Google Cloud

EU Data Boundary control package for Data Residency ACN compliance

Date: 2025-10-09

Google Cloud

Contents

This document is intended to help manage the delivery of a project and is provided for illustrative purposes only. The activities and goals serve as guidelines and additional detail and do not supersede any legal terms or conditions as defined in the partner's or customer's written contract with Google. The information in this document is submitted to the customer for evaluation and discussion purposes only and is non-binding between the parties.

Introduction

To meet the DRZ ACN requirements, Google Cloud offers Assured Workloads with the EU Data Boundary control package. This configuration is **not merely a recommendation** but a fundamental best practice and an **essential technical tool** for PAs aiming for compliance with ACN directives about Data residency (DRZ) and Data protection area.
This document provides an operational guide for:

1. Creating an EU Data Boundary environment.
2. Verifying and customising automatic security policies.
3. Testing the effectiveness of controls.
4. Simulating and monitoring violations.
5. Understanding the granularity of available controls.

First Phase: Creating a Controlled Folder with Assured Workloads

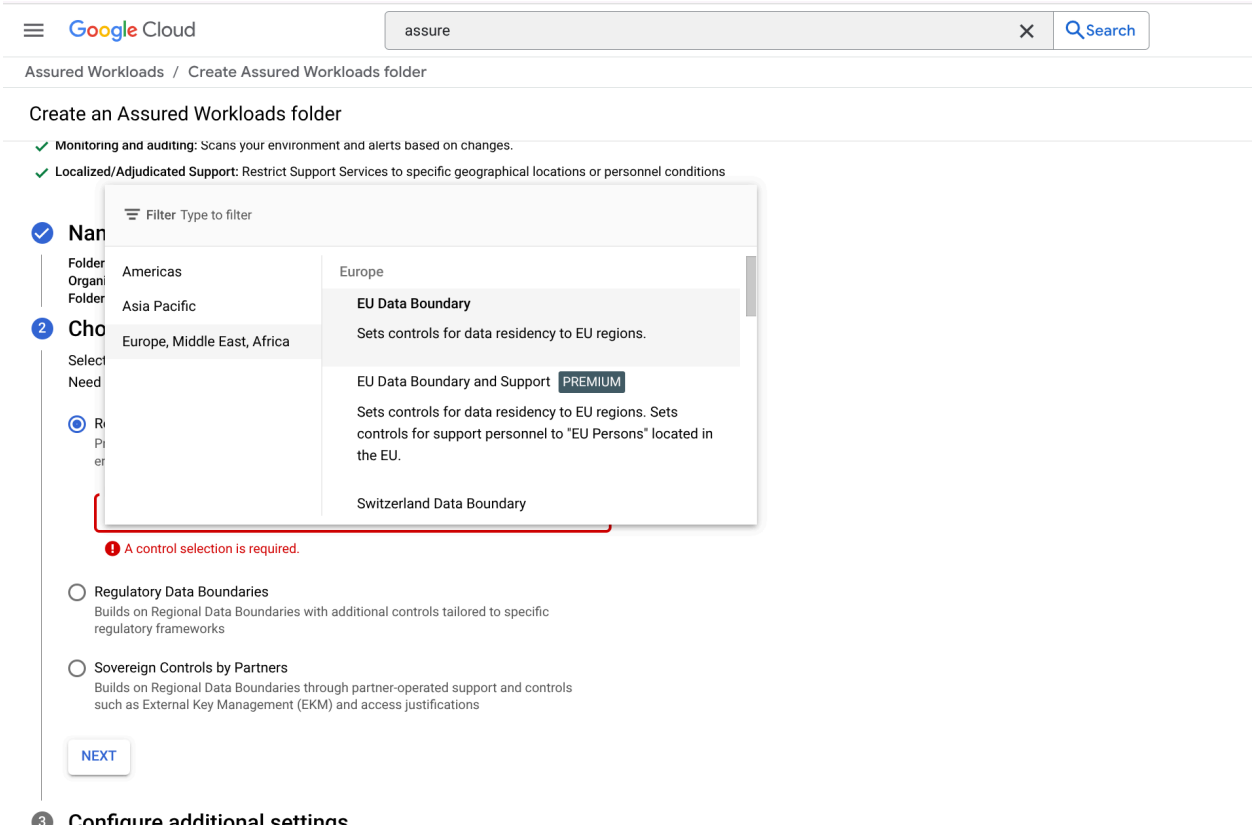
The first step is to create a secure "container" (a folder) where Public Sector Administrations projects will reside. Assured Workloads will automatically apply the necessary policies to this folder.

Prerequisites

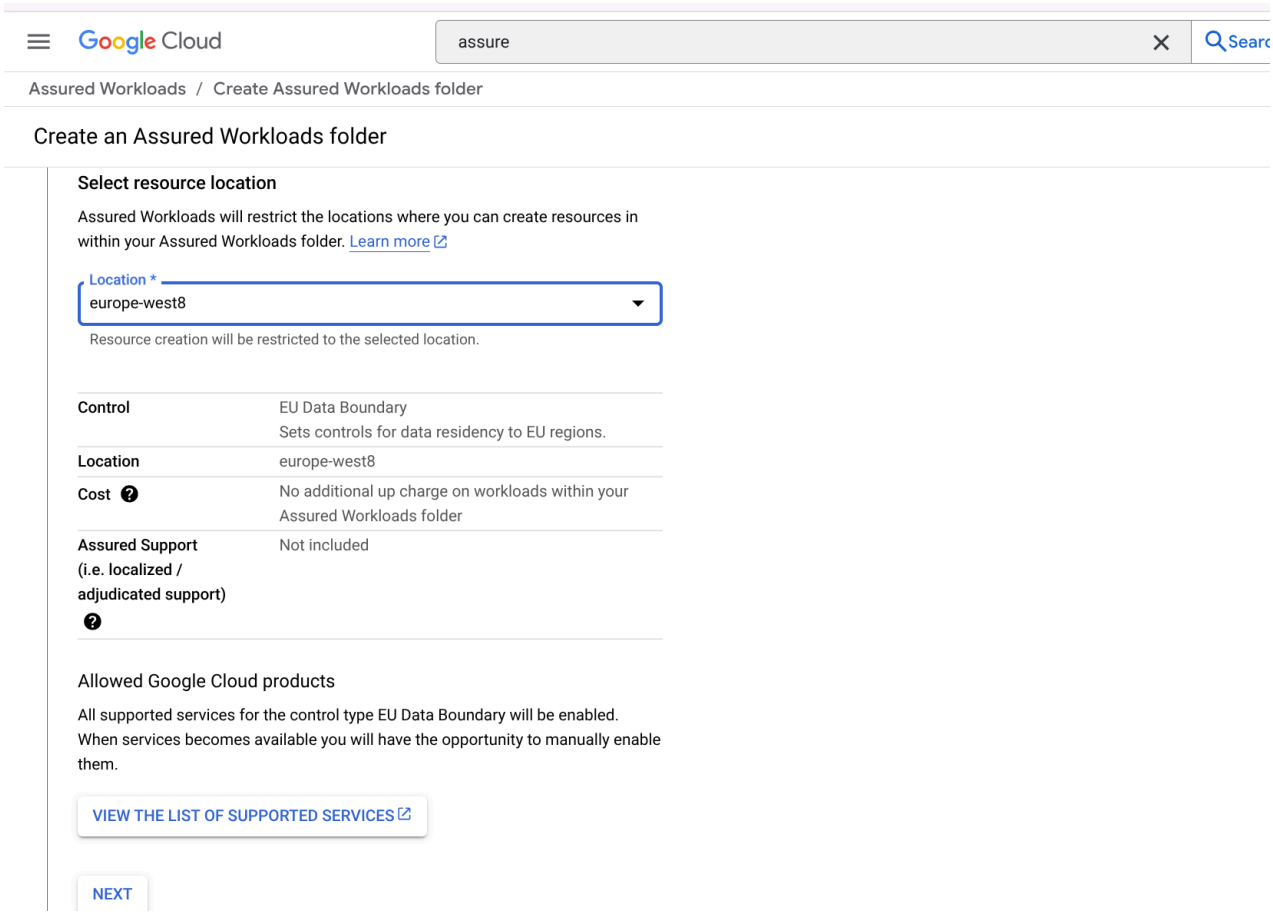
1. A Google Cloud Organization already configured.
2. IAM permissions for Assured Workloads Administrator (roles/assuredworkloads.admin) and Folder Admin (roles/resourcemanager.folderAdmin).

