# 

**CSWG- Policy As Code Documentation**

Logging and Monitoring Sentinel Policies

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

***Sentinel Policy Name:***

* + 2.1 Ensure That Cloud Audit Logging Is Configured Properly Across All Services and All Users From a Project

***Category:***

* + Logging and Monitoring

***Description of Policy:***

* + As per CIS benchmarks, It is recommended that Cloud Audit Logging is configured to track all admin activities and read, write access to user data.

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.
  + Data read: Records operations that read user-provided data.
  + Data write: Records operations that write user-provided data

***Sentinel Policy Restriction:***

* + we are checking to ensure that DATA\_READ, DATA\_WRITE, and ADMIN\_READ audit logs are properly defined within the resource **'google\_project\_iam\_audit\_config'** , **'google\_folder\_iam\_audit\_config'**, **'google\_organization\_iam\_audit\_config'** .
  + DATA\_READ, DATA\_WRITE, and ADMIN\_READ should be enabled for all services for at the Organization- level, project- level and the folder- level.
  + This policy will ensure the **'exempted\_members'** attribute is always empty for all of the affected resources to ensure that all Google Cloud users are subjected to this policy.
  + This will ensure that all of the Cloud Audit logs are collected and stored appropriately. This will promote accountability among all users.
  + DATA\_READ, DATA\_WRITE, and ADMIN\_READ should be configured for ALL services across the organization to ensure that the required audit logs are produced. This will promote accountability among all users from a Cyber Security and Networking standpoint.

***Terraform attributes:***

Provider Ref: [google\_project\_iam | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/google_project_iam#google_project_iam_audit_config)

Attributes affected

* + log\_type
  + Exempted\_members
  + service

***Test cases:***

**Pass cases**

NOTE: In order for a pass to occur, **all** of the requirements **must** be fulfilled:

* + For all **'iam\_audit\_config'** resources, the **'log\_type'** attribute is defined for DATA\_READ, DATA\_WRITE, and ADMIN\_READ per the CIS recommendation.
  + For all **'iam\_audit\_config'** resources, the **'exempted\_members'** attribute is not defined.
  + For all **'iam\_audit\_config'** resources, the 'service' attribute is set to **'allServices'**

"audit log_config" : 
"exempted members" : 
"log_type" : 
"exempted members" : 
"log_type" : 
"exempted members" : 
"log_type" : 
"folder" : 
"folders/{folder id}", 
"service": "allservices" , 
"ADMIN READ" , 
"DATA READ", 
"DATA WRITE", 

**Fail case:**

NOTE: If only one, two, or none of the "Pass Cases" are present, policy will consistently result in a fail. The following are some examples of fail cases:

* + For 'google\_project\_iam\_audit\_config', the 'log\_type is set to something other than DATA\_READ, DATA\_WRITE, ADMIN\_READ

"audit log_config" : 
"exempted members" : 
"log_type" : 
"exempted members" : 
"log_type" : 
"exempted members" : 
"log_type" : 
"folder" : 
"folders/{folder id}", 
"service": "allservices" , 
"null", 
"null", 
"null", 

* + For **iam\_audit\_config'** resources, the 'service' attribute is set to something other than "allServices"

"'audit log config": 
"'service": "Services" , 
{l 
"'folder" : 
"exempted members 
" log_type" : 
"exempted members 
" log_type" : 
"exempted members 
" log_type" : 
"folders/{folder id}", 
"null", 
"null", 
"null", 

* 1. For iam\_audit\_config' resources, the 'log\_type' attribute has DATA\_READ defined (not DATA\_WRITE or ADMIN\_READ)

"'audit log config": 
"exempted members 
" log_type" : 
"exempted members 
" log_type" : 
"exempted members 
" log_type" : 
"'folder" : 
"folders/{folder id}", 
"'service": "allservices" , 
"DATA READ", 
"null", 
"null", 

**Testcases Output:**

PASS - test\C10ud-Audit-Logging_p01icy\fai1.hc1 
trace : 
Cloud -Audit- Logging_policy. sentinel : 146 : 2 
- Rule 
Value : 
false 
Cloud-Audit-Logging_p01icy. sentinel : 58:1 - 
Rule 
Value : 
false 
PASS - test\C10ud-Audit-Logging_p01icy\pass.hc1 
trace : 
Cloud -Audit- Logging_policy. sentinel : 146 
Value : 
true 
Cloud -Audit- Logging_policy. sentinel : 186 
Value : 
true 
Cloud -Audit- Logging_policy. sentinel : 116 
Value : 
true 
Cloud -Audit- Logging_policy. sentinel : 126 
Value : 
true 
Cloud -Audit- Logging_policy. sentinel : 136 
Value : 
true 
Cloud-Audit-Logging_p01icy. sentinel: 58 1 
Value : 
true 
- Rule 
- Rule 
- Rule 
- Rule 
- Rule 
- Rule 
"main" 
"folder iam value 1" 
"main" 
"folder iam value 1" 

Cloud -Audit- Logging_policy. sentinel : 68 
Value : 
true 
Cloud -Audit- Logging_policy. sentinel : 78 
Value : 
true 
Cloud -Audit- Logging_policy. sentinel : 88 
Value : 
true 
Cloud -Audit- Logging_policy. sentinel : le 
Value : 
true 
Cloud -Audit- Logging_policy. sentinel : 2e 
Value : 
true 
Cloud -Audit- Logging_policy. sentinel : 3e 
Value : 
true 
Cloud -Audit- Logging_policy. sentinel : 4e 
Value : 
true 
- Rule 
- Rule 
- Rule 
- Rule 
- Rule 
- Rule 
- Rule 
"folder iam value 2" 
"folder iam value 3" 
"folder iam value 4" 

2.2 Ensure That Sinks Are Configured for All Log Entries

***Sentinel Policy Name:***

* + 2.2 Ensure That Sinks Are Configured for All Log Entries

***Category:***

* + Logging and Monitoring

***Description of Policy:***

* + 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).

***Sentinel Policy Restriction:***

* + For Sinks at the folder, project, and organization level, the policy will ensure that the 'filter' attribute is empty (null) to ensure that ALL logs are collected at every level (project, folder and organization)
  + For Sinks at the folder, project, and organization level, the policy will ensure that the a 'destination' attribute is present

***Terraform attributes:***

* + - Provider Ref: [google\_logging\_project\_sink | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/logging_project_sink)
    - [google\_logging\_folder\_sink | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/logging_folder_sink)
    - [google\_logging\_organization\_sink | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/logging_organization_sink)

***Test cases:***

**Pass cases**

* + For all 3 'google\_logging' resources ensure that 'filter = null' and that a 'destination' attribute is present

"after": 
children": false, 
"description" : 
"destination" : 
"disabled": 
"exclusions": 
"filter" : 
"folder" 
"include 
"name" : 
"some explanation on what this is", 
"Storage.googleapis.com/storage-I", 
null, 
o, 
null, 
"storage-folder-I", 
"my-folder-sink", 

**Fail case:**

* + For all 3 'google\_logging' resources ensure that 'filter' is something other than 'null'

"after" : 
"description" : 
"destination" : 
"di sabled"; 
"exclusions": 
"include children": 
"org_id"• 
"some explanation on what this is", 
" storage.googleapis.com", 
null, 
o, 
"resource . type 
false, 
"my-sink" , 
"123as67E9" , 
gce instance AND severity WARNING", 

**Testcases Output:**

PASS - 
PASS - hc1 
logs: 
Ramve all filters fran the Sink configuration. This will allæ the Sink to aggreate all logs in one location to prepare f 
or export to SIEM. the •destination • mild contain •projects/ • at the start of the path, this indicates the sink is at the proj 
ect- level 
Ramve all filters fran the Sink configuration. This will allcn the Sink to aggreate all logs in one location. It is easie 
r to exc»rt logs to a SIEN (Security Information and Event this way. 
- Rule "main 
- Rule "maln 
trace: 
Terraform-Sinks configured for all log_entriesmicy.sentinel :56:1 
Value: 
false 
Terraform-Sinks configured for all . sentinel : 34: 1 
Value: 
false 
Terraform-Sinks configured for all . sentinel : 23:1 
Value : 
false 
PASS - 
trace : 
Terraform-Sinks configured for all . sentinel :56:1 
Value: 
Terraform-Sinks configured for all :34:1 
Value : 
Terraform-Sinks configured for all . sentinel :23:1 
Value: 
- Rule 
- Rule 
- Rule 
- Rule 
"folder 
" project_si og_aggregation" 
"folder sinks_for log_aggregation" 
"project_sinks_for log_aggregation" 

2.3 Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket lock

***Sentinel Policy Name:***

* + 2.3 Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket

***Category:***

* + Google Cloud Platform

***Description of Policy:***

* + CIS recommends enabling retention policies and a Bucket Lock on all storage buckets used as log sinks. This allows for logs to permanently exist in case if a threat actor attempts to destroy/reduce activity logs.

