# 

**CSWG- Policy As Code Documentation**

IAM Sentinel Policies

1.5 Ensure That Service Account Has No Admin Privileges

***Policy Name:***

* + 1.5 Ensure That Service Account Has No Admin Privileges.

***Description of Policy:***

* + Service accounts represent service-level security of the Resources (application or a VM) which can be determined by the roles assigned to it.
  + Enrolling Service Account with Admin rights gives full access to an assigned application or a VM.
  + A Service Account 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.

***Terraform Provider:***

<https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/google_project_iam> - resource block “google\_project\_iam\_member” or “google\_project\_iam\_binding” or “google\_project\_iam\_policy” is used.

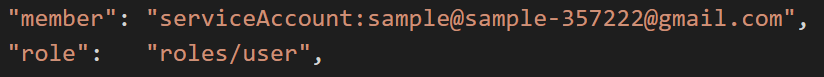
***Sentinel Policy Restriction:***

* + In this sentinel policy, a service account is not granted with the roles like Owner, Editor.

***Pass and fail cases of the above sentinel policy:***

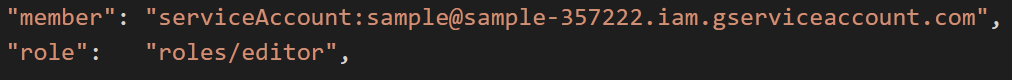
**Pass Case:**

1. Service account with roles like Owner, Editor are not granted.

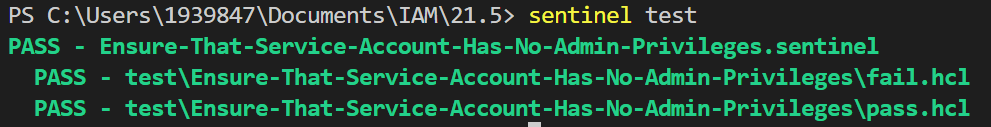


**Fail Case:**

1. Service account with roles like Owner, Editor is granted.



**Testcases Output:**



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

***Sentinel Policy Name:***

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

***Description of Policy:***

* + 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.

***Terraform Provider:***

<https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/google_project_iam> - resource block “google\_project\_iam\_member” or “google\_project\_iam\_binding” or “google\_project\_iam\_policy” is used.

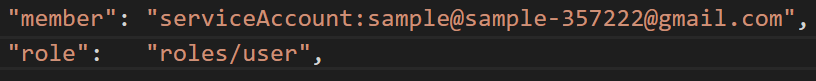
***Sentinel Policy Restriction:***

In this sentinel policy, IAM users should not be assigned the Service Account User or Service Account Token Creator roles at the project level.

***Pass and fail cases of the above sentinel policy:***

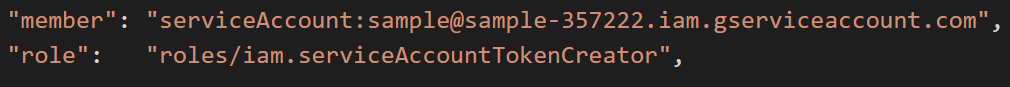
**Pass Case:**

1. IAM users should not be assigned the Service Account User or Service Account Token Creator roles at the project level.

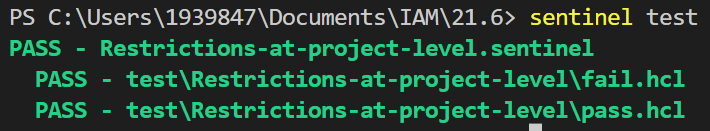


**Fail Case:**

1. IAM users should be assigned the Service Account User or Service Account Token Creator roles at the project level.



**Testcases Output:**



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

***Sentinel Policy Name:***

* + 1.7 Ensure User-Managed/External Keys for Service Accounts are Rotated Every 90 Days or Fewer

***Category :***

* + Identity and Access Management.

***Description of Policy:***

* + 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
  + In this policy, we are making sure that the service account key connected to the service account is rotated atleast every 90 days.

***Sentinel Policy Restriction:***

* + Sentinel will restrict service account key rotation anything more than 90 days.

