Persistent

CyRev

Getting Started Guide

Software Version: 1.1.3

Legal Notices

Warranty

The only warranties for products and services are set forth in the express license or service agreements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty of any kind, implied, statutory, or in any communication between them, including without limitation, the implied warranties of merchantability, non-infringement, title, and fitness for a particular purpose. Persistent Systems shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Persistent Systems or its licensors required for possession, use or copying. No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Persistent Systems.

Copyright Notices

Trademark Notices

Persistent Systems are trademarks or trade name or service mark or logo of Persistent. All other brands or products are trademarks, trade name, service mark, logo or registered trademarks of their respective holders/owners thereof.

Disclaimer

The Persistent System products are available and support only the English language.

Table of Contents

Introduction

Persistent System’s Cyber Recovery Director (CyRev) is an enterprise-class software appliance to discover and recover from ransomware attacks. These attacks require us all to rethink our security posture and we should assume that ransomware will eventually permeate even the most protected environments. CyRev helps you recover from such debilitating ransomware attacks. CyRev uses cyber resilience technology and process from Persistent Systems Ltd. to protect and recover from ransomware attacks in a short span of time with minimal loss of data, minimizing impact to business. CyRev is the most complete and easy-to-use solution available in market.

Ransomware Anatomy

Most ransomware attacks generally unfold in the same fashion and follow the same stages, ultimately ending with the unavailability of a system and/or the system’s data.

First, a system becomes infected with malware which allows the attacker access to at least modify some files on the system. As with any malware attack, this initial incursion can occur in a vast number of ways: through vulnerable network services, via a phishing or account password attack, through infected portable storage, etc.

Once the malware has become resident on a system it will attempt to disable any protections or other services on the system that might interfere with the progress of the attack (eg, antivirus software, backup processes, etc.) It may also attempt to spread itself to other systems via various vectors (network, storage exchange, and credential compromise, for example.)

It will then begin to transform critical data into a form that will be inaccessible by the rightful owner. As with the initial infection this stage can proceed in many different ways. Typically, data is slowly encrypted while still giving access to the unencrypted data to prevent discovery of the attack, either through excessive resource consumption on the system or the discovery of inaccessible data. To this end it also avoids encrypting operating system files that would cause the server or critical services to stop operating. In some cases, the unencrypted data is copied off the system by the attacker for exploitation outside of any ransom demand.

Once enough data has been encrypted (or otherwise made inaccessible) to cause significant inconvenience to the rightful owner, access to the original data is removed usually by deleting it from the system. At this point the attacker will issue a ransom demand to the data owner, insisting on payment before providing a key to unencrypt the data.

Discovery of the attack can occur at any point up to the ransom demand, either through unusual system operation (higher than typical CPU and memory resources, excessive disk usage or disk space consumption, rogue process recognition, etc.) However, ransomware has become proficient at hiding itself from casual discovery in this manner. Additionally once access to critical data is lost the attack has in effect succeeded: some sort of remediation is required by the system owner in order to avoid eventually paying the ransom demand or to avoid at least some critical service unavailability.

As is the case with other data access interruptions (disk or other hardware failure, loss of a site, etc.) remediation means restoring the data and reconstituting the affected systems and services. As ransomware attacks have evolved, however, attackers have learned to disable or destroy the sources for such remediation. For example, when the system is compromised it's not unusual for credentials for backup or DR systems to be stolen, allowing the malware or attackers to exclude data from being collected for backup or DR; to delete the backup or DR images that would be used for remediation; or to corrupt them to make them unusable or to insert trojan horses to make them instantly re-infectable after recovery. Therefore, it is essential to have a separate, uncompromisable and incorruptible system for keeping historical images safe from ransomware attacks, beyond just backup or DR.

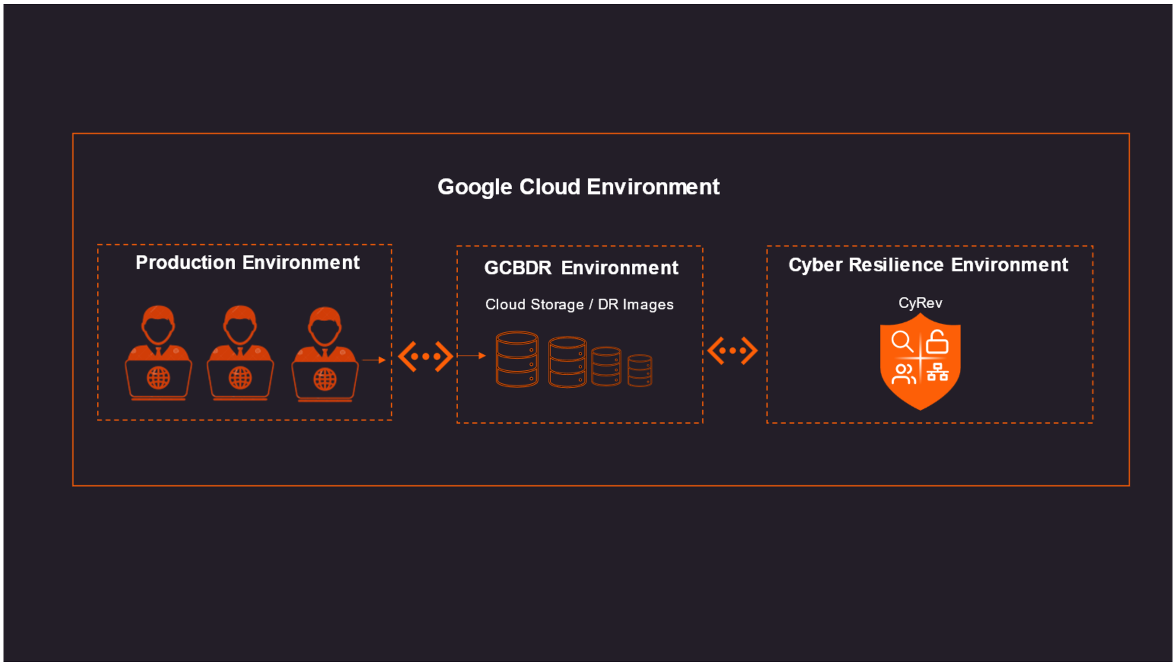
Even with valid historical images for the system and data, reconstruction of infected or inaccessible systems and datasets by hand is itself an arduous task. As images are obtained over time for backup or DR purposes, they will be actually copying infected systems and partially encrypted datasets. Since the process between infection and final ransom demand can take a significant amount of time a pre-infection image is unlikely to have the most desirable (most recent) data. And images taken post-infection will have the malware in them, meaning they must be scanned and scrubbed to prevent instant reinfection when they're reconstituted. They will also contain data that's transitionally corrupted or inaccessible, requiring that valid data be selected from multiple historical images and composed into a single consistent dataset. Finally, whatever the initial vector for attack through which the malware originally entered the system must be blocked and sealed (changing passwords, strengthening firewall rules, etc.)

Keep in mind that even this remediation process is itself subject to ransomware attack; since the original system was vulnerable, at least initially its reconstituted form is subject to the same type of attack, until the attack vector is discovered and closed. Additionally, it needs to be protected against reinfection via channels the attackers may have discovered in the initial attack (compromised credentials, other discovered system vulnerabilities, etc.) To assure that the system is functional, has a valid and desirable dataset, and is not subject to reattack it must be extensively tested. And this process, too is subject to attack. Therefore, it's critical to perform both the reconstitution of system and the testing of a candidate system in a sealed and protected environment.

Persistent's CyRev product addresses these side-ranging aspects of ransomware incursion and the process of protecting, discovering and reacting to an attack. The following sections describe how the solution is deployed and operates in your infrastructure.

Deployment Scenario

This section describes the CyRev integration with your organization infrastructure:



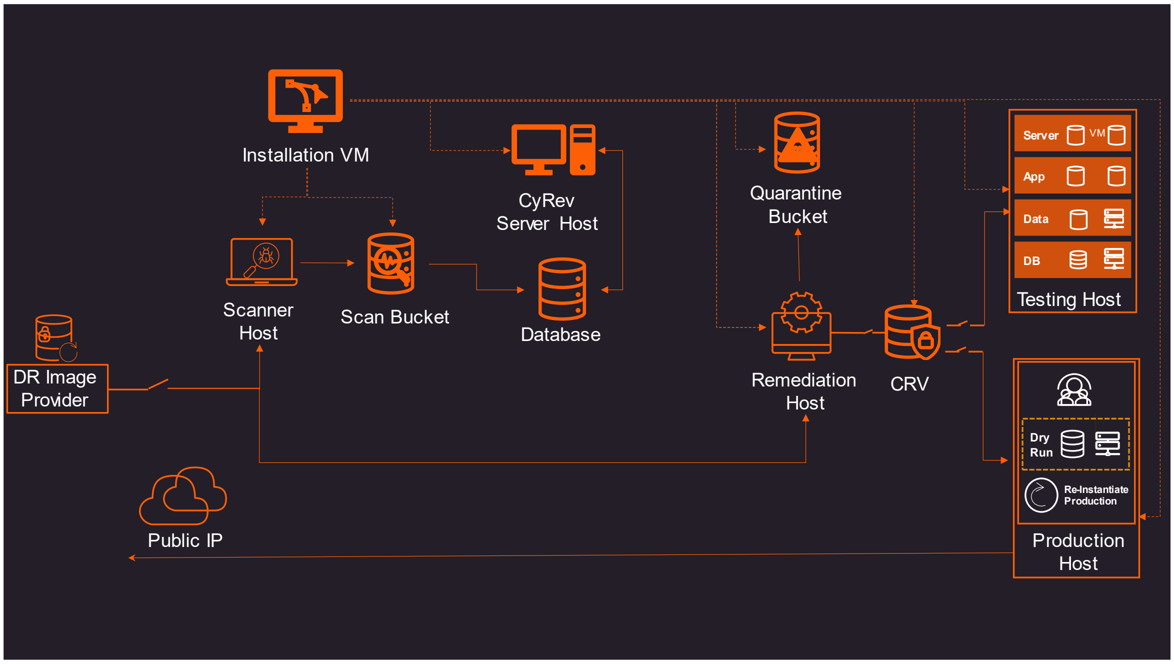
To protect a system and react to ransomware attacks CyRev requires access to images of the system on an ongoing basis, in order to scan them for attacks, allow for the creation of cleaned images, etc. CyRev gains access to these system images through a Trusted Image Provider (TIP); in this case, Google Cloud Backup and Disaster Recovery (GCBDR).

In a typical GCBDR deployment GCBDR components are deployed in your production environment to capture system images and store them in cloud storage. CyRev requires access to two types of GCBDR components – the Backup servers that provide access to captured images, and the Management Console. The CyRev solution is deployed in same GCP project and is connected to the necessary GCBDR components to gain access to images for the systems/applications being protected.

Below section helps you understand the architecture of the CyRev, and how it helps to recover from a ransomware attack.

CyRev Architecture

CyRev is a Cyber resilience product that protects your organization from various cyber threats mainly the Ransomware Attacks. Using CyRev, you can create a complete Cyber Resilience Recovery Plan to scan the DR images as they are created. CyRev's architecture consists of a several components that work together to discover and react to ransomware attacks.



The key components of the architecture are:

- **DR Image Provider:** CyRev connects with the Google Cloud Backup and Disaster Recovery (GCBDR) Management Console and GCBDR Backup server in order to gain access to system images of systems (applications) being protected. GCBDR captures the images in the production environment and stores them in the cloud environment. (For more information refer to the Backup and Disaster Recovery Documentation.) CyRev accesses and uses the DR images stored by GCBDR to perform the scanning and remediation operations.
- **CyRev Installation VM:** On the initial deployment of CyRev through the GCP Marketplace launcher an *Installation VM* is deployed in the CyRev project. This component controls creation, management, and deletion of other CyRev resources that are not created as a part of initial deployment, such as the Test Management Host, Production Management Host, etc. The Installation VM is accessible via RDP from your computer.
- **CyRev Scanner Host**: CyRev Scanner is a cyber resilience technology developed by Persistent Systems Ltd to protect the organization from various cyber threats. The Scanner host scans system images to detect anomalies and threats and raises alerts based on threats it detects.
- **CyRev Scan Bucket**: The Scan Bucket is the repository of the results of image scans. The scanning results from the Scanner Host are stored in the scan bucket, and other components like the CyRev database access it.
- **CyRev Server Host**: The CyRev Server Host presents the CyRev web interface which helps you to quickly identify the threats and attacks on the candidate images

and review the changes in them using a dashboard that allows fast review and action on hundreds of candidate images.

- **CyRev Remediation Host**: The Remediation Host performs the job of constructing clean images after an attack is detected. Using instructions on what to do to with corrupted files (For example: delete or quarantine them) and as result it produces a clean data image.
- **CyRev Quarantine Bucket**: Any files determined to be infected in system images during the remediation process are stored in the Quarantine Bucket to isolate them. These files will be available for forensic purposes.
- **Cyber Resilience Vault (CRV)**: The CRV is an air gapped, immutable storage system used to store and protect cleaned images, which are used for testing and production.
- **Test and Production Environment**: When candidate images are produced CyRev will deploy an isolated testing environment where the cleaned images can be tested and verified. Once cleaned images have passed the testing phase they can be deployed at scale into a new production environment.
- **CyRev Database (DB)**:. The CyRev database stores the scan information collected from scanner host for analysis and sends the updated information to UI Dashboard.

These CyRev components orchestrate the Cyber Recovery workflow at scale and provides the opportunity to rapidly react and recover from a ransomware attack.

Installation Overview

CyRev installation consists of deploying the hosts that perform CyRev operations: the CyRev Server VM, Scanner etc. and the creation of the storage components like the Database and Scan Bucket.

Before beginning the installation, you must obtain the required installation binaries and fulfil other pre-requisites for your GCP environment as mentioned in the section on Preparing for CyRev Deployment. You can then start deploying the CyRev components as described in the section on Deploying CyRev.

Preparing for CyRev Deployment

Before embarking on the deployment of CyRev there are some preparatory steps that you need to perform to ensure things go smoothly. The following sections detail what needs to be done to prepare for deployment.

GCP Projects

To get started it's assumed that the GCBDR Project and all the required GCBDR components have already been deployed and configured to capture images from the systems you wish to protect with CyRev.While it's possible to use a previously existing GCP project and deploy CyRev components into it, previously enabled access and other project parameters could expose the CyRev components and data to attack. The instructions below are carefully designed to secure the CyRev Project by enabling the minimal set of capabilities and access based on the default capabilities of GCP Project.

Note: Deploy CyRev in the Region and Zone in which GCBDR is deployed in a network that has outbound connections to the internet.

Deployment Parameters

While preparing and deploying CyRev there are parameters you will obtain or specify that you will need to have handy later in the deployment process or while using CyRev. You will need to know certain attributes, such as the identifiers, network address, etc., of these components as well as of other critical entities such as GCP objects, GCBDR image provider components, etc. Some of these parameters already exist prior to deploying CyRev (for example, GCBDR-related information); others are data that need to be noted as deployment progresses (such as CyRev projects and hosts) for later use in deployment or use of CyRev.

The following table summarizes and organizes this information so that you can obtain or record the information you need. You may wish to fill out this table to have all the necessary details close at hand as you deploy and use CyRev:

CyRev Components		
CyRev Project	CyRev Custom Service account email address	Cust SA Email ID:
Installation VM	The name/IP address and access credentials of the Installation VM.	ID/IP: Login:
CyRev Server Host	The name/IP address, VPC and credentials for the CyRev Server Host.	ID/IP:
		Login:
Test Management Host	The name/IP address, VPC and credentials for the CyRev Test Management Host.	ID/IP:
		VPC:
		Login:
Application Test Host	The name/IP address, VPC and credentials for the CyRev Application Test Host.	ID/IP:
		VPC:
		Login:
Production Deployment Host	The name/IP address, VPC and credentials for the CyRev Production Deployment Host.	ID/IP:
		VPC:
		Login:
Application Production Host	The name/IP address, VPC and credentials for the CyRev Application Production Host.	ID/IP:
		VPC:
		Login:
GCBDR Parameters		
API URL	GCBDR Management Console API URL used by CyRev to access DR images	URL
OAuth 2.0 client ID	Client ID of GCBDR	ID

You will also find a spreadsheet version of this table here: CyRev Deployment Information.

Enable Google Cloud Project APIs

For CyRev to be deployed and operate within the GCP project you will need to enable specific GCP APIs, as described in the following sections.

Enable IAM API

1. Navigate to the GCP Cloud Console **APIs and services** page.

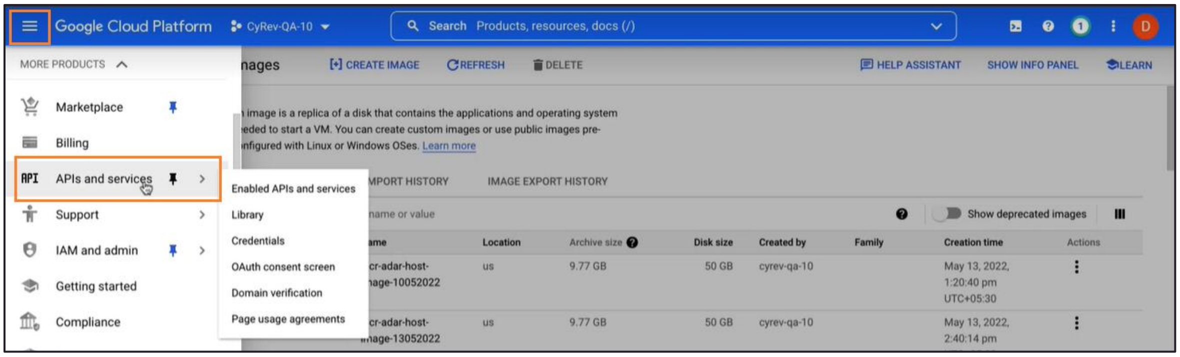
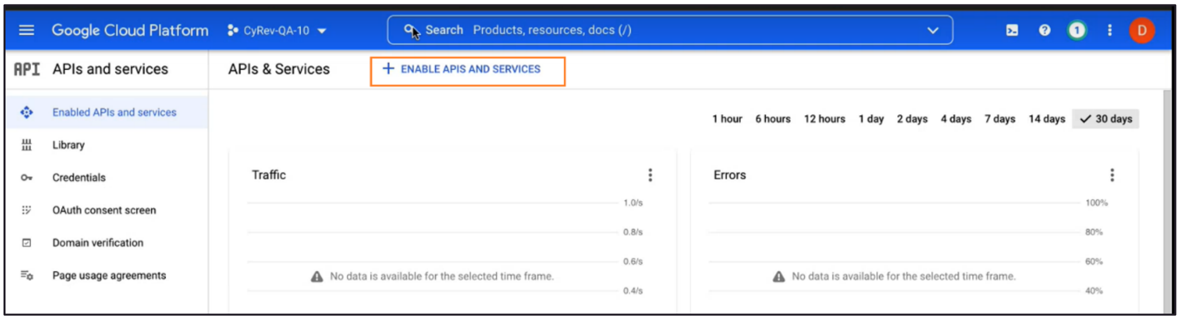


image is a replica of a disk that contains the applications and operating system
eded to start a VM. You can create custom images or use public images pre-
nfigured with Linux or Windows OSes. Learn more

ame	Location	Archive size	Disk size	Created by	Family	Creation time	Actions
cr-adar-host- age-10052022	us	9.77 GB	50 GB	cyrev-qa-10		May 13, 2022, 1:20:40 pm UTC+05:30	⋮
cr-adar-host- image-13052022	us	9.77 GB	50 GB	cyrev-qa-10		May 13, 2022, 2:40:14 pm	⋮

2. Select **+ENABLE APIS AND SERVICES** on top pane. API Library page opens.

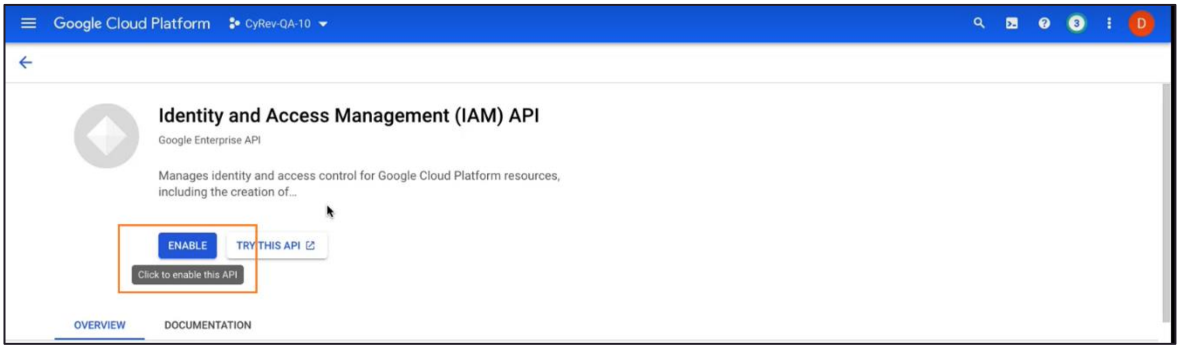


No data is available for the selected time frame.