Step-by-Step Procedure

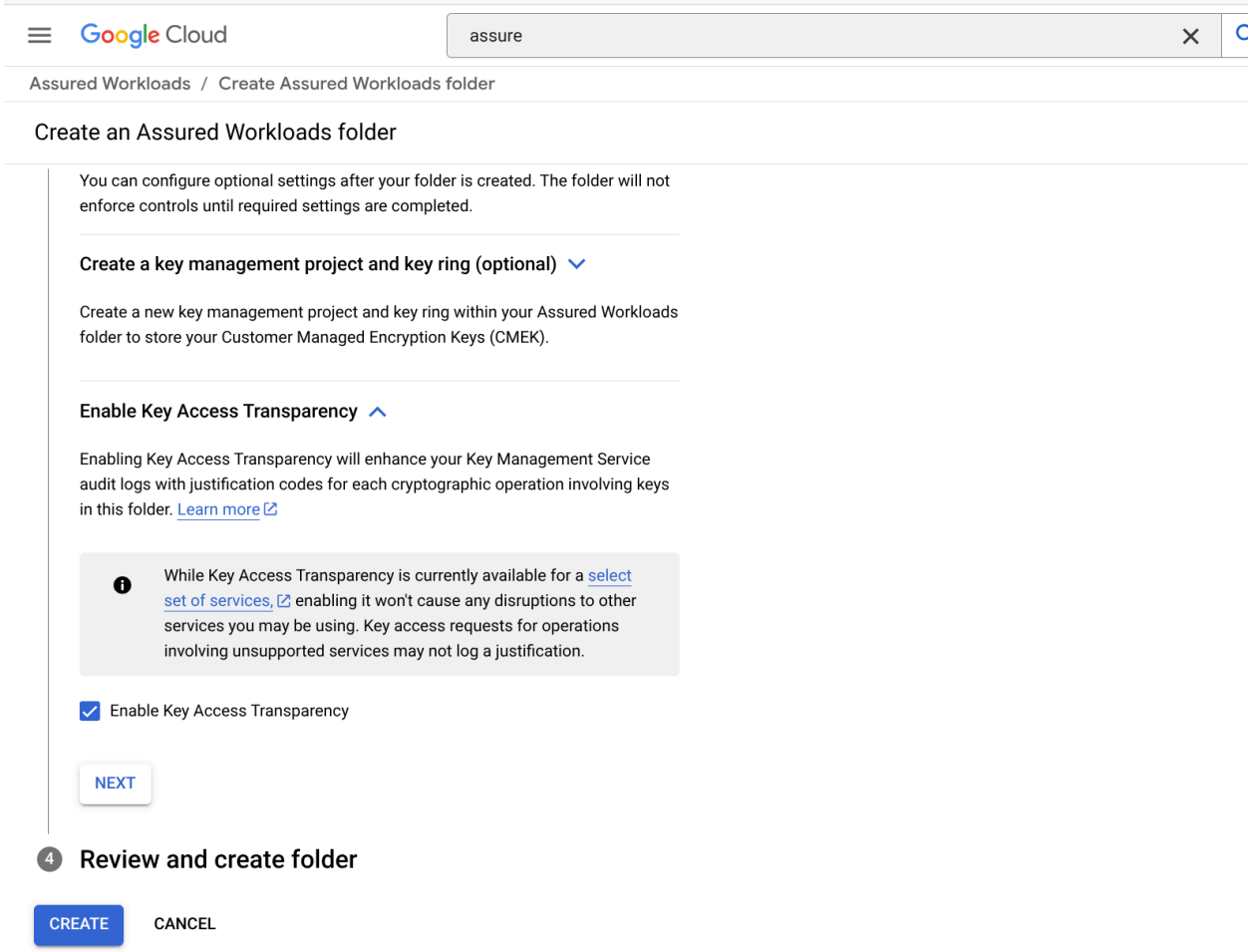
1. Navigate to Assured Workloads: From the Google Cloud console, search for "Assured Workloads" and access the section.
2. Create a New Folder: Click on "CREATE".
3. Select the Compliance Package:
    a. From the "Select a compliance program to help you meet your needs" drop-down menu, choose "Regional Data Boundary," then "Europe, Middle East, Africa," and finally "EU Data Boundary."
    b. Click "NEXT."



4. Configure the Base Region:
    a. In the "Select a region to create your workload in" menu, choose europe-west8 (Milan). This will be the default region for monitoring and other central services.
    b. Click "NEXT."



5. Configure the Folder:
    a. Folder name: Enter a descriptive name, e.g., folder-pa-acn-italy.
    b. Parent: Select your Organization as the parent resource.
    c. Key management (optional but recommended): Configure a project for customer-managed encryption keys (CMEK) if required by your standards. For this guide, we can skip this step.
    d. Click "NEXT."



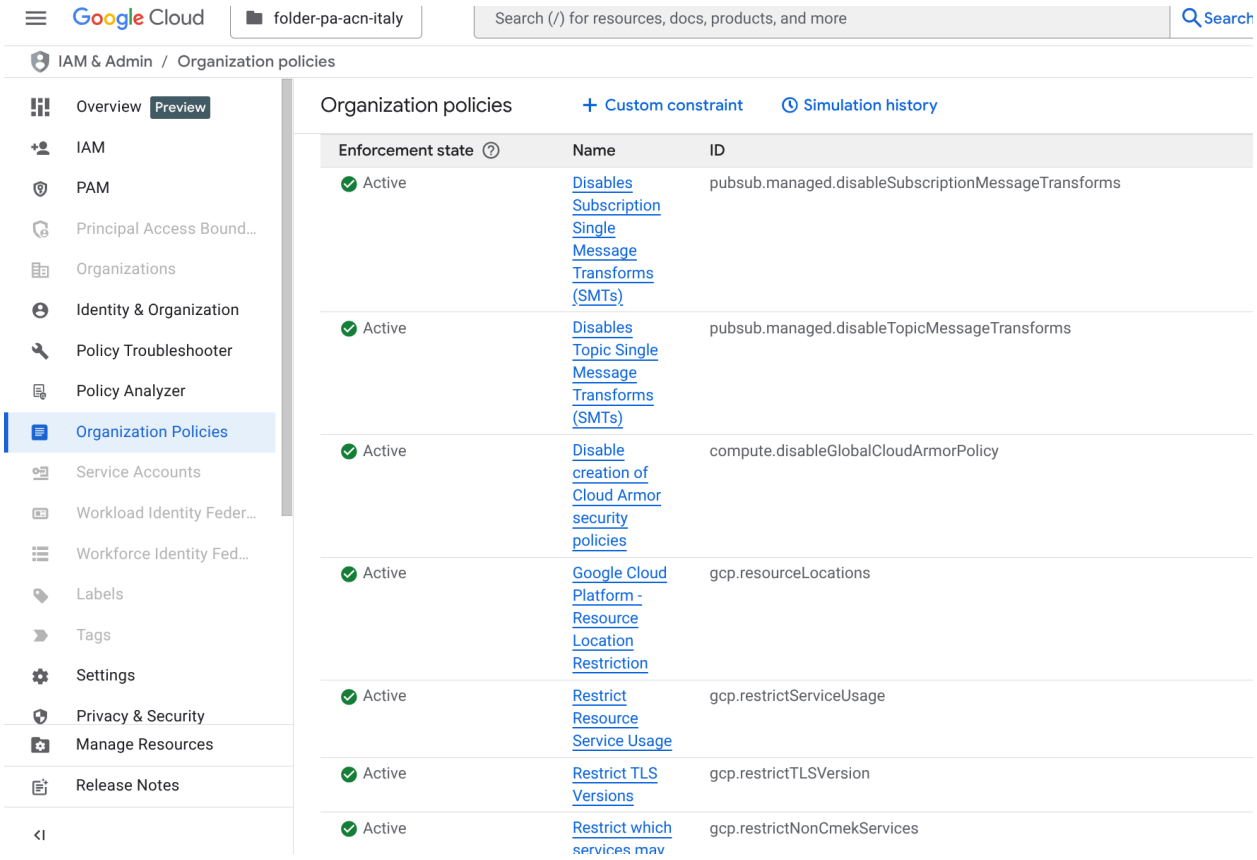
6. Enable Key Access Transparency:
    a. Access Transparency logs record actions taken by Google personnel when accessing customer data. The logs include details such as the affected resource and action, the time of the action, the reason for the action, and information about the user who performed the access. Information about who accessed it will include details about the physical location, the entity hiring them, and the Google employee's job category.
    b. Access Transparency logs are similar to Cloud Audit Logs. However, the latter records actions taken by members of your Google Cloud organization on your Google Cloud resources, while Access Transparency logs record actions taken by Google personnel.
7. Review and Create: Review the settings and click "CREATE." Creating the folder and applying the policies will take a few minutes.

Second Phase: Viewing and Customising Organization Policies

Once the folder is created, Assured Workloads has already applied a set of Organization Policies to ensure compliance. Let's see what they are and how to customize them to also include the Turin region (europe-west12).

