Cortex XDR Endpoint Verification for Google BeyondCorp Marketplace Deployment User Guide

PRE-REQUIREMENTS

- **Enable APIs:**
  - Used in deployment:
    - Pub/Sub
    - Scheduler
    - Cloud Functions
    - Cloud Spanner
  - Used for deployment:
    - Compute Engine
    - Cloud Build
    - Cloud Deployment Manager V2
    - Cloud Runtime Configuration
  - Used by integration:
    - Cloud Identity
- **Grant below two service accounts necessary roles for the build:**
  - PROJECT_ID-compute@developer.gserviceaccount.com -add storage object admin IAM role
  - PROJECT_ID@cloudservices.gserviceaccount.com - add storage object admin IAM role
- **Enable IAP access control**
- **License from Google:**
  - Cloud Identity Premium
  - BeyondCorp Enterprise

Overview

Google announced BeyondCorp Remote Access, a cloud-based solution that helps make access to internal applications easier and more secure. Palo Alto Networks partners with Google to enhance the Zero Trust security in consideration of the risk factors of remote users' endpoint devices. Cortex XDR Endpoint Verification for Google

BeyondCorp by Palo Alto Networks provides XDR endpoint risk exposures rating to Google Endpoint Management. Cortex XDR Endpoint Verification allows you control your critical applications access based on XDR endpoint risk exposure rating.

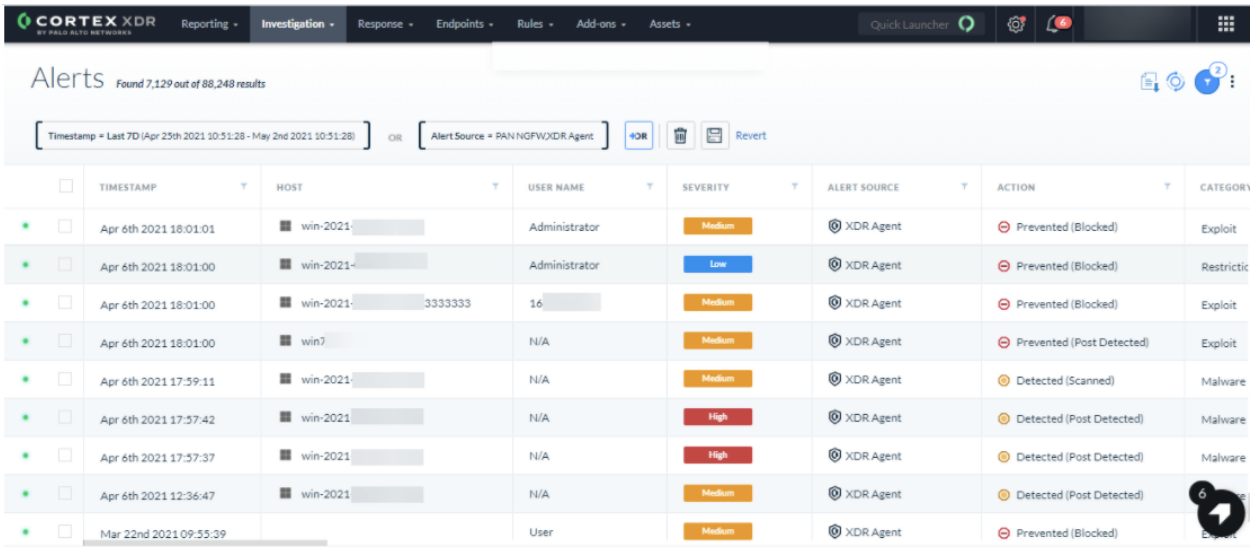
Cortex XDR and XDR Health Score for Endpoint

Cortex® XDR™ is the world's first extended detection and response platform that gathers and integrates all security data to stop sophisticated attacks. It unifies prevention, detection, investigation, and response in one platform for unrivaled security and operational efficiency.

The Cortex XDR agent safeguards endpoints from malware, exploits, and fileless attacks with industry-best, AI-driven local analysis and behavior-based protection. Organizations can stop never-before-seen threats with a single cloud-delivered agent for endpoint protection, detection, and response.

XDR Health Score for Endpoint

Cortex XDR Alerts page consolidates non-informational alerts from your detection sources including the XDR agents running at the endpoints.



Cortex XDR Endpoint Verification calculates XDR Health Score for each endpoint and stores it in a database at your Google Cloud project. The calculation uses the number of incidents and the serenity of the incident associated with an endpoint. Here is the possible XDR Health Score:

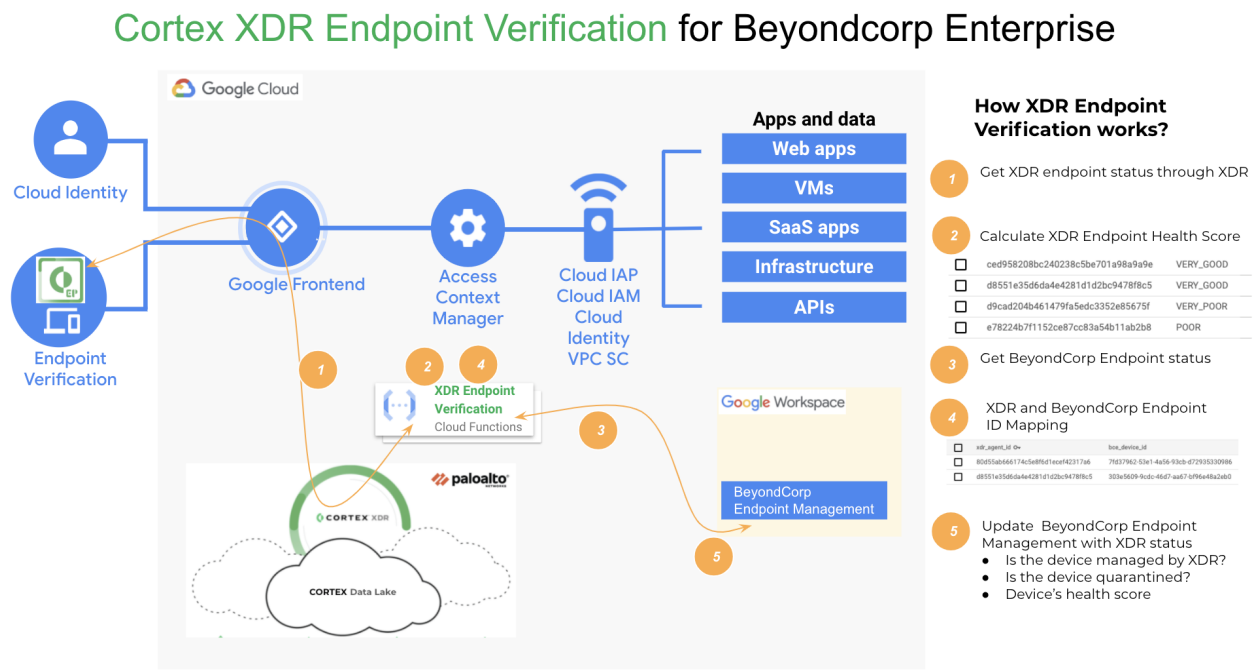
- Very Good
- Good
- Neutral

- Poor
- Very Poor

XDR endpoint security risk exposure rating is calculated base on the following factors:

1. Is the endpoint managed by Cortex XDR?
2. Is the endpoint quarantined by the Cortex XDR administrator?
3. What is the XDR Health Score?

Cortex XDR Endpoint Verification for Google BeyondCorp Architecture



Cortex XDR and Cortex Data Lake are cloud services provided by Palo Alto Networks and are running in Google Cloud. Cortex XDR manages XDR agents that are deployed to users endpoint devices. Cortex XDR Endpoint Verification is deployed as Cloud Functions to your Google Cloud project. Cortex XDR Endpoint Verification calculates the health score for XDR Endpoints based on the severity and the number of the alerts at the endpoint. Cortex XDR Endpoint Verification maps XDR agent ID to the device ID at Google Admin Endpoint Management. Cortex XDR Endpoint Verification updates the device status Google Admin Endpoint Management with XDR agent status.

Once you enable Cortex XDR Endpoint Verification as a Device Partner's Service at your Google Admin Site, you will be able to create an Access Level at Access Context Manager (ACM) based on Cortex XDR Endpoint risk factors:

- If the endpoint is a XDR managed device
- If the endpoint is quarantined by XDR administrator
- The minimum level for the endpoint health score.

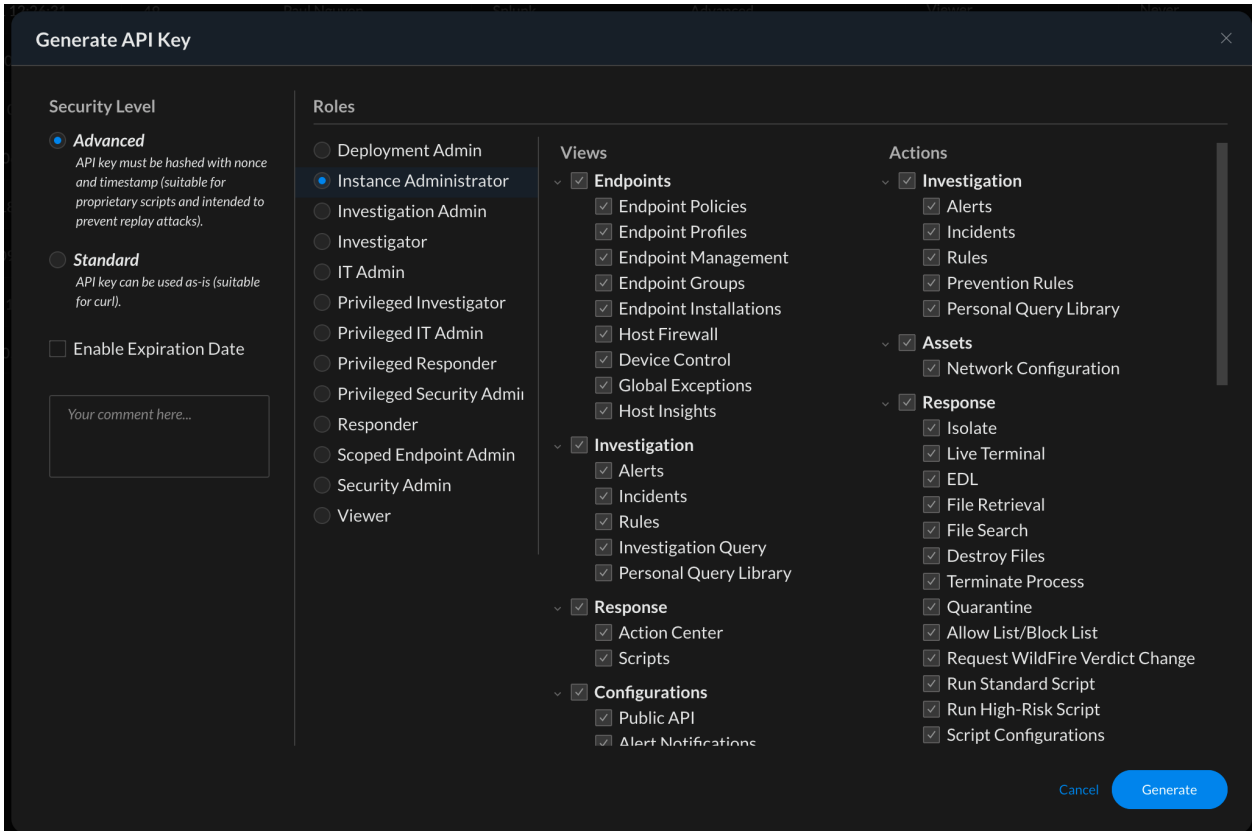
This enables you to control the application access in IAP using the Cortex XDR Endpoint Access Level you created in ACM.

