Google Compute Engine

Monday, August 1, 2022

12:07 PM

**Google Compute Engine**

Kind: IAMPolicy

Kind: IAMPolicyMember

**Image User Role Config**

**KCC**

* Control the use of compute.imageUser role
* [IAMPolicyMember  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/iam/iampolicymember)

spec:

member: string

role: compute.imageUser

**Terraform:**

* Allow ‘create’ events for resources of google\_organization\_iam\_policy, google\_organization\_iam\_binding, google\_organization\_iam\_member, google\_project\_iam\_policy, google\_project\_iam\_binding, google\_project\_iam\_member, google\_folder\_iam\_policy, google\_folder\_iam\_binding, google\_folder\_iam\_member and field ‘role’ or ‘binding -> role’ (depending on resource type) has roles (compute.imageUser) if the ‘member’ field has a ‘group’ in the allow list
* Block ‘create’ events for resources of google\_organization\_iam\_policy, google\_organization\_iam\_binding, google\_organization\_iam\_member, google\_project\_iam\_policy, google\_project\_iam\_binding, google\_project\_iam\_member, google\_folder\_iam\_policy, google\_folder\_iam\_binding, google\_folder\_iam\_member and field ‘role’ or ‘binding -> role’ (depending on resource type) has roles (compute.imageUser) if the ‘member’ field has a ‘group’ not in the allow list
* Do nothing for ‘no-op’ or ‘delete’ events
* Ignore the allow list if the ‘project’ is in the exemption list -> i.e., do not enforce the rule if the ‘project’ is in an exemption list.

**Google Compute Engine**

Kind: ComputeInstance

Kind: ComputeInstanceTemplate

**Image Approval Config**

**KCC**

* Block events for resources of type ‘kind: ComputeInstance’ and ‘kind: ComputeInstanceTemplate’ where spec values do not match as described in below table
* [ComputeInstance  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstance)
* [ComputeInstanceTemplate  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstancetemplate#custom_resource_definition_properties)

ComputeInstance

spec:  
 machineType: n1-standard-1  
  zone: us-west1-a  
  bootDisk:  
    initializeParams:  
      size: 24

      type: pd-ssd  
      sourceImageRef:  
        external: debian-cloud/debian-9

ComputeInstanceTemplate

spec:

disk:

- sourceImageRef:

name: instancetemplate-dep

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API** | **Kind** | **Key** | **Conditional** | **Value** |
| compute.cnrm.cloud.google.com | ComputeInstance | spec.bootDisk.initializeParams.sourceImageRef.external | equals | predefined image list |
| compute.cnrm.cloud.google.com | ComputeInstanceTemplate | spec.disk.sourceImageRef.name | equals | predefined image list |

**Terraform:**

* Block 'create' or 'no-op' or 'update' events for resources of type "google\_compute\_instance” and “google\_compute\_instance\_template” where field 'boot\_disk -> initialize\_params -> image' is not in a predefined image list.
* Do nothing for ‘delete’ events
* Ignore the allow list if the ‘project’ is in the exemption list -> i.e., do not enforce the rule if the ‘project’ is in an exemption list.

ComputeInstance

{

resource "google\_compute\_instance" "default" {

name = "test"

machine\_type = "e2-medium"

zone = "us-central1-a"

boot\_disk {

initialize\_params {

image = "debian-cloud/debian-9"

}

}

}

    "resource\_changes": [

        {

            "type": "google\_compute\_instance",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "boot\_disk": [

                        {

                            "auto\_delete": true,

                            "disk\_encryption\_key\_raw": null,

                            "initialize\_params": [

                                {

                                    "image": "only-approved-images"

                                }

                            ],

                            "mode": "READ\_WRITE"

                        }

                    ],

ComputeInstanceTemplate

    "resource\_changes": [

        {

            "type": "google\_compute\_instance\_template",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "disk": [

                        {

                            "source\_image": "Approved Images"

                        }

                    ],

**Google Compute Engine**

Kind: ComputeInstance

Kind: ComputeInstanceTemplate

**Prevent External IP Config**

**KCC**

* Block events for resources of type ‘kind: ComputeInstance’ and ‘kind: ComputeInstanceTemplate’ where spec values do not match as described in the table below
* [ComputeInstance  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstance)
* [ComputeInstanceTemplate  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstancetemplate#custom_resource_definition_properties)