No data is available for the selected time frame.

3. On API Library page search for the ‘**Identiy and Acess Management (IAM) API**’. Select the API from the list.

4. Select **ENABLE** to start to API service.

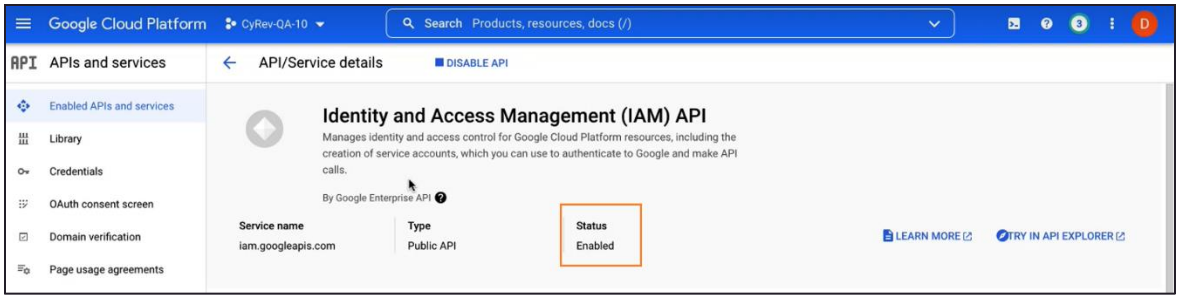


Identity and Access Management (IAM) API

Google Enterprise API

Manages identity and access control for Google Cloud Platform resources, including the creation of...

5. API Status is shown as Enabled on the page.



Identity and Access Management (IAM) API

Manages identity and access control for Google Cloud Platform resources, including the creation of service accounts, which you can use to authenticate to Google and make API calls.

By Google Enterprise API

Service name	Type	Status
iam.googleapis.com	Public API	Enabled

Additionally, the APIs listed below need to be enabled in order to grant the necessary permissions for the CyRev deployment. Repeat steps 3-5 for each of the APIs named below, substituting for the search value in step 3:

- Cloud Resource Manager API
- Cloud Build API
- IAM Service Account Credential API
- Google Cloud Deploy API
- Google Compute Engine API
- Network Management API
- Google Cloud Storage API
- Security Token Service API Cloud Deployment Manager V2 API
- Cloud Runtime Configuration API

Once required APIs enable for the project you must create and assign permissions to service accounts as described in the next section.

Service Account Overview

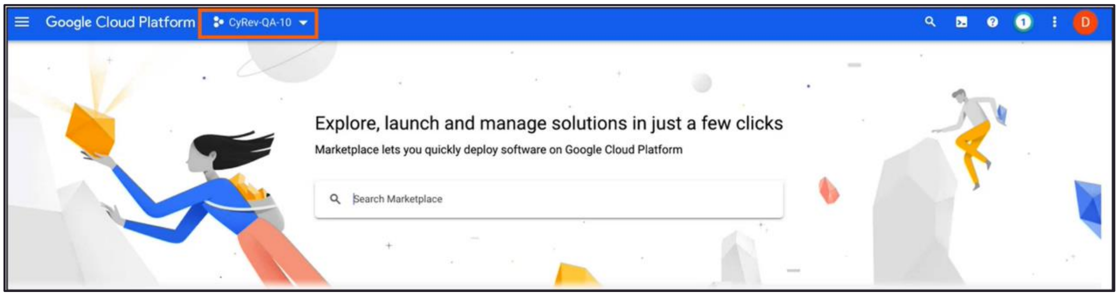
You need to assign certain permissions to the service accounts for CyRev Deployment. There are two service accounts that are involved in the deployment of CyRev:

- **CyRev Custom Service Account**: Once deployed, CyRev components themselves will perform operations itself that require specific roles and permissions. To address this need you need to Create a CyRev Custom Service Account.
- **GCP Cloud Build Service Account**: When you use the Google Cloud console or the gcloud CLI to import or export images for the first time, the tool attempts to enable the Cloud Build API and grant the required roles as described in Assigning Permissions to the GCP Cloud Build Service Account**.**

Create a CyRev Custom Service Account

For the various CyRev components to interoperate and to connect to the DR image service a Service Account (SA) with the Custom role and Token Creator Role must be created. Follow the steps to create the service account:

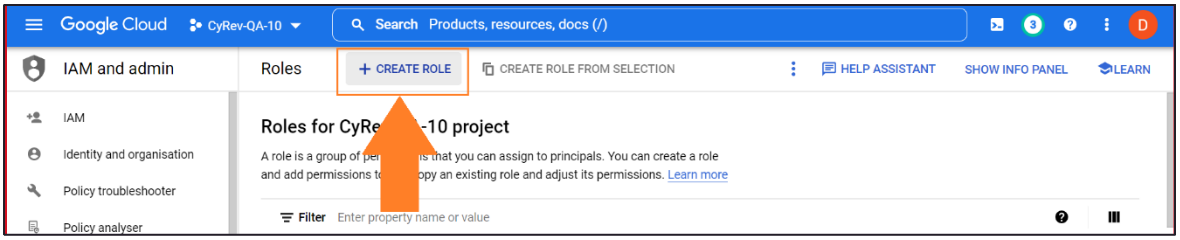
1. Log in to your google cloud account and select the project in which you wish to deploy CyRev.



Explore, launch and manage solutions in just a few clicks

Marketplace lets you quickly deploy software on Google Cloud Platform

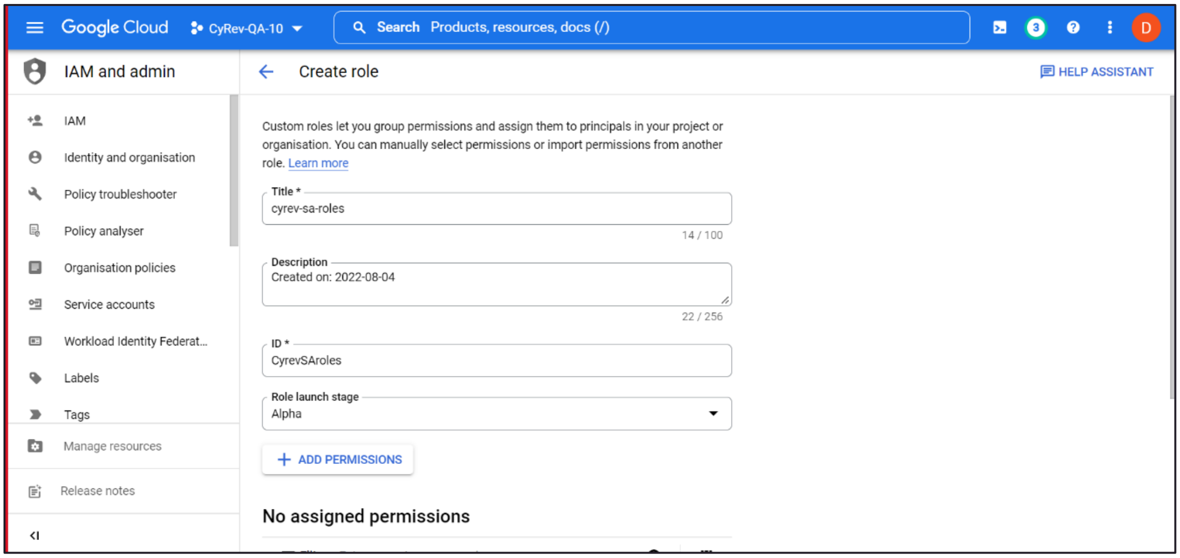
2. Navigate to **IAM & Admin→ Roles** page.
3. Select **+CREATE ROLE** on the top pane. Create role page opens.



Roles for CyRe -10 project

A role is a group of pe s that you can assign to principals. You can create a role and add permissions t opy an existing role and adjust its permissions. Learn more

4. In the Create Role page, enter a **Title (Name for the Role)**, **Description**, and account **identifier** to the fields. From the Role launch stage drop-down, select **Alpha.**



Custom roles let you group permissions and assign them to principals in your project or organisation. You can manually select permissions or import permissions from another role. Learn more

Title * cyrev-sa-roles 14 / 100

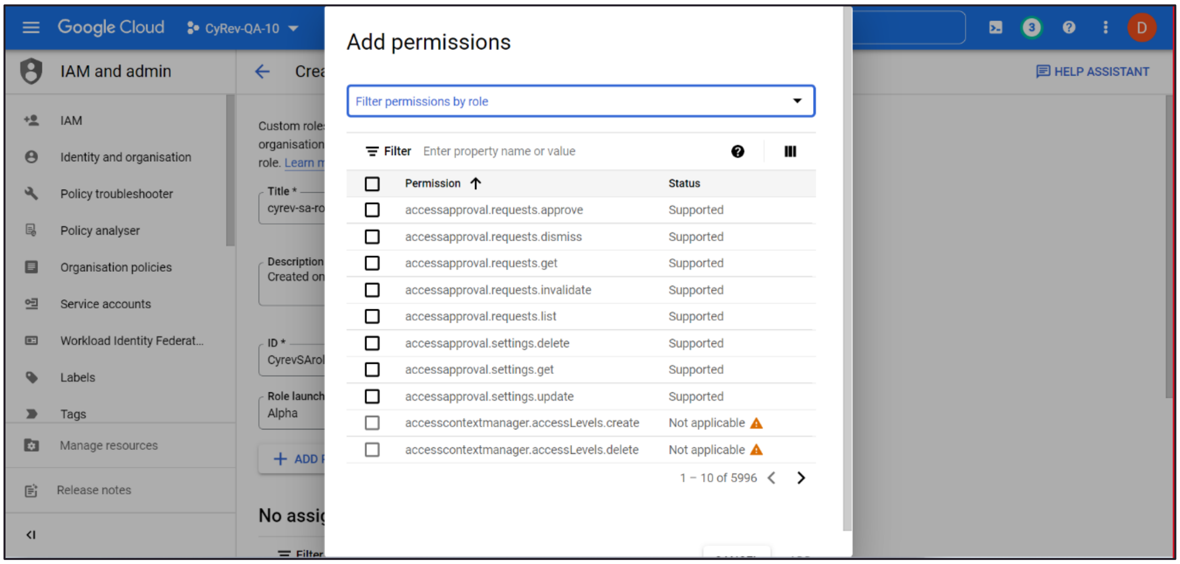
Description Created on: 2022-08-04 22 / 256

ID * CyrevSAroles

Role launch stage Alpha

No assigned permissions

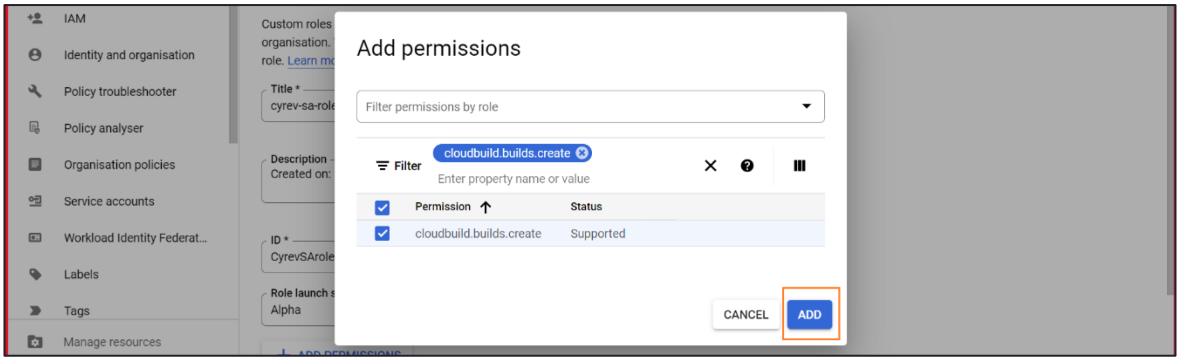
5. Click on **+ Add Permissions**. The permissions list opens.



□	Permission ↑	Status
□	accessapproval.requests.approve	Supported
□	accessapproval.requests.dismiss	Supported
□	accessapproval.requests.get	Supported
□	accessapproval.requests.invalidate	Supported
□	accessapproval.requests.list	Supported
□	accessapproval.settings.delete	Supported
□	accessapproval.settings.get	Supported
□	accessapproval.settings.update	Supported
□	accesscontextmanager.accessLevels.create	Not applicable ⚠
□	accesscontextmanager.accessLevels.delete	Not applicable ⚠

1 – 10 of 5996

6. Use search filter to find the permissions given in the permissions table. Check the box to select required permission. Click **ADD** to add the permission to list. Similarly add all the permissions given in the table.



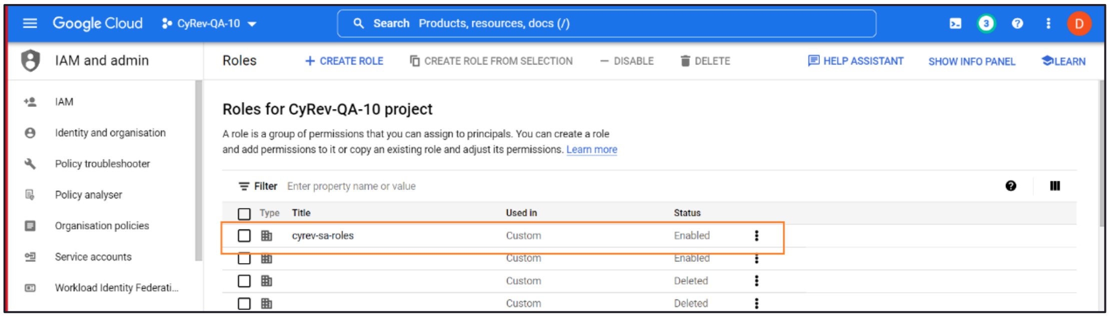
☑	Permission ↑	Status
☑	cloudbuild.builds.create	Supported

Permissions	Permissions
cloudbuild.builds.create	compute.routers.get
cloudbuild.builds.get	compute.routers.update
cloudbuild.builds.list	compute.routes.create
cloudbuild.builds.update	compute.routes.delete
compute.addresses.create	compute.subnetworks.create
compute.addresses.createInternal	compute.subnetworks.delete
compute.addresses.delete	compute.subnetworks.get
compute.addresses.deleteInternal	compute.subnetworks.list
compute.disks.create	compute.subnetworks.use
compute.disks.delete	compute.subnetworks.useExternalIp

compute.disks.get	compute.zoneOperations.get
compute.disks.getIamPolicy	compute.zones.get
compute.disks.list	compute.zones.list
compute.disks.resize	iam.roles.create
compute.disks.setLabels	iam.roles.delete
compute.disks.use	iam.roles.get
compute.disks.useReadOnly	iam.roles.list
compute.firewalls.create	iam.roles.update
compute.firewalls.delete	iam.serviceAccounts.actAs
compute.firewalls.get	iam.serviceAccounts.create
compute.firewalls.list	iam.serviceAccounts.delete
compute.firewalls.update	iam.serviceAccounts.disable
compute.globalOperations.get	iam.serviceAccounts.enable
compute.images.create	iam.serviceAccounts.get
compute.images.delete	iam.serviceAccounts.getAccessToken
compute.images.deprecate	iam.serviceAccounts.getIamPolicy
compute.images.get	iam.serviceAccounts.getOpenIdToken
compute.images.getFromFamily	iam.serviceAccounts.implicitDelegation
compute.images.getIamPolicy	iam.serviceAccounts.list
compute.images.list	iam.serviceAccounts.setIamPolicy
compute.images.update	iam.serviceAccounts.signBlob
compute.images.useReadOnly	iam.serviceAccounts.signJwt
compute.instances.attachDisk	iam.serviceAccounts.undelete
compute.instances.create	iam.serviceAccounts.update
compute.instances.delete	logging.logEntries.create
compute.instances.detachDisk	remotebuildexecution.blobs.get
compute.instances.get	resourcemanager.projects.get
compute.instances.getSerialPortOutput	resourcemanager.projects.getIamPolicy
compute.instances.list	resourcemanager.projects.setIamPolicy
compute.instances.setLabels	storage.buckets.create
compute.instances.setMetadata	storage.buckets.createTagBinding
compute.instances.setServiceAccount	storage.buckets.delete

compute.instances.setTags	storage.buckets.deleteTagBinding
compute.machineTypes.list	storage.buckets.get
compute.networks.addPeering	storage.buckets.getIamPolicy
compute.networks.create	storage.buckets.setIamPolicy
compute.networks.delete	storage.buckets.update
compute.networks.get	storage.objects.create
compute.networks.list	storage.objects.delete
compute.networks.removePeering	storage.objects.get
compute.networks.updatePolicy	storage.objects.getIamPolicy
compute.projects.get	storage.objects.list
compute.routers.create	storage.objects.setIamPolicy
compute.routers.delete	storage.objects.update
	compute.instances.setDeletionProtection

7. After you have added all of the permissions click **CREATE**.
8. The role gets created and will be added in the roles list:

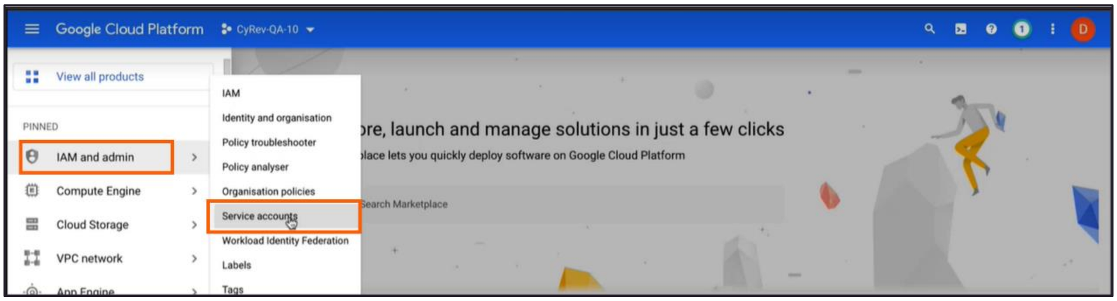


Roles for CyRev-QA-10 project

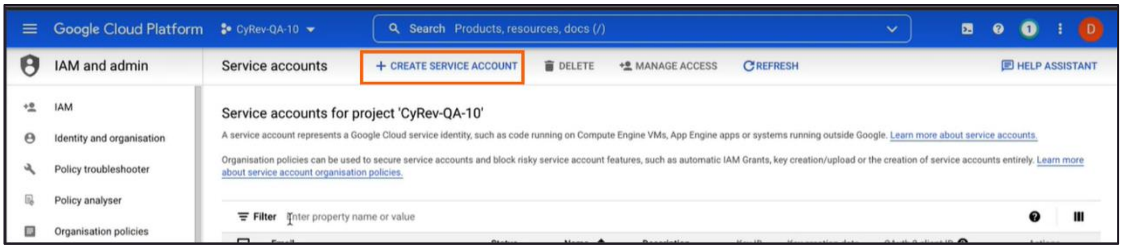
A role is a group of permissions that you can assign to principals. You can create a role and add permissions to it or copy an existing role and adjust its permissions. Learn more

Type	Title	Used in	Status
	cyrev-sa-roles	Custom	Enabled
		Custom	Enabled
		Custom	Deleted
		Custom	Deleted

9. In the Cloud console, go to the **IAM** page and select **Service accounts**.



10. Click **+CREATE SERVICE ACCOUNT** on top menu:

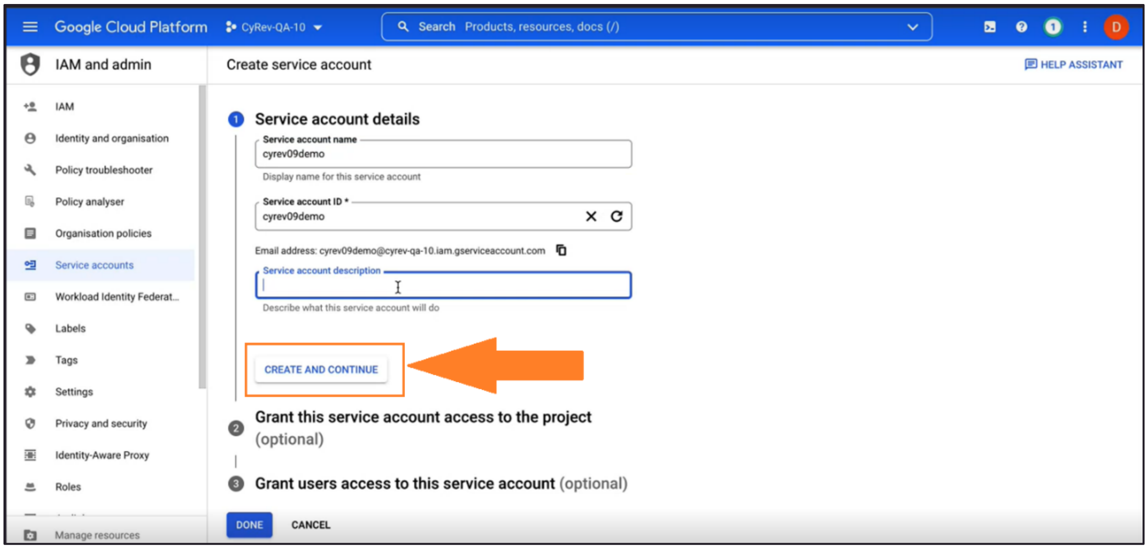


Service accounts for project 'CyRev-QA-10'

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps or systems running outside Google. Learn more about service accounts.