***Terraform attributes:***

* + - Provider Ref:[google\_service\_account\_key | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/google_service_account_key)

***Test cases:***

**Pass cases**

1. In pass case, if "rotation\_days" is set to 90 and below then the pass case will always pass.

" rfc3339" : 
" rotation_days" : 
" rotation 
hours" : 
" rotation 
minutes" : 
" rotation 
months" : 
"2Ø22-Ø9-28T12 : 49 : 48?' , 
90, 
null, 
null, 
null, 

**Fail case:**

1. In pass case, if "rotation\_days" is set to 91 and above then the pass case will always fail.

" rotation_days" : 
" rotation 
hours" : 
" rotation 
minutes" : 
" rotation 
months" : 
løø 
null, 
null, 
null, 

**Testcases Output:**

o (base) 
ServiceAccountKey % sentinel test 
— service—account—key—rotation. sentinel 
PASS 
— . hc1 
PASS 
— test/service-account—key-rotation/pass. hcl 
PASS 
ServiceAccountKey % C] 
(base) 

1.9 Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible

***Sentinel Policy Name:***

* + 1.9 Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible

***Category :***

* + Google Cloud Platform

***Description of Policy:***

* + It is recommended that the IAM policy on Cloud KMS cryptokeys should restrict anonymous and/or public access. Granting permissions to allUsers or allAuthenticatedUsers allows anyone to access the dataset which increases risk of sensitive data exposure.

***Sentinel Policy Restriction:***

* + This policy will ensure the "members" value under the google\_kms\_crypto\_key\_iam\_binding resource is *NOT* set to: ***allAuthenticatedUsers*** and ***allUsers***
  + This policy will ensure the "member" value under the google\_kms\_crypto\_key\_iam\_member resource is NOT set to: ***allUsers***

***Terraform attributes:***

* + Provider Ref:
    1. <https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/google_kms_crypto_key_iam>
  + Filter:
    1. google\_kms\_crypto\_key\_iam\_binding: *members*
    2. google\_kms\_crypto\_key\_iam\_member: member

***Test cases:***

**Pass cases**

* + google\_kms\_crypto\_key\_iam\_binding filter set to CIS recommendation.

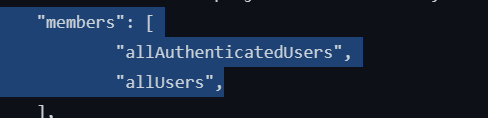
-proJects,' 
"member•s" : 
"group : Consulting" , 
"user:jane@outlook. 
Inaustr•l 

* + google\_kms\_crypto\_key\_iam\_member filter set to CIS recommendation.

"condition": 
c r y pto_key_ 
"member" : 
"role": 
[1, 
id": "projects/ industrious-eye-36261 
"rol I oudkms . cryptoKpyFncryp 

**Fail case:**

* 1. google\_kms\_crypto\_key\_iam\_binding filter not set to CIS recommendation.



* 1. google\_kms\_crypto\_key\_iam\_member filter not set to CIS recommendation.

"condition" : 
n, 
: "projects/indu• 
" all Users " 

**Testcases Output:**

In stat ing 
In stalling 
— Nodule 
test modules for 
t f plan—fun c 
test for 
t f ptan—fun c t ions 
marked for 
marked 
Installation complete for testiCIS_I.9 
9_AnonpubI . 
_Disabted\pass. hct 
installation 
_ Anon Public hct 
CIS_I . sentinel 
PASS - 
PASS - 
logs: 
Policy Violation: Resoun:e detected allAuthenticatedUsers and/or all Users 
Policy Violation: ResouH:e detected all AuthenticatedUsers and/or anusers 
trace: 
Value: 
false 
CIS_I _ — 
CIS_I _ L 
Value: 
PASS — 
trace; 
CIS_L. - 
Value; 
true 
Value: 
true 
sentinel - 
Rule 
Rule 
Rule 
Rule 
Rule 
" nun " 
"google_org_policy_gIObaI_enforc@mentl" 
" naun" 
Value: 
true 
Deskto 
c'. sue Not Pubs 

1.10 Ensure KMS Encryption Keys Are Rotated Within a Period of 90 Days

***Sentinel Policy Name:***

* + 1.10 Ensure KMS Encryption Keys Are Rotated Within a Period of 90 Days

***Category :***

* + Google Cloud Platform

***Description of Policy:***

* + Many people may have indefinite access to cryptographic keys. This poses a risk to the secure data. Therefore, CIS recommends to set a key rotation of 90 days or less.