Prepare your Cortex XDR

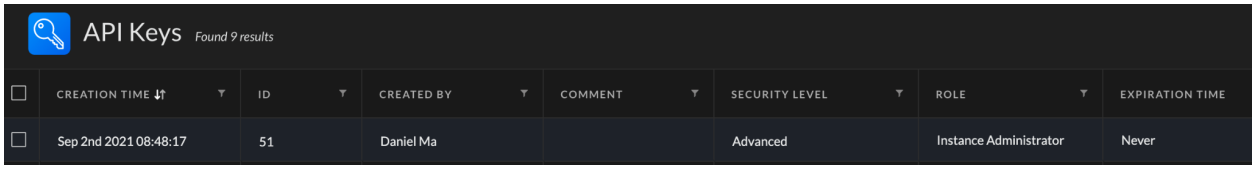
Create API key needed for the cloud function to integrate with Cortex XDR.

1. Go to XDR console
2. Go to Settings -> Configurations->Integrations-> API Keys
3. Click "+New Keys" at the top right
4. In the Generate API Key page, choose Security Level to be "Advanced" (this is for additional security, which requested the API Key be hashed with nonce and timestamp to prevent replay attacks). Choose Roles to be "Instance Administrator". Then click

“Generate”.



5. Copy the generated API key, and save it locally. (This key will not be access again, after you close the window)
6. And also copy the key ID, this will be needed later during the cloud function terraform deployment. (As example, the ID is 51)



7. Now you have done what you needed in XDR.

Deploy Cortex XDR Endpoint Verification to your Google Cloud project

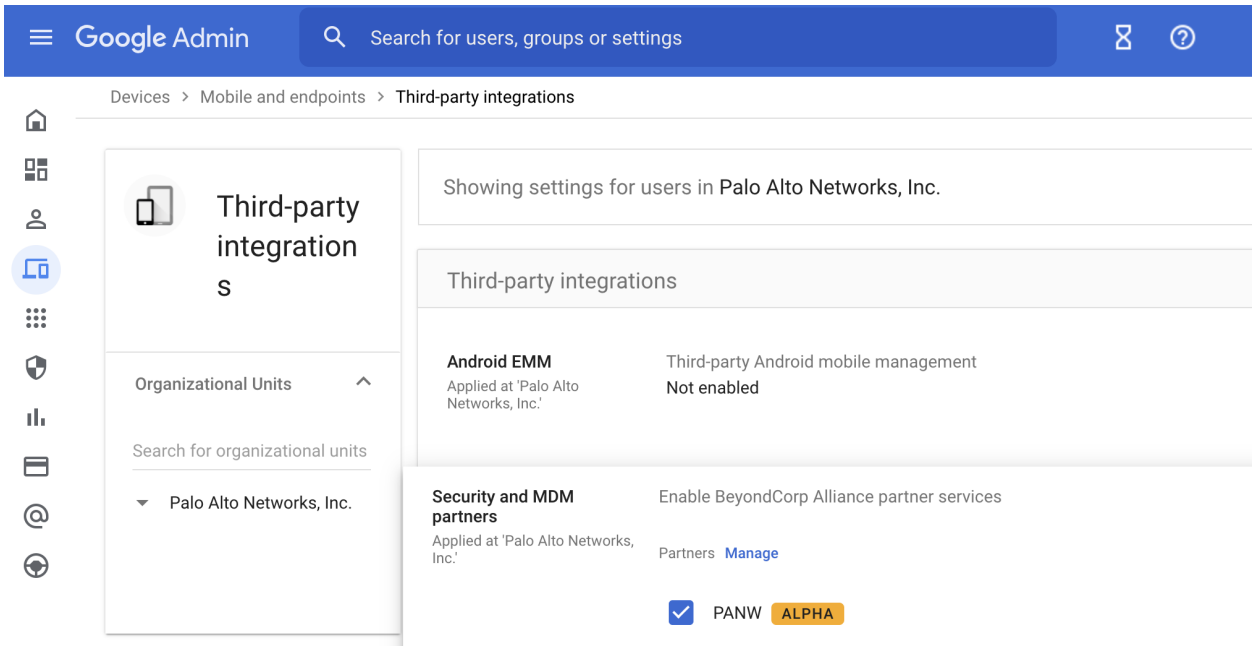
Cortex XDR Endpoint Verification Components

Deploy Cortex XDR Endpoint Verification

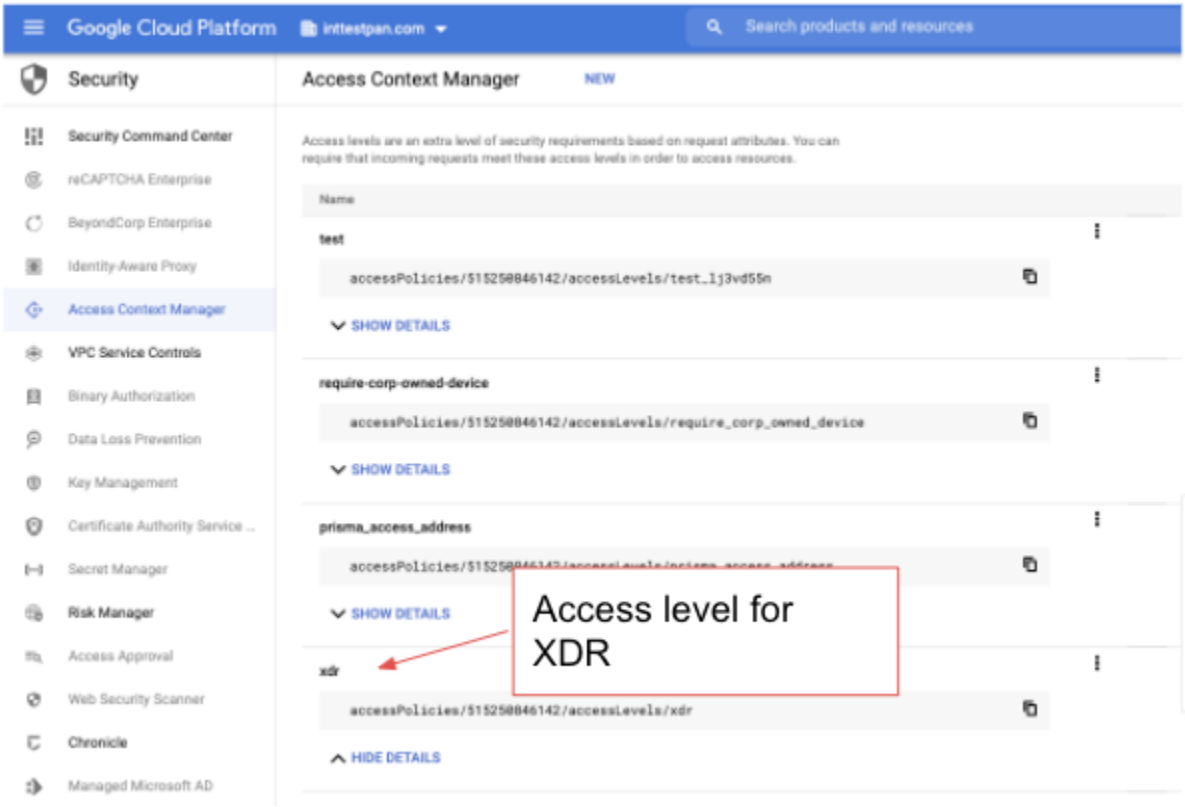
Configure Cortex XDR Endpoint Verification

Enable Cortex XDR Endpoint Verification as a Partner Service at your Workspace Google Admin. You would need to contact Google to whitelist the integration for your Org.

Then, you can go through the google Admin Portal, Device -> Mobile & endpoints -> Settings -> Third-party integrations, to enable the integration.



Create Custom Access Level at ACM

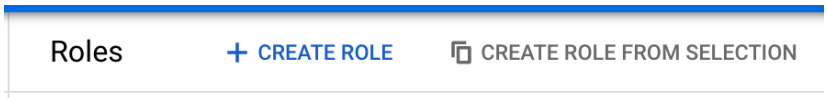


Example:
device.vendors["PANW"].is_compliant_device == true && device.vendors["PANW"].is_managed_device == true && device.vendors["PANW"].device_health_score == DeviceHealthScore.VERY_GOOD

Configure Google Cloud Service Account, and secret key

This secret key will be needed by the Cloud Function (will be created later by the Marketplace installation) to communicate with the Google Workspace API.

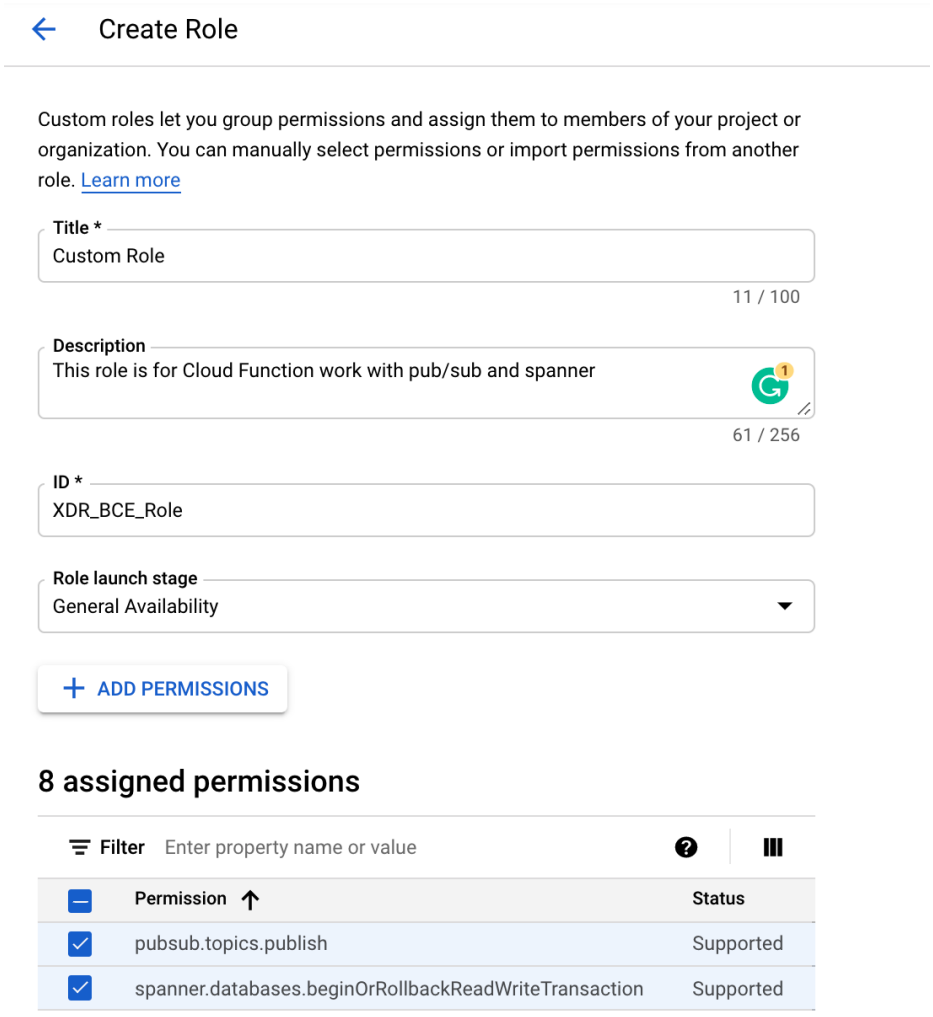
1. Create Custom Role in IAM, go to IAM & Admin -> Roles, click “+ CREATE ROLE”:



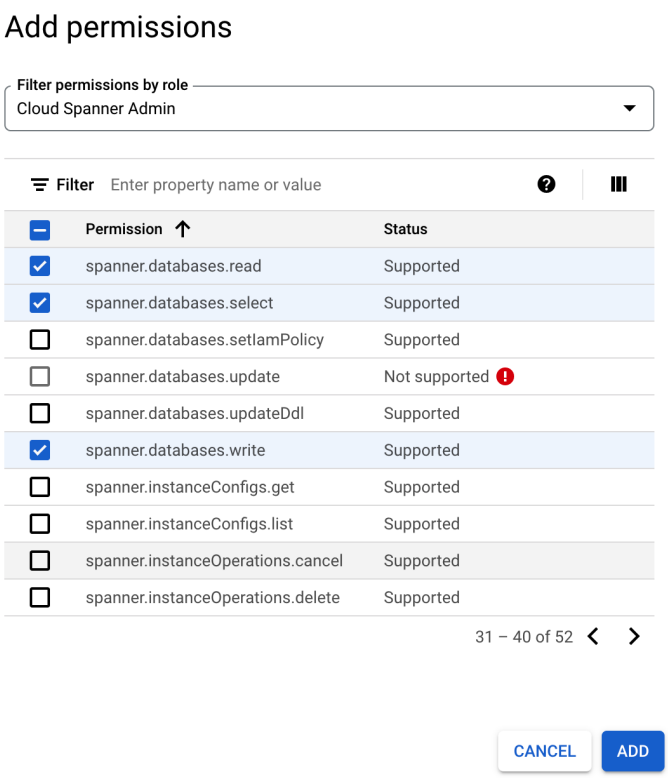
needed permission:

- pubsub.topics.publish
- spanner.databases.beginOrRollbackReadWriteTransaction
- spanner.databases.read

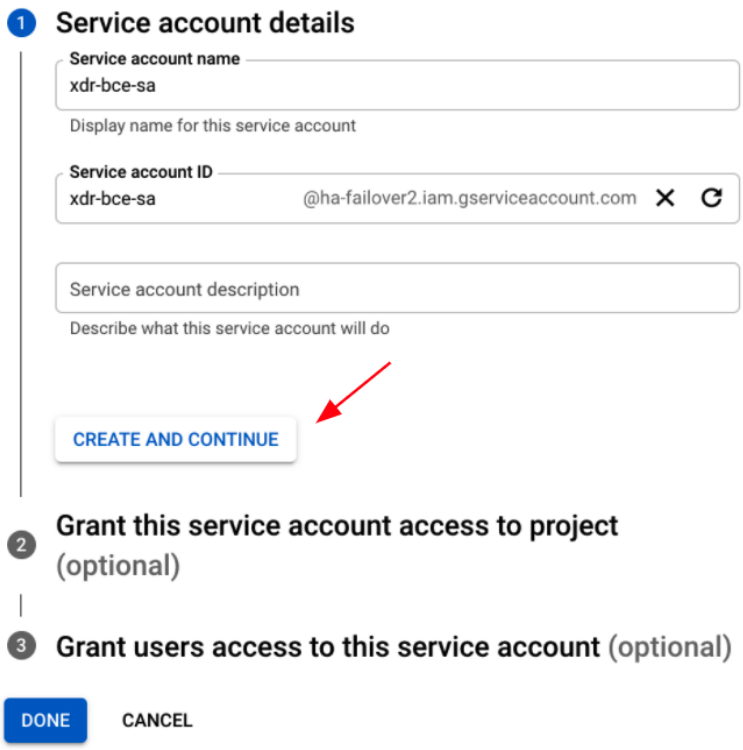
- spanner.databases.select
- spanner.databases.write
- spanner.instances.get
- spanner.sessions.create
- spanner.sessions.get

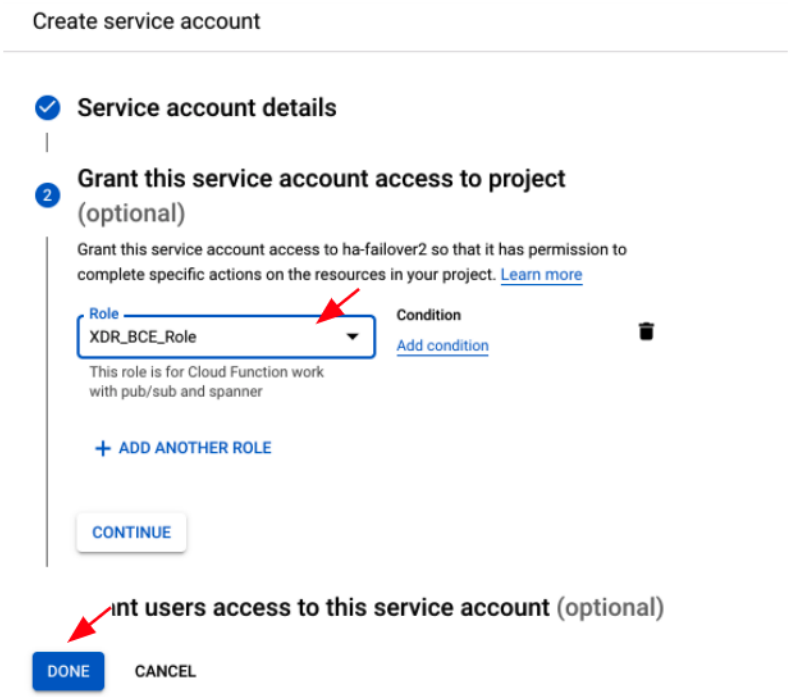


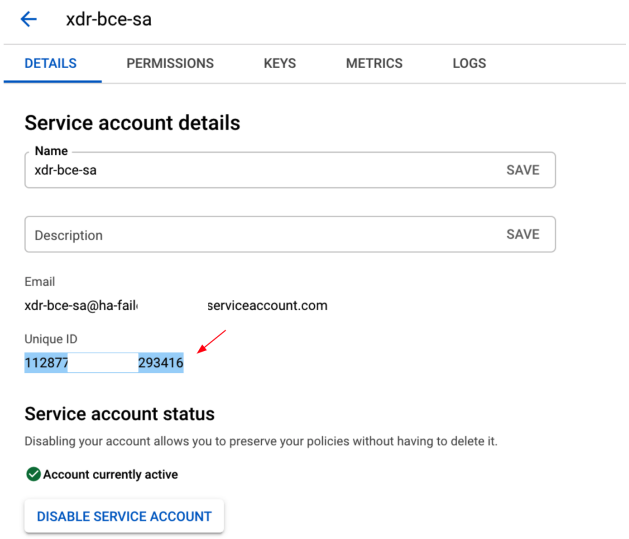
Find permissions filter by “Cloud Spanner Admin”



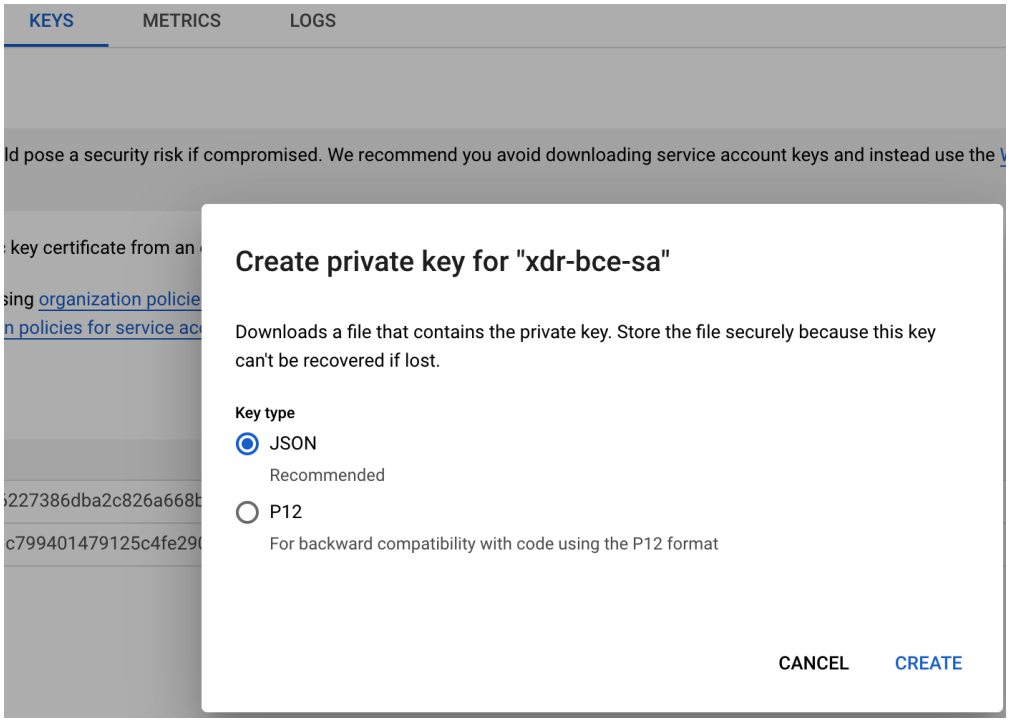
1. Go to Google Cloud Console -> IAM & Admin -> Service Accounts -> Create a new Service Account (grant the role you just created), copy the Unique ID, you will need this later





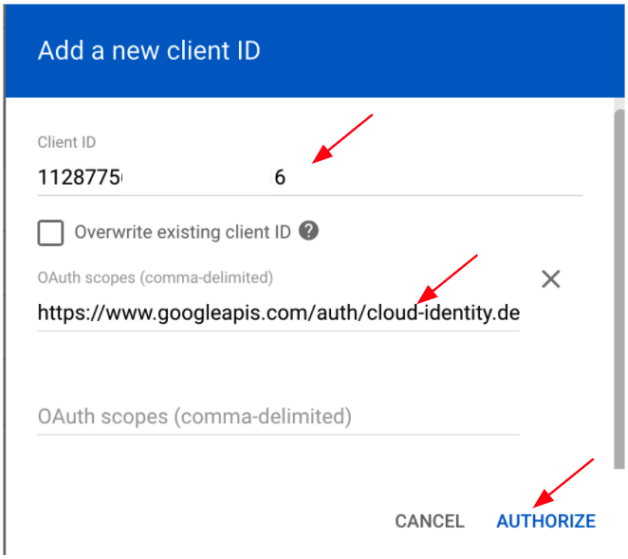


2. Go to the “KEYS” tab, and create a new Key in JSON format:



Click “CREATE”, and save the file locally. You will need this information later, and update in the Terraform template.