Organisation policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload or the creation of service accounts entirely. Learn more about service account organisation policies.

11. On the **Create service account** page you will specify details about the service account:



1 Service account details

Service account name: cyrev09demo

Display name for this service account

Service account ID *: cyrev09demo

Email address: cyrev09demo@cyrev-qa-10.iam.gserviceaccount.com

Service account description

Describe what this service account will do

2 Grant this service account access to the project (optional)

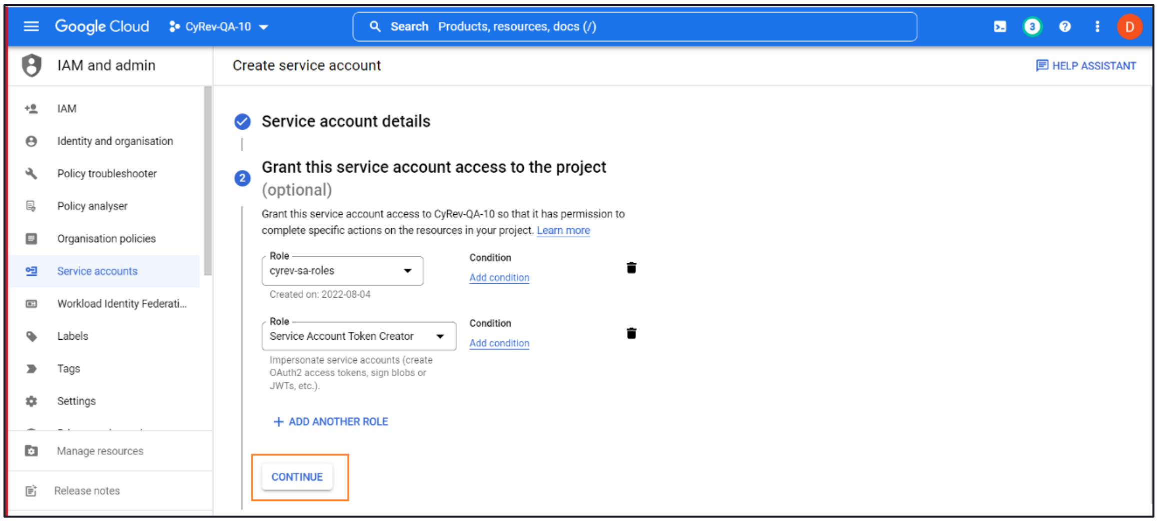
3 Grant users access to this service account (optional)

Fill the service account details as follows:

Parameter	Description
Service account name	Enter the service account name that you wish to assign.
Service Account ID	Enter the service account that you wish to create.
Service Account Description	Enter the description about the service account.

Click on **CREATE AND CONTINUE**. This brings up the details page for the service account.

On this page you will add roles for the new service account:



Service account details

2 Grant this service account access to the project (optional)

Grant this service account access to CyRev-QA-10 so that it has permission to complete specific actions on the resources in your project. Learn more

Role: cyrev-sa-roles — Condition: Add condition

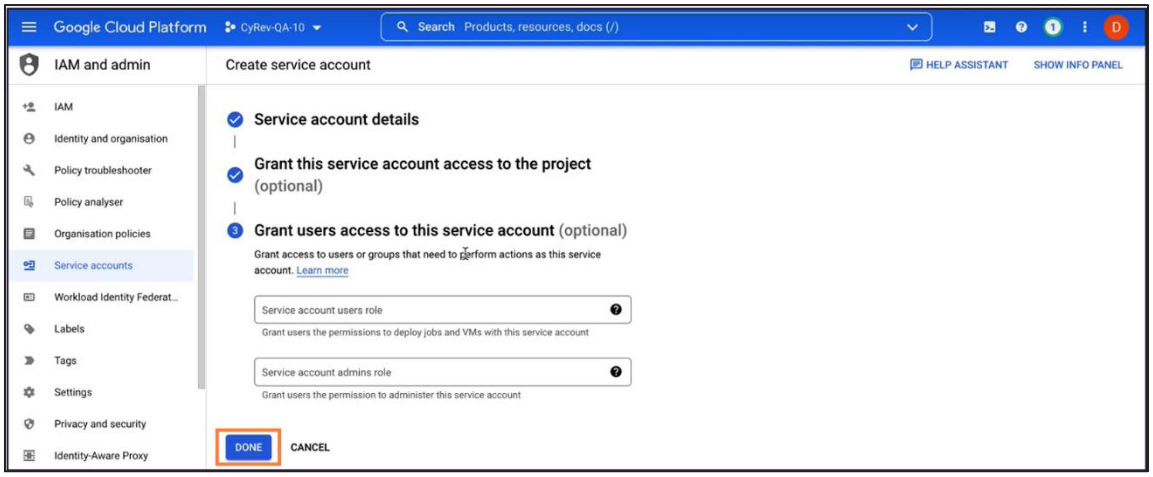
Created on: 2022-08-04

Role: Service Account Token Creator — Condition: Add condition

Impersonate service accounts (create OAuth2 access tokens, sign blobs or JWTs, etc.).

In the **Select a role** dropdown, choose the role of that was created in step 8. Then click **+ADD ANOTHER ROLE** and select **Service Account Token Creator Role**. Click **CONTINUE**.

12. Select **DONE** to finish setting up the new service account.



Service account details

Grant this service account access to the project (optional)

3 Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. Learn more

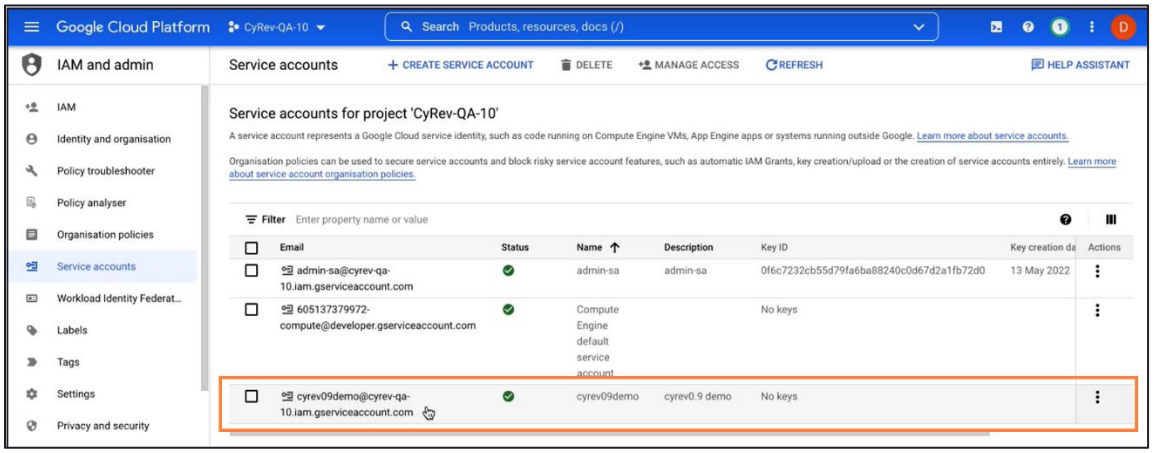
Service account users role

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

Grant users the permission to administer this service account

Once the new service account is created and configured it will appear in the service account list:



Service accounts for project 'CyRev-QA-10'

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps or systems running outside Google. Learn more about service accounts.

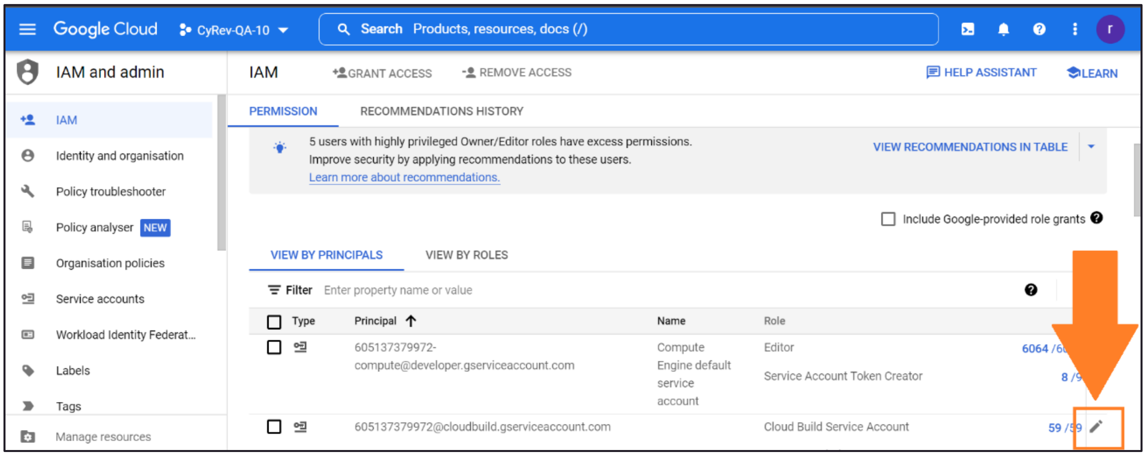
Organisation policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload or the creation of service accounts entirely. Learn more about service account organisation policies.

□	Email	Status	Name ↑	Description	Key ID	Key creation da	Actions
□	admin-sa@cyrev-qa-10.iam.gserviceaccount.com	✓	admin-sa	admin-sa	0f6c7232cb55d79fa6ba88240c0d67d2a1fb72d0	13 May 2022	⋮
□	605137379972-compute@developer.gserviceaccount.com	✓	Compute Engine default service account		No keys		⋮
□	cyrev09demo@cyrev-qa-10.iam.gserviceaccount.com	✓	cyrev09demo	cyrev0.9 demo	No keys		⋮

Assigning Permissions to the GCP Cloud Build Service Account

When you use the Google Cloud console or the `gcloud` CLI to import or export images for the first time, the tool attempts to enable the Cloud Build API and grant the required roles to the Cloud Build service account. You need to assign the below mentioned permissions to grant the access. Follow the steps to assign role for SA:

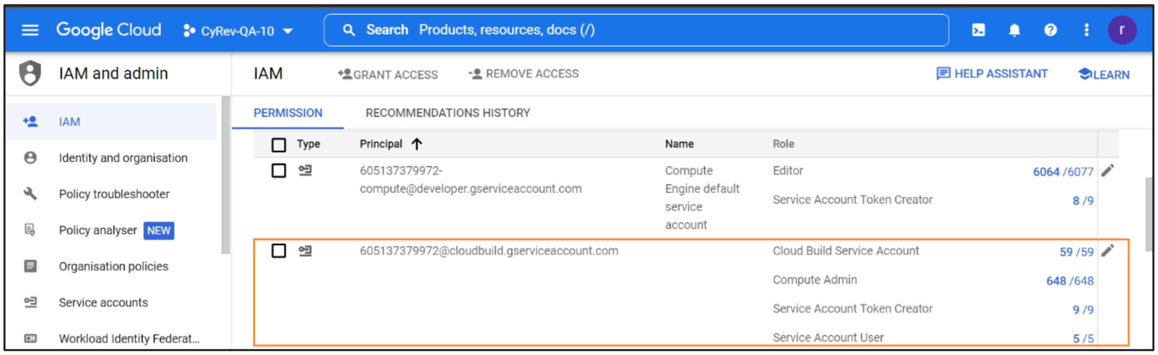
1. Navigate to **IAM and admin** page.
2. Select the **Cloud build service account** of the project. You can identify the cloud build service account project with naming (for example: *PROJECT_NUMBER*-compute@cloudbuild.gserviceaccount.com)
3. Click **Edit** button.



5 users with highly privileged Owner/Editor roles have excess permissions.
Improve security by applying recommendations to these users.
Learn more about recommendations.

Type	Principal	Name	Role	
☐	605137379972-compute@developer.gserviceaccount.com	Compute Engine default service account	Editor Service Account Token Creator	6064 /6 8 /9
☐	605137379972@cloudbuild.gserviceaccount.com		Cloud Build Service Account	59 /59

4. Click on **+ADD ANOTHER ROLE**. Select **Cloud Build Service Account Role** (if already not available) from drop-down. Similarly add the **Service Account User role, Service Account Token Creator Role,** and **Compute Admin role**.
5. Select **Save** to assign role. You can see the updated roles for Service Account.



Type	Principal	Name	Role	
☐	605137379972-compute@developer.gserviceaccount.com	Compute Engine default service account	Editor Service Account Token Creator	6064 /6077 8 /9
☐	605137379972@cloudbuild.gserviceaccount.com		Cloud Build Service Account Compute Admin Service Account Token Creator Service Account User	59 /59 648 /648 9 /9 5 /5

Configuring NAT

VM instances have IP addresses in Google Cloud. These IP addresses enable Google Cloud resources communicate with other resources in Google Cloud, in on-premises networks, or on the public internet.

Google Cloud offers both internal and external IP addresses. Internal IP addresses are not publicly routed and are only accessible within the Google Cloud platform. External IP addresses, on the other hand, are publicly routed and can be accessed from the internet.

Depending on your organization's security posture you can choose to deploy CyRev with either external or internal IP address during the installation.

If you choose internal IP address deployment you must configure NAT (Network Address Translation) for the VPC in the region where you wish to deploy CyRev to allow you to access CyRev components like the UI and the CyRev Server Host. Configuring NAT will allow the necessary network traffic to flow to the CyRev resources. You can refer to GCP documentation on how to Set up and manage network address translation with Cloud NAT for details on configuring NAT.

Obtain Persistent Image Access

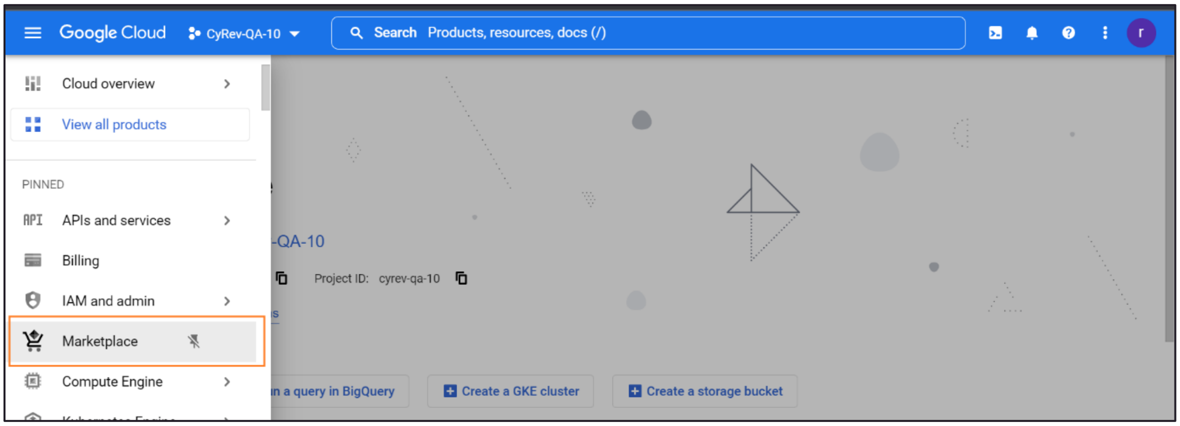
To start CyRev installation you must obtain access to the Persistent Systems GCP Public bucket containing them. You need to provide **CyRev Custom Service Account** details of the project where you wish CyRev to be deployed with the Persistent System's Support Team. To gain access you can reach out to the team at support@accelerite.com.

Deploying CyRev

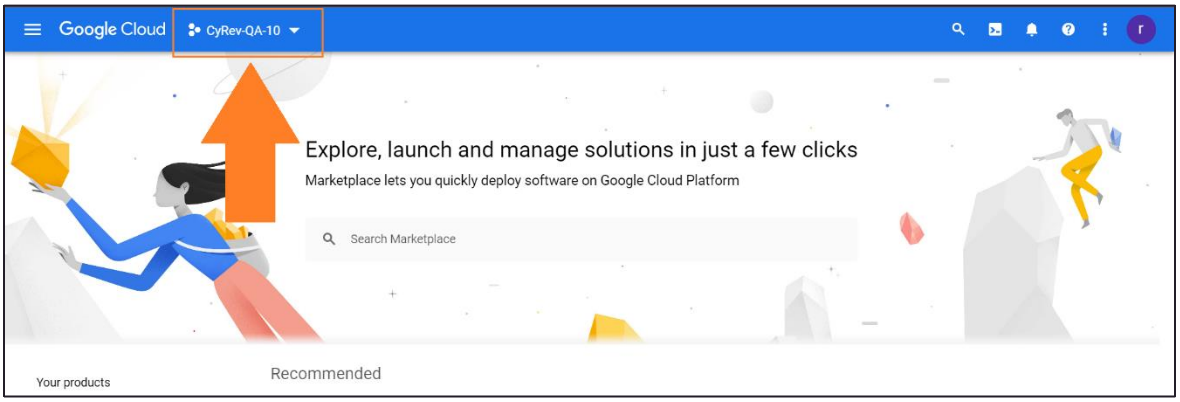
This section contains instructions for deploying CyRev on Google Cloud Platform.

Deployment through GCP Marketplace

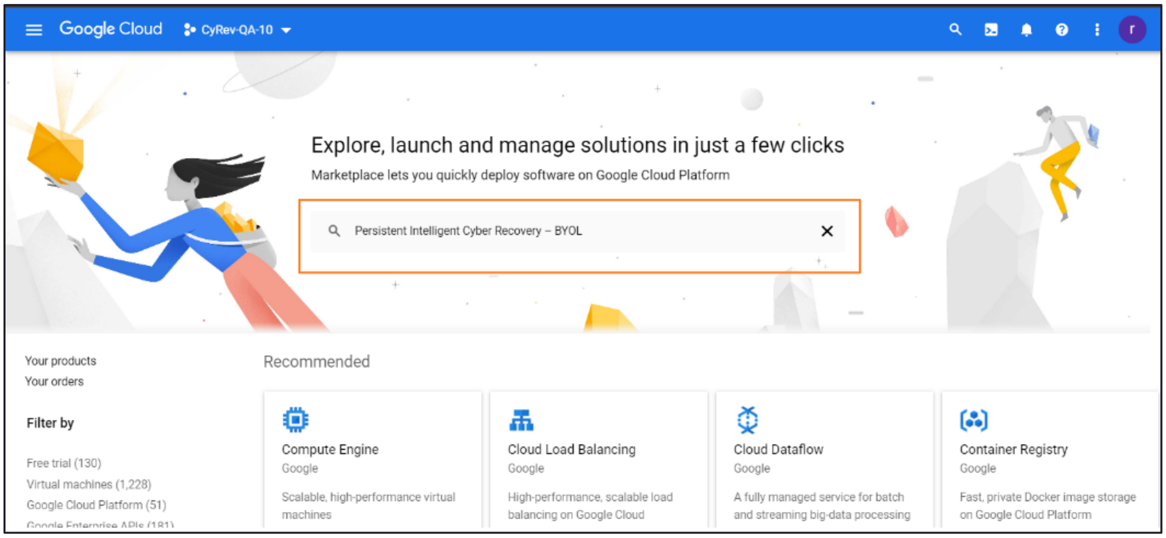
1. Login to your GCP account.
2. Navigate to the Marketplace (https://console.cloud.google.com/marketplace).



3. Select the GCP Project (the project where you wish to deploy the CyRev components; see the section on GCP Projects) from the project pulldown at the top of the window.