ComputeInstance

spec:

networkInterface:  
  - accessConfig:  
    - natIpRef:  
        external: string  
        name: string  
        namespace: string

ComputeInstanceTemplate

networkInterface:

- accessConfig:

- natIpRef:

external: string

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API** | **Kind** | **Key** | **Conditional** | **Value** |
| compute.cnrm.cloud.google.com | ComputeInstance | spec.networkInterface.accessConfig.natIpRef.external | equals | null |
| compute.cnrm.cloud.google.com | ComputeInstanceTemplate | networkInterface.accessConfig.natIpRef.external | equals | null |

**Terraform:**

* Block 'create' or 'no-op' or 'update' events for resources of type "google\_compute\_instance" and “google\_compute\_instance\_template” where field 'network\_interface -> access\_config ' is populated (Omit to ensure that the instance is not accessible from the Internet)
* Do nothing for ‘delete’ events
* Ignore the allow list if the ‘project’ is in the exemption list -> i.e., do not enforce the rule if the ‘project’ is in an exemption list.

ComputeInstance

resource "google\_compute\_instance" "default" {

name = "test"

machine\_type = "e2-medium"

zone = "us-central1-a"

network\_interface {

network = "default"

access\_config {

// Ephemeral public IP

}

}

}

    "resource\_changes": [

        {

            "type": "google\_compute\_instance",

            "change": {

                "actions": [

                    "create"

                ],

                "before": null,

                "after": {

                    "network\_interface": [

                        {

                            "access\_config": [], #Notice access\_config is empty

                            "alias\_ip\_range": [],

                            "ipv6\_access\_config": [],

                            "network": "default",

                            "nic\_type": null,

                            "queue\_count": null

                        }

                    ],

ComputeInstanceTemplate

    "resource\_changes": [

        {

            "type": "google\_compute\_instance\_template",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "network\_interface": [

                        {

                            "access\_config": [], # Access\_config is empty

                            "alias\_ip\_range": [],

                            "ipv6\_access\_config": [],

                            "network": "default",

                            "network\_ip": null,

                            "nic\_type": null,

                            "queue\_count": null

                        }

                    ],

**Google Compute Engine**

Kind: ComputeInstance

Kind: ComputeInstanceTemplate

**Prevent IP Forwarding Config**

**KCC**

* Block events for resources of type 'kind: ComputeInstance’ and ‘kind: ComputeInstanceTemplate’ where spec values do not match as described in below table
* [ComputeInstance  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstance)
* [ComputeInstanceTemplate  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstancetemplate#custom_resource_definition_properties)

ComputeInstance AND ComputeInstanceTemplate

spec:

canIpForward: false

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API** | **Kind** | **Key** | **Conditional** | **Value** |
| compute.cnrm.cloud.google.com | ComputeInstance, ComputeInstanceTemplate | spec.canIpForward | equals | False, or ignore if VM instanr project is in exemption list |

**Terraform**

* Block 'create' or 'no-op' or 'update' events for resources of type "google\_compute\_instance" and “google\_compute\_instance\_template” where field 'resource -> can\_ip\_forward' equals ‘true’ unless VM instance or project is an exemption list
* Do nothing for ‘delete’ events
* Ignore the allow list if the ‘project’ is in the exemption list -> i.e., do not enforce the rule if the ‘project’ is in an exemption list.

ComputeInstance

{

resource "google\_compute\_instance" "default" {

name = "test"

machine\_type = "e2-medium"

zone = "us-central1-a"

can\_ip\_forward = false

}

    "resource\_changes": [

        {

            "type": "google\_compute\_instance",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "can\_ip\_forward": false,

ComputeInstanceTemplate

    "resource\_changes": [

        {

            "type": "google\_compute\_instance\_template",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "can\_ip\_forward": false,

**Google Compute Engine**

Kind: ComputeInstance

Kind: ComputeInstanceTemplate

**Prevent Default SA Config**

**KCC**

* Block events for resources of type 'kind: ComputeInstance’ and ‘kind: ComputeInstanceTemplate’ where spec values do not match as described in below table
* [ComputeInstance  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstance)
* [ComputeInstanceTemplate  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstancetemplate#custom_resource_definition_properties)

