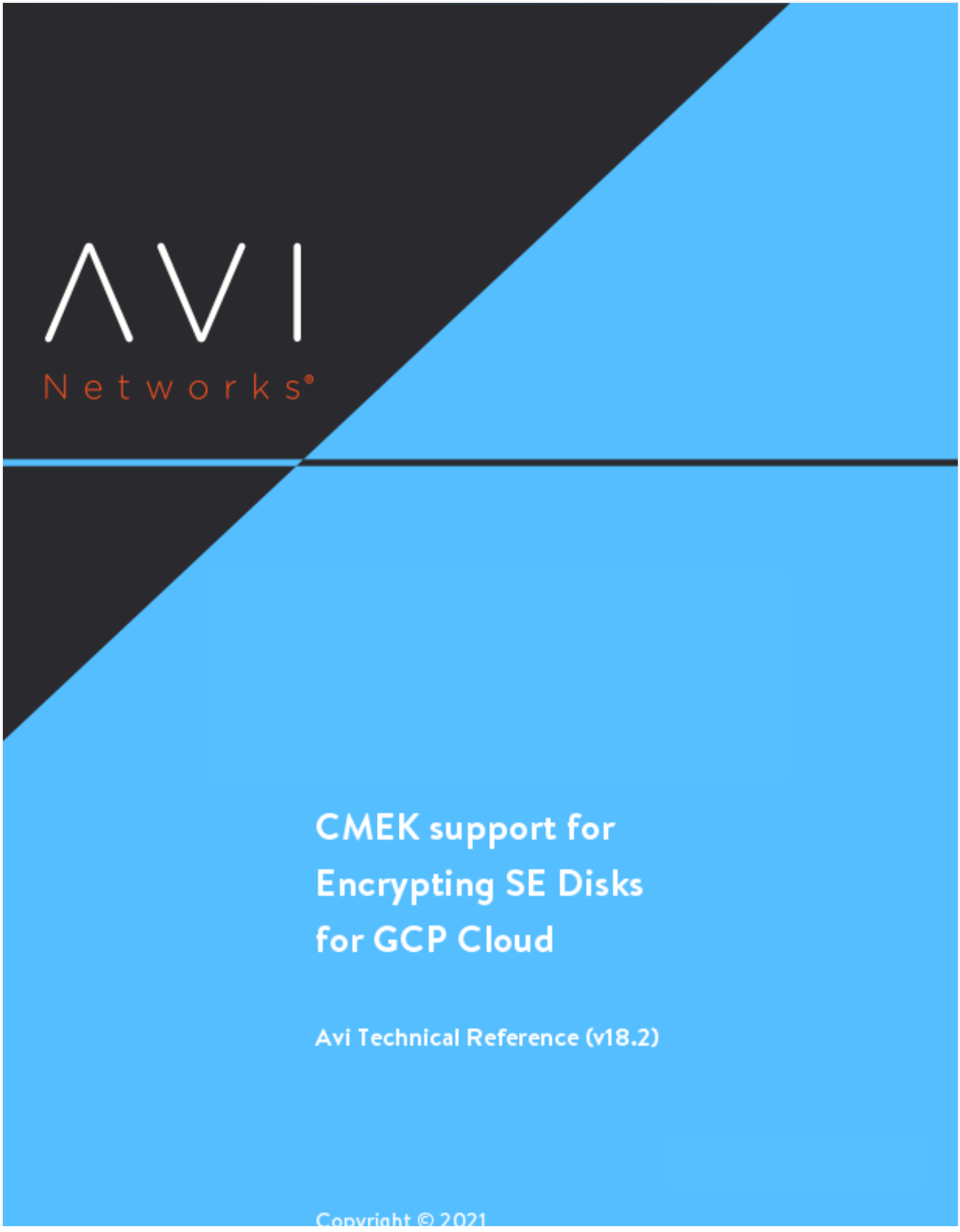

CMEK support for Encrypting SE Disks for GCP Cloud

Avi Technical Reference (v18.2)

CMEK support for Encrypting SE Disks for GCP Cloud

view online

Overview

This article describes the Customer Managed Encryption Key (CMEK) support for encrypting Service Engine (SE) disks for GCP cloud.

Avi GCP Cloud supports encryption of the following resources. Different encryption keys are supported for each resource.

- The GCS bucket created to upload the raw SE image file
- RAW SE image which is uploaded as GCS object
- The GCP image created out of the raw image
- The SE disk when SE is created

When keys are added to the cloud configuration, the cloud connector will check for its presence and permissions of the keys. In case validation for any key fails, the cloud will go to failed state. If the SE disk encryption key is deleted from the cloud after SEs are created, the corresponding SEs will fail to boot up if it shuts down later.

Prerequisites

Follow the steps below before using CMEK:

1. Create a key in Google's KMS
2. Provide permissions to Avi cloud service account to use one of the following keys:
    a. cloudkms.cryptoKeys.get, or
    b. role: roles/cloudkms.admin
3. Provide permissions to the following service accounts to enable Google compute and storage to use the key to encrypt/decrypt data:
    a. Permission
        i. cloudkms.cryptoKeyVersions.useToEncrypt
        ii. cloudkms.cryptoKeyVersions.useToDecrypt, or
        iii. role: roles/cloudkms.cryptoKeyEncrypterDecrypter
    b. For GCS Object and Bucket encryption key the following member should have above permissions
    i. service-[PROJECT_NUMBER]@gs-project-accounts.iam.gserviceaccount.com
    c. For SE Image and Disk encryption key the following member should have above permissions
    i. service-[PROJECT_NUMBER]@compute-system.iam.gserviceaccount.com

Cloud Configuration

To configure encryption key set the `encryption_keys` field in the GCP cloud configuration.