***Sentinel Policy Restriction:***

* + This policy will ensure the "is\_locked" value under "retention\_policy" for the google\_storage\_bucket resource is set to: ***true***
  + This policy will ensure the "retention\_period" value under "retention\_policy" for the google\_storage\_bucket resource is set to any value less than: ***2147483647*** (seconds)

***Terraform attributes:***

* + Provider Ref:
    1. <https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/storage_bucket>
  + Filter:
    1. google\_storage\_bucket: *retention\_policy >* is\_locked
    2. google\_storage\_bucket: retention\_policy > retention\_period

***Test cases:***

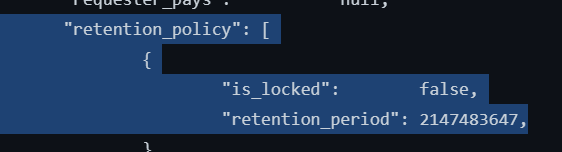
**Pass cases**

* + google\_storage\_bucket filters set to "is\_locked" set to true

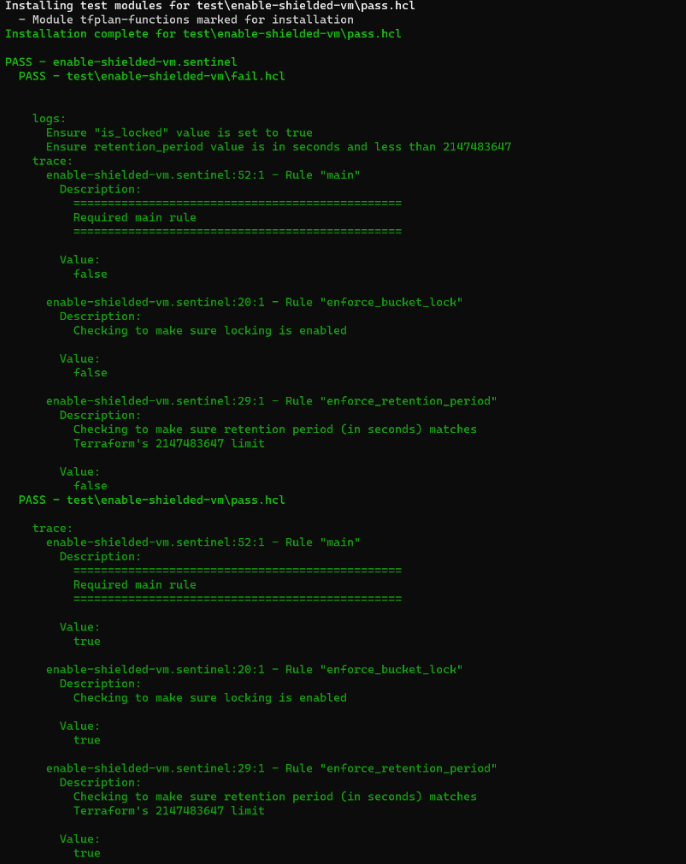
"retention_policy- : 
"is locked": 
true, 
"retention_period": 214748 
36, 

**Fail case:**

* + google\_storage\_bucket filters set to value not containing recommendation.



**Testcases Output:**



2.4 Ensure Log Metric/Alerts For Project Owners Changes

***Sentinel Policy Name:***

* + 2.4 Ensure Log Metric/Alerts For Project Owners Changes

***Category:***

* + Google Cloud Platform

***Description of Policy:***

* + It is recommended that a metric filter and alarm be established for unnecessary Owner role for users and service accounts.

***Sentinel Policy Restriction:***

* + This policy will ensure the "filter" value for the google\_logging\_metric resource is 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.role=\"roles/owner\")***

* + This policy will ensure the "filter" value for condition threshold in the google\_monitoring\_alert\_policy resource is set to: ***metric.type=\"logging.googleapis.com/user/<Log Metric Name>\" AND***

***resource.type=\"audited\_resource\"***

* 1. This policy will ensure the resource, google\_monitoring\_alert\_policy, has the enabled value set to *true.*

***Terraform attributes:***

NOTE: In Main.tf, Google logging metric resource must be run first, or an existing logging policy must exist in order for alert policy not to cause an error.

* + Provider Ref:
    1. [google\_logging\_metric | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/logging_metric)
    2. [google\_monitoring\_alert\_policy | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/monitoring_alert_policy)

* + Filter:
    1. google\_logging\_metric: *filter*
    2. google\_monitoring\_alert\_policy: *conditions > condition\_threshold > filter*

***Test cases:***

**Pass cases**

NOTE: In order for a pass to occur, all three requirements **must** be fulfilled:

* + google\_logging\_metric filter set to CIS recommendation.

"after" : 
"b ucket_option s 
"description" : 
"filter„ : 
"label ex 
AM) (Projectownership OR project(Nnerrnvitee) 

* + google\_monitoring\_alert\_policy condition threshold filter set to recommendation. For this filter, an exception is made for the values between "*metric.type=\"logging.googleapis.com/user/"* until "*AND resource.type=…"* since this is to be unique to each environment.

" aggregations " : 
"alignment _ period" : 
"cross series reducer": 
" denominator_aggregations 
"dencninator filter": 
"duration" : 
"filter- 
"threshold value": 
"ALIGN RATE", 
"C(WAR1scm GT", 
"metric.type=\"logging.googleapis.com/user/vpc/metric\ 
" AND 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to true.
  2. "di splay_name" : 
     "documentation" 
     "enabled" : 
     "my Alert policy for wc", 
     [1, 
     true, 

**Fail case:**

NOTE: If one, two, or none of the "Pass Cases" are present, policy will consistently result in a fail. The following are some examples of fail cases:

* 1. google\_logging\_metric filter set to value other than CIS recommendation.

after" : 
"bucket_options". 
"description " : 
i Iter-: 
"I abel extractors" 
AND OR project(hmerlnvitee) (p 
"mysql/metric" 