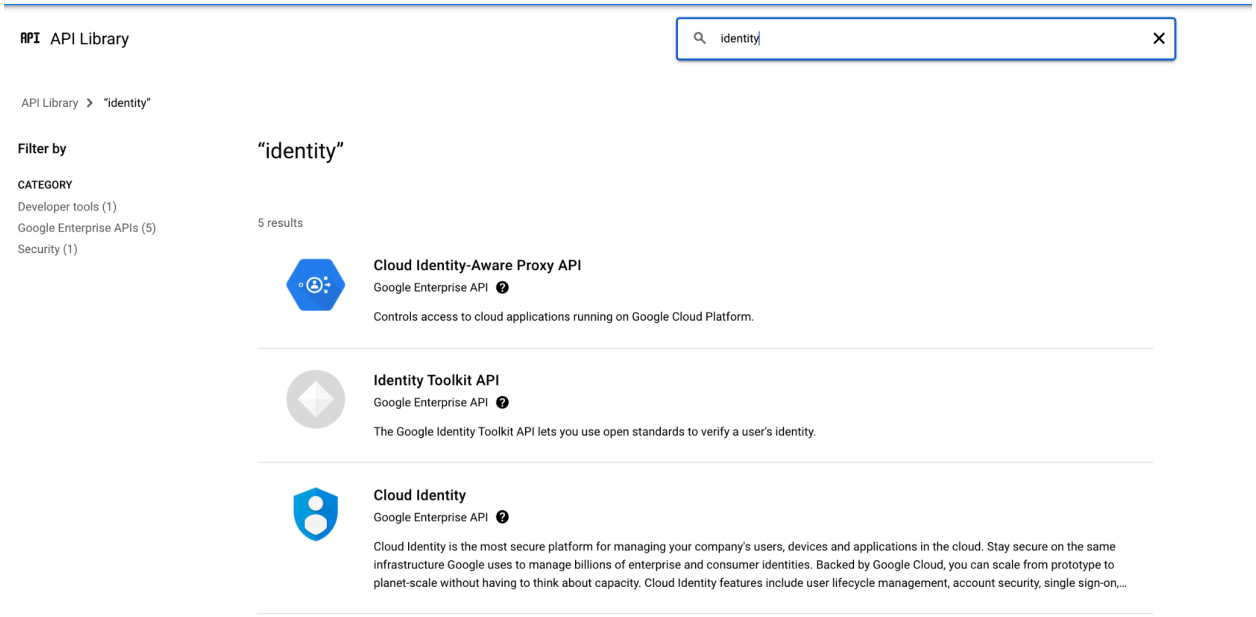
3. Now you need to go to Google Admin Site to grant this service account for the Google Admin API Call scope. Go to Google Admin (https://admin.google.com/), login with your administrator account. Go to Security -> API Controls -> Add new client by clicking “Add New”. Import the Unique ID you copied previously, and add the OAuth scope: **https://www.googleapis.com/auth/cloud-identity.devices**, like below:



Deploy the integration through the Marketplace

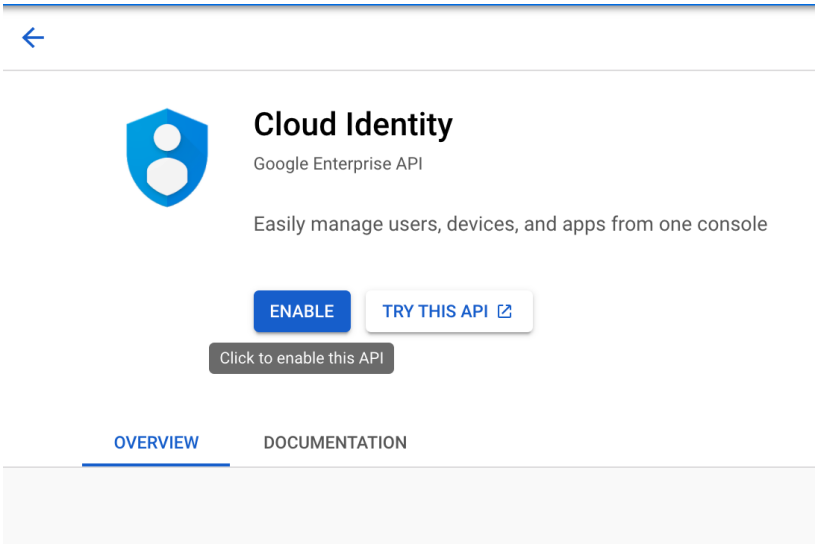
Enable Cloud Identity API in Google Cloud Console (optional: if you didn't enable this before)
Goto APIs & Services -> Dashboard -> click "Enable APIS and SERVICES"

Search for "Identity"



And click "Cloud Identity"

Enable the API



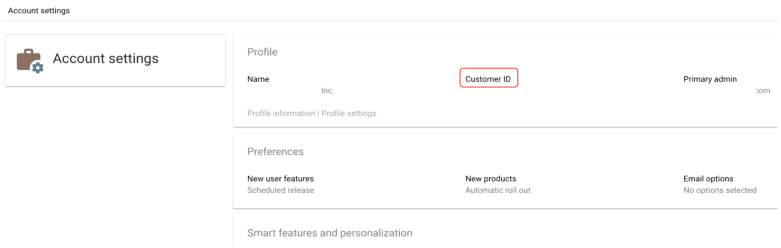
Parameters details:

variable	value
xdr_key	Your Cortex XDR key. As you created in the previous step
xdr_key_id	Your Cortex XDR key ID. As you created in the previous step
xdr_base_url	Your XDR API URL (i.e. https://api-<tenant_id>.xdr.us.paloaltonetworks.com /public_api/v1/) Reference to Doc
customer_id	Your GCP customer ID. See Notice #1
customer_email	An email address. The Google Admin Portal Administrator email address. The service account will impersonate this user to update BeyondCorp Health Score
service_account_email	A GCP service account email.

global_prefix	A name to prepend to all cloud resources created (i.e. demo-prefix-)
Cred JSON	Get the content from the JSON file you downloaded through the service account creation, copy the whole content and paste here
Update XDR info health score Source	Available options: incidents or alerts. Incidents will be preferred, as it tracks the incident generated in the XDR instead of alerts..
Update XDR info source list	Focused on the incidents triggered by the event sources, support multiple selections. Available Options: [“XDR Agent”, “XDR Analytics”, “XDR Managed Threat Hunting”, “Threat Intelligence”, “XDR Analytics BIOC”, “XDR BIOC”, “Correlation”, “PAN NGFW”, “XDR IOC”]. **For example: [“XDR Agent”, “XDR BIOC”, “XDR Analytics”]. This means any incidents triggered by either of these 3 alert sources, will affect the health score.**

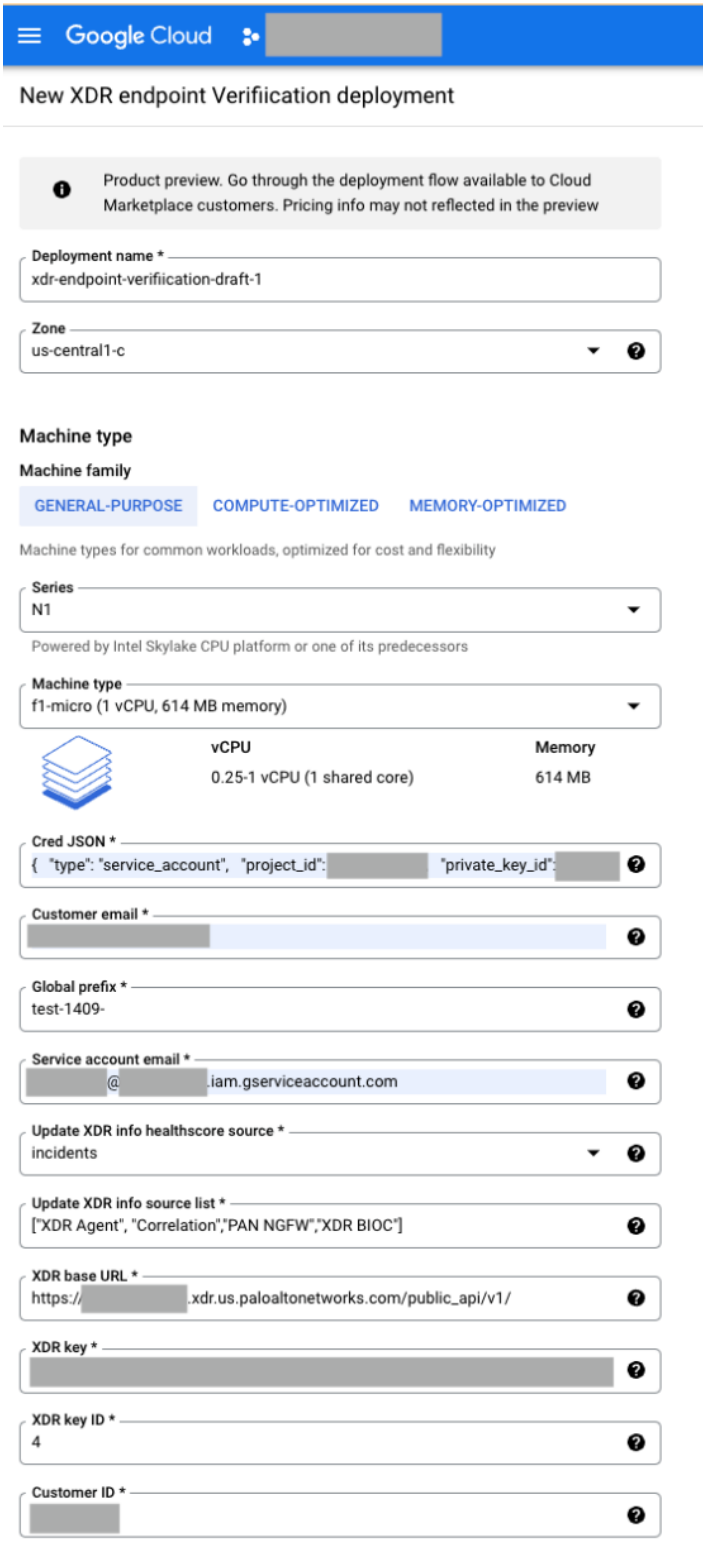
Notices:

1. **Customer ID**: You can get this through Admin Portal, Account -> Account Settings, find the Profile section, and you will get the customer ID. Screen Shot below:



Integration Deployment

Step 1. Provide deployment details (see attached screenshot) according to the Parameters details section.