Google Cloud
CyRev-QA-10
Explore, launch and manage solutions in just a few clicks
Marketplace lets you quickly deploy software on Google Cloud Platform
Search Marketplace
Your products
Recommended

4. Search for “Persistent Intelligent Cyber Recovery – BYOL” in search bar.



Explore, launch and manage solutions in just a few clicks

Marketplace lets you quickly deploy software on Google Cloud Platform

Persistent Intelligent Cyber Recovery – BYOL

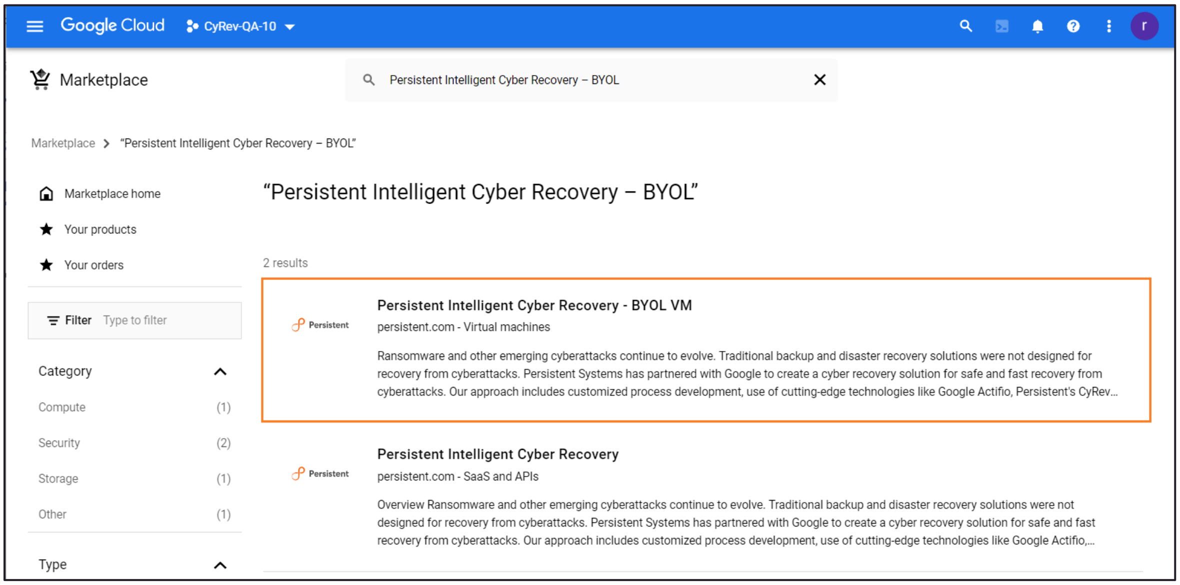
Scalable, high-performance virtual machines

High-performance, scalable load balancing on Google Cloud

A fully managed service for batch and streaming big-data processing

Fast, private Docker image storage on Google Cloud Platform

5. A listing for PICR-BYOL appears:



Persistent Intelligent Cyber Recovery – BYOL

“Persistent Intelligent Cyber Recovery – BYOL”

2 results

Persistent Intelligent Cyber Recovery - BYOL VM

persistent.com - Virtual machines

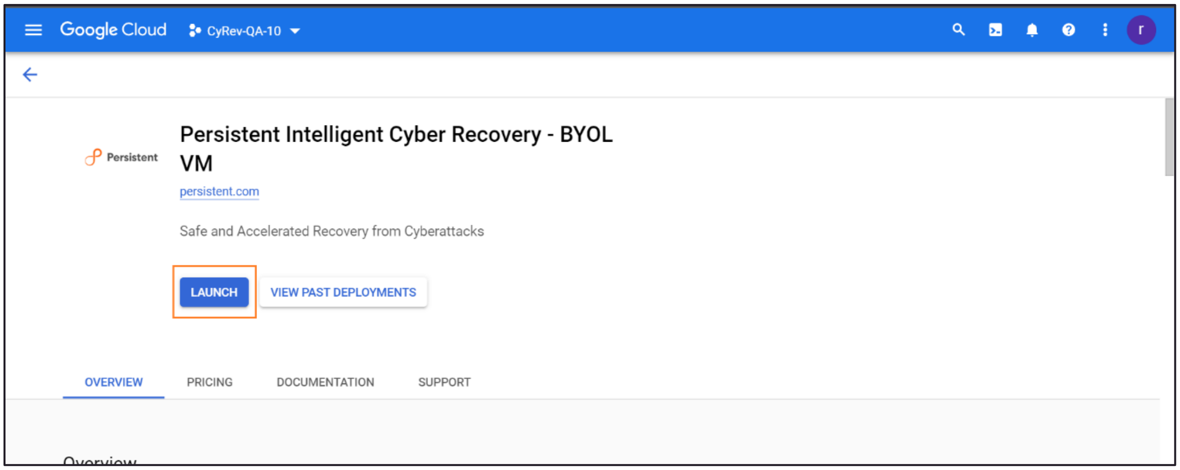
Ransomware and other emerging cyberattacks continue to evolve. Traditional backup and disaster recovery solutions were not designed for recovery from cyberattacks. Persistent Systems has partnered with Google to create a cyber recovery solution for safe and fast recovery from cyberattacks. Our approach includes customized process development, use of cutting-edge technologies like Google Actifio, Persistent's CyRev...

Persistent Intelligent Cyber Recovery

persistent.com - SaaS and APIs

Overview Ransomware and other emerging cyberattacks continue to evolve. Traditional backup and disaster recovery solutions were not designed for recovery from cyberattacks. Persistent Systems has partnered with Google to create a cyber recovery solution for safe and fast recovery from cyberattacks. Our approach includes customized process development, use of cutting-edge technologies like Google Actifio,...

6. Click the **PICR-BYOL** entry. This brings you to the PICR Marketplace Product Page:

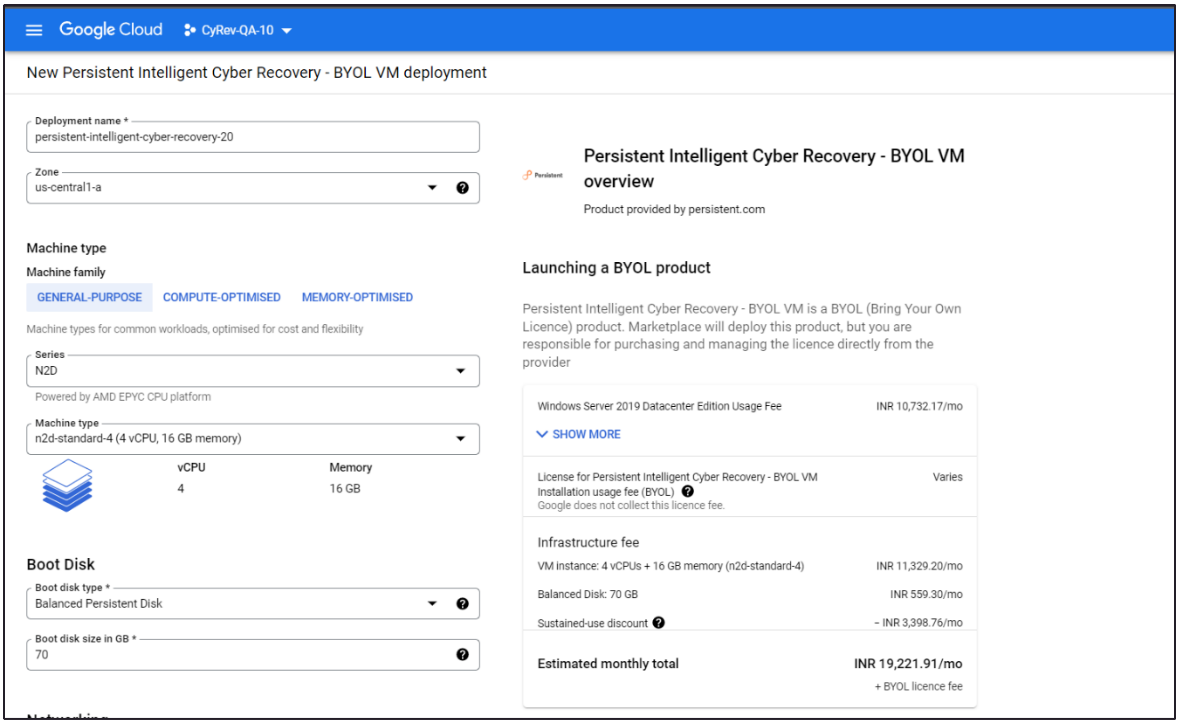


Persistent Intelligent Cyber Recovery - BYOL VM

persistent.com

Safe and Accelerated Recovery from Cyberattacks

7. Click **LAUNCH** to begin the deployment process. The PICR deployment page appears:



New Persistent Intelligent Cyber Recovery - BYOL VM deployment

Deployment name *: persistent-intelligent-cyber-recovery-20

Zone: us-central1-a

Machine type

Machine family

Machine types for common workloads, optimised for cost and flexibility

Series: N2D

Powered by AMD EPYC CPU platform

Machine type: n2d-standard-4 (4 vCPU, 16 GB memory)

vCPU	Memory
4	16 GB

Boot Disk

Boot disk type *: Balanced Persistent Disk

Boot disk size in GB *: 70

Persistent Intelligent Cyber Recovery - BYOL VM overview

Product provided by persistent.com

Launching a BYOL product

Persistent Intelligent Cyber Recovery - BYOL VM is a BYOL (Bring Your Own Licence) product. Marketplace will deploy this product, but you are responsible for purchasing and managing the licence directly from the provider

Windows Server 2019 Datacenter Edition Usage Fee	INR 10,732.17/mo
License for Persistent Intelligent Cyber Recovery - BYOL VM Installation usage fee (BYOL) Google does not collect this licence fee.	Varies
Infrastructure fee	
VM instance: 4 vCPUs + 16 GB memory (n2d-standard-4)	INR 11,329.20/mo
Balanced Disk: 70 GB	INR 559.30/mo
Sustained-use discount	– INR 3,398.76/mo
Estimated monthly total	INR 19,221.91/mo + BYOL licence fee

8. On the deployment page, you will specify details about the CyRev deployment and customize any of the deployment parameters as per your requirements.
   You must provide the following information:

   a. **Deployment name**: Specify an appropriate name for the CyRev deployment.

      Note: The length of the Deployment Name should not exceed 7-10 characters, all characters must be lower case, and it should not start with numbers.

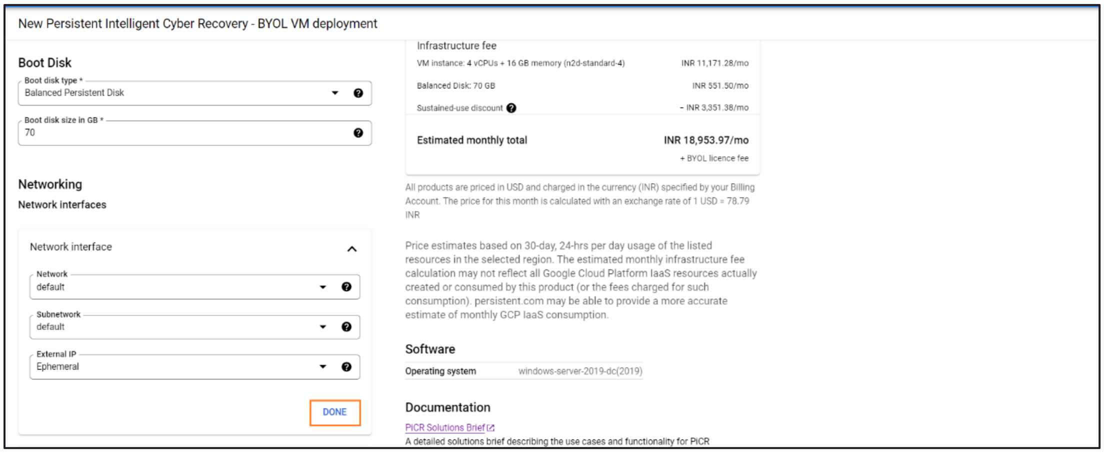
   b. **Zone**: Select the zone/country from the drop-down list where deployment will happen.

   c. **Series:** Choose the required CPU platform from the drop-down (**E2** is recommended).

   d. **Machine type**: Choose the required machine type from the drop-down (**e2-standard-4 (4vCPU,16 GB memory)** is recommended).

   e. In **Boot Disk** section, select the **boot disk type** from the drop-down (**Balanced Persistent Disk** is recommended) and enter the **Boot disk size in GB** (recommended size is 70GB).

f. Lower in the Deployment page you will find the **Networking** section:



New Persistent Intelligent Cyber Recovery - BYOL VM deployment

Boot Disk

Boot disk type *: Balanced Persistent Disk

Boot disk size in GB *: 70

Networking

Network interfaces

Network interface

Network: default

Subnetwork: default

External IP: Ephemeral

Infrastructure fee

VM instance: 4 vCPUs + 16 GB memory (n2d-standard-4)	INR 11,171.28/mo
Balanced Disk: 70 GB	INR 551.50/mo
Sustained-use discount	- INR 3,351.38/mo
Estimated monthly total	INR 18,953.97/mo + BYOL licence fee

All products are priced in USD and charged in the currency (INR) specified by your Billing Account. The price for this month is calculated with an exchange rate of 1 USD = 78.79 INR

Price estimates based on 30-day, 24-hrs per day usage of the listed resources in the selected region. The estimated monthly infrastructure fee calculation may not reflect all Google Cloud Platform IaaS resources actually created or consumed by this product (or the fees charged for such consumption). persistent.com may be able to provide a more accurate estimate of monthly GCP IaaS consumption.

Software

Operating system: windows-server-2019-dc(2019)

Documentation

PiCR Solutions Brief

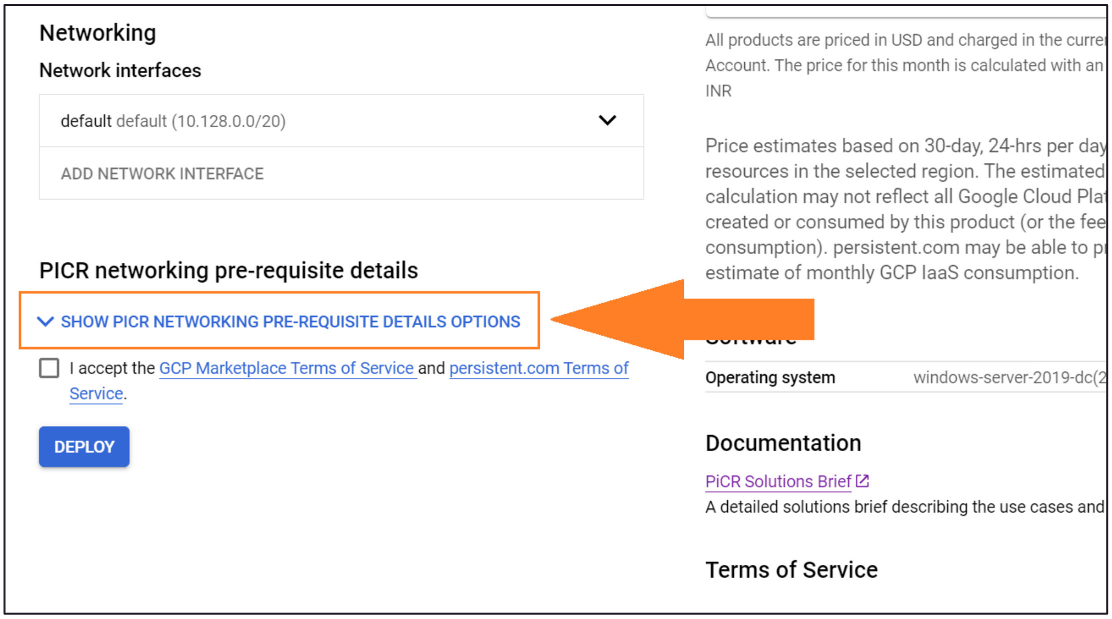
A detailed solutions brief describing the use cases and functionality for PiCR

Complete the Networking section by selecting the following values:

Parameters	Deployment With External IP	Deployment with Internal IP
Network	Choose Network where you wish to deploy CyRev.	Choose Network where you wish to deploy CyRev. (Note: This VPC Network should have NAT enabled as mentioned in Configuring NAT section).
Subnetwork	Choose Subnetwork where you wish to deploy CyRev.	Choose Subnetwork where you wish to deploy CyRev. (Note: This VPC Subnetwork should have NAT enabled as mentioned in Configuring NAT section).
External IP	Ephemeral	None

Then select **DONE**.

g. In the Networking section below the **Boot Disk** section is the **PICR networking pre-requisites details** section:



Networking

Network interfaces

default default (10.128.0.0/20)

ADD NETWORK INTERFACE

PICR networking pre-requisite details

SHOW PICR NETWORKING PRE-REQUISITE DETAILS OPTIONS

□ I accept the GCP Marketplace Terms of Service and persistent.com Terms of Service.

DEPLOY

All products are priced in USD and charged in the curre
Account. The price for this month is calculated with an
INR

Price estimates based on 30-day, 24-hrs per day
resources in the selected region. The estimated
calculation may not reflect all Google Cloud Plat
created or consumed by this product (or the fee
consumption). persistent.com may be able to pr
estimate of monthly GCP IaaS consumption.

Software

Operating system	windows-server-2019-dc(2

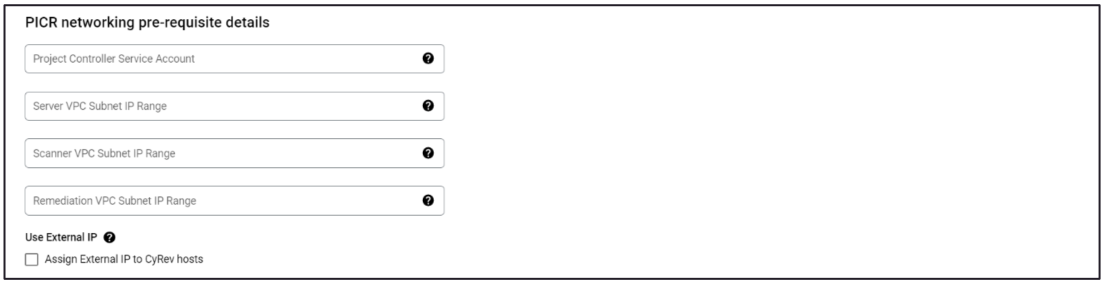
Documentation

PiCR Solutions Brief

A detailed solutions brief describing the use cases and

Terms of Service

Click the **SHOW PICR NETWORKING PRE-REQUISITE DETAILS OPTION** drop-down to expose the parameters that control CyRev deployment and operation:



PICR networking pre-requisite details

Project Controller Service Account

Server VPC Subnet IP Range

Scanner VPC Subnet IP Range

Remediation VPC Subnet IP Range

Use External IP

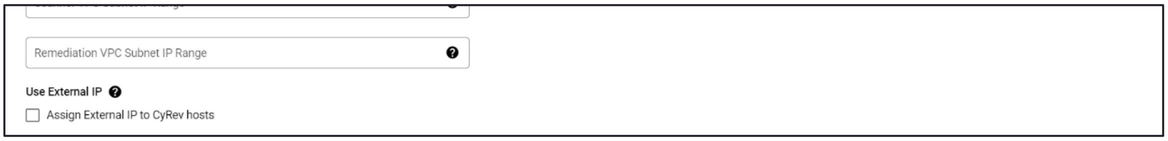
□ Assign External IP to CyRev hosts

h. Configure the fields as indicated below. These are parameters that you discovered or configured earlier (see the section on Preparing for CyRev Deployment):

Field	Description
Project Controller Service Account	A CyRev project service account name which has required permissions to provision the CyRev infrastructure. To obtain the service account details you can refer Create service account with a Custom Role section.
Server VPC Subnet IP Range	*Virtual Private Cloud* (VPC) networks are global resources. Each VPC network consists of one or more IP address range called *subnets*. Subnets are regional resources and have IP address ranges associated with them. Enter the unique & specific IP range which will be used as CyRev Server environment's subnet. (For more information refer Subnets

	Overview) Connect with your project network admin to get an available IP range as per your requirement. You can provide the IP range (CIDR) with difference of 16,32,48 in network ID. For Example: 10.208.16.0/20. 10.208.32.0/20 and 10.208.48.0/20. **Note**: The IP ranges must not overlap with the IP ranges of the subnets in which GCBDR is deployed.
Scanner VPC Subnet IP Range	Enter the unique & specific IP range which will be used as Scanner VPC environment's subnet. Connect with your project network admin to get an available IP range as per your requirement.
Remediation VPC Subnet IP Range	Enter the unique & specific IP range which will be used as Remediation VPC environment's subnet. Connect with your project network admin to get an available IP range as per your requirement.

i. The **Use External IP** section determines whether your CyRev deployment will be an external or internal deployment (see Configuring NAT for details.) For an external deployment check the box **Assign External IP to CyRev hosts**; leave it unchecked if you want to have an internal deployment:

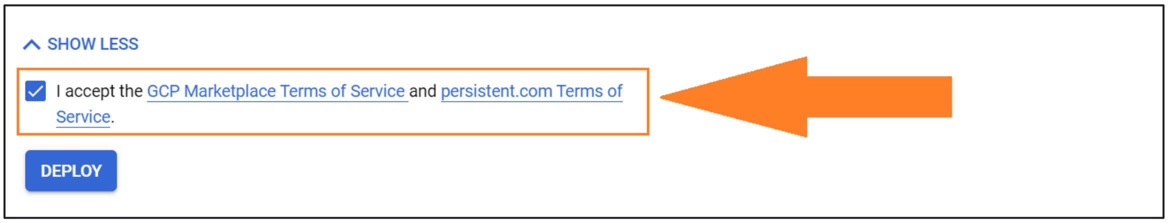


Remediation VPC Subnet IP Range

Use External IP

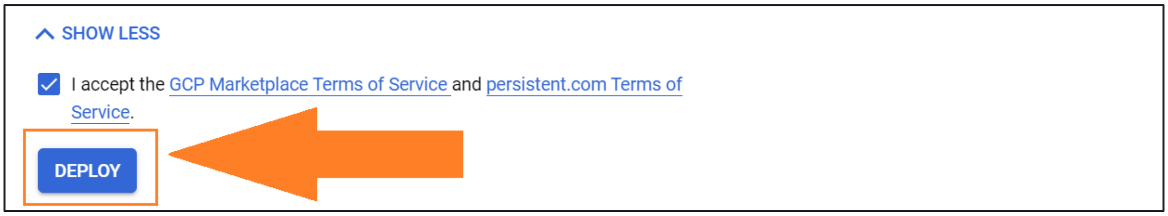
□ Assign External IP to CyRev hosts

j. Check the box to accept terms and conditions:



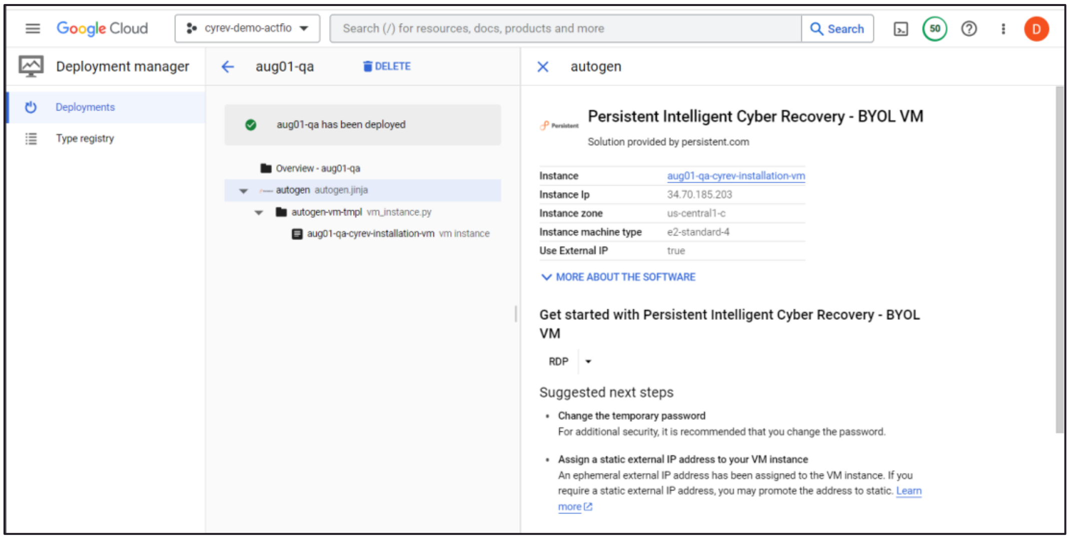
☑ I accept the GCP Marketplace Terms of Service and persistent.com Terms of Service.

k. Select **Deploy** to begin the deployment.



☑ I accept the GCP Marketplace Terms of Service and persistent.com Terms of Service.

Once deployment is complete, the post-deployment page appears:



aug01-qa has been deployed

- Overview - aug01-qa
- autogen autogen.jinja
  - autogen-vm-tmpl vm_instance.py
    - aug01-qa-cyrev-installation-vm vm instance

Persistent Intelligent Cyber Recovery - BYOL VM

Solution provided by persistent.com

Instance	aug01-qa-cyrev-installation-vm
Instance Ip	34.70.185.203
Instance zone	us-central1-c
Instance machine type	e2-standard-4
Use External IP	true

Get started with Persistent Intelligent Cyber Recovery - BYOL VM

Suggested next steps

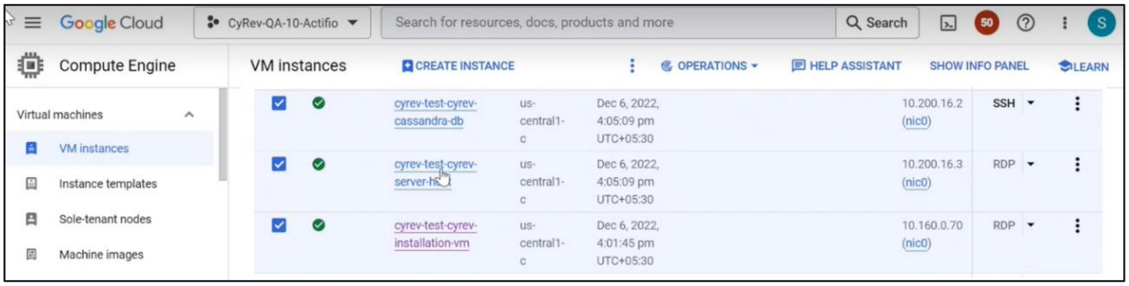
- Change the temporary password
  For additional security, it is recommended that you change the password.
- Assign a static external IP address to your VM instance
  An ephemeral external IP address has been assigned to the VM instance. If you require a static external IP address, you may promote the address to static. Learn more

This page shows details about the resources deployed.

As described in the Introduction CyRev is comprised of various VM components and storage resources securely deployed into the specified project. The section below contains the instructions for the configuration of some of the deployed CyRev components, such as the Installation VM, CyRev Server host, Database, VPC, Firewall rules, Service Accounts, Cloud routes, and Buckets.

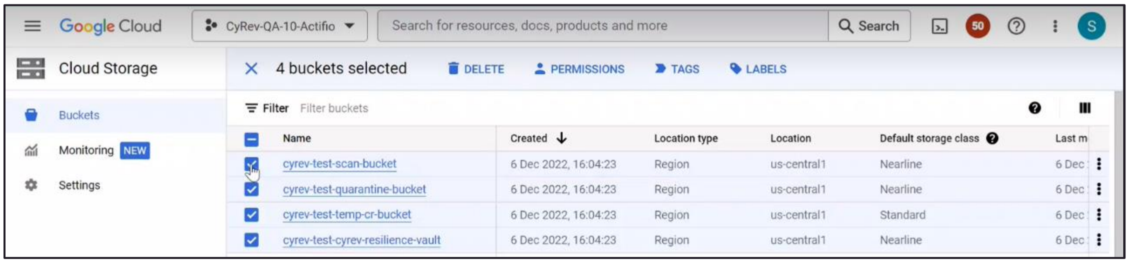
Accessing the CyRev Server Host and Buckets

You can check the status of the deployed CyRev hosts from the GCP Console by navigating to **Compute Engine →VM instances**.



☑	✓	cyrev-test-cyrev-cassandra-db	us-central1-c	Dec 6, 2022, 4:05:09 pm UTC+05:30	10.200.16.2 (nic0)	SSH
☑	✓	cyrev-test-cyrev-server-h	us-central1-c	Dec 6, 2022, 4:05:09 pm UTC+05:30	10.200.16.3 (nic0)	RDP
☑	✓	cyrev-test-cyrev-installation-vm	us-central1-c	Dec 6, 2022, 4:01:45 pm UTC+05:30	10.160.0.70 (nic0)	RDP

You can also check the status of the deployed buckets by selecting **Cloud Storage → Buckets.**



4 buckets selected

☐	Name	Created ↓	Location type	Location	Default storage class	Last m
☑	cyrev-test-scan-bucket	6 Dec 2022, 16:04:23	Region	us-central1	Nearline	6 Dec
☑	cyrev-test-quarantine-bucket	6 Dec 2022, 16:04:23	Region	us-central1	Nearline	6 Dec
☑	cyrev-test-temp-cr-bucket	6 Dec 2022, 16:04:23	Region	us-central1	Standard	6 Dec
☑	cyrev-test-cyrev-resilience-vault	6 Dec 2022, 16:04:23	Region	us-central1	Nearline	6 Dec

Note: You should make note of the VM names and IP addresses for the CyRev Server and Installation VM, and the names/IDs of the Scan and Cyber Resilience Vault buckets, as these will be needed when you start using CyRev for Test and Production.

You also need to create credentials for the CyRev Server host by referring to the section on Creating Host Credentials. Upon the successful deployment of infrastructure, you can access the hosts through RDP by using IP address.

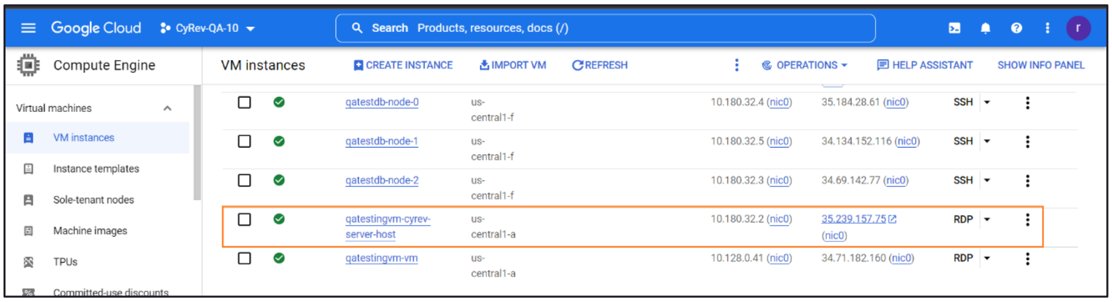
Note: Provide the CyRev Server Service Account to the persistent support team to add the necessary permissions to allow the necessary infrastructure deployment. To gain access you can reach out to the team at support@accelerite.com.

Note: The default windows updates are disabled on the CyRev Server Host you can take the updates as per your organization policy. You need to stop the CyRev services during update installation to avoid any issues.

Obtain Dashboard Credentials

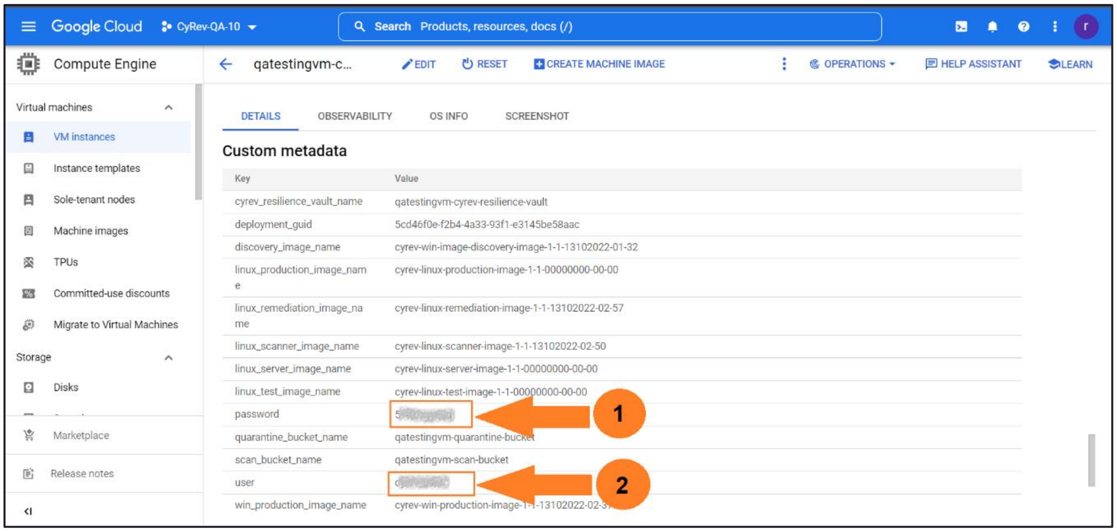
To use the CyRev dashboard you need to obtain the username and password for your UI. Follow the steps to obtain your UI credentials:

1. Navigate to **Compute Engine** → **VM instances** on your GCP cloud console.
2. Select the VM with deployment name with **cyrev-server-host** from the deployed VM's.



□	✓	qatestdb-node-0	us-central1-f	10.180.32.4 (nic0)	35.184.28.61 (nic0)	SSH
□	✓	qatestdb-node-1	us-central1-f	10.180.32.5 (nic0)	34.134.152.116 (nic0)	SSH
□	✓	qatestdb-node-2	us-central1-f	10.180.32.3 (nic0)	34.69.142.77 (nic0)	SSH
□	✓	qatestingvm-cyrev-server-host	us-central1-a	10.180.32.2 (nic0)	35.239.157.75 (nic0)	RDP
□	✓	qatestingvm-vm	us-central1-a	10.128.0.41 (nic0)	34.71.182.160 (nic0)	RDP

3. Scroll-down to the **Custom Metadata** section and make note of the **Password** (1) and **Username** (2) from the available data.



Custom metadata

Key	Value
cyrev_resilience_vault_name	qatestingvm-cyrev-resilience-vault
deployment_guid	5cd46f0e-f2b4-4a33-93f1-e3145be58aac
discovery_image_name	cyrev-win-image-discovery-image-1-1-13102022-01-32
linux_production_image_name	cyrev-linux-production-image-1-1-00000000-00-00
linux_remediation_image_name	cyrev-linux-remediation-image-1-1-13102022-02-57
linux_scanner_image_name	cyrev-linux-scanner-image-1-1-13102022-02-50
linux_server_image_name	cyrev-linux-server-image-1-1-00000000-00-00
linux_test_image_name	cyrev-linux-test-image-1-1-00000000-00-00
password	[redacted]
quarantine_bucket_name	qatestingvm-quarantine-bucket
scan_bucket_name	qatestingvm-scan-bucket
user	[redacted]
win_production_image_name	cyrev-win-production-image-1-1-13102022-02-3

Accessing The CyRev Dashboard

Follow these steps to access the CyRev Dashboard:

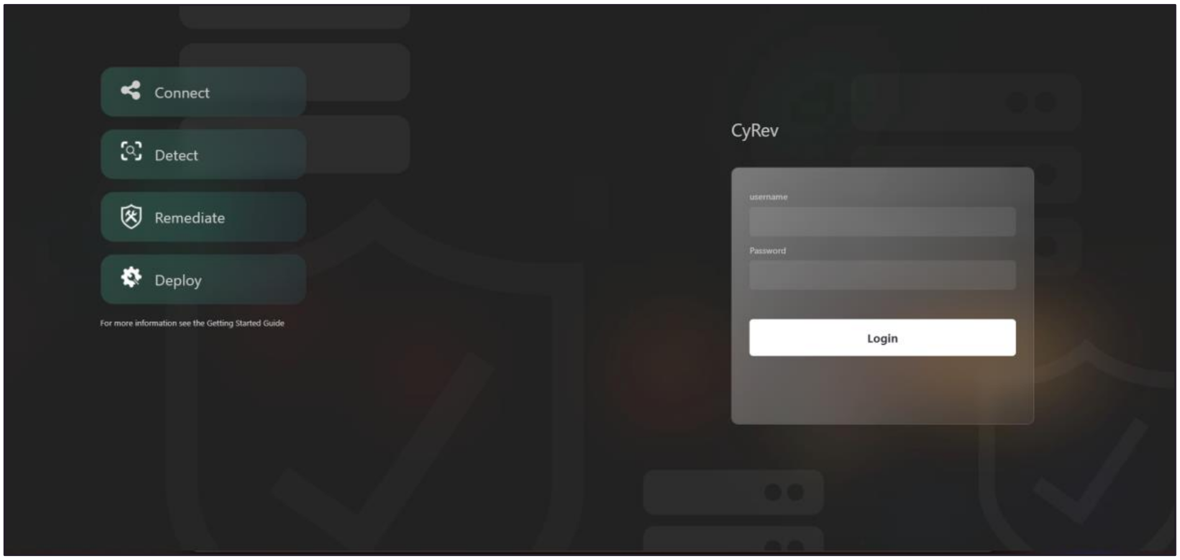
1. Connect to the CyRev Server Host from your desktop via RDP.
   (**Note**: You need to create VPC peering between Jump Serve/Bastion Host and CyRev Sever Host if you have an internal IP deployment.)
2. Wait for the browser to open automatically and connect to the CyRev Dashboard using the following URL:

   `https://127.0.0.1:3001`

   Note: CyRev UI Dashboard is supported on Microsoft Edge and Chrome browser**.**

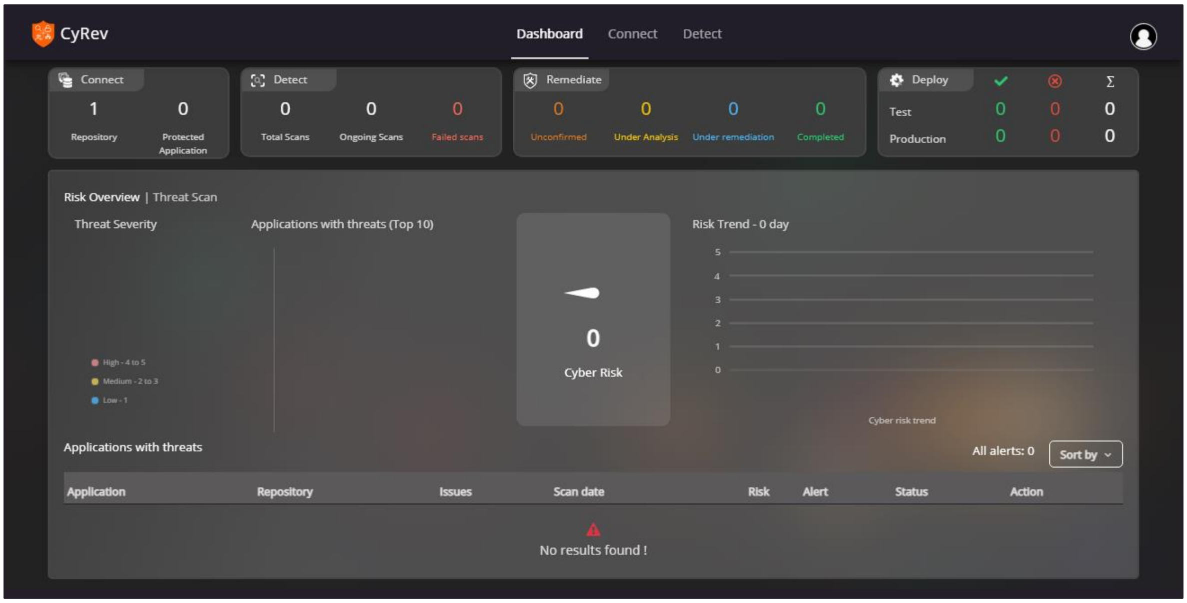
   Note: Do not terminate the command line services that are launched during startup.

3. This will show the CyRev login screen:



For more information see the Getting Started Guide

4. Enter your username and password you obtained in the section on Obtaining Dashboard Credentials. You will see the CyRev UI dashboard:



Application	Repository	Issues	Scan date	Risk	Alert	Status	Action

No results found !

Configuring GCBDR Image Provider

To access the DR images from GCBDR image provider you need to make necessary configuration to the GCBDR. You need to obtain the details of backup server service account and need to assign certain permission to configure GCBDR with CyRev.

Obtaining GCBDR Backup Appliance Details

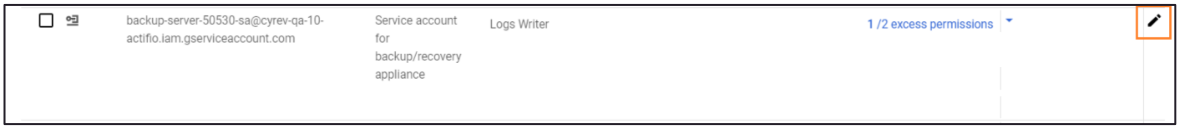
Follow the steps to obtain the Backup Appliance details:

1. Login to the Management Console of the GCP Backup and DR.
2. Click the **Manage** and select the **Appliances** option from drop-down list.
3. Make a note of the backup appliance name and associated service account name.

Assigning permissions to Backup Appliance sevice account

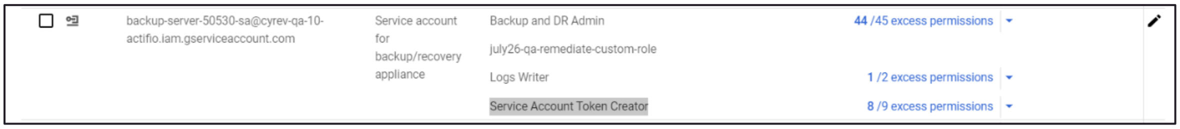
Follow the steps to assign permissions to Backup Server service account:

1. Go to GCP console.
2. Navigate to **IAM and admin** page.
3. Search for the backup appliance service account.
4. Select the backup appliance service account of the GCBDR.
5. Click **Edit** button.