ComputeInstance

spec:

serviceAccount:

serviceAccountRef:

external: gcp\_serviceaccount\_email

name: object\_name

namespace: object\_namespace

ComputeInstanceTemplate

spec:

serviceAccount:

serviceAccountRef:

name: instancetemplate-dep

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API** | **Kind** | **Key** | **Conditional** | **Value** |
| compute.cnrm.cloud.google.com | ComputeInstance, ComputeInstanceTemplate | spec.serviceAccount.serviceAccountRef.name or external | equals | Any string value - null not permitting |

**Terraform:**

* Block 'create' or 'no-op' or 'update' events for resources of type "google\_compute\_instance" and “google\_compute\_instance\_template” where field 'service\_account -> email' field exists with a string value (when directly referenced)
* Do nothing for ‘delete’ events
* Ignore the allow list if the ‘project’ is in the exemption list -> i.e., do not enforce the rule if the ‘project’ is in an exemption list.

ComputeInstance

{

resource "google\_compute\_instance" "default" {

name = "test"

machine\_type = "e2-medium"

zone = "us-central1-a"

service\_account {

# Google recommends custom service accounts that have cloud-platform scope and permissions granted via IAM Roles.

email = google\_service\_account.email

scopes = ["cloud-platform"]

}

}

}

    "resource\_changes": [

        {

            "type": "google\_compute\_instance",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "service\_account": [

                        {

                            "email": "google\_service\_account.email", #Non default

                            "scopes": [

<https://www.googleapis.com/auth/cloud-platform>

                            ] #separate rule dis-allowing cloud-platform scope

                        }

                    ],

ComputeInstanceTemplate

    "resource\_changes": [

        {

            "type": "google\_compute\_instance\_template",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "service\_account": [

                        {

                            "email": "google\_service\_account.non-default.email",

                            "scopes": [

                                "non-cloud-platform"

                            ]

                        }

                    ],

**Google Compute Engine**

Kind: ComputeInstance

Kind: ComputeInstanceTemplate

**Prevent OSLogin Config**

**KCC**

* Block events for resources of type 'kind: ComputeInstance’ and ‘kind: ComputeInstanceTemplate’ where spec values do not match as described in below table
* [ComputeInstance  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstance)
* [ComputeInstanceTemplate  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstancetemplate#custom_resource_definition_properties)

ComputeInstance and ComputeInstanceTemplate

spec:

metadata:

- key: enable-os-login

value: true

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API** | **Kind** | **Key** | **Conditional** | **Value** |
| compute.cnrm.cloud.google.com | ComputeInstance, ComputeInstanceTemplate | spec.metadata.key | Equals | enable-os-login does not exist, or when exists value = false |

**Terraform:**

* Block 'create' or 'no-op' or 'update' events for resources of type "google\_compute\_instance" and “google\_compute\_instance\_template” where field 'resource -> metadata -> enable-oslogin' is equal to true
* Do nothing for ‘delete’ events
* Ignore the allow list if the ‘project’ is in the exemption list -> i.e., do not enforce the rule if the ‘project’ is in an exemption list.

ComputeInstance

    "resource\_changes": [

        {

            "type": "google\_compute\_instance",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "metadata": {

                        "enable-oslogin": "true",

                        "foo": "bar"

                    },

ComputeInstanceTemplate

    "resource\_changes": [

        {

            "type": "google\_compute\_instance\_template",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "metadata": {

                        "enable-oslogin": "true"

                    },

**Google Compute Engine**

Kind: ComputeInstance

Kind: ComputeInstanceTemplate

**Enable vTPM, Secure Boot, Integrity Monitoring Config**

**KCC**

* Block events for resources of type 'kind: ComputeInstance’ and ‘kind: ComputeInstanceTemplate’ where spec values do not match as described in below table
* [ComputeInstance  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstance)
* [ComputeInstanceTemplate  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstancetemplate#custom_resource_definition_properties)

