# 

**CSWG- Policy As Code Documentation**

Compute Engine Sentinel Policies

4.1 Ensure That Instances Are Not Configured To Use the Default Service Account

***Sentinel Policy Name:***

* + 4.1 Ensure That Instances Are Not Configured To Use the Default Service Account

***Category:***

* + Compute Engine

***Description of Policy:***

* + 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](mailto:compute@developer.gserviceaccount.com).

***Terraform Provider:***

<https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/compute_instance> - resource block “google\_compute\_instance” is used.

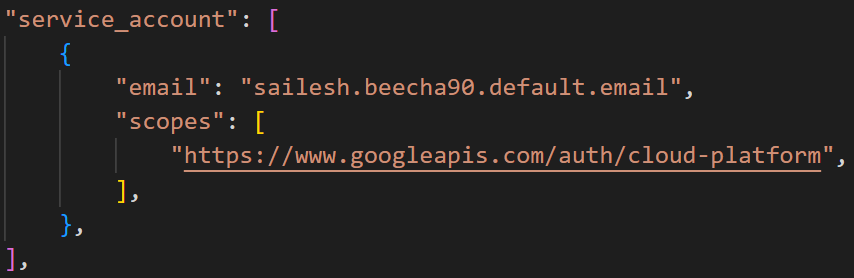
***Sentinel Policy Restriction:***

* + In this sentinel policy, we are ensuring that the service account section has an email that does not match the pattern [PROJECT\_NUMBER]-compute@developer.gserviceaccount.com.

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

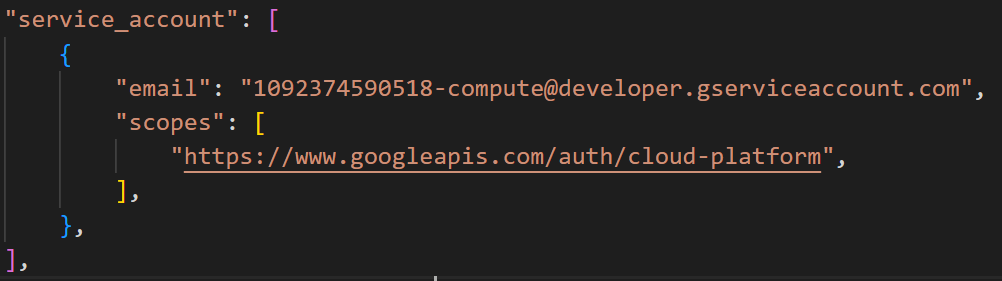
**Pass Case:**

1. Ensure that the service account section has an email that does not match the pattern [PROJECT\_NUMBER]-compute@developer.gserviceaccount.com.

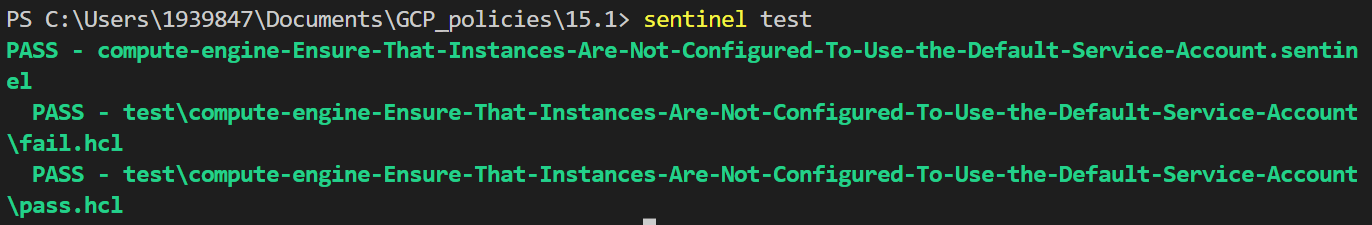


**Fail Case:**

1. Ensure that the service account section has an email that match the pattern [PROJECT\_NUMBER]-compute@developer.gserviceaccount.com.



**Testcases output:**



4.2 Ensure That Instances Are Not Configured to Use the Default Service Account with Full Access to All Cloud APIs

***Sentinel Policy Name:***

* + 4.2 Ensure That Instances Are Not Configured to Use the Default Service Account with Full Access to All Cloud APIs.

***Category :***

* + Compute Engine

***Description of Policy:***

* + 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.
  + When an instance is configured with Compute Engine default service account with Scope Allow full access to all Cloud APIs, 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.

***Terraform Provider:***

<https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/compute_instance> - resource block “google\_compute\_instance” is used.

***Sentinel Policy Restriction:***

* + In this sentinel policy, we are ensuring that the service account section has an email that match the pattern [[PROJECT\_NUMBER]-compute@developer.gserviceaccount.com](mailto:PROJECT_NUMBER]-compute@developer.gserviceaccount.com) is not configured with scope "<https://www.googleapis.com/auth/cloud-platform>".