***Sentinel Policy Restriction:***

* + This policy will ensure the "rotation\_period" value under all "google\_kms\_crypto" resources are set to anything less than: ***7776000*** (90 days in seconds)

***Terraform attributes:***

* + Provider Ref:
    1. <https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/google_kms_crypto_key_iam>
  + Filter:
    1. *rotation\_period*

***Test cases:***

**Pass cases**

* + In pass case, if google\_folder\_access\_approval\_settings filter set 90 days will always pass

"after" : 
"labels" : 
"purpose" : 
"rotation_period" : 
null, 
"crypto-key-exanvle" , 
"ENCRYPT DECRYPT" , 
"6776øøøs% 

**Fail case:**

* + In pass case, if google\_folder\_access\_approval\_settings filter set to more than 90 days will always fail.

"after" : 
"labels": 
"purpose" : 
" rotation_period- : 
"skip initial version 
null, 
"crypto-key -example" , 
"ENCRYPT DECRYPT" , 
creation": null, 

**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> 

1.12 Ensure API Keys Are Not Created for a Project

***Sentinel Policy Name:***

1.12 Ensure API Keys Are Not Created for a Project

***Category :***

* + Identity and Access Management.

***Description of Policy:***

* + 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.
  + 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.

***Sentinel Policy Restriction:***

* + The policy checks whether "**google\_apikeys\_key**" resource exists

***Terraform attributes:***

* + - [google\_apikeys\_key | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/apikeys_key)
    - Terraform resource: "google\_apikeys\_key"

***Test cases:***

**Pass case:**

1. In pass case, if "google\_apikeys\_key" resource is not included then the pass case will always pass.

No Screenshot of argument in mock file

**Fail case:**

1. In pass case, if "google\_apikeys\_key" resource is included then the pass case will always fail.

Screenshot of argument in mock file

resource_changes 
" google_apikeys_key. primary" : { 
"address" . 
" google_apikeys_key. primary" 
"change" • 
"actions" : 
create" 
" after 
"display _ name": "sample-key" , 
" key" 
name : 
"project" • 
"igneous-future-361414" 
restrictions" : 
"timeouts" : 
null, 
"after unknown" . 
'lid" : 
true, 
" key_s tri ng 
true , 
restrictions" : 
true, 
"uid" : 
"before" : 
null, 

**Testcases Output:**

Screenshot of test command successful

user@DESKTOP-GLNSQ3C:/mnt/e/ALL Wls/sentinel_hashicorp/policytesting$ sentinel test 
Installing test modules for test/ensure-apikeys-not-createdfor-project/fail . hcl 
module tfplan-functions marked for installation 
Installation complete for test/ensure-apikeys-not-createdfor-project/fail.hcl 
Installing test modules for test/ensure-apikeys-not-createdfor-project/pass . hcl 
module tfplan-functions marked for installation 
Installation complete for test/ensure-apikeys-not-createdfor-project/pass . hcl 
ensure - apikeys - not - createdfor - proj ect . sentinel 
PASS 
test/ ensure - apikeys - not - createdfor - proj ect/fail . hcl 
PASS 
logs : 
- run-ensure- api keys- not- createdfor- project 
- verbose 
As per policy, it is suggested to avoid using API keys due to security risk. 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 Google Cloud Translation API, but doesn't otherwise need a backend server, API keys are the simplest way to authenticate to the API. If a business requires API keys to be u 
sed, then the API keys should be secured properly. 
trace: 
ensure - apikeys - not - createdfor -project . sentinel : 13 : 1 
Value: 
false 
test/ ensure - apikeys - not - createdfor - proj ect/pass . hcl 
PASS 
trace: 
ensure - apikeys - not - createdfor -project . sentinel : 13 : 1 
Value: 
true 
Rule 
Rule 
"main" 
Activate Windows 
"main" 
Go to Settings to activate Windows. 