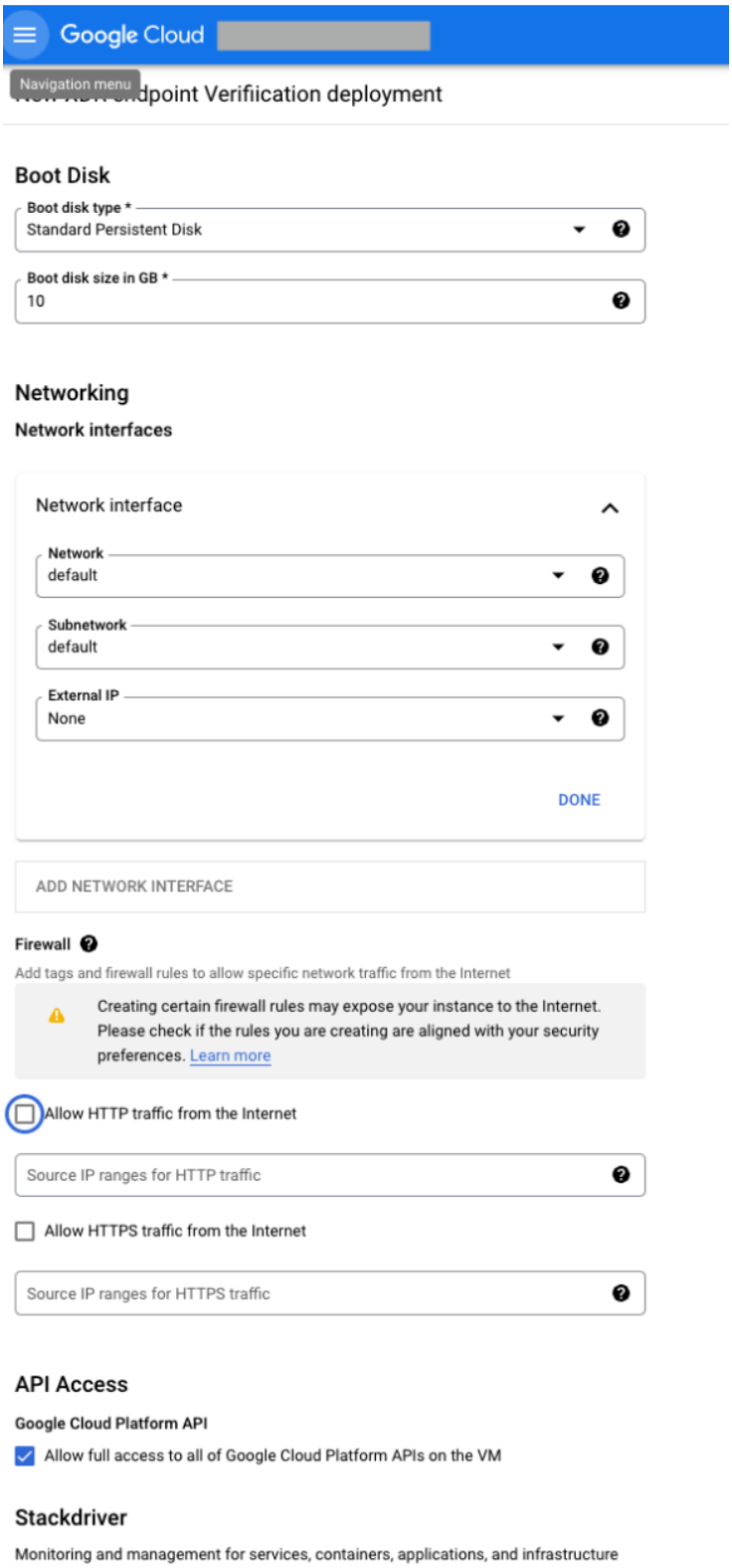
< select VM size (recommended the smallest)

< provide previously configured Service Account Key

< select from dropdown

<provide list of XDR source list in presented format

Step 2. Configure Boot Disk size and Networking.

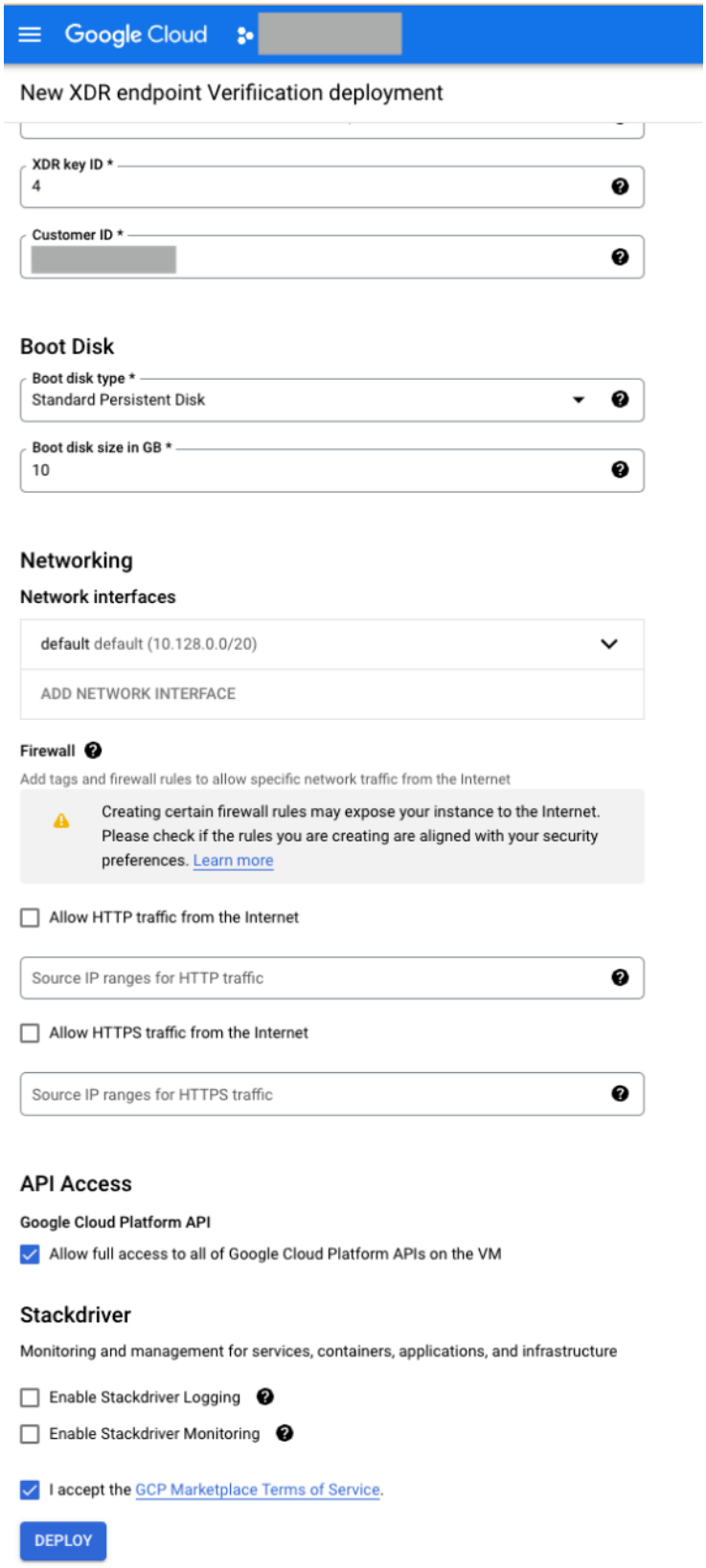


< we recommend disabling External IP and using IAP to connect to VM

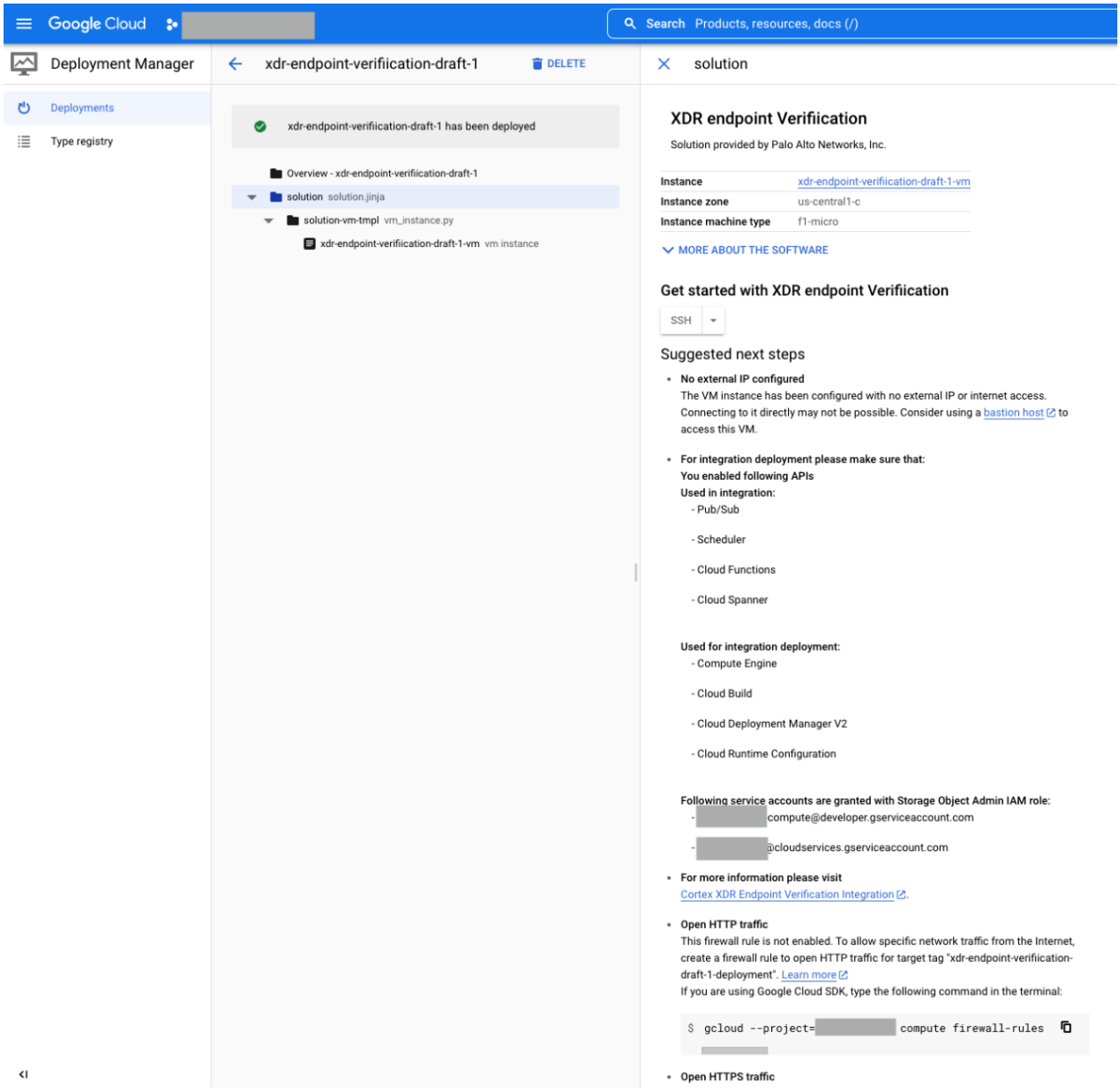
< HTTP and HTTPS traffic can be disabled

< Make sure “Allow full access to all of Google Cloud Platform APIs on the VM” is enabled

Step 3. Accept the GCP Marketplace Terms of Service and deploy the integration.