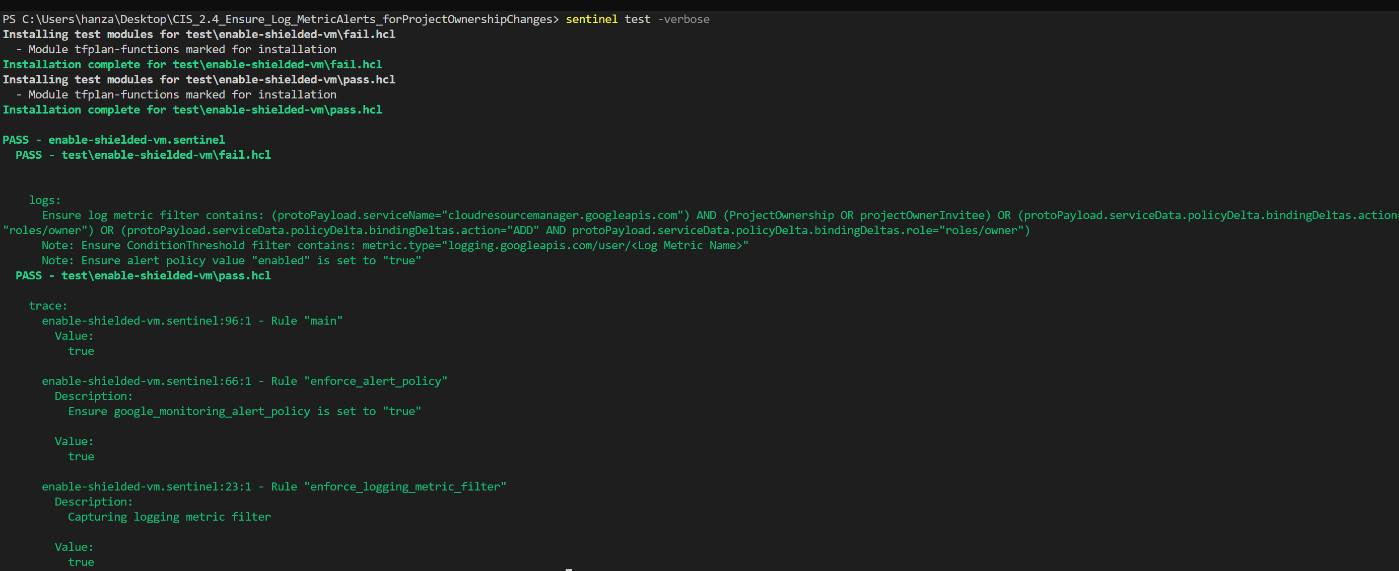
* 1. google\_monitoring\_alert\_policy condition threshold filter set to value other than recommendation.

"aggregations" : 
"comparison": 
"alignment_period" : 
"cross series 
"group_by_fields" : 
"per_series_aligner" : 
"ALIGN RATE", 
"denominator_aggregations" 
"denominator filter": 
"duration" : 
"C(WARISON GT" , 
c. type •N i . gooelpapis. user /vpc c \ " 
e, 
AND resource. 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to *false*.

"documentation" : 
"enabled" : 
false , 

**Testcases Output:**



2.5 Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes

***Sentinel Policy Name:***

* + 2.5 Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes

***Category:***

* + Google Cloud Platform

***Description of Policy:***

* + It is recommended that a metric filter and alarm be established for changes in how auditing is configured in the environment.

***Sentinel Policy Restriction:***

* + This policy will ensure the "filter" value for the google\_logging\_metric resource is set to:

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

* + This policy will ensure the "filter" value for condition threshold in the google\_monitoring\_alert\_policy resource is set to: ***metric.type=\"logging.googleapis.com/user/<Log Metric Name>\" AND***

***"resource.type=\"audited\_resource\"***

* 1. This policy will ensure the resource, google\_monitoring\_alert\_policy, has the enabled value set to *true.*

***Terraform attributes:***

NOTE: In Main.tf, Google logging metric resource must be run first, or an existing logging policy must exist in order for alert policy not to cause an error.

* + Provider Ref:
    1. [google\_logging\_metric | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/logging_metric)
    2. [google\_monitoring\_alert\_policy | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/monitoring_alert_policy)

* + Filter:
    1. google\_logging\_metric: *filter*
    2. google\_monitoring\_alert\_policy: *conditions > condition\_threshold > filter*

***Test cases:***

**Pass cases**

NOTE: In order for a pass to occur, all three requirements **must** be fulfilled:

* + google\_logging\_metric filter set to CIS recommendation.

" after" : 
"bucket_options . 
"description" : 
ffilter- : 
" protopayload. methodName— ampolicy\ " 
"mysql/metric" , 
"label extractors": 
protopayload. serviceData. policyDeIta. auditConfigDeItas : • 

* + google\_monitoring\_alert\_policy condition threshold filter set to recommendation. For this filter, an exception is made for the values between "*metric.type=\"logging.googleapis.com/user/"* until "*AND resource.type=…"* since this is to be unique to each environment.

"denominator_aggregations 
"denominator filter": 
"duration": 
"evaluation missing_data"• 
filter": 
"threshold value" 
"trigger" : 
[1, 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to true.

"di splay_name" : 
"documentation" 
"enabled" : 
"my Alert policy for wc", 
[1, 
true, 

**Fail case:**

NOTE: If one, two, or none of the "Pass Cases" are present, policy will consistently result in a fail. The following are some examples of fail cases:

* 1. google\_logging\_metric filter set to value other than CIS recommendation.

"bucket_options 
"description": 
"protopayload. ethodName— \ " set-nothi " 
"mysql/metric" , 
"label extractors": 
NO protopayload. : 

* 1. google\_monitoring\_alert\_policy condition threshold filter set to value other than recommendation.

"duration" : 
"evaluation missing_data": 
"threshold value": 
"trigger" . 
resource. , 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to *false*.

"documentation" : 
"enabled" : 
false , 

**Testcases Output:**

Wsers\nanza 
2 5 Ensure tor 
Installing test for 
- "'dule tfplan-functions marked for installation 
for 
- tfplan-functions marked for installation 
Installatim cmvlete for 
PASS - enable-shielded-w.sentinel 
PASS - 
Value; 
fal se 
enable-shielded-vm. sentinel - Rule 
Description : 
Capturing logging metric filter 
Value: 
false 
PASS - 
- Rule "main 
trace: 
enable-shielded-vm. sentinel 
Value: 
enable-shielded-vm. sentinel 
Description 
- Rule 
Ensure is set to "true" 
Value: 
true 
enable-shielded-vm. sentinel - Rule 
Description : 
Capturing logging metric filter 
Value; 

2.6 Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes

***Sentinel Policy Name:***

* + 2.6 Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes

***Category:***

* + Google Cloud Platform

***Description of Policy:***

* + 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.

***Sentinel Policy Restriction:***

* + This policy will ensure the "filter" value for the google\_logging\_metric resource is set to: ***resource.type=\"global\" AND protoPayload.methodName = \"google.iam.admin.v1.CreateRole\" OR protoPayload.methodName=\"google.iam.admin.v1.DeleteRole\" OR protoPayload.methodName=\"google.iam.admin.v1.UpdateRole\"***
  + This policy will ensure the "filter" value for condition threshold in the google\_monitoring\_alert\_policy resource is set to: ***metric.type=\"logging.googleapis.com/user/<Log Metric Name>\" AND resource.type=\"global\"***
  + This policy will ensure the resource, google\_monitoring\_alert\_policy, has the enabled value set to true.

***Terraform attributes:***

NOTE: In Main.tf, Google logging metric resource must be run first, or an existing logging policy must exist in order for alert policy not to cause an error.

* + Provider Ref:
    1. [google\_logging\_metric | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/logging_metric)
    2. [google\_monitoring\_alert\_policy | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/monitoring_alert_policy)

* + Filter:
    1. google\_logging\_metric: *filter*
    2. google\_monitoring\_alert\_policy: *conditions > condition\_threshold > filter*

***Test cases:***

**Pass cases**

NOTE: In order for a pass to occur, all three requirements **must** be fulfilled:

* + google\_logging\_metric filter set to CIS recommendation.

"values" : 
"bucket_options " 
"description" : 
"filter": 
-resource. " global \ " 
NO protopayload. methodName 

* + google\_monitoring\_alert\_policy condition threshold filter set to recommendation. For this filter, an exception is made for the values between "*metric.type=\"logging.googleapis.com/user/"* until "*AND resource.type=…"* since this is to be unique to each environment.

"filter": 
"threshold value": 
"trigger" : 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to true.