1.13 Ensure API Keys Are Restricted To Use by Only Specified Hosts and Apps

***Sentinel Policy Name:***

1.13 Ensure API Keys Are Restricted To Use by Only Specified Hosts and Apps

***Category :***

* + Identity and Access Management.

***Description of Policy:***

* + 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.
  + Application restrictions is to be set to any of HTTP referrers, IP addresses, Android apps, iOS apps.

***Sentinel Policy Restriction:***

* + The policy checks whether any of the blocks mentioned below under "restrictions" contains value
  + Also checks for "allowed\_referrers" attribute for "browser\_key\_restrictions" block does not contain any of the following : "\*","\*.[TLD]","\*.[TLD]/\*"
  + Also checks for "allowed\_ips" attribute for "server\_key\_restrictions" block does not any of the following : "0.0.0.0","0.0.0.0/0","::0"

***Terraform attributes:***

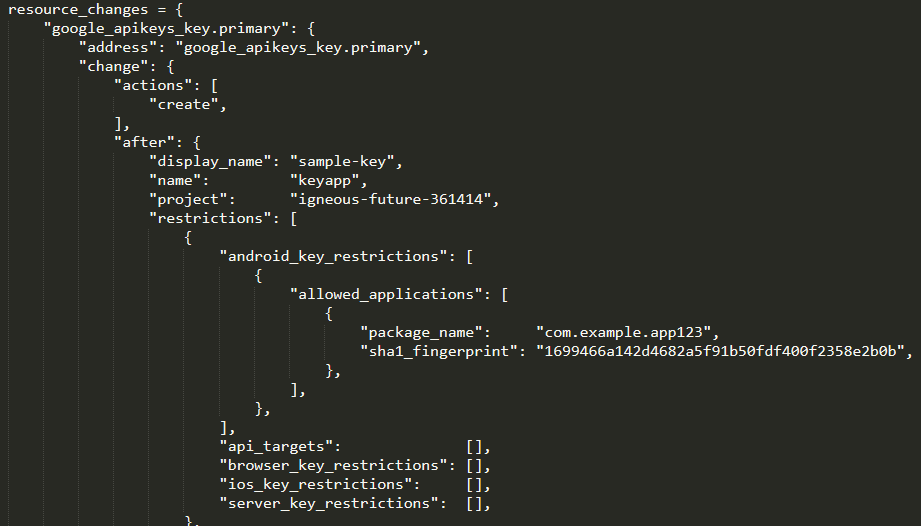
* + - Provider Ref:[google\_apikeys\_key | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/apikeys_key)
    - Terraform attribute: "server\_key\_restrictions","browser\_key\_restrictions","api\_targets","android\_key\_restrictions", and "ios\_key\_restrictions" blocks under "restrictions" block

***Test cases:***

**Pass cases**

1. In pass case, if any of the "ios\_key\_restrictions","android\_key\_restrictions", "api\_targets","browser\_key\_restrictions", "server\_key\_restrictions" blocks are included within "restrictions" block then the pass case will always pass.

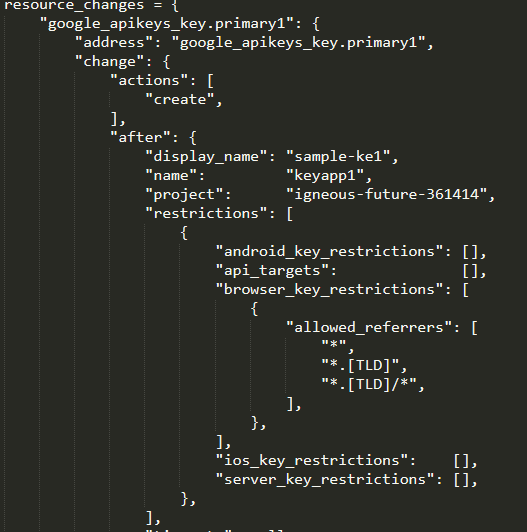
Screenshot of argument in mock file



**Fail case:**

1. In pass case, if "allowed\_referrers" attribute contain any of the following : "\*","\*.[TLD]","\*.[TLD]/\*" then the pass case will always fail.