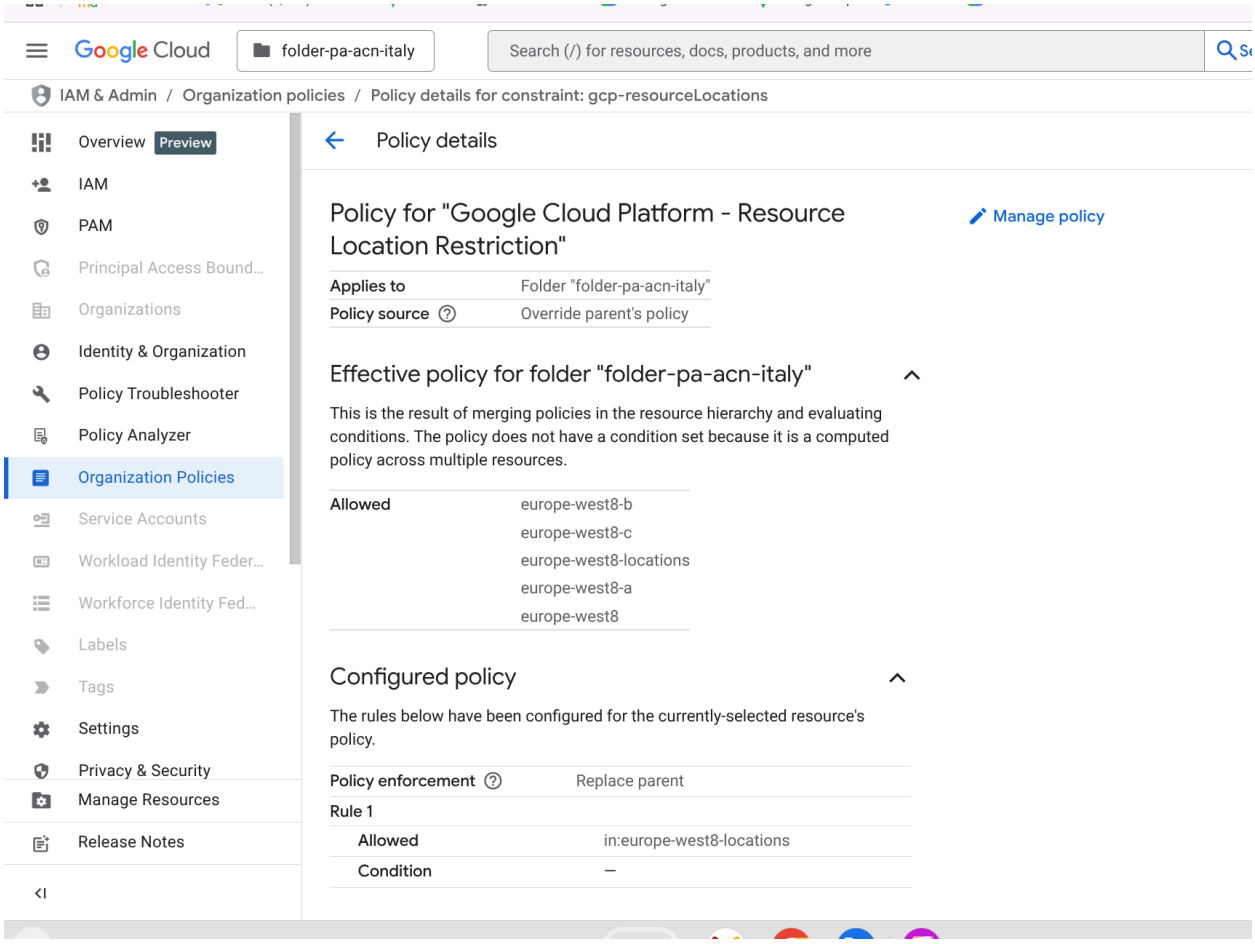
Step-by-Step Procedure

1. Navigate to Policies: Go to "IAM & Admin" > "Organization Policies."
2. Select the Folder: Use the "Resource Picker" at the top to select the folder you just created (folder-pa-acn-italy).
3. There are 3 policies across Google Cloud created automatically in this folder: https://cloud.google.com/assured-workloads/docs/control-packages/eu-data-boundary#restrictions_limitations
4. And 3 related to Compute Engine: https://cloud.google.com/assured-workloads/docs/control-packages/eu-data-boundary#org_compute

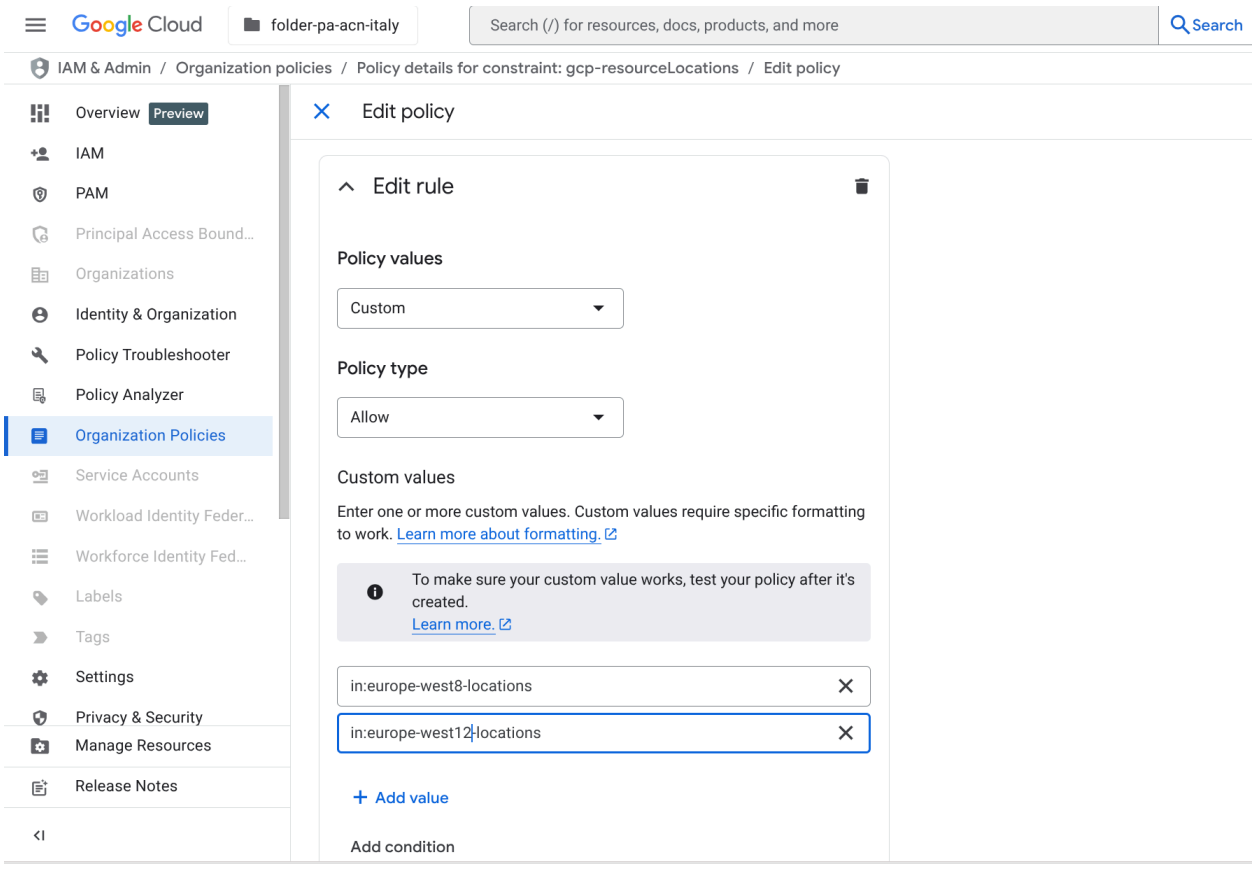


5. Show the Restrict Resource Service Usage policy

6. Filter for the Location Policy: In the search bar, type "Resource Locations" and select the policy with the gcp.resourceLocations constraint.
7. View the Policy: Click on the policy. You will notice that it is configured to inherit a policy from above (the in:eu-locations group) or has specific values. Our goal is to make it more restrictive.



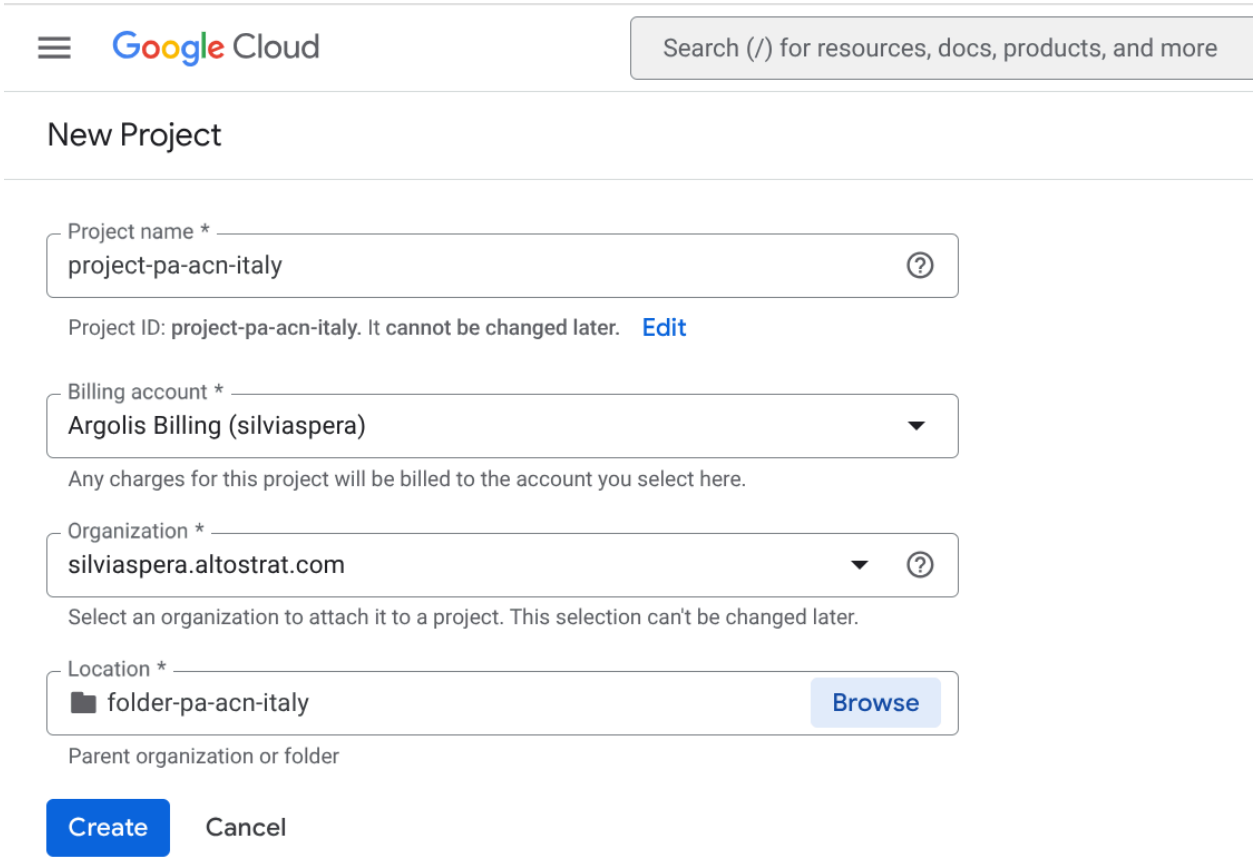
8. Modify the Policy:
    a. Click "EDIT."
    b. Select "Customize."
    c. In "Policy values," select "Custom."
    d. In the "Custom values" field, select "Add value."
    e. Add in:europe-west12-locations (which corresponds to the Turin region).
    f. Click "Set Policy."