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

**Pass Case:**

1. The service account section has an email that match the pattern [[PROJECT\_NUMBER]-compute@developer.gserviceaccount.com](mailto:PROJECT_NUMBER]-compute@developer.gserviceaccount.com) is not configured with scope "<https://www.googleapis.com/auth/cloud-platform>".

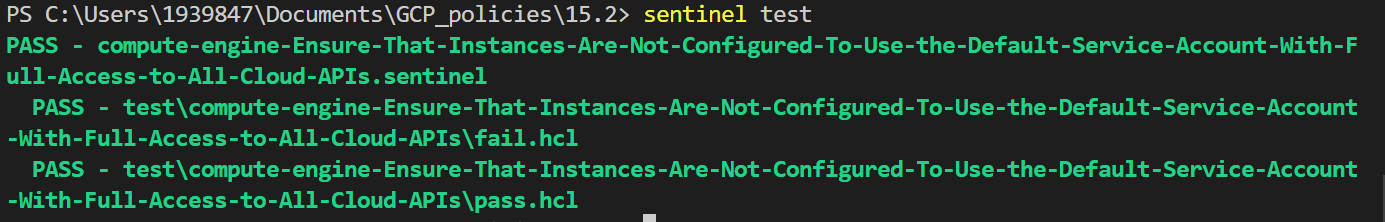


**Fail Case:**

1. The service account section has an email that match the pattern [[PROJECT\_NUMBER]-compute@developer.gserviceaccount.com](mailto:PROJECT_NUMBER]-compute@developer.gserviceaccount.com) is configured with scope "<https://www.googleapis.com/auth/cloud-platform>".



**Testcases output**



4.3 Ensure “Block Project-Wide SSH Keys” Is Enabled for VM Instances

***Sentinel Policy Name:***

* + 4.3 Ensure “Block Project-Wide SSH Keys” Is Enabled for VM Instances.

***Category :***

* + Compute Engine

***Description of Policy:***

* + 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.

***Terraform Provider:***

<https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/compute_instance> - resource block “google\_compute\_instance” is used.

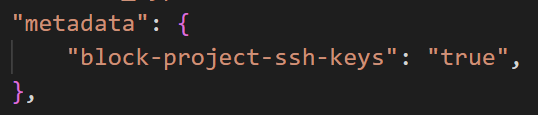
***Sentinel Policy Restriction:***

* + In this sentinel policy, “block-project-ssh-keys” parameter is set to “true”.

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

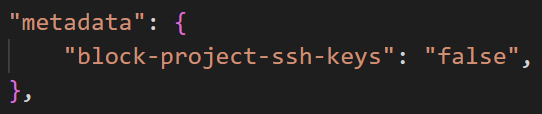
**Pass Case:**

1. “block-project-ssh-keys” parameter is set to “true”.

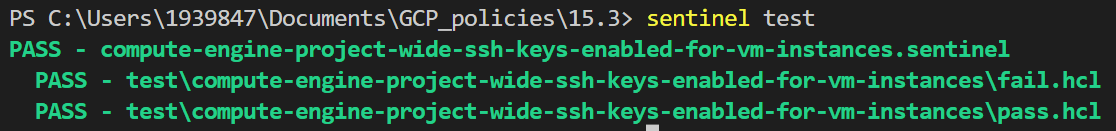


**Fail Case:**

1. In this sentinel policy, “block-project-ssh-keys” parameter is set to “false”.



**Testcases Output:**



4.4 Ensure Oslogin Is Enabled for a Project

***Sentinel Policy Name:***

* + 4.4 Ensure Oslogin Is Enabled for a Project.

***Category :***

* + Compute Engine

***Description of Policy:***

* + 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.

***Terraform Provider:***

<https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/compute_instance> - resource block “google\_compute\_instance” is used.

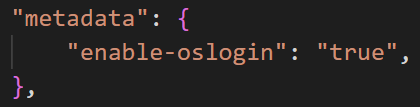
***Sentinel Policy Restriction:***

* + In this sentinel policy, “enable-oslogin” parameter is set to “true”.

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

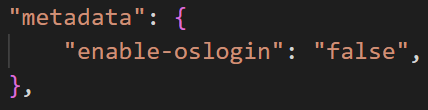
**Pass Case:**

1. “enable-oslogin” parameter is set to “true”.

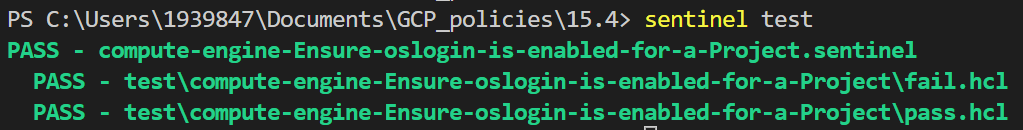


**Fail Case:**

1. “enable-oslogin” parameter is set to “false”.



