (Manual)225
	6.2.5 Ensure 'Log_hostname' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'on' (Automated)228

6.2.6 Ensure That the 'Log_min_messages' Database Flag for Cloud SQL PostgreSQL Instance Is Set to at least 'Warning' (Manual)
6.2.7 Ensure 'Log_min_error_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter (Automated)234
6.2.8 Ensure That the 'Log_min_duration_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled) (Automated)
6.2.9 Ensure That 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging (Automated)240
6.3 SQL Server245
6.3.1 Ensure 'external scripts enabled' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)246
6.3.2 Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)249
6.3.3 Ensure 'user Connections' Database Flag for Cloud Sql Sql Server Instance Is Set to a Non-limiting Value (Automated)252
6.3.4 Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured (Automated)255
6.3.5 Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)258
6.3.6 Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'off' (Automated)261
6.3.7 Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is set to 'off' (Automated)
6.4 Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL (Automated)267
6.5 Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses (Automated)270
6.6 Ensure That Cloud SQL Database Instances Do Not Have Public IPs (Automated)273
6.7 Ensure That Cloud SQL Database Instances Are Configured With Automated Backups (Automated)276
7 BigQuery
7.1 Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible (Manual)

7.2 Ensure That All BigQuery Tables Are Encrypted With Customer-Managed
Encryption Key (CMEK) (Automated)283
7.3 Ensure That a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets (Manual)
Appendix: Recommendation Summary Table289
Appendix: CIS Controls v7 IG 1 Mapped Recommendations294
Appendix: CIS Controls v7 IG 2 Mapped Recommendations296
Appendix: CIS Controls v7 IG 3 Mapped Recommendations
Appendix: CIS Controls v8 IG 1 Mapped Recommendations
Appendix: CIS Controls v8 IG 2 Mapped Recommendations
Appendix: CIS Controls v8 IG 3 Mapped Recommendations
Appendix: Change History

## **Overview**

This security configuration benchmark covers foundational elements of Google Cloud Platform. The recommendations detailed here are important security considerations when designing your infrastructure on Google Cloud Platform. Most of the recommendations provided with this release of the benchmark covers security considerations only at individual Project level and not at the organization level.

To obtain the latest version of this guide, please visit <u>http://benchmarks.cisecurity.org</u>. If you have questions, comments, or have identified ways to improve this guide, please write us at <u>BenchmarkInfo@cisecurity.org</u>.

## **Intended Audience**

This document is intended for system and application administrators, security specialists, auditors, help desk, platform deployment, and/or DevOps personnel who plan to develop, deploy, assess, or secure solutions on Google Cloud Platform.

## **Consensus Guidance**

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit <a href="https://workbench.cisecurity.org/">https://workbench.cisecurity.org/</a>.

## **Typographical Conventions**

The following typographical conventions are used throughout this guide:

Convention	Meaning
Stylized Monospace font	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic brackets="" font="" in=""></italic>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

### **Assessment Status**

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

#### Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

#### Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

## **Profile Definitions**

The following configuration profiles are defined by this Benchmark:

#### • Level 1

Items in this profile intend to:

- be practical and prudent;
- provide security focused best practice hardening of a technology; and
- limit impact to the utility of the technology beyond acceptable means.

#### • Level 2

This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is more critical than manageability and usability
- o acts as defense in depth measure
- may impact the utility or performance of the technology
- may include additional licensing, cost, or addition of third party software

### Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

#### Contributor

Shobha H D Pravin Goyal Aditi Sahasrabudhe Mike Wicks Jacqueline Kenny **Colin Estep** Anmol Baansal **Robin Drake** Nathael Leblanc Geoff Uyleman Jeremy Phillips David Lu Bhushan Bhat Prateek Khatri Logan McMillan Nandhini C Viktor Gazdag **Rachel Rice Iben Rodriguez** 

#### Editor

Prabhu Angadi Parag Patil Pradeep R B Iulia Ion Andrew Kiggins

## Recommendations

## 1 Identity and Access Management

This section covers recommendations addressing Identity and Access Management on Google Cloud Platform.

### 1.1 Ensure that Corporate Login Credentials are Used (Manual)

#### **Profile Applicability:**

• Level 1

#### **Description**:

Use corporate login credentials instead of personal accounts, such as Gmail accounts.

#### **Rationale:**

It is recommended fully-managed corporate Google accounts be used for increased visibility, auditing, and controlling access to Cloud Platform resources. Email accounts based outside of the user's organization, such as personal accounts, should not be used for business purposes.

#### Impact:

There will be increased overhead as maintaining accounts will now be required. For smaller organizations, this will not be an issue, but will balloon with size.

#### Audit:

For each Google Cloud Platform project, list the accounts that have been granted access to that project:

gcloud projects get-iam-policy PROJECT\_ID

Also list the accounts added on each folder:

gcloud resource-manager folders get-iam-policy FOLDER\_ID

And list your organization's IAM policy:

gcloud organizations get-iam-policy ORGANIZATION\_ID

No email accounts outside the organization domain should be granted permissions in the IAM policies. This excludes Google-owned service accounts.

#### **Remediation:**

Follow the documentation and setup corporate login accounts.

#### Prevention:

To ensure that no email addresses outside the organization can be granted IAM

permissions to its Google Cloud projects, folders or organization, turn on the Organization Policy for Domain Restricted Sharing. Learn more at:

https://cloud.google.com/resource-manager/docs/organization-policy/restrictingdomains

#### **Default Value:**

By default, no email addresses outside the organization's domain have access to its Google Cloud deployments, but any user email account can be added to the IAM policy for Google Cloud Platform projects, folders, or organizations.

#### **References:**

- 1. <u>https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#manage-identities</u>
- 2. <u>https://support.google.com/work/android/answer/6371476</u>
- 3. <u>https://cloud.google.com/sdk/gcloud/reference/organizations/get-iam-policy</u>
- 4. <u>https://cloud.google.com/sdk/gcloud/reference/beta/resource-</u> manager/folders/get-iam-policy
- 5. <u>https://cloud.google.com/sdk/gcloud/reference/projects/get-iam-policy</u>
- 6. <u>https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints</u>
- 7. <u>https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains</u>

#### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 <u>Centralize Account Management</u> Centralize account management through a directory or identity service.		•	•
v7	<b>16.2</b> <u>Configure Centralized Point of Authentication</u> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		•	•

## 1.2 Ensure that Multi-Factor Authentication is 'Enabled' for All Non-Service Accounts (Manual)

#### Profile Applicability:

• Level 1

#### **Description**:

Setup multi-factor authentication for Google Cloud Platform accounts.

#### **Rationale:**

Multi-factor authentication requires more than one mechanism to authenticate a user. This secures user logins from attackers exploiting stolen or weak credentials.

#### Audit:

#### From Console:

For each Google Cloud Platform project, folder, or organization:

- 1. Identify non-service accounts.
- 2. Manually verify that multi-factor authentication for each account is set.

#### **Remediation:**

#### From Console:

For each Google Cloud Platform project:

- 1. Identify non-service accounts.
- 2. Setup multi-factor authentication for each account.

#### **Default Value:**

By default, multi-factor authentication is not set.

#### **References:**

- 1. <u>https://cloud.google.com/solutions/securing-gcp-account-u2f</u>
- 2. <u>https://support.google.com/accounts/answer/185839</u>

#### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 <u>Require MFA for Externally-Exposed Applications</u> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		•	•
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		•	•

## 1.3 Ensure that Security Key Enforcement is Enabled for All Admin Accounts (Manual)

#### **Profile Applicability:**

• Level 2

#### **Description:**

Setup Security Key Enforcement for Google Cloud Platform admin accounts.

#### **Rationale:**

Google Cloud Platform users with Organization Administrator roles have the highest level of privilege in the organization. These accounts should be protected with the strongest form of two-factor authentication: Security Key Enforcement. Ensure that admins use Security Keys to log in instead of weaker second factors like SMS or one-time passwords (OTP). Security Keys are actual physical keys used to access Google Organization Administrator Accounts. They send an encrypted signature rather than a code, ensuring that logins cannot be phished.

#### Impact:

If an organization administrator loses access to their security key, the user could lose access to their account. For this reason, it is important to set up backup security keys.

#### Audit:

1. Identify users with Organization Administrator privileges:

```
gcloud organizations get-iam-policy ORGANIZATION_ID
```

Look for members granted the role "roles/resourcemanager.organizationAdmin".

2. Manually verify that Security Key Enforcement has been enabled for each account.

#### **Remediation:**

- 1. Identify users with the Organization Administrator role.
- 2. Setup Security Key Enforcement for each account. Learn more at: <u>https://cloud.google.com/security-key/</u>

#### **Default Value:**

By default, Security Key Enforcement is not enabled for Organization Administrators.

#### **References:**

- https://cloud.google.com/security-key/
   https://gsuite.google.com/learnmore/key for working smarter faster and more securely.html

#### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 <u>Require MFA for Externally-Exposed Applications</u> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		•	•
v7	<b>16.3</b> <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		•	

# 1.4 Ensure That There Are Only GCP-Managed Service Account Keys for Each Service Account (Automated)

#### Profile Applicability:

• Level 1

#### **Description**:

User managed service accounts should not have user-managed keys.

#### **Rationale:**

Anyone who has access to the keys will be able to access resources through the service account. GCP-managed keys are used by Cloud Platform services such as App Engine and Compute Engine. These keys cannot be downloaded. Google will keep the keys and automatically rotate them on an approximately weekly basis. User-managed keys are created, downloadable, and managed by users. They expire 10 years from creation.

For user-managed keys, the user has to take ownership of key management activities which include:

- Key storage
- Key distribution
- Key revocation
- Key rotation
- Protecting the keys from unauthorized users
- Key recovery

Even with key owner precautions, keys can be easily leaked by common development malpractices like checking keys into the source code or leaving them in the Downloads directory, or accidentally leaving them on support blogs/channels.

It is recommended to prevent user-managed service account keys.

#### Impact:

Deleting user-managed Service Account Keys may break communication with the applications using the corresponding keys.

#### Audit:

#### From Console:

- 1. Go to the IAM page in the GCP Console using https://console.cloud.google.com/iam-admin/iam
- 2. In the left navigation pane, click Service accounts. All service accounts and their corresponding keys are listed.
- 3. Click the service accounts and check if keys exist.

#### **From Command Line:**

List All the service accounts:

gcloud iam service-accounts list

Identify user-managed service accounts as such account EMAIL ends with iam.gserviceaccount.com

For each user-managed service account, list the keys managed by the user:

```
gcloud iam service-accounts keys list --iam-account=<Service Account> --
managed-by=user
```

No keys should be listed.

#### **Remediation:**

#### From Console:

- 1. Go to the IAM page in the GCP Console using https://console.cloud.google.com/iam-admin/iam
- 2. In the left navigation pane, click Service accounts. All service accounts and their corresponding keys are listed.
- 3. Click the service account.
- 4. Click the edit and delete the keys.

#### **From Command Line:**

To delete a user managed Service Account Key,

```
gcloud iam service-accounts keys delete --iam-account=<user-managed-service-
account-EMAIL> <KEY-ID>
```

#### **Prevention:**

You can disable service account key creation through the Disable service account key creation Organization policy by visiting <a href="https://console.cloud.google.com/iam-admin/orgpolicies/iam-disableServiceAccountKeyCreation">https://console.cloud.google.com/iam-admin/orgpolicies/iam-disableServiceAccountKeyCreation</a>. Learn more at: <a href="https://cloud.google.com/resource-manager/docs/organization-policy/restricting-">https://cloud.google.com/resource-manager/docs/organization-policy/restricting-</a>

#### service-accounts

In addition, if you do not need to have service accounts in your project, you can also prevent the creation of service accounts through the Disable service account creation Organization policy: <a href="https://console.cloud.google.com/iam-admin/orgpolicies/iam-disableServiceAccountCreation">https://console.cloud.google.com/iam-admin/orgpolicies/iam-disableServiceAccountCreation</a>.

#### **Default Value:**

By default, there are no user-managed keys created for user-managed service accounts.

#### **References:**

- 1. <u>https://cloud.google.com/iam/docs/understanding-service-accounts#managing\_service\_account\_keys</u>
- 2. <u>https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts</u>

#### **Additional Information:**

A user-managed key cannot be created on GCP-Managed Service Accounts.

### 1.5 Ensure That Service Account Has No Admin Privileges (Automated)

#### **Profile Applicability:**

• Level 1

#### **Description**:

A service account is a special Google account that belongs to an application or a VM, instead of to an individual end-user. The application uses the service account to call the service's Google API so that users aren't directly involved. It's recommended not to use admin access for ServiceAccount.

#### **Rationale:**

Service accounts represent service-level security of the Resources (application or a VM) which can be determined by the roles assigned to it. Enrolling ServiceAccount with Admin rights gives full access to an assigned application or a VM. A ServiceAccount Access holder can perform critical actions like delete, update change settings, etc. without user intervention. For this reason, it's recommended that service accounts not have Admin rights.

#### Impact:

Removing \*Admin or \*adminorEditororOwner`role assignments from service accounts may break functionality that uses impacted service accounts. Required role(s) should be assigned to impacted service accounts in order to restore broken functionalities.

#### Audit:

#### From Console:

- 1. Go to IAM & admin/IAM using https://console.cloud.google.com/iam-admin/iam
- $2. \ Go \ to \ the \ {\tt Members}$
- 3. Ensure that there are no User-Managed user created service account(s) with roles containing \*Admin or \*admin or role matching Editor or role matching Owner

#### **From Command Line:**

- 1. Get the policy that you want to modify, and write it to a JSON file: gcloud projects get-iam-policy PROJECT\_ID --format json > iam.json
- The contents of the JSON file will look similar to the following. Note that role of members group associated with each serviceaccount does not contain \*Admin or \*admin or does not match roles/editor or does not match roles/owner.

This recommendation is only applicable to User-Managed user-created service accounts. These accounts have the nomenclature:

SERVICE\_ACCOUNT\_NAME@PROJECT\_ID.iam.gserviceaccount.com. Note that some Googlemanaged, Google-created service accounts have the same naming format, and should be excluded (e.g., appsdev-apps-dev-script-auth@system.gserviceaccount.com which needs the Owner role).

#### Sample Json output:

```
"bindings": [
{
   "members": [
      "serviceAccount:our-project-123@appspot.gserviceaccount.com",
    ],
    "role": "roles/appengine.appAdmin"
},
{
    "members": [
     "user:email1@gmail.com"
    ],
    "role": "roles/owner"
},
   "members": [
      "serviceAccount:our-project-123@appspot.gserviceaccount.com",
      "serviceAccount:123456789012-compute@developer.gserviceaccount.com"
    ],
    "role": "roles/editor"
],
"etag": "BwUjMhCsNvY=",
"version": 1
```

#### **Remediation:**

#### From Console:

- 1. Go to IAM & admin/IAM using https://console.cloud.google.com/iam-admin/iam
- $2. \ Go \ to \ the \ {\tt Members}$
- 3. Identify User-Managed user created service account with roles containing \*Admin or \*admin or role matching Editor or role matching Owner
- 4. Click the Delete bin icon to remove the role from the member (service account in this case)

#### From Command Line:

gcloud projects get-iam-policy PROJECT\_ID --format json > iam.json

1. Using a text editor, Remove Role which contains roles/\*Admin or roles/\*admin or matched roles/editor or matches 'roles/owner'. Add a role to the bindings array that defines the group members and the role for those members.

For example, to grant the role roles/appengine.appViewer to the ServiceAccount which is roles/editor, you would change the example shown below as follows:

```
"bindings": [
{
   "members": [
     "serviceAccount:our-project-123@appspot.gserviceaccount.com",
    ],
    "role": "roles/appengine.appViewer"
},
{
    "members": [
     "user:email10gmail.com"
    ],
    "role": "roles/owner"
  },
{
    "members": [
      "serviceAccount:our-project-123@appspot.gserviceaccount.com",
      "serviceAccount:123456789012-compute@developer.gserviceaccount.com"
    ],
    "role": "roles/editor"
}
],
"etag": "BwUjMhCsNvY="
```

2. Update the project's IAM policy: gcloud projects set-iam-policy PROJECT\_ID iam.json

#### **Default Value:**

User Managed (and not user-created) default service accounts have the Editor (roles/editor) role assigned to them to support GCP services they offer.

By default, there are no roles assigned to User Managed User created service accounts.

#### **References:**

- 1. <u>https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/</u>
- 2. <u>https://cloud.google.com/iam/docs/understanding-roles</u>
- 3. <u>https://cloud.google.com/iam/docs/understanding-service-accounts</u>

#### Additional Information:

Default (user-managed but not user-created) service accounts have the Editor (roles/editor) role assigned to them to support GCP services they offer. Such Service accounts are: PROJECT\_NUMBER-compute@developer.gserviceaccount.com, PROJECT\_ID@appspot.gserviceaccount.com.

#### **CIS Controls**:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 <u>Restrict Administrator Privileges to Dedicated</u> <u>Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	•	•	•
v7	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.		•	

## 1.6 Ensure That IAM Users Are Not Assigned the Service Account User or Service Account Token Creator Roles at Project Level (Automated)

#### **Profile Applicability:**

• Level 1

#### **Description**:

It is recommended to assign the Service Account User (iam.serviceAccountUser) and Service Account Token Creator (iam.serviceAccountTokenCreator) roles to a user for a specific service account rather than assigning the role to a user at project level.

#### **Rationale:**

A service account is a special Google account that belongs to an application or a virtual machine (VM), instead of to an individual end-user. Application/VM-Instance uses the service account to call the service's Google API so that users aren't directly involved. In addition to being an identity, a service account is a resource that has IAM policies attached to it. These policies determine who can use the service account.

Users with IAM roles to update the App Engine and Compute Engine instances (such as App Engine Deployer or Compute Instance Admin) can effectively run code as the service accounts used to run these instances, and indirectly gain access to all the resources for which the service accounts have access. Similarly, SSH access to a Compute Engine instance may also provide the ability to execute code as that instance/Service account.

Based on business needs, there could be multiple user-managed service accounts configured for a project. Granting the iam.serviceAccountUser or iam.serviceAccountTokenCreator roles to a user for a project gives the user access to all service accounts in the project, including service accounts that may be created in the future. This can result in elevation of privileges by using service accounts and corresponding Compute Engine instances.

In order to implement least privileges best practices, IAM users should not be assigned the Service Account User or Service Account Token Creator roles at the project level. Instead, these roles should be assigned to a user for a specific service account, giving that user access to the service account. The Service Account User allows a user to bind a service account to a long-running job service, whereas the Service Account Token Creator role allows a user to directly impersonate (or assert) the identity of a service account.

#### Impact:

After revoking Service Account User or Service Account Token Creator roles at the project level from all impacted user account(s), these roles should be assigned to a user(s) for specific service account(s) according to business needs.

#### Audit:

#### From Console:

- 1. Go to the IAM page in the GCP Console by visiting https://console.cloud.google.com/iam-admin/iam
- 2. Click on the filter table text bar, Type Role: Service Account User.
- 3. Ensure no user is listed as a result of the filter.
- 4. Click on the filter table text bar, Type Role: Service Account Token Creator.
- 5. Ensure no user is listed as a result of the filter.

#### **From Command Line:**

To ensure IAM users are not assigned Service Account User role at the project level:

```
gcloud projects get-iam-policy PROJECT_ID --format json | jq
'.bindings[].role' | grep "roles/iam.serviceAccountUser"
gcloud projects get-iam-policy PROJECT_ID --format json | jq
```

'.bindings[].role' | grep "roles/iam.serviceAccountTokenCreator"

These commands should not return any output.

#### **Remediation:**

#### From Console:

- 1. Go to the IAM page in the GCP Console by visiting: https://console.cloud.google.com/iam-admin/iam.
- 2. Click on the filter table text bar. Type Role: Service Account User
- 3. Click the Delete Bin icon in front of the role Service Account User for every user listed as a result of a filter.
- 4. Click on the filter table text bar. Type Role: Service Account Token Creator
- 5. Click the Delete Bin icon in front of the role Service Account Token Creator for every user listed as a result of a filter.

#### From Command Line:

1. Using a text editor, remove the bindings with the roles/iam.serviceAccountUser or roles/iam.serviceAccountTokenCreator. For example, you can use the iam.json file shown below as follows:

```
"bindings": [
{
   "members": [
     "serviceAccount:our-project-123@appspot.gserviceaccount.com",
    ],
    "role": "roles/appengine.appViewer"
},
{
    "members": [
    "user:email1@gmail.com"
    ],
    "role": "roles/owner"
   },
{
    "members": [
      "serviceAccount:our-project-123@appspot.gserviceaccount.com",
      "serviceAccount:123456789012-compute@developer.gserviceaccount.com"
    ],
    "role": "roles/editor"
}
],
"etaq": "BwUjMhCsNvY="
```

2. Update the project's IAM policy:

gcloud projects set-iam-policy PROJECT\_ID iam.json

#### **Default Value:**

By default, users do not have the Service Account User or Service Account Token Creator role assigned at project level.

#### **References:**

- 1. <u>https://cloud.google.com/iam/docs/service-accounts</u>
- 2. <u>https://cloud.google.com/iam/docs/granting-roles-to-service-accounts</u>
- 3. <u>https://cloud.google.com/iam/docs/understanding-roles</u>
- 4. https://cloud.google.com/iam/docs/granting-changing-revoking-access
- 5. <u>https://console.cloud.google.com/iam-admin/iam</u>

#### Additional Information:

To assign the role roles/iam.serviceAccountUser or

roles/iam.serviceAccountTokenCreator to a user role on a service account instead of a
project:

- 1. Go to <u>https://console.cloud.google.com/projectselector/iam-admin/serviceaccounts</u>
- 2. Select Target Project
- 3. Select target service account. Click Permissions on the top bar. It will open permission pane on right side of the page
- 4. Add desired members with Service Account User or Service Account Token Creator role.

#### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3</b> <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	٠	•	
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	•	•	•

## 1.7 Ensure User-Managed/External Keys for Service Accounts Are Rotated Every 90 Days or Fewer (Automated)

#### **Profile Applicability:**

• Level 1

#### **Description**:

Service Account keys consist of a key ID (Private\_key\_Id) and Private key, which are used to sign programmatic requests users make to Google cloud services accessible to that particular service account. It is recommended that all Service Account keys are regularly rotated.

#### **Rationale:**

Rotating Service Account keys will reduce the window of opportunity for an access key that is associated with a compromised or terminated account to be used. Service Account keys should be rotated to ensure that data cannot be accessed with an old key that might have been lost, cracked, or stolen.

Each service account is associated with a key pair managed by Google Cloud Platform (GCP). It is used for service-to-service authentication within GCP. Google rotates the keys daily.

GCP provides the option to create one or more user-managed (also called external key pairs) key pairs for use from outside GCP (for example, for use with Application Default Credentials). When a new key pair is created, the user is required to download the private key (which is not retained by Google). With external keys, users are responsible for keeping the private key secure and other management operations such as key rotation. External keys can be managed by the IAM API, gcloud command-line tool, or the Service Accounts page in the Google Cloud Platform Console. GCP facilitates up to 10 external service account keys per service account to facilitate key rotation.

#### Impact:

Rotating service account keys will break communication for dependent applications. Dependent applications need to be configured manually with the new key ID displayed in the Service account keys section and the private key downloaded by the user.

#### Audit:

#### From Console:

- 1. Go to APIs & Services\Credentials using
   https://console.cloud.google.com/apis/credentials
- 2. In the section Service Account Keys, for every External (user-managed) service account key listed ensure the creation date is within the past 90 days.

#### From Command Line:

1. List all Service accounts from a project.

gcloud iam service-accounts list

2. For every service account list service account keys.

```
gcloud iam service-accounts keys list --iam-account
[Service_Account_Email_Id] --format=json
```

3. Ensure every service account key for a service account has a "validAfterTime" value within the past 90 days.

#### **Remediation:**

#### From Console:

#### Delete any external (user-managed) Service Account Key older than 90 days:

- 1. Go to APIs & Services\Credentials using
   https://console.cloud.google.com/apis/credentials
- 2. In the Section Service Account Keys, for every external (user-managed) service account key where creation date is greater than or equal to the past 90 days, click Delete Bin Icon to Delete Service Account key

#### Create a new external (user-managed) Service Account Key for a Service Account:

- Go to APIs & Services\Credentials using https://console.cloud.google.com/apis/credentials
- 2. Click Create Credentials and Select Service Account Key.
- 3. Choose the service account in the drop-down list for which an External (usermanaged) Service Account key needs to be created.
- 4. Select the desired key type format among JSON or P12.
- 5. Click Create. It will download the private key. Keep it safe.
- 6. Click close if prompted.
- 7. The site will redirect to the APIs & Services\Credentials page. Make a note of the new ID displayed in the Service account keys section.

#### **Default Value:**

GCP does not provide an automation option for External (user-managed) Service key rotation.

#### **References:**

- 1. <u>https://cloud.google.com/iam/docs/understanding-service-accounts#managing\_service\_account\_keys</u>
- 2. <u>https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/keys/list</u>
- 3. <u>https://cloud.google.com/iam/docs/service-accounts</u>

#### **Additional Information:**

For user-managed Service Account key(s), key management is entirely the user's responsibility.

## 1.8 Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users (Automated)

#### **Profile Applicability:**

• Level 2

#### **Description**:

It is recommended that the principle of 'Separation of Duties' is enforced while assigning service-account related roles to users.

#### **Rationale:**

The built-in/predefined IAM role Service Account admin allows the user/identity to create, delete, and manage service account(s). The built-in/predefined IAM role Service Account User allows the user/identity (with adequate privileges on Compute and App Engine) to assign service account(s) to Apps/Compute Instances.

Separation of duties is the concept of ensuring that one individual does not have all necessary permissions to be able to complete a malicious action. In Cloud IAM - service accounts, this could be an action such as using a service account to access resources that user should not normally have access to.

Separation of duties is a business control typically used in larger organizations, meant to help avoid security or privacy incidents and errors. It is considered best practice.

No user should have Service Account Admin and Service Account User roles assigned at the same time.

#### Impact:

The removed role should be assigned to a different user based on business needs.

#### Audit:

#### From Console:

- 1. Go to IAM & Admin/IAM using https://console.cloud.google.com/iam-admin/iam.
- 2. Ensure no member has the roles Service Account Admin and Service account User assigned together.

#### From Command Line:

1. List all users and role assignments:

```
gcloud projects get-iam-policy [Project ID] --format json | \
 jq -r '[
          (["Service Account Admin and User"] | (., map(length*"-"))),
              ſ
                .bindings[] |
                select(.role == "roles/iam.serviceAccountAdmin" or .role ==
"roles/iam.serviceAccountUser").members[]
              1 1
              group by(.) |
              map({User: ., Count: length}) |
              .[] |
              select(.Count == 2).User |
              unique
            )
        1 |
        .[] |
        @tsv'
```

2. All common users listed under <code>Service\_Account\_Admin\_and\_User</code> are assigned both the <code>roles/iam.serviceAccountAdmin</code> and <code>roles/iam.serviceAccountUser</code> roles.

#### **Remediation:**

#### From Console:

- $1. \ \ Go \ to \ \hbox{IAM \& Admin/IAM using https://console.cloud.google.com/iam-admin/iam.}$
- For any member having both Service Account Admin and Service account User roles granted/assigned, click the Delete Bin icon to remove either role from the member.

Removal of a role should be done based on the business requirements.

#### **References:**

- 1. <u>https://cloud.google.com/iam/docs/service-accounts</u>
- 2. https://cloud.google.com/iam/docs/understanding-roles
- 3. <u>https://cloud.google.com/iam/docs/granting-roles-to-service-accounts</u>

#### **Additional Information:**

Users granted with Owner (roles/owner) and Editor (roles/editor) have privileges equivalent to Service Account Admin and Service Account User. To avoid the misuse, Owner and Editor roles should be granted to very limited users and Use of these primitive privileges should be minimal. These requirements are addressed in separate recommendations.
Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3</b> <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	•	•	•

# 1.9 Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible (Automated)

# **Profile Applicability:**

• Level 1

# **Description:**

It is recommended that the IAM policy on Cloud KMS cryptokeys should restrict anonymous and/or public access.

# **Rationale:**

Granting permissions to allUsers or allAuthenticatedUsers allows anyone to access the dataset. Such access might not be desirable if sensitive data is stored at the location. In this case, ensure that anonymous and/or public access to a Cloud KMS cryptokey is not allowed.

# Impact:

Removing the binding for allusers and allAuthenticatedUsers members denies accessing cryptokeys to anonymous or public users.

# Audit:

## **From Command Line:**

1. List all Cloud KMS Cryptokeys.

```
gcloud kms keys list --keyring=[key_ring_name] --location=global --
format=json | jq '.[].name'
```

2. Ensure the below command's output does not contain allUsers or allAuthenticatedUsers.

```
gcloud kms keys get-iam-policy [key_name] --keyring=[key_ring_name] --
location=global --format=json | jq '.bindings[].members[]'
```

## **Remediation:**

## From Command Line:

1. List all Cloud KMS Cryptokeys.

```
gcloud kms keys list --keyring=[key_ring_name] --location=global --
format=json | jq '.[].name'
```

2. Remove IAM policy binding for a KMS key to remove access to allusers and allAuthenticatedUsers using the below command.

```
gcloud kms keys remove-iam-policy-binding [key_name] --
keyring=[key_ring_name] --location=global --member='allAuthenticatedUsers' --
role='[role]'
gcloud kms keys remove-iam-policy-binding [key_name] --
keyring=[key ring name] --location=global --member='allUsers' --role='[role]'
```

# **Default Value:**

By default Cloud KMS does not allow access to allUsers or allAuthenticatedUsers.

# **References:**

- 1. <u>https://cloud.google.com/sdk/gcloud/reference/kms/keys/remove-iam-policy-binding</u>
- 2. <u>https://cloud.google.com/sdk/gcloud/reference/kms/keys/set-iam-policy</u>
- 3. <u>https://cloud.google.com/sdk/gcloud/reference/kms/keys/get-iam-policy</u>
- 4. <u>https://cloud.google.com/kms/docs/object-hierarchy#key\_resource\_id</u>

# Additional Information:

[key\_ring\_name] : Is the resource ID of the key ring, which is the fully-qualified Key ring name. This value is case-sensitive and in the form: projects/PROJECT\_ID/locations/LOCATION/keyRings/KEY\_RING

You can retrieve the key ring resource ID using the Cloud Console:

- 1. Open the Cryptographic Keys page in the Cloud Console.
- 2. For the key ring whose resource ID you are retrieving, click the More icon (3 vertical dots).
- 3. Click Copy Resource ID. The resource ID for the key ring is copied to your clipboard.

[key\_name] : Is the resource ID of the key, which is the fully-qualified CryptoKey name. This value is case-sensitive and in the form:

projects/PROJECT\_ID/locations/LOCATION/keyRings/KEY\_RING/cryptoKeys/KEY

You can retrieve the key resource ID using the Cloud Console:

1. Open the Cryptographic Keys page in the Cloud Console.

- 2. Click the name of the key ring that contains the key.
- 3. For the key whose resource ID you are retrieving, click the More icon (3 vertical dots).
- 4. Click Copy Resource ID. The resource ID for the key is copied to your clipboard.

[role] : The role to remove the member from.

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3</b> <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	•		
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	•	•	•

# 1.10 Ensure KMS Encryption Keys Are Rotated Within a Period of 90 Days (Automated)

# **Profile Applicability:**

• Level 1

# **Description:**

Google Cloud Key Management Service stores cryptographic keys in a hierarchical structure designed for useful and elegant access control management.

The format for the rotation schedule depends on the client library that is used. For the gcloud command-line tool, the next rotation time must be in ISO or RFC3339 format, and the rotation period must be in the form INTEGER[UNIT], where units can be one of seconds (s), minutes (m), hours (h) or days (d).

# **Rationale:**

Set a key rotation period and starting time. A key can be created with a specified rotation period, which is the time between when new key versions are generated automatically. A key can also be created with a specified next rotation time. A key is a named object representing a cryptographic key used for a specific purpose. The key material, the actual bits used for encryption, can change over time as new key versions are created.

A key is used to protect some corpus of data. A collection of files could be encrypted with the same key and people with decrypt permissions on that key would be able to decrypt those files. Therefore, it's necessary to make sure the rotation period is set to a specific time.

# Impact:

After a successful key rotation, the older key version is required in order to decrypt the data encrypted by that previous key version.

# Audit:

# From Console:

- Go to Cryptographic Keys by visiting: https://console.cloud.google.com/security/kms.
- 2. Click on each key ring, then ensure each key in the keyring has Next Rotation set for less than 90 days from the current date.

#### From Command Line:

1. Ensure rotation is scheduled by <code>ROTATION\_PERIOD</code> and <code>NEXT\_ROTATION\_TIME</code> for each key :

```
gcloud kms keys list --keyring=<KEY_RING> --location=<LOCATION> --
format=json'(rotationPeriod)'
```

Ensure outcome values for rotationPeriod and nextRotationTime satisfy the below criteria:

```
rotationPeriod is <= 129600m
rotationPeriod is <= 7776000s
rotationPeriod is <= 2160h
rotationPeriod is <= 90d
nextRotationTime is <= 90days from current DATE</pre>
```

#### **Remediation:**

#### From Console:

- Go to Cryptographic Keys by visiting: https://console.cloud.google.com/security/kms.
- 2. Click on the specific key ring
- 3. From the list of keys, choose the specific key and Click on Right side pop up the blade (3 dots).
- 4. Click on Edit rotation period.
- 5. On the pop-up window, Select a new rotation period in days which should be less than 90 and then choose Starting on date (date from which the rotation period begins).

#### From Command Line:

1. Update and schedule rotation by ROTATION\_PERIOD and NEXT\_ROTATION\_TIME for each key:

```
gcloud kms keys update new --keyring=KEY_RING --location=LOCATION --next-
rotation-time=NEXT_ROTATION_TIME --rotation-period=ROTATION_PERIOD
```

#### **Default Value:**

By default, KMS encryption keys are rotated every 90 days.

#### **References:**

- 1. <u>https://cloud.google.com/kms/docs/key-rotation#frequency of key rotation</u>
- 2. https://cloud.google.com/kms/docs/re-encrypt-data

#### Additional Information:

- Key rotation does NOT re-encrypt already encrypted data with the newly generated key version. If you suspect unauthorized use of a key, you should re-encrypt the data protected by that key and then disable or schedule destruction of the prior key version.
- It is not recommended to rely solely on irregular rotation, but rather to use irregular rotation if needed in conjunction with a regular rotation schedule.

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		•	•
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			•

# 1.11 Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users (Automated)

# **Profile Applicability:**

• Level 2

# **Description**:

It is recommended that the principle of 'Separation of Duties' is enforced while assigning KMS related roles to users.

# **Rationale:**

The built-in/predefined IAM role Cloud KMS Admin allows the user/identity to create, delete, and manage service account(s). The built-in/predefined IAM role Cloud KMS CryptoKey Encrypter/Decrypter allows the user/identity (with adequate privileges on concerned resources) to encrypt and decrypt data at rest using an encryption key(s).

The built-in/predefined IAM role Cloud KMS CryptoKey Encrypter allows the user/identity (with adequate privileges on concerned resources) to encrypt data at rest using an encryption key(s). The built-in/predefined IAM role Cloud KMS CryptoKey Decrypter allows the user/identity (with adequate privileges on concerned resources) to decrypt data at rest using an encryption key(s).

Separation of duties is the concept of ensuring that one individual does not have all necessary permissions to be able to complete a malicious action. In Cloud KMS, this could be an action such as using a key to access and decrypt data a user should not normally have access to. Separation of duties is a business control typically used in larger organizations, meant to help avoid security or privacy incidents and errors. It is considered best practice.

No user(s) should have Cloud KMS Admin and any of the Cloud KMS CryptoKey Encrypter/Decrypter, Cloud KMS CryptoKey Encrypter, Cloud KMS CryptoKey Decrypter roles assigned at the same time.

# Impact:

Removed roles should be assigned to another user based on business needs.

# Audit:

## From Console:

- 1. Go to IAM & Admin/IAM by visiting: <u>https://console.cloud.google.com/iam-admin/iam</u>
- 2. Ensure no member has the roles Cloud KMS Admin and any of the Cloud KMS CryptoKey Encrypter/Decrypter, Cloud KMS CryptoKey Encrypter, Cloud KMS CryptoKey Decrypter assigned.

#### From Command Line:

1. List all users and role assignments:

gcloud projects get-iam-policy PROJECT\_ID

2. Ensure that there are no common users found in the member section for roles cloudkms.admin and any one of Cloud KMS CryptoKey Encrypter, Cloud KMS CryptoKey Encrypter, Cloud KMS CryptoKey Decrypter

## **Remediation:**

#### From Console:

- 1. Go to IAM & Admin/IAM using https://console.cloud.google.com/iam-admin/iam
- 2. For any member having Cloud KMS Admin and any of the Cloud KMS CryptoKey Encrypter/Decrypter, Cloud KMS CryptoKey Encrypter, Cloud KMS CryptoKey Decrypter roles granted/assigned, click the Delete Bin icon to remove the role from the member.

Note: Removing a role should be done based on the business requirement.

#### **References:**

1. <u>https://cloud.google.com/kms/docs/separation-of-duties</u>

## Additional Information:

Users granted with Owner (roles/owner) and Editor (roles/editor) have privileges equivalent to Cloud KMS Admin and Cloud KMS CryptoKey Encrypter/Decrypter. To avoid misuse, Owner and Editor roles should be granted to a very limited group of users. Use of these primitive privileges should be minimal. These requirements are addressed in separate recommendations.

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3</b> <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	٠	•	•
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	•	•	•

# 1.12 Ensure API Keys Are Not Created for a Project (Manual)

# **Profile Applicability:**

• Level 2

# **Description**:

Keys are insecure because they can be viewed publicly, such as from within a browser, or they can be accessed on a device where the key resides. It is recommended to use standard authentication flow instead.

## **Rationale:**

Security risks involved in using API-Keys appear below:

- API keys are simple encrypted strings
- API keys do not identify the user or the application making the API request
- API keys are typically accessible to clients, making it easy to discover and steal an API key

To avoid the security risk in using API keys, it is recommended to use standard authentication flow instead.

## Impact:

Deleting an API key will break dependent applications (if any).

## Audit:

## From Console:

- 1. Go to APIs & Services\Credentials using
   https://console.cloud.google.com/apis/credentials
- 2. In the section API Keys, no API key should be listed.

## **Remediation:**

## From Console:

- Go to APIs & Services\Credentials using https://console.cloud.google.com/apis/credentials
- 2. In the section API Keys, to delete API Keys: Click the Delete Bin Icon in front of every API Key Name.

# **References:**

1. <u>https://cloud.google.com/docs/authentication/api-keys</u>

# Additional Information:

Google recommends using the standard authentication flow instead of using API keys. However, there are limited cases where API keys are more appropriate. For example, if there is a mobile application that needs to use the Google Cloud Translation API, but doesn't otherwise need a backend server, API keys are the simplest way to authenticate to that API.

If a business requires API keys to be used, then the API keys should be secured properly.

# 1.13 Ensure API Keys Are Restricted To Use by Only Specified Hosts and Apps (Manual)

# Profile Applicability:

• Level 1

# **Description**:

Unrestricted keys are insecure because they can be viewed publicly, such as from within a browser, or they can be accessed on a device where the key resides. It is recommended to restrict API key usage to trusted hosts, HTTP referrers and apps.

# **Rationale:**

Security risks involved in using API-Keys appear below:

- API keys are simple encrypted strings
- API keys do not identify the user or the application making the API request
- API keys are typically accessible to clients, making it easy to discover and steal an API key

In light of these potential risks, Google recommends using the standard authentication flow instead of API keys. However, there are limited cases where API keys are more appropriate. For example, if there is a mobile application that needs to use the Google Cloud Translation API, but doesn't otherwise need a backend server, API keys are the simplest way to authenticate to that API.

In order to reduce attack vectors, API-Keys can be restricted only to trusted hosts, HTTP referrers and applications.

# Impact:

Setting Application Restrictions may break existing application functioning, if not done carefully.

# Audit:

# From Console:

- 1. Go to APIs & Services\Credentials using
   https://console.cloud.google.com/apis/credentials
- 2. In the section API Keys, Click the API Key Name. The API Key properties display on a new page.

3. For every API Key, ensure the section Key restrictions parameter Application restrictions is not set to None.

0r,

 $Ensure \; \texttt{Application restrictions} \; is \; set to \; \texttt{HTTP referrers} \; and \; the \; referrer \; is \; not \; set to \;$ 

 $wild\text{-}cards\;(* \text{ or }*.[\texttt{TLD}] \text{ or }*.[\texttt{TLD}]/*)$  allowing access to any/wide <code>HTTP</code> referrer(s)

## 0r,

Ensure Application restrictions is set to IP addresses and referrer is not set to any host (0.0.0.0 or 0.0.0/0 or ::0)

# **Remediation:**

# From Console:

- 1. Go to APIs & Services\Credentials using
   https://console.cloud.google.com/apis/credentials
- 2. In the section API Keys, Click the API Key Name. The API Key properties display on a new page.
- 3. In the Key restrictions section, set the application restrictions to any of HTTP referrers, IP addresses, Android apps, iOS apps.
- 4. Click Save.
- 5. Repeat steps 2,3,4 for every unrestricted API key. Note: Do not set HTTP referrers to wild-cards (\* or \*.[TLD] or .[TLD]/) allowing access to any/wide HTTP referrer(s) Do not set IP addresses and referrer to any host (0.0.0.0 or 0.0.0.0/0 or ::0)

# **Default Value:**

By default, Application Restrictions are set to None.

## **References:**

1. <u>https://cloud.google.com/docs/authentication/api-keys</u>

# 1.14 Ensure API Keys Are Restricted to Only APIs That Application Needs Access (Manual)

# Profile Applicability:

• Level 1

# **Description**:

API keys are always at risk because they can be viewed publicly, such as from within a browser, or they can be accessed on a device where the key resides. It is recommended to restrict API keys to use (call) only APIs required by an application.