Now your folder is configured to allow resource creation exclusively in the Milan and Turin regions.

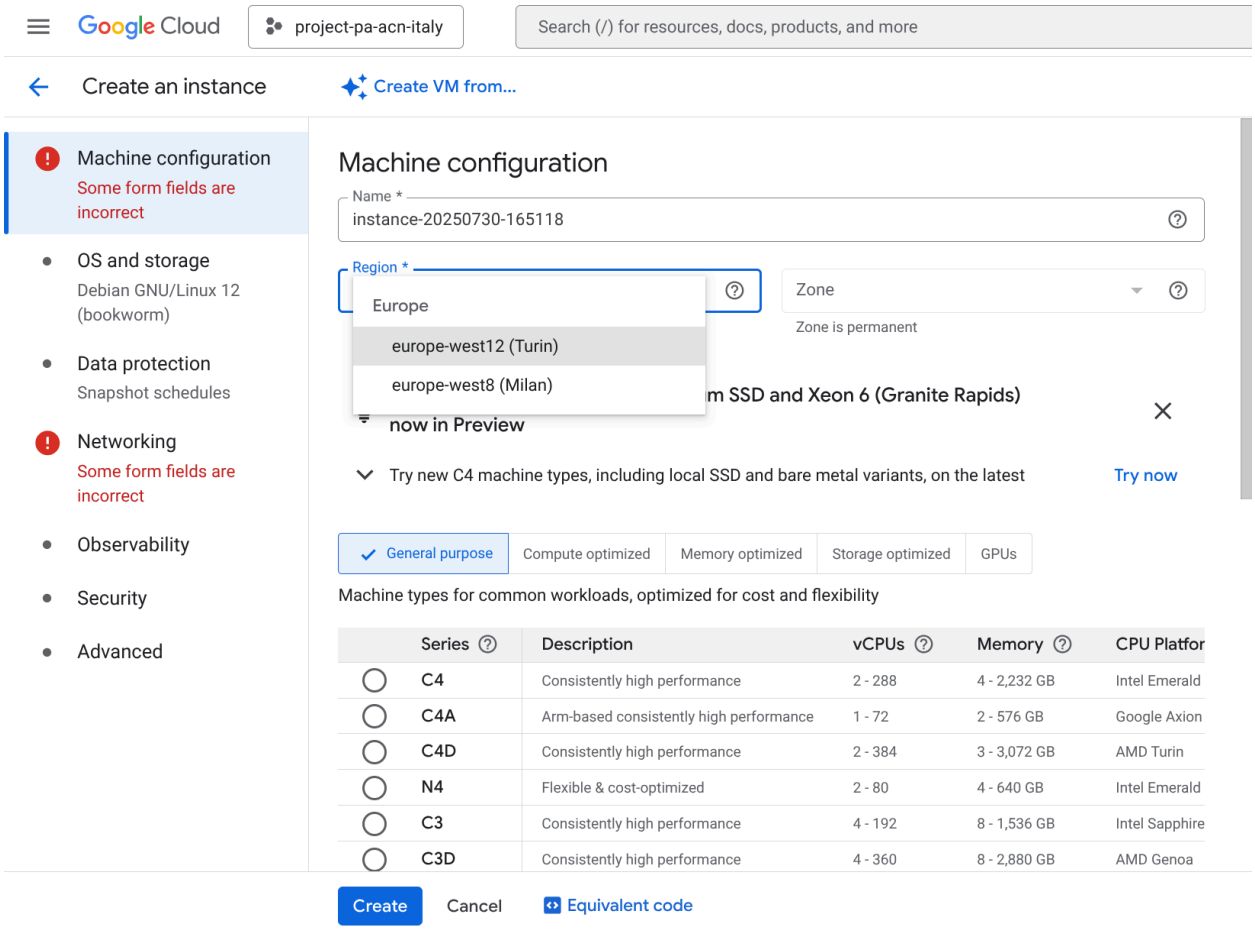
Third Phase: Verifying Policy Application (Enforcement)

Let's test if the controls are effective. We will create a project (project-pa-acn-italy) inside the folder folder-pa-acn-italy for our tests.



Test 1: Blocking Resource Creation by Location

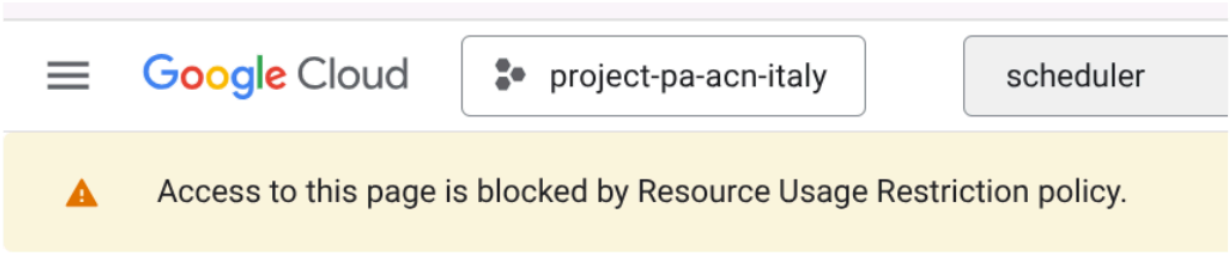
1. Within your new project, navigate to "Compute Engine" > "VM Instances."
2. Click on "CREATE INSTANCE."
3. In the "Region" section, the only regions that appear are europe-west8 and europe-west12, and I cannot create the resource outside Italy.



Test 2: Blocking the Use of Unallowed Services

The gcp.restrictServiceUsage policy limits which APIs/services can be used. Let's try to enable a service not included in the list of those supported by EU Data Boundary.

- Search for a service that is not yet fully supported in EU Data Boundary (e.g., Cloud Scheduler).
- Expected Result: You will receive an error indicating that the operation was blocked by the gcp.restrictServiceUsage policy.