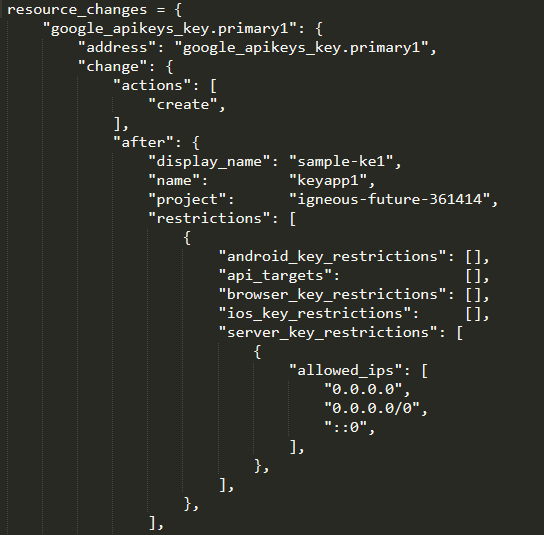
Screenshot of argument in mock file



**Fail 2 case:**

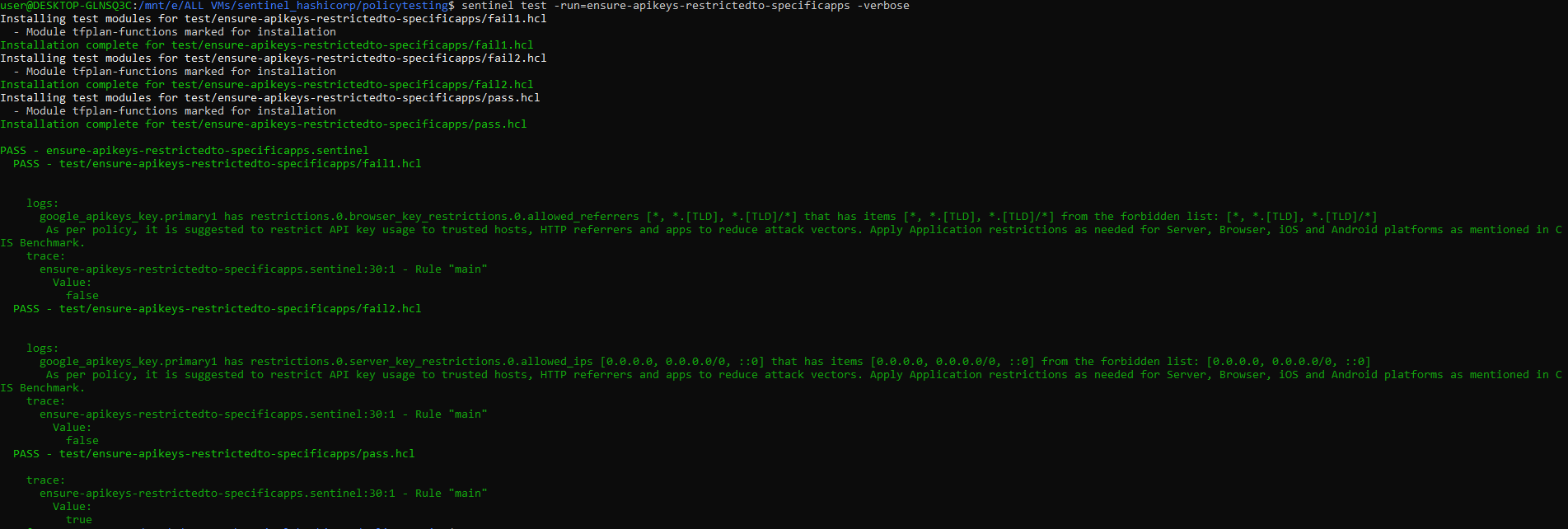
1. In pass case, if "allowed\_ips" attribute contain any of the following : "0.0.0.0","0.0.0.0/0","::0" then the pass case will always fail.