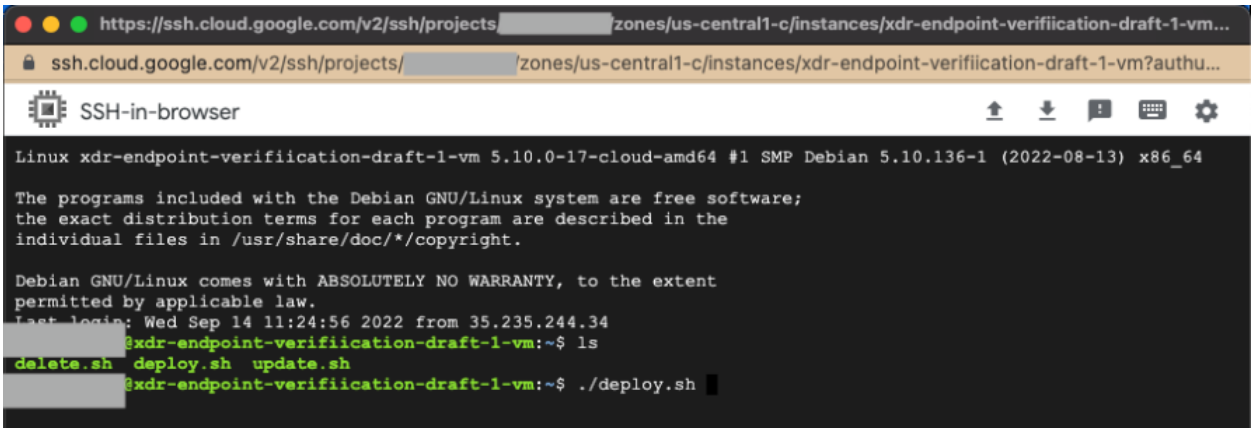


Step 4.After the deployment is complete you will see suggested next steps (APIs that need to be enabled as well as service account that you will have to configure).
At the same time at the top of the integration deployment description you still see an SSH button that you can use to connect the VM to proceed with integration deployment.

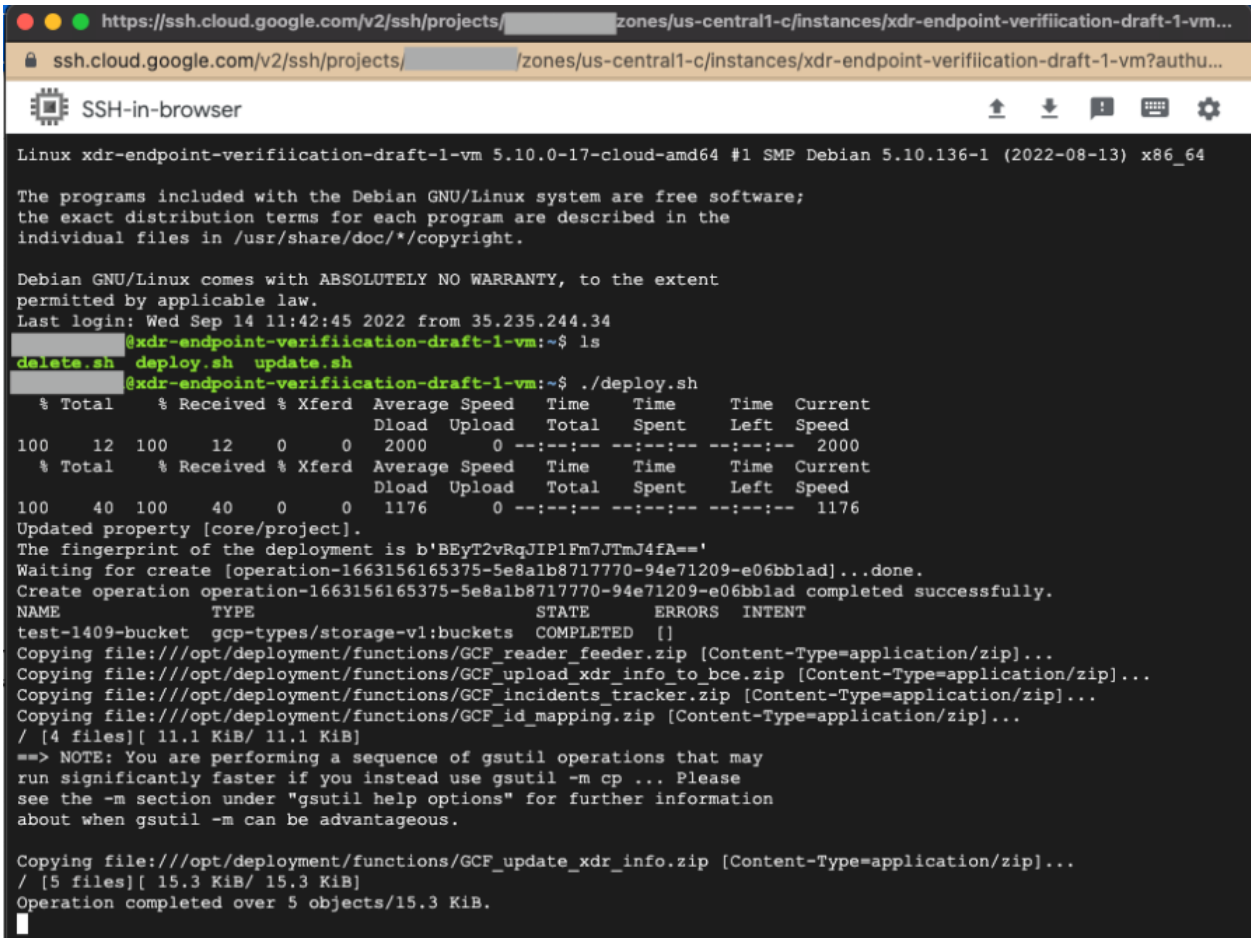


Step 5. On the VM you will have access to 3 scripts

1) Deploy - to deploy integration resources
2) Update - to update integration configuration (or redeploy failed resources)
3) Delete - script that removes all resources (something deployment manager cannot remove fully - GCS)