# **Rationale:**

Security risks involved in using API-Keys are below:

- API keys are simple encrypted strings
- API keys do not identify the user or the application making the API request
- API keys are typically accessible to clients, making it easy to discover and steal an API key

In light of these potential risks, Google recommends using the standard authentication flow instead of API-Keys. However, there are limited cases where API keys are more appropriate. For example, if there is a mobile application that needs to use the Google Cloud Translation API, but doesn't otherwise need a backend server, API keys are the simplest way to authenticate to that API.

In order to reduce attack surfaces by providing least privileges, API-Keys can be restricted to use (call) only APIs required by an application.

# Impact:

Setting API restrictions may break existing application functioning, if not done carefully.

# Audit:

# From Console:

- Go to APIs & Services\Credentials using https://console.cloud.google.com/apis/credentials
- 2. In the section API Keys, Click the API Key Name. The API Key properties display on a new page.

3. For every API Key, ensure the section Key restrictions parameter API restrictions is not set to None.

0r,

 $Ensure \, \texttt{API} \ \texttt{restrictions} \ is \ not \ set \ to \ \texttt{Google} \ \texttt{Cloud} \ \texttt{APIs}$ 

**Note:** Google Cloud APIs represents the API collection of all cloud services/APIs offered by Google cloud.

## **Remediation:**

## From Console:

- Go to APIs & Services\Credentials using https://console.cloud.google.com/apis/credentials
- 2. In the section API Keys, Click the API Key Name. The API Key properties display on a new page.
- 3. In the Key restrictions section go to API restrictions.
- 4. Click the Select API drop-down to choose an API.
- 5. Click Save.
- 6. Repeat steps 2,3,4,5 for every unrestricted API key

Note: Do not set API restrictions to Google Cloud APIs, as this option allows access to all services offered by Google cloud.

## **Default Value:**

By default, API restrictions are set to None.

## **References:**

- 1. <u>https://cloud.google.com/docs/authentication/api-keys</u>
- 2. <u>https://cloud.google.com/apis/docs/overview</u>

# 1.15 Ensure API Keys Are Rotated Every 90 Days (Manual)

# **Profile Applicability:**

• Level 1

# **Description**:

It is recommended to rotate API keys every 90 days.

# **Rationale:**

Security risks involved in using API-Keys are listed below:

- API keys are simple encrypted strings
- API keys do not identify the user or the application making the API request
- API keys are typically accessible to clients, making it easy to discover and steal an API key

Because of these potential risks, Google recommends using the standard authentication flow instead of API Keys. However, there are limited cases where API keys are more appropriate. For example, if there is a mobile application that needs to use the Google Cloud Translation API, but doesn't otherwise need a backend server, API keys are the simplest way to authenticate to that API.

Once a key is stolen, it has no expiration, meaning it may be used indefinitely unless the project owner revokes or regenerates the key. Rotating API keys will reduce the window of opportunity for an access key that is associated with a compromised or terminated account to be used.

API keys should be rotated to ensure that data cannot be accessed with an old key that might have been lost, cracked, or stolen.

## Impact:

Regenerating Key may break existing client connectivity as the client will try to connect with older API keys they have stored on devices.

## Audit:

## From Console:

1. Go to APIs & Services\Credentials using
 https://console.cloud.google.com/apis/credentials

2. In the section API Keys, for every key ensure the creation date is less than 90 days.

# **Remediation:**

#### From Console:

- 1. Go to APIs & Services\Credentials using
   https://console.cloud.google.com/apis/credentials
- 2. In the section API Keys, Click the API Key Name. The API Key properties display on a new page.
- 3. Click regenerate key to rotate API key.
- 4. Click Save.
- 5. Repeat steps 2,3,4 for every API key that has not been rotated in the last 90 days.

**Note:** Do not set HTTP referrers to wild-cards (\* or \*.[TLD] or *.[TLD]/*) allowing access to any/wide HTTP referrer(s)

Do not set IP addresses and referrer to any host (0.0.0.0 or 0.0.0.0/0 or ::0)

## **References:**

1. There is no option to automatically regenerate (rotate) API keys periodically.

# 1.16 Ensure Essential Contacts is Configured for Organization (Automated)

# **Profile Applicability:**

• Level 1

# **Description**:

It is recommended that Essential Contacts is configured to designate email addresses for Google Cloud services to notify of important technical or security information.

# **Rationale:**

Many Google Cloud services, such as Cloud Billing, send out notifications to share important information with Google Cloud users. By default, these notifications are sent to members with certain Identity and Access Management (IAM) roles. With Essential Contacts, you can customize who receives notifications by providing your own list of contacts.

## Impact:

There is no charge for Essential Contacts.

# Audit:

# From Console:

- Go to Essential Contacts by visiting <u>https://console.cloud.google.com/iam-admin/essential-contacts</u>
- 2. Make sure the organization appears in the resource selector at the top of the page. The resource selector tells you what project, folder, or organization you are currently managing contacts for.
- 3. Ensure that appropriate email addresses are configured for each of the following notification categories:

```
LegalSecurity
```

Suspension

```
•
Technical
```

54 | P a g e

Technical Incidents

Alternatively, appropriate email addresses can be configured for the All notification category to receive all possible important notifications. **From Command Line:** 

## From command Line.

1. To list all configured organization Essential Contacts run a command:

gcloud essential-contacts list --organization=<ORGANIZATION\_ID>

- 2. Ensure at least one appropriate email address is configured for each of the following notification categories:
- LEGAL SECURITY SUSPENSION TECHNICAL
  - TECHNICAL INCIDENTS

Alternatively, appropriate email addresses can be configured for the ALL notification category to receive all possible important notifications.

# **Remediation:**

# From Console:

- Go to Essential Contacts by visiting <u>https://console.cloud.google.com/iam-admin/essential-contacts</u>
- 2. Make sure the organization appears in the resource selector at the top of the page. The resource selector tells you what project, folder, or organization you are currently managing contacts for.
- 3. Click +Add contact
- 4. In the Email and Confirm Email fields, enter the email address of the contact.
- 5. From the Notification categories drop-down menu, select the notification categories that you want the contact to receive communications for.
- 6. Click Save

# From Command Line:

1. To add an organization Essential Contacts run a command:

```
gcloud essential-contacts create --email="<EMAIL>" \
    --notification-categories="<NOTIFICATION_CATEGORIES>" \
    --organization=<ORGANIZATION_ID>
```

## **Default Value:**

By default, there are no Essential Contacts configured.

In the absence of an Essential Contact, the following IAM roles are used to identify users to notify for the following categories:

- Legal: roles/billing.admin
- Security: roles/resourcemanager.organizationAdmin
- Suspension: roles/owner
- **Technical**: roles/owner
- Technical Incidents: roles/owner

#### **References:**

1. <u>https://cloud.google.com/resource-manager/docs/managing-notification-contacts</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	17.2 Establish and Maintain Contact Information for <u>Reporting Security Incidents</u> Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.		•	•
v7	19.5 <u>Maintain Contact Information For Reporting Security</u> <u>Incidents</u> Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.	•	•	•

# 1.17 Ensure that Dataproc Cluster is encrypted using Customer-Managed Encryption Key (Automated)

# **Profile Applicability:**

• Level 2

# **Description**:

When you use Dataproc, cluster and job data is stored on Persistent Disks (PDs) associated with the Compute Engine VMs in your cluster and in a Cloud Storage staging bucket. This PD and bucket data is encrypted using a Google-generated data encryption key (DEK) and key encryption key (KEK). The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK).

# **Rationale:**

"Cloud services offer the ability to protect data related to those services using encryption keys managed by the customer within Cloud KMS. These encryption keys are called customer-managed encryption keys (CMEK). When you protect data in Google Cloud services with CMEK, the CMEK key is within your control.

# Audit:

# **From Console**

- 1. Login to the GCP Console and navigate to the Dataproc Cluster page by visiting <u>https://console.cloud.google.com/dataproc/clusters</u>.
- 2. Select the project from the project dropdown list.
- 3. On the Dataproc Clusters page, select the cluster and click on the Name attribute value that you want to examine.
- 4. On the details page, select the Configurations tab.
- 5. On the Configurations tab, check the Encryption type configuration attribute value. If the value is set to Google-managed key, then Dataproc Cluster is not encrypted with Customer managed encryption keys.

Repeat step no. 3 - 5 for other Dataproc Clusters available in the selected project.

6. Change the project from the project dropdown list and repeat the audit procedure for other projects.

## **From Command Line**

1. Run clusters list command to list all the Dataproc Clusters available in the region:

gcloud dataproc clusters list --region='us-central1'

2. Run clusters describe command to get the key details of the selected cluster:

gcloud dataproc clusters describe <cluster\_name> --region=us-central1 -flatten=config.encryptionConfig.gcePdKmsKeyName

- 3. If the above command output return "null", then the selected cluster is not encrypted with Customer managed encryption keys.
- 4. Repeat step no. 2 and 3 for other Dataproc Clusters available in the selected region. Change the region by updating --region and repeat step no. 2 for other clusters available in the project. Change the project by running the below command and repeat the audit procedure for other Dataproc clusters available in other projects:

gcloud config set project <project\_ID>"

#### **Remediation:**

#### From Console

- 1. Login to the GCP Console and navigate to the Dataproc Cluster page by visiting <u>https://console.cloud.google.com/dataproc/clusters</u>.
- 2. Select the project from the projects dropdown list.
- 3. On the Dataproc Cluster page, click on the Create Cluster to create a new cluster with Customer managed encryption keys.
- 4. On Create a cluster page, perform below steps:
- Inside Set up cluster section perform below steps: -In the Name textbox, provide a name for your cluster.
  - From Location select the location in which you want to deploy a cluster.
  - Configure other configurations as per your requirements.
- Inside Configure Nodes and Customize cluster section configure the settings as per your requirements.
- Inside Manage security section, perform below steps:
  - o **From** Encryption, **select** Customer-managed key.
  - Select a customer-managed key from dropdown list.
  - Ensure that the selected KMS Key have Cloud KMS CryptoKey Encrypter/Decrypter role assign to Dataproc Cluster service account ("serviceAccount:service-<project\_number>@computesystem.iam.gserviceaccount.com").
  - Click on Create to create a cluster.

- Once the cluster is created migrate all your workloads from the older cluster to the new cluster and delete the old cluster by performing the below steps:
  - On the Clusters page, select the old cluster and click on Delete cluster.
  - On the Confirm deletion window, click on Confirm to delete the cluster.
  - Repeat step above for other Dataproc clusters available in the selected project.
- Change the project from the project dropdown list and repeat the remediation procedure for other Dataproc clusters available in other projects.

# **From Command Line**

Before creating cluster ensure that the selected KMS Key have Cloud KMS CryptoKey Encrypter/Decrypter role assign to Dataproc Cluster service account

("serviceAccount:service-<project\_number>@compute-system.iam.gserviceaccount.com"). Run clusters create command to create new cluster with customer-managed key:

```
gcloud dataproc clusters create <cluster_name> --region=us-central1 --gce-pd-
kms-key=<key_resource_name>
```

The above command will create a new cluster in the selected region.

Once the cluster is created migrate all your workloads from the older cluster to the new cluster and Run clusters delete command to delete cluster:

gcloud dataproc clusters delete <cluster\_name> --region=us-central1

Repeat step no. 1 to create a new Dataproc cluster.

Change the project by running the below command and repeat the remediation procedure for other projects:

gcloud config set project <project\_ID>"

#### **References:**

1. <u>https://cloud.google.com/docs/security/encryption/default-encryption</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		•	•

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

# 1.18 Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager (Manual)

# **Profile Applicability:**

• Level 1

# **Description**:

Google Cloud Functions allow you to host serverless code that is executed when an event is triggered, without the requiring the management a host operating system. These functions can also store environment variables to be used by the code that may contain authentication or other information that needs to remain confidential.

# **Rationale:**

It is recommended to use the Secret Manager, because environment variables are stored unencrypted, and accessible for all users who have access to the code.

## Impact:

There should be no impact on the Cloud Function. There are minor costs after 10,000 requests a month to the Secret Manager API as well for a high use of other functions. Modifying the Cloud Function to use the Secret Manager may prevent it running to completion as its environment variables are

## Audit:

# Determine if Confidential Information is Stored in your Functions in Cleartext From Console

- 1. Log in to the Google Cloud Web Portal (<u>https://console.cloud.google.com/</u>)
- 2. Within the project you wish to audit, select the Navigation hamburger menu in the top left. Scroll down to under the heading 'Serverless', then select 'Cloud Functions'
- 3. Click on a function name from the list
- 4. Open the Variables tab and you will see both buildEnvironmentVariables and environmentVariables
- 5. Review the variables whether they are secrets
- 6. Repeat step 3-5 until all functions are reviewed

## **From Command Line**

1. To view a list of your cloud functions run

2. For each cloud function in the list run the following command.

gcloud functions describe <function name>

3. Review the settings of the buildEnvironmentVariables and environmentVariables. Determine if this is data that should not be publicly accessible.

# Determine if Secret Manager API is 'Enabled' for your Project From Console

- 1. Within the project you wish to audit, select the Navigation hamburger menu in the top left. Hover over 'APIs & Services' to under the heading 'Serverless', then select 'Enabled APIs & Services' in the menu that opens up.
- 2. Click the button '+ Enable APIS and Services'
- 3. In the Search bar, search for 'Secret Manager API' and select it.
- 4. If it is enabled, the blue box that normally says 'Enable' will instead say 'Manage'.

#### From Command Line

1. Within the project you wish to audit, run the following command.

gcloud services list

2. If 'Secret Manager API' is in the list, it is enabled.

#### **Remediation:**

# Enable Secret Manager API for your Project From Console

- 1. Within the project you wish to enable, select the Navigation hamburger menu in the top left. Hover over 'APIs & Services' to under the heading 'Serverless', then select 'Enabled APIs & Services' in the menu that opens up.
- 2. Click the button '+ Enable APIS and Services'
- 3. In the Search bar, search for 'Secret Manager API' and select it.
- 4. Click the blue box that says 'Enable'.

#### From Command Line

1. Within the project you wish to enable the API in, run the following command.

gcloud services enable Secret Manager API

# Reviewing Environment Variables That Should Be Migrated to Secret Manager From Console

- 1. Log in to the Google Cloud Web Portal (<u>https://console.cloud.google.com/</u>)
- 2. Go to Cloud Functions
- 3. Click on a function name from the list
- 4. Click on Edit and review the Runtime environment for variables that should be secrets. Leave this list open for the next step.

## **From Command Line**

1. To view a list of your cloud functions run

cloud functions list

2. For each cloud function run the following command.

gcloud functions describe <function\_name>

3. Review the settings of the buildEnvironmentVariables and environmentVariables. Keep this information for the next step.

# Migrating Environment Variables to Secrets within the Secret Manager From Console

- 1. Go to the Secret Manager page in the Cloud Console.
- 2. On the Secret Manager page, click Create Secret.
- 3. On the Create secret page, under Name, enter the name of the Environment Variable you are replacing. This will then be the Secret Variable you will reference in your code.
- 4. You will also need to add a version. This is the actual value of the variable that will be referenced from the code. To add a secret version when creating the initial secret, in the Secret value field, enter the value from the Environment Variable you are replacing.
- 5. Leave the Regions section unchanged.
- 6. Click the Create secret button.
- 7. Repeat for all Environment Variables

## From Command Line

 Run the following command with the Environment Variable name you are replacing in the <secret-id>. It is most secure to point this command to a file with the Environment Variable value located in it, as if you entered it via command line it would show up in your shell's command history.

# Granting your Runtime's Service Account Access to Secrets From Console

- 1. Within the project containing your runtime login with account that has the 'roles/secretmanager.secretAccessor' permission.
- 2. Select the Navigation hamburger menu in the top left. Hover over 'Security' to under the then select 'Secret Manager' in the menu that opens up.
- 3. Click the name of a secret listed in this screen.
- 4. If it is not already open, click Show Info Panel in this screen to open the panel.
  5.In the info panel, click Add principal.
  6.In the New principals field, enter the service account your function uses for its identity. (If you need help locating or updating your runtime's service account, please see the 'docs/securing/function-identity#runtime\_service\_account' reference.)
- 5. In the Select a role dropdown, choose Secret Manager and then Secret Manager Secret Accessor.

# **From Command Line**

As of the time of writing, using Google CLI to list Runtime variables is only in beta. Because this is likely to change we are not including it here.

# Modifying the Code to use the Secrets in Secret Manager

## From Console

This depends heavily on which language your runtime is in. For the sake of the brevity of this recommendation, please see the '/docs/creating-and-accessing-secrets#access' reference

for language specific instructions.

## From Command Line

This depends heavily on which language your runtime is in. For the sake of the brevity of this recommendation, please see the' /docs/creating-and-accessing-secrets#access' reference

for language specific instructions.

## **Deleting the Insecure Environment Variables**

# Be certain to do this step last. Removing variables from code actively referencing them will prevent it from completing successfully.

## From Console

- 1. Select the Navigation hamburger menu in the top left. Hover over 'Security' then select 'Secret Manager' in the menu that opens up.
- 2. Click the name of a function. Click Edit.
- 3. Click Runtime, build and connections settings to expand the advanced configuration options.

- 4. Click 'Security'. Hover over the secret you want to remove, then click 'Delete'.
- 5. Click Next. Click Deploy. The latest version of the runtime will now reference the secrets in Secret Manager.

## From Command Line

gcloud functions deploy <Function name>--remove-env-vars <env vars>

If you need to find the env vars to remove, they are from the step where 'gcloud functions describe <function name>' was run.

## **Default Value:**

By default Secret Manager is not enabled.

#### **References:**

- 1. <u>https://cloud.google.com/functions/docs/configuring/env-var#managing\_secrets</u>
- 2. <u>https://cloud.google.com/secret-manager/docs/overview</u>

#### Additional Information:

There are slight additional costs to using the Secret Manager API. Review the documentation to determine your organizations' needs.

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11</b> Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		•	•
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			•
v7	<b>16.4</b> <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.		•	•

# 2 Logging and Monitoring

This section covers recommendations addressing Logging and Monitoring on Google Cloud Platform.

# 2.1 Ensure That Cloud Audit Logging Is Configured Properly Across All Services and All Users From a Project (Automated)

# **Profile Applicability:**

• Level 1

# **Description**:

It is recommended that Cloud Audit Logging is configured to track all admin activities and read, write access to user data.

# **Rationale:**

Cloud Audit Logging maintains two audit logs for each project, folder, and organization: Admin Activity and Data Access.

- 1. Admin Activity logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. Admin Activity audit logs are enabled for all services and cannot be configured.
- 2. Data Access audit logs record API calls that create, modify, or read user-provided data. These are disabled by default and should be enabled.

There are three kinds of Data Access audit log information:

- Admin read: Records operations that read metadata or configuration information. Admin Activity audit logs record writes of metadata and configuration information that cannot be disabled.
- $\circ$   $\;$  Data read: Records operations that read user-provided data.
- Data write: Records operations that write user-provided data.

It is recommended to have an effective default audit config configured in such a way that:

- 1. logtype is set to DATA\_READ (to log user activity tracking) and DATA\_WRITES (to log changes/tampering to user data).
- 2. audit config is enabled for all the services supported by the Data Access audit logs feature.
- 3. Logs should be captured for all users, i.e., there are no exempted users in any of the audit config sections. This will ensure overriding the audit config will not contradict the requirement.

# Impact:

There is no charge for Admin Activity audit logs. Enabling the Data Access audit logs might result in your project being charged for the additional logs usage.

# Audit:

## From Console:

- 1. Go to Audit Logs by visiting <u>https://console.cloud.google.com/iam-admin/audit</u>.
- 2. Ensure that Admin Read, Data Write, and Data Read are enabled for all Google Cloud services and that no exemptions are allowed.

## From Command Line:

1. List the Identity and Access Management (IAM) policies for the project, folder, or organization:

```
gcloud organizations get-iam-policy ORGANIZATION_ID
gcloud resource-manager folders get-iam-policy FOLDER_ID
gcloud projects get-iam-policy PROJECT ID
```

2. Policy should have a default auditConfigs section which has the logtype set to DATA\_WRITES and DATA\_READ for all services. Note that projects inherit settings from folders, which in turn inherit settings from the organization. When called, projects get-iam-policy, the result shows only the policies set in the project, not the policies inherited from the parent folder or organization. Nevertheless, if the parent folder has Cloud Audit Logging enabled, the project does as well.

Sample output for default audit configs may look like this:

auditConfigs: - auditLogConfigs: - logType: ADMIN\_READ - logType: DATA\_WRITE - logType: DATA\_READ service: allServices

3. Any of the auditConfigs sections should not have parameter "exemptedMembers:" set, which will ensure that Logging is enabled for all users and no user is exempted.

## **Remediation:**

## From Console:

1. Go to Audit Logs by visiting <u>https://console.cloud.google.com/iam-admin/audit</u>.

2. Follow the steps at <u>https://cloud.google.com/logging/docs/audit/configure-data-access</u> to enable audit logs for all Google Cloud services. Ensure that no exemptions are allowed.

# **From Command Line:**

1. To read the project's IAM policy and store it in a file run a command:

gcloud projects get-iam-policy PROJECT\_ID > /tmp/project\_policy.yaml

Alternatively, the policy can be set at the organization or folder level. If setting the policy at the organization level, it is not necessary to also set it for each folder or project.

```
gcloud organizations get-iam-policy ORGANIZATION_ID > /tmp/org_policy.yaml
gcloud resource-manager folders get-iam-policy FOLDER_ID >
/tmp/folder policy.yaml
```

 Edit policy in /tmp/policy.yaml, adding or changing only the audit logs configuration to: Note: Admin Activity Logs are enabled by default, and cannot be disabled. So they are not listed in these configuration changes.

```
auditConfigs:
- auditLogConfigs:
- logType: DATA_WRITE
- logType: DATA_READ
service: allServices
```

Note: exemptedMembers: is not set as audit logging should be enabled for all the users

3. To write new IAM policy run command:

```
gcloud organizations set-iam-policy ORGANIZATION_ID /tmp/org_policy.yaml
gcloud resource-manager folders set-iam-policy FOLDER_ID
/tmp/folder_policy.yaml
gcloud projects set-iam-policy PROJECT ID /tmp/project policy.yaml
```

If the preceding command reports a conflict with another change, then repeat these steps, starting with the first step.

# **Default Value:**

Admin Activity logs are always enabled. They cannot be disabled. Data Access audit logs are disabled by default because they can be quite large.

#### **References:**

- 1. <u>https://cloud.google.com/logging/docs/audit/</u>
- 2. <u>https://cloud.google.com/logging/docs/audit/configure-data-access</u>

#### **Additional Information:**

- Log type DATA\_READ is equally important to that of DATA\_WRITE to track detailed user activities.
- BigQuery Data Access logs are handled differently from other data access logs. BigQuery logs are enabled by default and cannot be disabled. They do not count against logs allotment and cannot result in extra logs charges.

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	•	•	•
v8	8.11 <u>Conduct Audit Log Reviews</u> Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		•	•
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.	•	•	•
v7	6.7 <u>Regularly Review Logs</u> On a regular basis, review logs to identify anomalies or abnormal events.		•	•

# 2.2 Ensure That Sinks Are Configured for All Log Entries (Automated)

# **Profile Applicability:**

• Level 1

# **Description**:

It is recommended to create a sink that will export copies of all the log entries. This can help aggregate logs from multiple projects and export them to a Security Information and Event Management (SIEM).

# **Rationale:**

Log entries are held in Cloud Logging. To aggregate logs, export them to a SIEM. To keep them longer, it is recommended to set up a log sink. Exporting involves writing a filter that selects the log entries to export, and choosing a destination in Cloud Storage, BigQuery, or Cloud Pub/Sub. The filter and destination are held in an object called a sink. To ensure all log entries are exported to sinks, ensure that there is no filter configured for a sink. Sinks can be created in projects, organizations, folders, and billing accounts.

#### Impact:

There are no costs or limitations in Cloud Logging for exporting logs, but the export destinations charge for storing or transmitting the log data.

## Audit:

## From Console:

- 1. Go to Logs Router by visiting <u>https://console.cloud.google.com/logs/router</u>.
- 2. For every sink, click the 3-dot button for Menu options and select <code>View sink details</code>.
- 3. Ensure there is at least one sink with an empty Inclusion filter.
- 4. Additionally, ensure that the resource configured as Destination exists.

## **From Command Line:**

1. Ensure that a sink with an empty filter exists. List the sinks for the project, folder or organization. If sinks are configured at a folder or organization level, they do not need to be configured for each project:

```
gcloud logging sinks list --folder=FOLDER_ID | --organization=ORGANIZATION_ID
| --project=PROJECT_ID
```
The output should list at least one sink with an empty filter.

2. Additionally, ensure that the resource configured as Destination exists.

See <u>https://cloud.google.com/sdk/gcloud/reference/beta/logging/sinks/list</u> for more information.

# **Remediation:**

#### From Console:

- 1. Go to Logs Router by visiting <a href="https://console.cloud.google.com/logs/router">https://console.cloud.google.com/logs/router</a>.
- 2. Click on the arrow symbol with CREATE SINK text.
- 3. Fill out the fields for Sink details.
- 4. Choose Cloud Logging bucket in the Select sink destination drop down menu.
- 5. Choose a log bucket in the next drop down menu.
- 6. If an inclusion filter is not provided for this sink, all ingested logs will be routed to the destination provided above. This may result in higher than expected resource usage.
- 7. Click Create Sink.

For more information, see

https://cloud.google.com/logging/docs/export/configure\_export\_v2#dest-create.

#### From Command Line:

To create a sink to export all log entries in a Google Cloud Storage bucket:

```
gcloud logging sinks create <sink-name>
storage.googleapis.com/DESTINATION BUCKET NAME
```

Sinks can be created for a folder or organization, which will include all projects.

```
gcloud logging sinks create <sink-name>
storage.googleapis.com/DESTINATION_BUCKET_NAME --include-children --
folder=FOLDER ID | --organization=ORGANIZATION ID
```

#### Note:

- A sink created by the command-line above will export logs in storage buckets. However, sinks can be configured to export logs into BigQuery, or Cloud Pub/Sub, or Custom Destination.
- 2. While creating a sink, the sink option --log-filter is not used to ensure the sink exports all log entries.
- 3. A sink can be created at a folder or organization level that collects the logs of all the projects underneath bypassing the option --include-children in the gcloud command.

# **Default Value:**

By default, there are no sinks configured.

#### **References:**

- 1. <u>https://cloud.google.com/logging/docs/reference/tools/gcloud-logging</u>
- 2. <u>https://cloud.google.com/logging/quotas</u>
- 3. <u>https://cloud.google.com/logging/docs/routing/overview</u>
- 4. <u>https://cloud.google.com/logging/docs/export/using\_exported\_logs</u>
- 5. <u>https://cloud.google.com/logging/docs/export/configure\_export\_v2</u>
- 6. <u>https://cloud.google.com/logging/docs/export/aggregated exports</u>
- 7. <u>https://cloud.google.com/sdk/gcloud/reference/beta/logging/sinks/list</u>

#### **Additional Information:**

For Command-Line Audit and Remediation, the sink destination of type Cloud Storage Bucket is considered. However, the destination could be configured to Cloud Storage Bucket or BigQuery or Cloud Pub\Sub or Custom Destination. Command Line Interface commands would change accordingly.

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	•	•	•
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.		•	•
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.	•	•	•
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.		•	

# 2.3 Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock (Automated)

# Profile Applicability:

• Level 2

# **Description**:

Enabling retention policies on log buckets will protect logs stored in cloud storage buckets from being overwritten or accidentally deleted. It is recommended to set up retention policies and configure Bucket Lock on all storage buckets that are used as log sinks.

# **Rationale:**

Logs can be exported by creating one or more sinks that include a log filter and a destination. As Cloud Logging receives new log entries, they are compared against each sink. If a log entry matches a sink's filter, then a copy of the log entry is written to the destination.

Sinks can be configured to export logs in storage buckets. It is recommended to configure a data retention policy for these cloud storage buckets and to lock the data retention policy; thus permanently preventing the policy from being reduced or removed. This way, if the system is ever compromised by an attacker or a malicious insider who wants to cover their tracks, the activity logs are definitely preserved for forensics and security investigations.

# Impact:

Locking a bucket is an irreversible action. Once you lock a bucket, you cannot remove the retention policy from the bucket or decrease the retention period for the policy. You will then have to wait for the retention period for all items within the bucket before you can delete them, and then the bucket.

# Audit:

# From Console:

- 1. Open the Cloud Storage browser in the Google Cloud Console by visiting <u>https://console.cloud.google.com/storage/browser</u>.
- 2. In the Column display options menu, make sure Retention policy is checked.
- 3. In the list of buckets, the retention period of each bucket is found in the Retention policy column. If the retention policy is locked, an image of a lock appears directly to the left of the retention period.

#### From Command Line:

1. To list all sinks destined to storage buckets:

```
gcloud logging sinks list --folder=FOLDER_ID | --organization=ORGANIZATION_ID
| --project=PROJECT ID
```

2. For every storage bucket listed above, verify that retention policies and Bucket Lock are enabled:

gsutil retention get gs://BUCKET\_NAME

For more information, see <u>https://cloud.google.com/storage/docs/using-bucket-lock#view-policy</u>.

#### **Remediation:**

#### From Console:

- 1. If sinks are **not** configured, first follow the instructions in the recommendation: Ensure that sinks are configured for all Log entries.
- 2. For each storage bucket configured as a sink, go to the Cloud Storage browser at https://console.cloud.google.com/storage/browser/<BUCKET NAME>.
- 3. Select the Bucket Lock tab near the top of the page.
- 4. In the Retention policy entry, click the Add Duration link. The set a retention policy dialog box appears.
- 5. Enter the desired length of time for the retention period and click <code>Save policy</code>.
- 6. Set the Lock status for this retention policy to Locked.

#### From Command Line:

1. To list all sinks destined to storage buckets:

```
gcloud logging sinks list --folder=FOLDER_ID | --organization=ORGANIZATION_ID
| --project=PROJECT ID
```

2. For each storage bucket listed above, set a retention policy and lock it:

```
gsutil retention set [TIME_DURATION] gs://[BUCKET_NAME]
gsutil retention lock gs://[BUCKET_NAME]
```

For more information, visit <u>https://cloud.google.com/storage/docs/using-bucket-lock#set-policy</u>.

# **Default Value:**

By default, storage buckets used as log sinks do not have retention policies and Bucket Lock configured.

#### **References:**

- 1. <u>https://cloud.google.com/storage/docs/bucket-lock</u>
- 2. <u>https://cloud.google.com/storage/docs/using-bucket-lock</u>
- 3. <u>https://cloud.google.com/storage/docs/bucket-lock</u>

#### **Additional Information:**

Caution: Locking a retention policy is an irreversible action. Once locked, you must delete the entire bucket in order to "remove" the bucket's retention policy. However, before you can delete the bucket, you must be able to delete all the objects in the bucket, which itself is only possible if all the objects have reached the retention period set by the retention policy.

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3</b> <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	٠	•	
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	•	•	•

# 2.4 Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes (Automated)

# **Profile Applicability:**

• Level 1

# **Description**:

In order to prevent unnecessary project ownership assignments to users/service-accounts and further misuses of projects and resources, all <code>roles/Owner</code> assignments should be monitored.

Members (users/Service-Accounts) with a role assignment to primitive role roles/Owner are project owners.

The project owner has all the privileges on the project the role belongs to. These are summarized below:

```
All viewer permissions on all GCP Services within the project
Permissions for actions that modify the state of all GCP services within the project
Manage roles and permissions for a project and all resources within the project
Set up billing for a project
```

Granting the owner role to a member (user/Service-Account) will allow that member to modify the Identity and Access Management (IAM) policy. Therefore, grant the owner role only if the member has a legitimate purpose to manage the IAM policy. This is because the project IAM policy contains sensitive access control data. Having a minimal set of users allowed to manage IAM policy will simplify any auditing that may be necessary.

# **Rationale:**

Project ownership has the highest level of privileges on a project. To avoid misuse of project resources, the project ownership assignment/change actions mentioned above should be monitored and alerted to concerned recipients.

```
Sending project ownership invites
Acceptance/Rejection of project ownership invite by user
Adding `role\Owner` to a user/service-account
Removing a user/Service account from `role\Owner`
```

# Impact:

Enabling of logging may result in your project being charged for the additional logs usage.

#### Audit:

# From Console: Ensure that the prescribed log metric is present:

- 1. Go to Logging/Log-based Metrics by visiting https://console.cloud.google.com/logs/metrics.
- 2. In the User-defined Metrics section, ensure that at least one metric <Log\_Metric\_Name> is present with filter text:

```
(protoPayload.serviceName="cloudresourcemanager.googleapis.com")
AND (ProjectOwnership OR projectOwnerInvitee)
OR (protoPayload.serviceData.policyDelta.bindingDeltas.action="REMOVE"
AND protoPayload.serviceData.policyDelta.bindingDeltas.role="roles/owner")
OR (protoPayload.serviceData.policyDelta.bindingDeltas.action="ADD"
AND protoPayload.serviceData.policyDelta.bindingDeltas.action="roles/owner")
```

# Ensure that the prescribed Alerting Policy is present:

- 3. Go to Alerting by visiting <a href="https://console.cloud.google.com/monitoring/alerting">https://console.cloud.google.com/monitoring/alerting</a>.
- 4. Under the Policies section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a threshold of zero(0) for greater than zero(0) seconds means that the alert will trigger for any new owner change. Verify that the chosen alerting thresholds make sense for your organization.
- 5. Ensure that the appropriate notifications channels have been set up.

# From Command Line: Ensure that the prescribed log metric is present:

1. List the log metrics:

gcloud beta logging metrics list --format json

2. Ensure that the output contains at least one metric with filter set to:

```
(protoPayload.serviceName="cloudresourcemanager.googleapis.com")
AND (ProjectOwnership OR projectOwnerInvitee)
OR (protoPayload.serviceData.policyDelta.bindingDeltas.action="REMOVE"
AND protoPayload.serviceData.policyDelta.bindingDeltas.role="roles/owner")
OR (protoPayload.serviceData.policyDelta.bindingDeltas.action="ADD"
AND protoPayload.serviceData.policyDelta.bindingDeltas.action="ADD"
```

3. Note the value of the property metricDescriptor.type for the identified metric, in the format logging.googleapis.com/user/<Log Metric Name>.

# Ensure that the prescribed alerting policy is present:

4. List the alerting policies:

gcloud alpha monitoring policies list --format json

- 5. Ensure that the output contains an least one alert policy where:
- conditions.conditionThreshold.filter is set to metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"
- AND enabled is set to true

# **Remediation:**

#### From Console: Create the prescribed log metric:

- Go to Logging/Logs-based Metrics by visiting <u>https://console.cloud.google.com/logs/metrics</u> and click "CREATE METRIC".
- 2. Click the down arrow symbol on the Filter Bar at the rightmost corner and select Convert to Advanced Filter.
- 3. Clear any text and add:

```
(protoPayload.serviceName="cloudresourcemanager.googleapis.com")
AND (ProjectOwnership OR projectOwnerInvitee)
OR (protoPayload.serviceData.policyDelta.bindingDeltas.action="REMOVE"
```

```
AND protoPayload.serviceData.policyDelta.bindingDeltas.role="roles/owner")
OR (protoPayload.serviceData.policyDelta.bindingDeltas.action="ADD"
AND protoPayload.serviceData.policyDelta.bindingDeltas.role="roles/owner")
```

- 4. Click Submit Filter. The logs display based on the filter text entered by the user.
- 5. In the Metric Editor menu on the right, fill out the name field. Set Units to 1 (default) and the Type to Counter. This ensures that the log metric counts the number of log entries matching the advanced logs query.
- 6. Click Create Metric.

# Create the display prescribed Alert Policy:

- 1. Identify the newly created metric under the section User-defined Metrics at <a href="https://console.cloud.google.com/logs/metrics">https://console.cloud.google.com/logs/metrics</a>.
- 2. Click the 3-dot icon in the rightmost column for the desired metric and select Create alert from Metric. A new page opens.
- 3. Fill out the alert policy configuration and click Save. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a threshold of zero(0) for the most recent value will ensure that a notification is triggered for every owner change in the project:

```
Set `Aggregator` to `Count`
Set `Configuration`:
- Condition: above
- Threshold: 0
- For: most recent value
```

- 4. Configure the desired notifications channels in the section Notifications.
- 5. Name the policy and click <code>Save</code>.

# From Command Line:

Create a prescribed Log Metric:

- Use the command: gcloud beta logging metrics create
- Reference for Command Usage: <u>https://cloud.google.com/sdk/gcloud/reference/beta/logging/metrics/create</u>

Create prescribed Alert Policy

- Use the command: gcloud alpha monitoring policies create
- Reference for Command Usage: <u>https://cloud.google.com/sdk/gcloud/reference/alpha/monitoring/policies/create</u>

#### **References:**

- 1. <u>https://cloud.google.com/logging/docs/logs-based-metrics/</u>
- 2. <u>https://cloud.google.com/monitoring/custom-metrics/</u>
- 3. <u>https://cloud.google.com/monitoring/alerts/</u>
- 4. <u>https://cloud.google.com/logging/docs/reference/tools/gcloud-logging</u>

#### Additional Information:

- 1. Project ownership assignments for a user cannot be done using the gcloud utility as assigning project ownership to a user requires sending, and the user accepting, an invitation.
- 2. Project Ownership assignment to a service account does not send any invites. SetIAMPolicy to role/owneris directly performed on service accounts.

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.		•	

# 2.5 Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes (Automated)

# **Profile Applicability:**

• Level 1

# **Description**:

Google Cloud Platform (GCP) services write audit log entries to the Admin Activity and Data Access logs to help answer the questions of, "who did what, where, and when?" within GCP projects.

Cloud audit logging records information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by GCP services. Cloud audit logging provides a history of GCP API calls for an account, including API calls made via the console, SDKs, command-line tools, and other GCP services.

# **Rationale:**

Admin activity and data access logs produced by cloud audit logging enable security analysis, resource change tracking, and compliance auditing.

Configuring the metric filter and alerts for audit configuration changes ensures the recommended state of audit configuration is maintained so that all activities in the project are audit-able at any point in time.

# Impact:

Enabling of logging may result in your project being charged for the additional logs usage.

# Audit:

# From Console: Ensure the prescribed log metric is present:

- 1. Go to Logging/Logs-based Metrics by visiting https://console.cloud.google.com/logs/metrics.
- 2. In the User-defined Metrics section, ensure that at least one metric <Log\_Metric\_Name> is present with the filter text:

```
protoPayload.methodName="SetIamPolicy" AND
protoPayload.serviceData.policyDelta.auditConfigDeltas:*
```

# Ensure that the prescribed alerting policy is present:

- 3. Go to Alerting by visiting <a href="https://console.cloud.google.com/monitoring/alerting">https://console.cloud.google.com/monitoring/alerting</a>.
- 4. Under the Policies section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a threshold of 0 for greater than zero(0) seconds, means that the alert will trigger for any new owner change. Verify that the chosen alerting thresholds make sense for the user's organization.
- 5. Ensure that appropriate notifications channels have been set up.

# From Command Line: Ensure that the prescribed log metric is present:

1. List the log metrics:

gcloud beta logging metrics list --format json

2. Ensure that the output contains at least one metric with the filter set to:

protoPayload.methodName="SetIamPolicy" AND protoPayload.serviceData.policyDelta.auditConfigDeltas:\*

3. Note the value of the property metricDescriptor.type for the identified metric, in the format logging.googleapis.com/user/<Log Metric Name>.

#### Ensure that the prescribed alerting policy is present:

4. List the alerting policies:

gcloud alpha monitoring policies list --format json

- 5. Ensure that the output contains at least one alert policy where:
- conditions.conditionThreshold.filter is set to metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"
- AND enabled is set to true

#### **Remediation:**

## From Console: Create the prescribed log metric:

 Go to Logging/Logs-based Metrics by visiting https://console.cloud.google.com/logs/metrics and click "CREATE METRIC".

- 2. Click the down arrow symbol on the Filter Bar at the rightmost corner and select Convert to Advanced Filter.
- 3. Clear any text and add:

```
protoPayload.methodName="SetIamPolicy" AND
protoPayload.serviceData.policyDelta.auditConfigDeltas:*
```

- 4. Click Submit Filter. Display logs appear based on the filter text entered by the user.
- 5. In the Metric Editor menu on the right, fill out the name field. Set Units to 1 (default) and Type to Counter. This will ensure that the log metric counts the number of log entries matching the user's advanced logs query.
- 6. Click Create Metric.

# **Create a prescribed Alert Policy:**

- 1. Identify the new metric the user just created, under the section User-defined Metrics at <a href="https://console.cloud.google.com/logs/metrics">https://console.cloud.google.com/logs/metrics</a>.
- 2. Click the 3-dot icon in the rightmost column for the new metric and select Create alert from Metric. A new page opens.
- 3. Fill out the alert policy configuration and click Save. Choose the alerting threshold and configuration that makes sense for the organization. For example, a threshold of zero(0) for the most recent value will ensure that a notification is triggered for every owner change in the project:

```
Set `Aggregator` to `Count`
Set `Configuration`:
- Condition: above
- Threshold: 0
- For: most recent value
```

- 4. Configure the desired notifications channels in the section Notifications.
- 5. Name the policy and click <code>Save</code>.