"di splay_name" : 
"documentation" 
"enabled" : 
"my Alert policy for wc", 
[1, 
true, 

**Fail case:**

NOTE: If one, two, or none of the "Pass Cases" are present, policy will consistently result in a fail. The following are some examples of fail cases:

* 1. google\_logging\_metric filter set to value other than CIS recommendation.

"after" : 
"bucket options" 
"description" 
"resource. APO protopayload. = 
"Tysql/metric" 
"label extractors": 
\ "google. VI. protoPayIoad.nethodNæ=VgoogIe. in. admin. 

* 1. google\_monitoring\_alert\_policy condition threshold filter set to value other than recommendation.

"duration" : 
"evaluation_mi s sing_data" : 
ilter": 
AM) resource. 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to *false*.

"documentation" : 
"enabled" : 
false , 

**Testcases Output:**

0 , 
010d0 

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

***Sentinel Policy Name:***

* + 2.7 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes

***Category:***

* + Google Cloud Platform

***Description of Policy:***

* + It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) Network Firewall rule changes to give a better insight in network changes.

***Sentinel Policy Restriction:***

* + This policy will ensure the "filter" value for the google\_logging\_metric resource is set to: ***resource.type=\"global\" AND protoPayload.methodName:\"compute.firewalls.patch\" OR protoPayload.methodName:\"compute.firewalls.insert\" OR protoPayload.methodName:\"compute.firewalls.delete\"***
  + This policy will ensure the "filter" value for condition threshold in the google\_monitoring\_alert\_policy resource is set to: ***metric.type=\"logging.googleapis.com/user/<Log Metric Name>\" AND resource.type=\"global\"***
  + This policy will ensure the resource, google\_monitoring\_alert\_policy, has the enabled value set to *true*.

***Terraform attributes:***

NOTE: In Main.tf, Google logging metric resource must be run first, or an existing logging policy must exist in order for alert policy not to cause an error.

* + Provider Ref:
    1. [google\_logging\_metric | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/logging_metric)
    2. [google\_monitoring\_alert\_policy | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/monitoring_alert_policy)

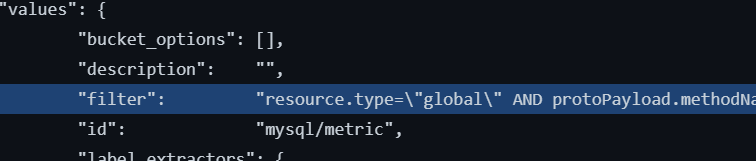
* + Filter:
    1. google\_logging\_metric: *filter*
    2. google\_monitoring\_alert\_policy: *conditions > condition\_threshold > filter*

***Test cases:***

**Pass cases**

NOTE: In order for a pass to occur, all three requirements **must** be fulfilled:

* + google\_logging\_metric filter set to CIS recommendation.



* + google\_monitoring\_alert\_policy condition threshold filter set to recommendation. For this filter, an exception is made for the values between "*metric.type=\"logging.googleapis.com/user/"* until "*AND resource.type=…"* since this is to be unique to each environment.

"duration" : 
"filter": 
"threshold value": 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to true.

"di splay_name" : 
"documentation" 
"enabled" : 
"my Alert policy for wc", 
[1, 
true, 

**Fail case:**

NOTE: If one, two, or none of the "Pass Cases" are present, policy will consistently result in a fail. The following are some examples of fail cases:

* 1. google\_logging\_metric filter set to value other than CIS recommendation.

" after" : 
"bucket options": [l 
"description" : 
"filter": 
"resource. AM) 

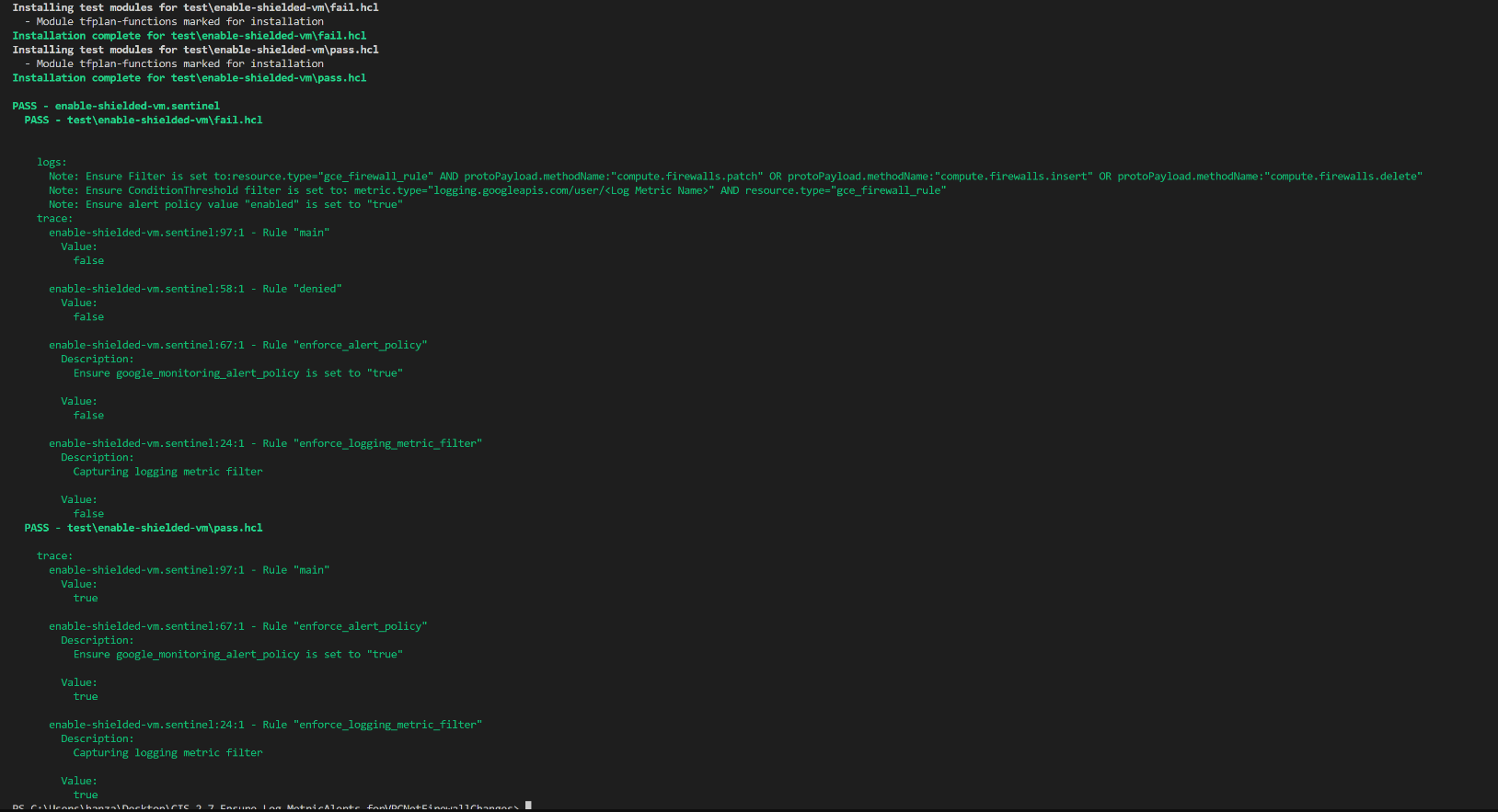
* 1. google\_monitoring\_alert\_policy condition threshold filter set to value other than recommendation.

"duration" : 
"evaluation missing_data" : 
"threshold value": 
- metric. type— iam.googleapis.com/user/vpc/metric\" 
resource. 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to *false*.

"documentation" : 
"enabled" : 
false , 

**Testcases Output:**



2.8 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes

***Sentinel Policy Name:***

* + 2.8 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes

***Category:***

* + Google Cloud Platform

***Description of Policy:***

* + It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network route changes to ensure expected traffic flow paths.