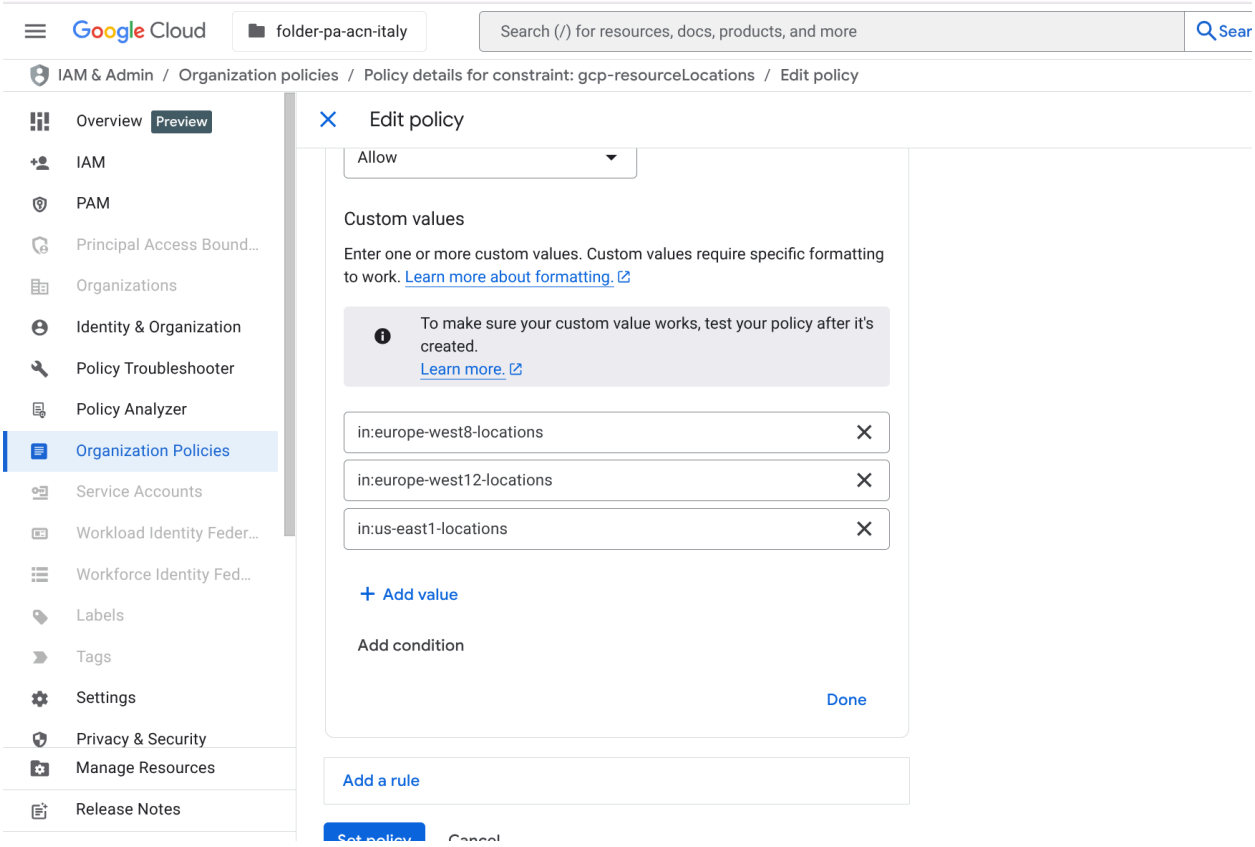


Fourth Phase: Simulating and Monitoring Violations

Now we will simulate a scenario where an administrator violates a policy and see how Assured Workloads detects and reports the incident.

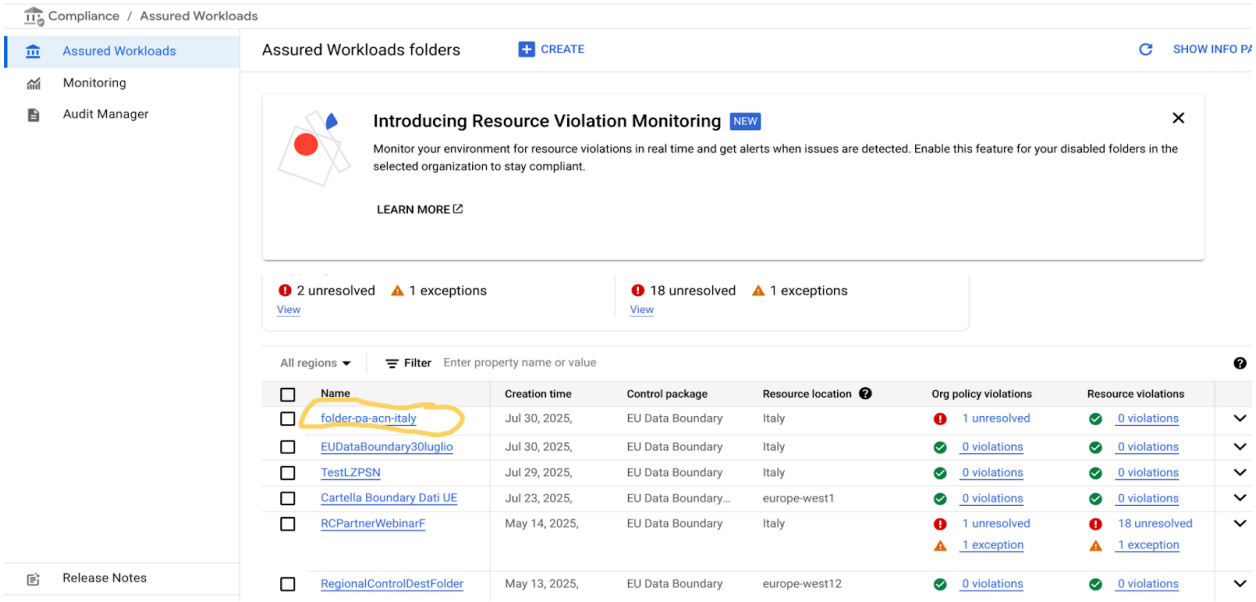
Step 1: Violating the Location Policy

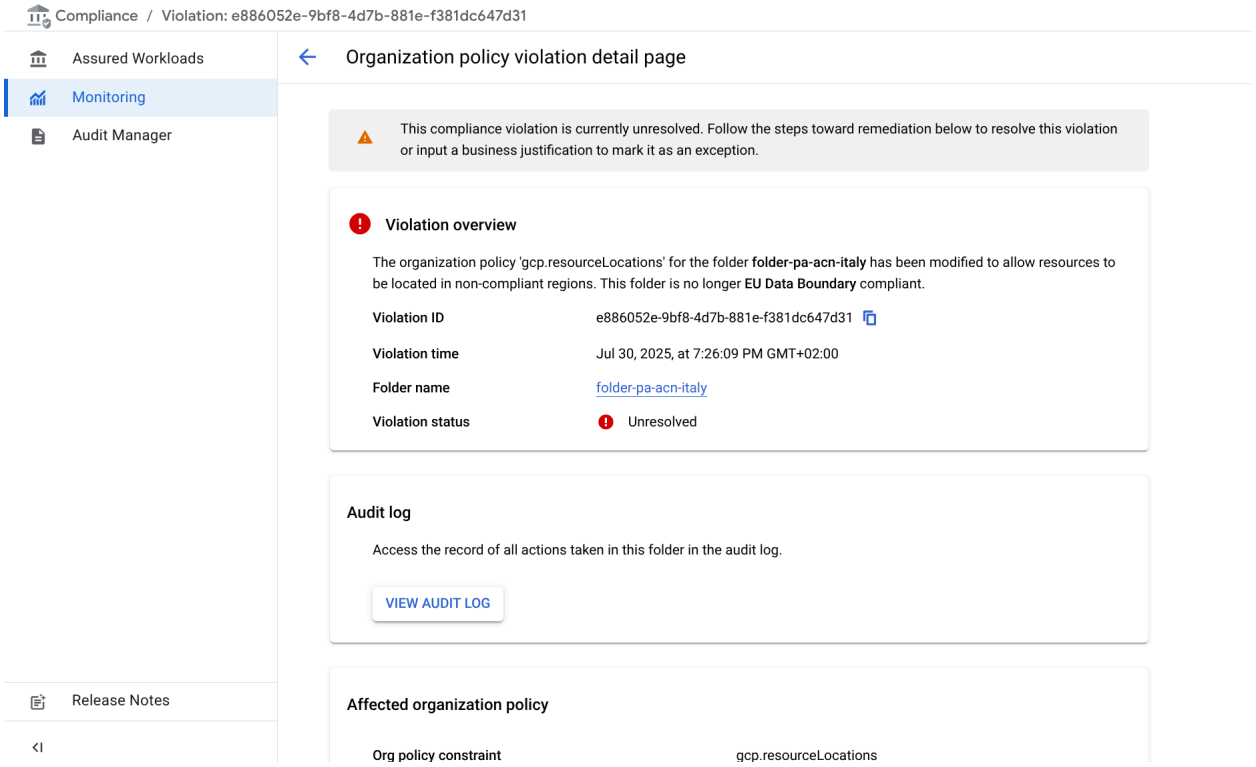
1. With Organization Policy Administrator permissions, return to the policies of the folder folder-pa-acn-milan.
2. Modify the gcp.resourceLocations policy again.
3. Add a non-EU region to the list of allowed values, for example, us-east1. Save the policy.



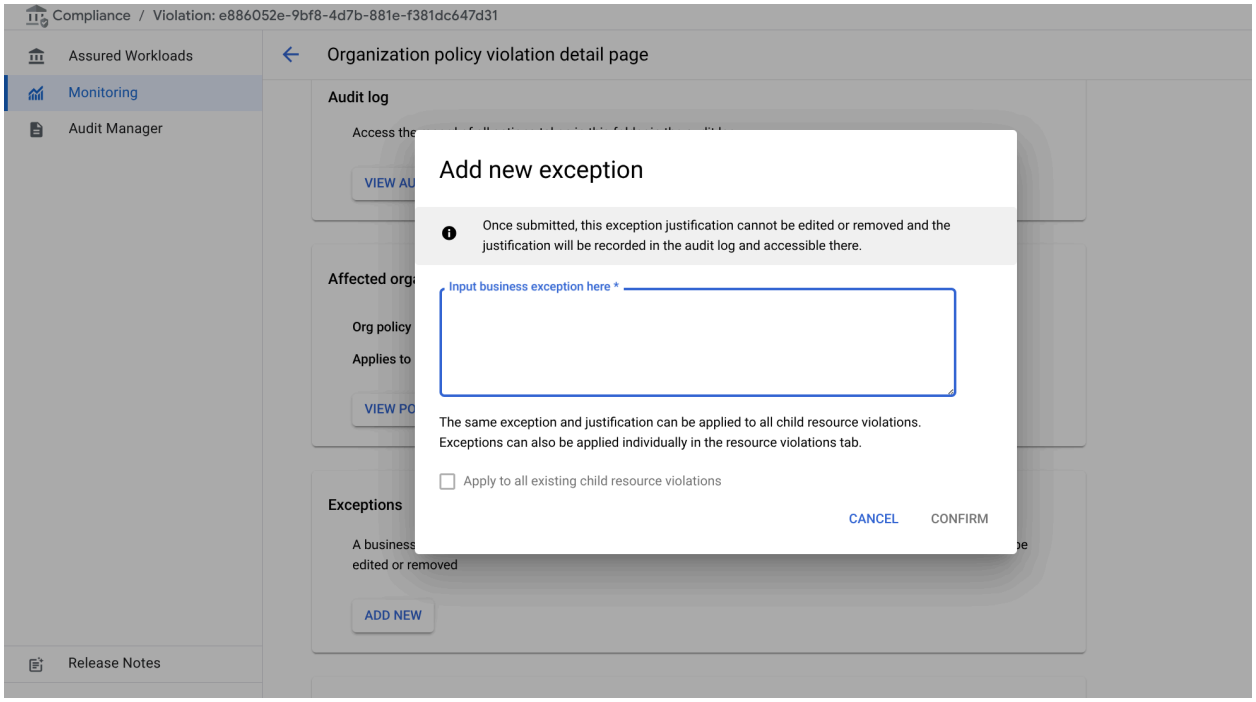
Step 2: Viewing the Policy Violation in Monitoring

4. Navigate to "Assured Workloads" and select your folder.
5. Go to the "MONITORING" tab.
6. After a few minutes, a new violation will appear.
    a. Violation Type: POLICY_VIOLATION
    b. Description: It will indicate that the gcp.resourceLocations policy has been modified and no longer matches the base configuration required by "EU Data Boundary."