# From Command Line:

Create a prescribed Log Metric:

- Use the command: gcloud beta logging metrics create
- Reference for command usage: https://cloud.google.com/sdk/gcloud/reference/beta/logging/metrics/create

Create prescribed Alert Policy

• Use the command: gcloud alpha monitoring policies create

• Reference for command usage: <u>https://cloud.google.com/sdk/gcloud/reference/alpha/monitoring/policies/create</u>

#### **References:**

- 1. <u>https://cloud.google.com/logging/docs/logs-based-metrics/</u>
- 2. <u>https://cloud.google.com/monitoring/custom-metrics/</u>
- 3. <u>https://cloud.google.com/monitoring/alerts/</u>
- 4. <u>https://cloud.google.com/logging/docs/reference/tools/gcloud-logging</u>
- 5. <u>https://cloud.google.com/logging/docs/audit/configure-data-access#getiampolicy-setiampolicy</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	•	•	•
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	•
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.	•	•	
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		•	

# 2.6 Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes (Automated)

# **Profile Applicability:**

• Level 1

# **Description**:

It is recommended that a metric filter and alarm be established for changes to Identity and Access Management (IAM) role creation, deletion and updating activities.

# **Rationale:**

Google Cloud IAM provides predefined roles that give granular access to specific Google Cloud Platform resources and prevent unwanted access to other resources. However, to cater to organization-specific needs, Cloud IAM also provides the ability to create custom roles. Project owners and administrators with the Organization Role Administrator role or the IAM Role Administrator role can create custom roles. Monitoring role creation, deletion and updating activities will help in identifying any over-privileged role at early stages.

# Impact:

Enabling of logging may result in your project being charged for the additional logs usage.

# Audit:

# From Console: Ensure that the prescribed log metric is present:

- 1. Go to Logging/Logs-based Metrics by visiting https://console.cloud.google.com/logs/metrics.
- 2. In the User-defined Metrics section, ensure that at least one metric <Log\_Metric\_Name> is present with filter text:

```
resource.type="iam_role"
AND protoPayload.methodName = "google.iam.admin.v1.CreateRole"
OR protoPayload.methodName="google.iam.admin.v1.DeleteRole"
OR protoPayload.methodName="google.iam.admin.v1.UpdateRole"
```

# Ensure that the prescribed alerting policy is present:

3. Go to Alerting by visiting <a href="https://console.cloud.google.com/monitoring/alerting">https://console.cloud.google.com/monitoring/alerting</a>.

- 4. Under the Policies section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a threshold of zero(0) for greater than zero(0) seconds means that the alert will trigger for any new owner change. Verify that the chosen alerting thresholds make sense for the user's organization.
- 5. Ensure that the appropriate notifications channels have been set up.

#### From Command Line: Ensure that the prescribed log metric is present:

1. List the log metrics:

gcloud beta logging metrics list --format json

2. Ensure that the output contains at least one metric with the filter set to:

```
resource.type="iam_role" AND protoPayload.methodName =
"google.iam.admin.v1.CreateRole" OR
protoPayload.methodName="google.iam.admin.v1.DeleteRole" OR
protoPayload.methodName="google.iam.admin.v1.UpdateRole"
```

3. Note the value of the property metricDescriptor.type for the identified metric, in the format logging.googleapis.com/user/<Log Metric Name>.

#### Ensure that the prescribed alerting policy is present:

4. List the alerting policies:

gcloud alpha monitoring policies list --format json

- 5. Ensure that the output contains an least one alert policy where:
- conditions.conditionThreshold.filter is set to metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"
- AND enabled is set to true.

# **Remediation:**

## From Console: Create the prescribed log metric:

- 1. Go to Logging/Logs-based Metrics by visiting https://console.cloud.google.com/logs/metrics and click "CREATE METRIC".
- 2. Click the down arrow symbol on the Filter Bar at the rightmost corner and select Convert to Advanced Filter.

#### 3. Clear any text and add:

```
resource.type="iam_role"
AND protoPayload.methodName = "google.iam.admin.v1.CreateRole"
OR protoPayload.methodName="google.iam.admin.v1.DeleteRole"
OR protoPayload.methodName="google.iam.admin.v1.UpdateRole"
```

- 4. Click Submit Filter. Display logs appear based on the filter text entered by the user.
- 5. In the Metric Editor menu on the right, fill out the name field. Set Units to 1 (default) and Type to Counter. This ensures that the log metric counts the number of log entries matching the advanced logs query.
- $6. \ Click \, \texttt{Create Metric.}$

# **Create a prescribed Alert Policy:**

- 1. Identify the new metric that was just created under the section User-defined Metrics at <a href="https://console.cloud.google.com/logs/metrics">https://console.cloud.google.com/logs/metrics</a>.
- 2. Click the 3-dot icon in the rightmost column for the metric and select Create alert from Metric. A new page displays.
- 3. Fill out the alert policy configuration and click Save. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a threshold of zero(0) for the most recent value ensures that a notification is triggered for every owner change in the project:

```
Set `Aggregator` to `Count`
Set `Configuration`:
- Condition: above
- Threshold: 0
- For: most recent value
```

- 4. Configure the desired notification channels in the section Notifications.
- 5. Name the policy and click <code>Save</code>.

# From Command Line:

Create the prescribed Log Metric:

- Use the command: gcloud beta logging metrics create
- Reference for command usage: <u>https://cloud.google.com/sdk/gcloud/reference/beta/logging/metrics/create</u>

Create the prescribed Alert Policy:

- Use the command: gcloud alpha monitoring policies create
- Reference for command usage: <u>https://cloud.google.com/sdk/gcloud/reference/alpha/monitoring/policies/create</u>

#### **References:**

- 1. <u>https://cloud.google.com/logging/docs/logs-based-metrics/</u>
- 2. <a href="https://cloud.google.com/monitoring/custom-metrics/">https://cloud.google.com/monitoring/custom-metrics/</a>
- 3. <u>https://cloud.google.com/monitoring/alerts/</u>
- 4. <u>https://cloud.google.com/logging/docs/reference/tools/gcloud-logging</u>
- 5. <u>https://cloud.google.com/iam/docs/understanding-custom-roles</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	•	•	•
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	•
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.	٠	•	•
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		•	

# 2.7 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes (Automated)

# **Profile Applicability:**

• Level 1

# **Description**:

It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) Network Firewall rule changes.

# **Rationale:**

Monitoring for Create or Update Firewall rule events gives insight to network access changes and may reduce the time it takes to detect suspicious activity.

#### Impact:

Enabling of logging may result in your project being charged for the additional logs usage.

# Audit:

# From Console:

# Ensure that the prescribed log metric is present:

- 1. Go to Logging/Logs-based Metrics by visiting https://console.cloud.google.com/logs/metrics.
- 2. In the User-defined Metrics section, ensure at least one metric <Log\_Metric\_Name> is present with this filter text:

```
resource.type="gce_firewall_rule"
AND protoPayload.methodName:"compute.firewalls.patch"
OR protoPayload.methodName:"compute.firewalls.insert"
OR protoPayload.methodName:"compute.firewalls.delete"
```

# Ensure that the prescribed alerting policy is present:

- 3. Go to Alerting by visiting <a href="https://console.cloud.google.com/monitoring/alerting">https://console.cloud.google.com/monitoring/alerting</a>.
- 4. Under the Policies section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a threshold of zero(0) for greater than zero(0) seconds means that the alert will trigger for any new owner change. Verify that the chosen alerting thresholds make sense for the user's organization.

5. Ensure that appropriate notification channels have been set up.

# From Command Line: Ensure that the prescribed log metric is present:

1. List the log metrics:

gcloud beta logging metrics list --format json

2. Ensure that the output contains at least one metric with the filter set to:

```
resource.type="gce_firewall_rule"
AND protoPayload.methodName:"compute.firewalls.patch"
OR protoPayload.methodName:"compute.firewalls.insert"
OR protoPayload.methodName:"compute.firewalls.delete"
```

3. Note the value of the property metricDescriptor.type for the identified metric, in the format logging.googleapis.com/user/<Log Metric Name>.

#### Ensure that the prescribed alerting policy is present:

4. List the alerting policies:

gcloud alpha monitoring policies list --format json

- 5. Ensure that the output contains an least one alert policy where:
- conditions.conditionThreshold.filter is set to metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"
- AND enabled is set to true

#### **Remediation:**

#### From Console:

#### **Create the prescribed log metric:**

- Go to Logging/Logs-based Metrics by visiting https://console.cloud.google.com/logs/metrics and click "CREATE METRIC".
- 2. Click the down arrow symbol on the Filter Bar at the rightmost corner and select Convert to Advanced Filter.
- 3. Clear any text and add:

```
resource.type="gce_firewall_rule"
AND protoPayload.methodName:"compute.firewalls.patch"
OR protoPayload.methodName:"compute.firewalls.insert"
OR protoPayload.methodName:"compute.firewalls.delete"
```

- 4. Click Submit Filter. Display logs appear based on the filter text entered by the user.
- In the Metric Editor menu on the right, fill out the name field. Set Units to 1 (default) and Type to Counter. This ensures that the log metric counts the number of log entries matching the advanced logs query.
- 6. Click Create Metric.

# Create the prescribed Alert Policy:

- 1. Identify the newly created metric under the section User-defined Metrics at <a href="https://console.cloud.google.com/logs/metrics">https://console.cloud.google.com/logs/metrics</a>.
- 2. Click the 3-dot icon in the rightmost column for the new metric and select Create alert from Metric. A new page displays.
- 3. Fill out the alert policy configuration and click Save. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a threshold of zero(0) for the most recent value ensures that a notification is triggered for every owner change in the project:

```
Set `Aggregator` to `Count`
Set `Configuration`:
- Condition: above
- Threshold: 0
- For: most recent value
```

- 4. Configure the desired notifications channels in the section Notifications.
- 5. Name the policy and click Save.

# From Command Line:

Create the prescribed Log Metric

- Use the command: gcloud beta logging metrics create
- Reference for command usage: https://cloud.google.com/sdk/gcloud/reference/beta/logging/metrics/create

Create the prescribed alert policy:

• Use the command: gcloud alpha monitoring policies create

• Reference for command usage: <u>https://cloud.google.com/sdk/gcloud/reference/alpha/monitoring/policies/create</u>

#### **References:**

- 1. <u>https://cloud.google.com/logging/docs/logs-based-metrics/</u>
- 2. <a href="https://cloud.google.com/monitoring/custom-metrics/">https://cloud.google.com/monitoring/custom-metrics/</a>
- 3. <u>https://cloud.google.com/monitoring/alerts/</u>
- 4. <u>https://cloud.google.com/logging/docs/reference/tools/gcloud-logging</u>
- 5. https://cloud.google.com/vpc/docs/firewalls

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.		•	•
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	•
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.		•	
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		•	

# 2.8 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes (Automated)

# **Profile Applicability:**

• Level 1

# **Description**:

It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network route changes.

# **Rationale:**

Google Cloud Platform (GCP) routes define the paths network traffic takes from a VM instance to another destination. The other destination can be inside the organization VPC network (such as another VM) or outside of it. Every route consists of a destination and a next hop. Traffic whose destination IP is within the destination range is sent to the next hop for delivery.

Monitoring changes to route tables will help ensure that all VPC traffic flows through an expected path.

# Impact:

Enabling of logging may result in your project being charged for the additional logs usage.

# Audit:

# From Console: Ensure that the prescribed Log metric is present:

- 1. Go to Logging/Logs-based Metrics by visiting https://console.cloud.google.com/logs/metrics.
- 2. In the User-defined Metrics section, ensure that at least one metric <Log\_Metric\_Name> is present with the filter text:

```
resource.type="gce_route"
AND (protoPayload.methodName:"compute.routes.delete"
OR protoPayload.methodName:"compute.routes.insert"
```

# Ensure the prescribed alerting policy is present:

- 3. Go to Alerting by visiting: <u>https://console.cloud.google.com/monitoring/alerting</u>.
- 4. Under the Policies section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a threshold of 0 for greater than zero(0) seconds means that the alert will trigger for any new owner change. Verify that the chosen alert thresholds make sense for the user's organization.
- 5. Ensure that the appropriate notification channels have been set up.

# From Command Line: Ensure the prescribed log metric is present:

1. List the log metrics:

gcloud beta logging metrics list --format json

2. Ensure that the output contains at least one metric with the filter set to:

```
resource.type="gce_route"
AND (protoPayload.methodName:"compute.routes.delete"
OR protoPayload.methodName:"compute.routes.insert"
```

3. Note the value of the property metricDescriptor.type for the identified metric, in the format logging.googleapis.com/user/<Log Metric Name>.

#### Ensure that the prescribed alerting policy is present:

4. List the alerting policies:

gcloud alpha monitoring policies list --format json

- 5. Ensure that the output contains an least one alert policy where:
- •

```
conditions.conditionThreshold.filter is set to
metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"
```

• AND enabled is set to true

#### **Remediation:**

# From Console: Create the prescribed Log Metric:

- 1. Go to Logging/Logs-based Metrics by visiting https://console.cloud.google.com/logs/metrics and click "CREATE METRIC".
- 2. Click the down arrow symbol on the Filter Bar at the rightmost corner and select Convert to Advanced Filter
- 3. Clear any text and add:

```
resource.type="gce_route"
AND (protoPayload.methodName:"compute.routes.delete"
OR protoPayload.methodName:"compute.routes.insert"
```

- 4. Click Submit Filter. Display logs appear based on the filter text entered by the user.
- 5. In the Metric Editor menu on the right, fill out the name field. Set Units to 1 (default) and Type to Counter. This ensures that the log metric counts the number of log entries matching the user's advanced logs query.
- 6. Click Create Metric.

# Create the prescribed alert policy:

- 1. Identify the newly created metric under the section User-defined Metrics at <a href="https://console.cloud.google.com/logs/metrics">https://console.cloud.google.com/logs/metrics</a>.
- 2. Click the 3-dot icon in the rightmost column for the new metric and select Create alert from Metric. A new page displays.
- 3. Fill out the alert policy configuration and click Save. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a threshold of zero(0) for the most recent value ensures that a notification is triggered for every owner change in the project:

```
Set `Aggregator` to `Count`
Set `Configuration`:
- Condition: above
- Threshold: 0
- For: most recent value
```

- 4. Configure the desired notification channels in the section Notifications.
- 5. Name the policy and click Save.

# From Command Line:

Create the prescribed Log Metric:

- Use the command: gcloud beta logging metrics create
- Reference for command usage: https://cloud.google.com/sdk/gcloud/reference/beta/logging/metrics/create

Create the prescribed the alert policy:

- Use the command: gcloud alpha monitoring policies create
- Reference for command usage: https://cloud.google.com/sdk/gcloud/reference/alpha/monitoring/policies/create

#### **References:**

- 1. <u>https://cloud.google.com/logging/docs/logs-based-metrics/</u>
- 2. <u>https://cloud.google.com/monitoring/custom-metrics/</u>
- 3. <u>https://cloud.google.com/monitoring/alerts/</u>
- 4. <u>https://cloud.google.com/logging/docs/reference/tools/gcloud-logging</u>
- 5. <u>https://cloud.google.com/storage/docs/access-control/iam</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	•	•	
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.	٠	•	
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		•	

# 2.9 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes (Automated)

# **Profile Applicability:**

• Level 1

# **Description**:

It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network changes.

# **Rationale:**

It is possible to have more than one VPC within a project. In addition, it is also possible to create a peer connection between two VPCs enabling network traffic to route between VPCs.

Monitoring changes to a VPC will help ensure VPC traffic flow is not getting impacted.

#### Impact:

Enabling of logging may result in your project being charged for the additional logs usage.

# Audit:

# From Console: Ensure the prescribed log metric is present:

- 1. Go to Logging/Logs-based Metrics by visiting https://console.cloud.google.com/logs/metrics.
- 2. In the User-defined Metrics section, ensure at least one metric <Log\_Metric\_Name> is present with filter text:

```
resource.type=gce_network
```

```
AND (protoPayload.methodName:"compute.networks.insert"
```

```
OR protoPayload.methodName:"compute.networks.patch"
```

```
OR protoPayload.methodName:"compute.networks.delete"
```

```
OR protoPayload.methodName:"compute.networks.removePeering"
```

```
OR protoPayload.methodName:"compute.networks.addPeering")
```

# Ensure the prescribed alerting policy is present:

3. Go to Alerting by visiting <a href="https://console.cloud.google.com/monitoring/alerting">https://console.cloud.google.com/monitoring/alerting</a>.

- 4. Under the Policies section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a threshold of 0 for greater than 0 seconds means that the alert will trigger for any new owner change. Verify that the chosen alerting thresholds make sense for the user's organization.
- 5. Ensure that appropriate notification channels have been set up.

# From Command Line: Ensure the log metric is present:

1. List the log metrics:

gcloud beta logging metrics list --format json

2. Ensure that the output contains at least one metric with filter set to:

```
resource.type=gce_network
AND protoPayload.methodName="beta.compute.networks.insert"
OR protoPayload.methodName="beta.compute.networks.patch"
OR protoPayload.methodName="v1.compute.networks.delete"
OR protoPayload.methodName="v1.compute.networks.removePeering"
OR protoPayload.methodName="v1.compute.networks.addPeering"
```

3. Note the value of the property metricDescriptor.type for the identified metric, in the format logging.googleapis.com/user/<Log Metric Name>.

# Ensure the prescribed alerting policy is present:

4. List the alerting policies:

gcloud alpha monitoring policies list --format json

- 5. Ensure that the output contains at least one alert policy where:
- conditions.conditionThreshold.filter is set to metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"
- AND enabled is set to true

## **Remediation:**

## From Console: Create the prescribed log metric:

 Go to Logging/Logs-based Metrics by visiting https://console.cloud.google.com/logs/metrics and click "CREATE METRIC".

- 2. Click the down arrow symbol on  ${\tt Filter}$   ${\tt Bar}$  at the rightmost corner and select
  - Convert to Advanced Filter.
- 3. Clear any text and add:

```
resource.type=gce_network
```

```
AND (protoPayload.methodName:"compute.networks.insert"
```

```
OR protoPayload.methodName:"compute.networks.patch"
```

```
OR protoPayload.methodName:"compute.networks.delete"
```

OR protoPayload.methodName:"compute.networks.removePeering"

OR protoPayload.methodName:"compute.networks.addPeering")

- 4. Click Submit Filter. Display logs appear based on the filter text entered by the user.
- 5. In the Metric Editor menu on the right, fill out the name field. Set Units to 1 (default) and Type to Counter. This ensures that the log metric counts the number of log entries matching the user's advanced logs query.
- 6. Click Create Metric.

# Create the prescribed alert policy:

- 1. Identify the newly created metric under the section User-defined Metrics at <a href="https://console.cloud.google.com/logs/metrics">https://console.cloud.google.com/logs/metrics</a>.
- 2. Click the 3-dot icon in the rightmost column for the new metric and select Create alert from Metric. A new page appears.
- 3. Fill out the alert policy configuration and click Save. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a threshold of 0 for the most recent value will ensure that a notification is triggered for every owner change in the project:

```
Set `Aggregator` to `Count`
Set `Configuration`:
- Condition: above
- Threshold: 0
- For: most recent value
```

- 4. Configure the desired notification channels in the section Notifications.
- 5. Name the policy and click  ${\tt Save}.$

# From Command Line:

Create the prescribed Log Metric:

• Use the command: gcloud beta logging metrics create

• Reference for command usage: <u>https://cloud.google.com/sdk/gcloud/reference/beta/logging/metrics/create</u>

Create the prescribed alert policy:

- Use the command: gcloud alpha monitoring policies create
- Reference for command usage: <u>https://cloud.google.com/sdk/gcloud/reference/alpha/monitoring/policies/create</u>

#### **References:**

- 1. <u>https://cloud.google.com/logging/docs/logs-based-metrics/</u>
- 2. https://cloud.google.com/monitoring/custom-metrics/
- 3. <u>https://cloud.google.com/monitoring/alerts/</u>
- 4. <u>https://cloud.google.com/logging/docs/reference/tools/gcloud-logging</u>
- 5. <u>https://cloud.google.com/vpc/docs/overview</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.		•	•
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	•
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			•
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		•	•

# 2.10 Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes (Automated)

# **Profile Applicability:**

• Level 1

# **Description**:

It is recommended that a metric filter and alarm be established for Cloud Storage Bucket IAM changes.

# **Rationale:**

Monitoring changes to cloud storage bucket permissions may reduce the time needed to detect and correct permissions on sensitive cloud storage buckets and objects inside the bucket.

#### Impact:

Enabling of logging may result in your project being charged for the additional logs usage.

# Audit:

# From Console:

# Ensure the prescribed log metric is present:

- 1. For each project that contains cloud storage buckets, go to Logging/Logs-based Metrics by visiting <a href="https://console.cloud.google.com/logs/metrics">https://console.cloud.google.com/logs/metrics</a>.
- 2. In the User-defined Metrics section, ensure at least one metric
   <Log\_Metric\_Name> is present with the filter text:

```
resource.type=gcs_bucket
AND protoPayload.methodName="storage.setIamPermissions"
```

#### Ensure that the prescribed alerting policy is present:

- 3. Go to Alerting by visiting <a href="https://console.cloud.google.com/monitoring/alerting">https://console.cloud.google.com/monitoring/alerting</a>.
- 4. Under the Policies section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a threshold of 0 for greater than 0 seconds means that the alert will trigger for any new owner change. Verify that the chosen alerting thresholds make sense for the user's organization.
- 5. Ensure that the appropriate notifications channels have been set up.

# From Command Line: Ensure that the prescribed log metric is present:

1. List the log metrics:

gcloud beta logging metrics list --format json

2. Ensure that the output contains at least one metric with the filter set to:

resource.type=gcs\_bucket
AND protoPayload.methodName="storage.setIamPermissions"

3. Note the value of the property metricDescriptor.type for the identified metric, in the format logging.googleapis.com/user/<Log Metric Name>.

#### Ensure the prescribed alerting policy is present:

4. List the alerting policies:

gcloud alpha monitoring policies list --format json

- 5. Ensure that the output contains an least one alert policy where:
- conditions.conditionThreshold.filter is set to metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"
- AND enabled is set to true

#### **Remediation:**

#### From Console: Create the prescribed log metric:

- 1. Go to Logging/Logs-based Metrics by visiting https://console.cloud.google.com/logs/metrics and click "CREATE METRIC".
- 2. Click the down arrow symbol on the Filter Bar at the rightmost corner and select Convert to Advanced Filter.
- 3. Clear any text and add:

resource.type=gcs\_bucket
AND protoPayload.methodName="storage.setIamPermissions"

4. Click Submit Filter. Display logs appear based on the filter text entered by the user.

- 5. In the Metric Editor menu on right, fill out the name field. Set Units to 1 (default) and Type to Counter. This ensures that the log metric counts the number of log entries matching the user's advanced logs query.
- 6. Click Create Metric.

# **Create the prescribed Alert Policy:**

- 1. Identify the newly created metric under the section User-defined Metrics at <a href="https://console.cloud.google.com/logs/metrics">https://console.cloud.google.com/logs/metrics</a>.
- 2. Click the 3-dot icon in the rightmost column for the new metric and select Create alert from Metric. A new page appears.
- 3. Fill out the alert policy configuration and click Save. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a threshold of zero(0) for the most recent value will ensure that a notification is triggered for every owner change in the project:

```
Set `Aggregator` to `Count`
Set `Configuration`:
- Condition: above
- Threshold: 0
- For: most recent value
```

- 4. Configure the desired notifications channels in the section Notifications.
- 5. Name the policy and click  ${\tt Save}.$

# From Command Line:

Create the prescribed Log Metric:

- Use the command: gcloud beta logging metrics create
- Reference for command usage: <u>https://cloud.google.com/sdk/gcloud/reference/beta/logging/metrics/create</u>

Create the prescribed alert policy:

- Use the command: gcloud alpha monitoring policies create
- Reference for command usage: <u>https://cloud.google.com/sdk/gcloud/reference/alpha/monitoring/policies/create</u>

# **References:**

- 1. <u>https://cloud.google.com/logging/docs/logs-based-metrics/</u>
- 2. <u>https://cloud.google.com/monitoring/custom-metrics/</u>

- 3. <u>https://cloud.google.com/monitoring/alerts/</u>
- 4. <u>https://cloud.google.com/logging/docs/reference/tools/gcloud-logging</u>
- 5. <u>https://cloud.google.com/storage/docs/overview</u>
- 6. https://cloud.google.com/storage/docs/access-control/iam-roles

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.		•	
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

# 2.11 Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes (Automated)

# Profile Applicability:

• Level 1

# **Description**:

It is recommended that a metric filter and alarm be established for SQL instance configuration changes.

# **Rationale:**

Monitoring changes to SQL instance configuration changes may reduce the time needed to detect and correct misconfigurations done on the SQL server.

Below are a few of the configurable options which may the impact security posture of an SQL instance:

- Enable auto backups and high availability: Misconfiguration may adversely impact business continuity, disaster recovery, and high availability
- Authorize networks: Misconfiguration may increase exposure to untrusted networks

#### Impact:

Enabling of logging may result in your project being charged for the additional logs usage.

#### Audit:

# From Console:

# Ensure the prescribed log metric is present:

- 1. For each project that contains Cloud SQL instances, go to Logging/Logs-based Metrics by visiting <a href="https://console.cloud.google.com/logs/metrics">https://console.cloud.google.com/logs/metrics</a>.
- 2. In the User-defined Metrics section, ensure that at least one metric
   <Log\_Metric\_Name> is present with the filter text:

protoPayload.methodName="cloudsql.instances.update"

# Ensure that the prescribed alerting policy is present:

- 3. Go to Alerting by visiting <a href="https://console.cloud.google.com/monitoring/alerting">https://console.cloud.google.com/monitoring/alerting</a>.
- 4. Under the Policies section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a threshold of zero(0) for greater than zero(0) seconds means that the alert will trigger for any new owner change. Verify that the chosen alerting thresholds make sense for the user's organization.
- 5. Ensure that the appropriate notifications channels have been set up.

# From Command Line: Ensure that the prescribed log metric is present:

1. List the log metrics:

gcloud beta logging metrics list --format json

2. Ensure that the output contains at least one metric with the filter set to

protoPayload.methodName="cloudsql.instances.update"

3. Note the value of the property metricDescriptor.type for the identified metric, in the format logging.googleapis.com/user/<Log Metric Name>.

#### Ensure that the prescribed alerting policy is present:

4. List the alerting policies:

gcloud alpha monitoring policies list --format json

- 5. Ensure that the output contains at least one alert policy where:
- conditions.conditionThreshold.filter is set to metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"
- AND enabled is set to true

#### **Remediation:**

#### From Console: Create the prescribed Log Metric:

 Go to Logging/Logs-based Metrics by visiting https://console.cloud.google.com/logs/metrics and click "CREATE METRIC".
- 2. Click the down arrow symbol on the Filter Bar at the rightmost corner and select Convert to Advanced Filter.
- 3. Clear any text and add:

protoPayload.methodName="cloudsql.instances.update"

- 4. Click Submit Filter. Display logs appear based on the filter text entered by the user.
- 5. In the Metric Editor menu on right, fill out the name field. Set Units to 1 (default) and Type to Counter. This ensures that the log metric counts the number of log entries matching the user's advanced logs query.
- 6. Click Create Metric.

#### **Create the prescribed alert policy:**

- 1. Identify the newly created metric under the section User-defined Metrics at <a href="https://console.cloud.google.com/logs/metrics">https://console.cloud.google.com/logs/metrics</a>.
- 2. Click the 3-dot icon in the rightmost column for the new metric and select Create alert from Metric. A new page appears.
- 3. Fill out the alert policy configuration and click Save. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a threshold of zero(0) for the most recent value will ensure that a notification is triggered for every owner change in the user's project:

```
Set `Aggregator` to `Count`
Set `Configuration`:
- Condition: above
- Threshold: 0
- For: most recent value
```

- 4. Configure the desired notification channels in the section Notifications.
- 5. Name the policy and click Save.

#### From Command Line:

Create the prescribed log metric:

- Use the command: gcloud beta logging metrics create
- Reference for command usage: <u>https://cloud.google.com/sdk/gcloud/reference/beta/logging/metrics/create</u>

Create the prescribed alert policy:

- Use the command: gcloud alpha monitoring policies create
- Reference for command usage: <u>https://cloud.google.com/sdk/gcloud/reference/alpha/monitoring/policies/create</u>

#### **References:**

- 1. <u>https://cloud.google.com/logging/docs/logs-based-metrics/</u>
- 2. <u>https://cloud.google.com/monitoring/custom-metrics/</u>
- 3. <u>https://cloud.google.com/monitoring/alerts/</u>
- 4. <u>https://cloud.google.com/logging/docs/reference/tools/gcloud-logging</u>
- 5. <u>https://cloud.google.com/storage/docs/overview</u>
- 6. https://cloud.google.com/sql/docs/
- 7. <u>https://cloud.google.com/sql/docs/mysql/</u>
- 8. https://cloud.google.com/sql/docs/postgres/

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.		•	•
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	•
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.		•	•
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		•	

## 2.12 Ensure That Cloud DNS Logging Is Enabled for All VPC Networks (Automated)

## **Profile Applicability:**

• Level 1

## **Description:**

Cloud DNS logging records the queries from the name servers within your VPC to Stackdriver. Logged queries can come from Compute Engine VMs, GKE containers, or other GCP resources provisioned within the VPC.

## **Rationale:**

Security monitoring and forensics cannot depend solely on IP addresses from VPC flow logs, especially when considering the dynamic IP usage of cloud resources, HTTP virtual host routing, and other technology that can obscure the DNS name used by a client from the IP address. Monitoring of Cloud DNS logs provides visibility to DNS names requested by the clients within the VPC. These logs can be monitored for anomalous domain names, evaluated against threat intelligence, and

Note: For full capture of DNS, firewall must block egress UDP/53 (DNS) and TCP/443 (DNS over HTTPS) to prevent client from using external DNS name server for resolution.

## Impact:

Enabling of Cloud DNS logging might result in your project being charged for the additional logs usage.

## Audit:

## From Command Line:

1. List all VPCs networks in a project:

```
gcloud compute networks list --format="table[box,title='All VPC
Networks'](name:label='VPC Network Name')"
```

2. List all DNS policies, logging enablement, and associated VPC networks:

```
gcloud dns policies list --flatten="networks[]" --
format="table[box,title='All DNS Policies By VPC Network'](name:label='Policy
Name',enableLogging:label='Logging
```

```
Enabled':align=center,networks.networkUrl.basename():label='VPC Network
Name')"
```

Each VPC Network should be associated with a DNS policy with logging enabled.

#### **Remediation:**

#### From Command Line:

#### Add New DNS Policy With Logging Enabled

For each VPC network that needs a DNS policy with logging enabled:

gcloud dns policies create enable-dns-logging --enable-logging -description="Enable DNS Logging" --networks=VPC NETWORK NAME

## The VPC\_NETWORK\_NAME can be one or more networks in comma-separated list **Enable Logging for Existing DNS Policy**

For each VPC network that has an existing DNS policy that needs logging enabled:

```
gcloud dns policies update POLICY_NAME --enable-logging -- networks=VPC NETWORK NAME
```

The VPC\_NETWORK\_NAME can be one or more networks in comma-separated list

#### **Default Value:**

Cloud DNS logging is disabled by default on each network.

#### **References:**

1. <u>https://cloud.google.com/dns/docs/monitoring</u>

## Additional Information:

Additional Info

• Only queries that reach a name server are logged. Cloud DNS resolvers cache responses, queries answered from caches, or direct queries to an external DNS resolver outside the VPC are not logged.

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	•	•	•
v8	8.6 <u>Collect DNS Query Audit Logs</u> Collect DNS query audit logs on enterprise assets, where appropriate and supported.		•	•
v8	8.11 <u>Conduct Audit Log Reviews</u> Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		•	•
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.	•	•	•
v7	6.7 <u>Regularly Review Logs</u> On a regular basis, review logs to identify anomalies or abnormal events.		•	•
v7	8.7 <u>Enable DNS Query Logging</u> Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.		•	•

## 2.13 Ensure Cloud Asset Inventory Is Enabled (Automated)

## **Profile Applicability:**

- Level 2
- Level 1

## **Description:**

GCP Cloud Asset Inventory is services that provides a historical view of GCP resources and IAM policies through a time-series database. The information recorded includes metadata on Google Cloud resources, metadata on policies set on Google Cloud projects or resources, and runtime information gathered within a Google Cloud resource.

#### **Rationale:**

The GCP resources and IAM policies captured by GCP Cloud Asset Inventory enables security analysis, resource change tracking, and compliance auditing.

#### Impact:

It is recommended GCP Cloud Asset Inventory be enabled for all GCP projects.

## Audit:

#### From Console: Ensure that the Cloud Asset API is enabled:

- 1. Go to API & Services/Library by visiting
   https://console.cloud.google.com/apis/library
- 2. Search for Cloud Asset API and select the result for Cloud Asset API
- 3. Ensure that API Enabled is displayed.

## From Command Line: Ensure that the Cloud Asset API is enabled:

1. Query enabled services:

gcloud services list --enabled --filter=name:cloudasset.googleapis.com

If the API is listed, then it is enabled. If the response is <code>Listed 0 items</code> the API is not enabled.

#### **Remediation:**

## From Console: Enable the Cloud Asset API:

- 1. Go to API & Services/Library by visiting https://console.cloud.google.com/apis/library
- 2. Search for Cloud Asset API and select the result for Cloud Asset API
- 3. Click the ENABLE button.

#### From Command Line: Enable the Cloud Asset API:

1. Enable the Cloud Asset API through the services interface:

gcloud services enable cloudasset.googleapis.com

#### **Default Value:**

The Cloud Asset Inventory API is disabled by default in each project.

#### **References:**

1. <u>https://cloud.google.com/asset-inventory/docs</u>

#### **Additional Information:**

Additional info

• Cloud Asset Inventory only keeps a five-week history of Google Cloud asset metadata. If a longer history is desired, automation to export the history to Cloud Storage or BigQuery should be evaluated.

Controls Version	Control	IG 1	IG 2	IG 3
v8	1.1 Establish and Maintain Detailed Enterprise Asset Inventory Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user	•	•	•

Controls Version	Control	IG 1	IG 2	IG 3
	devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.			
v8	6.6 Establish and Maintain an Inventory of Authentication and Authorization Systems Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.		•	•
v7	1.4 <u>Maintain Detailed Asset Inventory</u> Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	•	•	•
v7	<b>11.2</b> <u>Document Traffic Configuration Rules</u> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		•	•
v7	16.1 <u>Maintain an Inventory of Authentication Systems</u> Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.		•	

## 2.14 Ensure 'Access Transparency' is 'Enabled' (Manual)

## **Profile Applicability:**

• Level 1

## **Description**:

GCP Access Transparency provides audit logs for all actions that Google personnel take in your Google Cloud resources.

## **Rationale:**

Controlling access to your information is one of the foundations of information security. Given that Google Employees do have access to your organizations' projects for support reasons, you should have logging in place to view who, when, and why your information is being accessed.

## Impact:

To use Access Transparency your organization will need to have at one of the following support level: Premium, Enterprise, Platinum, or Gold. There will be subscription costs associated with support, as well as increased storage costs for storing the logs. You will also not be able to turn Access Transparency off yourself, and you will need to submit a service request to Google Cloud Support.

## Audit:

## **Determine if Access Transparency is Enabled**

- 1. From the Google Cloud Home, click on the Navigation hamburger menu in the top left. Hover over the IAM & Admin Menu. Select settings in the middle of the column that opens.
- 2. The status will be under the heading Access Transparency. Status should be Enabled

## **Remediation:**

## Add privileges to enable Access Transparency

- 1. From the Google Cloud Home, within the project you wish to check, click on the Navigation hamburger menu in the top left. Hover over the 'IAM and Admin'. Select IAM in the top of the column that opens.
- 2. Click the blue button the says +add at the top of the screen.

- 3. In the principals field, select a user or group by typing in their associated email address.
- 4. Click on the role field to expand it. In the filter field enter Access Transparency Admin and select it.
- 5. Click save.

## Verify that the Google Cloud project is associated with a billing account

- 1. From the Google Cloud Home, click on the Navigation hamburger menu in the top left. Select Billing.
- 2. If you see This project is not associated with a billing account you will need to enter billing information or switch to a project with a billing account.

## **Enable Access Transparency**

- 1. From the Google Cloud Home, click on the Navigation hamburger menu in the top left. Hover over the IAM & Admin Menu. Select settings in the middle of the column that opens.
- 2. Click the blue button labeled Enable Access Transparency for Organization

## **Default Value:**

By default Access Transparency is not enabled.

## **References:**

- 1. <u>https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/overview</u>
- 2. <u>https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/enable</u>
- 3. <u>https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/reading-logs</u>
- 4. <u>https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/reading-logs#justification\_reason\_codes</u>
- 5. <u>https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/supported-services</u>

## Additional Information:

To enable Access Transparency for your Google Cloud organization, your Google Cloud organization must have one of the following customer support levels: Premium, Enterprise, Platinum, or Gold.

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.		•	•
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	•
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			•
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 2.15 Ensure 'Access Approval' is 'Enabled' (Automated)

## **Profile Applicability:**

• Level 2

## **Description**:

GCP Access Approval enables you to require your organizations' explicit approval whenever Google support try to access your projects. You can then select users within your organization who can approve these requests through giving them a security role in IAM. All access requests display which Google Employee requested them in an email or Pub/Sub message that you can choose to Approve. This adds an additional control and logging of who in your organization approved/denied these requests.

## **Rationale:**

Controlling access to your information is one of the foundations of information security. Google Employees do have access to your organizations' projects for support reasons. With Access Approval, organizations can then be certain that their information is accessed by only approved Google Personnel.

## Impact:

To use Access Approval your organization will need have enabled Access Transparency and have at one of the following support level: Enhanced or Premium. There will be subscription costs associated with these support levels, as well as increased storage costs for storing the logs. You will also not be able to turn the Access Transparency which Access Approval depends on, off yourself. To do so you will need to submit a service request to Google Cloud Support. There will also be additional overhead in managing user permissions. There may also be a potential delay in support times as Google Personnel will have to wait for their access to be approved.

## Audit:

## From Console:

## Determine if Access Transparency is Enabled as it is a Dependency

1. From the Google Cloud Home inside the project you wish to audit, click on the Navigation hamburger menu in the top left. Hover over the IAM & Admin Menu. Select settings in the middle of the column that opens.

2. The status should be "Enabled' under the heading Access Transparency

#### **Determine if Access Approval is Enabled**

- 1. From the Google Cloud Home, within the project you wish to check, click on the Navigation hamburger menu in the top left. Hover over the Security Menu. Select Access Approval in the middle of the column that opens.
- 2. The status will be displayed here. If you see a screen saying you need to enroll in Access Approval, it is not enabled.

#### From CLI:

#### **Determine if Access Approval is Enabled**

1. From within the project you wish to audit, run the following command.

gcloud access-approval settings get

2. The status will be displayed in the output.

#### **Remediation:**

#### From Console:

- 1. From the Google Cloud Home, within the project you wish to enable, click on the Navigation hamburger menu in the top left. Hover over the Security Menu. Select Access Approval in the middle of the column that opens.
- 2. The status will be displayed here. On this screen, there is an option to click Enroll. If it is greyed out and you see an error bar at the top of the screen that says Access Transparency is not enabled please view the corresponding reference within this section to enable it.
- 3. In the second screen click Enroll.

## Grant an IAM Group or User the role with permissions to Add Users to be Access Approval message Recipients

- 1. From the Google Cloud Home, within the project you wish to enable, click on the Navigation hamburger menu in the top left. Hover over the IAM and Admin. Select IAM in the middle of the column that opens.
- 2. Click the blue button the says +add at the top of the screen.
- 3. In the principals field, select a user or group by typing in their associated email address.

- 4. Click on the role field to expand it. In the filter field enter Access Approval Approver and select it.
- 5. Click save.

## Add a Group or User as an Approver for Access Approval Requests

- 1. As a user with the Access Approval Approver permission, within the project where you wish to add an email address to which request will be sent, click on the Navigation hamburger menu in the top left. Hover over the Security Menu. Select Access Approval in the middle of the column that opens.
- 2. Click Manage Settings
- 3. Under Set up approval notifications, enter the email address associated with a Google Cloud User or Group you wish to send Access Approval requests to. All future access approvals will be sent as emails to this address.

## From CLI:

1. To update all services in an entire project, run the following command from an account that has permissions as an 'Approver for Access Approval Requests'

```
gcloud access-approval settings update --project=<project name> --
enrolled_services=all --notification_emails='<email recipient for access
approval requests>@<domain name>'
```

## **Default Value:**

By default Access Approval and its dependency of Access Transparency are not enabled.

#### **References:**

- 1. <u>https://cloud.google.com/cloud-provider-access-management/access-approval/docs</u>
- 2. <u>https://cloud.google.com/cloud-provider-access-management/access-approval/docs/overview</u>
- 3. <u>https://cloud.google.com/cloud-provider-access-management/access-approval/docs/quickstart-custom-key</u>
- 4. <u>https://cloud.google.com/cloud-provider-access-management/access-approval/docs/supported-services</u>
- 5. <u>https://cloud.google.com/cloud-provider-access-management/access-approval/docs/view-historical-requests</u>

## Additional Information:

The recipients of Access Requests will also need to be logged into a Google Cloud account associated with an email address in this list. To approve requests they can click approve

within the email. Or they can view requests at the the Access Approval page within the Security submenu.

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	•	•	•
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	•	•	•

## 3 Networking

This section covers recommendations addressing networking on Google Cloud Platform.

## *3.1 Ensure That the Default Network Does Not Exist in a Project (Automated)*

## Profile Applicability:

• Level 2

## **Description**:

To prevent use of default network, a project should not have a default network.

## **Rationale:**

The default network has a preconfigured network configuration and automatically generates the following insecure firewall rules:

- default-allow-internal: Allows ingress connections for all protocols and ports among instances in the network.
- default-allow-ssh: Allows ingress connections on TCP port 22(SSH) from any source to any instance in the network.
- default-allow-rdp: Allows ingress connections on TCP port 3389(RDP) from any source to any instance in the network.
- default-allow-icmp: Allows ingress ICMP traffic from any source to any instance in the network.

These automatically created firewall rules do not get audit logged and cannot be configured to enable firewall rule logging.