***Sentinel Policy Restriction:***

* + This policy will ensure the "filter" value for the google\_logging\_metric resource is set to: ***resource.type=\"gce\_route\" AND (protoPayload.methodName:\"compute.routes.delete\" OR protoPayload.methodName:\"compute.routes.insert\")***
  + This policy will ensure the "filter" value for condition threshold in the google\_monitoring\_alert\_policy resource contains: ***metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"***
  + This policy will ensure the resource, google\_monitoring\_alert\_policy, has the enabled value set to *true.*

***Terraform attributes:***

NOTE: In Main.tf, Google logging metric resource must be run first, or an existing logging policy must exist in order for alert policy not to cause an error.

* + Provider Ref:
    1. [google\_logging\_metric | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/logging_metric)
    2. [google\_monitoring\_alert\_policy | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/monitoring_alert_policy)

* + Filter:
    1. google\_logging\_metric: *filter*
    2. google\_monitoring\_alert\_policy: *conditions > condition\_threshold > filter*

***Test cases:***

**Pass cases**

NOTE: In order for a pass to occur, all three requirements **must** be fulfilled:

* + google\_logging\_metric filter set to CIS recommendation.

"after" : 
"bucket_options 
"description" : 
"filter" : 
" resource. type—N " gce_route \ " 
(metric", 
(R protrpayload. methodNa 

* + google\_monitoring\_alert\_policy condition threshold filter set to recommendation. For this filter, an exception is made for values after "*metric.type=\"logging.googleapis.com/user/"* since this is to be unique to each environment.

comparison" : 
"denominator_ageregations" : 
"denominator filter": 
"duration" : 
"eval uation_ni ssing_data" : 
"filter": 
"threshold value": 
"trigger". 
"cc.pARISON CT" , 
"metric. type• X" logging. googleapis. con/user/vpc/metric\" 
NO resource. 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to true.

"di splay_name" : 
"documentation" 
"enabled" : 
"my Alert policy for wc", 
[1, 
true, 

**Fail case:**

NOTE: If one, two, or none of the "Pass Cases" are present, policy will consistently result in a fail. The following are some examples of fail cases:

* 1. google\_logging\_metric filter set to value other than CIS recommendation.

" after• : 
"bucket_options . 
"description" : 
"filter 
APO protopayload.met 
"mysql/metric" , 
"label extractors": 

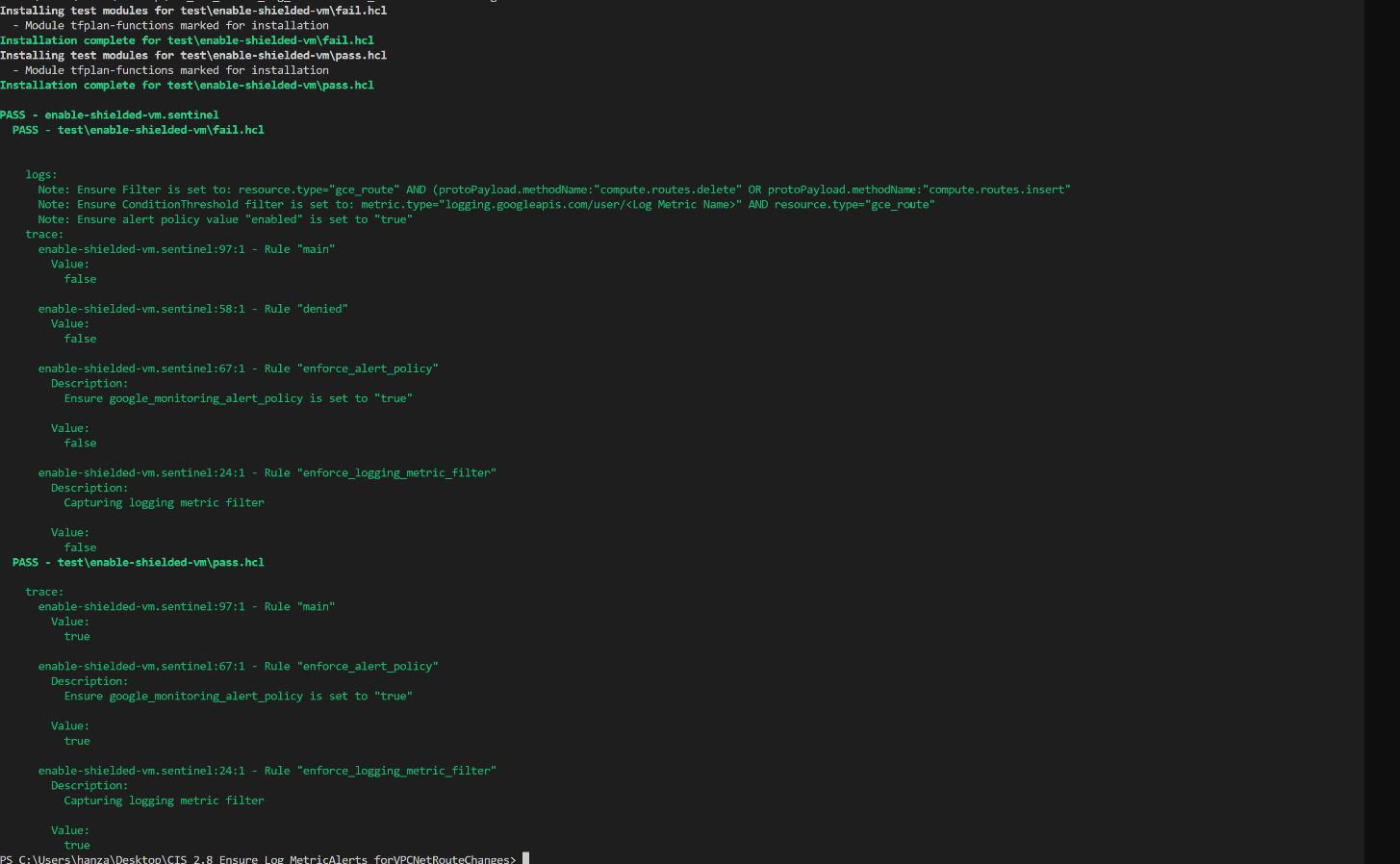
* 1. google\_monitoring\_alert\_policy condition threshold filter set to value other than recommendation.

"comparlson " : 
" dencmi n at or_aggreg at ion s 
"dencminator filter": 
"duration" : 
"filter": 
"threshold value": 
"CCWARISm GT", 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to *false*.

"documentation" : 
"enabled" : 
false , 

**Testcases Output:**



2.9 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes

***Sentinel Policy Name:***

* + 2.9 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes

***Category:***

* + Google Cloud Platform

***Description of Policy:***

* + It is recommended that a metric filter and alarm be established for VPC network changes to monitor traffic flow.

***Sentinel Policy Restriction:***

* + This policy will ensure the "filter" value for the google\_logging\_metric resource is set to: ***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\")***
  + This policy will ensure the "filter" value for condition threshold in the google\_monitoring\_alert\_policy resource is set to: ***metric.type=\"logging.googleapis.com/user/<Log Metric Name>\" AND resource.type=\"gce\_network\"***
  + This policy will ensure the resource, google\_monitoring\_alert\_policy, has the enabled value set to *true.*

***Terraform attributes:***

NOTE: In Main.tf, Google logging metric resource must be run first, or an existing logging policy must exist in order for alert policy not to cause an error.

* + Provider Ref:
    1. [google\_logging\_metric | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/logging_metric)
    2. [google\_monitoring\_alert\_policy | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/monitoring_alert_policy)

* + Filter:
    1. google\_logging\_metric: *filter*
    2. google\_monitoring\_alert\_policy: *conditions > condition\_threshold > filter*

***Test cases:***

**Pass cases**

NOTE: In order for a pass to occur, all three requirements **must** be fulfilled:

* + google\_logging\_metric filter set to CIS recommendation.

after" : 
"bucket_options" : [l 
"description" : 
"resource. AND (protopay10ad.æthodName: 
"mysql/metric" , 
"label_extractors" : { 
mass": "FXTR,WT -sonpa load.re 
protopayload .methodName 

* + google\_monitoring\_alert\_policy condition threshold filter set to recommendation. For this filter, an exception is made for the values between "*metric.type=\"logging.googleapis.com/user/"* until "*AND resource.type=…"* since this is to be unique to each environment.