ComputeInstance AND ComputeInstanceTemplate

shieldedInstanceConfig:

enableIntegrityMonitoring: true

enableSecureBoot: true

enableVtpm: true

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API** | **Kind** | **Key** | **Conditional** | **Value** |
| compute.cnrm.cloud.google.com | ComputeInstance, ComputeInstanceTemplate | spec.shieldedInstanceConfig.enableIntegrityMonitoring | equals | true |
| compute.cnrm.cloud.google.com | ComputeInstance, ComputeInstanceTemplate | spec.shieldedInstanceConfig.enableSecureBoot | equals | true |
| compute.cnrm.cloud.google.com | ComputeInstance, ComputeInstanceTemplate | spec.shieldedInstanceConfig.enableVtpm | equals | true |

**Terraform:**

* Block 'create' or 'no-op' or 'update' events for resources of type "google\_compute\_instance" and “google\_compute\_instance\_template” where field 'shielded\_instance\_config -> enable\_secure\_boot, enable\_vtpm, enable\_integrity\_monitoring' fields are not equal to true
* Do nothing for ‘delete’ events
* Ignore the allow list if the ‘project’ is in the exemption list -> i.e., do not enforce the rule if the ‘project’ is in an exemption list.

ComputeInstance

resource "google\_compute\_instance" "default" {

name = "test"

machine\_type = "e2-medium"

zone = "us-central1-a"

shielded\_instance\_config {

enable\_secure\_boot = true,

enable\_vtpm = true,

enable\_integrity\_monitoring = true

}

}

    "resource\_changes": [

        {

            "type": "google\_compute\_instance",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "shielded\_instance\_config": [

                        {

                            "enable\_integrity\_monitoring": true,

                            "enable\_secure\_boot": true,

                            "enable\_vtpm": true

                        }

                    ],

ComputeInstanceTemplate

    "resource\_changes": [

        {

            "type": "google\_compute\_instance\_template",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "shielded\_instance\_config": [

                        {

                            "enable\_integrity\_monitoring": true,

                            "enable\_secure\_boot": true,

                            "enable\_vtpm": true

                        }

                    ],

**Google Compute Engine**

Kind: ComputeInstance

Kind: ComputeInstanceTemplate

**CMEK for Persistent Disks Config**

**KCC**

* Block events for resources of type 'kind: ComputeInstance’ and ‘kind: ComputeInstanceTemplate’ where spec values do not match as described in below table
* [ComputeInstance  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstance)
* [ComputeInstanceTemplate  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstancetemplate#custom_resource_definition_properties)

ComputeInstance

bootDisk:

kmsKeyRef:

external: string

name: string

namespace: string

attachedDisk:

kmsKeyRef:

external: string

name: string

namespace: string

ComputeInstanceTemplate

disk:

diskEncryptionKey:

kmsKeyRef:

external: string

name: string

namespace: string

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API** | **Kind** | **Key** | **Conditional** | **Value** |
| compute.cnrm.cloud.google.com | ComputeInstance | bootDisk.kmsKeyRef | Must exist | External or name fields must exist to set CMEK key |
| compute.cnrm.cloud.google.com | ComputeInstance | attachedDisk.kmsKeyRef | Must exist | External or name fields must exist to set CMEK key |
| compute.cnrm.cloud.google.com | ComputeInstanceTemplate | disk.diskEncryption.kmsKeyRef | Must exist | External or name fields must exist to set CMEK key |

**Terraform:**

* Block 'create' or 'no-op' or 'update' events for resources of type "google\_compute\_instance" and “google\_compute\_instance\_template” where field 'boot\_disk -> kms\_key\_self\_link, or attached\_disk -> kms\_key\_self\_link' fields don’t use CMEK for persistent disks (boot\_disk required, attached\_disk field may not exist but CMEK is required if it does exist)
* Do nothing for ‘delete’ events
* Ignore the allow list if the ‘project’ is in the exemption list -> i.e., do not enforce the rule if the ‘project’ is in an exemption list.