**Testcases output**



4.5 Ensure ‘Enable Connecting to Serial Ports’ Is Not Enabled for VM Instance

***Sentinel Policy Name:***

* + 4.5 Ensure ‘Enable Connecting to Serial Ports’ Is Not Enabled for VM Instance.

***Category :***

* + Compute Engine

***Description of Policy:***

* + If you enable serial ports on an instance, clients can attempt to connect to that instance from any IP address.
  + Therefore, connection from to ports support should be disabled.

***Terraform Provider:***

<https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/compute_instance> - resource block “google\_compute\_instance” is used.

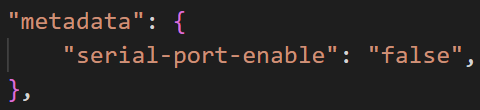
***Sentinel Policy Documentation:***

* + In this sentinel policy, “serial-port-enable" is set to “false”.

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

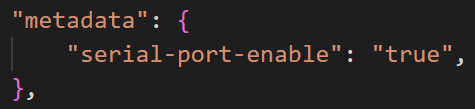
**Pass Case:**

1. “serial-port-enable" is set to “false”.

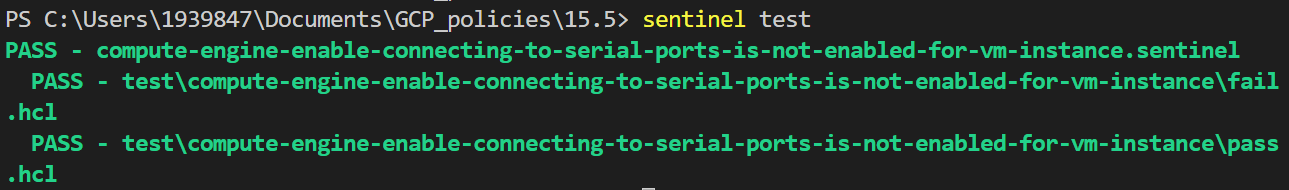


**Fail Case:**

1. “serial-port-enable" is set to “true”.



**Testcases Output:**



4.6 Ensure That IP Forwarding Is Not Enabled on Instances

***Sentinel Policy Name:***

* + 4.6 Ensure That IP Forwarding Is Not Enabled on Instances (Automated)

***Category :***

* + Compute Engine

***Description of Policy:***

* + IP Forwarding will let instance route packets in the VPC.
  + Forwarding packets should be disabled in order to prevent data loss or information disclosure.

***Terraform Provider:***

<https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/compute_instance> - resource block “google\_compute\_instance” is used.

***Sentinel Policy Restriction:***

* + In this sentinel policy, “can\_ip\_forward” parameter is set to “false”.

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

**Pass Case:**

1.  “can\_ip\_forward” parameter is set to “false”.

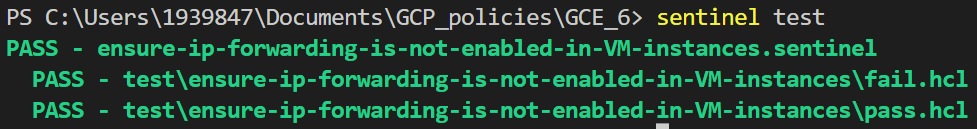


**Fail Case:**

1. ”can\_ip\_forward” parameter is set to “true”.



***Testcases Output:***



4.7 Ensure VM Disks for Critical VMs Are Encrypted with Customer Supplied Encryption Keys (CSEK)

***Sentinel Policy Name:***

* + 4.7 Ensure VM Disks for Critical VMs Are Encrypted with Customer Supplied Encryption Keys (CSEK).

***Category :***

* + Compute Engine

***Description of Policy:***

* + 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.

***Terraform Provider:***

<https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/compute_disk>

- resource block “google\_compute\_instance” or “google\_compute\_disk”is used.

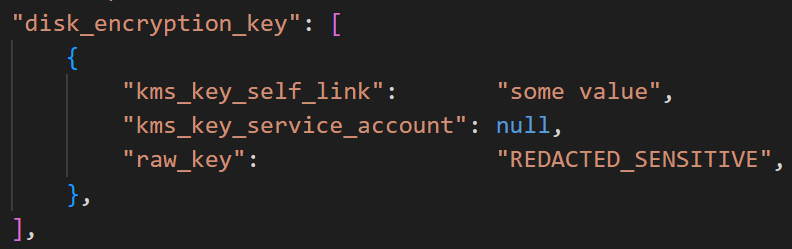
***Sentinel Policy Restriction:***

* + In this sentinel policy, disk can be created in 2 ways.
  + 1. Disk as a separate resource.
  + 2. Creating a VM instance with boot disk or attached disk.
  + If we are creating a disk as a separate resource, it should contain disk\_encryption\_key block with “kms\_key\_self\_link” parameter.
  + If we are creating a VM instance with boot disk or attached disk, it should contain either a parameter disk\_encryption\_key\_raw or kms\_key\_self\_link with some key.