" comparison" : 
"denominator_aggregations 
"denominator filter": 
"duration" : 
"evaluation_mi ssing_data" : 
"filter": 
"threshold value": 
"trigger" : 
"CC%'ARISON GT", 
" etric. type= X" logging. googleapis. ctn/user/vpc/metric\ 
n, 
" AM) resource. " 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to true.

"di splay_name" : 
"documentation" 
"enabled" : 
"my Alert policy for wc", 
[1, 
true, 

**Fail case:**

NOTE: If one, two, or none of the "Pass Cases" are present, policy will consistently result in a fail. The following are some examples of fail cases:

* 1. google\_logging\_metric filter set to value other than CIS recommendation.

"after" : 
"bucket_option s 
"description" • 
"fail. (protopayload insert\ 
"mysql/metric" , 
"label extractors": { 
" OR protopayload. •etho 

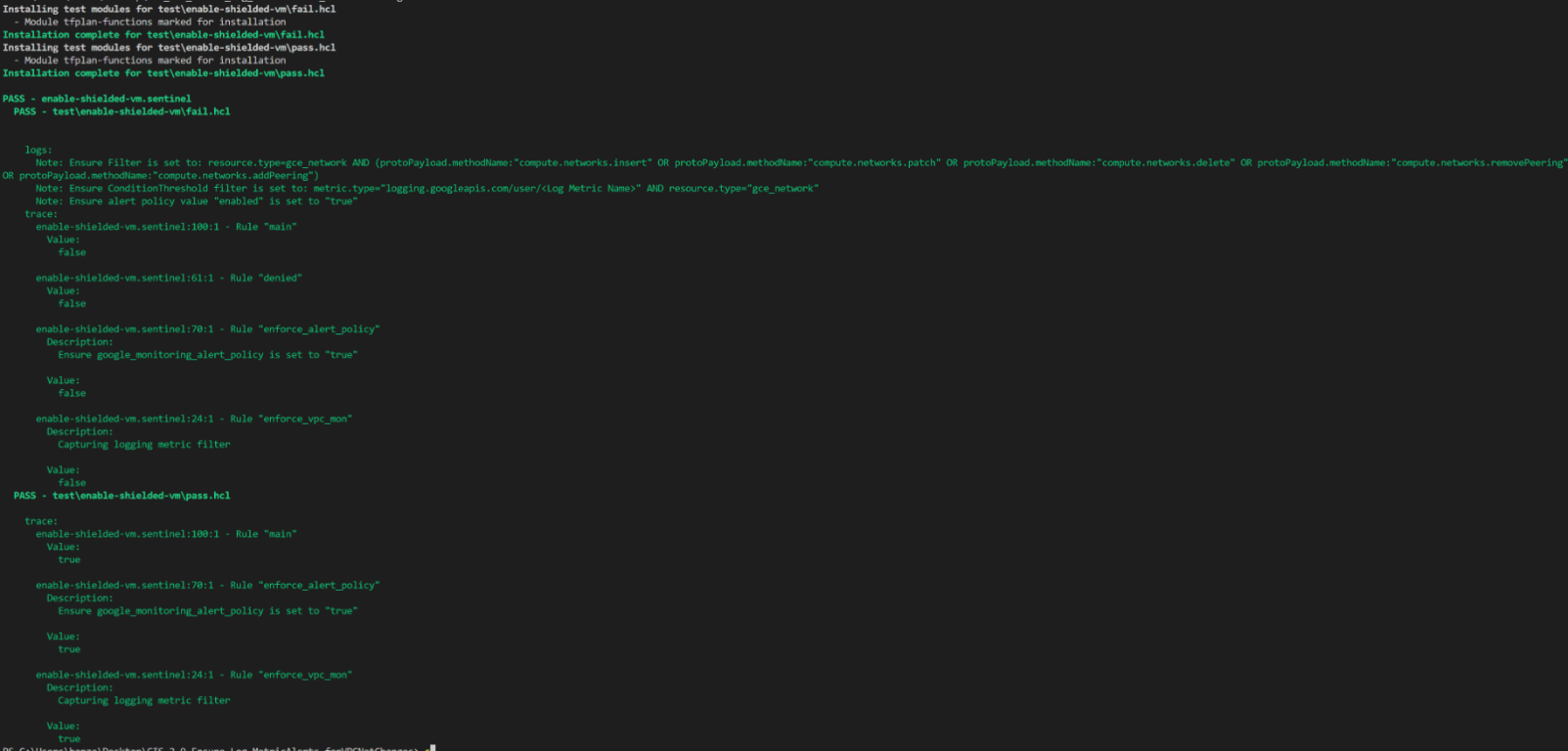
* 1. google\_monitoring\_alert\_policy condition threshold filter set to value other than recommendation.

"comparlson" : 
" dencmi n ator_aggre g at ion s 
"dencminator filter" : 
"duration" : 
"evaluation missing_data": 
"filter " : 
"threshold value": 
"trigger" : 
"CCWARISm GT", 
APO resource.type=\"cc—ute.googIeapis.com/VpcNeOwrk\"", 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to *false*.

"documentation" : 
"enabled" : 
false , 

**Testcases Output:**



2.10 Ensure That the Log Metric Filter and Alerts Exist for CloudStorage IAM Permission Changes

***Sentinel Policy Name:***

* + 2.10 Ensure That the Log Metric Filter and Alerts Exist for CloudStorage IAM Permission Changes

***Category:***

* + Google Cloud Platform

***Description of Policy:***

* + As per CIS benchmark ,It is recommended that a metric filter and alarm be established for Cloud Storage Bucket IAM changes.
  + 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.

***Sentinel Policy Restriction:***

* + This policy will ensure the "filter" value for the google\_logging\_metric resource is set to: ***resource.type=gcs\_bucket AND protoPayload.methodName=\"storage.setIamPermissions\"***
  + This policy will ensure the "filter" value for condition threshold in the google\_monitoring\_alert\_policy resource is set to: ***metric.type=\"logging.googleapis.com/user/<Log Metric Name>\" AND resource.type=\"gcs\_bucket\"***
  + This policy will ensure the resource, **google\_monitoring\_alert\_policy, has the enabled value set to *true.***

***Terraform attributes:***

NOTE: In Main.tf, Google logging metric resource must be run first, or an existing logging policy must exist in order for alert policy not to cause an error.

* + Provider Ref:
    1. [google\_logging\_metric | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/logging_metric)
    2. [google\_monitoring\_alert\_policy | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/monitoring_alert_policy)

* + Filter:
    1. google\_logging\_metric: *filter*
    2. google\_monitoring\_alert\_policy: *conditions > condition\_threshold > filter*

***Test cases:***

**Pass cases**

NOTE: In order for a pass to occur, all three requirements **must** be fulfilled:

* + google\_logging\_metric filter set to CIS recommendation.

"after" 
"bucket options" 
"description" : 
"filter" . 
"id": 
"resource.type=gcs bucket AND protopayload setlampermissions\"", 
"mysql/metric" 
"label extractors": 
"mass" : 
" EXTRACT (j sonpayload . request) " , 

* + google\_monitoring\_alert\_policy condition threshold filter set to recommendation. For this filter, an exception is made for the values between "*metric.type=\"logging.googleapis.com/user/"* until "*AND resource.type=\"gcs\_bucket\"* since this is to be unique to each environment.