Screenshot of argument in mock file



**Testcases Output:**

Screenshot of test command successful



1.16 Ensure Essential Contacts is Configured for Organization

***Sentinel Policy Name:***

1.16 Ensure Essential Contacts is Configured for Organization

***Category:***

* + Identity and Access Management.

***Description of Policy:***

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

* + 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.

***Sentinel Policy Restriction:***

* + The policy checks whether attribute "email" contains value and not null

***Terraform attributes:***

* + - Provider Ref: <https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/essential_contacts_contact>
    - Terraform attribute: "email"

***Test cases:***

**Pass cases**

1. In pass case, if "email" contains value and not null then the pass case will always pass.

Screenshot of argument in mock file



**Fail case:**

1. In pass case, "email" does not contains value and null then the pass case will always fail.

Screenshot of argument in mock file



**Testcases Output:**

Screenshot of test command successful

((base) alexcardona@A1exs—Air—2 Essential—Contacts—Configured.Org % sentinel test 
Installing test modules for 
— Module tfplan—functions marked for installation 
Installation complete for 
Installing test modules for 
— Module tfplan—functions marked for installation 
Installation complete for 
— essential—contacts—configured—org.sentinel 
PASS 
PASS — 
contact. contact2 
contact. contact5 
—verbose 
logs: 
google_essential_ 
google_essential 
google_essential_ 
google_essential 
trace: 
contacts 
. contact3 
contacts 
google_essential_contacts_contact . contact6 
contacts_contact contactl 
contacts_contact . contact4 
has 
has 
has 
has 
has 
has 
email 
email 
email 
email 
email 
email 
with 
with 
with 
with 
with 
with 
value 
value 
value 
value 
value 
value 
that 
that 
that 
that 
that 
that 
is 
is 
in 
in 
the 
the 
the 
the 
the 
the 
forbidden 
forbidden 
forbidden 
forbidden 
forbidden 
forbidden 
list: 
list: 
list: 
list: 
list: 
list: 
essential—contacts—configured.org . sentinel • 
.14:1 - Rule 
Value: 
false 
PASS — 
trace: 
essential—contacts—configured—org.sentinel:14:1 — 
Value: 
Rule 
" malnu 
" malnu 

1.17 Ensure that Dataproc Cluster is encrypted using CustomerManaged Encryption Key

Wednesday, October 26, 2022

9:41 AM

***Sentinel Policy Name:***

1.17 Ensure that Dataproc Cluster is encrypted using CustomerManaged Encryption Key

***Category:***

* + Identity and Access Management.

***Description of Policy:***

* + 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).
  + 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.

***Sentinel Policy Restriction:***

* + The policy checks whether "encryption\_config" contains kms\_key\_name

***Terraform attributes:***

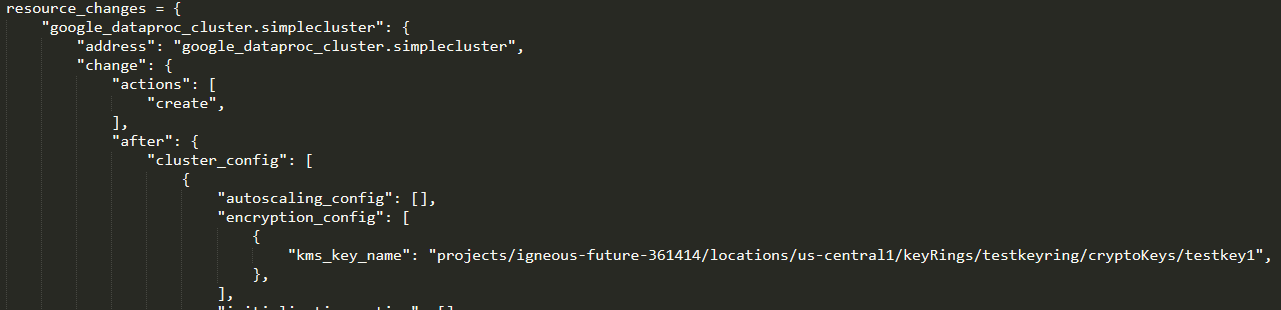
* + - Provider Ref:[google\_dataproc\_cluster | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/dataproc_cluster)
    - Terraform attribute: "encryption\_config" under "cluster\_config" block