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

**Pass Case:**

1. The disk\_encryption\_key block contains kms\_key\_self\_link.

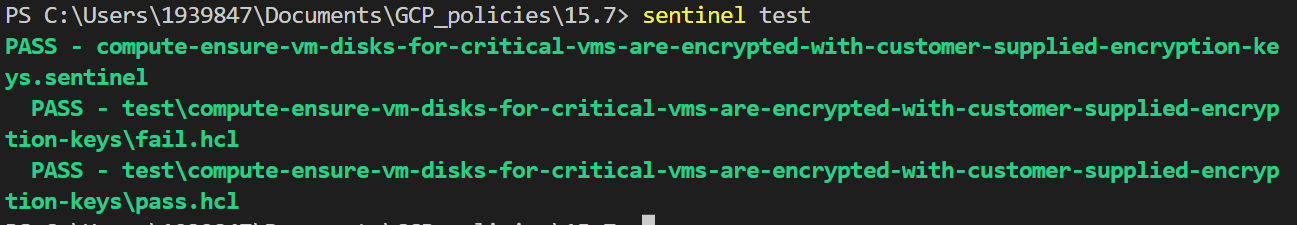


**Fail Case:**

1.  The disk\_encryption\_key block is null.



**Testcases Output:**



4.8 Ensure Compute Instances Are Launched with Shielded VM Enabled

***Sentinel Policy Name:***

* + 4.8 Ensure Compute Instances Are Launched with Shielded VM Enabled

***Category :***

* + Compute Engine

***Description of Policy:***

* + To defend 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.

***Terraform Provider:***

<https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/compute_instance> - resource block “google\_compute\_instance” is used.

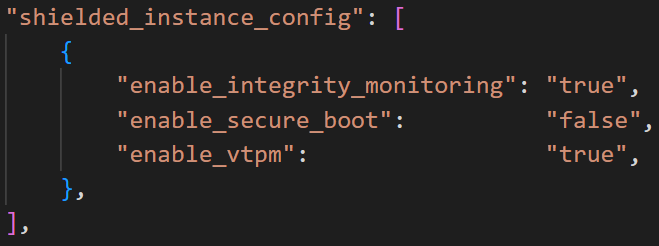
***Sentinel Policy Restriction:***

In this sentinel policy, in shielded instance config block, parameters like “enable integrity monitoring” is set to “true” and also “enable vtpm” is set to “true”.

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

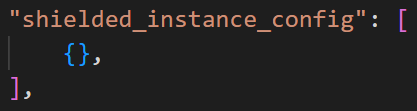
**Pass Case:**

When the shielded instance config is not null, contains parameters like enable integrity monitoring as “true” and enable vtpm as “true”.

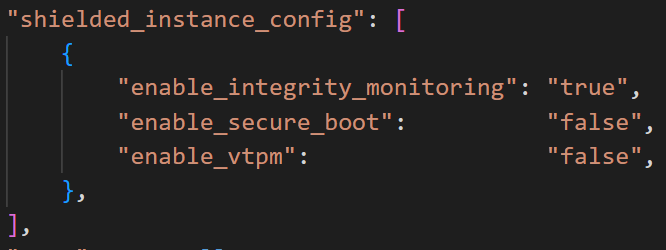


**Fail Cases:**

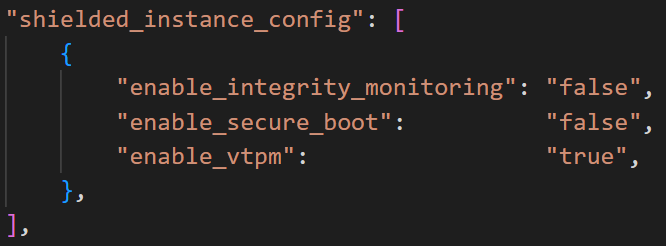
1. When the shielded instance config is null.



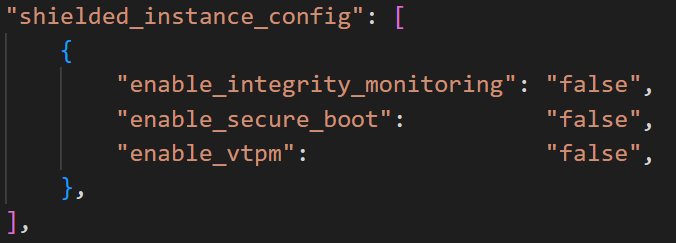
2. When the shielded instance config is not null, contains parameters like enable integrity monitoring as “true” and enable vtpm as “false”.