Furthermore, the default network is an auto mode network, which means that its subnets use the same predefined range of IP addresses, and as a result, it's not possible to use Cloud VPN or VPC Network Peering with the default network.

Based on organization security and networking requirements, the organization should create a new network and delete the default network.

## Impact:

When an organization deletes the default network, it may need to migrate or service onto a new network.

#### Audit:

#### From Console:

- 1. Go to the VPC networks page by visiting: https://console.cloud.google.com/networking/networks/list.
- 2. Ensure that a network with the name default is not present.

#### From Command Line:

1. Set the project name in the Google Cloud Shell:

gcloud config set project PROJECT\_ID

2. List the networks configured in that project:

gcloud compute networks list

It should not list default as one of the available networks in that project.

#### **Remediation:**

#### From Console:

- Go to the VPC networks page by visiting: <u>https://console.cloud.google.com/networking/networks/list</u>.
- 2. Click the network named default.
- 3. On the network detail page, click EDIT.
- 4. Click delete vpc network.
- 5. If needed, create a new network to replace the default network.

#### From Command Line:

For each Google Cloud Platform project,

1. Delete the default network:

gcloud compute networks delete default

2. If needed, create a new network to replace it:

gcloud compute networks create NETWORK\_NAME

#### **Prevention:**

The user can prevent the default network and its insecure default firewall rules from being

created by setting up an Organization Policy to Skip default network creation at
https://console.cloud.google.com/iam-admin/orgpolicies/computeskipDefaultNetworkCreation.

#### **Default Value:**

By default, for each project, a default network is created.

#### **References:**

- 1. <u>https://cloud.google.com/compute/docs/networking#firewall\_rules</u>
- 2. <u>https://cloud.google.com/compute/docs/reference/latest/networks/insert</u>
- 3. <u>https://cloud.google.com/compute/docs/reference/latest/networks/delete</u>
- 4. https://cloud.google.com/vpc/docs/firewall-rules-logging
- 5. <u>https://cloud.google.com/vpc/docs/vpc#default-network</u>
- 6. <u>https://cloud.google.com/sdk/gcloud/reference/compute/networks/delete</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process</u> <u>for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	•	•	•
v7	11.1 <u>Maintain Standard Security Configurations for Network</u> <u>Devices</u> Maintain standard, documented security configuration standards for all authorized network devices.		•	

## 3.2 Ensure Legacy Networks Do Not Exist for Older Projects (Automated)

## **Profile Applicability:**

• Level 1

## **Description**:

In order to prevent use of legacy networks, a project should not have a legacy network configured. As of now, Legacy Networks are gradually being phased out, and you can no longer create projects with them. This recommendation is to check older projects to ensure that they are not using Legacy Networks.

#### **Rationale:**

Legacy networks have a single network IPv4 prefix range and a single gateway IP address for the whole network. The network is global in scope and spans all cloud regions. Subnetworks cannot be created in a legacy network and are unable to switch from legacy to auto or custom subnet networks. Legacy networks can have an impact for high network traffic projects and are subject to a single point of contention or failure.

#### Impact:

None.

#### Audit:

For each Google Cloud Platform project,

1. Set the project name in the Google Cloud Shell:

gcloud config set project <Project-ID>

2. List the networks configured in that project:

gcloud compute networks list

None of the listed networks should be in the legacy mode.

#### **Remediation:**

For each Google Cloud Platform project,

- 1. Follow the documentation and create a non-legacy network suitable for the organization's requirements.
- 2. Follow the documentation and delete the networks in the legacy mode.

#### **Default Value:**

By default, networks are not created in the <code>legacy</code> mode.

#### **References:**

- 1. <u>https://cloud.google.com/vpc/docs/using-legacy#creating a legacy network</u>
- 2. <u>https://cloud.google.com/vpc/docs/using-legacy#deleting a legacy network</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process</u> for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	•	•	•
v7	11.1 <u>Maintain Standard Security Configurations for Network</u> <u>Devices</u> Maintain standard, documented security configuration standards for all authorized network devices.		•	

## 3.3 Ensure That DNSSEC Is Enabled for Cloud DNS (Automated)

## **Profile Applicability:**

• Level 1

## **Description**:

Cloud Domain Name System (DNS) is a fast, reliable and cost-effective domain name system that powers millions of domains on the internet. Domain Name System Security Extensions (DNSSEC) in Cloud DNS enables domain owners to take easy steps to protect their domains against DNS hijacking and man-in-the-middle and other attacks.

#### **Rationale:**

Domain Name System Security Extensions (DNSSEC) adds security to the DNS protocol by enabling DNS responses to be validated. Having a trustworthy DNS that translates a domain name like <u>www.example.com</u> into its associated IP address is an increasingly important building block of today's web-based applications. Attackers can hijack this process of domain/IP lookup and redirect users to a malicious site through DNS hijacking and man-inthe-middle attacks. DNSSEC helps mitigate the risk of such attacks by cryptographically signing DNS records. As a result, it prevents attackers from issuing fake DNS responses that may misdirect browsers to nefarious websites.

#### Audit:

#### From Console:

- 1. Go to cloud DNS by visiting <u>https://console.cloud.google.com/net-services/dns/zones</u>.
- 2. For each zone of Type Public, ensure that DNSSEC is set to On.

#### From Command Line:

1. List all the Managed Zones in a project:

gcloud dns managed-zones list

2. For each zone of VISIBILITY public, get its metadata:

gcloud dns managed-zones describe ZONE\_NAME

3. Ensure that dnssecConfig.state property is on.

#### **Remediation:**

#### From Console:

- 1. Go to cloud DNS by visiting <u>https://console.cloud.google.com/net-services/dns/zones</u>.
- 2. For each zone of Type Public, set DNSSEC to On.

#### From Command Line:

Use the below command to enable DNSSEC for Cloud DNS Zone Name.

gcloud dns managed-zones update ZONE\_NAME --dnssec-state on

#### **Default Value:**

By default DNSSEC is not enabled.

#### **References:**

- 1. <u>https://cloudplatform.googleblog.com/2017/11/DNSSEC-now-available-in-Cloud-DNS.html</u>
- 2. <u>https://cloud.google.com/dns/dnssec-config#enabling</u>
- 3. https://cloud.google.com/dns/dnssec

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process</u> <u>for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	•	•	•
v7	11.1 <u>Maintain Standard Security Configurations for Network</u> <u>Devices</u> Maintain standard, documented security configuration standards for all authorized network devices.		•	

# 3.4 Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC (Manual)

## Profile Applicability:

• Level 1

## **Description**:

NOTE: Currently, the SHA1 algorithm has been removed from general use by Google, and, if being used, needs to be whitelisted on a project basis by Google and will also, therefore, require a Google Cloud support contract.

DNSSEC algorithm numbers in this registry may be used in CERT RRs. Zone signing (DNSSEC) and transaction security mechanisms (SIG(0) and TSIG) make use of particular subsets of these algorithms. The algorithm used for key signing should be a recommended one and it should be strong.

## **Rationale:**

Domain Name System Security Extensions (DNSSEC) algorithm numbers in this registry may be used in CERT RRs. Zonesigning (DNSSEC) and transaction security mechanisms (SIG(0) and TSIG) make use of particular subsets of these algorithms.

The algorithm used for key signing should be a recommended one and it should be strong. When enabling DNSSEC for a managed zone, or creating a managed zone with DNSSEC, the user can select the DNSSEC signing algorithms and the denial-of-existence type. Changing the DNSSEC settings is only effective for a managed zone if DNSSEC is not already enabled. If there is a need to change the settings for a managed zone where it has been enabled, turn DNSSEC off and then re-enable it with different settings.

## Audit:

Currently there is no support to audit this setting through console.

## From Command Line:

Ensure the property algorithm for keyType keySigning is not using RSASHA1.

```
gcloud dns managed-zones describe ZONENAME --
format="json(dnsName,dnssecConfig.state,dnssecConfig.defaultKeySpecs)"
```

#### **Remediation:**

1. If it is necessary to change the settings for a managed zone where it has been enabled, NSSEC must be turned off and re-enabled with different settings. To turn off DNSSEC, run the following command:

gcloud dns managed-zones update ZONE\_NAME --dnssec-state off

2. To update key-signing for a reported managed DNS Zone, run the following command:

```
gcloud dns managed-zones update ZONE_NAME --dnssec-state on --ksk-algorithm
KSK_ALGORITHM --ksk-key-length KSK_KEY_LENGTH --zsk-algorithm ZSK_ALGORITHM -
-zsk-key-length ZSK KEY LENGTH --denial-of-existence DENIAL OF EXISTENCE
```

#### Supported algorithm options and key lengths are as follows.

Algorithm	KSK Length	ZSK Length
RSASHA1	1024,2048	1024,2048
RSASHA256	1024,2048	1024,2048
RSASHA512	1024,2048	1024,2048
ECDSAP256SHA256	256	256
ECDSAP384SHA384	384	384

#### **References:**

1. <u>https://cloud.google.com/dns/dnssec-advanced#advanced\_signing\_options</u>

#### **Additional Information:**

- 1. RSASHA1 key-signing support may be required for compatibility reasons.
- 2. Remediation CLI works well with gcloud-cli version 221.0.0 and later.

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process</u> <u>for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	•	•	•

Controls Version	Control	IG 1	IG 2	IG 3
v7	11.1 <u>Maintain Standard Security Configurations for Network</u> <u>Devices</u> Maintain standard, documented security configuration standards for all		•	•
	authorized network devices.			

# 3.5 Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC (Manual)

## Profile Applicability:

• Level 1

## **Description:**

NOTE: Currently, the SHA1 algorithm has been removed from general use by Google, and, if being used, needs to be whitelisted on a project basis by Google and will also, therefore, require a Google Cloud support contract.

DNSSEC algorithm numbers in this registry may be used in CERT RRs. Zone signing (DNSSEC) and transaction security mechanisms (SIG(0) and TSIG) make use of particular subsets of these algorithms. The algorithm used for key signing should be a recommended one and it should be strong.

## **Rationale:**

DNSSEC algorithm numbers in this registry may be used in CERT RRs. Zone signing (DNSSEC) and transaction security mechanisms (SIG(0) and TSIG) make use of particular subsets of these algorithms.

The algorithm used for key signing should be a recommended one and it should be strong. When enabling DNSSEC for a managed zone, or creating a managed zone with DNSSEC, the DNSSEC signing algorithms and the denial-of-existence type can be selected. Changing the DNSSEC settings is only effective for a managed zone if DNSSEC is not already enabled. If the need exists to change the settings for a managed zone where it has been enabled, turn DNSSEC off and then re-enable it with different settings.

## Audit:

Currently there is no support to audit this setting through the console.

## From Command Line:

Ensure the property algorithm for keyType zone signing is not using RSASHA1.

```
gcloud dns managed-zones describe --
format="json(dnsName,dnssecConfig.state,dnssecConfig.defaultKeySpecs)"
```

#### **Remediation:**

1. If the need exists to change the settings for a managed zone where it has been enabled, DNSSEC must be turned off and then re-enabled with different settings. To turn off DNSSEC, run following command:

gcloud dns managed-zones update ZONE\_NAME --dnssec-state off

2. To update zone-signing for a reported managed DNS Zone, run the following command:

```
gcloud dns managed-zones update ZONE_NAME --dnssec-state on --ksk-algorithm
KSK_ALGORITHM --ksk-key-length KSK_KEY_LENGTH --zsk-algorithm ZSK_ALGORITHM -
-zsk-key-length ZSK KEY LENGTH --denial-of-existence DENIAL OF EXISTENCE
```

Supported algorithm options and key lengths are as follows.

Algorithm	KSK Length	ZSK Length
RSASHA1	1024,2048	1024,2048
RSASHA256	1024,2048	1024,2048
RSASHA512	1024,2048	1024,2048
ECDSAP256SHA256	256	384
ECDSAP384SHA384	384	384

#### **References:**

1. <u>https://cloud.google.com/dns/dnssec-advanced#advanced\_signing\_options</u>

#### **Additional Information:**

- 1. RSASHA1 zone-signing support may be required for compatibility reasons.
- 2. The remediation CLI works well with gcloud-cli version 221.0.0 and later.

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process</u> <u>for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	•	•	•

Controls Version	Control	IG 1	IG 2	IG 3
v7	11.1 <u>Maintain Standard Security Configurations for Network</u> <u>Devices</u> Maintain standard, documented security configuration standards for all authorized network devices.		•	•

## 3.6 Ensure That SSH Access Is Restricted From the Internet (Automated)

## **Profile Applicability:**

• Level 2

## **Description**:

GCP Firewall Rules are specific to a VPC Network. Each rule either allows or denies traffic when its conditions are met. Its conditions allow the user to specify the type of traffic, such as ports and protocols, and the source or destination of the traffic, including IP addresses, subnets, and instances.

Firewall rules are defined at the VPC network level and are specific to the network in which they are defined. The rules themselves cannot be shared among networks. Firewall rules only support IPv4 traffic. When specifying a source for an ingress rule or a destination for an egress rule by address, only an IPv4 address or IPv4 block in CIDR notation can be used. Generic (0.0.0.0/0) incoming traffic from the internet to VPC or VM instance using SSH on Port 22 can be avoided.

## **Rationale:**

GCP Firewall Rules within a VPC Network apply to outgoing (egress) traffic from instances and incoming (ingress) traffic to instances in the network. Egress and ingress traffic flows are controlled even if the traffic stays within the network (for example, instance-to-instance communication). For an instance to have outgoing Internet access, the network must have a valid Internet gateway route or custom route whose destination IP is specified. This route simply defines the path to the Internet, to avoid the most general (0.0.0/0) destination IP Range specified from the Internet through SSH with the default Port 22. Generic access from the Internet to a specific IP Range needs to be restricted.

## Impact:

All Secure Shell (SSH) connections from outside of the network to the concerned VPC(s) will be blocked. There could be a business need where SSH access is required from outside of the network to access resources associated with the VPC. In that case, specific source IP(s) should be mentioned in firewall rules to white-list access to SSH port for the concerned VPC(s).

## Audit:

#### From the Console:

- 1. Go to VPC network.
- 2. Go to the Firewall Rules.
- 3. Ensure that Port is not equal to 22 and Action is not set to Allow.
- 4. Ensure IP Ranges is not equal to 0.0.0.0/0 under Source filters.

#### **From Command Line:**

```
gcloud compute firewall-rules list --
format=table'(name,direction,sourceRanges,allowed)'
```

Ensure that there is no rule matching the below criteria:

- SOURCE\_RANGES is 0.0.0/0
- AND DIRECTION is INGRESS
- AND IPProtocol is top or All
- AND PORTS is set to 22 or range containing 22 or Null (not set)

#### Note:

- When ALL TCP ports are allowed in a rule, PORT does not have any value set (NULL)
- When ALL Protocols are allowed in a rule, PORT does not have any value set (NULL)

#### **Remediation:**

#### From the Console:

- 1. Go to VPC Network.
- $2. \ Go \ to \ the \ {\tt Firewall Rules}.$
- 3. Click the Firewall Rule you want to modify.
- 4. Click Edit.
- 5. Modify Source IP ranges to specific IP.
- 6. Click Save.

#### **From Command Line:**

1.Update the Firewall rule with the new SOURCE RANGE from the below command:

```
gcloud compute firewall-rules update FirewallName --allow=[PROTOCOL[:PORT[-
PORT]],...] --source-ranges=[CIDR_RANGE,...]
```

#### **References:**

- 1. <u>https://cloud.google.com/vpc/docs/firewalls#blockedtraffic</u>
- 2. <u>https://cloud.google.com/blog/products/identity-security/cloud-iap-enables-context-aware-access-to-vms-via-ssh-and-rdp-without-bastion-hosts</u>

#### Additional Information:

Currently, GCP VPC only supports IPV4; however, Google is already working on adding IPV6 support for VPC. In that case along with source IP range 0.0.0.0, the rule should be checked for IPv6 equivalent ::0 as well.

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	•	•	
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	٠	•	•
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are <u>Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		•	•
v7	12.4 <u>Deny Communication over Unauthorized Ports</u> Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.		•	

## 3.7 Ensure That RDP Access Is Restricted From the Internet (Automated)

## **Profile Applicability:**

• Level 2

## **Description**:

GCP Firewall Rules are specific to a VPC Network. Each rule either allows or denies traffic when its conditions are met. Its conditions allow users to specify the type of traffic, such as ports and protocols, and the source or destination of the traffic, including IP addresses, subnets, and instances.

Firewall rules are defined at the VPC network level and are specific to the network in which they are defined. The rules themselves cannot be shared among networks. Firewall rules only support IPv4 traffic. When specifying a source for an ingress rule or a destination for an egress rule by address, an IPv4 address or IPv4 block in CIDR notation can be used. Generic (0.0.0.0/0) incoming traffic from the Internet to a VPC or VM instance using RDP on Port 3389 can be avoided.

## **Rationale:**

GCP Firewall Rules within a VPC Network. These rules apply to outgoing (egress) traffic from instances and incoming (ingress) traffic to instances in the network. Egress and ingress traffic flows are controlled even if the traffic stays within the network (for example, instance-to-instance communication). For an instance to have outgoing Internet access, the network must have a valid Internet gateway route or custom route whose destination IP is specified. This route simply defines the path to the Internet, to avoid the most general (0.0.0/0) destination IP Range specified from the Internet through RDP with the default Port 3389. Generic access from the Internet to a specific IP Range should be restricted.

## Impact:

All Remote Desktop Protocol (RDP) connections from outside of the network to the concerned VPC(s) will be blocked. There could be a business need where secure shell access is required from outside of the network to access resources associated with the VPC. In that case, specific source IP(s) should be mentioned in firewall rules to white-list access to RDP port for the concerned VPC(s).

## Audit:

#### From the Console:

- 1. Go to VPC network.
- $2. \ Go \ to \ the \ {\tt Firewall Rules}.$
- 3. Ensure Port is not equal to 3389 and Action is not Allow.
- 4. Ensure IP Ranges is not equal to 0.0.0.0/0 under Source filters.

#### **From Command Line:**

```
gcloud compute firewall-rules list --
format=table'(name,direction,sourceRanges,allowed.ports)'
```

Ensure that there is no rule matching the below criteria:

- SOURCE\_RANGES is 0.0.0.0/0
- AND DIRECTION is INGRESS
- AND IPProtocol is TCP or All
- AND PORTS is set to 3389 or range containing 3389 or Null (not set)

#### Note:

- When ALL TCP ports are allowed in a rule, PORT does not have any value set (NULL)
- When ALL Protocols are allowed in a rule, PORT does not have any value set (NULL)

#### **Remediation:**

#### From the Console:

- 1. Go to VPC Network.
- $2. \ Go \ to \ the \ {\tt Firewall Rules}.$
- 3. Click the Firewall Rule to be modified.
- 4. Click Edit.
- 5. Modify Source IP ranges to specific IP.
- 6. Click Save.

#### From Command Line:

1.Update RDP Firewall rule with new SOURCE RANGE from the below command:

```
gcloud compute firewall-rules update FirewallName --allow=[PROTOCOL[:PORT[-
PORT]],...] --source-ranges=[CIDR_RANGE,...]
```

#### **References:**

- 1. <u>https://cloud.google.com/vpc/docs/firewalls#blockedtraffic</u>
- 2. <u>https://cloud.google.com/blog/products/identity-security/cloud-iap-enables-context-aware-access-to-vms-via-ssh-and-rdp-without-bastion-hosts</u>

#### Additional Information:

Currently, GCP VPC only supports IPV4; however, Google is already working on adding IPV6 support for VPC. In that case along with source IP range 0.0.0.0, the rule should be checked for IPv6 equivalent ::0 as well.

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	•		
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	٠	•	•
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are <u>Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		•	•
v7	12.4 <u>Deny Communication over Unauthorized Ports</u> Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.			

## 3.8 Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network (Automated)

## **Profile Applicability:**

• Level 1

## **Description:**

Flow Logs is a feature that enables users to capture information about the IP traffic going to and from network interfaces in the organization's VPC Subnets. Once a flow log is created, the user can view and retrieve its data in Stackdriver Logging. It is recommended that Flow Logs be enabled for every business-critical VPC subnet.

## **Rationale:**

VPC networks and subnetworks not reserved for internal HTTP(S) load balancing provide logically isolated and secure network partitions where GCP resources can be launched. When Flow Logs are enabled for a subnet, VMs within that subnet start reporting on all Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) flows. Each VM samples the TCP and UDP flows it sees, inbound and outbound, whether the flow is to or from another VM, a host in the on-premises datacenter, a Google service, or a host on the Internet. If two GCP VMs are communicating, and both are in subnets that have VPC Flow Logs enabled, both VMs report the flows.

Flow Logs supports the following use cases:

- Network monitoring
- Understanding network usage and optimizing network traffic expenses
- Network forensics
- Real-time security analysis

Flow Logs provide visibility into network traffic for each VM inside the subnet and can be used to detect anomalous traffic or provide insight during security workflows.

The Flow Logs must be configured such that all network traffic is logged, the interval of logging is granular to provide detailed information on the connections, no logs are filtered, and metadata to facilitate investigations are included.

**Note**: Subnets reserved for use by internal HTTP(S) load balancers do not support VPC flow logs.
# Impact:

Standard pricing for Stackdriver Logging, BigQuery, or Cloud Pub/Sub applies. VPC Flow Logs generation will be charged starting in GA as described in reference: <u>https://cloud.google.com/vpc/</u>

#### Audit:

#### From Console:

- 1. Go to the VPC network GCP Console visiting
   https://console.cloud.google.com/networking/networks/list
- 2. From the list of network subnets, make sure for each subnet:
  - Flow Logs is set to On
  - Aggregation Interval is set to 5 sec
  - Include metadata checkbox is checked
  - Sample rate is set to 100%

**Note**: It is not possible to determine if a Log filter has been defined from the console. **From Command Line**:

```
gcloud compute networks subnets list --format json | \
 jq -r
'(["Subnet", "Purpose", "Flow Logs", "Aggregation Interval", "Flow Sampling", "Met
adata", "Logs Filtered"] | (., map(length*"-"))),
        (.[] |
          Γ
            .name,
            .purpose,
            (if has("enableFlowLogs") and .enableFlowLogs == true then
"Enabled" else "Disabled" end),
            (if has("logConfig") then .logConfig.aggregationInterval else
"N/A" end),
            (if has("logConfig") then .logConfig.flowSampling else "N/A"
end),
            (if has("logConfig") then .logConfig.metadata else "N/A" end),
            (if has("logConfig") then (.logConfig | has("filterExpr")) else
"N/A" end)
          1
        ) |
        @tsv' | \
  column -t
```

The output of the above command will list:

- each subnet
- the subnet's purpose
- a Enabled or Disabled value if Flow Logs are enabled

- the value for  $\mbox{Aggregation Interval or N/A}$  if disabled, the value for  $\mbox{Flow Sampling or N/A}$  if disabled
- the value for Metadata or N/A if disabled
- 'true' or 'false' if a Logging Filter is configured or 'N/A' if disabled.

If the subnet's purpose is private then flow  $\mbox{Logs}$  should be  $\mbox{Enabled}.$ 

If  ${\tt Flow}\ {\tt Logs}\ is enabled then:$ 

- Aggregation\_Interval should be INTERVAL\_5\_SEC
- Flow\_Sampling should be 1
- Metadata should be INCLUDE\_ALL\_METADATA
- Logs\_Filtered should be false.

#### **Remediation:**

#### From Console:

- 1. Go to the VPC network GCP Console visiting https://console.cloud.google.com/networking/networks/list
- 2. Click the name of a subnet, The Subnet details page displays.
- 3. Click the EDIT button.
- 4. Set Flow Logs to On.
- 5. Expand the Configure Logs section.
- 6. Set Aggregation Interval to 5 SEC.
- 7. Check the box beside Include metadata.
- 8. Set Sample rate to 100.
- 9. Click Save.

#### **Note**: It is not possible to configure a Log filter from the console.

#### From Command Line:

To enable VPC Flow Logs for a network subnet, run the following command:

```
gcloud compute networks subnets update [SUBNET_NAME] --region [REGION] --
enable-flow-logs --logging-aggregation-interval=interval-5-sec --logging-
flow-sampling=1 --logging-metadata=include-all
```

#### **Default Value:**

By default, Flow Logs is set to Off when a new VPC network subnet is created.

#### **References:**

- 1. <u>https://cloud.google.com/vpc/docs/using-flow-logs#enabling vpc flow logging</u>
- 2. https://cloud.google.com/vpc/

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.		•	•
v8	13.6 <u>Collect Network Traffic Flow Logs</u> Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		•	•
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.		•	
v7	12.8 <u>Deploy NetFlow Collection on Networking Boundary</u> <u>Devices</u> Enable the collection of NetFlow and logging data on all network boundary devices.		•	•

# 3.9 Ensure No HTTPS or SSL Proxy Load Balancers Permit SSL Policies With Weak Cipher Suites (Manual)

# **Profile Applicability:**

• Level 1

# **Description:**

Secure Sockets Layer (SSL) policies determine what port Transport Layer Security (TLS) features clients are permitted to use when connecting to load balancers. To prevent usage of insecure features, SSL policies should use (a) at least TLS 1.2 with the MODERN profile; or (b) the RESTRICTED profile, because it effectively requires clients to use TLS 1.2 regardless of the chosen minimum TLS version; or (3) a CUSTOM profile that does not support any of the following features:

```
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

# **Rationale:**

Load balancers are used to efficiently distribute traffic across multiple servers. Both SSL proxy and HTTPS load balancers are external load balancers, meaning they distribute traffic from the Internet to a GCP network. GCP customers can configure load balancer SSL policies with a minimum TLS version (1.0, 1.1, or 1.2) that clients can use to establish a connection, along with a profile (Compatible, Modern, Restricted, or Custom) that specifies permissible cipher suites. To comply with users using outdated protocols, GCP load balancers can be configured to permit insecure cipher suites. In fact, the GCP default SSL policy uses a minimum TLS version of 1.0 and a Compatible profile, which allows the widest range of insecure cipher suites. As a result, it is easy for customers to configure a load balancer without even knowing that they are permitting outdated cipher suites.

# Impact:

Creating more secure SSL policies can prevent clients using older TLS versions from establishing a connection.

# Audit:

#### From Console:

- 1. See all load balancers by visiting <u>https://console.cloud.google.com/net-services/loadbalancing/loadBalancers/list</u>.
- 2. For each load balancer for SSL (Proxy) or HTTPS, click on its name to go the Load balancer details page.
- 3. Ensure that each target proxy entry in the Frontend table has an SSL Policy configured.
- 4. Click on each SSL policy to go to its SSL policy details page.
- 5. Ensure that the SSL policy satisfies one of the following conditions:
- has a Min TLS set to TLS 1.2 and Profile set to Modern profile, or
- has Profile set to Restricted. Note that a Restricted profile effectively requires clients to use TLS 1.2 regardless of the chosen minimum TLS version, or
- has Profile set to Custom and the following features are all disabled:

```
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

#### **From Command Line:**

1. List all TargetHttpsProxies and TargetSslProxies.

```
gcloud compute target-https-proxies list
gcloud compute target-ssl-proxies list
```

2. For each target proxy, list its properties:

gcloud compute target-https-proxies describe TARGET\_HTTPS\_PROXY\_NAME gcloud compute target-ssl-proxies describe TARGET\_SSL PROXY NAME

3. Ensure that the sslPolicy field is present and identifies the name of the SSL policy:

```
sslPolicy:
https://www.googleapis.com/compute/v1/projects/PROJECT_ID/global/sslPolicies/
SSL POLICY NAME
```

If the sslPolicy field is missing from the configuration, it means that the GCP default policy is used, which is insecure.

#### 4. Describe the SSL policy:

gcloud compute ssl-policies describe SSL\_POLICY\_NAME

- 5. Ensure that the policy satisfies one of the following conditions:
- has Profile set to Modern and minTlsVersion set to TLS\_1\_2, or
- has Profile set to Restricted, or
- has Profile set to Custom and enabledFeatures does not contain any of the following values:

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

#### **Remediation:**

#### From Console:

If the TargetSSLProxy or TargetHttpsProxy does not have an SSL policy configured, create a new SSL policy. Otherwise, modify the existing insecure policy.

- 2. Navigate to the SSL Policies page by visiting: https://console.cloud.google.com/net-security/sslpolicies
- 3. Click on the name of the insecure policy to go to its SSL policy details page.
- 4. Click EDIT.
- 5. Set Minimum TLS version to TLS 1.2.
- 6. Set Profile to Modern or Restricted.
- 7. Alternatively, if teh user selects the profile Custom, make sure that the following features are disabled:

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

#### From Command Line:

1. For each insecure SSL policy, update it to use secure cyphers:

```
gcloud compute ssl-policies update NAME [--profile
COMPATIBLE|MODERN|RESTRICTED|CUSTOM] --min-tls-version 1.2 [--custom-features
FEATURES]
```

2. If the target proxy has a GCP default SSL policy, use the following command corresponding to the proxy type to update it.

```
gcloud compute target-ssl-proxies update TARGET_SSL_PROXY_NAME --ssl-policy
SSL_POLICY_NAME
gcloud compute target-https-proxies update TARGET_HTTPS_POLICY_NAME --ssl-
policy SSL POLICY NAME
```

#### **Default Value:**

The GCP default SSL policy is the least secure setting: Min TLS 1.0 and Compatible profile

#### **References:**

- 1. <u>https://cloud.google.com/load-balancing/docs/use-ssl-policies</u>
- 2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		•	•
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.		•	•

# 3.10 Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed' (Manual)

# **Profile Applicability:**

• Level 2

# **Description**:

IAP authenticates the user requests to your apps via a Google single sign in. You can then manage these users with permissions to control access. It is recommended to use both IAP permissions and firewalls to restrict this access to your apps with sensitive information.

# **Rationale:**

IAP ensure that access to VMs is controlled by authenticating incoming requests. Access to your apps and the VMs should be restricted by firewall rules that allow only the proxy IAP IP addresses contained in the 35.235.240.0/20 subnet. Otherwise, unauthenticated requests can be made to your apps. To ensure that load balancing works correctly health checks should also be allowed.

#### Impact:

If firewall rules are not configured correctly, legitimate business services could be negatively impacted. It is recommended to make these changes during a time of low usage.

# Audit:

From the Console:

- 1. For each of your apps that have IAP enabled go to the Cloud Console VPC network > Firewall rules.
- 2. Verify that the only rules correspond to the following values:

```
    Targets: All instances in the network
    Source IP ranges

            IAP Proxy Addresses
            35.235.240.0/20
                  Google Health Check
            130.211.0.0/22
                 Google Health Check
            35.191.0.0/16

    Protocols and ports:
```

- Specified protocols and ports required for access and management of your app. For example most health check connection protocols would be covered by;
- tcp:80 (Default HTTP Health Check port)
- tcp:443--(Default HTTPS Health Check port)
   Note: if you have custom ports used by your load balancers, you will need to list them here

# **Remediation:**

From the Console:

- 1. Go to the Cloud Console <u>VPC network > Firewall rules</u>.
- 2. Select the checkbox next to the following rules:
  - default-allow-http
  - default-allow-https
  - default-allow-internal
- 3. Click **Delete**.
- 4. Click **Create firewall rule** and set the following values:

0

Name: allow-iap-traffic

0

- Targets: All instances in the network
- **Source IP ranges** (press Enter after you paste each value in the box, copy the value below the bold text including the dash):

IAP Proxy Addresses

- 35.235.240.0/20

Google Health Check

- 130.211.0.0/22
  - \*\*```Google Health Check
- 0

# **Protocols and ports**:

- Specified protocols and ports required for access and management of your app. For example most health check connection protocols would be covered by;
- tcp:80 (Default HTTP Health Check port)
- tcp:443--(Default HTTPS Health Check port)

# Note: if you have custom ports used by your load balancers, you will need to list them here

5. When you're finished updating values, click **Create**.

#### **Default Value:**

By default all traffic is allowed.

#### **References:**

- 1. <u>https://cloud.google.com/iap/docs/concepts-overview</u>
- 2. <u>https://cloud.google.com/iap/docs/concepts-overview</u>
- 3. <u>https://cloud.google.com/iap/docs/load-balancer-howto</u>
- 4. https://cloud.google.com/load-balancing/docs/health-checks
- <u>https://cloud.google.com/blog/products/identity-security/cloud-iap-enables-</u> <u>context-aware-access-to-vms-via-ssh-and-rdp-without-bastion-hosts</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 <u>Centralize Account Management</u> Centralize account management through a directory or identity service.		•	
v7	16.2 <u>Configure Centralized Point of Authentication</u> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		•	•

# **4** Virtual Machines

This section covers recommendations addressing virtual machines on Google Cloud Platform.

# 4.1 Ensure That Instances Are Not Configured To Use the Default Service Account (Automated)

# Profile Applicability:

• Level 1

# **Description**:

It is recommended to configure your instance to not use the default Compute Engine service account because it has the Editor role on the project.

# **Rationale:**

The default Compute Engine service account has the Editor role on the project, which allows read and write access to most Google Cloud Services. To defend against privilege escalations if your VM is compromised and prevent an attacker from gaining access to all of your project, it is recommended to not use the default Compute Engine service account. Instead, you should create a new service account and assigning only the permissions needed by your instance.

The default Compute Engine service account is named [PROJECT\_NUMBER] - compute@developer.gserviceaccount.com.

# Audit:

# From Console:

- Go to the VM instances page by visiting: <u>https://console.cloud.google.com/compute/instances</u>.
- 2. Click on each instance name to go to its VM instance details page.
- 3. Under the section API and identity management, ensure that the default Compute Engine service account is not used. This account is named [PROJECT\_NUMBER] compute@developer.gserviceaccount.com.

# From Command Line:

1. List the instances in your project and get details on each instance:

```
gcloud compute instances list --format=json | jq -r '. | "SA:
\(.[].serviceAccounts[].email) Name: \(.[].name)"'
```

2. Ensure that the service account section has an email that does not match the pattern [PROJECT\_NUMBER]-compute@developer.gserviceaccount.com.

#### **Exception**:

VMs created by GKE should be excluded. These VMs have names that start with gke- and are labeled goog-gke-node.

#### **Remediation:**

#### From Console:

- Go to the VM instances page by visiting: <u>https://console.cloud.google.com/compute/instances</u>.
- 2. Click on the instance name to go to its VM instance details page.
- 3. Click STOP and then click EDIT.
- 4. Under the section API and identity management, select a service account other than the default Compute Engine service account. You may first need to create a new service account.
- 5. Click save and then click START.

#### From Command Line:

1. Stop the instance:

gcloud compute instances stop <INSTANCE NAME>

2. Update the instance:

```
gcloud compute instances set-service-account <INSTANCE_NAME> --service-
account=<SERVICE ACCOUNT>
```

3. Restart the instance:

gcloud compute instances start <INSTANCE NAME>

#### **Default Value:**

By default, Compute instances are configured to use the default Compute Engine service account.

#### **References:**

- 1. https://cloud.google.com/compute/docs/access/service-accounts
- 2. <u>https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances</u>

# 3. <u>https://cloud.google.com/sdk/gcloud/reference/compute/instances/set-service-account</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 <u>Manage Default Accounts on Enterprise Assets and</u> <u>Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	•	•	•
v7	4.7 <u>Limit Access to Script Tools</u> Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.		•	•

# 4.2 Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs (Automated)

# **Profile Applicability:**

• Level 1

# **Description:**

To support principle of least privileges and prevent potential privilege escalation it is recommended that instances are not assigned to default service account Compute Engine default service account with Scope Allow full access to all Cloud APIs.

# **Rationale:**

Along with ability to optionally create, manage and use user managed custom service accounts, Google Compute Engine provides default service account Compute Engine default service account for an instances to access necessary cloud services. Project Editor role is assigned to Compute Engine default service account hence, This service account has almost all capabilities over all cloud services except billing. However, when Compute Engine default service account assigned to an instance it can operate in 3 scopes.

```
    Allow default access: Allows only minimum access required to run an
Instance (Least Privileges)
    Allow full access to all Cloud APIs: Allow full access to all the cloud
APIs/Services (Too much access)
    Set access for each API: Allows Instance administrator to choose only
those APIs that are needed to perform specific business functionality
expected by instance
```

When an instance is configured with <code>Compute Engine default service account</code> with Scope <code>Allow full access to all Cloud APIs</code>, based on IAM roles assigned to the user(s) accessing Instance, it may allow user to perform cloud operations/API calls that user is not supposed to perform leading to successful privilege escalation.

# Impact:

In order to change service account or scope for an instance, it needs to be stopped.

#### Audit:

#### From Console:

- Go to the VM instances page by visiting: <u>https://console.cloud.google.com/compute/instances</u>.
- 2. Click on each instance name to go to its VM instance details page.
- 3. Under the API and identity management, ensure that Cloud API access scopes is not set to Allow full access to all Cloud APIs.

#### From Command Line:

1. List the instances in your project and get details on each instance:

```
gcloud compute instances list --format=json | jq -r '. | "SA Scopes:
\(.[].serviceAccounts[].scopes) Name: \(.[].name)"'
```

2. Ensure that the service account section has an email that does not match the pattern [PROJECT\_NUMBER]-compute@developer.gserviceaccount.com.

#### Exception:

VMs created by GKE should be excluded. These VMs have names that start with gke- and are labeled `goog-gke-node

#### **Remediation:**

#### From Console:

- Go to the VM instances page by visiting: https://console.cloud.google.com/compute/instances.
- 2. Click on the impacted VM instance.
- 3. If the instance is not stopped, click the stop button. Wait for the instance to be stopped.
- 4. Next, click the Edit button.
- 5. Scroll down to the Service Account section.
- 6. Select a different service account or ensure that Allow full access to all Cloud APIs is not selected.
- 7. Click the save button to save your changes and then click START.

#### From Command Line:

1. Stop the instance:

gcloud compute instances stop <INSTANCE\_NAME>

#### 2. Update the instance:

```
gcloud compute instances set-service-account <INSTANCE_NAME> --service-
account=<SERVICE_ACCOUNT> --scopes [SCOPE1, SCOPE2...]
```

#### 3. Restart the instance:

gcloud compute instances start <INSTANCE NAME>

#### **Default Value:**

While creating an VM instance, default service account is used with scope Allow default access.

#### **References:**

- 1. <u>https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances</u>
- 2. <u>https://cloud.google.com/compute/docs/access/service-accounts</u>

#### Additional Information:

- User IAM roles will override service account scope but configuring minimal scope ensures defense in depth
- Non-default service accounts do not offer selection of access scopes like default service account. IAM roles with non-default service accounts should be used to control VM access.

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 <u>Manage Default Accounts on Enterprise Assets and</u> <u>Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	•	•	•
v7	4.7 Limit Access to Script Tools Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.		•	

# 4.3 Ensure "Block Project-Wide SSH Keys" Is Enabled for VM Instances (Automated)

# **Profile Applicability:**

• Level 1

# **Description**:

It is recommended to use Instance specific SSH key(s) instead of using common/shared project-wide SSH key(s) to access Instances.

# **Rationale:**

Project-wide SSH keys are stored in Compute/Project-meta-data. Project wide SSH keys can be used to login into all the instances within project. Using project-wide SSH keys eases the SSH key management but if compromised, poses the security risk which can impact all the instances within project. It is recommended to use Instance specific SSH keys which can limit the attack surface if the SSH keys are compromised.

#### Impact:

Users already having Project-wide ssh key pairs and using third party SSH clients will lose access to the impacted Instances. For Project users using gcloud or GCP Console based SSH option, no manual key creation and distribution is required and will be handled by GCE (Google Compute Engine) itself. To access Instance using third party SSH clients Instance specific SSH key pairs need to be created and distributed to the required users.

# Audit:

# From Console:

- Go to the VM instances page by visiting <u>https://console.cloud.google.com/compute/instances</u>. It will list all the instances in your project.
- 2. For every instance, click on the name of the instance.
- 3. Under SSH Keys, ensure Block project-wide SSH keys is selected.

# From Command Line:

1. List the instances in your project and get details on each instance:

gcloud compute instances list --format=json

2. Ensure key: block-project-ssh-keys is set to value: 'true'.

#### **Remediation:**

#### From Console:

- Go to the VM instances page by visiting: <u>https://console.cloud.google.com/compute/instances</u>. It will list all the instances in your project.
- 2. Click on the name of the Impacted instance
- 3. Click Edit in the toolbar
- 4. Under SSH Keys, go to the Block project-wide SSH keys checkbox
- 5. To block users with project-wide SSH keys from connecting to this instance, select Block project-wide SSH keys
- $6. \quad Click \text{ save at the bottom of the page}$
- 7. Repeat steps for every impacted Instance

# From Command Line:

To block project-wide public SSH keys, set the metadata value to TRUE:

gcloud compute instances add-metadata <INSTANCE\_NAME> --metadata blockproject-ssh-keys=TRUE

# **Default Value:**

By Default Block Project-wide SSH keys is not enabled.

#### **References:**

- 1. <u>https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys</u>
- 2. <u>https://cloud.google.com/sdk/gcloud/reference/topic/formats</u>

# Additional Information:

If OS Login is enabled, SSH keys in instance metadata are ignored, and therefore blocking project-wide SSH keys is not necessary.

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10</b> Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		•	•

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14- character password for accounts not using MFA.	•	•	•
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		•	•
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		•	•

# 4.4 Ensure Oslogin Is Enabled for a Project (Automated)

# **Profile Applicability:**

• Level 1

# **Description**:

Enabling OS login binds SSH certificates to IAM users and facilitates effective SSH certificate management.

# **Rationale:**

Enabling osLogin ensures that SSH keys used to connect to instances are mapped with IAM users. Revoking access to IAM user will revoke all the SSH keys associated with that particular user. It facilitates centralized and automated SSH key pair management which is useful in handling cases like response to compromised SSH key pairs and/or revocation of external/third-party/Vendor users.

# Impact:

Enabling OS Login on project disables metadata-based SSH key configurations on all instances from a project. Disabling OS Login restores SSH keys that you have configured in project or instance meta-data.