***Test cases:***

**Pass cases**

1. In pass case, if"encryption\_config" block is included then the pass case will always pass.

Screenshot of argument in mock file



**Fail case:**

1. In pass case, if "encryption\_config" block is not included then the pass case will always fail.

Screenshot of argument in mock file

resource_changes 
" google_dataproc_cluster. simplecluster" . 
"address" : " google_dataproc_cluster. simplecluster" 
"change" • 
"actions" : 
create" 
" after 
name : 
region" . 
"timeouts" : 
"simplecluster" 
"us-centrall" 
null, 
"after_unknown" : { 
"cluster_config" 
'lid" : 
"labels" : 
"project" • 
true , 
true , 
true , 
true , 

**Testcases Output:**

Screenshot of test command successful

vms/sentinel 
hashicorp/policytesting$ 
sentinel 
Installing test modules for test/ensure-dataproc-has-customerkey/fail . hcl 
module tfplan-functions marked for installation 
Installation complete for test/ensure-dataproc-has-customerkey/fail . hcl 
Installing test modules for test/ensure-dataproc-has-customerkey/pass . hcl 
module tfplan-functions marked for installation 
Installation complete for test/ensure-dataproc-has-customerkey/pass . hcl 
ensure-dataproc-has-customerkey . sentinel 
PASS 
test/ensure-dataproc-has-customerkey/fail . hcl 
PASS 
logs : 
test 
- run-ensure- 
dataproc- has- customerkey 
- ver 
se 
. simplecluster has cluster_config.8 that is missing, null, or is not a map or a list. It should have had these items: [encryption _ config] 
Policy failed because Dataproc Cluster referenced in the mock file is not encrypted with Customer managed Encryption Key (CMEK). Please use encryption _ config to include key. 
trace: 
ensure-dataproc-has-customerkey . sentinel : : 1 
Rule 
Value: 
false 
test/ensure-dataproc-has-customerkey/pass . hcl 
PASS 
trace: 
ensure-dataproc-has-customerkey . sentinel : : 1 
Value: 
true 
Rule 
"main" 
"main" 

1.18 Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager

***Sentinel Policy Name:***

1.18 Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager

***Category:***

* + Identity and Access Management.

***Description of Policy:***

* + 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.
  + 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.

***Sentinel Policy Restriction:***

* + The policy checks whether "secret\_environment\_variables" contains any values

***Terraform attributes:***

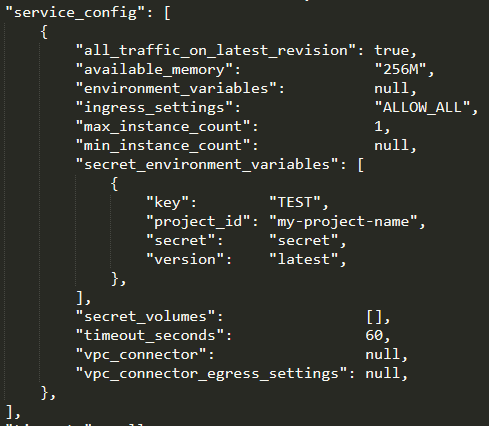
* + - Provider Ref:[google\_cloudfunctions2\_function | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/cloudfunctions2_function)
      * [google\_cloudfunctions\_function | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/cloudfunctions_function)
    - Terraform attribute:
      * "secret\_environment\_variables" block under "service\_config" block for "google\_cloudfunctions\_function" resource
      * "secret\_environment\_variables" block for "google\_cloudfunctions2\_function" resource

***Test cases:***

**Pass cases**

1. In pass case, if "secret\_environment\_variables" block contains values for either of the "google\_cloudfunctions\_function" or "google\_cloudfunctions2\_function" resource then the pass case will always pass.