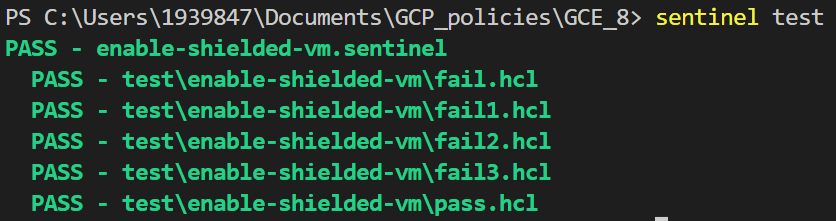
3. When the shielded instance config is not null, contains parameters like enable integrity monitoring as “false” and enable vtpm as “true”.



4. When the shielded instance config is not null, contains parameters like enable integrity monitoring as “false” and enable vtpm as “false”.



**Testcases Output:**



4.9 Ensure That Compute Instances Do Not Have Public IP Addresses

***Sentinel Policy Name:***

* + 4.9 Ensure That Compute Instances Do Not Have Public IP Addresses.

***Category:***

* + Compute Engine

***Description of Policy:***

* + 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.

***Terraform Provider:***

<https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/compute_instance> - resource block “google\_compute\_instance” is used.

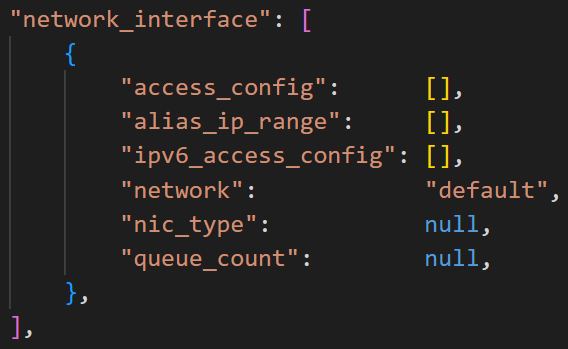
***Sentinel Policy Restriction:***

* + In this sentinel policy, VM instances are not configured with public IP.
  + Network interface block should contain access config parameter.

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

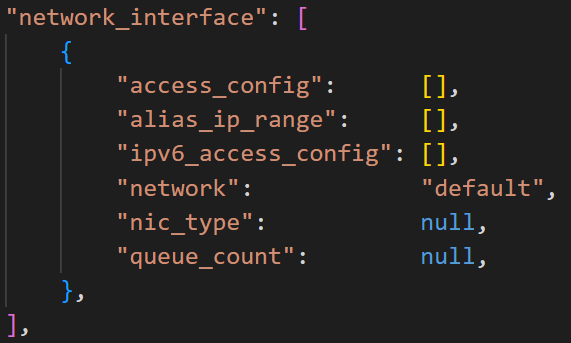
**Pass Case:**

1. Network interface block does not contain access config block.

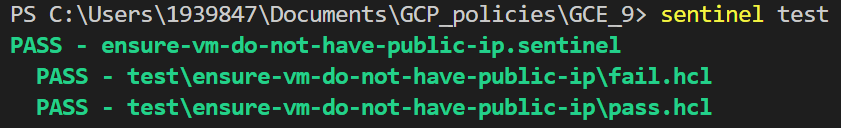


**Fail Case:**

1. Network interface block contains “access config” parameter.



**Testcases Output:**



4.10 Ensure That App Engine Applications Enforce HTTPS Connections

***Sentinel Policy Name:***

* + 4.10 Ensure That App Engine Applications Enforce HTTPS Connections

***Category :***

* + Google Compute Engine/ Google Application Engine

***Description of Policy:***

* + In order to maintain the highest level of security, all connections to an application should be secure by default.
  + Insecure HTTP connections maybe subject to eavesdropping by hackers which can expose sensitive data.
  + When creating an Application using the Google Application Engine, an application version must be selected: Either Standard version or Flexible version. This policy will ensure that security of the Application is strong from a Cyber Security standpoint.

***Sentinel Policy Restriction:***

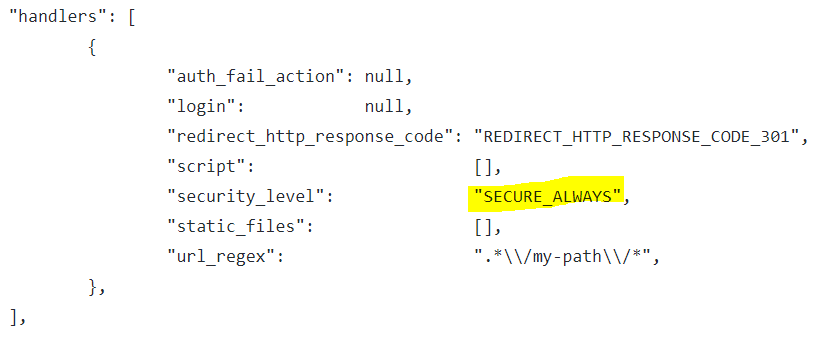
* + We are checking the ensure that applications created via the Google Application Engine enforce HTTPS connections (as opposed to insecure HTTP connections) in all network communication scenarios.