# Audit:

# From Console:

- 1. Go to the VM compute metadata page by visiting https://console.cloud.google.com/compute/metadata.
- 2. Ensure that key enable-oslogin is present with value set to TRUE.
- 3. Because instances can override project settings, ensure that no instance has custom metadata with key enable-oslogin and value FALSE.

# From Command Line:

1. List the instances in your project and get details on each instance:

gcloud compute instances list --format=json

2. Verify that the section commonInstanceMetadata has a key enable-oslogin set to value TRUE.

#### **Exception**:

VMs created by GKE should be excluded. These VMs have names that start with  $\tt gke-$  and are labeled  $\tt goog-gke-node$ 

#### **Remediation:**

#### From Console:

- 1. Go to the VM compute metadata page by visiting: <u>https://console.cloud.google.com/compute/metadata</u>.
- 2. Click Edit.
- 3. Add a metadata entry where the key is enable-oslogin and the value is TRUE.
- 4. Click save to apply the changes.
- 5. For every instances that overrides the project setting, go to the VM Instances page at <u>https://console.cloud.google.com/compute/instances</u>.
- 6. Click the name of the instance on which you want to remove the metadata value.
- 7. At the top of the instance details page, click Edit to edit the instance settings.
- 8. Under Custom metadata, remove any entry with key enable-oslogin and the value is FALSE
- 9. At the bottom of the instance details page, click save to apply your changes to the instance.

#### From Command Line:

1. Configure oslogin on the project:

gcloud compute project-info add-metadata --metadata enable-oslogin=TRUE

2. Remove instance metadata that overrides the project setting.

```
gcloud compute instances remove-metadata <INSTANCE_NAME> --keys=enable-
oslogin
```

Optionally, you can enable two factor authentication for OS login. For more information, see: <u>https://cloud.google.com/compute/docs/oslogin/setup-two-factor-authentication</u>.

#### **Default Value:**

By default, parameter enable-oslogin is not set, which is equivalent to setting it to FALSE.

#### **References:**

1. <u>https://cloud.google.com/compute/docs/instances/managing-instance-access</u>

- 2. <u>https://cloud.google.com/compute/docs/instances/managing-instance-access#enable\_oslogin</u>
- 3. <u>https://cloud.google.com/sdk/gcloud/reference/compute/instances/remove-metadata</u>
- 4. <u>https://cloud.google.com/compute/docs/oslogin/setup-two-factor-authentication</u>

# Additional Information:

1. In order to use osLogin, instance using Custom Images must have the latest version of the Linux Guest Environment installed. The following image families do not yet support OS Login:

```
Project cos-cloud (Container-Optimized OS) image family cos-stable.
All project coreos-cloud (CoreOS) image families
Project suse-cloud (SLES) image family sles-11
All Windows Server and SQL Server image families
```

2. Project enable-oslogin can be over-ridden by setting enable-oslogin parameter to an instance metadata individually.

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 <u>Centralize Account Management</u> Centralize account management through a directory or identity service.		•	
v8	6.7 <u>Centralize Access Control</u> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		•	•
v7	16.2 <u>Configure Centralized Point of Authentication</u> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		•	

# 4.5 Ensure 'Enable Connecting to Serial Ports' Is Not Enabled for VM Instance (Automated)

# **Profile Applicability:**

• Level 1

# **Description**:

Interacting with a serial port is often referred to as the serial console, which is similar to using a terminal window, in that input and output is entirely in text mode and there is no graphical interface or mouse support.

If you enable the interactive serial console on an instance, clients can attempt to connect to that instance from any IP address. Therefore interactive serial console support should be disabled.

# **Rationale:**

A virtual machine instance has four virtual serial ports. Interacting with a serial port is similar to using a terminal window, in that input and output is entirely in text mode and there is no graphical interface or mouse support. The instance's operating system, BIOS, and other system-level entities often write output to the serial ports, and can accept input such as commands or answers to prompts. Typically, these system-level entities use the first serial port (port 1) and serial port 1 is often referred to as the serial console.

The interactive serial console does not support IP-based access restrictions such as IP whitelists. If you enable the interactive serial console on an instance, clients can attempt to connect to that instance from any IP address. This allows anybody to connect to that instance if they know the correct SSH key, username, project ID, zone, and instance name.

Therefore interactive serial console support should be disabled.

# Audit:

# From Console:

- 1. Login to Google Cloud console
- 2. Go to Computer Engine
- 3. Go to VM instances
- 4. Click on the Specific VM
- 5. Ensure Enable connecting to serial ports below Remote access block is unselected.

#### From Command Line:

Ensure the below command's output shows null:

```
gcloud compute instances describe <vmName> --zone=<region> --
format="json(metadata.items[].key,metadata.items[].value)"
```

or key and value properties from below command's json response are equal to serial-port-enable and 0 or false respectively.

#### **Remediation:**

#### From Console:

- 1. Login to Google Cloud console
- 2. Go to Computer Engine
- 3. Go to VM instances
- 4. Click on the Specific VM
- 5. Click EDIT
- 6. Unselect Enable connecting to serial ports below Remote access block.
- $7. \ Click \, {\tt Save}$

#### From Command Line:

Use the below command to disable

```
gcloud compute instances add-metadata <INSTANCE_NAME> --zone=<ZONE> --
metadata=serial-port-enable=false
```

or

```
gcloud compute instances add-metadata <INSTANCE_NAME> --zone=<ZONE> --
metadata=serial-port-enable=0
```

#### **Prevention:**

You can prevent VMs from having serial port access enable by Disable VM serial port access organization policy:

https://console.cloud.google.com/iam-admin/orgpolicies/computedisableSerialPortAccess.

# **Default Value:**

By default, connecting to serial ports is not enabled.

# **References:**

1. <u>https://cloud.google.com/compute/docs/instances/interacting-with-serial-console</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise</u> <u>Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		•	•
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are</u> <u>Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		•	•

# 4.6 Ensure That IP Forwarding Is Not Enabled on Instances (Automated)

# **Profile Applicability:**

• Level 1

# **Description**:

Compute Engine instance cannot forward a packet unless the source IP address of the packet matches the IP address of the instance. Similarly, GCP won't deliver a packet whose destination IP address is different than the IP address of the instance receiving the packet. However, both capabilities are required if you want to use instances to help route packets.

Forwarding of data packets should be disabled to prevent data loss or information disclosure.

# **Rationale:**

Compute Engine instance cannot forward a packet unless the source IP address of the packet matches the IP address of the instance. Similarly, GCP won't deliver a packet whose destination IP address is different than the IP address of the instance receiving the packet. However, both capabilities are required if you want to use instances to help route packets. To enable this source and destination IP check, disable the canIpForward field, which allows an instance to send and receive packets with non-matching destination or source IPs.

#### Impact:

Deleting instance(s) acting as routers/packet forwarders may break the network connectivity.

#### Audit:

#### From Console:

- Go to the VM Instances page by visiting: <u>https://console.cloud.google.com/compute/instances</u>.
- 2. For every instance, click on its name to go to the VM instance details page.
- 3. Under the Network interfaces section, ensure that IP forwarding is set to Off for every network interface.

#### From Command Line:

1. List all instances:

2. Ensure that CAN\_IP\_FORWARD column in the output of above command does not contain True for any VM instance.

#### **Exception**:

Instances created by GKE should be excluded because they need to have IP forwarding enabled and cannot be changed. Instances created by GKE have names that start with "gke-".

#### **Remediation:**

You only edit the canIpForward setting at instance creation time. Therefore, you need to delete the instance and create a new one where canIpForward is set to false.

#### From Console:

- 1. Go to the VM Instances page by visiting: https://pantheon.corp.google.com/compute/instances.
- 2. Select the VM Instance you want to remediate.
- 3. Click the Delete button.
- 4. On the 'VM Instances' page, click `CREATE INSTANCE'.
- 5. Create a new instance with the desired configuration. By default, the instance is configured to not allow IP forwarding.

#### From Command Line:

1. Delete the instance:

gcloud compute instances delete INSTANCE\_NAME

2. Create a new instance to replace it, with IP forwarding set to Off

gcloud compute instances create

#### **Default Value:**

By default, instances are not configured to allow IP forwarding.

#### **References:**

1. <u>https://cloud.google.com/vpc/docs/using-routes#canipforward</u>

#### Additional Information:

You can only set the canIpForward field at instance creation time. After an instance is created, the field becomes read-only.

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	•	•	
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	•	•	•
v7	11.1 <u>Maintain Standard Security Configurations for Network</u> <u>Devices</u> Maintain standard, documented security configuration standards for all authorized network devices.		•	
v7	<b>11.2</b> Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		•	

# 4.7 Ensure VM Disks for Critical VMs Are Encrypted With Customer-Supplied Encryption Keys (CSEK) (Automated)

# **Profile Applicability:**

• Level 2

# **Description**:

Customer-Supplied Encryption Keys (CSEK) are a feature in Google Cloud Storage and Google Compute Engine. If you supply your own encryption keys, Google uses your key to protect the Google-generated keys used to encrypt and decrypt your data. By default, Google Compute Engine encrypts all data at rest. Compute Engine handles and manages this encryption for you without any additional actions on your part. However, if you wanted to control and manage this encryption yourself, you can provide your own encryption keys.

# **Rationale:**

By default, Google Compute Engine encrypts all data at rest. Compute Engine handles and manages this encryption for you without any additional actions on your part. However, if you wanted to control and manage this encryption yourself, you can provide your own encryption keys.

If you provide your own encryption keys, Compute Engine uses your key to protect the Google-generated keys used to encrypt and decrypt your data. Only users who can provide the correct key can use resources protected by a customer-supplied encryption key.

Google does not store your keys on its servers and cannot access your protected data unless you provide the key. This also means that if you forget or lose your key, there is no way for Google to recover the key or to recover any data encrypted with the lost key.

At least business critical VMs should have VM disks encrypted with CSEK.

#### Impact:

If you lose your encryption key, you will not be able to recover the data.

# Audit:

# From Console:

- 1. Go to Compute Engine Disks by visiting: https://console.cloud.google.com/compute/disks.
- 2. Click on the disk for your critical VMs to see its configuration details.
- 3. Ensure that  ${\tt Encryption}$  type is set to  ${\tt Customer}$  supplied.

# From Command Line:

Ensure <code>diskEncryptionKey</code> property in the below command's response is not null, and contains key <code>sha256</code> with corresponding value

```
gcloud compute disks describe <DISK_NAME> --zone <ZONE> --
format="json(diskEncryptionKey,name)"
```

#### **Remediation:**

Currently there is no way to update the encryption of an existing disk. Therefore you should create a new disk with Encryption set to Customer supplied.

#### From Console:

- 1. Go to Compute Engine Disks by visiting: https://console.cloud.google.com/compute/disks.
- 2. Click CREATE DISK.
- 3. Set Encryption type to Customer supplied,
- 4. Provide the Key in the box.
- 5. Select Wrapped key.
- 6. Click Create.

# From Command Line:

In the gcloud compute tool, encrypt a disk using the --csek-key-file flag during instance creation. If you are using an RSA-wrapped key, use the gcloud beta component:

```
gcloud compute instances create <INSTANCE_NAME> --csek-key-file <example-
file.json>
```

To encrypt a standalone persistent disk:

gcloud compute disks create <DISK\_NAME> --csek-key-file <example-file.json>

# **Default Value:**

By default, VM disks are encrypted with Google-managed keys. They are not encrypted with Customer-Supplied Encryption Keys.

#### **References:**

- 1. <u>https://cloud.google.com/compute/docs/disks/customer-supplied-encryption#encrypt a new persistent disk with your own keys</u>
- 2. <u>https://cloud.google.com/compute/docs/reference/rest/v1/disks/get</u>
- 3. <u>https://cloud.google.com/compute/docs/disks/customer-supplied-encryption#key\_file</u>

# Additional Information:

Note 1: When you delete a persistent disk, Google discards the cipher keys, rendering the data irretrievable. This process is irreversible.

Note 2: It is up to you to generate and manage your key. You must provide a key that is a 256-bit string encoded in RFC 4648 standard base64 to Compute Engine.

Note 3: An example key file looks like this.

```
Γ
  {
  "uri": "https://www.googleapis.com/compute/v1/projects/myproject/zones/us-
central1-a/disks/example-disk",
  "key": "acXTX3rxrKAFTF0tYVLvydU1riRZTvUNC4q5I11NY-c=",
  "key-type": "raw"
  },
  {
  "uri":
"https://www.googleapis.com/compute/v1/projects/myproject/global/snapshots/my
-private-snapshot",
  "kev":
"ieCx/NcW06PcT7Ep1X6LUTc/hLvUDYyzSZPPVCVPTVEohpeHASqC8uw5TzyO9U+Fka9JFHz0mBib
XUInrC/jEk014kCK/NPjYgEMOyssZ4ZINPKxlUh2zn1bV+MCaTICrdmuSBTWlUUiFoDD6PYznLwh8
ZNdaheCeZ8ewEXqFQ8V+sDroLaN3Xs3MDTXQEMMoNUXMCZEIpq9Vtp9x2oeQ5lAbtt7bYAAHf5l+q
JWw3sUfs0/Glw5fpdjT8Ugqrr+RMZezGrltJEF293rvTIjWOEB3z5OHyHwQkvdrPDFcTqsLfh+8Hr
8g+mf+7zVPEC8nEbqpdl3GPv3A7AwpFp7MA=="
  "key-type": "rsa-encrypted"
  }
```

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		•	•
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			•

# 4.8 Ensure Compute Instances Are Launched With Shielded VM Enabled (Automated)

# **Profile Applicability:**

• Level 2

# **Description**:

To defend against against advanced threats and ensure that the boot loader and firmware on your VMs are signed and untampered, it is recommended that Compute instances are launched with Shielded VM enabled.

# **Rationale:**

Shielded VMs are virtual machines (VMs) on Google Cloud Platform hardened by a set of security controls that help defend against rootkits and bootkits.

Shielded VM offers verifiable integrity of your Compute Engine VM instances, so you can be confident your instances haven't been compromised by boot- or kernel-level malware or rootkits. Shielded VM's verifiable integrity is achieved through the use of Secure Boot, virtual trusted platform module (vTPM)-enabled Measured Boot, and integrity monitoring.

Shielded VM instances run firmware which is signed and verified using Google's Certificate Authority, ensuring that the instance's firmware is unmodified and establishing the root of trust for Secure Boot.

Integrity monitoring helps you understand and make decisions about the state of your VM instances and the Shielded VM vTPM enables Measured Boot by performing the measurements needed to create a known good boot baseline, called the integrity policy baseline. The integrity policy baseline is used for comparison with measurements from subsequent VM boots to determine if anything has changed.

Secure Boot helps ensure that the system only runs authentic software by verifying the digital signature of all boot components, and halting the boot process if signature verification fails.

# Audit:

# From Console:

 Go to the VM instances page by visiting: <u>https://console.cloud.google.com/compute/instances</u>.

- 2. Click on the instance name to see its VM instance details page.
- 3. Under the section Shielded VM, ensure that vTPM and Integrity Monitoring are on.

# From Command Line:

1. For each instance in your project, get its metadata:

```
gcloud compute instances list --format=json | jq -r '. | "vTPM:
\(.[].shieldedInstanceConfig.enableVtpm) IntegrityMonitoring:
\(.[].shieldedInstanceConfig.enableIntegrityMonitoring) Name: \(.[].name)"'
```

2. Ensure that there is a shieldedInstanceConfig configuration and that configuration has the enableIntegrityMonitoring and enableVtpm set to true. If the VM is not a Shield VM image, you will not see a shieldedInstanceConfig` in the output.

#### **Remediation:**

To be able turn on Shielded VM on an instance, your instance must use an image with Shielded VM support.

#### From Console:

- Go to the VM instances page by visiting: https://console.cloud.google.com/compute/instances.
- 2. Click on the instance name to see its VM instance details page.
- 3. Click STOP to stop the instance.
- 4. When the instance has stopped, click EDIT.
- 5. In the Shielded VM section, select Turn on vTPM and Turn on Integrity Monitoring.
- 6. Optionally, if you do not use any custom or unsigned drivers on the instance, also select Turn on Secure Boot.
- 7. Click the save button to modify the instance and then click START to restart it.

# From Command Line:

You can only enable Shielded VM options on instances that have Shielded VM support. For a list of Shielded VM public images, run the gcloud compute images list command with the following flags:

gcloud compute images list --project gce-uefi-images --no-standard-images

1. Stop the instance:

gcloud compute instances stop <INSTANCE\_NAME>

#### 2. Update the instance:

```
gcloud compute instances update <INSTANCE_NAME> --shielded-vtpm --shielded-
vm-integrity-monitoring
```

3. Optionally, if you do not use any custom or unsigned drivers on the instance, also turn on secure boot.

gcloud compute instances update <INSTANCE\_NAME> --shielded-vm-secure-boot

4. Restart the instance:

gcloud compute instances start <INSTANCE\_NAME>

#### **Prevention:**

You can ensure that all new VMs will be created with Shielded VM enabled by setting up an Organization Policy to for shielded VM at <a href="https://console.cloud.google.com/iam-admin/orgpolicies/compute-requireShieldedVm">https://console.cloud.google.com/iam-admin/orgpolicies/compute-requireShieldedVm</a>. Learn more at: <a href="https://cloud.google.com/security/shielded-cloud/shielded-vm#organization-policy-constraint">https://cloud.google.com/security/shielded-cloud/shielded-vm#organization-policy-constraint</a>.

#### **Default Value:**

By default, Compute Instances do not have Shielded VM enabled.

#### **References:**

- 1. <u>https://cloud.google.com/compute/docs/instances/modifying-shielded-vm</u>
- 2. <u>https://cloud.google.com/shielded-vm</u>
- 3. <u>https://cloud.google.com/security/shielded-cloud/shielded-vm#organization-policy-constraint</u>

#### Additional Information:

If you do use custom or unsigned drivers on the instance, enabling Secure Boot will cause the machine to no longer boot. Turn on Secure Boot only on instances that have been verified to not have any custom drivers installed.

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.2 <u>Maintain Secure Images</u> Maintain secure images or templates for all systems in the enterprise based on the		•	
Controls Version	Control	IG 1	IG 2	IG 3
---------------------	---	------	------	------
	organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.			

# 4.9 Ensure That Compute Instances Do Not Have Public IP Addresses (Automated)

#### Profile Applicability:

• Level 2

#### **Description:**

Compute instances should not be configured to have external IP addresses.

#### **Rationale:**

To reduce your attack surface, Compute instances should not have public IP addresses. Instead, instances should be configured behind load balancers, to minimize the instance's exposure to the internet.

#### Impact:

Removing the external IP address from your Compute instance may cause some applications to stop working.

#### Audit:

#### From Console:

- Go to the VM instances page by visiting: <u>https://console.cloud.google.com/compute/instances</u>.
- 2. For every VM, ensure that there is no External IP configured.

#### From Command Line:

gcloud compute instances list --format=json

2. The output should not contain an accessConfigs section under networkInterfaces. Note that the natIP value is present only for instances that are running or for instances that are stoped but have a static IP address. For instances that are stopped and are configured to have an ephemeral public IP address, the natIP field will not be present. Example output:

```
networkInterfaces:
```

```
- accessConfigs:
```

```
- kind: compute#accessConfig
```

```
name: External NAT
```

```
networkTier: STANDARD
type: ONE TO ONE NAT
```

#### **Exception:**

Instances created by GKE should be excluded because some of them have external IP addresses and cannot be changed by editing the instance settings. Instances created by GKE should be excluded. These instances have names that start with "gke-" and are labeled "goog-gke-node".

#### **Remediation:**

#### From Console:

- Go to the VM instances page by visiting: <u>https://console.cloud.google.com/compute/instances</u>.
- 2. Click on the instance name to go the the Instance detail page.
- 3. Click Edit.
- 4. For each Network interface, ensure that External IP is set to None.
- 5. Click Done and then click Save.

#### From Command Line:

1. Describe the instance properties:

gcloud compute instances describe <INSTANCE NAME> --zone=<ZONE>

2. Identify the access config name that contains the external IP address. This access config appears in the following format:

```
networkInterfaces:
- accessConfigs:
- kind: compute#accessConfig
name: External NAT
natIP: 130.211.181.55
type: ONE_TO_ONE_NAT
```

2. Delete the access config.

```
gcloud compute instances delete-access-config <INSTANCE_NAME> --zone=<ZONE> -
-access-config-name <ACCESS_CONFIG_NAME>
```

In the above example, the <code>access\_config\_NAME</code> is <code>External NAT</code>. The name of your access config might be different.

#### **Prevention:**

You can configure the Define allowed external IPs for VM instances Organization

Policy to prevent VMs from being configured with public IP addresses. Learn more at: <u>https://console.cloud.google.com/orgpolicies/compute-vmExternalIpAccess</u>

#### **Default Value:**

By default, Compute instances have a public IP address.

#### **References:**

- 1. <u>https://cloud.google.com/load-balancing/docs/backend-</u> service#backends and external ip addresses
- 2. <u>https://cloud.google.com/compute/docs/instances/connecting-advanced#sshbetweeninstances</u>
- 3. <u>https://cloud.google.com/compute/docs/instances/connecting-to-instance</u>
- 4. <u>https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#unassign\_ip</u>
- 5. <u>https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints</u>

#### Additional Information:

You can connect to Linux VMs that do not have public IP addresses by using Identity-Aware Proxy for TCP forwarding. Learn more at <a href="https://cloud.google.com/compute/docs/instances/connecting-">https://cloud.google.com/compute/docs/instances/connecting-</a>

advanced#sshbetweeninstances

For Windows VMs, see <u>https://cloud.google.com/compute/docs/instances/connecting-to-instance</u>.

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	٠	•	•
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.		•	•

# *4.10 Ensure That App Engine Applications Enforce HTTPS Connections (Manual)*

#### **Profile Applicability:**

• Level 2

#### **Description**:

In order to maintain the highest level of security all connections to an application should be secure by default.

#### **Rationale:**

Insecure HTTP connections maybe subject to eavesdropping which can expose sensitive data.

#### Impact:

All connections to appengine will automatically be redirected to the HTTPS endpoint ensuring that all connections are secured by TLS.

#### Audit:

Verify that the app.yaml file controlling the application contains a line which enforces secure connections. For example

```
handlers:
- url: /.*
secure: always
redirect_http_response_code: 301
script: auto
```

https://cloud.google.com/appengine/docs/standard/python3/config/appref

#### **Remediation:**

Add a line to the app.yaml file controlling the application which enforces secure connections. For example

```
handlers:
- url: /.*
 **secure: always**
 redirect_http_response_code: 301
 script: auto
```

[https://cloud.google.com/appengine/docs/standard/python3/config/appref]

#### **Default Value:**

By default both HTTP and HTTP are supported

#### **References:**

- 1. <u>https://cloud.google.com/appengine/docs/standard/python3/config/appref</u>
- 2. https://cloud.google.com/appengine/docs/flexible/nodejs/configuring-your-appwith-app-yaml

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		•	•
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		•	•
v7	18.5 <u>Use Only Standardized and Extensively Reviewed</u> <u>Encryption Algorithms</u> Use only standardized and extensively reviewed encryption algorithms.		•	•

# *4.11 Ensure That Compute Instances Have Confidential Computing Enabled (Automated)*

#### Profile Applicability:

• Level 2

#### **Description:**

Google Cloud encrypts data at-rest and in-transit, but customer data must be decrypted for processing. Confidential Computing is a breakthrough technology which encrypts data in-use—while it is being processed. Confidential Computing environments keep data encrypted in memory and elsewhere outside the central processing unit (CPU).

Confidential VMs leverage the Secure Encrypted Virtualization (SEV) feature of AMD EPYC<sup>™</sup> CPUs. Customer data will stay encrypted while it is used, indexed, queried, or trained on. Encryption keys are generated in hardware, per VM, and not exportable. Thanks to built-in hardware optimizations of both performance and security, there is no significant performance penalty to Confidential Computing workloads.

#### **Rationale:**

Confidential Computing enables customers' sensitive code and other data encrypted in memory during processing. Google does not have access to the encryption keys. Confidential VM can help alleviate concerns about risk related to either dependency on Google infrastructure or Google insiders' access to customer data in the clear.

#### Impact:

- Confidential Computing for Compute instances does not support live migration. Unlike regular Compute instances, Confidential VMs experience disruptions during maintenance events like a software or hardware update.
- Additional charges may be incurred when enabling this security feature. See <a href="https://cloud.google.com/compute/confidential-vm/pricing">https://cloud.google.com/compute/confidential-vm/pricing</a> for more info.

#### Audit:

Note: Confidential Computing is currently only supported on N2D machines. To learn more about types of N2D machines, visit <u>https://cloud.google.com/compute/docs/machine-types#n2d machine types</u>

#### From Console:

- Go to the VM instances page by visiting: <u>https://console.cloud.google.com/compute/instances</u>.
- 2. Click on the instance name to see its VM instance details page.
- 3. Ensure that Confidential VM service is Enabled.

#### **From Command Line:**

1. List the instances in your project and get details on each instance:

```
gcloud compute instances list --format=json
```

2. Ensure that enableConfidentialCompute is set to true for all instances with machine type starting with "n2d-".

```
confidentialInstanceConfig:
   enableConfidentialCompute: true
```

#### **Remediation:**

Confidential Computing can only be enabled when an instance is created. You must delete the current instance and create a new one.

#### From Console:

- 1. Go to the VM instances page by visiting: https://console.cloud.google.com/compute/instances.
- $2. Click {\tt CREATE INSTANCE}.$
- 3. Fill out the desired configuration for your instance.
- 4. Under the Confidential VM service section, check the option Enable the Confidential Computing service on this VM instance.
- 5. Click Create.

#### From Command Line:

Create a new instance with Confidential Compute enabled.

```
gcloud beta compute instances create <INSTANCE_NAME> --zone <ZONE> --
confidential-compute --maintenance-policy=TERMINATE
```

#### **Default Value:**

By default, Confidential Computing is disabled for Compute instances.

#### **References:**

- 1. <u>https://cloud.google.com/compute/confidential-vm/docs/creating-cvm-instance</u>
- 2. <u>https://cloud.google.com/compute/confidential-vm/docs/about-cvm</u>
- 3. <u>https://cloud.google.com/confidential-computing</u>
- 4. <u>https://cloud.google.com/blog/products/identity-security/introducing-google-cloud-confidential-computing-with-confidential-vms</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11</b> <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		•	•
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

# 4.12 Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects (Manual)

#### **Profile Applicability:**

• Level 2

#### **Description**:

For the virtual machines where you manage the operating system in Infrastructure as a Service (IaaS), you are responsible for keeping these operating systems and programs up to date. There are multiple ways to manage updates yourself that would be difficult to fit into one recommendation. Check the CIS Benchmarks for each of your Operating Systems as well for potential solutions there. In this recommendation we will use a feature in Google Cloud via its VM manager API to manage updates called Operating System Patch Management (referred to OS Patch Management from here on out). This may requires installing the OS Config API if it is not already installed. Also if you install custom operating systems, they may not functionally support the local OS config agent required to gather operating system patch information and issue update commands. These update commands are the default Linux and Windows commands to install updates such as yum or apt. This feature allows for a central management to issue those commands. OS Patch management also does not host the updates itself, so your VMs will need to be public or be able to access the internet. This is not the only Patch Management solution available to your organization and you should weigh your needs before committing to using this.

#### **Rationale:**

Keeping an operating system up to date is the best way to secure against ever evolving known vulnerabilities and bugs in programs that can be used in cyber attacks by bad actors.

#### Impact:

Most Operating Systems require a restart or changing critical resources to apply the updates. Make certain to apply updates during a time of low availability, as unforeseen complications may cause an outage of services. Using the Google Cloud VM manager for its OS Patch management will incur additional costs for each VM managed by it. Please view the VM manager pricing reference for further information.

#### Audit:

#### Verifying that VM Manager and related services are installed on your Compute Operating Systems on a project by project basis

#### Determine if OS Config API is Enabled for the Project

- 1. Navigate into a project. In the expanded hamburger menu located at the top left of the screen hover over "APIs & Services". Then in the menu right of that select "API Libraries"
- 2. Search for "VM Manager (OS Config API) or scroll down in the left hand column and select the filter labeled "Compute" where it is the last listed. Open this API.
- 3. Verify the blue button at the top is enabled.

#### Determine if VM Instances have correct metadata tags for OSConfig parsing

- 1. From the main Google Cloud console, open the hamburger menu in the top left. Mouse over Computer Engine to expand the menu next to it.
- 2. Under the "Settings" heading, select "Metadata".
- 3. In this view there will be a list of the project wide metadata tags for VMs. Determine if the tag "enable-osconfig" is set to "true".

# Determine if the Operating System of VM Instances have the local OS-Config Agent running

There is no way to determine this from the Google Cloud console. The only way is to run operating specific commands locally inside the operating system via remote connection. For the sake of brevity of this recommendation please view the docs/troubleshooting/vm-manager/verify-setup reference at the bottom of the page. If you initialized your VM instance with a Google Supplied OS Image with a build date of later than v20200114 it will have the service installed. You should still determine its status for proper operation.

# Verify the service account you have setup for the project in Recommendation 4.1 is running

- Go to the VM instances page by visiting: https://console.cloud.google.com/compute/instances.
- 2. Click on each instance name to go to its VM instance details page.
- 3. Under the section Service Account, take note of the service account

4. Run the commands locally for your operating system that are located at the docs/troubleshooting/vm-manager/verify-setup#service-account-enabled reference located at the bottom of this page. They should return the name of your service account.

#### Determine if Instances can connect to public update hosting

Linux Debian Based Operating Systems

sudo apt update

The output should have a numbered list of lines with Hit: URL of updates. Redhat Based Operating Systems

yum check-update

The output should show a list of packages that have updates available. Windows

ping http://windowsupdate.microsoft.com/

The ping should successfully be delivered and received.

#### **Determine if OS Config API is Enabled for the Project**

1. In each project you wish to enable run the following command

gcloud services list

2. If osconfig.googleapis.com is in the left hand column it is enabled for this project.

#### Determine if VM Manager is Enabled for the Project

1. Within the project run the following command:

gcloud compute instances os-inventory describe VM-NAME \
--zone=ZONE

#### The output will look like

```
        INSTANCE_ID
        INSTANCE_NAME
        OS

        OSCONFIG_AGENT_VERSION
        UPDATE_TIME

        29255009728795105
        centos7
        CentOS Linux 7 (Core)

        20210217.00-g1.el7
        2021-04-12T22:19:36.559Z

        5138980234596718741
        rhel-8
        Red Hat Enterprise Linux 8.3 (Ootpa)

        20210316.00-g1.el8
        2021-09-16T17:19:24Z
```

## 7127836223366142250 windows Microsoft Windows Server 2019 Datacenter 20210316.00.0+win@1 2021-09-16T17:13:18Z

#### Determine if VM Instances have correct metadata tags for OSConfig parsing

1. Select the project you want to view tagging in.

Google Cloud Console

- 1. From the main Google Cloud console, open the hamburger menu in the top left. Mouse over Computer Engine to expand the menu next to it.
- 2. Under the "Settings" heading, select "Metadata".
- 3. In this view there will be a list of the project wide metadata tags for Vms. Verify a tag of 'enable-osconfig' is in this list and it is set to 'true'.

Command Line

Run the following command to view instance data

gcloud compute instances list --format="table(name, status, tags.list())"

On each instance it should have a tag of 'enable-osconfig' set to 'true'

## Determine if the Operating System of VM Instances have the local OS-Config Agent running

There is no way to determine this from the Google Cloud CLI. The best way is to run the the commands inside the operating system located at 'Check OS-Config agent is installed and running' at the /docs/troubleshooting/vm-manager/verify-setup reference at the bottom of the page. If you initialized your VM instance with a Google Supplied OS Image with a build date of later than v20200114 it will have the service installed. You should still determine its status.

## Verify the service account you have setup for the project in Recommendation 4.1 is running

- Go to the VM instances page by visiting: <u>https://console.cloud.google.com/compute/instances</u>.
- 2. Click on each instance name to go to its VM instance details page.
- 3. Under the section Service Account, take note of the service account
- 4. View the compute/docs/troubleshooting/vm-manager/verify-setup#serviceaccount-enabled resource at the bottom of the page for operating system specific commands to run locally.

#### **Determine if Instances can connect to public update hosting**

Linux Debian Based Operating Systems

sudo apt update

The output should have a numbered list of lines with Hit: URL of updates. Redhat Based Operating Systems

yum check-update

The output should show a list of packages that have updates available. Windows

ping http://windowsupdate.microsoft.com/

The ping should successfully be delivered and received.

#### **Remediation:**

#### **Enabling OS Patch Management on a Project by Project Basis**

#### **Install OS Config API for the Project**

- 1. Navigate into a project. In the expanded hamburger menu located at the top left of the screen hover over "APIs & Services". Then in the menu right of that select "API Libraries"
- 2. Search for "VM Manager (OS Config API) or scroll down in the left hand column and select the filter labeled "Compute" where it is the last listed. Open this API.
- 3. Click the blue 'Enable' button.

#### Add MetaData Tags for OSConfig Parsing

- 1. From the main Google Cloud console, open the hamburger menu in the top left. Mouse over Computer Engine to expand the menu next to it.
- 2. Under the "Settings" heading, select "Metadata".
- 3. In this view there will be a list of the project wide metadata tags for VMs. Click edit and 'add item' in the key column type 'enable-osconfig' and in the value column set it to 'true'.

#### **From Command Line**

1. For project wide tagging, run the following command

```
gcloud compute project-info add-metadata \
    --project <PROJECT_ID>\
    --metadata=enable-osconfig=TRUE
```

Please see the reference /compute/docs/troubleshooting/vm-manager/verifysetup#metadata-enabled at the bottom for more options like instance specific tagging. Note: Adding a new tag via commandline may overwrite existing tags. You will need to do this at a time of low usage for the least impact.

#### Install and Start the Local OSConfig for Data Parsing

There is no way to centrally manage or start the Local OSConfig agent. Please view the reference of manage-os#agent-install to view specific operating system commands.

#### Setup a project wide Service Account

Please view Recommendation 4.1 to view how to setup a service account. Rerun the audit procedure to test if it has taken effect.

# Enable NAT or Configure Private Google Access to allow Access to Public Update Hosting

For the sake of brevity, please see the attached resources to enable NAT or Private Google Access. Rerun the audit procedure to test if it has taken effect. From Command Line:

#### Install OS Config API for the Project

1. In each project you wish to audit run gcloud services enable osconfig.googleapis.com

#### Install and Start the Local OSConfig for Data Parsing

Please view the reference of manage-os#agent-install to view specific operating system commands.

#### Setup a project wide Service Account

Please view Recommendation 4.1 to view how to setup a service account. Rerun the audit procedure to test if it has taken effect.

# Enable NAT or Configure Private Google Access to allow Access to Public Update Hosting

For the sake of brevity, please see the attached resources to enable NAT or Private Google Access. Rerun the audit procedure to test if it has taken effect. Determine if Instances can connect to public update hosting

Linux

**Debian Based Operating Systems** 

sudo apt update

The output should have a numbered list of lines with Hit: URL of updates. **Redhat Based Operating Systems** 

yum check-update

The output should show a list of packages that have updates available. Windows

ping http://windowsupdate.microsoft.com/

The ping should successfully be delivered and received.

#### **Default Value:**

By default most operating systems and programs do not update themselves. The Google Cloud VM Manager which is a dependency of the OS Patch management feature is installed on Google Built OS images with a build date of v20200114 or later. The VM manager is not enabled in a project by default and will need to be setup.

#### **References:**

- 1. <u>https://cloud.google.com/compute/docs/manage-os</u>
- 2. https://cloud.google.com/compute/docs/os-patch-management
- 3. https://cloud.google.com/compute/docs/vm-manager
- 4. <u>https://cloud.google.com/compute/docs/images/os-details#vm-manager</u>
- 5. <u>https://cloud.google.com/compute/docs/vm-manager#pricing</u>
- 6. https://cloud.google.com/compute/docs/troubleshooting/vm-manager/verifysetup
- 7. <u>https://cloud.google.com/compute/docs/instances/view-os-details#view-data-</u> tools
- 8. <u>https://cloud.google.com/compute/docs/os-patch-management/create-patch-job</u>
- 9. https://cloud.google.com/nat/docs/set-up-network-address-translation
- 10. https://cloud.google.com/vpc/docs/configure-private-google-access
- 11. https://workbench.cisecurity.org/sections/811638/recommendations/1334335
- 12. <u>https://cloud.google.com/compute/docs/manage-os#agent-install</u>

- 13. <u>https://cloud.google.com/compute/docs/troubleshooting/vm-manager/verify-setup#service-account-enabled</u>
- 14. https://cloud.google.com/compute/docs/os-patch-management#use-dashboard
- 15. <u>https://cloud.google.com/compute/docs/troubleshooting/vm-manager/verify-setup#metadata-enabled</u>

#### Additional Information:

This is not your only solution to handle updates. This is a Google Cloud specific recommendation to leverage a resource to solve the need for comprehensive update procedures and policy. If you have a solution already in place you do not need to make the switch.

There are also further resources that would be out of the scope of this recommendation. If you need to allow your VMs to access public hosted updates, please see the reference to setup NAT or Private Google Access.

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	•	•	•
v7	2.2 <u>Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.		•	

### 5 Storage

This section covers recommendations addressing storage on Google Cloud Platform.

# 5.1 Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible (Automated)

#### **Profile Applicability:**

• Level 1

#### **Description**:

It is recommended that IAM policy on Cloud Storage bucket does not allows anonymous or public access.

#### **Rationale:**

Allowing anonymous or public access grants permissions to anyone to access bucket content. Such access might not be desired if you are storing any sensitive data. Hence, ensure that anonymous or public access to a bucket is not allowed.

#### Impact:

No storage buckets would be publicly accessible. You would have to explicitly administer bucket access.

#### Audit:

#### From Console:

- 1. Go to Storage browser by visiting https://console.cloud.google.com/storage/browser.
- 2. Click on each bucket name to go to its Bucket details page.
- 3. Click on the Permissions tab.
- 4. Ensure that allUsers and allAuthenticatedUsers are not in the Members list.

#### From Command Line:

1. List all buckets in a project

#### gsutil ls

2. Check the IAM Policy for each bucket:

gsutil iam get gs://BUCKET\_NAME

No role should contain allUsers and/or allAuthenticatedUsers as a member. Using Rest API

1. List all buckets in a project

Get https://www.googleapis.com/storage/v1/b?project=<ProjectName>

2. Check the IAM Policy for each bucket

GET https://www.googleapis.com/storage/v1/b/<bucketName>/iam

No role should contain allUsers and/or allAuthenticatedUsers as a member.

#### **Remediation:**

#### From Console:

- Go to Storage browser by visiting https://console.cloud.google.com/storage/browser.
- 2. Click on the bucket name to go to its Bucket details page.
- 3. Click on the Permissions tab.
- 4. Click Delete button in front of allUsers and allAuthenticatedUsers to remove that particular role assignment.

#### From Command Line:

 $Remove \; \texttt{allUsers} \; and \; \texttt{allAuthenticatedUsers} \; access.$ 

gsutil iam ch -d allUsers gs://BUCKET\_NAME
gsutil iam ch -d allAuthenticatedUsers gs://BUCKET NAME

#### **Prevention:**

You can prevent Storage buckets from becoming publicly accessible by setting up the Domain restricted sharing organization policy at:

https://console.cloud.google.com/iam-admin/orgpolicies/iamallowedPolicyMemberDomains.

#### **Default Value:**

By Default, Storage buckets are not publicly shared.

#### **References:**

- 1. <u>https://cloud.google.com/storage/docs/access-control/iam-reference</u>
- 2. <u>https://cloud.google.com/storage/docs/access-control/making-data-public</u>
- 3. <u>https://cloud.google.com/storage/docs/gsutil/commands/iam</u>

#### Additional Information:

To implement Access restrictions on buckets, configuring Bucket IAM is preferred way than configuring Bucket ACL. On GCP console, "Edit Permissions" for bucket exposes IAM configurations only. Bucket ACLs are configured automatically as per need in order to implement/support User enforced Bucket IAM policy. In-case administrator changes bucket ACL using command-line(gsutils)/API bucket IAM also gets updated automatically.

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	•	•	
v7	12.4 <u>Deny Communication over Unauthorized Ports</u> Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.			

### 5.2 Ensure That Cloud Storage Buckets Have Uniform Bucket-Level Access Enabled (Automated)

#### **Profile Applicability:**

• Level 2

#### **Description:**

It is recommended that uniform bucket-level access is enabled on Cloud Storage buckets.

#### **Rationale:**

It is recommended to use uniform bucket-level access to unify and simplify how you grant access to your Cloud Storage resources.

Cloud Storage offers two systems for granting users permission to access your buckets and objects: Cloud Identity and Access Management (Cloud IAM) and Access Control Lists (ACLs). These systems act in parallel - in order for a user to access a Cloud Storage resource, only one of the systems needs to grant the user permission. Cloud IAM is used throughout Google Cloud and allows you to grant a variety of permissions at the bucket and project levels. ACLs are used only by Cloud Storage and have limited permission options, but they allow you to grant permissions on a per-object basis.

In order to support a uniform permissioning system, Cloud Storage has uniform bucketlevel access. Using this feature disables ACLs for all Cloud Storage resources: access to Cloud Storage resources then is granted exclusively through Cloud IAM. Enabling uniform bucket-level access guarantees that if a Storage bucket is not publicly accessible, no object in the bucket is publicly accessible either.

#### Impact:

If you enable uniform bucket-level access, you revoke access from users who gain their access solely through object ACLs.

Certain Google Cloud services, such as Stackdriver, Cloud Audit Logs, and Datastore, cannot export to Cloud Storage buckets that have uniform bucket-level access enabled.

#### Audit:

#### From Console:

1. Open the Cloud Storage browser in the Google Cloud Console by visiting: https://console.cloud.google.com/storage/browser 2. For each bucket, make sure that Access control column has the value Uniform.