"condition threshold": 
"aggregations" : 
"comparison" : 
"alignment_period " : 
"60s" 
"cross series reducer": null, 
"group_by fields": 
null, 
"per series aligner" . 
"ALIGN RATE", 
"denominator aggregations 
"denominator filter" : 
"duration" : 
"evaluation missing_data": 
"filter" : 
"threshold value": 
"trigger" : 
"COMPARISON GT" , 
null, 
"60s" 
null, 
"metric.type=\"logging.googleapis.com/user/gcsbucket/metric\" 
null, 
AND resource. bucket\"", 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to true.

"display _ name" : 
"documentation" : 
"enabled": 
"notification channels" : 
"timeouts " : 
"My Alert policy" 
[1, 
true , 
null, 
null, 

**Fail case:**

NOTE: If one, two, or none of the "Pass Cases" are present, policy will consistently result in a fail. The following are some examples of fail cases:

* 1. google\_logging\_metric filter set to value other than CIS recommendation.

"after" 
"bucket options" 
"description" : 
"filter" . 
"id": 
"resource.type=gcs bucket OR protopay10ad.methodName=\"storage.setIampermissions\"", 
"mysql/metric" 
"label extractors": 
"mass": "EXTRACT(j sonpayload . request)" , 

* 1. google\_monitoring\_alert\_policy condition threshold filter set to value other than recommendation.

"condition threshold": 
" aggregations" : 
"comparison" : 
"alignment_period " : 
"60s" 
"cross series reducer": null, 
"group_by fields": 
null, 
"per series aligner" . 
"ALIGN RATE", 
"denominator aggregations 
"denominator filter" : 
"duration" : 
"evaluation missing_data": 
"filter" : 
"threshold value": 
"trigger" : 
"COMPARISON GT" , 
null, 
"60s" 
null, 
"metric.type=\"iam.googleapis.com/user/gcsbucket/metric\" 
null, 
AND resource . bucket\"", 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to *false*.

"display _ name" : 
"documentation" : 
"enabled": 
"notification channels" : 
"timeouts " : 
"My Alert policy" 
[1, 
false, 
null, 
null, 

**Testcases Output:**

Installing test modules for 
Module tfplan-functions narked for installation 
Installatim cmplete for hcI 
Installing test modules for 
- Module tfplan-functions marked for installation 
Installatim for test\enable 
PASS - enable-shielded-m. sentinel 
PASS - 
logs: 
Note : 
Note : 
Note : 
trace : 
Ensure Filter is set to: 
Ensure ConditionThreshOId 
Ensure alert policy value 
"resource. type-gcs_bucket AM) protopay10ad.nethodName-"storage. setlarnpermissions" 
filter is set to; metric. con/ user/ (Log Metric Nano" 
"enabled" 
enable-shielded-vm. sentinel: lae: 
Val ue: 
fal se 
enable-shielded-vm. sentinel : 61 : I 
Val ue: 
fal se 
enable-shielded-vm. sentinel: 7B: I 
Des cription : 
Rule 
- Rule 
- Rule 
is set to "true" 
" nun 
"denied" 
"enforce alert_policy" 
Ensure is set to "true" 
Val ue: 
fal se 
enable-shielded-vm.sentineI:24:I - Rule 
Des cription : 
Capturing logging netric filter 
Val ue: 
fal se 
PASS - 
"enforce iam" 
"naun" 
enable-shielded-vm.sentinel - 
Val ue: 
enable-shielded-vm. sentinel: 7B:I - 
Description : 
Rule 
Rule 
Ensure is set to "true" 
Val ue: 
enable-shielded-vm. sentinel: 24:1 - Rule 
Description : 
Capturing logging netric filter 
Value: 
"enforce iam" 
PS C: 

2.11 Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes

***Sentinel Policy Name:***

* + 2.11 Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes

***Category:***

* + Google Cloud Platform

***Description of Policy:***

* + It is recommended that a metric filter and alarm be established for SQL Instance Configuration Changes
  + 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

***Sentinel Policy Restriction:***

* + This policy will ensure the "filter" value for the google\_logging\_metric resource is set to: ***protoPayload.methodName=\"cloudsql.instances.update\***
  + This policy will ensure the "filter" value for condition threshold in the google\_monitoring\_alert\_policy resource is set to: ***metric.type=\"logging.googleapis.com/user/<Log Metric Name>\" AND resource.type=\"cloudsql\_instance\_database\"***
  + This policy will ensure the resource, g**oogle\_monitoring\_alert\_policy, has the enabled value set to *true****.*

***Terraform attributes:***

NOTE: In Main.tf, Google logging metric resource must be run first, or an existing logging policy must exist in order for alert policy not to cause an error.

* + Provider Ref:
    - [google\_logging\_metric | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/logging_metric)
    - [google\_monitoring\_alert\_policy | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/monitoring_alert_policy)

* + Filter:
    - google\_logging\_metric: *filter*
    - google\_monitoring\_alert\_policy: *conditions > condition\_threshold > filter*

***Test cases:***

**Pass cases**

NOTE: In order for a pass to occur, all three requirements **must** be fulfilled:

* + google\_logging\_metric filter set to CIS recommendation.

"after" : 
"bucket options" 
"description" : 
"filter" : 
"id": 
"protopayload . methodName= \ "cloudsql . instances . update\" " , 
"mysql/metric" 

* + google\_monitoring\_alert\_policy condition threshold filter set to recommendation. For this filter, an exception is made for the values between "*metric.type=\"logging.googleapis.com/user/"* until "*AND resource.type=…"* since this is to be unique to each environment.

"condition threshold" : 
"aggregations" : 
"comparison" : 
"alignment_period " : 
"60s" 
"cross series reducer": null, 
"group_by fields": 
null, 
"per series aligner" . 
"ALIGN RATE", 
"denominator aggregations 
"denominator filter" : 
"duration" : 
"evaluation missing_data": 
"filter" : 
"COMPARISON GT" , 
null, 
"60s" 
null, 
"metric.type=\"logging.googleapis.com/user/mysql/metric\" 
AND resource . instance database\"", 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to true.

"display _ name" : 
"documentation" : 
"enabled": 
"notification channels" : 
"timeouts " : 
"My Alert policy" 
[1, 
true , 
null, 
null, 

**Fail case:**

NOTE: If one, two, or none of the "Pass Cases" are present, policy will consistently result in a fail. The following are some examples of fail cases:

* 1. google\_logging\_metric filter set to value other than CIS recommendation.

"after" : 
"bucket options" 
"description" : 
"filter" : 
"id": 
"protopayload . methodName=c10udsq1. database . update " 
"mysql/metric" 

* 1. google\_monitoring\_alert\_policy condition threshold filter set to value other than recommendation.

"condition threshold": 
" aggregations" : 
"comparison" : 
"alignment_period " : 
"60s" 
"cross series reducer": null, 
"group_by fields": 
null, 
"per series aligner" . 
"ALIGN RATE", 
"denominator aggregations 
"denominator filter" : 
"duration" : 
"evaluation missing_data": 
"filter" : 
"threshold value": 
"trigger" : 
"COMPARISON GT" , 
null, 
"60s" 
null, 
"metric.type=\"iam.googleapis.com/user/gcsbucket/metric\" 
null, 
AND resource . bucket\"", 

* 1. google\_monitoring\_alert\_policy with "enabled" value set to *false*.