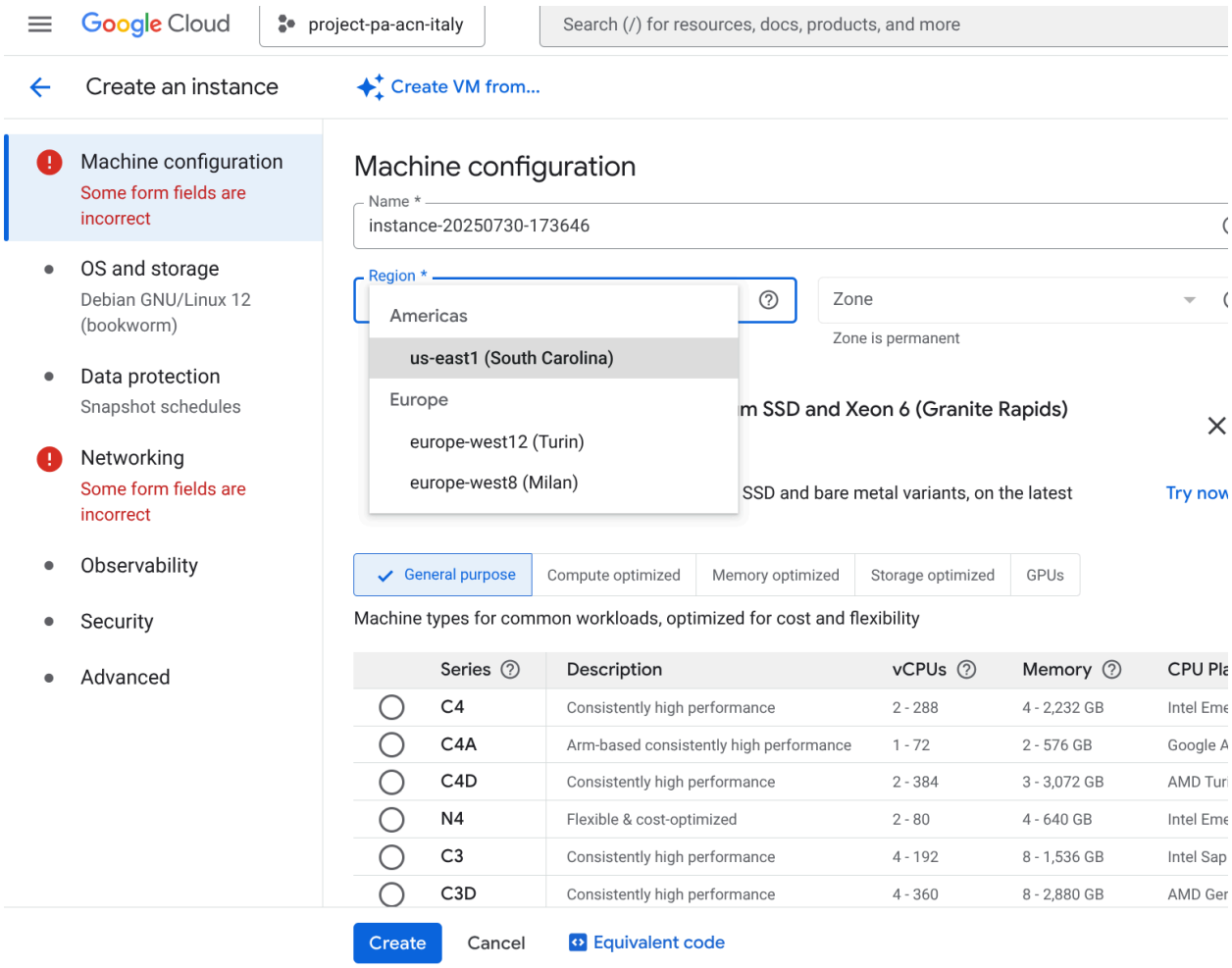


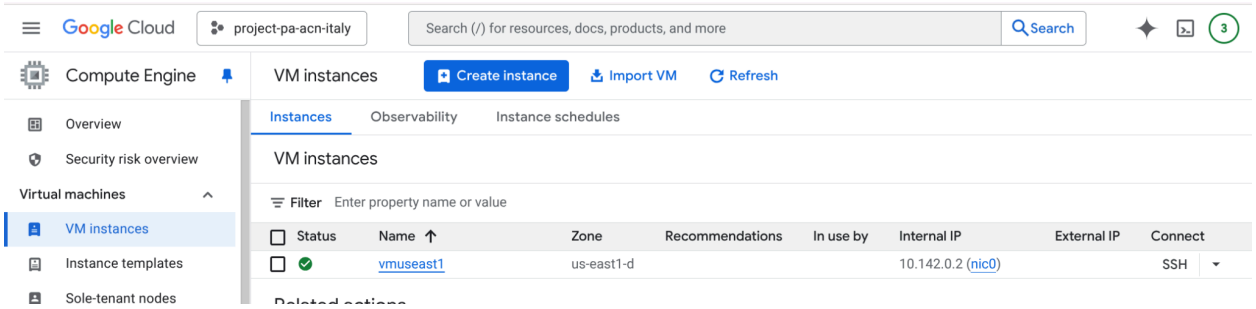
You can enter a reason to manage the exception.



Step 3: Creating a Non-Compliant Resource

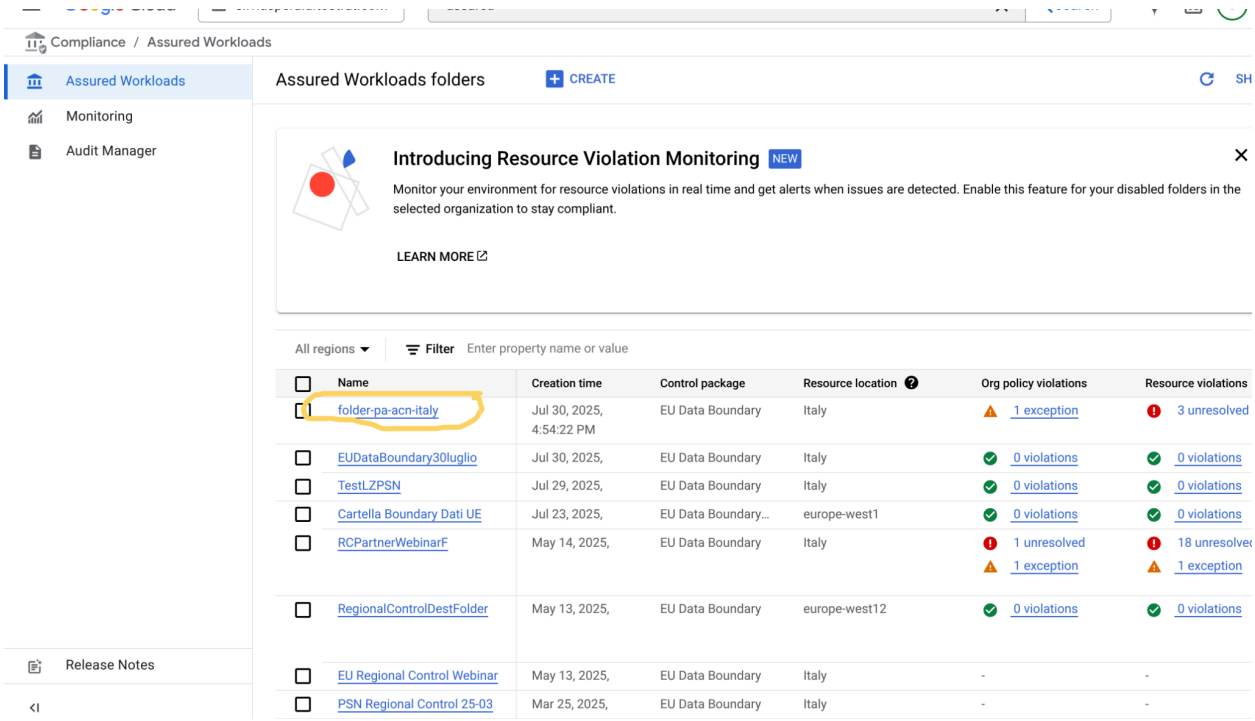
1. Now that the policy has been weakened, go back to "Compute Engine" in your test project.
2. Create a new VM and this time select us-east1 as the region.
3. Result: The VM creation will be successful, as the enforcement policy has been tampered with.