The encryption key can be in any GCP project independent of the SE project, but should be in the same region as the SE or it can be global. The kms key ID should be in following format `projects/project-id/locations/region/keyRings/key-ring-name/cryptoKeys/key-name`

Configuration Fields

The following are the configuration fields:

```
gcs_bucket_kms_key_id    CMEK Resource ID to encrypt Google Cloud Storage Bucket. This Bucket is used to upload Service
gcs_objects_kms_key_id   CMEK Resource ID to encrypt Service Engine raw image. The raw image is a Google Cloud Storage
se_disk_kms_key_id       CMEK Resource ID to encrypt Service Engine Disks.
se_image_kms_key_id      CMEK Resource ID to encrypt Service Engine GCE Image.
```

Configuring GCP Cloud

While configuring the Google cloud, you need a key to be used for encryption. You can provide the key ID in an URI format as follows:

The following is the CLI format:

```
[admin:10-138-10-66]: > configure cloud gcp-cloud
[admin:10-138-10-66]: cloud> gcp_configuration
[admin:10-138-10-66]: cloud:gcp_configuration> encryption_keys
[admin:10-138-10-66]: cloud:gcp_configuration:encryption_keys> se_disk_kms_key_id projects/kms-project/locations/us-cen
[admin:10-138-10-66]: cloud:gcp_configuration:encryption_keys> gcs_bucket_kms_key_id projects/kms-project/locations/us-
[admin:10-138-10-66]: cloud:gcp_configuration:encryption_keys> se_image_kms_key_id projects/kms-project/locations/us-ce
[admin:10-138-10-66]: cloud:gcp_configuration:encryption_keys> gcs_objects_kms_key_id projects/kms-project/locations/us
[admin:10-138-10-66]: cloud:gcp_configuration:encryption_keys> save
save[admin:10-138-10-66]: cloud:gcp_configuration> save
[admin:10-138-10-66]: cloud> save
+----------------------------+-----------------------------------------------------------------------------------+
| Field                      | Value                                                                             |
+----------------------------+-----------------------------------------------------------------------------------+
| uuid                       | cloud-d4513a65-0907-4f67-b75f-bb47a6990423                                        |
| name                       | gcp-cloud                                                                         |
| vtype                      | CLOUD_GCP                                                                         |
| apic_mode                  | False                                                                             |
| gcp_configuration          |                                                                                   |
|   cloud_credentials_ref    | gcp-creds                                                                         |
|   region_name              | us-central1                                                                       |
|   zones[1]                 | us-central1-a                                                                     |
|   zones[2]                 | us-central1-b                                                                     |
|   se_project_id            | development-237409                                                                |
|   network_config           |                                                                                   |
|     config                 | INBAND_MANAGEMENT                                                                 |
|     inband                 |                                                                                   |
|       vpc_subnet_name      | subnet-1                                                                          |
|       vpc_project_id       | net-project                                                                       |
|       vpc_network_name     | net-1                                                                             |
|   vip_allocation_strategy  |                                                                                   |
|     mode                   | ROUTES                                                                            |
|     routes                 |                                                                                   |
|       match_se_group_subnet| False                                                                             |
```

```
|   encryption_keys            |                                                                                    |
|     se_image_kms_key_id      | projects/kms-project/locations/us-central1/keyRings/keyring/cryptoKeys/se-image    |
|     se_disk_kms_key_id       | projects/kms-project/locations/us-central1/keyRings/keyring/cryptoKeys/se-disk     |
|     gcs_bucket_kms_key_id    | projects/kms-project/locations/us-central1/keyRings/keyring/cryptoKeys/bucket      |
|     gcs_objects_kms_key_id   | projects/kms-project/locations/us-central1/keyRings/keyring/cryptoKeys/se-raw      |
| dhcp_enabled                 | True                                                                               |
| mtu                          | 1500 bytes                                                                         |
| prefer_static_routes         | False                                                                              |
| enable_vip_static_routes     | False                                                                              |
| license_type                 | LIC_CORES                                                                          |
| ipam_provider_ref            | ipam-gcp-cloud                                                                      |
| state_based_dns_registration | True                                                                               |
| ip6_autocfg_enabled          | False                                                                              |
| dns_resolution_on_se         | False                                                                              |
| enable_vip_on_all_interfaces | False                                                                              |
| tenant_ref                   | admin                                                                              |
| license_tier                 | ENTERPRISE_18                                                                      |
| autoscale_polling_interval   | 60 seconds                                                                         |
+------------------------------+------------------------------------------------------------------------------------+
}
```

Modifying the Encryption Options

You can modify the encryption options on a cloud that is already created. The modifications include:

1. Enabling/Disabling encryption
2. Changing the key for encryption

You can update the SE disk encryption key only if there are no SEs created for the GCP cloud.

Other encryption key can be changed at any point of time. SE image will be recreated in GCP with new encryption key if SE Image encryption key is updated.

Note the following:

1. Key format should be in URI format.
2. SE Disk encryption key modification allowed only if no SEs are created.
3. Key region must be checked. It should be in the same region as the SEs or be global. You can copy the key ID from the Disk Encryption Key field in the GCP console as shown below.

Additional Reading

- Using CMEK ? Customer Managed Encryption
- Permissions for CMEK ? Using Customer managed Keys
- Protecting Resources with Cloud KMS Keys ? Customer Managed Keys
- Restricting Encrypt Permission to Service Account ? Permission denied on cloud KMS key while using cloud storage