"display _ name" : 
"documentation" : 
"enabled": 
"notification channels" : 
"timeouts " : 
"My Alert policy" 
[1, 
false, 
null, 
null, 

**Testcases Output:**

PS C: sentinel test 
Installing test "oduLes for 
— Module tfptan—functions marked for installation 
Installation complete for test \ _hcL 
Installing test modules for 
— Nodule tfptan—functions marked for installation 
Installation complete for .hct 
PASS — enable—shielded-w. sentinel 
— .hct 
PASS 
logs: 
—verbose 
Note: Ensure Filter is set to: protopayload. instances . update" 
Note: Ensure Condition Threshold filter is set to: metric. type:" logging . Metric Nane>" 
AND resource . 
trace: 
enable-shielded-vm .sentinet - 
Value: 
false 
enable-shielded-vm sentinel - 
Value: 
false 
. sentinel — 
Description: 
Rule 
Rule 
Rul e 
"main" 
"denied" 
n enforce _ alert_po licyn 
Ensure is set to "true " 
Value: 
true 
. sentinel : 23: I 
Rule 
Description: 
Capturing togging metric filter 
Value : 
false 
test\enabte-shietded-vm\pass . hct 
PASS - 
"enforce _sqtfilter" 
"main" 
trace: 
enable-shielded-vm .sentinet - 
Value: 
true 
enable-shielded-vm sentinel - 
Description: 
Rule 
Rule 
Ensure is set to "true n 
Value: 
true 
. sentinel - 
Rule 
Description: 
Capturing Logging metric filter 
Value: 
true 
"enforce_sqlfilter" 

2.12 Ensure That Cloud DNS Logging Is Enabled for All VPC Networks

***Sentinel Policy Name:***

* + 2.12 Ensure That Cloud DNS Logging Is Enabled for All VPC Networks

***Category:***

* + Google Cloud Platform

***Description of Policy:***

* + It is recommended that Cloud DNS logging is enabled for all VPC networks to assist in security monitoring and forensics.
  + 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 and evaluated against threat intelligence.

***Sentinel Policy Restriction:***

* + This policy will ensure the "service" value for the google\_project\_service resource contains: [***http://dns.googleapis.com/***](http://dns.googleapis.com/)as the DNS API is required for DNS logging.
  + This policy will ensure the "enable\_logging" value for the google\_dns\_policy resource is set to: *true*

***Terraform attributes:***

* + **Provider Ref**:
    1. [google\_project\_service | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/google_project_service)
    2. [google\_dns\_policy | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/dns_policy)
  + **Filter**:
    1. google\_project\_service: *service*
    2. google\_dns\_policy: *enable\_logging*

***Test cases:***

**Pass cases**

* + google\_project\_service with DNS service enabled.

" after 
"disable 
dependent services" : 
"disable 
on destroy": 
"project" : 
"servlce" : 
"timeouts" : 
null, 
true , 
"terraform-gcp-36252Ø" , 
" dns . googleapis . com" , 
null, 

* + google\_dns\_policy ensuring logging is enabled.

"description" . 
"enable inbound forwarding": true, 
"enable logging": 
"Managed by Terraform" , 
true , 
"example- policy", 
"name" : 
"networks" : 

**Fail case:**

* 1. google\_project\_service resource not containing a DNS logging service.

" after 
"disable 
dependent services" : 
"disable 
on destroy": 
"project" : 
"servlce" : 
"timeouts" : 
null, 
true , 
"terraform-gcp-36252Ø" , 
" lam. secure . com" 
null, 

* 1. google\_dns\_policy with enable logging as disabled.

"description" . 
"Managed by Terraform" , 
"enable inbound forwarding": true, 
"enable logging": 
false, 
"name" : 
"example- policy", 

**Testcases Output:**

Installing test modules for . hcl 
— Module tfplan—functions marked for installation 
Installation complete for 
Installing test modules for . hcl 
— Module tfptan—functions marked for installation 
Installation complete for test\enable—shielded—vm\pass.hcl 
PASS 
test \ . hcl 
PASS - 
logs: 
. "dns . googleapis . com" should be enabled to enforce VPC DNS logging . 
Note • 
Note . 
• "enable _ logging" should be enabled to enforce VPC DNS logging . 
trace : 
sentinel: 57: 1 — 
Value: 
false 
sentinel: 39: 1 — 
Value: 
false 
. sentinel : 17 : 1 
Value: 
false 
Rule 
Rule 
" main " 
"enabte_dnstogging " 
— Rule "enable_googleapis" 
. hcl 
PASS - 
trace : 
sentinel: 57: 1 — 
Rule "main" 
Value: 
true 
. sentinel : 17 : 1 
— Rule "enable_googleapis" 
Value: 
true 

2.13 Ensure Cloud Asset Inventory Is Enabled

***Sentinel Policy Name:***

* + 2.13 Ensure Cloud Asset Inventory Is Enabled

***Category:***

* + Google Cloud Platform

***Description of Policy:***

* + It is recommended that Cloud Asset Inventory is enabled to provide a time-series historical view of GCP resources and IAM policies.

***Sentinel Policy Restriction:***

* + This policy will ensure the "service" value for the google\_project\_service resource is set to: ***cloudasset.googleapis.com***

***Terraform attributes:***

* + Provider Ref:
    1. <https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/google_project_service>
  + Filter:
    1. google\_project\_service: *service*

***Test cases:***

**Pass cases**

* + google\_project\_service filter set to CIS recommendation.

"disable_dependent_services": null, 
"di sable_on_destroy" : 
true, 
"project": 
"terraform-gcp-36252ø" , 
"service- : 
"cloudasset. googleapis. c«, 
"timeouts" : 
null, 

**Fail case:**

* + google\_project\_service filter set to value not containing recommendation.

"project" : 
"timeouts": 
null, 
true, 
"terraform-gcp-36252ø" 
" lam. secure. 
null, 

**Testcases Output:**

Installing test modules for . hct 
— Module tfptan—functions marked for installation 
Installation complete for 
Installing test modules for . hcI 
— Module tfptan-functions marked for installation 
Installation complete for . hcl 
PASS - 
. sentinel 
PASS - 
. hcl 
trace : 
. sentinel : 23:1 — 
false 
. sentinel : 15:1 — 
Value: 
false 
PASS 
trace: 
enable-shielded-vm . sentinel : 23:1 — 
Value: 
true 
enable-shielded-vm . sentinel - 
Value: 
true 
Rule 
Rule 
Rule 
Rule 
"main" 
"violations" 
"main" 
"violations" 

2.15 Ensure 'Access Approval' is 'Enabled'

***Sentinel Policy Name:***

* + 2.15 Ensure 'Access Approval' is 'Enabled'

***Category:***

* + Google Cloud Platform

***Description of Policy:***

* + Access Approval allows an organization to select users to approve or disapprove Google support personnel access requests to projects. CIS recommends enabling Access Approval to provide explicit approval for such requests allowing better security for information access.

***Sentinel Policy Restriction:***

* + This policy will ensure the "cloud\_product" value under enrolled\_services for the google\_folder\_access\_approval\_settings resource is set to: ***all***

***Terraform attributes:***

* + Provider Ref:
    1. <https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/folder_access_approval_settings>
  + Filter:
    1. google\_folder\_access\_approval\_settings: *enrolled\_services > cloud\_product*

***Test cases:***

**Pass cases**

* + google\_folder\_access\_approval\_settings filter set to CIS recommendation.

"enrolled set".'ices": 
"cloud_product" ; 
"enrollment level": 
"gL(XK ALL", 

**Fail case:**

* + google\_folder\_access\_approval\_settings filter set to value not containing recommendation.

"enrolled services": [ 
" cloud_product" : 
"bigquery. googleapis. ccm 
"enrollment level": "BLOCK ALL", 

**Testcases Output:**

Installing test modules for . hct 
— Module tfplan—functions marked for installation 
Installation complete for .hcl 
Installing test modules for . hct 
— Module tfplan—functions marked for installation 
Installation complete for .hct 
. sentinel 
PASS - 
PASS — . hc1 
trace: 
. sentinel : 23 : 1 
— Rule 
Value: 
false 
: 15:1 — 
Value : 
false 
main " 
PASS — . hc1 
trace : 
Value : 
true 
: 15:1 - 
Value : 
true 
Rule 'Iviolations" 
Rule "main 
Rule "violations" 
PS C:\Users\hanza\Desktop\Enab1ing Access Approval using Terraform> 