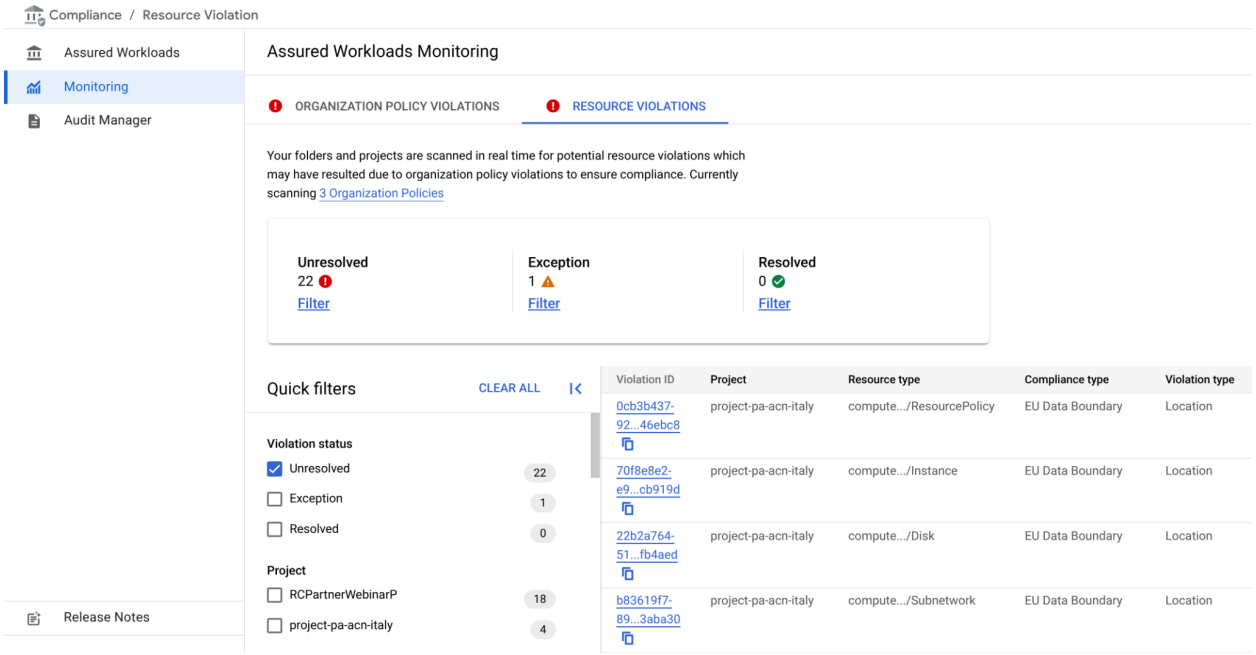


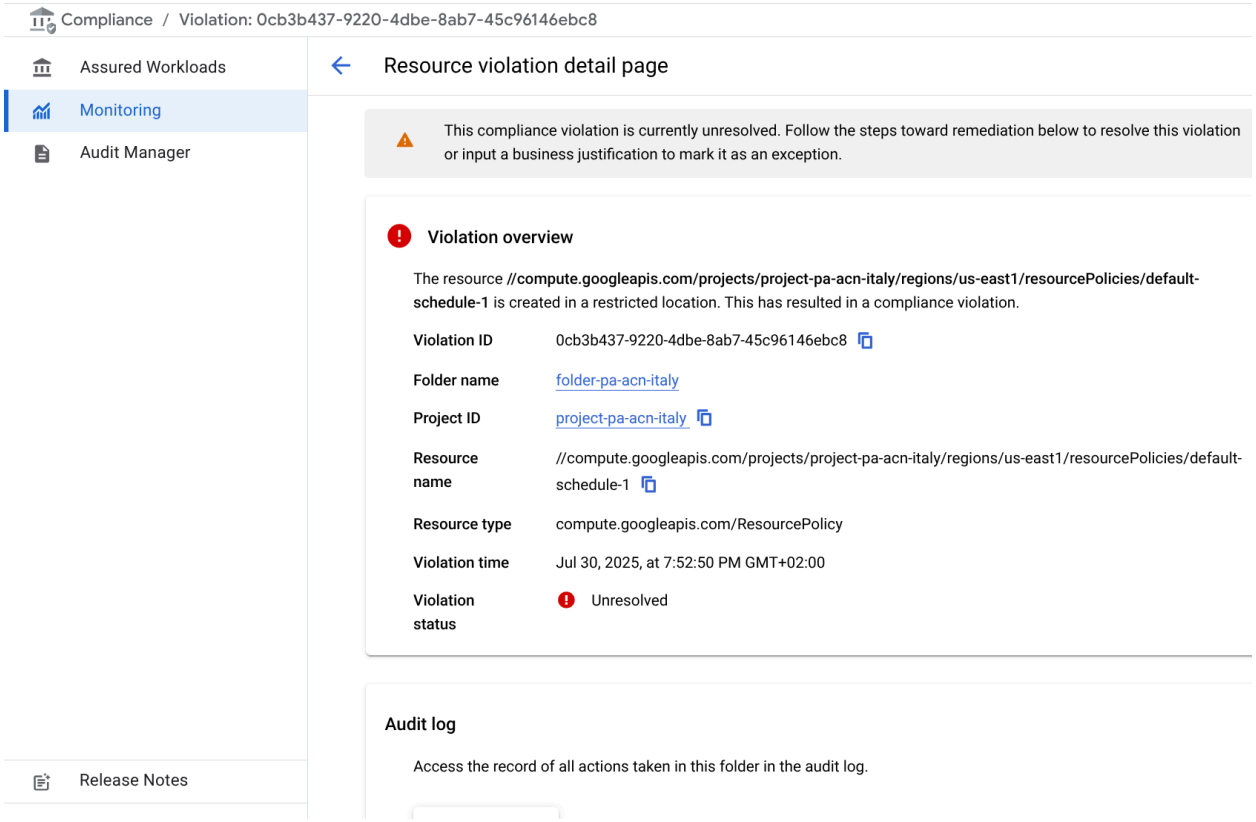
Step 4: Viewing the Resource Creation Violation

1. Return to the "MONITORING" tab of Assured Workloads.
2. After another scan (it may take several minutes), a second violation will appear.
    a. Violation Type: RESOURCE_VIOLATION
    b. Description: It will indicate that a resource (your new VM) has been found in a location (us-east1) not allowed by the original compliance baseline of the folder.

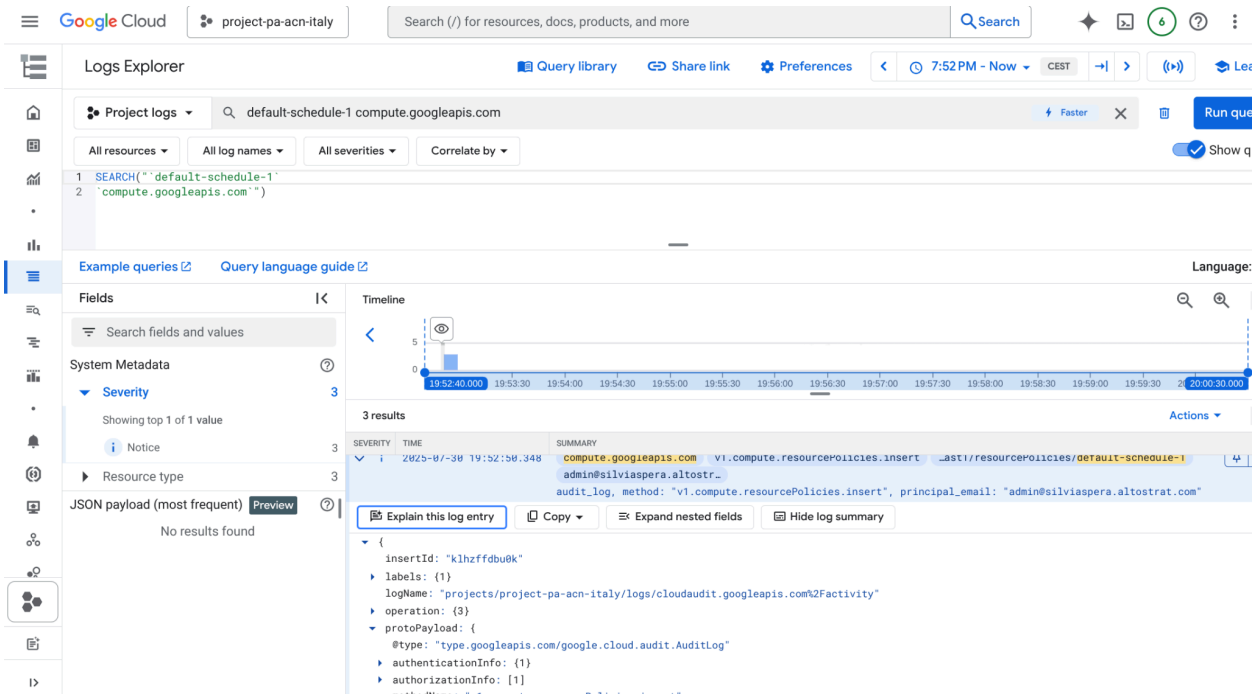


This time the violations are of the type: Resource Violations, because we have created the resource.