#### From Command Line:

1. List all buckets in a project

gsutil ls

2. For each bucket, verify that uniform bucket-level access is enabled.

gsutil uniformbucketlevelaccess get gs://BUCKET\_NAME/

If uniform bucket-level access is enabled, the response looks like:

```
Uniform bucket-level access setting for gs://BUCKET_NAME/:
    Enabled: True
    LockedTime: LOCK DATE
```

#### **Remediation:**

#### From Console:

- 1. Open the Cloud Storage browser in the Google Cloud Console by visiting: <u>https://console.cloud.google.com/storage/browser</u>
- 2. In the list of buckets, click on the name of the desired bucket.
- 3. Select the Permissions tab near the top of the page.
- 4. In the text box that starts with This bucket uses fine-grained access control..., click Edit.
- 5. In the pop-up menu that appears, select Uniform.
- 6. Click Save.

#### From Command Line:

Use the on option in a uniformbucketlevelaccess set command:

gsutil uniformbucketlevelaccess set on gs://BUCKET\_NAME/

#### Prevention

You can set up an Organization Policy to enforce that any new bucket has uniform bucket level access enabled. Learn more at:

https://cloud.google.com/storage/docs/setting-org-policies#uniform-bucket

#### **Default Value:**

By default, Cloud Storage buckets do not have uniform bucket-level access enabled.

#### **References:**

- 1. <u>https://cloud.google.com/storage/docs/uniform-bucket-level-access</u>
- 2. <u>https://cloud.google.com/storage/docs/using-uniform-bucket-level-access</u>
- 3. <u>https://cloud.google.com/storage/docs/setting-org-policies#uniform-bucket</u>

#### Additional Information:

Uniform bucket-level access can no longer be disabled if it has been active on a bucket for 90 consecutive days.

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3</b> <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	•	•	•
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	•	•	•

### 6 Cloud SQL Database Services

This section covers security recommendations to follow to secure Cloud SQL database services.

The recommendations in this section on setting up database flags are also present in the <u>CIS Oracle MySQL Community Server 5.7 Benchmarks</u> and in the <u>CIS PostgreSQL 12</u> <u>Benchmarks</u>. We, nevertheless, include them here as well, the remediation instructions are different on Cloud SQL. Settings these flags require superuser privileges and can only be configured through GCP controls.

Learn more at: <u>https://cloud.google.com/sql/docs/postgres/users</u> and <u>https://cloud.google.com/sql/docs/mysql/flags</u>.

## 6.1 MySQL Database

This section covers recommendations addressing Cloud SQL for MySQL on Google Cloud Platform.

### 6.1.1 Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges (Manual)

#### **Profile Applicability:**

• Level 1

#### **Description**:

It is recommended to set a password for the administrative user (root by default) to prevent unauthorized access to the SQL database instances.

This recommendation is applicable only for MySQL Instances. PostgreSQL does not offer any setting for No Password from the cloud console.

#### **Rationale:**

At the time of MySQL Instance creation, not providing an administrative password allows anyone to connect to the SQL database instance with administrative privileges. The root password should be set to ensure only authorized users have these privileges.

#### Impact:

Connection strings for administrative clients need to be reconfigured to use a password.

#### Audit:

#### **From Command Line:**

1. List All SQL database instances of type MySQL:

```
gcloud sql instances list --filter='DATABASE_VERSION:MYSQL* --project
<project_id> --format="(NAME,PRIMARY_ADDRESS)"'
```

2. For every MySQL instance try to connect using the **PRIMARY\_ADDRESS**, if available:

mysql -u root -h <mysql\_instance\_ip\_address>

The command should return either an error message or a password prompt. Sample Error message:

```
ERROR 1045 (28000): Access denied for user 'root'@'<Instance_IP>' (using password: NO)
```

If a command produces the mysql> prompt, the MySQL instance allows anyone to connect with administrative privileges without needing a password.

**Note:** The No Password setting is exposed only at the time of MySQL instance creation. Once the instance is created, the Google Cloud Platform Console does not expose the set to confirm whether a password for an administrative user is set to a MySQL instance.

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Platform Console using https://console.cloud.google.com/sql/
- 2. Select the instance to open its Overview page.
- 3. Select Access Control > Users.
- 4. Click the More actions icon for the user to be updated.
- 5. Select Change password, specify a New password, and click OK.

#### **From Command Line:**

1. Set a password to a MySql instance:

```
gcloud sql users set-password root --host=<host> --instance=<instance_name> -
-prompt-for-password
```

2. A prompt will appear, requiring the user to enter a password:

Instance Password:

3. With a successful password configured, the following message should be seen:

Updating Cloud SQL user...done.

#### **Default Value:**

From the Google Cloud Platform Console, the Create Instance workflow enforces the rule to enter the root password unless the option No Password is selected explicitly.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/mysql/create-manage-users</u>
- 2. <u>https://cloud.google.com/sql/docs/mysql/create-instance</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 <u>Manage Default Accounts on Enterprise Assets and</u> <u>Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	•	•	•
v7	4.2 <u>Change Default Passwords</u> Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.		•	•

### 6.1.2 Ensure 'Skip\_show\_database' Database Flag for Cloud SQL MySQL Instance Is Set to 'On' (Automated)

#### Profile Applicability:

• Level 1

#### **Description**:

It is recommended to set skip\_show\_database database flag for Cloud SQL Mysql instance to on

#### **Rationale:**

'skip\_show\_database' database flag prevents people from using the SHOW DATABASES statement if they do not have the SHOW DATABASES privilege. This can improve security if you have concerns about users being able to see databases belonging to other users. Its effect depends on the SHOW DATABASES privilege: If the variable value is ON, the SHOW DATABASES statement is permitted only to users who have the SHOW DATABASES privilege, and the statement displays all database names. If the value is OFF, SHOW DATABASES is permitted to all users, but displays the names of only those databases for which the user has the SHOW DATABASES or other privilege. This recommendation is applicable to Mysql database instances.

#### Audit:

#### Using Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Instance Overview page
- 3. Ensure the database flag skip\_show\_database that has been set is listed under the Database flags section.

#### **Using Command Line:**

1. List all Cloud SQL database Instances

gcloud sql instances list

2. Ensure the below command returns on for every Cloud SQL Mysql database instance

#### **Remediation:**

#### **Using Console:**

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the Mysql instance for which you want to enable to database flag.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag skip show database from the drop-down menu, and set its value to on.
- 6. Click save to save your changes.
- 7. Confirm your changes under Flags on the Overview page.

#### **Using Command Line:**

1. List all Cloud SQL database Instances

gcloud sql instances list

2. Configure the skip\_show\_database database flag for every Cloud SQL Mysql database instance using the below command.

```
gcloud sql instances patch INSTANCE_NAME --database-flags
skip_show_database=on
Note :
This command will overwrite all database flags previously set. To keep those
and add new ones, include the values for all flags you want set on the
instance; any flag not specifically included is set to its default value. For
flags that do not take a value, specify the flag name followed by an equals
sign ("=").
```

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/mysql/flags</u>
- 2. <u>https://dev.mysql.com/doc/refman/5.7/en/server-system-variables.html#sysvar\_skip\_show\_database</u>

#### **Additional Information:**

```
"WARNING: This patch modifies database flag values, which may require
```

https://cloud.google.com/sql/docs/mysql/flags - to see if your instance will be restarted when this patch is submitted. Note: some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines."

Note: Configuring the above flag restarts the Cloud SQL instance.

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3</b> <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	•	•	•
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	•	•	•

### 6.1.3 Ensure That the 'Local\_infile' Database Flag for a Cloud SQL MySQL Instance Is Set to 'Off' (Automated)

#### Profile Applicability:

• Level 1

#### **Description**:

It is recommended to set the <code>local\_infile</code> database flag for a Cloud SQL MySQL instance to <code>off</code>.

#### **Rationale:**

The <code>local\_infile</code> flag controls the server-side LOCAL capability for LOAD DATA statements. Depending on the <code>local\_infile</code> setting, the server refuses or permits local data loading by clients that have LOCAL enabled on the client side.

To explicitly cause the server to refuse LOAD DATA LOCAL statements (regardless of how client programs and libraries are configured at build time or runtime), start mysqld with local\_infile disabled. local\_infile can also be set at runtime.

Due to security issues associated with the <code>local\_infile</code> flag, it is recommended to disable it. This recommendation is applicable to MySQL database instances.

#### Impact:

Disabling <code>local\_infile</code> makes the server refuse local data loading by clients that have LOCAL enabled on the client side.

#### Audit:

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Instance Overview page
- 3. Ensure the database flag local\_infile that has been set is listed under the Database flags section.

#### From Command Line:

1. List all Cloud SQL database instances:

gcloud sql instances list

2. Ensure the below command returns off for every Cloud SQL MySQL database instance.

```
gcloud sql instances describe INSTANCE_NAME --format=json | jq
'.settings.databaseFlags[] | select(.name=="local infile")|.value'
```

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the MySQL instance where the database flag needs to be enabled.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag local\_infile from the drop-down menu, and set its value to off.
- 6. Click Save.
- 7. Confirm the changes under Flags on the Overview page.

#### From Command Line:

1. List all Cloud SQL database instances using the following command:

gcloud sql instances list

2. Configure the local\_infile database flag for every Cloud SQL Mysql database instance using the below command:

```
gcloud sql instances patch INSTANCE_NAME --database-flags local_infile=off
```

#### Note :

```
This command will overwrite all database flags that were previously set. To keep those and add new ones, include the values for all flags to be set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").
```

#### **Default Value:**

By default local\_infile is on.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/mysql/flags</u>
- 2. <u>https://dev.mysql.com/doc/refman/5.7/en/server-system-variables.html#sysvar\_local\_infile</u>
- 3. <u>https://dev.mysql.com/doc/refman/5.7/en/load-data-local.html</u>

#### **Additional Information:**

"WARNING: This patch modifies database flag values, which may require the instance to be restarted. Check the list of supported flags https://cloud.google.com/sql/docs/mysql/flags - to see if your instance will be restarted when this patch is submitted. Note: some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines."

Note: Configuring the above flag restarts the Cloud SQL instance.

## 6.2 PostgreSQL Database

This section covers recommendations addressing Cloud SQL for PostgreSQL on Google Cloud Platform.
## 6.2.1 Ensure 'Log\_error\_verbosity' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'DEFAULT' or Stricter (Manual)

### **Profile Applicability:**

• Level 2

### **Description:**

The log\_error\_verbosity flag controls the verbosity/details of messages logged. Valid values are:

- TERSE
- DEFAULT
- VERBOSE

TERSE excludes the logging of detail, Hint, Query, and Context error information.

VERBOSE output includes the SQLSTATE error code, source code file name, function name, and line number that generated the error.

Ensure an appropriate value is set to 'DEFAULT' or stricter.

#### **Rationale:**

Auditing helps in troubleshooting operational problems and also permits forensic analysis. If <code>log\_error\_verbosity</code> is not set to the correct value, too many details or too few details may be logged. This flag should be configured with a value of 'DEFAULT' or stricter. This recommendation is applicable to PostgreSQL database instances.

#### Impact:

Turning on logging will increase the required storage over time. Mismanaged logs may cause your storage costs to increase. Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

#### Audit:

#### From Console:

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.

- 2. Select the instance to open its Instance Overview page
- 3. Go to Configuration card
- 4. Under Database flags, check the value of log\_error\_verbosity flag is set to 'DEFAULT' or stricter.

#### From Command Line:

 Use the below command for every Cloud SQL PostgreSQL database instance to verify the value of log\_error\_verbosity

```
gcloud sql instances list --format=json | jq '.settings.databaseFlags[] |
select(.name=="log_error_verbosity")|.value'
```

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the PostgreSQL instance for which you want to enable the database flag.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag log\_error\_verbosity from the drop-down menu and set appropriate value.
- 6. Click Save to save your changes.
- 7. Confirm your changes under Flags on the Overview page.

#### From Command Line:

1. Configure the log\_error\_verbosity database flag for every Cloud SQL PosgreSQL database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags
log_error_verbosity=<TERSE|DEFAULT|VERBOSE>
Note: This command will overwrite all database flags previously set. To keep
those and add new ones, include the values for all flags you want set on the
instance; any flag not specifically included is set to its default value. For
flags that do not take a value, specify the flag name followed by an equals
sign ("=").
```

#### **Default Value:**

By default log\_error\_verbosity is default.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/postgres/flags</u>
- 2. <u>https://www.postgresql.org/docs/current/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHAT</u>

#### **Additional Information:**

WARNING: This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags - https://cloud.google.com/sql/docs/postgres/flags - to see if your instance will be restarted when this patch is submitted.

Note: some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

Note: Configuring the above flag does not require restarting the Cloud SQL instance.

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	•
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		•	•

## 6.2.2 Ensure That the 'Log\_connections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' (Automated)

### **Profile Applicability:**

• Level 1

### **Description**:

Enabling the log\_connections setting causes each attempted connection to the server to be logged, along with successful completion of client authentication. This parameter cannot be changed after the session starts.

#### **Rationale:**

PostgreSQL does not log attempted connections by default. Enabling the log\_connections setting will create log entries for each attempted connection as well as successful completion of client authentication which can be useful in troubleshooting issues and to determine any unusual connection attempts to the server. This recommendation is applicable to PostgreSQL database instances.

#### Impact:

Turning on logging will increase the required storage over time. Mismanaged logs may cause your storage costs to increase. Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

#### Audit:

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Instance Overview page.
- $3. \ \ Go \ to \ the \ {\tt Configuration} \ card.$
- 4. Under Database flags, check the value of log\_connections flag to determine if it is configured as expected.

#### From Command Line:

1. Ensure the below command returns on for every Cloud SQL PostgreSQL database instance:

```
gcloud sql instances list --format=json | jq '.settings.databaseFlags[] |
select(.name=="log connections")|.value'
```

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the PostgreSQL instance for which you want to enable the database flag.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag log\_connections from the drop-down menu and set the value as on.
- 6. Click Save.
- 7. Confirm the changes under Flags on the Overview page.

#### From Command Line:

1. Configure the log\_connections database flag for every Cloud SQL PosgreSQL database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags
log_connections=on
Note:
This command will overwrite all previously set database flags. To keep those
and add new ones, include the values for all flags to be set on the instance;
any flag not specifically included is set to its default value. For flags
that do not take a value, specify the flag name followed by an equals sign
("=").
```

#### **Default Value:**

 $By \ default \ \texttt{log\_connections} \ is \ \texttt{off.}$ 

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/postgres/flags</u>
- 2. <u>https://www.postgresql.org/docs/9.6/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHAT</u>

#### **Additional Information:**

WARNING: This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags - https://cloud.google.com/sql/docs/postgres/flags - to see if your instance will be restarted when this patch is submitted.

Note: some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see the Operational Guidelines.

```
Note: Configuring the above flag does not require restarting the Cloud SQL instance.
```

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			•

## 6.2.3 Ensure That the 'Log\_disconnections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' (Automated)

### **Profile Applicability:**

• Level 1

### **Description**:

Enabling the log\_disconnections setting logs the end of each session, including the session duration.

#### **Rationale:**

PostgreSQL does not log session details such as duration and session end by default. Enabling the log\_disconnections setting will create log entries at the end of each session which can be useful in troubleshooting issues and determine any unusual activity across a time period. The log\_disconnections and log\_connections work hand in hand and generally, the pair would be enabled/disabled together. This recommendation is applicable to PostgreSQL database instances.

#### Impact:

Turning on logging will increase the required storage over time. Mismanaged logs may cause your storage costs to increase. Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

#### Audit:

### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Instance Overview page
- 3. Go to the Configuration card.
- 4. Under Database flags, check the value of log\_disconnections flag is configured as expected.

#### From Command Line:

1. Ensure the below command returns on for every Cloud SQL PostgreSQL database instance:

```
gcloud sql instances list --format=json | jq '.settings.databaseFlags[] |
select(.name=="log disconnections")|.value'
```

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the PostgreSQL instance where the database flag needs to be enabled.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag log\_disconnections from the drop-down menu and set the value as on.
- 6. Click Save.
- 7. Confirm the changes under Flags on the Overview page.

#### **From Command Line:**

1. Configure the log\_disconnections database flag for every Cloud SQL PosgreSQL database instance using the below command:

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags log disconnections=on
```

Note: This command will overwrite all previously setdatabase flags. To keep those and add new ones, include the values for all flags to be set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

#### **Default Value:**

By default log disconnections is off.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/postgres/flags</u>
- 2. <u>https://www.postgresql.org/docs/9.6/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHAT</u>

#### Additional Information:

WARNING: This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags - https://cloud.google.com/sql/docs/postgres/flags - to see if your instance will be restarted when this patch is submitted.

Note: some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

```
Note: Configuring the above flag does not require restarting the Cloud SQL instance.
```

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			•
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		•	•

## 6.2.4 Ensure 'Log\_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately (Manual)

### **Profile Applicability:**

• Level 1

### **Description**:

The value of  $\log_{statement}$  flag determined the SQL statements that are logged. Valid values are:

- none
- ddl
- mod
- all

The value ddl logs all data definition statements. The value mod logs all ddl statements, plus data-modifying statements.

The statements are logged after a basic parsing is done and statement type is determined, thus this does not logs statements with errors. When using extended query protocol, logging occurs after an Execute message is received and values of the Bind parameters are included.

A value of 'ddl' is recommended unless otherwise directed by your organization's logging policy.

#### **Rationale:**

Auditing helps in forensic analysis. If <code>log\_statement</code> is not set to the correct value, too many statements may be logged leading to issues in finding the relevant information from the logs, or too few statements may be logged with relevant information missing from the logs. Setting log\_statement to align with your organization's security and logging policies facilitates later auditing and review of database activities. This recommendation is applicable to PostgreSQL database instances.

#### Impact:

Turning on logging will increase the required storage over time. Mismanaged logs may cause your storage costs to increase. Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose

custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

#### Audit:

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Instance Overview page
- 3. Go to Configuration card
- 4. Under Database flags, check the value of log\_statement flag is set to appropriately.

#### From Command Line:

1. Use the below command for every Cloud SQL PostgreSQL database instance to verify the value of  $\log\_statement$ 

```
gcloud sql instances list --format=json | jq '.settings.databaseFlags[] |
select(.name=="log_statement")|.value'
```

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the PostgreSQL instance for which you want to enable the database flag.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag log\_statement from the drop-down menu and set appropriate value.
- 6. Click Save to save your changes.
- 7. Confirm your changes under Flags on the Overview page.

#### From Command Line:

1. Configure the <code>log\_statement</code> database flag for every Cloud SQL PosgreSQL database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags
log_statement=<ddl|mod|all|none>
Note: This command will overwrite all database flags previously set. To keep
those and add new ones, include the values for all flags you want set on the
```

```
instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").
```

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/postgres/flags</u>
- 2. <u>https://www.postgresql.org/docs/current/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHAT</u>

#### Additional Information:

WARNING: This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags - https://cloud.google.com/sql/docs/postgres/flags - to see if your instance will be restarted when this patch is submitted.

Note: some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

Note: Configuring the above flag does not require restarting the Cloud SQL instance.

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	•
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		•	•

## 6.2.5 Ensure 'Log\_hostname' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'on' (Automated)

### **Profile Applicability:**

• Level 1

### **Description**:

PostgreSQL logs only the IP address of the connecting hosts. The log\_hostname flag controls the logging of hostnames in addition to the IP addresses logged. The performance hit is dependent on the configuration of the environment and the host name resolution setup. This parameter can only be set in the postgresql.conf file or on the server command line.

#### **Rationale:**

Logging hostnames allows for the association of hostname to IP address at the time of connection. This information can aid with incident response efforts particularly in an environment that utilized dynamic IP addresses. Logging hostnames may incur overhead on server performance as for each statement logged, DNS resolution will be required to convert IP address to hostname. Depending on the setup, this may be non-negligible. This recommendation is applicable to PostgreSQL database instances.

#### Impact:

Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

#### Audit:

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Instance Overview page
- 3. Go to Configuration card
- 4. Under Database flags, check the value of log\_hostname flag is set to 'On'.

#### From Command Line:

 Use the below command for every Cloud SQL PostgreSQL database instance to verify the value of log\_hostname

gcloud sql instances list --format=json | jq '.settings.databaseFlags[] |
select(.name=="log\_hostname")|.value'

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the PostgreSQL instance for which you want to enable the database flag.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag log hostname from the drop-down menu and the value to On.
- 6. Click Save to save your changes.
- 7. Confirm your changes under Flags on the Overview page.

#### From Command Line:

1. Configure the log\_hostname database flag for every Cloud SQL PosgreSQL database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags log_hostname=on
Note: This command will overwrite all database flags previously set. To keep
those and add new ones, include the values for all flags you want set on the
instance; any flag not specifically included is set to its default value. For
flags that do not take a value, specify the flag name followed by an equals
sign ("=").
```

#### **Default Value:**

By default log\_hostname is off.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/postgres/flags</u>
- 2. <u>https://www.postgresql.org/docs/current/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHAT</u>

#### Additional Information:

WARNING: This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags –  $\,$ 

https://cloud.google.com/sql/docs/postgres/flags - to see if your instance will be restarted when this patch is submitted.

Note: some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

Note: Configuring the above flag does not require restarting the Cloud SQL instance.

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		•	•

## 6.2.6 Ensure That the 'Log\_min\_messages' Database Flag for Cloud SQL PostgreSQL Instance Is Set to at least 'Warning' (Manual)

### **Profile Applicability:**

• Level 1

### **Description**:

The log\_min\_messages flag defines the minimum message severity level that is considered as an error statement. Messages for error statements are logged with the SQL statement. Valid values include DEBUG5, DEBUG4, DEBUG3, DEBUG2, DEBUG1, INFO, NOTICE, WARNING, ERROR, LOG, FATAL, and PANIC. Each severity level includes the subsequent levels mentioned above. ERROR is considered the best practice setting. Changes should only be made in accordance with the organization's logging policy.

#### **Rationale:**

Auditing helps in troubleshooting operational problems and also permits forensic analysis. If  $\log_min\_error\_statement$  is not set to the correct value, messages may not be classified as error messages appropriately. An organization will need to decide their own threshold for logging  $\log_min\_messages$  flag.

This recommendation is applicable to PostgreSQL database instances.

#### Impact:

Setting the threshold too low will might result in increased log storage size and length making it difficult to find actual errors. Setting the threshold to 'Warning' will log messages most needed error messages. Higher severity levels may cause errors needed to troubleshoot to not be logged.

Note: To effectively turn off logging failing statements, set this parameter to PANIC.

#### Audit:

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting https://console.cloud.google.com/sql/instances.
- 2. Select the instance to open its Instance Overview page.
- $3. \ \ Go \ to \ the \ {\tt Configuration} \ card.$

4. Under Database flags, check the value of log\_min\_messages flag is in accordance with the organization's logging policy.

#### From Command Line:

1. Use the below command for every Cloud SQL PostgreSQL database instance to verify that the value of log\_min\_messages is in accordance with the organization's logging policy.

```
gcloud sql instances list --format=json | jq '.settings.databaseFlags[] |
select(.name=="log min messages")|.value'
```

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting https://console.cloud.google.com/sql/instances
- 2. Select the PostgreSQL instance for which you want to enable the database flag.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag log\_min\_messages from the drop-down menu and set appropriate value.
- 6. Click Save to save the changes.
- 7. Confirm the changes under Flags on the Overview page.

#### From Command Line:

1. Configure the log\_min\_messages database flag for every Cloud SQL PosgreSQL database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags
log_min_messages=<DEBUG5|DEBUG4|DEBUG3|DEBUG2|DEBUG1|INFO|NOTICE|WARNING|ERRO
R|LOG|FATAL|PANIC>
Note: This command will overwrite all database flags previously set. To keep
those and add new ones, include the values for all flags to be set on the
instance; any flag not specifically included is set to its default value. For
flags that do not take a value, specify the flag name followed by an equals
sign ("=").
```

#### **Default Value:**

By default log\_min\_error\_statement is ERROR.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/postgres/flags</u>
- 2. <u>https://www.postgresql.org/docs/9.6/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHEN</u>

#### Additional Information:

WARNING: This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags - https://cloud.google.com/sql/docs/postgres/flags - to see if your instance will be restarted when this patch is submitted.

Note: Some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

Note: Configuring the above flag does not require restarting the Cloud SQL instance.

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	•
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		•	•

## 6.2.7 Ensure 'Log\_min\_error\_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter (Automated)

### **Profile Applicability:**

• Level 1

### **Description:**

The log\_min\_error\_statement flag defines the minimum message severity level that are considered as an error statement. Messages for error statements are logged with the SQL statement. Valid values include DEBUG5, DEBUG4, DEBUG3, DEBUG2, DEBUG1, INFO, NOTICE, WARNING, ERROR, LOG, FATAL, and PANIC. Each severity level includes the subsequent levels mentioned above. Ensure a value of ERROR or stricter is set.

#### **Rationale:**

Auditing helps in troubleshooting operational problems and also permits forensic analysis. If log\_min\_error\_statement is not set to the correct value, messages may not be classified as error messages appropriately. Considering general log messages as error messages would make is difficult to find actual errors and considering only stricter severity levels as error messages may skip actual errors to log their SQL statements. The log\_min\_error\_statement flag should be set to ERROR or stricter. This recommendation is applicable to PostgreSQL database instances.

#### Impact:

Turning on logging will increase the required storage over time. Mismanaged logs may cause your storage costs to increase.Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

### Audit:

### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Instance Overview page
- 3. Go to Configuration card
- 4. Under Database flags, check the value of log\_min\_error\_statement flag is configured as to ERROR or stricter.

#### From Command Line:

1. Use the below command for every Cloud SQL PostgreSQL database instance to verify the value of log\_min\_error\_statement is set to ERROR or stricter.

```
gcloud sql instances list --format=json | jq '.settings.databaseFlags[] |
select(.name=="log_min_error_statement")|.value'
```

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the PostgreSQL instance for which you want to enable the database flag.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag log\_min\_error\_statement from the drop-down menu and set appropriate value.
- 6. Click save to save your changes.
- 7. Confirm your changes under Flags on the Overview page.

#### From Command Line:

1. Configure the log\_min\_error\_statement database flag for every Cloud SQL PosgreSQL database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags
log_min_error_statement=<DEBUG5|DEBUG4|DEBUG3|DEBUG2|DEBUG1|INFO|NOTICE|WARNI
NG|ERROR>
```

```
Note: This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags you want set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").
```

#### **Default Value:**

By default log\_min\_error\_statement is ERROR.

#### **References:**

- 1. https://cloud.google.com/sql/docs/postgres/flags
- 2. <u>https://www.postgresql.org/docs/9.6/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHEN</u>

#### Additional Information:

WARNING: This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags - https://cloud.google.com/sql/docs/postgres/flags - to see if your instance will be restarted when this patch is submitted.

Note: some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

```
Note: Configuring the above flag does not require restarting the Cloud SQL instance.
```

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		•	•

## 6.2.8 Ensure That the 'Log\_min\_duration\_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled) (Automated)

### **Profile Applicability:**

• Level 1

### **Description**:

The log\_min\_duration\_statement flag defines the minimum amount of execution time of a statement in milliseconds where the total duration of the statement is logged. Ensure that log\_min\_duration\_statement is disabled, i.e., a value of -1 is set.

#### **Rationale:**

Logging SQL statements may include sensitive information that should not be recorded in logs. This recommendation is applicable to PostgreSQL database instances.

#### Impact:

Turning on logging will increase the required storage over time. Mismanaged logs may cause your storage costs to increase.Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

#### Audit:

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Instance Overview page.
- 3. Go to the Configuration card.
- 4. Under Database flags, check that the value of <code>log\_min\_duration\_statement</code> flag is set to -1.

#### From Command Line:

1. Use the below command for every Cloud SQL PostgreSQL database instance to verify the value of log\_min\_duration\_statement is set to -1.

```
gcloud sql instances list --format=json| jq '.settings.databaseFlags[] |
select(.name=="log_min_duration_statement")|.value'
```

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the PostgreSQL instance where the database flag needs to be enabled.
- $3. \ Click\, {\tt Edit}.$
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag log min duration statement from the drop-down menu and set a value of -1.
- 6. Click Save.
- 7. Confirm the changes under Flags on the Overview page.

#### **From Command Line:**

1. List all Cloud SQL database instances using the following command:

gcloud sql instances list

2. Configure the log\_min\_duration\_statement flag for every Cloud SQL PosgreSQL database instance using the below command:

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags
log_min_duration_statement=-1
Note: This command will overwrite all database flags previously set. To keep
those and add new ones, include the values for all flags to be set on the
instance; any flag not specifically included is set to its default value. For
flags that do not take a value, specify the flag name followed by an equals
sign ("=").
```

#### **Default Value:**

By default log\_min\_duration\_statement is -1.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/postgres/flags</u>
- 2. <u>https://www.postgresql.org/docs/current/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHAT</u>

#### Additional Information:

```
WARNING: This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags - https://cloud.google.com/sql/docs/postgres/flags - to see if your instance will be restarted when this patch is submitted.
```

Note: Some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

Note: Configuring the above flag does not require restarting the Cloud SQL instance.

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		•	

## 6.2.9 Ensure That 'cloudsql.enable\_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging (Automated)

### Profile Applicability:

• Level 1

#### **Description**:

Ensure cloudsql.enable\_pgaudit database flag for Cloud SQL PostgreSQL instance is set to on to allow for centralized logging.

#### **Rationale:**

As numerous other recommendations in this section consist of turning on flags for logging purposes, your organization will need a way to manage these logs. You may have a solution already in place. If you do not, consider installing and enabling the open source pgaudit extension within PostgreSQL and enabling its corresponding flag of cloudsql.enable\_pgaudit. This flag and installing the extension enables database auditing in PostgreSQL through the open-source pgAudit extension. This extension provides detailed session and object logging to comply with government, financial, & ISO standards and provides auditing capabilities to mitigate threats by monitoring security events on the instance. Enabling the flag and settings later in this recommendation will send these logs to Google Logs Explorer so that you can access them in a central location. to This recommendation is applicable only to PostgreSQL database instances.

#### Impact:

Enabling the pgAudit extension can lead to increased data storage requirements and to ensure durability of pgAudit log records in the event of unexpected storage issues, it is recommended to enable the Enable automatic storage increases setting on the instance. Enabling flags via the command line will also overwrite all existing flags, so you should apply all needed flags in the CLI command. Also flags may require a restart of the server to be implemented or will break existing functionality so update your servers at a time of low usage.

#### Audit:

#### Determining if the pgAudit Flag is set to 'on'

#### From Console:

- 1. Go to <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Overview page.
- 3. Click Edit.
- 4. Scroll down and expand Flags.
- 5. Ensure that cloudsql.enable\_pgaudit flag is set to on.

#### **From Command Line:**

Run the command by providing <instance\_name>. Ensure the value of the flag is on.

```
gcloud sql instances describe <INSTANCE_NAME> --format="json" | jq
'.settings|.|.databaseFlags[]|select(.name=="cloudsql.enable_pgaudit")|.value
```

#### Determine if the pgAudit extension is installed

- 1. Connect to the the server running PostgreSQL or through a SQL client of your choice.
- 2. Via command line open the PostgreSQL shell by typing psql
- 3. Run the following command

```
SELECT *
FROM pg_extension;
```

4. If pgAudit is in this list. If so, it is installed.

# Determine if Data Access Audit logs are enabled for your project and have sufficient privileges

- 1. From the homepage open the hamburger menu in the top left.
- 2. Scroll down to IAM & Adminand hover over it.
- 3. In the menu that opens up, select Audit Logs
- 4. In the middle of the page, in the search box next to filter search for Cloud Composer API
- 5. Select it, and ensure that both 'Admin Read' and 'Data Read' are checked.

#### Determine if logs are being sent to Logs Explorer

- 1. From the Google Console home page, open the hamburger menu in the top left.
- 2. In the menu that pops open, scroll down to Logs Explorer under Operations.
- 3. In the query box, paste the following and search

```
resource.type="cloudsql_database"
logName="projects/<your-project-
name>/logs/cloudaudit.googleapis.com%2Fdata access"
```

4. If it returns any log sources, they are correctly setup.

#### **Remediation:**

#### Initialize the pgAudit flag

#### From Console:

- 1. Go to <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Overview page.
- 3. Click Edit.
- 4. Scroll down and expand Flags.
- 5. To set a flag that has not been set on the instance before, click Add item.
- 6. Enter cloudsql.enable pgaudit for the flag name and set the flag to on.
- 7. Click Done.
- 8. Click save to update the configuration.
- 9. Confirm your changes under Flags on the Overview page.

#### From Command Line:

Run the below command by providing <instance name> to enable

cloudsql.enable\_pgaudit flag.

```
gcloud sql instances patch <INSTANCE_NAME> --database-
flags=cloudsql.enable pgaudit=on
```

Note: RESTART is required to get this configuration in effect.

#### Creating the extension

- 1. Connect to the the server running PostgreSQL or through a SQL client of your choice.
- 2. If SSHing to the server in the command line open the PostgreSQL shell by typing  $_{\tt psql}$
- 3. Run the following command as a superuser.

CREATE EXTENSION pgaudit;

#### Updating the previously created pgaudit.log flag for your Logging Needs

#### From Console:

Note: there are multiple options here. This command will enable logging for all databases

on a server. Please see the customizing database audit logging reference for more flag options.

- 1. Go to <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Overview page.
- 3. Click Edit.
- 4. Scroll down and expand Flags.
- 5. To set a flag that has not been set on the instance before, click Add item.
- 6. Enter pgaudit.log=all for the flag name and set the flag to on.
- 7. Click Done.
- 8. Click Save to update the configuration.
- 9. Confirm your changes under Flags on the Overview page.

#### From Command Line:

Run the command

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags \
    cloudsql.enable_pgaudit=on,pgaudit.log=all
```

#### Determine if logs are being sent to Logs Explorer

- 1. From the Google Console home page, open the hamburger menu in the top left.
- 2. In the menu that pops open, scroll down to Logs Explorer under Operations.
- 3. In the query box, paste the following and search

resource.type="cloudsql\_database"

logName="projects//logs/cloudaudit.googleapis.com%2Fdata\_access"

protoPayload.request.@type="type.googleapis.com/google.cloud.sql.audit.v1.PgAuditEntry
"

If it returns any log sources, they are correctly setup.

#### **Default Value:**

By default cloudsql.enable\_pgaudit database flag is set to off and the extension is not enabled.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/postgres/flags#list-flags-postgres</u>
- 2. <u>https://cloud.google.com/sql/docs/postgres/pg-audit#enable-auditing-flag</u>
- 3. <u>https://cloud.google.com/sql/docs/postgres/pg-audit#customizing-database-audit-logging</u>
- 4. <u>https://cloud.google.com/logging/docs/audit/configure-data-access#config-console-enable</u>

#### Additional Information:

WARNING: This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags -

<u>https://cloud.google.com/sql/docs/postgres/flags</u> - to see if your instance will be restarted when this patch is submitted.

Note: Configuring the 'cloudsql.enable\_pgaudit' database flag requires restarting the Cloud SQL PostgreSQL instance.

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		•	•
v8	<b>8.9</b> <u>Centralize Audit Logs</u> Centralize, to the extent possible, audit log collection and retention across enterprise assets.		•	•
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		•	
v7	6.5 <u>Central Log Management</u> Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		•	

## 6.3 SQL Server

This section covers recommendations addressing Cloud SQL for SQL Server on Google Cloud Platform.

## 6.3.1 Ensure 'external scripts enabled' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)

### Profile Applicability:

• Level 1

### **Description**:

It is recommended to set <code>external scripts enabled</code> database flag for Cloud SQL SQL Server instance to <code>off</code>

#### **Rationale:**

external scripts enabled enable the execution of scripts with certain remote language extensions. This property is OFF by default. When Advanced Analytics Services is installed, setup can optionally set this property to true. As the External Scripts Enabled feature allows scripts external to SQL such as files located in an R library to be executed, which could adversely affect the security of the system, hence this should be disabled. This recommendation is applicable to SQL Server database instances.

#### Impact:

Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

#### Audit:

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Instance Overview page
- 3. Ensure the database flag external scripts enabled that has been set is listed under the Database flags section.

#### From Command Line:

1. Ensure the below command returns  ${\tt off}$  for every Cloud SQL SQL Server database instance

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the SQL Server instance for which you want to enable to database flag.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag external scripts enabled from the drop-down menu, and set its value to off.
- 6. Click Save to save your changes.
- 7. Confirm your changes under Flags on the Overview page.

#### From Command Line:

1. Configure the external scripts enabled database flag for every Cloud SQL SQL Server database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags "external scripts
enabled=off"
Note :
This command will overwrite all database flags previously set. To keep those
```

and add new ones, include the values for all flags you want set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

#### **Default Value:**

 $By \ default \ \texttt{external} \ \texttt{scripts} \ \texttt{enabled} \ is \ \texttt{off}$ 

#### **References:**

- 1. <u>https://docs.microsoft.com/en-us/sql/database-engine/configure-</u> windows/external-scripts-enabled-server-configuration-option?view=sql-serverver15
- 2. <u>https://cloud.google.com/sql/docs/sqlserver/flags</u>
- 3. <u>https://docs.microsoft.com/en-us/sql/advanced-analytics/concepts/security?view=sql-server-ver15</u>
- 4. <u>https://www.stigviewer.com/stig/ms\_sql\_server\_2016\_instance/2018-03-09/finding/V-79347</u>

#### **Additional Information:**

"WARNING: This patch modifies database flag values, which may require

your instance to be restarted. Check the list of supported flags -

https://cloud.google.com/sql/docs/sqlserver/flags - to see if your

instance will be restarted when this patch is submitted.

Note: some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines."

Note: Configuring the above flag restarts the Cloud SQL instance.

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 <u>Allowlist Authorized Scripts</u> Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			
v7	2.9 Implement Application Whitelisting of Scripts The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.			

## 6.3.2 Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)

### Profile Applicability:

• Level 1

### **Description**:

It is recommended to set cross db ownership chaining database flag for Cloud SQL SQL Server instance to off.

#### **Rationale:**

Use the cross db ownership for chaining option to configure cross-database ownership chaining for an instance of Microsoft SQL Server. This server option allows you to control cross-database ownership chaining at the database level or to allow cross-database ownership chaining for all databases. Enabling cross db ownership is not recommended unless all of the databases hosted by the instance of SQL Server must participate in cross-database ownership chaining and you are aware of the security implications of this setting. This recommendation is applicable to SQL Server database instances.

#### Impact:

Updating flags may cause the database to restart. This may cause it to unavailable for a short amount of time, so this is best done at a time of low usage. You should also determine if the tables in your databases reference another table without using credentials for that database, as turning off cross database ownership will break this relationship.

#### Audit:

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console.
- 2. Select the instance to open its Instance Overview page
- 3. Ensure the database flag cross db ownership chaining that has been set is listed under the Database flags section.

#### From Command Line:

1. Ensure the below command returns <code>off</code> for every Cloud SQL SQL Server database instance:

### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the SQL Server instance for which you want to enable to database flag.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag cross db ownership chaining from the drop-down menu, and set its value to off.
- 6. Click Save.
- 7. Confirm the changes under Flags on the Overview page.

#### From Command Line:

1. Configure the cross db ownership chaining database flag for every Cloud SQL SQL Server database instance using the below command:

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags "cross db
ownership chaining=off"
```

#### Note:

This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags to be set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

#### **Default Value:**

As you have to manually turn on this flag, the default value for this is 'On'. Though you would have had to design your database schema from the start to include this feature, it often is not enabled.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/sqlserver/flags</u>
- 2. <u>https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/cross-db-ownership-chaining-server-configuration-option?view=sql-server-ver15</u>

### Additional Information:

WARNING: This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags -

<u>https://cloud.google.com/sql/docs/sqlserver/flags</u> - to see if your instance will be restarted when this patch is submitted.

Note: Some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

Note: Configuring the above flag does not restart the Cloud SQL instance.

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	٠	•	•
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	•	•	•
# 6.3.3 Ensure 'user Connections' Database Flag for Cloud Sql Sql Server Instance Is Set to a Non-limiting Value (Automated)

## **Profile Applicability:**

• Level 1

## **Description**:

It is recommended to check the user connections for a Cloud SQL SQL Server instance to ensure that it is not artificially limiting connections.

## **Rationale:**

The user connections option specifies the maximum number of simultaneous user connections that are allowed on an instance of SQL Server. The actual number of user connections allowed also depends on the version of SQL Server that you are using, and also the limits of your application or applications and hardware. SQL Server allows a maximum of 32,767 user connections. Because user connections is by default a self-configuring value, with SQL Server adjusting the maximum number of user connections automatically as needed, up to the maximum value allowable. For example, if only 10 users are logged in, 10 user connection objects are allocated. In most cases, you do not have to change the value for this option. The default is 0, which means that the maximum (32,767) user connections are allowed. However if there is a number defined here that limits connections, SQL Server will not allow anymore above this limit. If the connections are at the limit, any new requests will be dropped, potentially causing lost data or outages for those using the database.

## Impact:

Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

## Audit:

## **Using Console:**

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Instance Overview page

3. Ensure the database flag user connections listed under the Database flags section is .

### **Using Command Line:**

1. Ensure the below command returns a value of 0, for every Cloud SQL SQL Server database instance.