ComputeInstance

{

resource "google\_compute\_instance" "default" {

name = "test"

machine\_type = "e2-medium"

zone = "us-central1-a"

boot\_disk {

initialize\_params {

image = "debian-cloud/debian-9"

}

kms\_key\_self\_link = \_\_\_\_\_\_\_\_\_\_

}

attached\_disk {

kms\_key\_self\_link = \_\_\_\_\_\_\_\_

}

}

}

    "resource\_changes": [

        {

            "type": "google\_compute\_instance",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "attached\_disk": [

                        {

                            "kms\_key\_self\_link": "CMEK Key",

                            "source": "Approved Image"

                        }

                    ],

                    "boot\_disk": [

                        {

                            "initialize\_params": [

                                {

                                    "image": "debian-cloud/debian-9"

                                }

                            ],

                            "kms\_key\_self\_link": "CMEK Key",

                        }

                    ],

ComputeInstanceTemplate

    "resource\_changes": [

        {

            "type": "google\_compute\_instance\_template",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "disk": [

                        {

                            "disk\_encryption\_key": [

                                {

                                    "kms\_key\_self\_link": "CMEK Key"

                                }

                            ],

                        }

                    ],

**Google Compute Engine**

Kind: ComputeInstance

Kind: ComputeInstanceTemplate

**Block Cloud-Platform Access Scopes Config**

**KCC**

* Block events for resources of type 'kind: ComputeInstance’ and ‘kind: ComputeInstanceTemplate’ where spec values do not match as described in below table
* [ComputeInstance  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstance)
* [ComputeInstanceTemplate  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstancetemplate#custom_resource_definition_properties)

ComputeInstance AND ComputeInstanceTemplate

spec:

serviceAccount:

scopes:

- string

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API** | **Kind** | **Key** | **Conditional** | **Value** |
| compute.cnrm.cloud.google.com | ComputeInstance, ComputeInstanceTemplate | spec.serviceAccount.scopes | Not equal | ‘cloud-platform’ |

**Terraform:**

* Block 'create' or 'no-op' or 'update' events for resources of type "google\_compute\_instance" and “google\_compute\_instance\_template” where field 'resource -> service\_account -> scopes' is equal to ‘cloud-platform’
* Do nothing for ‘delete’ events
* Ignore the allow list if the ‘project’ is in the exemption list -> i.e., do not enforce the rule if the ‘project’ is in an exemption list.

ComputeInstance

{

resource "google\_compute\_instance" "default" {

name = "test"

machine\_type = "e2-medium"

zone = "us-central1-a"

service\_account {

# Google recommends custom service accounts that have cloud-platform scope and permissions granted via IAM Roles.

email = google\_service\_account.default.email

scopes = ["cloud-platform"]

}

}

    "resource\_changes": [

        {

            "type": "google\_compute\_instance",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "service\_account": [

                        {

                            "email": "google\_service\_account.email",

                            "scopes": [

                                “cloud-platform”

                            ]

ComputeInstanceTemplate

    "resource\_changes": [

        {

            "type": "google\_compute\_instance\_template",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "service\_account": [

                        {

                            "email": "google\_service\_account.non-default.email",

                            "scopes": [

                                "cloud-platform"

                            ]

                        }

                    ],

**Google Compute Engine**

Kind: ComputeInstance

Kind: ComputeInstanceTemplate

**Disallow use of Local SSD Config**

“Scratch Disks” – aka Local SSD’s – do not support KMS encryption keys.

**KCC**

* Block events for resources of type 'kind: ComputeInstance’ and ‘kind: ComputeInstanceTemplate’ where spec values do not match as described in below table
* [ComputeInstance  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstance)
* [ComputeInstanceTemplate  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstancetemplate#custom_resource_definition_properties)

ComputeInstance

spec:

scratchDisk:

- interface:

ComputeInstanceTemplate

spec:

disk:

diskType: local-ssd

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API** | **Kind** | **Key** | **Conditional** | **Value** |
| compute.cnrm.cloud.google.com | ComputeInstance | spec.scratchDisk.interface | Not Exist | Should not be attached so field should not exist |
| compute.cnrm.cloud.google.com | ComputeInstanceTemplate | spec.disk.diskType | Not equal | local-ssd |

**Terraform:**

* Block 'create' or 'no-op' or 'update' events for resources of type "google\_compute\_instance" and “google\_compute\_instance\_template” where field 'resource -> scratch\_disk’ exists (no Local SSD’s attached)
* Do nothing for ‘delete’ events
* Ignore the allow list if the ‘project’ is in the exemption list -> i.e., do not enforce the rule if the ‘project’ is in an exemption list.