* + ***Terraform attributes:***
    - Provider Ref: [google\_app\_engine\_standard\_app\_version | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/app_engine_standard_app_version)
    - Provider ref: [google\_app\_engine\_flexible\_app\_version | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/app_engine_flexible_app_version)

***Test cases:***

**Pass cases**

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

* + For 'google\_app\_engine\_standard\_app\_version' , the 'security level' argument is set to 'SECURE\_ALWAYS'
  + For 'google\_app\_engine\_flexible\_app\_version' , the 'security level' argument is set to 'SECURE\_ALWAYS'
  + 

**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\_app\_engine\_standard\_app\_version' , the 'security level' argument is set to something other than 'SECURE\_ALWAYS'
  + For 'google\_app\_engine\_flexible\_app\_version' , the 'security level' argument is set to something other than 'SECURE\_ALWAYS'
  + "handlers" 
    "auth fail action": null, 
    "login": 
    null, 
    null, 
    "script": 
    o, 
    "security_level" : 
    null, 
    "static files". 
    o, 
    "url_regex" : 
    null, 

**Testcases Output:**

cmplete fw 
PASS - 
PASS - . 
has with 
Hut is in list: 
1 10 ensure of is 
sdmpping is that within 
is 'SECURE 
SECURE 
eav 
PASS • 
1 - Rule "min" 
• Rule "min" 

4.11 Ensure That Compute Instances Have Confidential Computing Enabled

***Sentinel Policy Name:***

* + 4.11 Ensure That Compute Instances Have Confidential Computing Enabled.

***Category :***

* + Compute Engine

***Description of Policy:***

* + 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.

***Terraform Provider:***

<https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/compute_instance>  - resource block “google\_compute\_instance” is used.

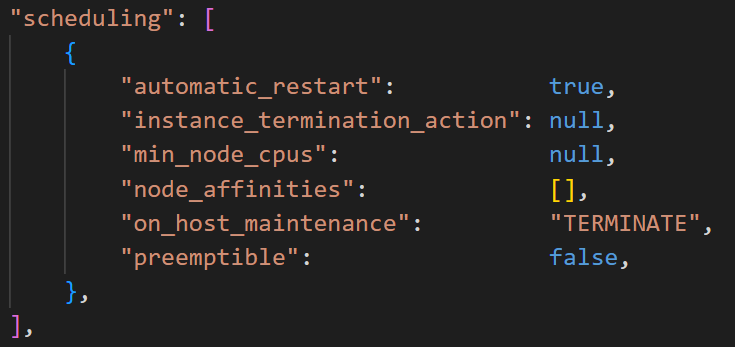
***Sentinel Policy Restriction:***

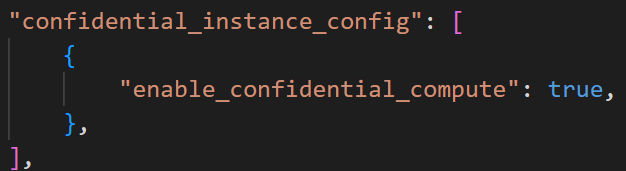
* + In this sentinel policy, Scheduling block should contain “on host maintenance” parameter as “TERMINATE” and confidential instance config should contain “enable confidential compute” parameter as “true”.

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

**Pass Case:**

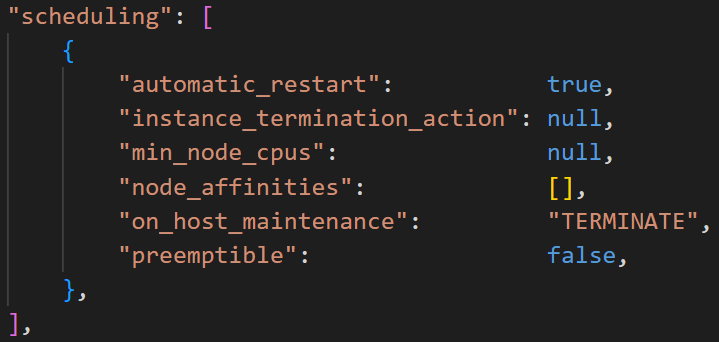
1. Scheduling block should contain “on host maintenance” parameter as “TERMINATE” and confidential instance config should contain “enable confidential compute” parameter as “true”.