By clicking on "Audit Log," you get the details.



This proves that even if a preventive control is bypassed, the detection control of Assured Workloads identifies and reports the non-compliance, allowing for corrective action.

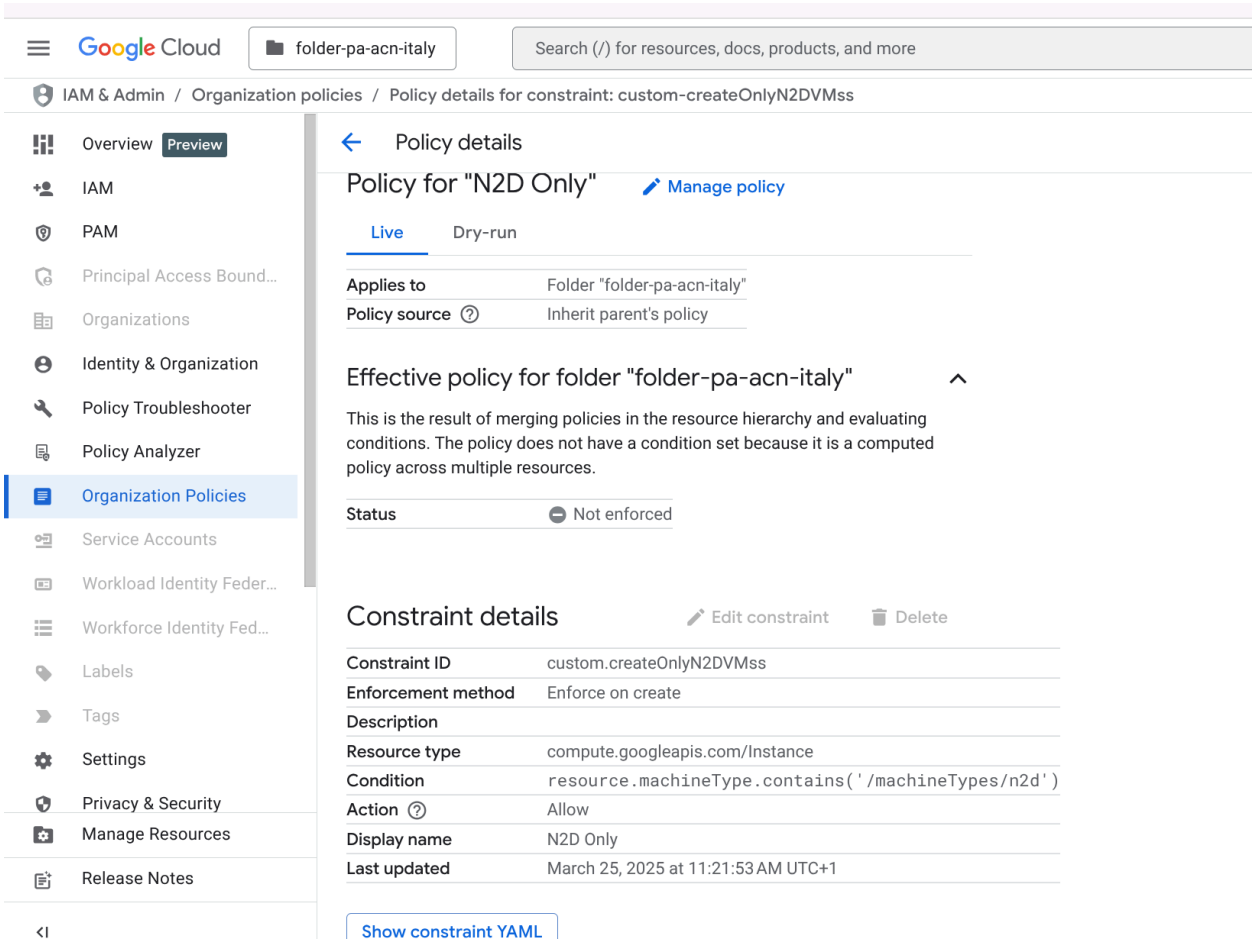
Terraform link for new workloads here, in GitHub.

Deeper Dive: Granularity of Organization Policies

A common question concerns the level of detail that can be achieved with Organization Policies.

What granularity can I achieve? There are constraints that can be enabled at the Org Policy level to limit and block services and/or specific features and functionalities of the services themselves.

The list of all applicable Constraints is available here. As an example, we have limited the ability to create VMs exclusively of type N2D.



Moving an Existing Folder or Project into an EU Data Boundary Folder

It is possible to analyse an existing project that you want to make compliant with EU Data Boundary and make the required changes. Then, move the project/folder into the newly created Assured Workloads folder.

- When you run an analysis on the source project and the destination Assured Workloads folder, you must resolve any non-compliances before moving the project to the destination. Although the results will not prevent you from moving the project, they could cause compliance violations in the destination Assured Workloads folder.
- These results are of two different types:
    - Warning: A warning result occurs when the source project is potentially incompatible with the destination and could lead to a compliance violation. Warnings should be reviewed to verify that the incompatibility is acceptable or needs to be resolved before the transfer.
    - Blocking: A blocking result occurs when a compliance violation is detected between the source project and the destination. Blocks must be resolved before proceeding with a move.
- The following types of results are reported:
    - Resource locations: Many control packages apply location restrictions for resources so that they respect compliance requirements, for example, if the source project contains resources located in an unallowed location.
    - Unsupported products/services: Each control package supports a specific list of Google Cloud products and services. If the project uses a service not supported by the destination Assured Workloads folder's control package, this will be indicated as a detection.
    - Org policy constraints: The source project may be configured with different org policy constraint values than those of the destination Assured Workloads folder or may not be compliant with the destination control package. This analysis is performed only for constraints relevant to the target Assured Workloads folder control package. Not all project constraint values are evaluated. Several outcomes are possible, for example, the following issues:
        - The project and the target's effective policy are not compatible.
        - The project contains organization policy constraint values that are not set on the target, or vice versa.
        - The project contains organization policy constraint values that are not compliant with the target control package.
        - If a block is found for an organization policy constraint, the response includes the expected values that are compliant with the target control package. You can use these expected values to make changes to the project before performing a migration.

Terraform link for existing workloads:

https://github.com/GoogleCloudPlatform/assured-workloads-terraform

EU Data Boundary vs. Manual Policies

For companies operating in Europe, ensuring that customer data remains within the borders of the European Union is not only a best practice but often a legal requirement (e.g., GDPR). Google Cloud offers two approaches to achieve this goal: the manual application of Organization Policies (Org Policies) and the use of the EU Data Boundary feature of Assured Workloads. Although both tools aim to control data geolocation, the Assured Workloads approach, even in its free version, offers significant advantages in terms of simplicity, automation, and reliability.

The Limitations of the Manual Approach with Org Policies

The manual approach, while flexible, presents significant challenges:

- Risk of Human Error: Manual configuration is prone to errors. An incorrectly applied policy or an incomplete configuration can create a critical flaw in the strategy.
- Complexity and Maintenance: Policies may need to be updated manually, creating a constant maintenance burden.
- Difficulty of Audit: Demonstrating to an auditor that only Italian regions are in use requires checking the applied policies and verifying that there are no exceptions or incorrect configurations in the entire resource hierarchy.

The Advantages of EU Data Boundary (Assured Workloads)

The EU Data Boundary feature is activated by creating an Assured Workloads folder with the "EU Regions" regime. This operation is free and creates an environment where data residency is programmatically guaranteed by Google Cloud.
Here are the main advantages compared to the manual approach:

1. Out-of-the-Box Automation and Assurance The biggest advantage is automation. Instead of having to manually create and manage a list of allowed locations, you simply select the "EU Regions" regime. From that moment on, Google Cloud automatically enforces the controls.
2. Access Transparency: Total Visibility Included Access Transparency is a service that records every access to your data by Google personnel. With the "EU Regions" regime of Assured Workloads, Access Transparency is enabled by default and at no additional cost.
3. Simplified Audits Demonstrating compliance becomes much simpler. Instead of having to document and defend a manual configuration of Org Policies, it is sufficient to demonstrate that the workloads are within an Assured Workloads folder with the "EU Regions" regime. The data residency guarantee is provided directly by the Google Cloud service.

Comparative Table

Feature	EU Data Boundary (Managed and Free Approach)	Org Policy (Manual Approach)
Enforcement	Automatic and programmatic. Prevents violations.	Manual. Risk of incorrect or incomplete configuration.
Ease of Use	High. You choose the regime, Google does the rest.	Medium/Low. Requires expertise and maintenance.
Access Transparency	Integrated and guaranteed by default.	Optional. Must be enabled and managed separately.
Audit	Simplified. Compliance is guaranteed by the service.	Complex. Requires demonstration of the correctness of the configuration.
Maintenance	Minimal. Google updates the controls automatically.	High. Requires constant manual updates.

Conclusion

For a company that needs to guarantee data residency in the EU, the manual approach with Org Policies is a possible but fragile and laborious solution.

The free EU Data Boundary feature of Assured Workloads represents a clearly superior approach. Instead of relying on a complex manual configuration, you get a programmatic guarantee that data will remain in Europe, with the added benefit of having Access Transparency enabled by default. This reduces risks, operational costs, and greatly simplifies compliance management.