Screenshot of argument in mock file - "google\_cloudfunctions\_function" resource



"google\_cloudfunctions2\_function" resource:

secret environment 
" key" : 
secret" 
•version : 
variables" : 
"TEST" , 
" project_id"• "my-project-name' 
" secret" , 
"latest" , 

**Fail cases:**

1. In pass case, if "secret\_environment\_variables" block does not contains values for either of the "google\_cloudfunctions\_function" or "google\_cloudfunctions2\_function" resource then the pass case will always fail.

Screenshot of argument in mock file -"google\_cloudfunctions\_function" resource

service config": [ 
" all traffic on latest revision . 
" available_memory . 
"environment variables" : 
ingress_settings . 
"max instance count " : 
"min instance count" : 
secret environment 
variables " : 
'secret volumes" : 
"timeout seconds" : 
"vpc connector" • 
settings" • 
true , 
" 256M" , 
null, 
"ALLOW ALL", 
1, 
null, 
o, 
o, 
null, 
null, 

"google\_cloudfunctions2\_function" resource:



**Testcases Output:**

Screenshot of test command successful

Wls/sentinel_hashicorp/policytesting$ sentinel test -run-ensure-usingsecretsmanager-notstoredincloudfunctionsenv 
Installing test modules for test/ensure-usingsecretsmanager-notstoredincloudfunctionsenv/fail . hcl 
module tfplan-functions marked for installation 
Installation complete for test/ensure-usingsecretsmanager-notstoredincloudfunctionsenv/fail.hcl 
Installing test modules for test/ensure-usingsecretsmanager-notstoredinc10udfunctionsenv/fai12. hcl 
module tfplan-functions marked for installation 
Installation complete for test/ensure-usingsecretsmanager-notstoredinc10udfunctionsenv/fai12.hc1 
Installing test modules for test/ensure-usingsecretsmanager-notstoredincloudfunctionsenv/pass . hcl 
module tfplan-functions marked for installation 
Installation complete for test/ensure-usingsecretsmanager-notstoredincloudfunctionsenv/pass . hcl 
Installing test modules for test/ensure-usingsecretsmanager-notstoredinc10udfunctionsenv/pass2. hcl 
module tfplan-functions marked for installation 
Installation complete for test/ensure-usingsecretsmanager-notstoredinc10udfunctionsenv/pass2.hc1 
ensure - usingsecretsmanager - notstoredincloudfunctionsenv . sentinel 
PASS 
test/ ensure - usingsecretsmanager - notstoredincloudfunctionsenv 'fail . hcl 
PASS 
logs : 
- verbose 
google_c10udfunctions2_function.function has service _ config.8.secret_environment_variab1es.8 that is missing, null, or is not a map or a list. It should have had these items: [secret] 
This policy is used to ensure the recommendation to use Secret manager instead of usual environment variables for Cloud Functions. Environment Variables are stored unencrypted, 
e code. 
trace: 
ensure - usingsecretsmanager - notstoredincloudfunctionsenv . sentinel : 38 : 1 
Value: 
false 
Rule "main" 
PASS 
test/ ensure - usingsecretsmanager - notstoredincloudfunctionsenv /fai12 . hcl 
logs : 
google_cloudfunctions_function.function has secret _ environment_variables.a that is missing, null, or is not a map or a list. It should have had these items: [secret] 
This policy is used to ensure the recommendation to use Secret manager instead of usual environment variables for Cloud Functions. Environment Variables are stored unencrypted, 
and are accessible for all users who have access to th 
and are accessible for all users who have access to th 
e code. 
trace: 
ensure - usingsecretsmanager - notstoredincloudfunctionsenv . sentinel : 38 : 1 
Value: 
false 
test/ ensure - usingsecretsmanager - notstoredincloudfunctionsenv / pass . hcl 
PASS 
trace: 
ensure - usingsecretsmanager - notstoredincloudfunctionsenv . sentinel : 38 : 1 
Value: 
true 
Rule 
Rule 
test/ ensure - usingsecretsmanager - notstoredincloudfunctionsenv / pass2 . hcl 
PASS 
trace: 
ensure - usingsecretsmanager - notstoredincloudfunctionsenv . sentinel : 38 : 1 
Value: 
true 
Rule 
"main" 
"main" 
"main" 