```
gcloud sql instances list --format=json | jq '.settings.databaseFlags[] |
select(.name=="user connections")|.value'
```

#### **Remediation:**

#### **Using Console:**

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the SQL Server instance for which you want to enable to database flag.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag user connections from the drop-down menu, and set its value to your organization recommended value.
- 6. Click save to save your changes.
- 7. Confirm your changes under Flags on the Overview page.

#### **Using Command Line:**

1. Configure the user connections database flag for every Cloud SQL SQL Server database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags "user
connections=[0-32,767]"
Note :
This command will overwrite all database flags previously set. To keep those
and add new ones, include the values for all flags you want set on the
instance; any flag not specifically included is set to its default value. For
flags that do not take a value, specify the flag name followed by an equals
sign ("=").
```

#### **Default Value:**

By default user connections is set to '0' which does not limit the number of connections, giving the server free reign to facilitate a max of 32,767 connections.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/sqlserver/flags</u>
- 2. <u>https://docs.microsoft.com/en-us/sql/database-engine/configure-</u> <u>windows/configure-the-user-connections-server-configuration-option?view=sql-</u> <u>server-ver15</u>
- 3. <u>https://www.stigviewer.com/stig/ms\_sql\_server\_2016\_instance/2018-03-09/finding/V-79119</u>

#### Additional Information:

WARNING: This patch modifies database flag values, which may require

your instance to be restarted. Check the list of supported flags -

https://cloud.google.com/sql/docs/sqlserver/flags - to see if your

instance will be restarted when this patch is submitted.

Note: some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

Note: Configuring the above flag does not restart the Cloud SQL instance.

# 6.3.4 Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured (Automated)

## **Profile Applicability:**

• Level 1

## **Description**:

It is recommended that, user options database flag for Cloud SQL SQL Server instance should not be configured.

## **Rationale:**

The user options option specifies global defaults for all users. A list of default query processing options is established for the duration of a user's work session. The user options option allows you to change the default values of the SET options (if the server's default settings are not appropriate).

A user can override these defaults by using the SET statement. You can configure user options dynamically for new logins. After you change the setting of user options, new login sessions use the new setting; current login sessions are not affected. This recommendation is applicable to SQL Server database instances.

## Impact:

Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

## Audit:

## From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting https://console.cloud.google.com/sql/instances.
- 2. Select the instance to open its Instance Overview page
- 3. Ensure the database flag user options that has been set is not listed under the Database flags section.

#### From Command Line:

1. Ensure the below command returns empty result for every Cloud SQL SQL Server database instance

```
gcloud sql instances list --format=json | jq '.settings.databaseFlags[] |
select(.name=="user options")|.value'
```

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the SQL Server instance for which you want to enable to database flag.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. Click the X next user options flag shown
- 6. Click save to save your changes.
- 7. Confirm your changes under Flags on the Overview page.

#### **From Command Line:**

1. List all Cloud SQL database Instances

gcloud sql instances list

2. Clear the user options database flag for every Cloud SQL SQL Server database instance using either of the below commands.

```
1.Clearing all flags to their default value
gcloud sql instances patch <INSTANCE_NAME> --clear-database-flags
OR
2. To clear only `user options` database flag, configure the database flag by
overriding the `user options`. Exclude `user options` flag and its value, and
keep all other flags you want to configure.
gcloud sql instances patch <INSTANCE_NAME> --database-flags
[FLAG1=VALUE1,FLAG2=VALUE2]
Note :
This command will overwrite all database flags previously set. To keep those
and add new ones, include the values for all flags you want set on the
instance; any flag not specifically included is set to its default value. For
flags that do not take a value, specify the flag name followed by an equals
sign ("=").
```

#### **Default Value:**

By default 'user options' is not configured.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/sqlserver/flags</u>
- 2. <u>https://docs.microsoft.com/en-us/sql/database-engine/configure-</u> windows/configure-the-user-options-server-configuration-option?view=sql-serverver15
- 3. <u>https://www.stigviewer.com/stig/ms sql server 2016 instance/2018-03-09/finding/V-79335</u>

#### Additional Information:

WARNING: This patch modifies database flag values, which may require

your instance to be restarted. Check the list of supported flags -

https://cloud.google.com/sql/docs/sqlserver/flags - to see if your

instance will be restarted when this patch is submitted.

Note: some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

Note: Configuring the above flag does not restart the Cloud SQL instance.

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end- user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	•	•	•
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.		•	

# 6.3.5 Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)

## Profile Applicability:

• Level 1

## **Description**:

It is recommended to set  ${\tt remote}$   ${\tt access}$  database flag for Cloud SQL SQL Server instance to off.

## **Rationale:**

The remote access option controls the execution of stored procedures from local or remote servers on which instances of SQL Server are running. This default value for this option is 1. This grants permission to run local stored procedures from remote servers or remote stored procedures from the local server. To prevent local stored procedures from being run on the local server, this must be disabled. The Remote Access option controls the execution of local stored procedures on remote servers or remote stored procedures on local server. 'Remote access' functionality can be abused to launch a Denial-of-Service (DoS) attack on remote servers by off-loading query processing to a target, hence this should be disabled. This recommendation is applicable to SQL Server database instances.

## Impact:

Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

## Audit:

## From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Instance Overview page
- 3. Ensure the database flag remote access that has been set is listed under the Database flags section.

## From Command Line:

1. Ensure the below command returns <code>off</code> for every Cloud SQL SQL Server database instance

gcloud sql instances list --format=json | jq '.settings.databaseFlags[] |
select(.name=="remote access")|.value'

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the SQL Server instance for which you want to enable to database flag.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag remote access from the drop-down menu, and set its value to off.
- 6. Click Save to save your changes.
- 7. Confirm your changes under Flags on the Overview page.

#### From Command Line:

1. Configure the remote access database flag for every Cloud SQL SQL Server database instance using the below command

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags "remote
access=off"
Note :
This command will overwrite all database flags previously set. To keep those
and add new ones, include the values for all flags you want set on the
instance; any flag not specifically included is set to its default value. For
flags that do not take a value, specify the flag name followed by an equals
sign ("=").
```

#### **Default Value:**

By default 'remote access' is 'on'.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/sqlserver/flags</u>
- 2. <u>https://docs.microsoft.com/en-us/sql/database-engine/configure-</u> windows/configure-the-remote-access-server-configuration-option?view=sqlserver-ver15
- 3. <u>https://www.stigviewer.com/stig/ms sql server 2016 instance/2018-03-09/finding/V-79337</u>

#### Additional Information:

WARNING: This patch modifies database flag values, which may require

your instance to be restarted. Check the list of supported flags -

https://cloud.google.com/sql/docs/sqlserver/flags - to see if your

instance will be restarted when this patch is submitted.

Note: some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

Note: Configuring the above flag does not restart the Cloud SQL instance.

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise</u> <u>Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		•	
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are <u>Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		•	•

# 6.3.6 Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'off' (Automated)

## Profile Applicability:

• Level 1

## **Description**:

It is recommended to set  $\tt 3625$  (trace flag) database flag for Cloud SQL SQL Server instance to off.

## **Rationale:**

Microsoft SQL Trace Flags are frequently used to diagnose performance issues or to debug stored procedures or complex computer systems, but they may also be recommended by Microsoft Support to address behavior that is negatively impacting a specific workload. All documented trace flags and those recommended by Microsoft Support are fully supported in a production environment when used as directed. 3625(trace log) Limits the amount of information returned to users who are not members of the sysadmin fixed server role, by masking the parameters of some error messages using '\*\*\*\*\*'. Setting this in a Google Cloud flag for the instance allows for security through obscurity and prevents the disclosure of sensitive information, hence this is recommended to set this flag globally to off to prevent the flag having been left on, or turned on by bad actors. This recommendation is applicable to SQL Server database instances.

## Impact:

Changing flags on a database may cause it to be restarted. The best time to do this is at a time where there is low usage.

## Audit:

## From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Instance Overview page
- 3. Ensure the database flag 3625 that has been set is listed under the Database flags section.

## From Command Line:

1. Ensure the below command returns <code>off</code> for every Cloud SQL SQL Server database instance

gcloud sql instances list --format=json | jq '.settings.databaseFlags[] |
select(.name=="3625")|.value'

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the SQL Server instance for which you want to enable to database flag.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag 3625 from the drop-down menu, and set its value to off.
- 6. Click save to save your changes.
- 7. Confirm your changes under Flags on the Overview page.

#### From Command Line:

1. Configure the 3625 database flag for every Cloud SQL SQL Server database instance using the below command.

gcloud sql instances patch <INSTANCE\_NAME> --database-flags "3625=off"

#### Note :

This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags you want set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

#### **Default Value:**

MySQL implementations by default do not have trace flags turned on, as they are used for logging purposes.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/sqlserver/flags</u>
- 2. <u>https://docs.microsoft.com/en-us/sql/t-sql/database-console-commands/dbcc-traceon-trace-flags-transact-sql?view=sql-server-ver15#trace-flags</u>

## Additional Information:

## WARNING:

This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags - <u>https://cloud.google.com/sql/docs/sqlserver/flags</u> - to see if your instance will be restarted when this patch is submitted.

Note:

some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

Note:

Configuring the above flag restarts the Cloud SQL instance.

# 6.3.7 Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is set to 'off' (Automated)

## **Profile Applicability:**

• Level 1

## **Description**:

It is recommended to set contained database authentication database flag for Cloud SQL on the SQL Server instance is set to off.

## **Rationale:**

A contained database includes all database settings and metadata required to define the database and has no configuration dependencies on the instance of the Database Engine where the database is installed. Users can connect to the database without authenticating a login at the Database Engine level. Isolating the database from the Database Engine makes it possible to easily move the database to another instance of SQL Server. Contained databases have some unique threats that should be understood and mitigated by SQL Server Database Engine administrators. Most of the threats are related to the USER WITH PASSWORD authentication process, which moves the authentication boundary from the Database Engine level to the database level, hence this is recommended to disable this flag. This recommendation is applicable to SQL Server database instances.

## Impact:

When contained database authentication is off (0) for the instance, contained databases cannot be created, or attached to the Database Engine. Turning on logging will increase the required storage over time. Mismanaged logs may cause your storage costs to increase.Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

## Audit:

## From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance to open its Instance Overview page

3. Ensure the database flag contained database authentication that has been set is listed under the Database flags section.

#### From Command Line:

1. Ensure the below command returns  ${\tt off}$  for every Cloud SQL SQL Server database instance.

gcloud sql instances list --format=json | jq '.settings.databaseFlags[] |
select(.name=="contained database authentication")|.value'

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the SQL Server instance for which you want to enable to database flag.
- 3. Click Edit.
- 4. Scroll down to the Flags section.
- 5. To set a flag that has not been set on the instance before, click Add item, choose the flag contained database authentication from the drop-down menu, and set its value to off.
- 6. Click Save.
- 7. Confirm the changes under Flags on the Overview page.

#### **From Command Line:**

1. Configure the contained database authentication database flag for every Cloud SQL SQL Server database instance using the below command:

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags "contained
database authentication=off"
Note:
This command will overwrite all database flags previously set. To keep those
and add new ones, , include the values for all flags to be set on the
instance; any flag not specifically included is set to its default value. For
flags that do not take a value, specify the flag name followed by an equals
sign ("=").
```

#### **References:**

1. <u>https://cloud.google.com/sql/docs/sqlserver/flags</u>

- 2. <u>https://docs.microsoft.com/en-us/sql/database-engine/configure-</u> <u>windows/contained-database-authentication-server-configuration-</u> <u>option?view=sql-server-ver15</u>
- 3. <u>https://docs.microsoft.com/en-us/sql/relational-databases/databases/security-best-practices-with-contained-databases?view=sql-server-ver15</u>

#### Additional Information:

WARNING: This patch modifies database flag values, which may require

your instance to be restarted. Check the list of supported flags -

https://cloud.google.com/sql/docs/sqlserver/flags - to see if your

instance will be restarted when this patch is submitted.

Note: Some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

Note: Configuring the above flag does not restart the Cloud SQL instance.

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3</b> <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	•	•	•
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	•	•	•

## 6.4 Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL (Automated)

## **Profile Applicability:**

• Level 1

## **Description**:

It is recommended to enforce all incoming connections to SQL database instance to use SSL.

## **Rationale:**

SQL database connections if successfully trapped (MITM); can reveal sensitive data like credentials, database queries, query outputs etc. For security, it is recommended to always use SSL encryption when connecting to your instance. This recommendation is applicable for Postgresql, MySql generation 1, MySql generation 2 and SQL Server 2017 instances.

## Impact:

After enforcing SSL connection, existing client will not be able to communicate with SQL server unless configured with appropriate client-certificates to communicate to SQL database instance.

## Audit:

## From Console:

- 1. Go to <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Click on an instance name to see its configuration overview.
- 3. In the left-side panel, select Connections.
- 4. In the SSL connections section, ensure that Only secured connections are allowed to connect to this instance..

## From Command Line:

1. Get the detailed configuration for every SQL database instance using the following command:

gcloud sql instances list --format=json

Ensure that section settings: ipConfiguration has the parameter requireSsl set to true.

#### **Remediation:**

#### From Console:

- 1. Go to <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Click on an instance name to see its configuration overview.
- 3. In the left-side panel, select Connections.
- 4. In the SSL connections section, click Allow only SSL connections.
- 5. Under Configure SSL server certificates  $click\, {\tt Create}$  new certificate.
- $6. \ Under \, \texttt{Configure SSL client certificates} \, click \, \texttt{Create a client certificate.}$
- 7. Follow the instructions shown to learn how to connect to your instance.

#### From Command Line:

To enforce SSL encryption for an instance run the command:

gcloud sql instances patch <INSTANCE\_NAME> --require-ssl

#### Note:

RESTART is required for type MySQL Generation 1 Instances (backendType: FIRST\_GEN) to get this configuration in effect.

#### **Default Value:**

By default parameter settings: ipConfiguration: requireSsl is not set which is equivalent to requireSsl:false.

#### **References:**

1. <u>https://cloud.google.com/sql/docs/postgres/configure-ssl-instance/</u>

#### Additional Information:

By default Settings: ipConfiguration has no authorizedNetworks set/configured. In that case even if by default requireSsl is not set, which is equivalent to requireSsl:false there is no risk as instance cannot be accessed outside of the network unless authorizedNetworks are configured. However, If default for requireSsl is not updated to true any authorizedNetworks created later on will not enforce SSL only connection.

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		•	
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.		•	
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		•	•

## 6.5 Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses (Automated)

## **Profile Applicability:**

• Level 1

## **Description**:

Database Server should accept connections only from trusted Network(s)/IP(s) and restrict access from public IP addresses.

#### **Rationale:**

To minimize attack surface on a Database server instance, only trusted/known and required IP(s) should be white-listed to connect to it.

An authorized network should not have IPs/networks configured to 0.0.0/0 which will allow access to the instance from anywhere in the world. Note that authorized networks apply only to instances with public IPs.

#### Impact:

The Cloud SQL database instance would not be available to public IP addresses.

## Audit:

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Click the instance name to open its Instance details page.
- 3. Under the Configuration section click Edit configurations
- 4. Under Configuration options expand the Connectivity section.
- 5. Ensure that no authorized network is configured to allow 0.0.0/0.

#### From Command Line:

1. Get detailed configuration for every Cloud SQL database instance.

#### gcloud sql instances list --format=json

Ensure that the section settings: ipConfiguration : authorizedNetworks does not have any parameter value containing 0.0.0/0.

## **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Click the instance name to open its Instance details page.
- 3. Under the Configuration section click Edit configurations
- 4. Under Configuration options expand the Connectivity section.
- 5. Click the delete icon for the authorized network 0.0.0/0.
- 6. Click Save to update the instance.

#### From Command Line:

Update the authorized network list by dropping off any addresses.

```
gcloud sql instances patch <INSTANCE_NAME> --authorized-
networks=IP ADDR1,IP ADDR2...
```

#### **Prevention:**

To prevent new SQL instances from being configured to accept incoming connections from any IP addresses, set up a Restrict Authorized Networks on Cloud SQL instances Organization Policy at: <a href="https://console.cloud.google.com/iam-admin/orgpolicies/sql-restrictAuthorizedNetworks">https://console.cloud.google.com/iam-admin/orgpolicies/sql-restrictAuthorizedNetworks</a>.

#### **Default Value:**

By default, authorized networks are not configured. Remote connection to Cloud SQL database instance is not possible unless authorized networks are configured.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/mysql/configure-ip</u>
- 2. <u>https://console.cloud.google.com/iam-admin/orgpolicies/sql-restrictAuthorizedNetworks</u>
- 3. <u>https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints</u>
- 4. <u>https://cloud.google.com/sql/docs/mysql/connection-org-policy</u>

#### Additional Information:

There is no IPv6 configuration found for Google cloud SQL server services.

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3</b> <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	•	•	•

# 6.6 Ensure That Cloud SQL Database Instances Do Not Have Public IPs (Automated)

## Profile Applicability:

• Level 2

## **Description**:

It is recommended to configure Second Generation Sql instance to use private IPs instead of public IPs.

#### **Rationale:**

To lower the organization's attack surface, Cloud SQL databases should not have public IPs. Private IPs provide improved network security and lower latency for your application.

#### Impact:

Removing the public IP address on SQL instances may break some applications that relied on it for database connectivity.

## Audit:

## From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console: https://console.cloud.google.com/sql/instances
- 2. Ensure that every instance has a private IP address and no public IP address configured.

#### From Command Line:

1. List all Cloud SQL database instances using the following command:

gcloud sql instances list

2. For every instance of type instanceType: CLOUD\_SQL\_INSTANCE with backendType: SECOND\_GEN, get detailed configuration. Ignore instances of type READ\_REPLICA\_INSTANCE because these instances inherit their settings from the primary instance. Also, note that first generation instances cannot be configured to have a private IP address.

gcloud sql instances describe <INSTANCE\_NAME>

3. Ensure that the setting ipAddresses has an IP address configured of type: PRIVATE and has no IP address of type: PRIMARY. PRIMARY IP addresses are public addresses. An instance can have both a private and public address at the same time. Note also that you cannot use private IP with First Generation instances.

### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console: <u>https://console.cloud.google.com/sql/instances</u>
- 2. Click the instance name to open its Instance details page.
- 3. Select the Connections tab.
- 4. Deselect the Public IP checkbox.
- 5. Click Save to update the instance.

#### From Command Line:

1. For every instance remove its public IP and assign a private IP instead:

```
gcloud sql instances patch <INSTANCE_NAME> --network=<VPC_NETWORK_NAME> --no-
assign-ip
```

2. Confirm the changes using the following command::

gcloud sql instances describe <INSTANCE\_NAME>

#### **Prevention:**

To prevent new SQL instances from getting configured with public IP addresses, set up a Restrict Public IP access on Cloud SQL instances Organization policy at: <a href="https://console.cloud.google.com/iam-admin/orgpolicies/sql-restrictPublicIP">https://console.cloud.google.com/iam-admin/orgpolicies/sql-restrictPublicIP</a>.

#### **Default Value:**

By default, Cloud Sql instances have a public IP.

#### **References:**

- 1. <u>https://cloud.google.com/sql/docs/mysql/configure-private-ip</u>
- 2. <u>https://cloud.google.com/sql/docs/mysql/private-ip</u>
- 3. <u>https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints</u>
- 4. <u>https://console.cloud.google.com/iam-admin/orgpolicies/sql-restrictPublicIp</u>

## **Additional Information:**

Replicas inherit their private IP status from their primary instance. You cannot configure a private IP directly on a replica.

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3</b> <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	•	•	•
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	•	•	•

## 6.7 Ensure That Cloud SQL Database Instances Are Configured With Automated Backups (Automated)

## **Profile Applicability:**

• Level 1

## **Description:**

It is recommended to have all SQL database instances set to enable automated backups.

#### **Rationale:**

Backups provide a way to restore a Cloud SQL instance to recover lost data or recover from a problem with that instance. Automated backups need to be set for any instance that contains data that should be protected from loss or damage. This recommendation is applicable for SQL Server, PostgreSql, MySql generation 1 and MySql generation 2 instances.

#### Impact:

Automated Backups will increase required size of storage and costs associated with it.

## Audit:

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Click the instance name to open its instance details page.
- 3. Go to the Backups menu.
- 4. Ensure that Automated backups is set to Enabled and Backup time is mentioned.

## From Command Line:

1. List all Cloud SQL database instances using the following command:

gcloud sql instances list

2. Ensure that the below command returns **True** for every Cloud SQL database instance.

```
gcloud sql instances describe <INSTANCE_NAME> --
format="value('Enabled':settings.backupConfiguration.enabled)"
```

#### **Remediation:**

#### From Console:

- 1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <u>https://console.cloud.google.com/sql/instances</u>.
- 2. Select the instance where the backups need to be configured.
- 3. Click Edit.
- 4. In the Backups section, check `Enable automated backups', and choose a backup window.
- 5. Click Save.

#### **From Command Line:**

1. List all Cloud SQL database instances using the following command:

gcloud sql instances list

2. Enable Automated backups for every Cloud SQL database instance using the below command:

gcloud sql instances patch <INSTANCE\_NAME> --backup-start-time <[HH:MM]>

The backup-start-time parameter is specified in 24-hour time, in the UTC±00 time zone, and specifies the start of a 4-hour backup window. Backups can start any time during the backup window.

#### **Default Value:**

By default, automated backups are not configured for Cloud SQL instances. Data backup is not possible on any Cloud SQL instance unless Automated Backup is configured.

#### **References:**

- 1. https://cloud.google.com/sql/docs/mysql/backup-recovery/backups
- 2. <u>https://cloud.google.com/sql/docs/postgres/backup-recovery/backing-up</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.2 <u>Perform Automated Backups</u> Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	•	•	•
v7	<b>10.1</b> Ensure Regular Automated Back Ups Ensure that all system data is automatically backed up on regular basis.	•	•	•

# 7 BigQuery

This section addresses Google CloudPlatform BigQuery. BigQuery is a serverless, highlyscalable, and cost-effective cloud data warehouse with an in-memory BI Engine and machine learning built in.

# 7.1 Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible (Manual)

## Profile Applicability:

• Level 1

#### **Description**:

It is recommended that the IAM policy on BigQuery datasets does not allow anonymous and/or public access.

#### **Rationale:**

Granting permissions to allusers or allAuthenticatedUsers allows anyone to access the dataset. Such access might not be desirable if sensitive data is being stored in the dataset. Therefore, ensure that anonymous and/or public access to a dataset is not allowed.

#### Impact:

The dataset is not publicly accessible. Explicit modification of IAM privileges would be necessary to make them publicly accessible.

#### Audit:

#### From Console:

- 1. Go to BigQuery by visiting: <u>https://console.cloud.google.com/bigquery</u>.
- 2. Select a dataset from Resources.
- 3. Click SHARING near the right side of the window and select Permissions.
- 4. Validate that none of the attached roles contain allUsers or allAuthenticatedUsers.

#### **From Command Line:**

List the name of all datasets.

bq ls

Retrieve each dataset details using the following command:

#### bq show PROJECT\_ID:DATASET\_NAME

Ensure that allUsers and allAuthenticatedUsers have not been granted access to the dataset.

#### **Remediation:**

#### From Console:

- 1. Go to BigQuery by visiting: <u>https://console.cloud.google.com/bigquery</u>.
- 2. Select the dataset from 'Resources'.
- 3. Click SHARING near the right side of the window and select Permissions.
- 4. Review each attached role.
- 5. Click the delete icon for each member allUsers or allAuthenticatedUsers. On the popup click Remove.

#### **From Command Line:**

List the name of all datasets.

bq ls

Retrieve the data set details:

bq show --format=prettyjson PROJECT ID:DATASET NAME > PATH TO FILE

In the access section of the JSON file, update the dataset information to remove all roles

 $containing \ \texttt{allUsers} \ or \ \texttt{allAuthenticatedUsers}.$ 

Update the dataset:

bq update --source PATH TO FILE PROJECT ID:DATASET NAME

#### **Prevention:**

You can prevent Bigquery dataset from becoming publicly accessible by setting up the Domain restricted sharing organization policy at: <a href="https://console.cloud.google.com/iam-admin/orgpolicies/iam-allowedPolicyMemberDomains">https://console.cloud.google.com/iam-admin/orgpolicies/iam-allowedPolicyMemberDomains</a> .

#### **Default Value:**

By default, BigQuery datasets are not publicly accessible.

#### **References:**

1. <u>https://cloud.google.com/bigquery/docs/dataset-access-controls</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3</b> <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	•	•	•

# 7.2 Ensure That All BigQuery Tables Are Encrypted With Customer-Managed Encryption Key (CMEK) (Automated)

## **Profile Applicability:**

• Level 2

## **Description**:

BigQuery by default encrypts the data as rest by employing Envelope Encryption using Google managed cryptographic keys. The data is encrypted using the data encryption keys and data encryption keys themselves are further encrypted using key encryption keys. This is seamless and do not require any additional input from the user. However, if you want to have greater control, Customer-managed encryption keys (CMEK) can be used as encryption key management solution for BigQuery Data Sets. If CMEK is used, the CMEK is used to encrypt the data encryption keys instead of using google-managed encryption keys.

## **Rationale:**

BigQuery by default encrypts the data as rest by employing Envelope Encryption using Google managed cryptographic keys. This is seamless and does not require any additional input from the user.

For greater control over the encryption, customer-managed encryption keys (CMEK) can be used as encryption key management solution for BigQuery tables. The CMEK is used to encrypt the data encryption keys instead of using google-managed encryption keys. BigQuery stores the table and CMEK association and the encryption/decryption is done automatically.

Applying the Default Customer-managed keys on BigQuery data sets ensures that all the new tables created in the future will be encrypted using CMEK but existing tables need to be updated to use CMEK individually.

```
Note: Google does not store your keys on its servers and cannot access your protected data unless you provide the key. This also means that if you forget or lose your key, there is no way for Google to recover the key or to recover any data encrypted with the lost key.
```

#### Impact:

Using Customer-managed encryption keys (CMEK) will incur additional labor-hour investment to create, protect, and manage the keys.

## Audit:

#### From Console:

- 1. Go to Analytics
- 2. Go to BigQuery
- 3. Under SQL Workspace, select the project
- 4. Select Data Set, select the table
- 5. Go to Details tab
- 6. Under Table info, verify Customer-managed key is present.
- 7. Repeat for each table in all data sets for all projects.

#### **From Command Line:**

List all dataset names

bq ls

Use the following command to view the table details. Verify the kmsKeyName is present.

bq show <table\_object>

#### **Remediation:**

Currently, there is no way to update the encryption of existing data in the table. The data needs to be copied to either an original table or another table while specifying the customer managed encryption key (CMEK).

#### From Command Line:

Use the following command to copy the data. The source and the destination needs to be same in case copying to the original table.

bq cp --destination\_kms\_key <customer\_managed\_key>
source dataset.source table destination dataset.destination table

#### **Default Value:**

Google Managed keys are used as key encryption keys.

#### **References:**

1. <u>https://cloud.google.com/bigquery/docs/customer-managed-encryption</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11</b> <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		•	
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

# 7.3 Ensure That a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets (Manual)

## **Profile Applicability:**

• Level 2

## **Description**:

BigQuery by default encrypts the data as rest by employing Envelope Encryption using Google managed cryptographic keys. The data is encrypted using the data encryption keys and data encryption keys themselves are further encrypted using key encryption keys. This is seamless and do not require any additional input from the user. However, if you want to have greater control, Customer-managed encryption keys (CMEK) can be used as encryption key management solution for BigQuery Data Sets.

## **Rationale:**

BigQuery by default encrypts the data as rest by employing Envelope Encryption using Google managed cryptographic keys. This is seamless and does not require any additional input from the user.

For greater control over the encryption, customer-managed encryption keys (CMEK) can be used as encryption key management solution for BigQuery Data Sets. Setting a Default Customer-managed encryption key (CMEK) for a data set ensure any tables created in future will use the specified CMEK if none other is provided.

```
Note: Google does not store your keys on its servers and cannot access your protected data unless you provide the key. This also means that if you forget or lose your key, there is no way for Google to recover the key or to recover any data encrypted with the lost key.
```

#### Impact:

Using Customer-managed encryption keys (CMEK) will incur additional labor-hour investment to create, protect, and manage the keys.

## Audit:

#### From Console:

- 1. Go to Analytics
- 2. Go to BigQuery
- 3. Under Analysis click on SQL Workspaces, select the project

- 4. Select Data Set
- 5. Ensure Customer-managed key is present under Dataset info section.
- 6. Repeat for each data set in all projects.

#### From Command Line:

List all dataset names

#### bq ls

Use the following command to view each dataset details.

bq show <data\_set\_object>

Verify the kmsKeyName is present.

#### **Remediation:**

The default CMEK for existing data sets can be updated by specifying the default key in the EncryptionConfiguration.kmsKeyName field when calling the datasets.insert or datasets.patch methods

#### **Default Value:**

Google Managed keys are used as key encryption keys.

#### **References:**

1. <u>https://cloud.google.com/bigquery/docs/customer-managed-encryption</u>

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11</b> Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		•	
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			
# Appendix: Recommendation Summary Table

	Control		et
		Vos	No
1	Identity and Access Management	103	NU
1.1	Ensure that Corporate Login Credentials are Used (Manual)		
1.2	Ensure that Multi-Factor Authentication is 'Enabled' for All		_
	Non-Service Accounts (Manual)		
1.3	Ensure that Security Key Enforcement is Enabled for All		
	Admin Accounts (Manual)		
1.4	Ensure That There Are Only GCP-Managed Service Account		
	Keys for Each Service Account (Automated)		
1.5	Ensure That Service Account Has No Admin Privileges		
	(Automated)		
1.6	Ensure That IAM Users Are Not Assigned the Service		
	Account User or Service Account Token Creator Roles at		
	Project Level (Automated)		
1.7	Ensure User-Managed/External Keys for Service Accounts		
	Are Rotated Every 90 Days or Fewer (Automated)		
1.8	Ensure That Separation of Duties Is Enforced While		
	Assigning Service Account Related Roles to Users		
	(Automated)		
1.9	Ensure That Cloud KMS Cryptokeys Are Not Anonymously		
	or Publicly Accessible (Automated)		
1.10	Ensure KMS Encryption Keys Are Rotated Within a Period of		
	90 Days (Automated)		
1.11	Ensure That Separation of Duties Is Enforced While		
4.40	Assigning KMS Related Roles to Users (Automated)		
1.12	Ensure API Keys Are Not Created for a Project (Manual)		
1.13	Ensure API Keys Are Restricted To Use by Only Specified		
	Hosts and Apps (Manual)		
1.14	Ensure API Keys Are Restricted to Only APIs That		
4.45	Application Needs Access (Manual)		
1.15	Ensure API Keys Are Rotated Every 90 Days (Manual)		
1.16	Ensure Essential Contacts is Configured for Organization		
1 1 7	[Automated]		
1.17	Ensure that Dataproc Cluster is encrypted using Customer-		
	Managed Encryption Key (Automated)		

1.18	Ensure Secrets are Not Stored in Cloud Functions	
2	Environment variables by Using Secret Manager (Manual)	
2	Logging and Monitoring	
2.1	Ensure That Cloud Audit Logging Is Configured Properly	_
	Across All Services and All Users From a Project	
2.2	[Automated]	
2.2	Ensure That Sinks Are Configured for All Log Entries	
2.2	(Automateu)	
2.3	Lisure That Retention Policies on Cloud Storage Buckets	
	(Automated)	
2.4	(Automateu)	
2.4	Ensure Log Metric Filter and Aleris Exist for Project	
25	Ensure That the Log Matrice Filter and Alerta Evict for Audit	
2.5	Configuration Changes (Automated)	
2.(	Ensure That the Log Matrie Filter and Alerta Fuict for	
2.0	Ensure That the Log Metric Filter and Alerts Exist for Custom Dala Changes (Automated)	
27	Ensure That the Log Matrie Filter and Alerta Evict for VDC	
2.7	Notwork Firewall Pule Changes (Automated)	
20	Ensure That the Log Metric Filter and Alerta Evict for VDC	
2.0	Notwork Pouto Changes (Automated)	
2.0	Ensure That the Log Matric Filter and Alerte Exist for VDC	
2.9	Network Changes (Automated)	
2.10	Ensure That the Log Metric Filter and Alerts Exist for Cloud	
	Storage IAM Permission Changes (Automated)	
2.11	Ensure That the Log Metric Filter and Alerts Exist for SQL	
	Instance Configuration Changes (Automated)	
2.12	Ensure That Cloud DNS Logging Is Enabled for All VPC	
	Networks (Automated)	
2.13	Ensure Cloud Asset Inventory Is Enabled (Automated)	
2.14	Ensure 'Access Transparency' is 'Enabled' (Manual)	
2.15	Ensure 'Access Approval' is 'Enabled' (Automated)	
3	Networking	-
3.1	Ensure That the Default Network Does Not Exist in a Project	_
	(Automated)	
3.2	Ensure Legacy Networks Do Not Exist for Older Projects	
	(Automated)	
3.3	Ensure That DNSSEC Is Enabled for Cloud DNS (Automated)	
3.4	Ensure That RSASHA1 Is Not Used for the Key-Signing Key	
	in Cloud DNS DNSSEC (Manual)	
3.5	Ensure That RSASHA1 Is Not Used for the Zone-Signing Key	
	in Cloud DNS DNSSEC (Manual)	
3.6	Ensure That SSH Access Is Restricted From the Internet	
	(Automated)	

3.7	Ensure That RDP Access Is Restricted From the Internet (Automated)	
3.8	Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network (Automated)	
3.9	Ensure No HTTPS or SSL Proxy Load Balancers Permit SSL Policies With Weak Cipher Suites (Manual)	
3.10	Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed' (Manual)	
4	Virtual Machines	 
4.1	Ensure That Instances Are Not Configured To Use the Default Service Account (Automated)	
4.2	Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs (Automated)	
4.3	Ensure "Block Project-Wide SSH Keys" Is Enabled for VM Instances (Automated)	
4.4	Ensure Oslogin Is Enabled for a Project (Automated)	
4.5	Ensure 'Enable Connecting to Serial Ports' Is Not Enabled for VM Instance (Automated)	
4.6	Ensure That IP Forwarding Is Not Enabled on Instances (Automated)	
4.7	Ensure VM Disks for Critical VMs Are Encrypted With Customer-Supplied Encryption Keys (CSEK) (Automated)	
4.8	Ensure Compute Instances Are Launched With Shielded VM Enabled (Automated)	
4.9	Ensure That Compute Instances Do Not Have Public IP Addresses (Automated)	
4.10	Ensure That App Engine Applications Enforce HTTPS Connections (Manual)	
4.11	Ensure That Compute Instances Have Confidential Computing Enabled (Automated)	
4.12	Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects (Manual)	
5	Storage	
5.1	Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible (Automated)	
5.2	Ensure That Cloud Storage Buckets Have Uniform Bucket- Level Access Enabled (Automated)	
6	Cloud SQL Database Services	
6.1	MySQL Database	
6.1.1	Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges (Manual)	

6.1.2	Ensure 'Skip_show_database' Database Flag for Cloud SQL MySQL Instance Is Set to 'On' (Automated)		
6.1.3	Ensure That the 'Local_infile' Database Flag for a Cloud SQL MySQL Instance Is Set to 'Off' (Automated)		
6.2	PostgreSQL Database		
6.2.1	Ensure 'Log_error_verbosity' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'DEFAULT' or Stricter (Manual)		
6.2.2	Ensure That the 'Log_connections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' (Automated)		
6.2.3	Ensure That the 'Log_disconnections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' (Automated)		
6.2.4	Ensure 'Log_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately (Manual)		
6.2.5	Ensure 'Log_hostname' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'on' (Automated)		
6.2.6	Ensure That the 'Log_min_messages' Database Flag for Cloud SQL PostgreSQL Instance Is Set to at least 'Warning' (Manual)		
6.2.7	Ensure 'Log_min_error_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter (Automated)		
6.2.8	Ensure That the 'Log_min_duration_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled) (Automated)		
6.2.9	Ensure That 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging (Automated)		
6.3	SQL Server	-	-
6.3.1	Ensure 'external scripts enabled' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)		
6.3.2	Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)		
6.3.3	Ensure 'user Connections' Database Flag for Cloud Sql Sql Server Instance Is Set to a Non-limiting Value (Automated)		
6.3.4	Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured (Automated)		
6.3.5	Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)		
6.3.6	Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'off' (Automated)		
6.3.7	Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is set to 'off' (Automated)		

6.4	Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL (Automated)	
6.5	Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses (Automated)	
6.6	Ensure That Cloud SQL Database Instances Do Not Have Public IPs (Automated)	
6.7	Ensure That Cloud SQL Database Instances Are Configured With Automated Backups (Automated)	
7	BigQuery	
7.1	Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible (Manual)	
7.2	Ensure That All BigQuery Tables Are Encrypted With Customer-Managed Encryption Key (CMEK) (Automated)	
7.3	Ensure That a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets (Manual)	

# Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		S	et
		Corr	ectly
		Yes	No
1.5	Ensure That Service Account Has No Admin Privileges		
1.6	Ensure That IAM Users Are Not Assigned the Service		
	Account User or Service Account Token Creator Roles at		
	Project Level		
1.8	Ensure That Separation of Duties Is Enforced While		
	Assigning Service Account Related Roles to Users		
1.9	Ensure That Cloud KMS Cryptokeys Are Not Anonymously		
	or Publicly Accessible		
1.11	Ensure That Separation of Duties Is Enforced While		
	Assigning KMS Related Roles to Users		
1.16	Ensure Essential Contacts is Configured for Organization		
2.1	Ensure That Cloud Audit Logging Is Configured Properly		
	Across All Services and All Users From a Project		
2.2	Ensure That Sinks Are Configured for All Log Entries		
2.3	Ensure That Retention Policies on Cloud Storage Buckets		
	Used for Exporting Logs Are Configured Using Bucket Lock		
2.4	Ensure Log Metric Filter and Alerts Exist for Project		
	Ownership Assignments/Changes		
2.5	Ensure That the Log Metric Filter and Alerts Exist for Audit		
	Configuration Changes		
2.6	Ensure That the Log Metric Filter and Alerts Exist for		
	Custom Role Changes		
2.7	Ensure That the Log Metric Filter and Alerts Exist for VPC		
	Network Firewall Rule Changes		
2.8	Ensure That the Log Metric Filter and Alerts Exist for VPC		
	Network Route Changes		
2.9	Ensure That the Log Metric Filter and Alerts Exist for VPC		
	Network Changes		
2.10	Ensure That the Log Metric Filter and Alerts Exist for Cloud		
	Storage IAM Permission Changes		
2.11	Ensure That the Log Metric Filter and Alerts Exist for SQL		
	Instance Configuration Changes		
2.12	Ensure That Cloud DNS Logging Is Enabled for All VPC		
	Networks		
2.13	Ensure Cloud Asset Inventory Is Enabled		

2.14	Ensure 'Access Transparency' is 'Enabled'	
2.15	Ensure 'Access Approval' is 'Enabled'	
3.6	Ensure That SSH Access Is Restricted From the Internet	
3.7	Ensure That RDP Access Is Restricted From the Internet	
3.8	Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network	
4.9	Ensure That Compute Instances Do Not Have Public IP Addresses	
4.12	Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects	
5.1	Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible	
5.2	Ensure That Cloud Storage Buckets Have Uniform Bucket- Level Access Enabled	
6.1.1	Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges	
6.1.2	Ensure 'Skip_show_database' Database Flag for Cloud SQL MySQL Instance Is Set to 'On'	
6.3.2	Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'	
6.3.4	Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured	
6.3.7	Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is set to 'off'	
6.5	Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses	
6.6	Ensure That Cloud SQL Database Instances Do Not Have Public IPs	
6.7	Ensure That Cloud SQL Database Instances Are Configured With Automated Backups	
7.1	Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible	

# Appendix: CIS Controls v7 IG 2 Mapped Recommendations

	Recommendation		et
		Corr	ectly
		Yes	No
1.1	Ensure that Corporate Login Credentials are Used		
1.2	Ensure that Multi-Factor Authentication is 'Enabled' for All		
	Non-Service Accounts		
1.3	Ensure that Security Key Enforcement is Enabled for All Admin Accounts		
1.5	Ensure That Service Account Has No Admin Privileges		
1.6	Ensure That IAM Users Are Not Assigned the Service		
	Account User or Service Account Token Creator Roles at Project Level		
1.8	Ensure That Separation of Duties Is Enforced While		
1.0	Assigning Service Account Related Roles to Users	──	
1.9	Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible		
1.11	Ensure That Separation of Duties Is Enforced While		
	Assigning KMS Related Roles to Users		
1.16	Ensure Essential Contacts is Configured for Organization		
1.18	Ensure Secrets are Not Stored in Cloud Functions		
	Environment Variables by Using Secret Manager		
2.1	Ensure That Cloud Audit Logging Is Configured Properly		
2.2	Across All Services and All Users From a Project	┝╤╴	
2.2	Ensure That Sinks Are Configured for All Log Entries	$+$ $\square$	
2.3	Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock		
2.4	Ensure Log Metric Filter and Alerts Exist for Project		
	Ownership Assignments/Changes		
2.5	Ensure That the Log Metric Filter and Alerts Exist for Audit		
	Configuration Changes		
2.6	Ensure That the Log Metric Filter and Alerts Exist for Custom Bole Changes		
27	Ensure That the Log Metric Filter and Alerts Exist for VPC	+	
2.7	Network Firewall Rule Changes		
2.8	Ensure That the Log Metric Filter and Alerts Exist for VPC		
	Network Route Changes		
2.9	Ensure That the Log Metric Filter and Alerts Exist for VPC		
	Network Changes		