☐	backup-server-50530-sa@cyrev-qa-10-actifio.iam.gserviceaccount.com	Service account for backup/recovery appliance	Logs Writer	1 /2 excess permissions

6. Click on **+ADD ANOTHER ROLE**. Select **Backup and DR Admi**n (if already not available) from drop-down. Similarly add the **Log Writers**, **Service Account Token Creator Role**, and add the **remediate custom role** created during CyRev deployment.
7. Select **Save** to assign role. You can see the updated roles for Service Account.



☐	backup-server-50530-sa@cyrev-qa-10-actifio.iam.gserviceaccount.com	Service account for backup/recovery appliance	Backup and DR Admin july26-qa-remediate-custom-role Logs Writer Service Account Token Creator	44 /45 excess permissions 1 /2 excess permissions 8 /9 excess permissions

Configuring Backup Appliance Service Account Credentials

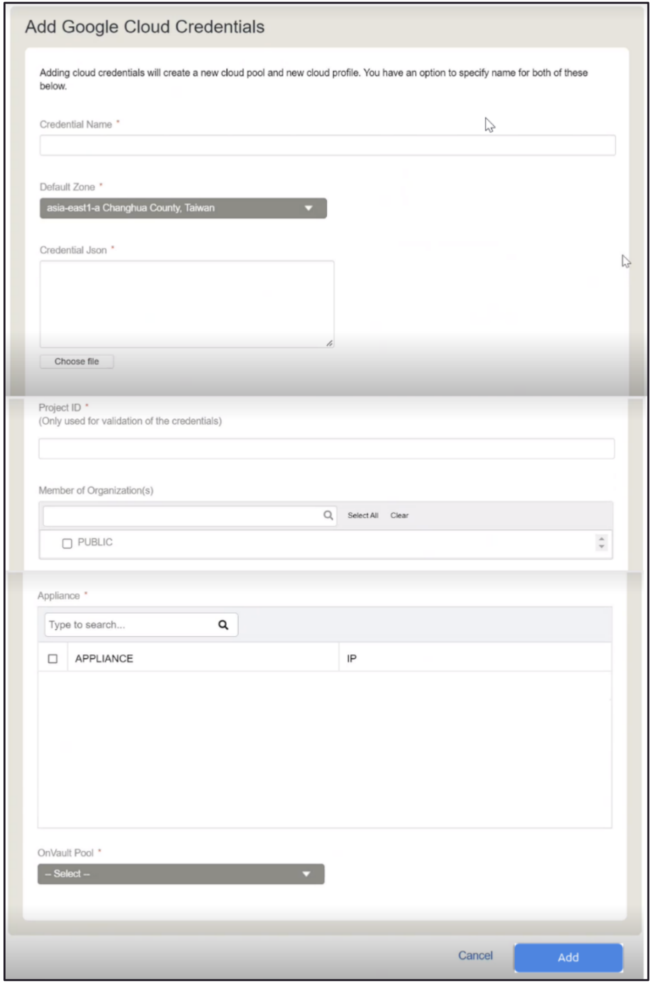
Before proceeding to use CyRev, you must configure Backup Appliance SA with GCBDR to access information about applications and system images and you must the add the configuration file name to

Configuring cloud credentials for Backup Appliance Service Account on GCBDR

Follow the steps to register the Backup Appliance Service Account with the GCBDR Management Console:

1. Login to the **Management Console** of the GCP Backup and DR.
2. Click the **Manage** and select the **Credentials** option from drop-down list.
3. Select **+ADD GOOGLE CLOUD CREDENTIALS** and enter below details:

Parameter	Description
Credential Name	Unique name that you want to identify the credential with. **Note:** Make a note of the credential name that is required in configuration.
Default Zone	Select the zone in which backup appliance is deployed.
Appliance	Choose the backup appliance to which the credentials should be linked. This credential will only be available to the selected appliance.
On Vault Pool	Select the associated Vault pool from the drop-down.


Add Google Cloud Credentials

Adding cloud credentials will create a new cloud pool and new cloud profile. You have an option to specify name for both of these below.

Credential Name *

Default Zone *: asia-east1-a Changhua County, Taiwan

Credential Json *

Project ID *
(Only used for validation of the credentials)

Member of Organization(s)

□ PUBLIC

Appliance *

□	APPLIANCE	IP

OnVault Pool *: -- Select --

4. Click **Add** to save the credentials.

You can see the added credentials in the list of cloud credentials. Your configuration of the Service account is completed. Following section guide you to configure the credential name in configuration file.

Configuring Cloud Credential Name Parameters in CyRev Configuration file

You need to update the configuration file for the cloud credentials details. Follow the steps to update configuration file:

1. Connect to the CyRev Server Host from your desktop via Remote Desktop Protocol (RDP).
   (**Note**: You need to create VPC peering between Jump Serve/Bastion Host and CyRev Sever Host if you have an internal IP deployment.)
2. Run **Notepad** with administrative privileges.
3. In Notepad open the file “`C:\cyrev\bin\config.json`”
4. Update the cloud credential information in the below parameter:

Parameter	Description
`Cloud_credential_name`	Provide CyRev project credentials name added in Configure cloud credentials for Backup Appliance Service Account on GCBDR section.

5. **Save** the file.

Next Steps

Once you have deployed the CyRev Server you can proceed and start using CyRev to scan images, detect ransomware attacks and create clean images, as described in the *CyRev User Guide*.

There are other components of the CyRev deployment that are employed during a reaction to a ransomware attack – the Remediation Environment, Testing Environment, and the replacement application Production Environment. These components need not be deployed until needed to save resource costs. The deployment of the Test Environment and the Production Environment are covered in the reference section of this guide.

Contacting Support

Persistent Systems Software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by being able to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Submit enhancement requests online
- Download software patches
- Look up Persistent support contacts
- Enter into discussions with other software customers
- Research and register for software training

To access the Self-serve knowledge base, visit the Persistent System Support home page at

https://support.persistent.com/hc/en-us

Most of the support areas require that you register on the Persistent Systems Support Portal. Many also require a support contract.

To register an account at the Persistent Systems Support Portal, visit

https://support.persistent.com/hc/en-us

To know more about registration process at Persistent Systems support portal, visit

https://support.persistent.com/hc/en-us/articles/202042570-New-user-registration-process

Reference Information

Deploying A Test Management Host

You can initiate a test and select the images to be run in the air-gapped testing environment. Once the clean images are saved in the CR Vault they are ready to deploy. The exported disks in CRV are attached to the new Application Test host. Prior to taking applications into production.

Follow the steps to deploy the Test Management Host:

1. RDP to Installation VM.
2. Navigate to 'C:\cyber_recovery\installer\infra\services' directory.
3. Open the variables.json file in notepad.
4. Update the below:

Parameter	Example	Description
subnet_test	10.162.80.0/20	Enter the unique & specific IP range in CIDR notation which will be used as Test environment's subnet. Connect with your project network admin to get an available IP range as per your requirement.
project_sa_email	admin-sa@cyrev-qa-1-actifio.iam.gserviceaccount.com	A CyRev project service account name which has required permissions to provision the CyRev infrastructure. To obtain the service account details you can refer Create service account with a Custom Role section.
peer_project_sa_email	admin-sa@cyrev-qa-1-actifio.iam.gserviceaccount.com	A CyRev project service account name which has required permissions to provision the CyRev infrastructure. To obtain the service account details you can refer Create a CyRev Custom Service Account section.

5. Open **PowerShell prompt** with administrative privileges.
6. Navigate to the directory ‘`c:\cyber_recovery\installer\infra\’` with the following command:

```
cd .\cyber_recovery\installer\infra\
```

7. Enter the following command to create the test management host:

```
pwsh.\picr_deployment.ps1 -input_env “create_testing”
```

You can check the status of the deployed host from the **Compute Engine → VM instances** page on GCP console.
Note: You should make note of the VM name and IP address for the Test Management Host, as these will be needed when you start using CyRev for testing.

You also need to create the credentials for Test Management host by referring Create Host Credentials. You can connect to Test Host via RDP by using a internal/external IP address. (**Note**: You need to create VPC peering between Jump Serve/Bastion Host and CyRev Test Management Host if you have an internal IP deployment.) Refer **CyRev User Guide** to deploy test application VM.

Deploying A Production Deployment Management Host

Upon successful testing of the images on Test Application VM, it's time to establish production environment and select the tested images to deploy in the production environment. You must confirm proper operation of host before going live.

Follow the steps to deploy the Production Deployment Management Host:

1. RDP to Installation VM.
2. Navigate to ‘`C:\cyber_recovery\installer\infra\services`’ directory.
3. Open the `variables.json` file in notepad.
4. Update the below:

Parameter	Example	Description
`subnet_ production`	10.162.64.0/20	Enter the unique & specific IP range in CIDR notation which will be used as Production environment’s subnet. Connect with your project network admin to get an available IP range as per your requirement.

Parameter	Example	Description
`project_sa_email`	admin-sa@cyrev-qa-1-actifio.iam.gserviceaccount.com	A CyRev project service account name which has required permissions to provision the CyRev infrastructure. To obtain the service account details you can refer Create service account with a Custom Role section.
`peer_project_sa_email`	admin-sa@cyrev-qa-1-actifio.iam.gserviceaccount.com	A CyRev project service account name which has required permissions to provision the CyRev infrastructure. To obtain the service account details you can refer Create service account with a Custom Role section.

5. Open **PowerShell prompt** with administrative privileges.
6. Navigate to the directory ‘`c:\cyber_recovery\installer\infra\`’ with the following command:

```
cd .\cyber_recovery\installer\infra\
```

7. Enter the following command to create the production Deployment Management host:

```
pwsh.\picr_deployment.ps1 -input_env "create_production"
```

You can check the status of the deployed host from the **Compute Engine → VM instances** Page on GCP console.

Note: You should make note of the VM name and IP address for the Production Deployment Management Host, as these will be needed when you start using CyRev for Production.

You also need to create the credentials for Production Deployment Management host by referring Create Host Credentials section. You can connect to Production Host via RDP by using a internal/external IP address. (**Note**: You need to create VPC peering between Jump Serve/Bastion Host and CyRev Production Deployment Management Host if you have an internal IP deployment). Refer **CyRev User Guide** to deploy production application VM.

Uninstalling CyRev and Resources

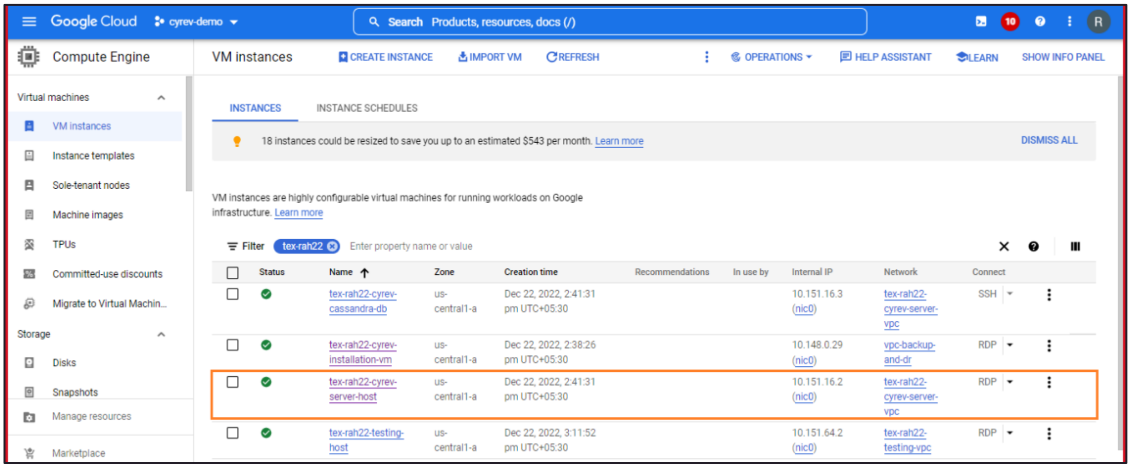
The resources installed during CyRev installation must be uninstalled in the order listed below to ensure that all resources created by CyRev are cleaned.

Uninstall CyRev Resources

To release the resources consumed by the components deployed by CyRev (such as the CyRev Server VM, VPC, firewall rules and subnets, etc) you may use the `cyrev_uninstall` command as described below. This command does not delete the storage buckets and Installation VM; to reclaim those resources you need to delete them manually via the GCP console as described in subsequent sesctions..

Follow the steps to use `crev_uninstall` to remove the CyRev components from your infrastructure:

1. Go to the VM instances page on GCP console.
2. CyRev Resources are protected by accidental deletion by enabling the **Delete Protection** feature on VMs. In order to delete the resources you must disable this feature as follows:
   a. Click the name of the **CyRev Server Host instance** to see VM the instance details. The instance details page displays.

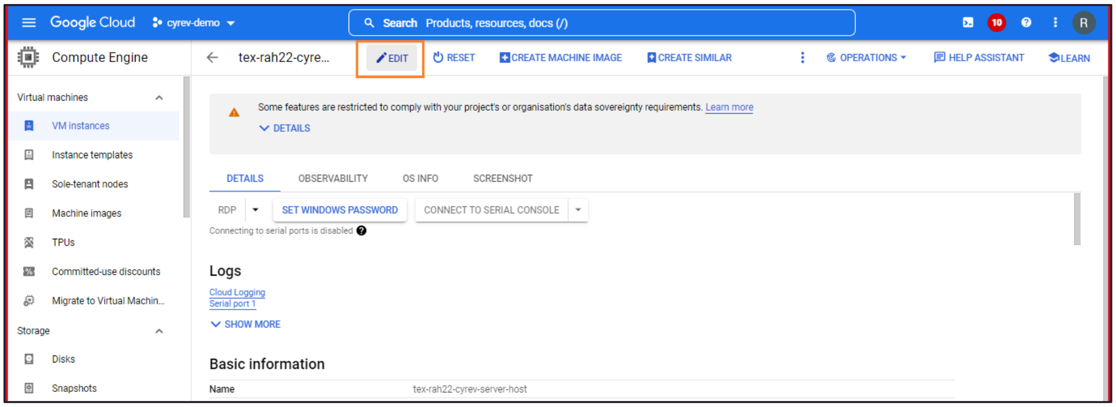


18 instances could be resized to save you up to an estimated $543 per month. Learn more

VM instances are highly configurable virtual machines for running workloads on Google infrastructure. Learn more

□	Status	Name ↑	Zone	Creation time	Recommendations	In use by	Internal IP	Network	Connect
□	✓	tex-rah22-cyrev-cassandra-db	us-central1-a	Dec 22, 2022, 2:41:31 pm UTC+05:30			10.151.16.3 (nic0)	tex-rah22-cyrev-server-vpc	SSH
□	✓	tex-rah22-cyrev-installation-vm	us-central1-a	Dec 22, 2022, 2:38:26 pm UTC+05:30			10.148.0.29 (nic0)	vpc-backup-and-dr	RDP
□	✓	tex-rah22-cyrev-server-host	us-central1-a	Dec 22, 2022, 2:41:31 pm UTC+05:30			10.151.16.2 (nic0)	tex-rah22-cyrev-server-vpc	RDP
□	✓	tex-rah22-testing-host	us-central1-a	Dec 22, 2022, 3:11:52 pm UTC+05:30			10.151.64.2 (nic0)	tex-rah22-testing-vpc	RDP

b. Click the **Edit** button at the top of the page.

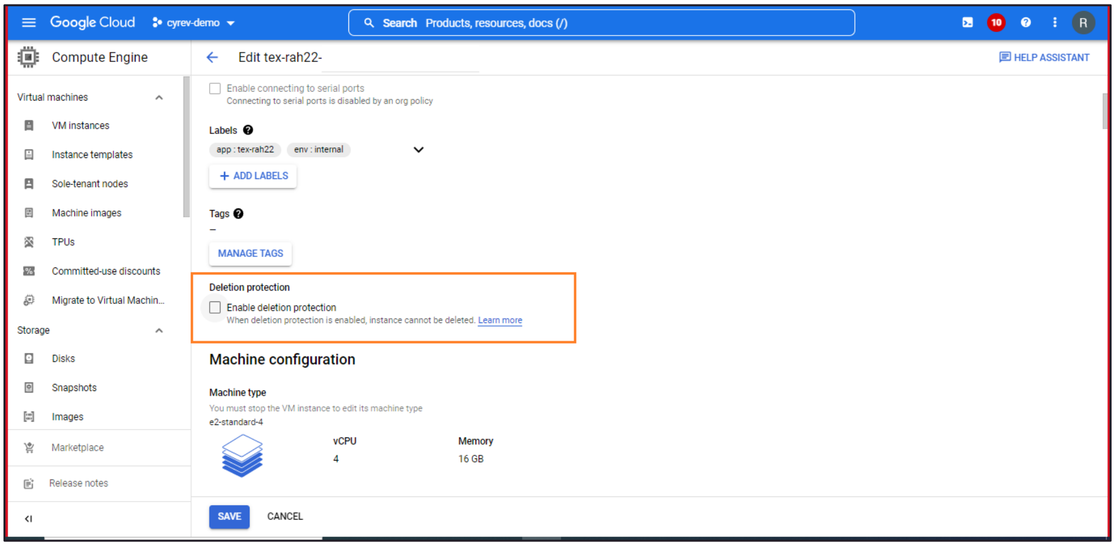


Some features are restricted to comply with your project's or organisation's data sovereignty requirements. Learn more

Connecting to serial ports is disabled

Name tex-rah22-cyrev-server-host

c. Under **Deletion Protection**, uncheck the **Enable Delete Protection** box:



□ Enable connecting to serial ports
Connecting to serial ports is disabled by an org policy

Labels: app : tex-rah22, env : internal

Tags: –

Deletion protection
□ Enable deletion protection
When deletion protection is enabled, instance cannot be deleted. Learn more

Machine type
You must stop the VM instance to edit its machine type
e2-standard-4
vCPU 4
Memory 16 GB

d. **Save** your changes.

e. Similarly disable the Deletion protection on CyRev **Database**.

3. Connect to the CyRev Installation VM via RDP.
4. Open **PowerShell** with administrative privileges.Go to the directory `c:\cyber_recovery\installer\infra\services` using the following command:

```
cd c:\cyber_recovery\installer\infra\services
```

5. Delete the CyRev Resources using following command:

```
pwsh .\picr_deployment.ps1 -input_env "cyrev_uninstall"
```

You can verify the resources deletion from the GCP cloud console.

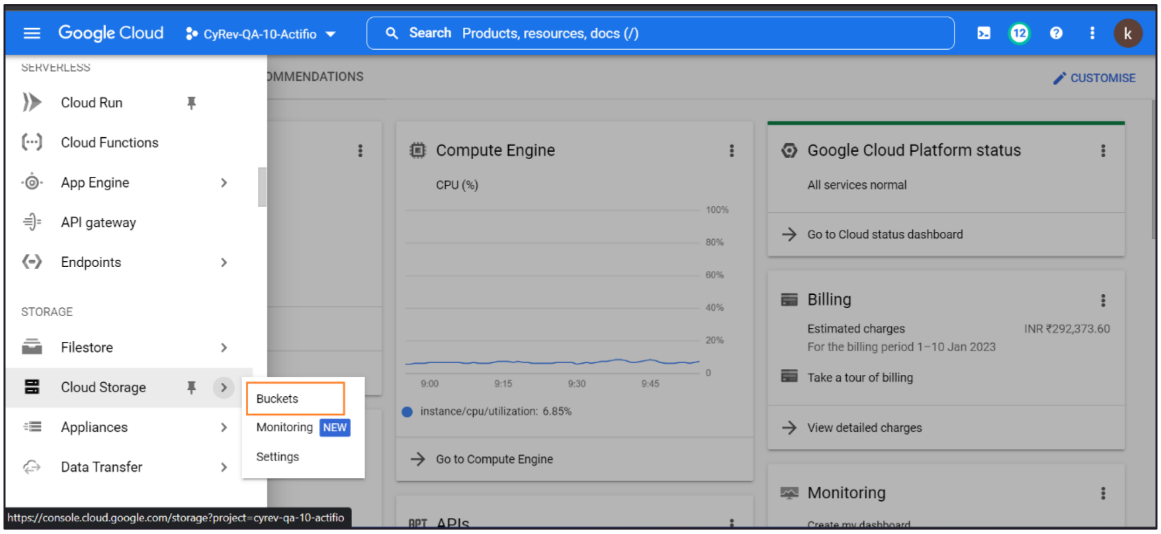
Again, **note that the above steps do not delete the CyRev Scan or Quarantine buckets, the Cyber Resilience Vault or the Installation VM**. If you wish to free those resources you will need to manually delete them via the GCP cloud console. You can delete the Installation VM as described in Uninstall Installation VM and storage buckets as described in Delete Storage Buckets below.