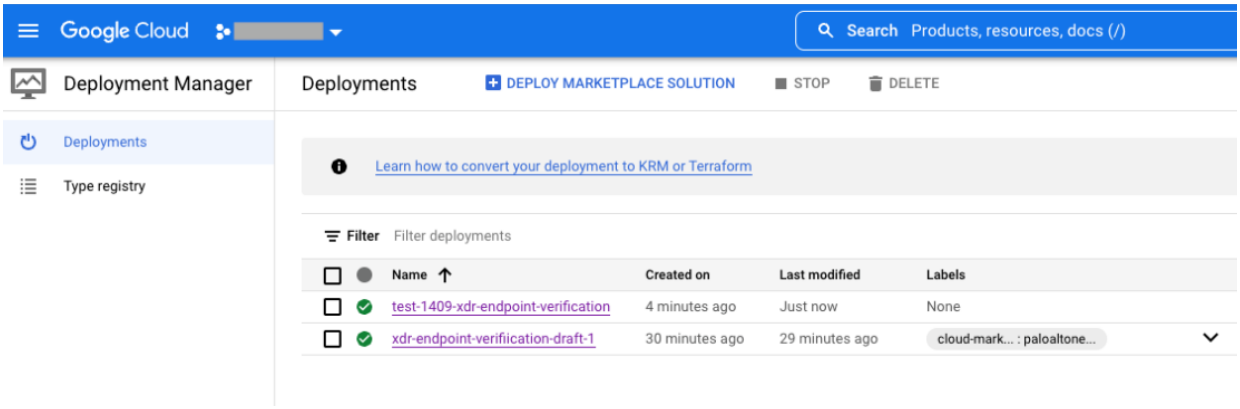


type: “./deploy.sh” and press enter to deploy the solution

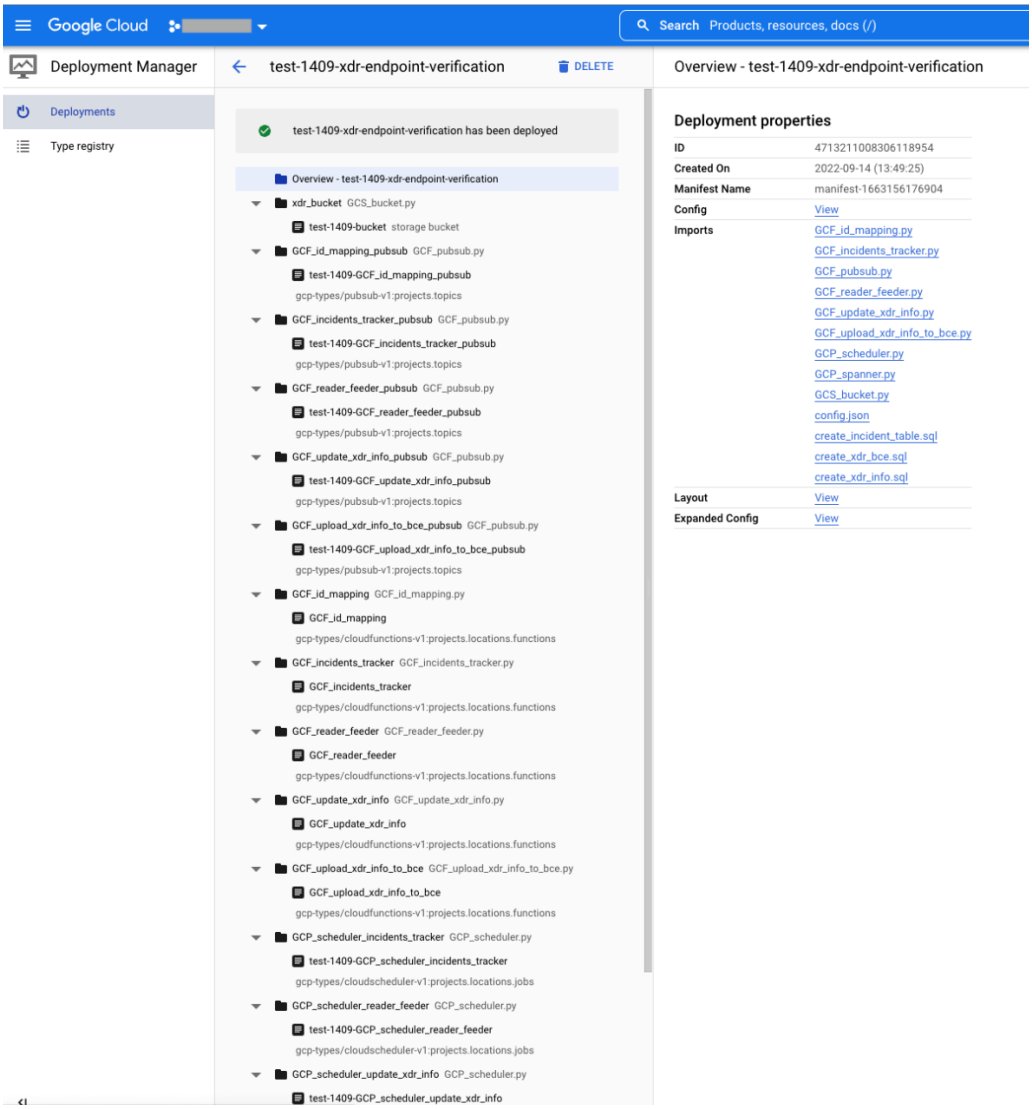


after successful deployment you should see following information (that all resources deployment is “COMPLETED”):

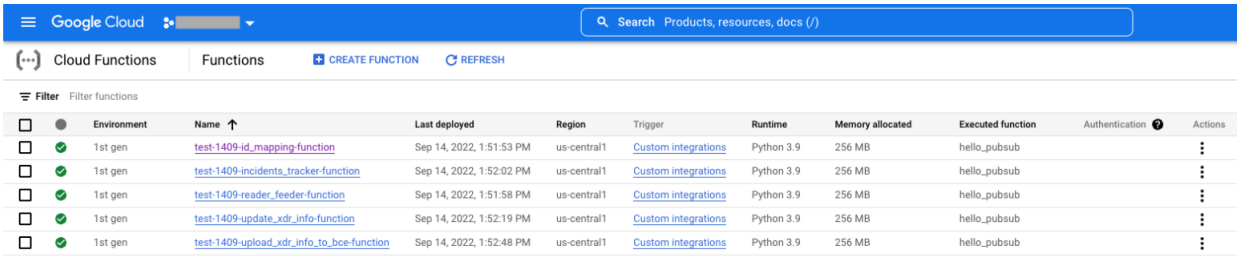
Step 6. Going to you deployment list you should now see second deployment (actual integration resources deployment)



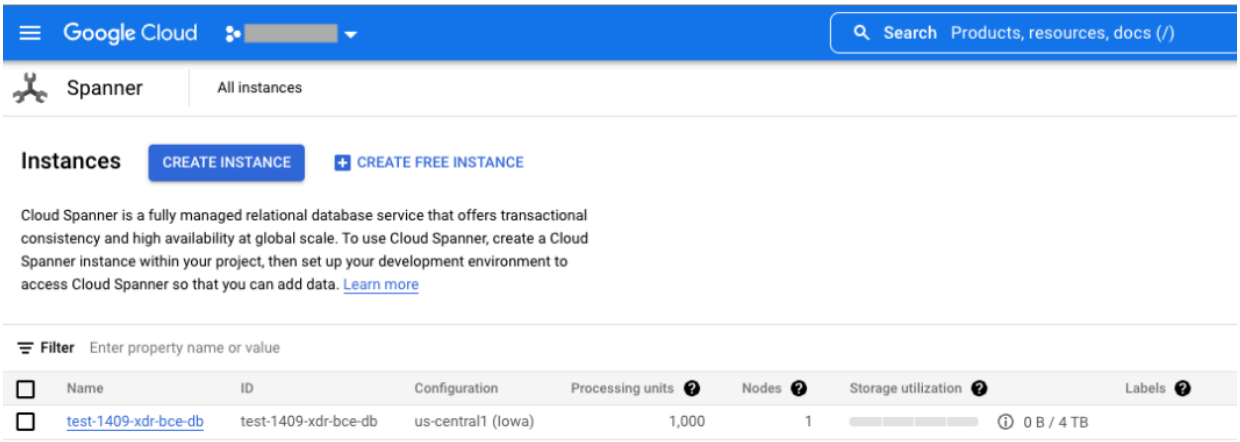
Clicking details you should see information about deployed resources and success status at the top of the list



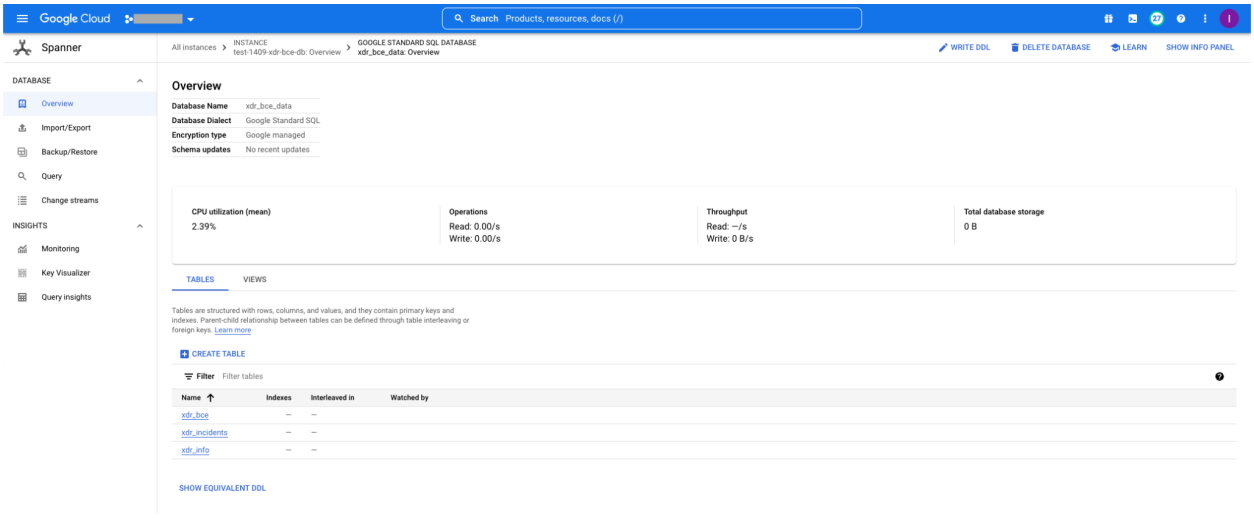
you can check the status of Cloud Function:



Spanner instance:



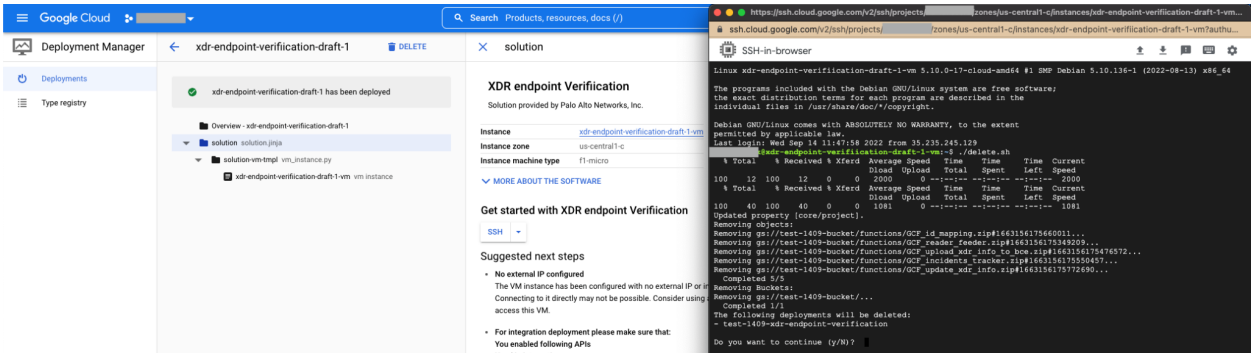
and finally Spanner tables



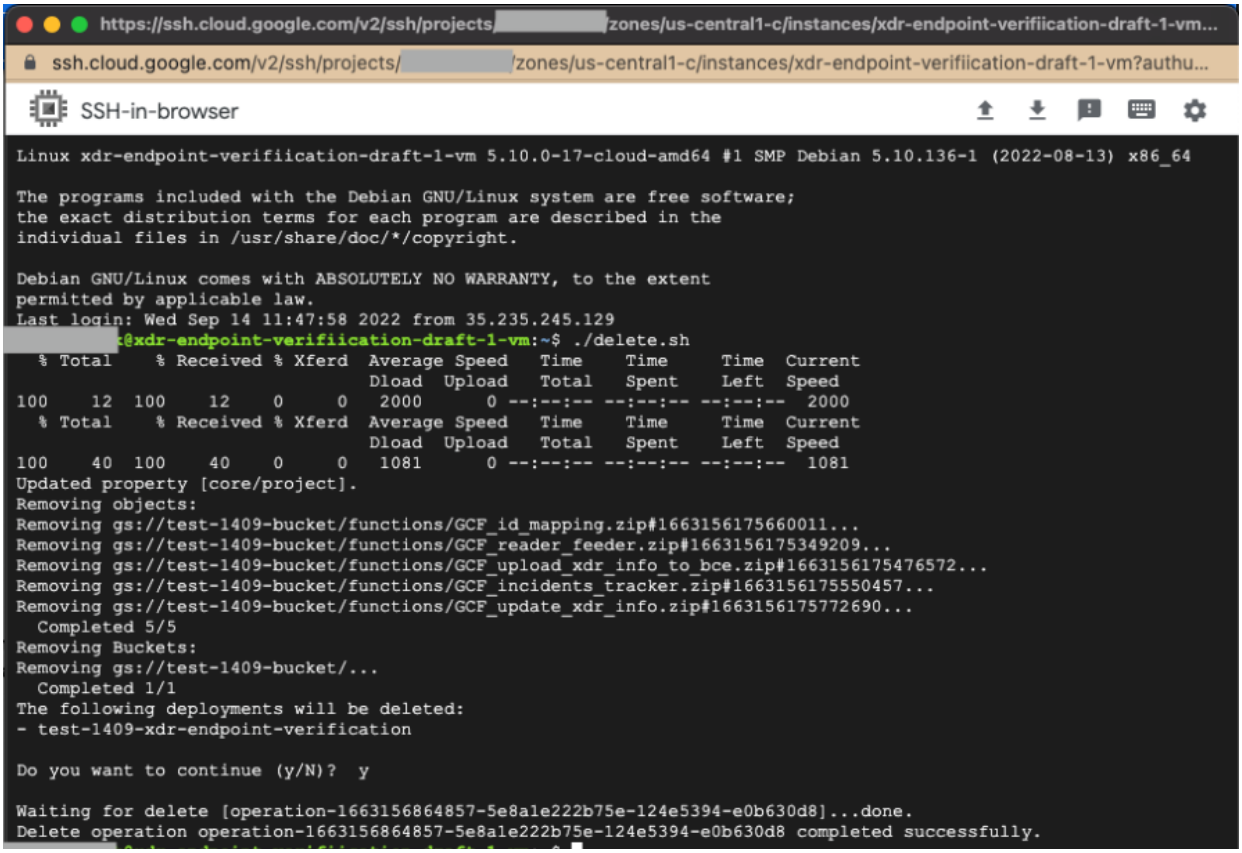
Step 7. Now you can shut down a VM instance on the Compute Engine screen (keep it in case you need to update configuration or delete resources).