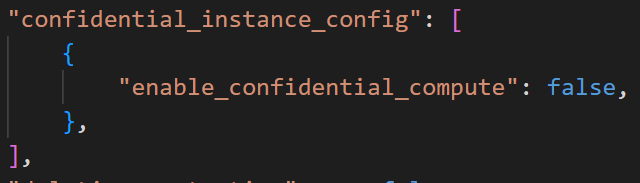




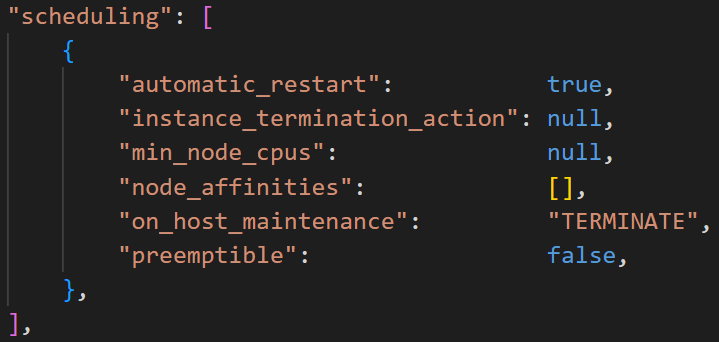
**Fail Case:**

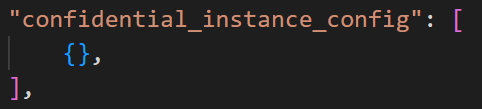
1. When confidential instances config block contains “enable confidential compute” parameter as “false”.



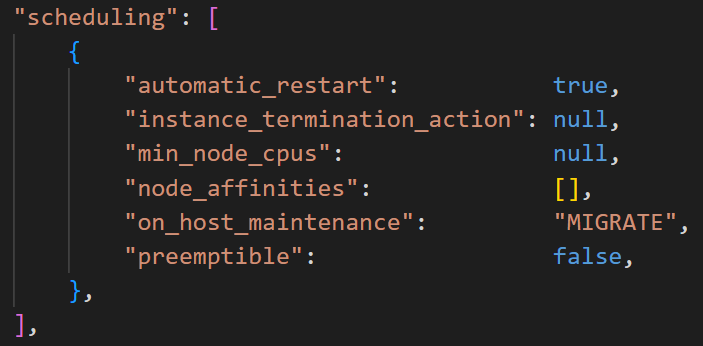


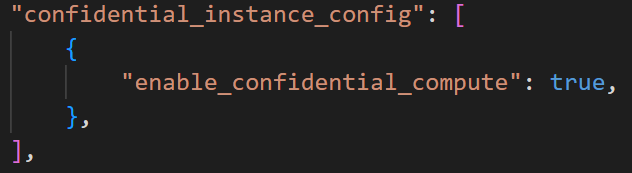
2. When the confidential instance config block is null.



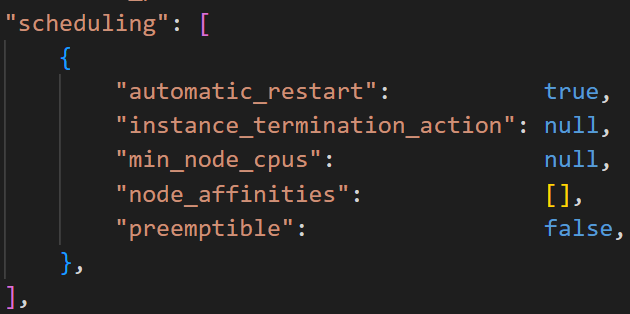


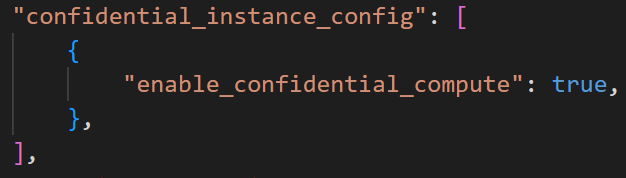
3. When the scheduling block contains “on host maintenance” parameter as “MIGRATE” and confidential instance config block contains “enable confidential compute” parameter as “true”.



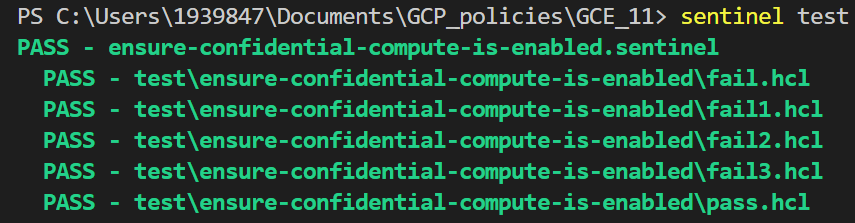


4. When scheduling block does not contain “on host maintenance” parameter.





**Testcases Output:**



4.12 Ensure the Latest Operating System Updates Are Installed on all Virtual Machines in All Projects

***Sentinel Policy Name:***

* + 4.12 Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects

***Category :***

* + Google Compute Engine

***Description of Policy:***

* + As per CIS benchmarks, it is recommended to keep an operating system up to date with operating system updates and security patching. This 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.