Delete the Cyrev Storage Buckets

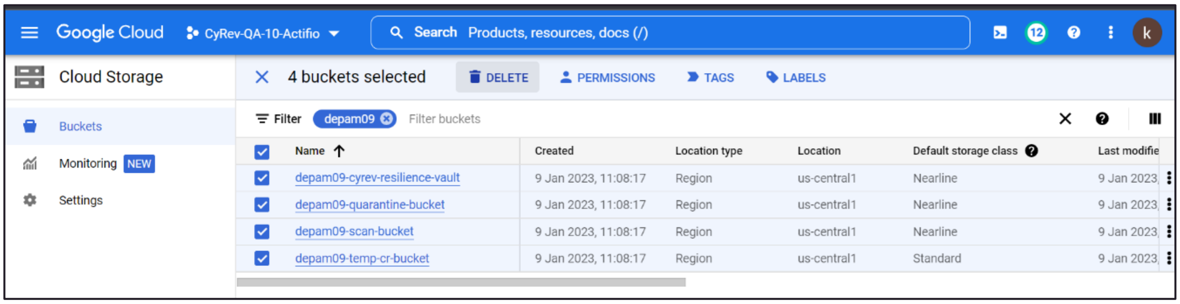
You need to delete the CyRev storage buckets manually using the Google Cloud Console. Follow these steps to delete the storage buckets:

Note: Deleting a bucket also deletes any objects stored within the bucket. These objects cannot be recovered.

1. Sign into the Google Cloud Console.
2. Go to the **Cloud Storage** → **Buckets** page.

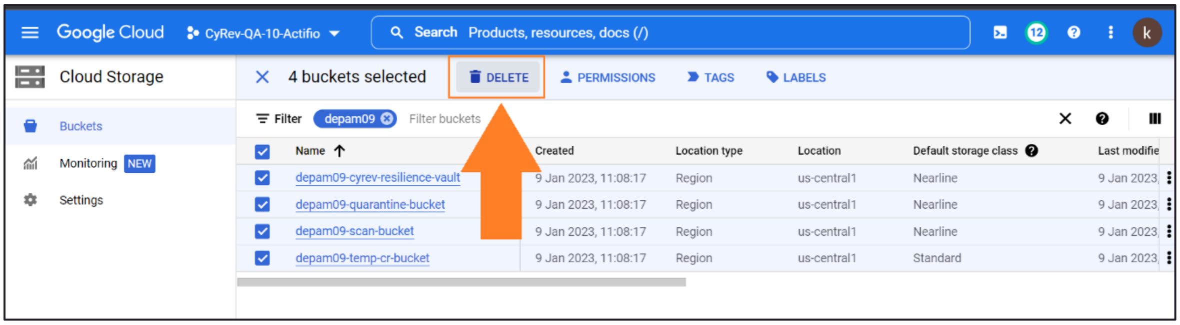


3. Select the checkbox for the following buckets:
   a. CyRev Scan Bucket
   b. CyRev Quarantine Bucket
   c. CyRev Temp CR bucket
   d. CyRev Cyber Resilience Vault



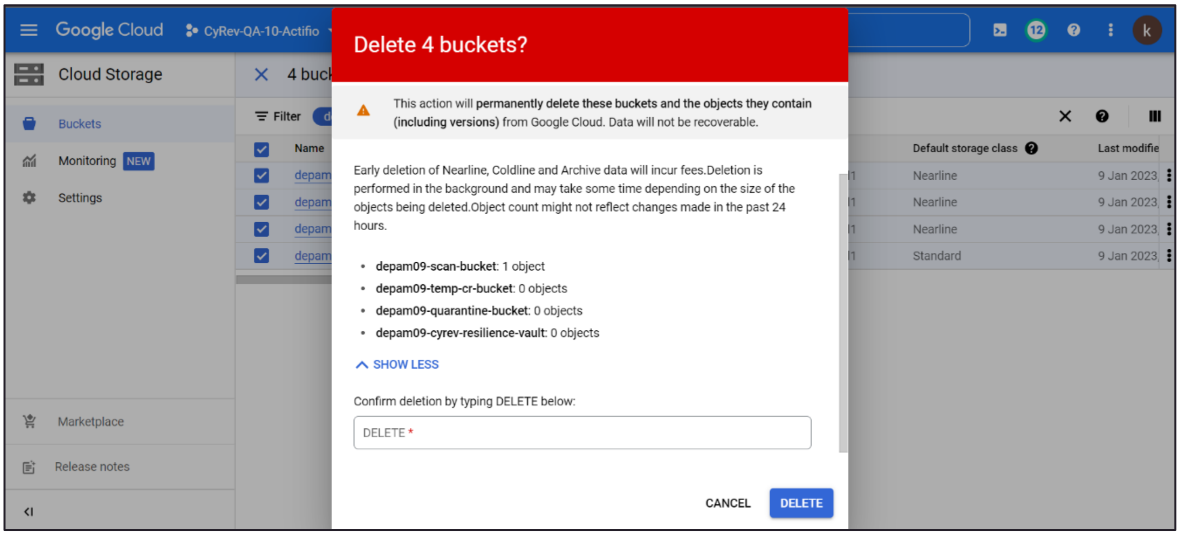
☑	Name ↑	Created	Location type	Location	Default storage class	Last modifie
☑	depam09-cyrev-resilience-vault	9 Jan 2023, 11:08:17	Region	us-central1	Nearline	9 Jan 2023,
☑	depam09-quarantine-bucket	9 Jan 2023, 11:08:17	Region	us-central1	Nearline	9 Jan 2023,
☑	depam09-scan-bucket	9 Jan 2023, 11:08:17	Region	us-central1	Nearline	9 Jan 2023,
☑	depam09-temp-cr-bucket	9 Jan 2023, 11:08:17	Region	us-central1	Standard	9 Jan 2023,

4. Click **Delete**. The confirmation window appears.



Name	Created	Location type	Location	Default storage class	Last modifie
depam09-cyrev-resilience-vault	9 Jan 2023, 11:08:17	Region	us-central1	Nearline	9 Jan 2023,
depam09-quarantine-bucket	9 Jan 2023, 11:08:17	Region	us-central1	Nearline	9 Jan 2023,
depam09-scan-bucket	9 Jan 2023, 11:08:17	Region	us-central1	Nearline	9 Jan 2023,
depam09-temp-cr-bucket	9 Jan 2023, 11:08:17	Region	us-central1	Standard	9 Jan 2023,

5. Type **DELETE** in the description box to confirm the operation.



Delete 4 buckets?

This action will **permanently delete these buckets and the objects they contain (including versions)** from Google Cloud. Data will not be recoverable.

Early deletion of Nearline, Coldline and Archive data will incur fees.Deletion is performed in the background and may take some time depending on the size of the objects being deleted.Object count might not reflect changes made in the past 24 hours.

- **depam09-scan-bucket**: 1 object
- **depam09-temp-cr-bucket**: 0 objects
- **depam09-quarantine-bucket**: 0 objects
- **depam09-cyrev-resilience-vault**: 0 objects

Confirm deletion by typing DELETE below:

DELETE *

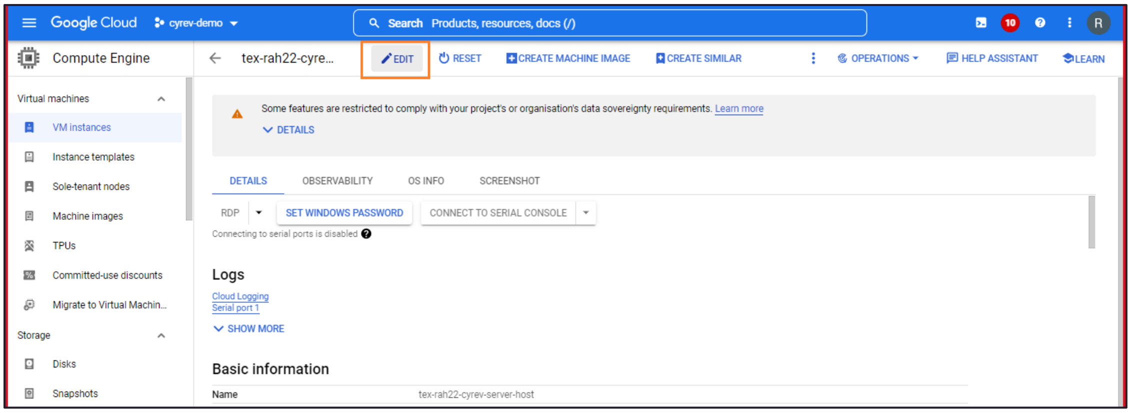
6. Click **DELETE** to delete bucket permanently.

Uninstall Test Environment

You can delete any deployed Test Environment after completing the Testing process. Follow the steps to uninstall the Test Management Host:

1. Go to the VM instances page on the GCP console.
2. CyRev Resources are protected by accidental deletion by enabling the **Delete Protection** feature on VMs. In order to delete the resources you must disable this feature as follows:
   a. Click the name of the **CyRev Test Management Host instance** to toggle deletion protection. The instance details page displays.

b. Click the **Edit** button at the top of the page.

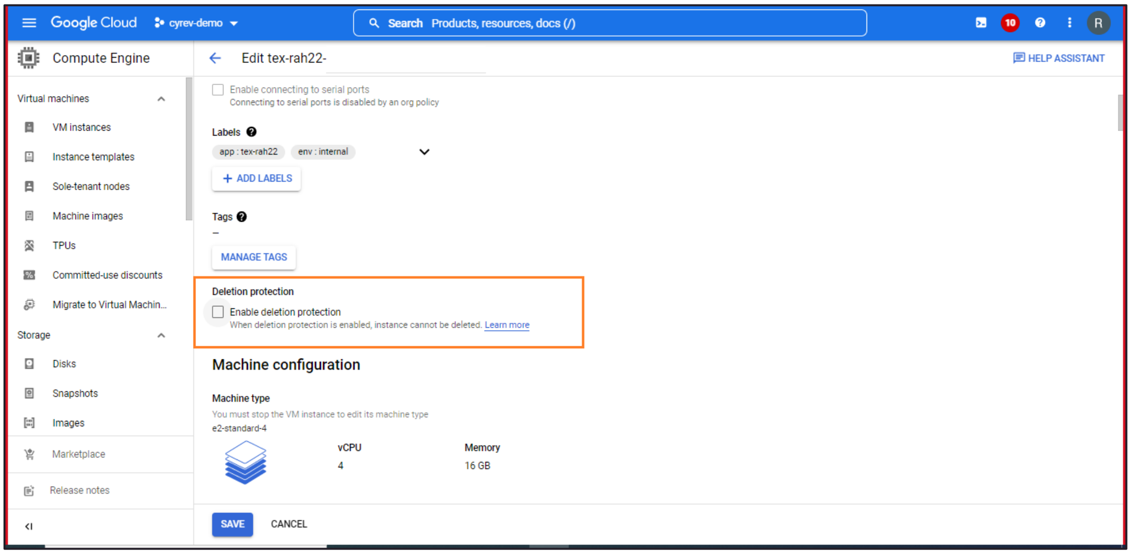


Some features are restricted to comply with your project's or organisation's data sovereignty requirements. Learn more

Connecting to serial ports is disabled

Name tex-rah22-cyrev-server-host

c. Under **Deletion Protection**, uncheck the **Enable Delete Protection** box:



☐ Enable connecting to serial ports
Connecting to serial ports is disabled by an org policy

Labels
app : tex-rah22 env : internal

Tags
–

Deletion protection
☐ Enable deletion protection
When deletion protection is enabled, instance cannot be deleted. Learn more

Machine configuration

Machine type
You must stop the VM instance to edit its machine type
e2-standard-4

vCPU 4

Memory 16 GB

d. **Save** your changes.

3. Connect to the CyRev Installation VM via RDP.
4. Open PowerShell with administrative privileges.
5. Go to directory `c:\cyber_recovery\installer\infra` using the following command:

```
cd c:\cyber_recovery\installer\infra
```

6. Delete the CyRev Test Resources using following command:

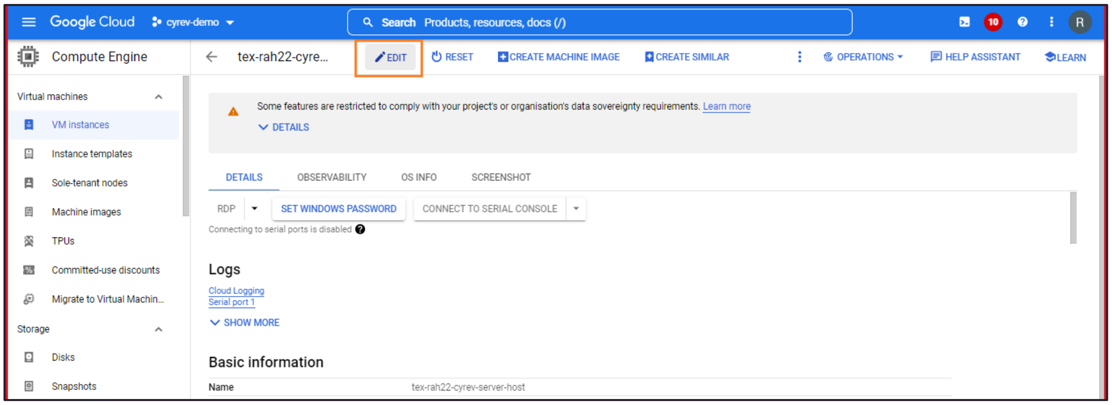
```
pwsh.\picr_deployment.ps1 -input_env "destroy_testing"
```

The above command deletes the Testing environment.

Uninstall Production Environment

You can delete any deployed Production Environment after completing the production deployment. Follow the steps to uninstall CyRev Production Deployment Management Host:

1. Go to the VM instances page on GCP console.
2. CyRev Resources are protected by accidental deletion by enabling the **Delete Protection** feature on VMs. In order to delete the resources you must disable this feature as follows:
   a. Click the name of the **CyRev Production Deployment Management Host instance** to toggle deletion protection. The instance details page displays.
   b. Click the **Edit** button at the top of the page.

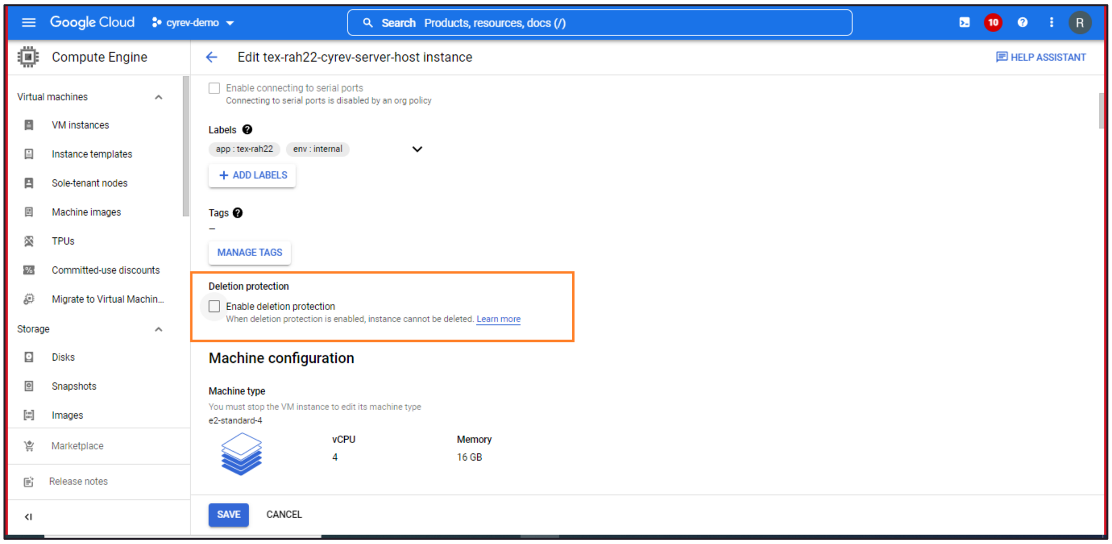


Some features are restricted to comply with your project's or organisation's data sovereignty requirements. Learn more

Connecting to serial ports is disabled

Name tex-rah22-cyrev-server-host

   c. Under **Deletion Protection**, uncheck the **Enable Delete Protection** box:



Edit tex-rah22-cyrev-server-host instance

□ Enable connecting to serial ports
Connecting to serial ports is disabled by an org policy

Labels
app : tex-rah22 env : internal

Tags
–

Deletion protection
□ Enable deletion protection
When deletion protection is enabled, instance cannot be deleted. Learn more

Machine configuration

Machine type
You must stop the VM instance to edit its machine type
e2-standard-4

vCPU	Memory
4	16 GB

   d. **Save** your changes
3. Connect to the CyRev Installation VM via RDP.
4. Open PowerShell with administrative privileges.

5. Go to directory “`c:\cyber_recovery\installer\infra`” using following command:

   ```
   cd c:\cyber_recovery\installer\infra
   ```

6. Delete the CyRev Resources using following command:

   ```
   pwsh.\picr_deployment.ps1 -input_env "destroy_production"
   ```

   The above command deletes the Production environment..

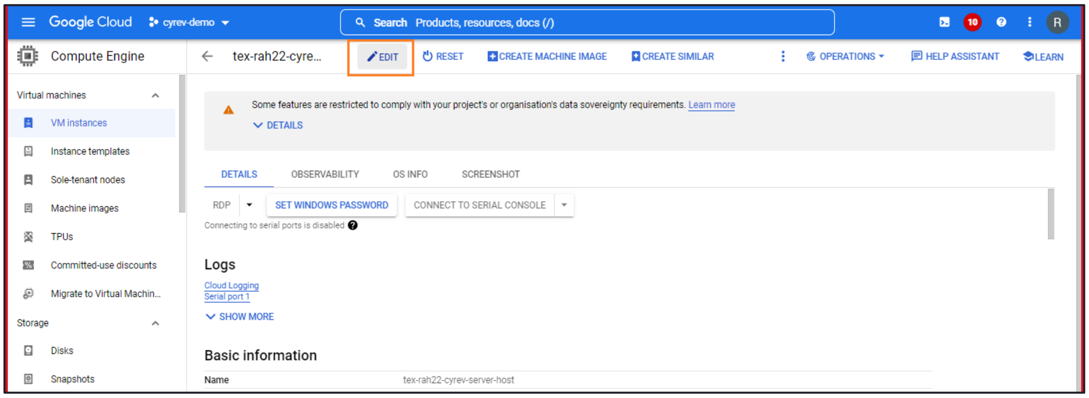
Uninstall the CyRev Installation VM

You need to delete the installation manually from the GCP cloud console. Follow these steps to delete installation VM from cloud console:

1. Go to the **VM instances** page on GCP console.
2. CyRev Resources are protected by accidental deletion by enabling the **Delete Protection** feature on VMs. In order to delete the resources you must disable this feature as follows :

   a. Click the name of the **CyRev Installation VM** to toggle deletion protection. The instance details page displays.

   b. Click the **Edit** button at the top of the page.