ComputeInstance

{

resource "google\_compute\_instance" "default" {

name = "test"

machine\_type = "e2-medium"

zone = "us-central1-a"

scratch\_disk {

interface = “SCSI”

}

    "resource\_changes": [

        {

            "type": "google\_compute\_instance",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "scratch\_disk": [

                        {

                            "interface": "SCSI"

                        }

                    ],

ComputeInstanceTemplate

    "resource\_changes": [

        {

            "type": "google\_compute\_instance\_template",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "disk": [

                        {

                            "interface": "SCSI"

                        }

                    ],

**Google Compute Engine**

Kind: ComputeInstance

Kind: ComputeInstanceTemplate

**Require ‘block-project-ssh-keys’ Config**

**KCC**

* Block events for resources of type 'kind: ComputeInstance’ and ‘kind: ComputeInstanceTemplate’ where spec values do not match as described in below table
* [ComputeInstance  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstance)
* [ComputeInstanceTemplate  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstancetemplate#custom_resource_definition_properties)

ComputeInstance

spec:

metadata:

- key: block-project-ssh-keys

value: true

ComputeInstanceTemplate

metadata:

- key: block-project-ssh-keys

value: true

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API** | **Kind** | **Key** | **Conditional** | **Value** |
| compute.cnrm.cloud.google.com | ComputeInstance | spec.metadata.key / .value | equals | block-project-ssh-keys / true |
| compute.cnrm.cloud.google.com | ComputeInstanceTemplate | spec.metadata.key / .value | equals | block-project-ssh-keys / true |

**Terraform:**

* Block 'create' or 'no-op' or 'update' events for resources of type "google\_compute\_instance" and “google\_compute\_instance\_template” where field 'resource -> metadata -> block\_project\_ssh\_keys’ is not equal to “true”
* Do nothing for ‘delete’ events
* Ignore the allow list if the ‘project’ is in the exemption list -> i.e., do not enforce the rule if the ‘project’ is in an exemption list.

ComputeInstance

{

resource "google\_compute\_instance" "default" {

name = "test"

machine\_type = "e2-medium"

zone = "us-central1-a"

metadata {

block\_project\_ssh\_keys = “true”

}

}

    "resource\_changes": [

        {

            "type": "google\_compute\_instance",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "metadata": {

                        "block\_project\_ssh\_keys": "true",

                    },

ComputeInstanceTemplate

    "resource\_changes": [

        {

            "type": "google\_compute\_instance\_template",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "metadata": {

                        "block\_project\_ssh\_keys": "true"

                    },

**Google Compute Engine**

Kind: ComputeInstance

Kind: ComputeInstanceTemplate

**Block Virtual Displays Config**

**KCC**

* Block events for resources of type 'kind: ComputeInstance’ and ‘kind: ComputeInstanceTemplate’ where spec values do not match as described in below table
* [ComputeInstance  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstance)
* [ComputeInstanceTemplate  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computeinstancetemplate#custom_resource_definition_properties)

ComputeInstance

Spec:

enableDisplay: false

ComputeInstanceTemplate

sepc:

enableDisplay: false

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API** | **Kind** | **Key** | **Conditional** | **Value** |
| compute.cnrm.cloud.google.com | ComputeInstance | spec.enableDisplay | equal | false |
| compute.cnrm.cloud.google.com | ComputeInstanceTemplate | spec.enableDisplay | equal | false |

**Terraform:**

* Block 'create' or 'no-op' or 'update' events for resources of type "google\_compute\_instance" and “google\_compute\_instance\_template” where field 'resource -> enable\_display' is not equal to “false”
* Do nothing for ‘delete’ events
* Ignore the allow list if the ‘project’ is in the exemption list -> i.e., do not enforce the rule if the ‘project’ is in an exemption list.

