# 

**Policy-as-Code Documentation**

SQL Sentinel Policies

6.6 Ensure That Cloud SQL Database Instances Do Not Have Public IPs

***Sentinel Policy Name:***

* 6.6 Ensure That Cloud SQL Database Instances Do Not Have Public IPs

***Category:***

* Cloud SQL

***Description of Policy:***

* It is recommended to configure SQL database instance to use private IPs instead of public IPs.
* To lower the organization's attack surface, Cloud SQL databases should not have public IPs. Private IPs provide improved network security and lower latency for your application.

***Sentinel Policy Restriction:***

* For 'google\_sql\_database\_instances' the default configuration assigns the asset a public IP. This policy will enforce a configuration where public IP can not be defined

***Terraform attributes:***

* + Provider Ref: [google\_sql\_database\_instance | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/sql_database_instance)

***Test cases:***

**Pass cases**

1. For resource 'google\_sql\_database\_instance' the attribute 'ipv4\_enabled = false'

"ip_configuration": [ 
"al : 
"authorized networks . 
"require_ssl": 
null, 
false, 
null, 

**Fail case:**

1. For resource 'google\_sql\_database\_instance' the attribute 'ipv4\_enabled' is something other than 'false'

"ip_configuration": [ 
"authorized networks . 
"require SSI": 
null, 
true, 
null, 

6.7 Ensure That Cloud SQL Database Instances Are Configured with Automated Backups.

***Sentinel Policy Name:***

* + 6.7 Ensure That Cloud SQL Database Instances Are Configured with Automated Backups.

***Category:***

* + Cloud SQL

***Description of Policy:***

* + Backups provide a way to restore a Cloud SQL instance to recover lost data or recover from a problem with that instance.
  + Automated backups need to be set for any instance that contains data that should be protected from loss or damage.

***Terraform Providers:***

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

***Sentinel Policy restriction:***

* + In this sentinel policy, in backup\_configuration block, “enabled” parameter is set to “true”

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

**Pass Case:**

1. In backup\_configuration block, “enabled” parameter is set to “true”.

"backup _ configuration" : 
" enabled " : 
" location" : 
'point_in_time recovery 
"start time" : 
enabled" : 
null, 
true, 
null, 
null, 

**Fail Cases:**

1. In backup\_configuration block, “enabled” parameter is set to “false”.

"backup _ configuration" : 
" enabled " : 
" location" : 
'point_in_time recovery 
"start time" : 
enabled" : 
null, 
false, 
null, 
null, 

2. When the backup\_configuration block is empty.

" backup _ configuration " : 

6.1.1 Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges

***Sentinel Policy Name:***

* CIS 6.1.1 Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges

***Category :***

* Cloud SQL

***Description of Policy:***

* It is recommended to set a password for the administrative user (root by default) to prevent unauthorized access to the SQL database instances
* This recommendation is applicable only for MySQL Instances. PostgreSQL does not offer any setting for No Password from the cloud console.

***Sentinel Policy Restriction:***

* At the time of MySQL Instance creation, not providing an administrative password allows anyone to connect to the SQL database instance with administrative privileges. The root password should be set to ensure only authorized users have these privileges.
* This policy enforces Password Validation on all MySQL database Admins/ Superusers/ and regular users

***Terraform attributes:***

* + Provider Ref: [google\_sql\_database\_instance | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/sql_database_instance)

***Test cases:***

**Pass cases**

1. For resource 'google\_sql\_database\_instance' the attribute 'enable\_password\_policy' is 'true'
2. For resource 'google\_sql\_database\_instance' the attribute 'disallow\_username\_substring' is 'true'
3. For resource 'google\_sql\_database\_instance' the attribute 'min\_length' is in the 'allsupported\_min\_length' (per the Sentinel Policy)
4. For resource 'google\_sql\_database\_instance' the attribute 'reuse\_interval' is in the 'allsupported\_reuse\_interval' (per the Sentinel Policy)

"password_val idation_policy" : 
" complexity" : 
"disallow_username_substring": true, 
cy" : 
"min _ length" : 
nterval" : 
"reuse interval": 
null, 
true , 
null, 

**Fail case:**

1. For resource 'google\_sql\_database\_instance' the attribute 'enable\_password\_policy' is 'false'
2. For resource 'google\_sql\_database\_instance' the attribute 'disallow\_username\_substring' is 'false'
3. For resource 'google\_sql\_database\_instance' the attribute 'min\_length' is something outside of the 'allsupported\_min\_length' (per the Sentinel Policy)
4. For resource 'google\_sql\_database\_instance' the attribute 'reuse\_interval' is something outside of the 'allsupported\_reuse\_interval' (per the Sentinel Policy)

" icy" : 
"complexity" : 
"min_length": 
"pas " : 
"reuse interval": 
true , 
true, 
true , 
null, 