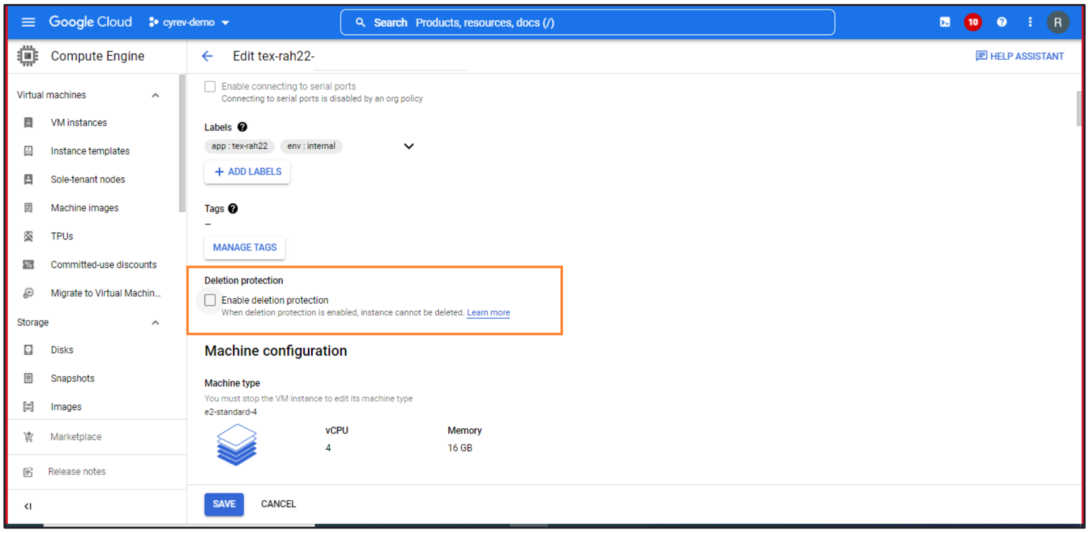


Some features are restricted to comply with your project's or organisation's data sovereignty requirements. Learn more

Connecting to serial ports is disabled

Name tex-rah22-cyrev-server-host

c. Under **Deletion Protection**, uncheck the **Enable Delete Protection** box:



□ Enable connecting to serial ports
Connecting to serial ports is disabled by an org policy

Labels
app : tex-rah22 env : internal

Tags
–

Deletion protection
□ Enable deletion protection
When deletion protection is enabled, instance cannot be deleted. Learn more

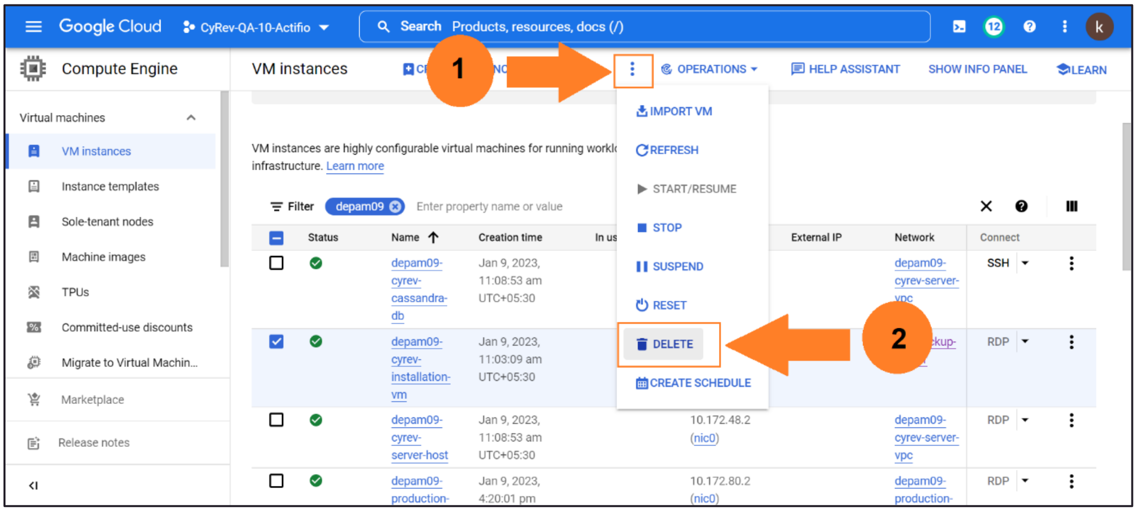
Machine configuration

Machine type
You must stop the VM instance to edit its machine type
e2-standard-4

vCPU	Memory
4	16 GB

d. **Save** your changes.

3. Select the Installation VM. Click the **more actions** button (1), then choose **Delete** (2) to remove installation VM.



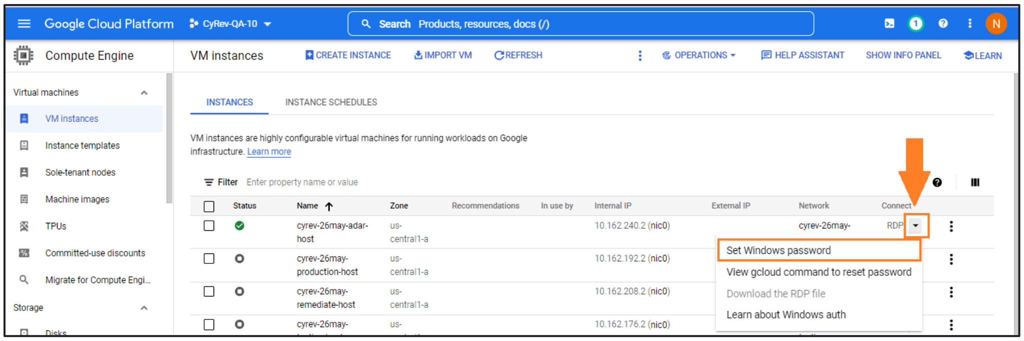
VM instances are highly configurable virtual machines for running workl
infrastructure. Learn more

	Status	Name ↑	Creation time	In us		External IP	Network	Connect
□	✓	depam09-cyrev-cassandra-db	Jan 9, 2023, 11:08:53 am UTC+05:30				depam09-cyrev-server-vpc	SSH
☑	✓	depam09-cyrev-installation-vm	Jan 9, 2023, 11:03:09 am UTC+05:30				ckup-	RDP
□	✓	depam09-cyrev-server-host	Jan 9, 2023, 11:08:53 am UTC+05:30		10.172.48.2 (nic0)		depam09-cyrev-server-vpc	RDP
□	✓	depam09-production-	Jan 9, 2023, 4:20:01 pm		10.172.80.2 (nic0)		depam09-production-	RDP

Creating Host Credentials

To use the CyRev Hosts you will need credentials to be able to connect to it. In most cases it’s necessary to create a new set of credentials for this purpose. Follow the steps to create credentials:

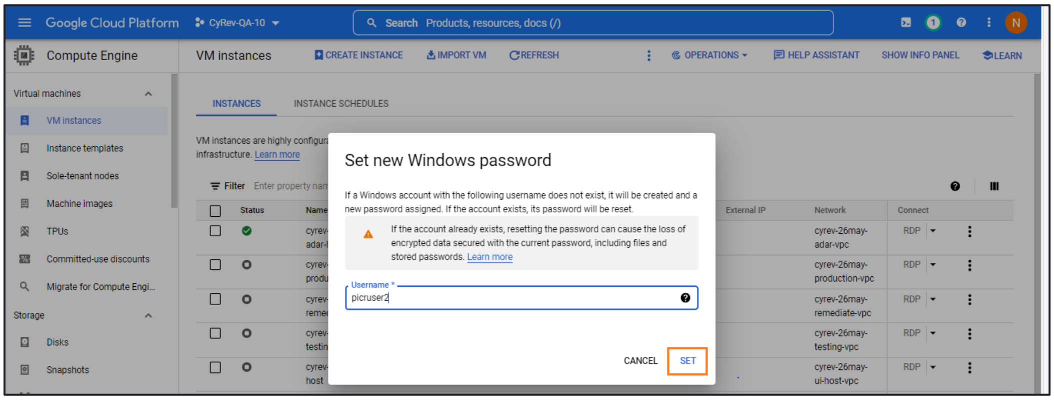
1. Navigate to **Compute Engine** → **VM instances**.
2. Select the Host **VM** form the list.
3. Select the **drop-down arrow** beside the **RDP** button in the **Connect** column for the VM.



VM instances are highly configurable virtual machines for running workloads on Google infrastructure. Learn more

Status	Name	Zone	Recommendations	In use by	Internal IP	External IP	Network	Connect
✓	cyrev-26may-adar-host	us-central1-a			10.162.240.2 (nic0)		cyrev-26may-	RDP
○	cyrev-26may-production-host	us-central1-a			10.162.192.2 (nic0)			
○	cyrev-26may-remediate-host	us-central1-a			10.162.208.2 (nic0)			
○	cyrev-26may-	us-			10.162.176.2 (nic0)			

4. Select the **Set Windows password** button. The **Set new Windows password** pop-up opens.
5. Enter the **Username** of your choice in the box and make a note of it.
6. Click **SET** to set the username.



Set new Windows password

If a Windows account with the following username does not exist, it will be created and a new password assigned. If the account exists, its password will be reset.

If the account already exists, resetting the password can cause the loss of encrypted data secured with the current password, including files and stored passwords. Learn more

Username * picruser2

Network	Connect
cyrev-26may-adar-vpc	RDP
cyrev-26may-production-vpc	RDP
cyrev-26may-remediate-vpc	RDP
cyrev-26may-testing-vpc	RDP
cyrev-26may-ui-host-vpc	RDP

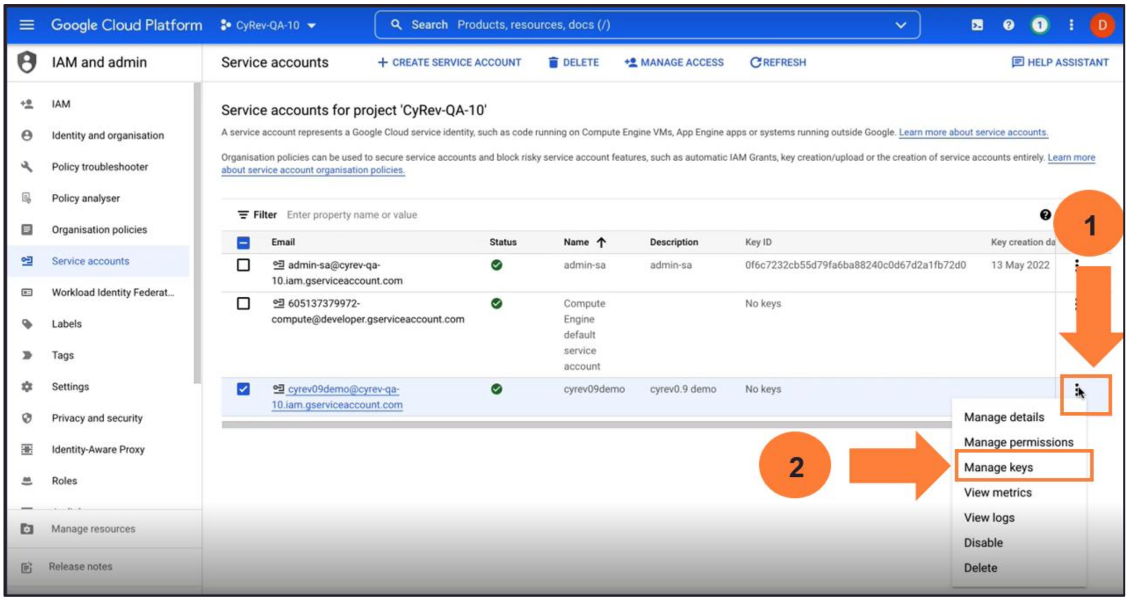
7. The **Password** is autogenerated and displayed on the page.

Note: You **must** remember these credentials for later use in connecting to the host to access. To avoid having to create and configure new host credentials you should note down the credentials that you just created, or save them to a credentials manager, etc.

Obtaining service account keys

Follow the steps to download the service keys for the CyRev Project service account:

1. Go to cloud console of CyRev GCP Project.
2. In the Cloud console, go to **IAM** page. Select the **Service accounts**.
3. Select the service account that you created for which you want to create keys and click on the three-dot button (1 below). Select **Manage keys** (**2**).



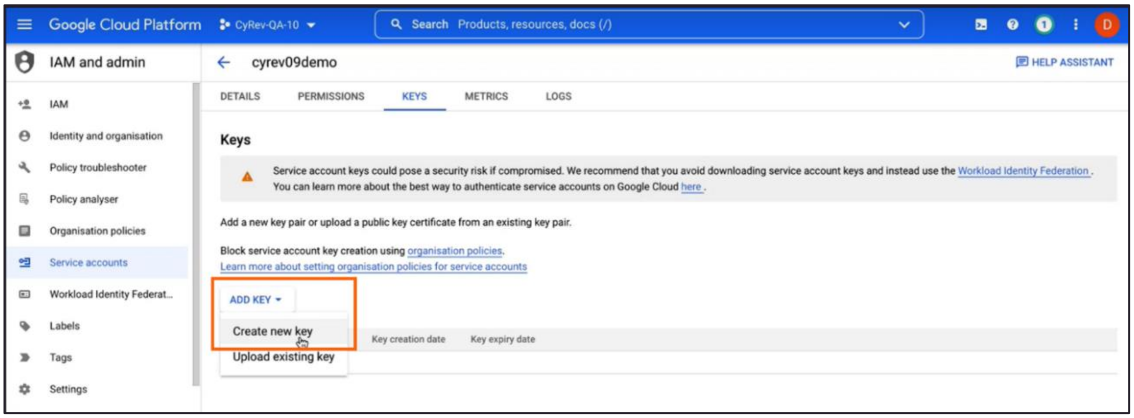
Service accounts for project 'CyRev-QA-10'

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps or systems running outside Google. Learn more about service accounts.

Organisation policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload or the creation of service accounts entirely. Learn more about service account organisation policies.

	Email	Status	Name ↑	Description	Key ID	Key creation da
□	admin-sa@cyrev-qa-10.iam.gserviceaccount.com	✓	admin-sa	admin-sa	0f6c7232cb55d79fa6ba88240c0d67d2a1fb72d0	13 May 2022
□	605137379972-compute@developer.gserviceaccount.com	✓	Compute Engine default service account		No keys	
☑	cyrev09demo@cyrev-qa-10.iam.gserviceaccount.com	✓	cyrev09demo	cyrev0.9 demo	No keys	

4. Click **ADD KEY** drop-down menu and select **Create new key**.



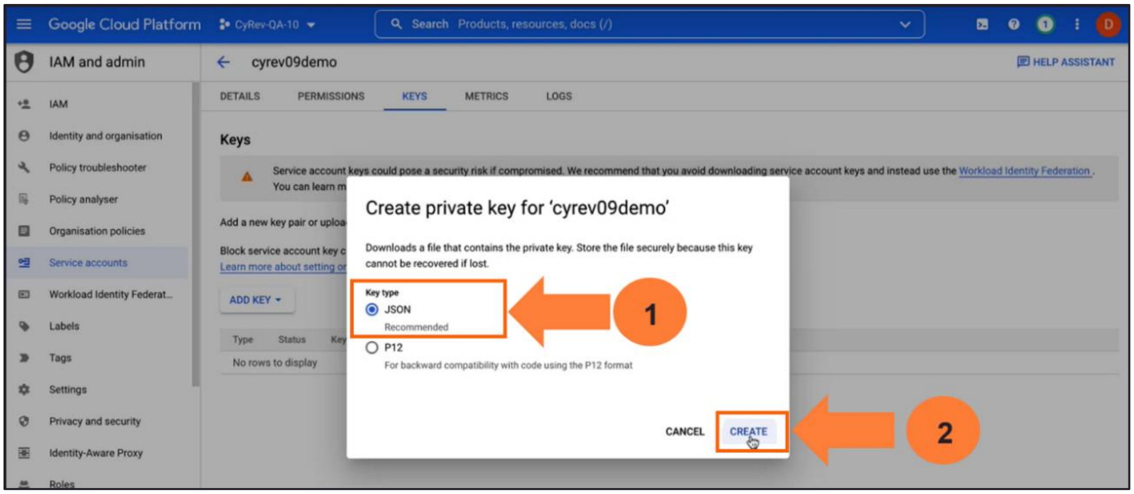
Keys

Service account keys could pose a security risk if compromised. We recommend that you avoid downloading service account keys and instead use the Workload Identity Federation . You can learn more about the best way to authenticate service accounts on Google Cloud here .

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using organisation policies.
Learn more about setting organisation policies for service accounts

5. Choose the JSON key type **(1)**. Then click **CREATE (2)** to generate the key. The key will get download to your computer.



Create private key for 'cyrev09demo'

Downloads a file that contains the private key. Store the file securely because this key cannot be recovered if lost.

Key type

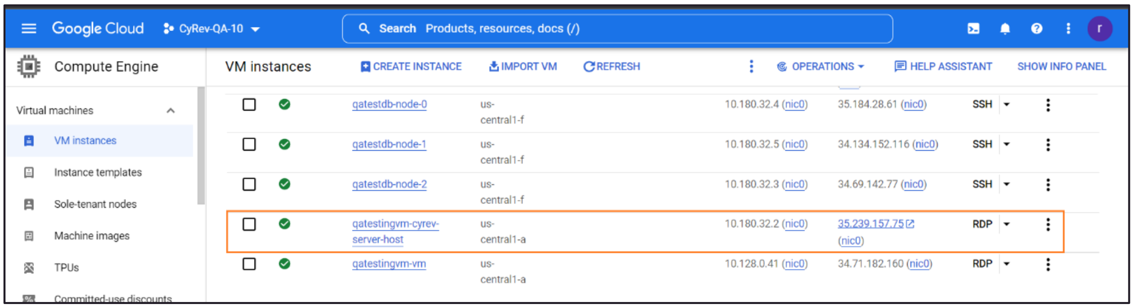
● JSON
Recommended

○ P12
For backward compatibility with code using the P12 format

Obtain CyRev Server Parameters

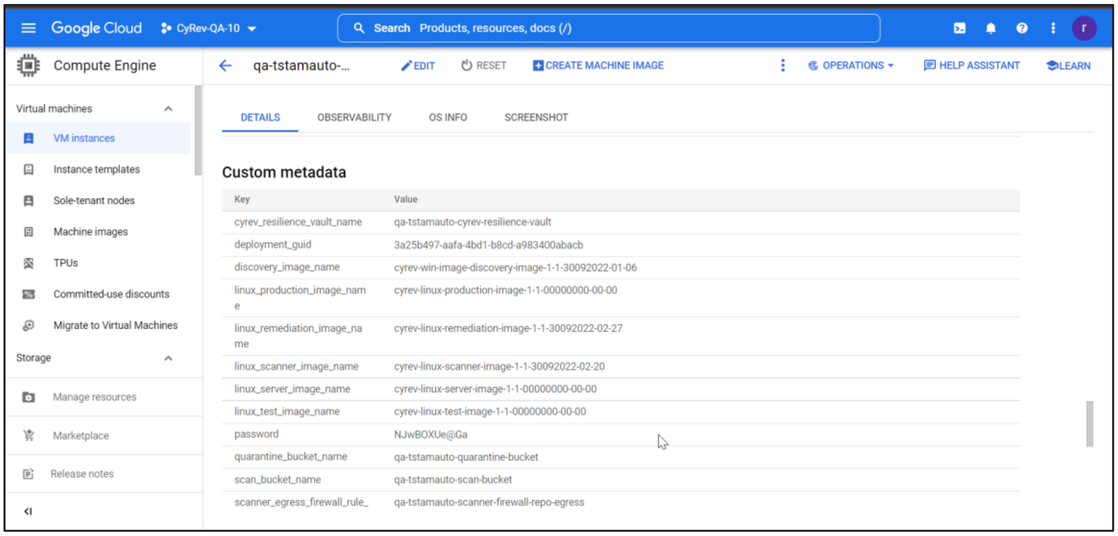
To use the CyRev dashboard you need to obtain the username and password for your UI. Follow the steps to obtain your UI credentials:

1. Navigate to **Compute Engine → VM instances** on your GCP cloud console.
2. Select the VM with deployment name with **cyrev-server-host** from the deployed VM's.



□	✓	qatestdb-node-0	us-central1-f	10.180.32.4 (nic0)	35.184.28.61 (nic0)	SSH
□	✓	qatestdb-node-1	us-central1-f	10.180.32.5 (nic0)	34.134.152.116 (nic0)	SSH
□	✓	qatestdb-node-2	us-central1-f	10.180.32.3 (nic0)	34.69.142.77 (nic0)	SSH
□	✓	qatestingvm-cyrev-server-host	us-central1-a	10.180.32.2 (nic0)	35.239.157.75 (nic0)	RDP
□	✓	qatestingvm-vm	us-central1-a	10.128.0.41 (nic0)	34.71.182.160 (nic0)	RDP

3. Scroll-down to the **Custom Metadata** section and make note of the parameters you want.



Custom metadata

Key	Value
cyrev_resilience_vault_name	qa-tstamauto-cyrev-resilience-vault
deployment_guid	3a25b497-aafa-4bd1-b8cd-a983400abacb
discovery_image_name	cyrev-win-image-discovery-image-1-1-30092022-01-06
linux_production_image_name	cyrev-linux-production-image-1-1-00000000-00-00
linux_remediation_image_name	cyrev-linux-remediation-image-1-1-30092022-02-27
linux_scanner_image_name	cyrev-linux-scanner-image-1-1-30092022-02-20
linux_server_image_name	cyrev-linux-server-image-1-1-00000000-00-00
linux_test_image_name	cyrev-linux-test-image-1-1-00000000-00-00
password	NJwBOXUe@Ga
quarantine_bucket_name	qa-tstamauto-quarantine-bucket
scan_bucket_name	qa-tstamauto-scan-bucket
scanner_egress_firewall_rule_	qa-tstamauto-scanner-firewall-repo-egress

About Persistent

With over 13,500 employees around the world, Persistent Systems (BSE & NSE: PERSISTENT) is a global services and solutions company delivering Digital Engineering and Enterprise Modernization.

www.persistent.com

India

Persistent Systems Limited

Bhageerath, 402,

Senapati Bapat Road

Pune 411016.

Tel: +91 (20) 6703 0000

Fax: +91 (20) 6703 0008

USA

Persistent Systems, Inc.

2055 Laurelwood Road, Suite 210

Santa Clara, CA 95054

Tel: +1 (408) 216 7010

Fax: +1 (408) 451 9177

Email: info@persistent.com