***Sentinel Policy Restriction:***

* + This policy ensures that the **latest** security /updates patches as well as **critical** operating system updates are installed on all virtual machines for all projects.
  + The **latest** security patches and **critical** operating system updates are deployed to virtual machines in all projects on the **first Tuesday of every month at 12:00 AM EST (midnight)**
  + Optional updates and non- critical patches are optional and can be configured as needed, this policy ensure that the patches and updates with "Critical" or "High priority" association are applied.

***Terraform attributes:***

Provider Ref: [google\_os\_config\_patch\_deployment | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/os_config_patch_deployment)

***Test cases:***

**Pass cases**

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

* + For all 'google\_os\_config\_patch\_deployment' resources, the "Instance\_filter.all" must be TRUE. The ensures that **ALL** VMs are included in the patch deployment
  + For all 'google\_os\_config\_patch\_deployment' resources, ensure that 'excludes = null' (or ensure this is not defined in main.tf) This will ensure that all security and OS update packages are included in the patch deployment
  + For all 'google\_os\_config\_patch\_deployment' resources, ensure the 'apt' update type is 'UPGRADE'. This ensure that packages are only updated (older packages are not removed, only updated). This will reduce the potential that a packaged need for an application to run is removed. This is the Patch configuration for Linux VMs: Debian, Ubuntu
  + For all 'google\_os\_config\_patch\_deployment' resources, ensure the 'yum' update has 'security = true' This will ensure all security updates are installed on Linux VMs: RHEL, CentOS
  + For all 'google\_os\_config\_patch\_deployment' resources, ensure the 'zypper' update has 'categories = ["security"]' and 'with\_update = true'. This will ensure that optional security updates are not installed, only the required security updates are installed. Patch configuration for Linux Enterprise servers: SuSE (German-based open-source software firm)
  + For all 'google\_os\_config\_patch\_deployment' resources, ensure the 'windows\_update' update has 'classifications = ["SECURITY", "CRITICAL"]' This will all CRITICAL security updates and CRITICAL operating system updates are installed
  + Other patch configurations are optional, however, the 'main.tf' presents recommended configuration such as 'disruption\_budget' and 'rollout'

"patch_config": [ 
"excludes": 
null, 
"exclusive_packages": null, 
"type": 
" UPGRADE" , 

"Wi ndows_update": 
"classifications": [ 
"SECURITY" , 
"CRITICAL , 
"yum": 
"zypper": 
"categories": [ 
"security" , 
"excludes": 
"exclusive_patches": null, 
"severities" : 
"with_optional" : 
"with_update": 
"excludes": 
null, 
"exclusive_patches" 
: null, 
"excludes": 
null 
: null 
"exclusive_packages" 
"minimal": 
null 
"security" : 
true 
null, 
null, 
null, 
true, 

**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\_os\_config\_patch\_deployment', the 'Instance\_filter.all' attribute is set to something other than "true"

"instance filter": 
true, 

* + For 'google\_os\_config\_patch\_deployment', the 'excludes' attribute is set to something other than "null"

"yum" 
"excludes": 
null, 

**Testcases Output:**

are u 
PASS - 
logs: 
es 
securi _ pa c s.se Ine 
The defined patch configuration is rx)n- In the •patch_config• block, ensure there are exclusions. (i.e. excludes = null) Ensui 
e that APT upgrade type - UPGRA)E (this ensures packages are only updated, rx)thing is replaced/ r«mved. If legacy applications are in the Cloud 
nvioranent, they will wt be effected by L4Niates/ patches.) Ensure that security are set to •true' to ensure WIS are updated fran a C: 
ber Security staruiX)int. With regards to Zypper updates, ensure that the caregory of •security' is defined. Ensure •with update' is set to •true' 
(This ensures that only required are deployed, as to •with optional' that deploys optional updates as part of the patch process.) 
Regarding •windcvs upxiate•, ensure that the classifications are listed as •SECURITY • 
, •CRITICAL • (This ensures that only security updates and cr: 
tical operating system are deployed) The ranaining parneters of the patch management configuration as defined in main.tf are opt 
Onal but recumended. Finally, ensure the • instance_filter• is set it all, this ensures that ALL WE in ALL projects are included in the Patch Mal 
aganent process 
trace: 
latest_security_patches. sentinel - Rule "main 
Value: 
false 
Ws_are_updated_with sentinel : 26 : 1 - Rule 
"Validate 
Value: 
false 
sentinel : 52 : 1 - Rule 
"Validate 
Value: 
false 
sentinel : 17 : 1 - Rule 
"Validate_Targets_a11_Ws all_Projects" 
Value: 

PASS - hcl 
trace : 
Value : 
true 
Value: 
true 
Value: 
true 
Value: 
true 
Value : 
sentinel • 
sentinel - Rule 
sentinel - Rule 
sentinel - Rule 
sentinel : 17:1 - Rule 
"main" 
" Val id ate_P atch_Conf igur pper_Upd ates " 