ComputeInstance

{

resource "google\_compute\_instance" "default" {

name = "test"

machine\_type = "e2-medium"

zone = "us-central1-a"

enable\_display = false

}

    "resource\_changes": [

        {

            "type": "google\_compute\_instance",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "enable\_display": false,

                    },

ComputeInstanceTemplate

**Google Compute Engine**

Kind: ComputeDisk

**CMEK for Persistent Disks Config**

**KCC**

* Block events for resources of type 'kind: ComputeDisk’ where spec values do not match as described in below table
* [ComputeDisk  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computedisk)

ComputeDisk

spec:

diskEncryptionKey:

kmsKeyRef:

external: string

name: string

namespace: string

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API** | **Kind** | **Key** | **Conditional** | **Value** |
| compute.cnrm.cloud.google.com | ComputeDisk | spec.diskEncryptionKey.kmsKeyRef.external/name/namespace | equal | External or name must exist |

**Terraform:**

* Block 'create' or 'no-op' or 'update' events for resources of type "google\_compute\_disk" where field 'resource -> disk\_encryption\_key -> kms\_key\_self\_link’ is not populated
* Do nothing for ‘delete’ events
* Ignore the allow list if the ‘project’ is in the exemption list -> i.e., do not enforce the rule if the ‘project’ is in an exemption list.

ComputeDisk

resource "google\_compute\_disk" "default" {

name = "test-disk"

type = "pd-ssd"

zone = "us-central1-a"

image = "debian-9-stretch-v20200805"

labels = {

environment = "dev"

}

physical\_block\_size\_bytes = 4096

disk\_ecryption\_key {

kms\_key\_self\_link = “”

}

}

    "resource\_changes": [

        {

            "type": "google\_compute\_disk",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "disk\_encryption\_key": [

                        {

                            "kms\_key\_self\_link": "CMEK Key",

                            "kms\_key\_service\_account": null,

                            "raw\_key": null

                        }

                    ],

**Google Compute Engine**

Kind: ComputeDisk

**Approved Imaged for Persistent Disks Config**

**KCC**

* Block events for resources of type 'kind: ComputeDisk’ where spec values do not match as described in below table
* [ComputeDisk  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computedisk)

ComputeDisk

spec:

imageRef:

external: string

name: string

namespace: string

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API** | **Kind** | **Key** | **Conditional** | **Value** |
| compute.cnrm.cloud.google.com | ComputeDisk | spec.imageRef.external/name/namespace | equal | Approved images |

**Terraform:**

* Block 'create' or 'no-op' or 'update' events for resources of type "google\_compute\_disk" where field 'resource -> image’ is equal to an approved image
* Do nothing for ‘delete’ events
* Ignore the allow list if the ‘project’ is in the exemption list -> i.e., do not enforce the rule if the ‘project’ is in an exemption list.

ComputeDisk

resource "google\_compute\_disk" "default" {

name = "test-disk"

type = "pd-ssd"

zone = "us-central1-a"

image = "approved-image"

labels = {

environment = "dev"

}

physical\_block\_size\_bytes = 4096

}

    "resource\_changes": [

        {

            "type": "google\_compute\_disk",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "image": "Approved Images",

                    },

**Google Compute Engine**

Kind: ComputeDisk

**Disallow use of Local SSD Config**

**KCC**

* Block events for resources of type 'kind: ComputeDisk’ where spec values do not match as described in below table
* [ComputeDisk  |  Config Connector Documentation  |  Google Cloud](https://cloud.google.com/config-connector/docs/reference/resource-docs/compute/computedisk)

ComputeDisk

spec:

type: pd-ssd

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **API** | **Kind** | **Key** | **Conditional** | **Value** |
| compute.cnrm.cloud.google.com | ComputeDisk | spec.type | Not equal | local-ssd |

**Terraform:**

* Block 'create' or 'no-op' or 'update' events for resources of type "google\_compute\_disk" where field 'resource -> type’ is equal to “local-ssd”
* Do nothing for 'delete' events

ComputeDisk

resource "google\_compute\_disk" "default" {

name = "test-disk"

type = "local-ssd"

zone = "us-central1-a"

image = " debian-9-stretch-v20200805"

labels = {

environment = "dev"

}

physical\_block\_size\_bytes = 4096

}

    "resource\_changes": [

        {

            "type": "google\_compute\_disk",

            "change": {

                "actions": [

                    "create"

                ],

                "after": {

                    "type": "local-ssd", #block local-ssd

                },