Removing integrations

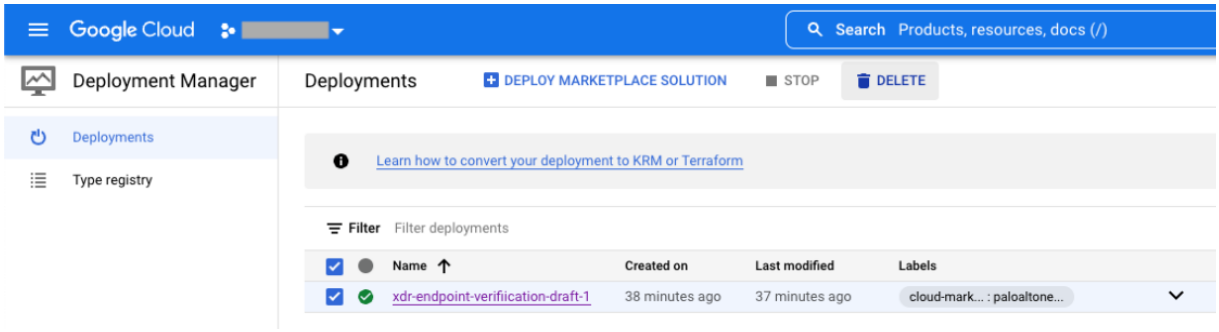
Step 1. Go to the VM integration deployment page and press SSH to connect to the VM.



Step 2. In the SSH session type “./delete.sh” and press enter.



Step 3. Confirm that the integration resources were removed (you should only see VM integration deployment in the Deployment Manager screen).



Step 4. Remove VM integration deployment using DELETE button.

Test your Cortex XDR Endpoint Verification Deployment

1. Create Access Context Manager Access Level:

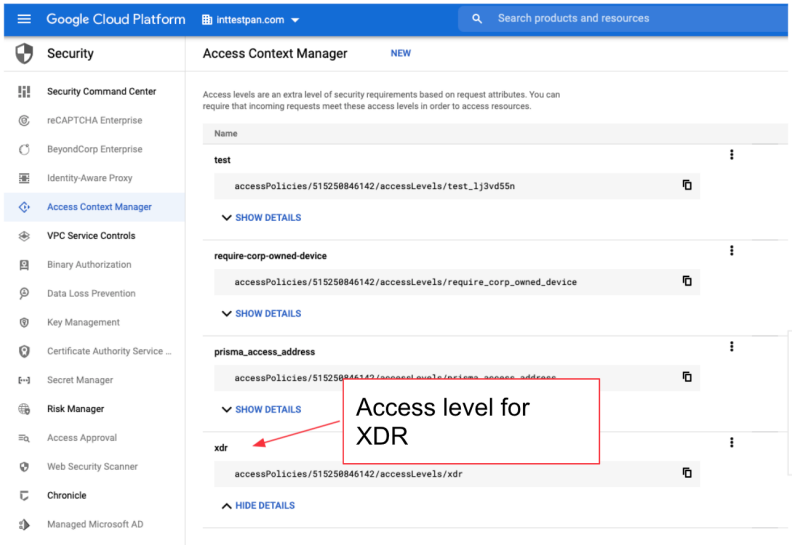
   Sample CEL could be:
   device.vendors["PANW"].is_compliant_device == true &&
   device.vendors["PANW"].is_managed_device == true
   && device.vendors["PANW"].device_health_score == DeviceHealthScore.VERY_GOOD

   Or define a range for the health score:

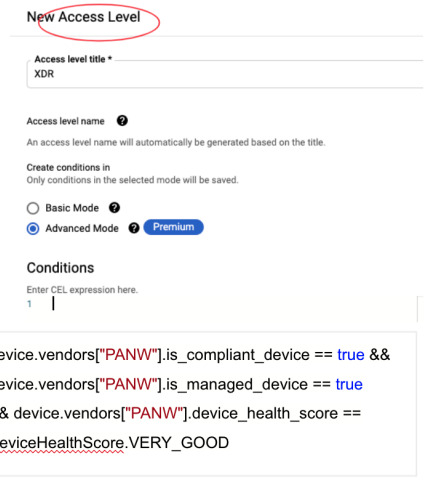
```
device.vendors["PANW"].is_compliant_device == true &&
device.vendors["PANW"].is_managed_device == true
&& device.vendors["PANW"].device_health_score >= DeviceHealthScore.POOR
```

   You can define yours based on your requirements.

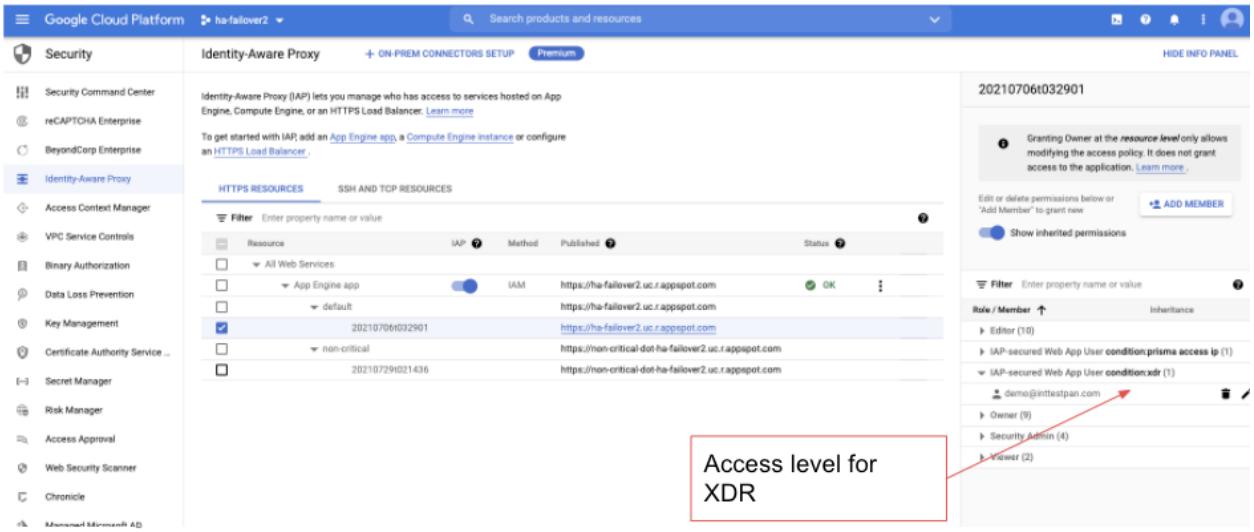
Create a Access Level with XDR Endpoint Risk Context



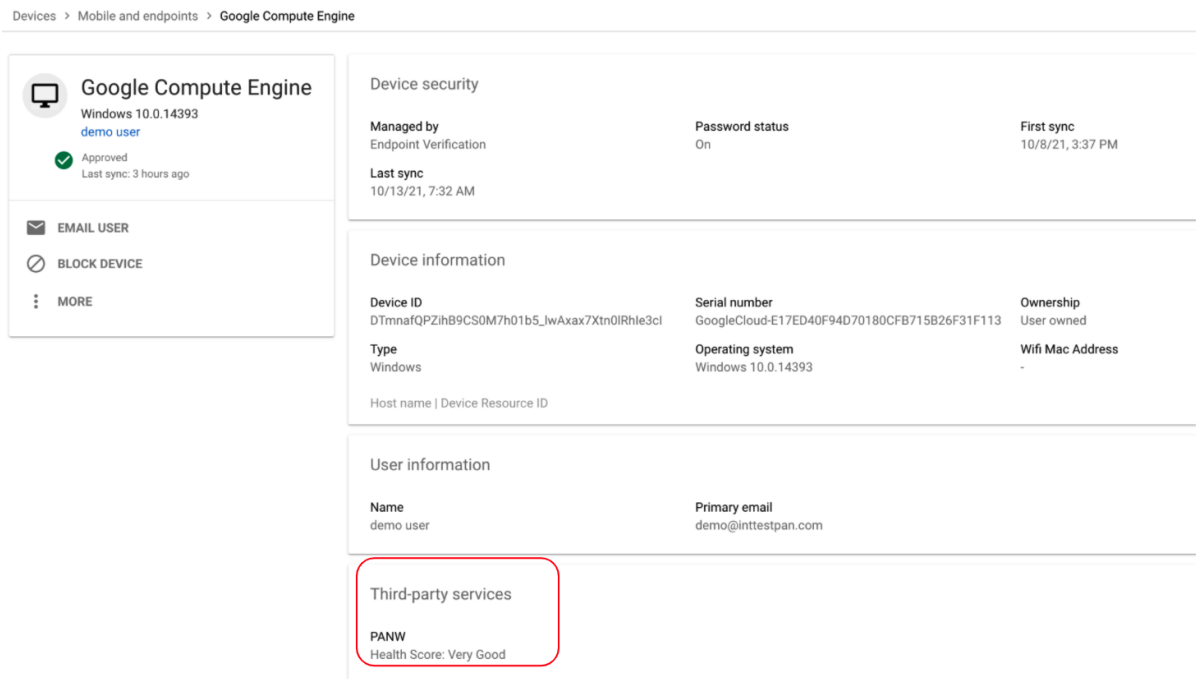
Options to create a Access Level



2. Enforce XDR Endpoint Verification Access Level for Application Access



3. Check the Health Score of Endpoints in Google Admin Site (Devices -> Mobile and Endpoints):



Additional Info:

Health score Calculation:

- Critical severity incident - Very Poor
- High severity incident - Poor
- Medium severity incident - Neutral
- Low severity Incident - Good
- No incident - Very Good
- For multiple incidents, the most severe incident level will be used