2.10	Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes		
2.11	Ensure That the Log Metric Filter and Alerts Exist for SQL		
2.12	Instance Configuration Changes		
2.12	Networks		
2.13	Ensure Cloud Asset Inventory Is Enabled		
2.14	Ensure 'Access Transparency' is 'Enabled'		
2.15	Ensure 'Access Approval' is 'Enabled'		
3.1	Ensure That the Default Network Does Not Exist in a Project		
3.2	Ensure Legacy Networks Do Not Exist for Older Projects		
3.3	Ensure That DNSSEC Is Enabled for Cloud DNS		
3.4	Ensure That RSASHA1 Is Not Used for the Key-Signing Key		
	in Cloud DNS DNSSEC		
3.5	Ensure That RSASHA1 Is Not Used for the Zone-Signing Key		
	in Cloud DNS DNSSEC		
3.6	Ensure That SSH Access Is Restricted From the Internet		
3.7	Ensure That RDP Access Is Restricted From the Internet		
3.8	Ensure that VPC Flow Logs is Enabled for Every Subnet in a		
	VPC Network		
3.9	Ensure No HTTPS or SSL Proxy Load Balancers Permit SSL Policies With Weak Cipher Suites		
3.10	Use Identity Aware Proxy (IAP) to Ensure Only Traffic From		
	Google IP Addresses are 'Allowed'		
4.1	Ensure That Instances Are Not Configured To Use the		
4.2	Ensure That Instances Are Not Configured To Use the		
4.2	Default Service Account With Full Access to All Cloud APIs		
4.3	Ensure "Block Project-Wide SSH Keys" Is Enabled for VM		
	Instances		
4.4	Ensure Oslogin Is Enabled for a Project		
4.5	Ensure 'Enable Connecting to Serial Ports' Is Not Enabled for VM Instance		
4.6	Ensure That IP Forwarding Is Not Enabled on Instances		
4.8	Ensure Compute Instances Are Launched With Shielded VM		
4.9	Ensure That Compute Instances Do Not Have Public IP	_	
	Addresses	Ш	Ш
4.10	Ensure That App Engine Applications Enforce HTTPS		
4 1 2	Connections		
4.12	On Your Virtual Machines in All Projects		
5.1	Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible		
B			

5.2	Ensure That Cloud Storage Buckets Have Uniform Bucket- Level Access Enabled	
6.1.1	Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges	
6.1.2	Ensure 'Skip_show_database' Database Flag for Cloud SQL MySQL Instance Is Set to 'On'	
6.2.1	Ensure 'Log_error_verbosity' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'DEFAULT' or Stricter	
6.2.2	Ensure That the 'Log_connections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On'	
6.2.3	Ensure That the 'Log_disconnections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On'	
6.2.4	Ensure 'Log_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately	
6.2.5	Ensure 'Log_hostname' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'on'	
6.2.6	Ensure That the 'Log_min_messages' Database Flag for Cloud SQL PostgreSQL Instance Is Set to at least 'Warning'	
6.2.7	Ensure 'Log_min_error_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter	
6.2.8	Ensure That the 'Log_min_duration_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled)	
6.2.9	Ensure That 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging	
6.3.2	Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'	
6.3.4	Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured	
6.3.5	Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off'	
6.3.7	Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is set to 'off'	
6.4	Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL	
6.5	Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses	
6.6	Ensure That Cloud SQL Database Instances Do Not Have Public IPs	
6.7	Ensure That Cloud SQL Database Instances Are Configured With Automated Backups	

7.1	Ensure That BigQuery Datasets Are Not Anonymously or	
	Publicly Accessible	

# Appendix: CIS Controls v7 IG 3 Mapped Recommendations

	Recommendation	S	et
		Corr	ectly
		Yes	No
1.1	Ensure that Corporate Login Credentials are Used		
1.2	Ensure that Multi-Factor Authentication is 'Enabled' for All Non-Service Accounts		
1.3	Ensure that Security Key Enforcement is Enabled for All Admin Accounts		
1.5	Ensure That Service Account Has No Admin Privileges		
1.6	Ensure That IAM Users Are Not Assigned the Service Account User or Service Account Token Creator Roles at Project Level		
1.8	Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users		
1.9	Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible		
1.10	Ensure KMS Encryption Keys Are Rotated Within a Period of 90 Days		
1.11	Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users		
1.16	Ensure Essential Contacts is Configured for Organization		
1.17	Ensure that Dataproc Cluster is encrypted using Customer- Managed Encryption Key		
1.18	Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager		
2.1	Ensure That Cloud Audit Logging Is Configured Properly Across All Services and All Users From a Project		
2.2	Ensure That Sinks Are Configured for All Log Entries		
2.3	Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock		
2.4	Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes		
2.5	Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes		
2.6	Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes		
2.7	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes		

2.8	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes	
2.9	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes	
2.10	Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes	
2.11	Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes	
2.12	Ensure That Cloud DNS Logging Is Enabled for All VPC Networks	
2.13	Ensure Cloud Asset Inventory Is Enabled	
2.14	Ensure 'Access Transparency' is 'Enabled'	
2.15	Ensure 'Access Approval' is 'Enabled'	
3.1	Ensure That the Default Network Does Not Exist in a Project	
3.2	Ensure Legacy Networks Do Not Exist for Older Projects	
3.3	Ensure That DNSSEC Is Enabled for Cloud DNS	
3.4	Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC	
3.5	Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC	
3.6	Ensure That SSH Access Is Restricted From the Internet	
3.7	Ensure That RDP Access Is Restricted From the Internet	
3.8	Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network	
3.9	Ensure No HTTPS or SSL Proxy Load Balancers Permit SSL Policies With Weak Cipher Suites	
3.10	Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed'	
4.1	Ensure That Instances Are Not Configured To Use the Default Service Account	
4.2	Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs	
4.3	Ensure "Block Project-Wide SSH Keys" Is Enabled for VM Instances	
4.4	Ensure Oslogin Is Enabled for a Project	
4.5	Ensure 'Enable Connecting to Serial Ports' Is Not Enabled for VM Instance	
4.6	Ensure That IP Forwarding Is Not Enabled on Instances	
4.7	Ensure VM Disks for Critical VMs Are Encrypted With Customer-Supplied Encryption Keys (CSEK)	
4.8	Ensure Compute Instances Are Launched With Shielded VM Enabled	
4.9	Ensure That Compute Instances Do Not Have Public IP Addresses	

4.10	Ensure That App Engine Applications Enforce HTTPS Connections	
4.11	Ensure That Compute Instances Have Confidential Computing Enabled	
4.12	Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects	
5.1	Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible	
5.2	Ensure That Cloud Storage Buckets Have Uniform Bucket- Level Access Enabled	
6.1.1	Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges	
6.1.2	Ensure 'Skip_show_database' Database Flag for Cloud SQL MySQL Instance Is Set to 'On'	
6.2.1	Ensure 'Log_error_verbosity' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'DEFAULT' or Stricter	
6.2.2	Ensure That the 'Log_connections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On'	
6.2.3	Ensure That the 'Log_disconnections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On'	
6.2.4	Ensure 'Log_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately	
6.2.5	Ensure 'Log_hostname' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'on'	
6.2.6	Ensure That the 'Log_min_messages' Database Flag for Cloud SQL PostgreSQL Instance Is Set to at least 'Warning'	
6.2.7	Ensure 'Log_min_error_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter	
6.2.8	Ensure That the 'Log_min_duration_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled)	
6.2.9	Ensure That 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging	
6.3.1	Ensure 'external scripts enabled' database flag for Cloud SQL SQL Server instance is set to 'off'	
6.3.2	Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'	
6.3.4	Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured	
6.3.5	Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off'	

6.3.7	Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is set to 'off'	
6.4	Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL	
6.5	Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses	
6.6	Ensure That Cloud SQL Database Instances Do Not Have Public IPs	
6.7	Ensure That Cloud SQL Database Instances Are Configured With Automated Backups	
7.1	Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible	
7.2	Ensure That All BigQuery Tables Are Encrypted With Customer-Managed Encryption Key (CMEK)	
7.3	Ensure That a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets	

# Appendix: CIS Controls v8 IG 1 Mapped Recommendations

	Recommendation		et
		Corr	ectly
		Yes	No
1.5	Ensure That Service Account Has No Admin Privileges		
1.6	Ensure That IAM Users Are Not Assigned the Service		
	Account User or Service Account Token Creator Roles at		
	Project Level		
1.8	Ensure That Separation of Duties Is Enforced While		
	Assigning Service Account Related Roles to Users		
1.9	Ensure That Cloud KMS Cryptokeys Are Not Anonymously		
	or Publicly Accessible		
1.11	Ensure That Separation of Duties Is Enforced While		
	Assigning KMS Related Roles to Users		
1.16	Ensure Essential Contacts is Configured for Organization		
2.1	Ensure That Cloud Audit Logging Is Configured Properly		
	Across All Services and All Users From a Project		
2.2	Ensure That Sinks Are Configured for All Log Entries		
2.3	Ensure That Retention Policies on Cloud Storage Buckets		
	Used for Exporting Logs Are Configured Using Bucket Lock		
2.4	Ensure Log Metric Filter and Alerts Exist for Project		
	Ownership Assignments/Changes		
2.5	Ensure That the Log Metric Filter and Alerts Exist for Audit		
	Configuration Changes		
2.6	Ensure That the Log Metric Filter and Alerts Exist for		
	Custom Role Changes		
2.7	Ensure That the Log Metric Filter and Alerts Exist for VPC		
	Network Firewall Rule Changes		
2.8	Ensure That the Log Metric Filter and Alerts Exist for VPC		
	Network Route Changes		
2.9	Ensure That the Log Metric Filter and Alerts Exist for VPC		
	Network Changes		
2.10	Ensure That the Log Metric Filter and Alerts Exist for Cloud		
	Storage IAM Permission Changes		
2.11	Ensure That the Log Metric Filter and Alerts Exist for SQL		
	Instance Configuration Changes		
2.12	Ensure That Cloud DNS Logging Is Enabled for All VPC		
	Networks		
2.13	Ensure Cloud Asset Inventory Is Enabled		

2.14	Ensure 'Access Transparency' is 'Enabled'	
2.15	Ensure 'Access Approval' is 'Enabled'	
3.1	Ensure That the Default Network Does Not Exist in a Project	
3.2	Ensure Legacy Networks Do Not Exist for Older Projects	
3.3	Ensure That DNSSEC Is Enabled for Cloud DNS	
3.4	Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC	
3.5	Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC	
3.6	Ensure That SSH Access Is Restricted From the Internet	
3.7	Ensure That RDP Access Is Restricted From the Internet	
3.8	Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network	
4.1	Ensure That Instances Are Not Configured To Use the Default Service Account	
4.2	Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs	
4.3	Ensure "Block Project-Wide SSH Keys" Is Enabled for VM Instances	
4.6	Ensure That IP Forwarding Is Not Enabled on Instances	
4.9	Ensure That Compute Instances Do Not Have Public IP Addresses	
4.12	Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects	
5.1	Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible	
5.2	Ensure That Cloud Storage Buckets Have Uniform Bucket- Level Access Enabled	
6.1.1	Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges	
6.1.2	Ensure 'Skip_show_database' Database Flag for Cloud SQL MySQL Instance Is Set to 'On'	
6.3.2	Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'	
6.3.4	Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured	
6.3.7	Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is set to 'off'	
6.5	Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses	
6.6	Ensure That Cloud SQL Database Instances Do Not Have Public IPs	

6.7	Ensure That Cloud SQL Database Instances Are Configured With Automated Backups	
7.1	Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible	

# Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set	
		Corr	ectly
		Yes	No
1.1	Ensure that Corporate Login Credentials are Used		
1.2	Ensure that Multi-Factor Authentication is 'Enabled' for All Non-Service Accounts		
1.3	Ensure that Security Key Enforcement is Enabled for All Admin Accounts		
1.5	Ensure That Service Account Has No Admin Privileges	П	
1.6	Ensure That IAM Users Are Not Assigned the Service Account User or Service Account Token Creator Roles at Project Level		
1.8	Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users		
1.9	Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible		
1.10	Ensure KMS Encryption Keys Are Rotated Within a Period of 90 Days		
1.11	Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users		
1.16	Ensure Essential Contacts is Configured for Organization		
1.17	Ensure that Dataproc Cluster is encrypted using Customer- Managed Encryption Key		
1.18	Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager		
2.1	Ensure That Cloud Audit Logging Is Configured Properly Across All Services and All Users From a Project		
2.2	Ensure That Sinks Are Configured for All Log Entries		
2.3	Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock		
2.4	Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes		
2.5	Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes		
2.6	Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes		
2.7	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes		

2.8	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes	
2.9	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes	
2.10	Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes	
2.11	Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes	
2.12	Ensure That Cloud DNS Logging Is Enabled for All VPC Networks	
2.13	Ensure Cloud Asset Inventory Is Enabled	
2.14	Ensure 'Access Transparency' is 'Enabled'	
2.15	Ensure 'Access Approval' is 'Enabled'	
3.1	Ensure That the Default Network Does Not Exist in a Project	
3.2	Ensure Legacy Networks Do Not Exist for Older Projects	
3.3	Ensure That DNSSEC Is Enabled for Cloud DNS	
3.4	Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC	
3.5	Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC	
3.6	Ensure That SSH Access Is Restricted From the Internet	
3.7	Ensure That RDP Access Is Restricted From the Internet	
3.8	Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network	
3.9	Ensure No HTTPS or SSL Proxy Load Balancers Permit SSL Policies With Weak Cipher Suites	
3.10	Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed'	
4.1	Ensure That Instances Are Not Configured To Use the Default Service Account	
4.2	Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs	
4.3	Ensure "Block Project-Wide SSH Keys" Is Enabled for VM Instances	
4.4	Ensure Oslogin Is Enabled for a Project	
4.5	Ensure 'Enable Connecting to Serial Ports' Is Not Enabled for VM Instance	
4.6	Ensure That IP Forwarding Is Not Enabled on Instances	
4.7	Ensure VM Disks for Critical VMs Are Encrypted With Customer-Supplied Encryption Keys (CSEK)	
4.9	Ensure That Compute Instances Do Not Have Public IP Addresses	
4.10	Ensure That App Engine Applications Enforce HTTPS Connections	

4.11	Ensure That Compute Instances Have Confidential Computing Enabled	
4.12	Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects	
5.1	Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible	
5.2	Ensure That Cloud Storage Buckets Have Uniform Bucket- Level Access Enabled	
6.1.1	Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges	
6.1.2	Ensure 'Skip_show_database' Database Flag for Cloud SQL MySQL Instance Is Set to 'On'	
6.2.1	Ensure 'Log_error_verbosity' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'DEFAULT' or Stricter	
6.2.2	Ensure That the 'Log_connections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On'	
6.2.3	Ensure That the 'Log_disconnections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On'	
6.2.4	Ensure 'Log_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately	
6.2.5	Ensure 'Log_hostname' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'on'	
6.2.6	Ensure That the 'Log_min_messages' Database Flag for Cloud SQL PostgreSQL Instance Is Set to at least 'Warning'	
6.2.7	Ensure 'Log_min_error_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter	
6.2.8	Ensure That the 'Log_min_duration_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled)	
6.2.9	Ensure That 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging	
6.3.2	Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'	
6.3.4	Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured	
6.3.5	Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off'	
6.3.7	Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is set to 'off'	
6.4	Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL	

6.5	Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses	
6.6	Ensure That Cloud SQL Database Instances Do Not Have Public IPs	
6.7	Ensure That Cloud SQL Database Instances Are Configured With Automated Backups	
7.1	Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible	
7.2	Ensure That All BigQuery Tables Are Encrypted With Customer-Managed Encryption Key (CMEK)	
7.3	Ensure That a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets	

# Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set	
		Corr	ectly
		Yes	No
1.1	Ensure that Corporate Login Credentials are Used		
1.2	Ensure that Multi-Factor Authentication is 'Enabled' for All Non-Service Accounts		
1.3	Ensure that Security Key Enforcement is Enabled for All Admin Accounts		
1.5	Ensure That Service Account Has No Admin Privileges	П	
1.6	Ensure That IAM Users Are Not Assigned the Service Account User or Service Account Token Creator Roles at Project Level		
1.8	Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users		
1.9	Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible		
1.10	Ensure KMS Encryption Keys Are Rotated Within a Period of 90 Days		
1.11	Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users		
1.16	Ensure Essential Contacts is Configured for Organization		
1.17	Ensure that Dataproc Cluster is encrypted using Customer- Managed Encryption Key		
1.18	Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager		
2.1	Ensure That Cloud Audit Logging Is Configured Properly Across All Services and All Users From a Project		
2.2	Ensure That Sinks Are Configured for All Log Entries		
2.3	Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock		
2.4	Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes		
2.5	Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes		
2.6	Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes		
2.7	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes		

2.8	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes	
2.9	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes	
2.10	Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes	
2.11	Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes	
2.12	Ensure That Cloud DNS Logging Is Enabled for All VPC Networks	
2.13	Ensure Cloud Asset Inventory Is Enabled	
2.14	Ensure 'Access Transparency' is 'Enabled'	
2.15	Ensure 'Access Approval' is 'Enabled'	
3.1	Ensure That the Default Network Does Not Exist in a Project	
3.2	Ensure Legacy Networks Do Not Exist for Older Projects	
3.3	Ensure That DNSSEC Is Enabled for Cloud DNS	
3.4	Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC	
3.5	Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC	
3.6	Ensure That SSH Access Is Restricted From the Internet	
3.7	Ensure That RDP Access Is Restricted From the Internet	
3.8	Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network	
3.9	Ensure No HTTPS or SSL Proxy Load Balancers Permit SSL Policies With Weak Cipher Suites	
3.10	Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed'	
4.1	Ensure That Instances Are Not Configured To Use the Default Service Account	
4.2	Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs	
4.3	Ensure "Block Project-Wide SSH Keys" Is Enabled for VM Instances	
4.4	Ensure Oslogin Is Enabled for a Project	
4.5	Ensure 'Enable Connecting to Serial Ports' Is Not Enabled for VM Instance	
4.6	Ensure That IP Forwarding Is Not Enabled on Instances	
4.7	Ensure VM Disks for Critical VMs Are Encrypted With Customer-Supplied Encryption Keys (CSEK)	
4.9	Ensure That Compute Instances Do Not Have Public IP Addresses	
4.10	Ensure That App Engine Applications Enforce HTTPS Connections	

4.11	Ensure That Compute Instances Have Confidential Computing Enabled	
4.12	Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects	
5.1	Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible	
5.2	Ensure That Cloud Storage Buckets Have Uniform Bucket- Level Access Enabled	
6.1.1	Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges	
6.1.2	Ensure 'Skip_show_database' Database Flag for Cloud SQL MySQL Instance Is Set to 'On'	
6.2.1	Ensure 'Log_error_verbosity' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'DEFAULT' or Stricter	
6.2.2	Ensure That the 'Log_connections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On'	
6.2.3	Ensure That the 'Log_disconnections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On'	
6.2.4	Ensure 'Log_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately	
6.2.5	Ensure 'Log_hostname' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'on'	
6.2.6	Ensure That the 'Log_min_messages' Database Flag for Cloud SQL PostgreSQL Instance Is Set to at least 'Warning'	
6.2.7	Ensure 'Log_min_error_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter	
6.2.8	Ensure That the 'Log_min_duration_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled)	
6.2.9	Ensure That 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging	
6.3.1	Ensure 'external scripts enabled' database flag for Cloud SQL SQL Server instance is set to 'off'	
6.3.2	Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'	
6.3.4	Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured	
6.3.5	Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off'	
6.3.7	Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is set to 'off'	

6.4	Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL	
6.5	Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses	
6.6	Ensure That Cloud SQL Database Instances Do Not Have Public IPs	
6.7	Ensure That Cloud SQL Database Instances Are Configured With Automated Backups	
7.1	Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible	
7.2	Ensure That All BigQuery Tables Are Encrypted With Customer-Managed Encryption Key (CMEK)	
7.3	Ensure That a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets	

#### **Appendix: Change History**

Date	Version	Changes for this version
Apr 30, 2021	1.3.0	ADD - Ensure that Compute instances have Confidential Computing enabled (Ticket 12721)
Nov 30, 2021	1.3.0	UPDATE- Ensure Cloud Asset Inventory is enabled - ADD: Propose enabling of Cloud Asset Inventory (Ticket 13677)
Dec 8, 2021	1.3.0	UPDATE- Ensure "Block Project-Wide SSH Keys" Is Enabled for VM Instances - 4.3 - list instances should be sufficient (Ticket 13500)
Dec 8, 2021	1.3.0	UPDATE- Ensure That Instances Are Not Configured To Use the Default Service Account -4.1 - List instances should be sufficient (Ticket 13499)
Dec 8, 2021	1.3.0	UPDATE- Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'- Rule 6.3.2 has no default value and document formatting issues (Ticket 13497)
Dec 8, 2021	1.3.0	UPDATE- Ensure that Corporate Login Credentials are Used -Rule 1.1: Rule should be manual rather than automated assessment (Ticket 13592)
Dec 8, 2021	1.3.0	UPDATE- Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'off' -Rule 6.3.6 - No default value is provided (Ticket 13501)
Mar 19, 2022	1.3.0	UPDATE - Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network - gcloud command makes unnecessary calls (Ticket 13490)
Dec 28, 2021	1.3.0	UPDATE- Ensure That Cloud Audit Logging Is Configured Properly Across All Services and All Users From a Project -Audit Procedure Doesn't Match Remediation Procedure (Ticket 13540)
Jan 18, 2022	1.3.0	UPDATE - Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'off' - Rule 6.3.6 (Ticket 13604)

Jan 18, 2022	1.3.0	UPDATE- Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'off' - The Description seems to be ambiguous needs to be reviewed (Ticket 13128)
Jan 18, 2022	1.3.0	UPDATE - Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'off' -[6.3.6] Recommend '3625 (trace flag)' database flag to be "ON" (Ticket 14295)
Jan 25, 2022	1.3.0	UPDATE - Ensure 'Log_hostname' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Off' - Explicit recommendation it set it "Off" instead "set appropriately" (Ticket 14297)
Jan 25, 2022	1.3.0	UPDATE- Ensure 'user Connections' Database Flag for Cloud Sql Sql Server Instance Is Set to a Non-limiting Value - Require clarification on what an 'appropriate value' should be (Ticket 13498)
Jan 25, 2022	1.3.0	UPDATE - Ensure That the 'Log_min_messages' Database Flag for Cloud SQL PostgreSQL Instance Is Set to at least 'Warning' - Recommend to set the parameter as WARNING (Ticket 14296)
Jan 25, 2022	1.3.0	UPDATE- Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes - Implement a more flexible approach in the filter for a better matching capability (Ticket 14294)
Jan 25, 2022	1.3.0	UPDATE - Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes - Implement a more flexible approach in the filter for a better matching capability (Ticket 14293)
Jan 25, 2022	1.3.0	UPDATE - Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes - Implement a more flexible approach in the filter for a better matching capability (Ticket 14292)
Jan 25, 2022	1.3.0	UPDATE Multiple in Big Data section - List data sets on CLI to get DATASET_NAME (Ticket 13538)
Mar 1, 2022	1.3.0	UPDATE - Multiple in section 3 - The RSASHA1 algorithm now requires explicit whitelisting to access (due to deprecation) (Ticket 14757)
Mar 1, 2022	1.3.0	UPDATE - Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed' - The Audit Procedure steps needs to be updated (Ticket 13137)

Mar 1, 2022	1.3.0	UPDATE - Multiple in section 4 - gcloud commands can be reduced (Ticket 13502)
Mar 1, 2022	1.3.0	DELETE - Ensure 'Log_duration' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' - any security implication of this setting (Ticket 14708)
Mar 1, 2022	1.3.0	DELETE - Ensure 'Log_parser_stats' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Off' - security value? (Ticket 14710)
Mar 1, 2022	1.3.0	DELETE - Ensure 'Log_planner_stats' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Off' - security value? (Ticket 14711)
Mar 1, 2022	1.3.0	DELETE - Ensure 'Log_executor_stats' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Off' - what security value? (Ticket 14712)
Mar 1, 2022	1.3.0	DELETE - Ensure 'Log_statement_stats' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Off' - security value? (Ticket 14713)
Mar 1, 2022	1.3.0	DELETE - Ensure That the 'Log_lock_waits' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' - any security implication of this setting (Ticket 14727)
Mar 1, 2022	1.3.0	DELETE - Ensure That the 'Log_temp_files' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '0' (On) - any security implication of this setting (Ticket 14728)
Mar 1, 2022	1.3.0	DELETE - Ensure That the 'Log_checkpoints' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' - security value (Ticket 14729)
Mar 3, 2022	1.3.0	UPDATE - Ensure That Sinks Are Configured for All Log Entries - Audit and Remediation steps updated (Ticket 14950)
Mar 3, 2022	1.3.0	UPDATE - Ensure 'Log_hostname' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Off' - security value? (Ticket 14709)
Mar 31, 2022	1.3.0	UPDATE - Ensure That Cloud SQL Database Instances Do Not Have Public IPs -Correct 'email' to 'IP' (Ticket 15115)
Mar 17, 2022	1.3.0	ADD - Ensure that Dataproc Cluster is encrypted using Customer- Managed Encryption Key (Ticket 13029)

Mar 17, 2022	1.3.0	UPDATE- Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock - Make L2 and update remediation steps (Ticket 13047)
Mar 19, 2022	1.3.0	UPDATE - Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges - should be manual assessment rather than automated. updated audit and remediation (Ticket 13507)
Mar 17, 2022	1.3.0	ADD - Ensure Essential Contacts is Configured for Organization (Ticket 15118)
Mar 17, 2022	1.3.0	ADD - Ensure that 'Access Approval' is 'Enabled' (Ticket 15180)
Mar 17, 2022	1.3.0	ADD - Ensure 'Access Transparency' is 'Enabled' - & - Ensure that 'Access Approval' is 'Enabled' (Ticket 12749)
Mar 17, 2022	1.3.0	UPDATE - Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users - Add Automation for audit (Ticket 15117)
Mar 17, 2022	1.3.0	UPATE - Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network - Ensure config parameters, add to rationale, audit, and remediation (Ticket 13920)
Mar 18, 2022	1.3.0	ADD - Ensure That 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Central Logging in Google Cloud - (Ticket 12866)
Mar 18, 2022	1.3.0	ADD - Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects (Ticket 13301)
Mar 18, 2022	1.3.0	ADD - Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager (Ticket 10159)
Mar 25, 2022	1.3.0	UPDATE - Ensure "Block Project-Wide SSH Keys" Is Enabled for VM Instances - provide the reason for the "Exception" in audit section (Ticket 13660)
Mar 25, 2022	1.3.0	UPDATE - Ensure API Keys Are Restricted to Only APIs That Application Needs Access - amend the description text to be less severe (Ticket 15195)

Mar 25, 2022	1.3.0	UPDATE - Ensure that Dataproc Cluster is encrypted using Customer-Managed Encryption Key - assessment status and syntax changes (Ticket 15187)
Mar 31, 2022	1.3.0	UPDATE - Ensure That Instances Are Not Configured To Use the Default Service Account - GUI changes to audit and remediation/audit CLI change (Ticket 15269)
Mar 31, 2022	1.3.0	UPDATE - Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs - GUI and Audit CLI changes (Ticket 15270)
Mar 31, 2022	1.3.0	UPDATE - Ensure Compute Instances Are Launched With Shielded VM Enabled - GUI and audit CLI changes (Ticket 15271)
Mar 31, 2022	1.3.0	UPDATE - Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible - Assessment Status, Audit and Remediation Steps Changed (Ticket 15242)
Mar 31, 2022	1.3.0	UPDATE - Ensure That a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets - Audit Procedure and Assessment Status Change (Ticket 15241)
Mar 31, 2022	1.3.0	UPDATE - Ensure That All BigQuery Tables Are Encrypted With Customer-Managed Encryption Key (CMEK) - GUI change in audit (Ticket 15273)
Mar 31, 2022	1.3.0	UPDATE - Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible - update Command Line Audit Procedure Step 2 (Ticket 15218)
Mar 31, 2022	1.3.0	UPDATE - Ensure API Keys Are Restricted To Use by Only Specified Hosts and Apps - update Console Remediation Procedure step 3 (Ticket 15219)
Apr 10, 2020	1.2.0	ADD - Ensure 'skip_show_database' database flag for Cloud SQL Mysql instance is set to 'on' (Ticket 10215)
Mar 16, 2021	1.2.0	ADD - Ensure 'log_parser_stats' database flag for Cloud SQL PostgreSQL instance is set to 'off' (Ticket 10117)

Mar 16, 2021	1.2.0	ADD - Ensure 'log_planner_stats' database flag for Cloud SQL PostgreSQL instance is set to 'off' (Ticket 10118)
Mar 16, 2021	1.2.0	ADD - Ensure 'log executor stats' database flag for Cloud SQL
,		PostgreSQL instance is set to 'off' (Ticket 10119)
Mar 16, 2021	1.2.0	ADD - Ensure 'log_statement_stats' database flag for Cloud SQL
		PostgreSQL instance is set to 'off' (Ticket 10120)
Mar 16, 2021	1.2.0	ADD - Ensure 'log_min_error_statement' database flag for Cloud SQL
		PostgreSQL instance is set to 'Error' or stricter (Ticket 10122)
Apr 13, 2021	1.2.0	ADD - Ensure 'log_error_verbosity' database flag for Cloud SQL
		PostgreSQL instance is set to 'DEFAULT' or stricter (Ticket 10110)
Apr 13, 2021	1.2.0	ADD - Ensure 'log_statement' database flag for Cloud SQL
		PostgreSQL instance is set to 'ddl' or stricter (Ticket 10115)
Apr 13, 2021	1.2.0	ADD - Ensure 'log_hostname' database flag for Cloud SQL
		PostgreSQL instance is set to 'off' (Ticket 10116)
Apr 13, 2021	1.2.0	ADD- Ensure 'external scripts enabled' database flag for Cloud SQL
		SQL Server instance is set to 'off' (Ticket 10217)
Apr 13, 2021	1.2.0	ADD - Ensure 'user connections' database flag for Cloud SQL SQL
		Server instance is set as appropriate (Ticket 10219)
Apr 13, 2021	1.2.0	ADD - Ensure 'user options' database flag for Cloud SQL SQL Server
		instance is not configured (Ticket 10220)
Apr 13, 2021	1.2.0	ADD - Ensure 'remote access' database flag for Cloud SQL SQL
		Server instance is set to 'off' (Ticket 10222)
Apr 13, 2021	1.2.0	ADD - Ensure '3625 (trace flag)' database flag for Cloud SQL SQL
		Server instance is set to 'off' (Ticket 10223)
Apr 14, 2021	1.2.0	UPDATE - Ensure that the 'log_min_messages' database flag for
		Cloud SQL PostgreSQL instance is set appropriately - Title and
		Guideline content are not matching (Ticket 11145)
Apr 19, 2021	1.2.0	ADD - Ensure Firewall Rules for instances behind IAP only allow the
		traffic from GCLB Health Check and Proxy Addresses (Ticket 9464)

Apr 19, 2021	1.2.0	ADD - Ensure that all BigQuery Tables are encrypted with Customer-managed encryption key (CMEK) (Ticket 9975)
Apr 19, 2021	1.2.0	UPDATE - Ensure that the Cloud SQL database instance requires all incoming connections to use SSL - include SQL Server 2017 (Ticket 11885)
Apr 19, 2021	1.2.0	ADD - Ensure that a Default Customer-managed encryption key (CMEK) is specified for all BigQuery Data Setss (Ticket 9974)
Apr 19, 2021	1.2.0	ADD - Ensure 'log_duration' database flag for Cloud SQL PostgreSQL instance is set to 'on' (Ticket 10113)
Apr 19, 2021	1.2.0	UPDATE - Ensure that VPC Flow Logs is enabled for every subnet in a VPC Network - VPC Flow Logs not supported for internal HTTPS LB subnets (Ticket 12553)
Apr 29, 2021	1.2.0	Modify - Ensure 'log_hostname' database flag for Cloud SQL PostgreSQL instance is set appropriately - Sync with Postgresql 9.5 benchmark v1.1.0 (Ticket 10413)
Apr 29, 2021	1.2.0	UPDATE - Multiple in Logging section - log metric filters use the protoPayload fields (Ticket 12325)
Apr 30, 2021	1.2.0	UPDATE - Ensure 'log_statement' database flag for Cloud SQL PostgreSQL instance is set to 'ddl' or stricter - Align with PostgreSQL 9.5 Benchmark v1.1.0 (Ticket 10412)
Apr 30, 2021	1.2.0	UPDATE - Multiple Recommendations - Update menu references for Logging\Metrics; remove references to Stackdriver Account (Ticket 12755)
Apr 30, 2021	1.2.0	ADD - Ensure that Cloud DNS logging is enabled for all VPC networks (Ticket 12493)
Mar 3, 2020	1.1.0	ADD - Ensure 'log_checkpoints' database flag for Cloud SQL PostgreSQL instance is set to 'on'
Feb 26, 2020	1.1.0	UPDATE - Ensure "Block Project-wide SSH keys" enabled for VM instances - Small command typo: instacnces -> instances (Ticket 6956)

Feb 26, 2020	1.1.0	UPDATE - Ensure that Service Account has no Admin privileges - The suggested Audit Procedure steps for 1.4 exclude "*admin" roles. (Ticket 6955)
Feb 26, 2020	1.1.0	UPDATE - Ensure that there are only GCP-managed service account keys for each service account - Remediation Procedure Typo (Ticket 6974)
Feb 26, 2020	1.1.0	UPDATE- Ensure that Separation of duties is enforced while assigning KMS related roles to users - Rationale Statement Typo (Ticket 7001)
Feb 26, 2020	1.1.0	UPDATE - Ensure that there are only GCP-managed service account keys for each service account - Add Audit steps (Ticket 9833)
Feb 26, 2020	1.1.0	ADD - Ensure Cloud SQL Instances do not have public IP addresses (Ticket 9233)
Feb 26, 2020	1.1.0	ADD - Ensure that Cloud SQL database instances are configured with automated backups (Ticket 10018)
Feb 26, 2020	1.1.0	Update - Ensure that IP forwarding is not enabled on Instances - limit the scope of virtual machines this recommendation is applicable on (Ticket 10089)
Feb 26, 2020	1.1.0	UPDATE - Ensure that the default network does not exist in a project - add an explain of the default network to the rationale statement (Ticket 10082)
Feb 26, 2020	1.1.0	UPDATE - Ensure API keys are rotated every 90 days - Change to Unscored (Ticket 9972)
Feb 26, 2020	1.1.0	UPDATE - Ensure that SSH access is restricted from the internet - Adding Protocol TCP (Ticket 9807)
Feb 26, 2020	1.1.0	UPDATE - Ensure "Block Project-wide SSH keys" enabled for VM instances - limit the scope of virtual machines this recommendation is applicable on (Ticket 10084)
Feb 26, 2020	1.1.0	Update - Ensure that instances are not configured to use the default service account with full access to all Cloud APIs - limit the scope of

		virtual machines this recommendation is applicable on (Ticket 10085)
Feb 26, 2020	1.1.0	ADD - Ensure 'log_min_messages' database flag for Cloud SQL PostgreSQL instance is set appropriately (Ticket 10121)
Feb 26, 2020	1.1.0	ADD - Ensure that instances are not configured to use the default service account (Ticket 10108)
Feb 26, 2020	1.1.0	ADD - Ensure 'log_temp_files' database flag for Cloud SQL PostgreSQL instance is set to '0' (on) (Ticket 10123)
Feb 26, 2020	1.1.0	ADD - Ensure 'log_min_duration_statement' database flag for Cloud SQL PostgreSQL instance is set to '-1' (disabled) (Ticket 10124)
Feb 26, 2020	1.1.0	ADD - Ensure 'local_infile' database flag for Cloud SQL Mysql instance is set to 'off' (Ticket 10216)
Feb 26, 2020	1.1.0	ADD - Ensure 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off' (Ticket 10218)
Feb 26, 2020	1.1.0	ADD - Ensure 'contained database authentication' database flag for Cloud SQL SQL Server instance is set to 'off' (Ticket 10224)
Feb 20, 2020	1.1.0	ADD - Ensure Appengine Applications are exposed via TLS (Ticket 9447)
Feb 19, 2020	1.1.0	ADD - Ensure 'log_connections' database flag for Cloud SQL PostgreSQL instance is set to 'on' (Ticket 10111)
Feb 19, 2020	1.1.0	ADD - Ensure 'log_disconnections' database flag for Cloud SQL PostgreSQL instance is set to 'on' (Ticket 10112)
Feb 19, 2020	1.1.0	ADD - Ensure 'log_lock_waits' database flag for Cloud SQL PostgreSQL instance is set to 'on' (Ticket 10114)
Feb 16, 2020	1.1.0	ADD - Ensure that BigQuery datasets are not anonymously or publicly accessible (Ticket 9449)
Feb 16, 2020	1.1.0	ADD - Ensure that Cloud KMS cryptokeys are not anonymously or publicly accessible (Ticket 10081)
Feb 16, 2020	1.1.0	ADD - Ensure Compute instances are launched with Shielded VM enabled (Ticket 9446)
--------------	-------	---
Feb 16, 2020	1.1.0	ADD - Ensure that Compute instances do not have public IP addresses (Ticket 9823)
Feb 16, 2020	1.1.0	ADD - Ensure HTTPS and SSL proxy load balancers do not permit SSL policies with weak cipher suites (Ticket 9450)
Feb 10, 2020	1.1.0	UPDATE - Ensure the default network does not exist in a project - provide specific remediation instructions (Ticket 8358)
Feb 7, 2020	1.1.0	UPDATE - Ensure that corporate login credentials are used - Fix references (Ticket 9971)
Feb 6, 2020	1.1.0	UPDATE - Ensure legacy networks does not exists for a project - Change reference URLs (Ticket 10091)
Feb 6, 2020	1.1.0	UPDATE - Ensure that multi-factor authentication is enabled for all non-service accounts - add reference URL (Ticket 9973)
Feb 3, 2020	1.1.0	UPDATE - Ensure log metric filter and alerts exists for Project Ownership assignments/changes (Ticket 9514)
Feb 3, 2020	1.1.0	UPDATE- Ensure log metric filter and alerts exists for Audit Configuration Changes (Ticket 9515)
Feb 3, 2020	1.1.0	UPDATE - Ensure log metric filter and alerts exists for Custom Role changes (Ticket 9516)
Feb 3, 2020	1.1.0	UPDATE - Ensure log metric filter and alerts exists for VPC Network Firewall rule changes (Ticket 9517)
Feb 3, 2020	1.1.0	UPDATE - Ensure log metric filter and alerts exists for VPC network route changes (Ticket 9518)
Feb 3, 2020	1.1.0	UPDATE - Ensure log metric filter and alerts exists for VPC network changes (Ticket 9519)
Feb 3, 2020	1.1.0	UPDATE - Ensure log metric filter and alerts exists for Project Ownership assignments/changes - UI changes needed (Ticket 6960)

Feb 3, 2020	1.1.0	UPDATE - Multiple in section 2: 2.4-2.11 - Changes in Monitoring API and UI. Need update. (Ticket 8726)
Feb 2, 2020	1.1.0	DELETE - Ensure that MySQL Database Instance does not allows root login from any Host - suggest we remove this recommendation (Ticket 9410)
Feb 2, 2020	1.1.0	ADD - Ensure that Security Key enforcement is enabled for all admin accounts (Ticket 9444)
Feb 2, 2020	1.1.0	UPDATE - Ensure that corporate login credentials are used instead of Gmail accounts - change to include org-level IAM (Ticket 9442)
Feb 2, 2020	1.1.0	UPDATE - Ensure that ServiceAccount has no Admin privileges Ignore Apps Script service account (Ticket 9495)
Feb 2, 2020	1.1.0	UPDATE - Ensure the default network does not exist in a project Move to Level 2 profile (Ticket 9461)
Feb 2, 2020	1.1.0	ADD - Ensure that retention policies on log buckets are configured using Bucket Lock should replace object versioning (Ticket 9822)
Feb 2, 2020	1.1.0	ADD - Ensure that IAM users are not assigned Service Account Token Creator role at project level (Ticket 9445)
Feb 2, 2020	1.1.0	ADD - Ensure that Cloud Storage buckets have Bucket Policy Only enabled (Ticket 9448)
Feb 2, 2020	1.1.0	UPDATE - Ensure that sinks are configured for all Log entries - configure at organization or folder level (Ticket 9456)
Feb 2, 2020	1.1.0	DELETE - Ensure that object versioning is enabled on log-buckets (Ticket 9513)
Feb 2, 2020	1.1.0	UPDATE - Ensure that Cloud Audit Logging is configured properly across all services and all configure at folder or organization level (Ticket 9455)
Jan 28, 2020	1.1.0	DELETE - Ensure Private Google Access is enabled for all subnetwork in VPC Network - Following the recommendation doesn't make you more secure (Ticket 9462)

Jan 28, 2020	1.1.0	DELETE - Ensure that logging is enabled for Cloud storage buckets - redundant given CIS Benchmark 2.1 (Ticket 9486)
Jan 15, 2020	1.1.0	REMOVE - Ensure Stackdriver Logging is set to Enabled on Kubernetes Engine Clusters (Ticket 9465)
Jan 15, 2020	1.1.0	DELETE - Kubernetes Engine Section (Ticket 9824)
Jan 15, 2020	1.1.0	UPDATE - Ensure that sinks are configured for all Log entries - Grammatical Findings (Ticket 6984)
Jan 15, 2020	1.1.0	UPDATE - Ensure Encryption keys are rotated within a period of 365 days - Audit and Remediation Procedure Update (Ticket 7036)
Jan 15, 2020	1.1.0	UPDATE - Ensure that object versioning is enabled on log-buckets - update Description, Impact statement and Remediation (Ticket 7040)
Jan 15, 2020	1.1.0	UPDATE - Ensure that RSASHA1 is not used for key-signing key in Cloud DNS DNSSEC - Remediation CLI broken (Ticket 7073)
Jan 15, 2020	1.1.0	UPDATE - Ensure that RSASHA1 is not used for zone-signing key in Cloud DNS DNSSEC - Audit CLI update (Ticket 7075)
Jan 15, 2020	1.1.0	UPDATE - Ensure that RSASHA1 is not used for zone-signing key in Cloud DNS DNSSEC - Remediation CLI broken (Ticket 7074)
Jan 8, 2020	1.1.0	UPDATE - Ensure log metric filter and alerts exists for Audit Configuration Changes - Typo (AWS API calls) (Ticket 9668)
Feb 4, 2019	1.1.0	UPDATE - Ensure that RSASHA1 is not used for key-signing key - update audit CLI (Ticket 7072)
Sep 5, 2018	1.0.0	Document created