

EU Data Boundary control package for Data Residency ACN compliance

Date: 2025-10-09

Contents

Introduction	2
First Phase: Creating a Controlled Folder with Assured Workloads	2
Prerequisites	2
Step-by-Step Procedure	2
Second Phase: Viewing and Customising Organization Policies	6
Step-by-Step Procedure	6
Third Phase: Verifying Policy Application (Enforcement)	8
Test 1: Blocking Resource Creation by Location	9
Test 2: Blocking the Use of Unallowed Services	10
Fourth Phase: Simulating and Monitoring Violations	11
Step 1: Violating the Location Policy	11
Step 2: Viewing the Policy Violation in Monitoring	12
Step 3: Creating a Non-Compliant Resource	14
Step 4: Viewing the Resource Creation Violation	15
Deeper Dive: Granularity of Organization Policies	18
Moving an Existing Folder or Project into an EU Data Boundary Folder	19
EU Data Boundary vs. Manual Policies	20
The Limitations of the Manual Approach with Org Policies	20
The Advantages of EU Data Boundary (Assured Workloads)	20
Conclusion	21

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."

- Google Cloud

Google Cloud

assure

X

Search

Assured Workloads / Create Assured Workloads folder

Create an Assured Workloads folder

Select resource location

Assured Workloads will restrict the locations where you can create resources in within your Assured Workloads folder. [Learn more](#)

Location *

europa-west8

Resource creation will be restricted to the selected location.

Control	EU Data Boundary Sets controls for data residency to EU regions.
Location	europa-west8
Cost ?	No additional up charge on workloads within your Assured Workloads folder
Assured Support (i.e. localized / adjudicated support) ?	Not included

Allowed Google Cloud products

All supported services for the control type EU Data Boundary will be enabled. When services becomes available you will have the opportunity to manually enable them.

VIEW THE LIST OF SUPPORTED SERVICES

NEXT

5. Configure the Folder:

- Folder name: Enter a descriptive name, e.g., folder-pa-acn-italy.
- Parent: Select your Organization as the parent resource.
- 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.
- Click "NEXT."

assure

Assured Workloads / Create Assured Workloads folder

Create an Assured Workloads folder

You can configure optional settings after your folder is created. The folder will not enforce controls until required settings are completed.

Create a key management project and key ring (optional)

Create a new key management project and key ring within your Assured Workloads folder to store your Customer Managed Encryption Keys (CMEK).

Enable Key Access Transparency

Enabling Key Access Transparency will enhance your Key Management Service audit logs with justification codes for each cryptographic operation involving keys in this folder. [Learn more](#)

While Key Access Transparency is currently available for a [select set of services](#), enabling it won't cause any disruptions to other services you may be using. Key access requests for operations involving unsupported services may not log a justification.

☒ Enable Key Access Transparency

[NEXT](#)

4 Review and create folder

[CREATE](#) [CANCEL](#)

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

Google Cloud

folder-pa-acn-italy

Search (/) for resources, docs, products, and more

Search

IAM & Admin / Organization policies

Overview

Preview

IAM

PAM

Principal Access Bound...

Organizations

Identity & Organization

Policy Troubleshooter

Policy Analyzer

Organization Policies

Service Accounts

Workload Identity Feder...

Workforce Identity Fed...

Labels

Tags

Settings

Privacy & Security

Manage Resources

Release Notes

Organization policies

+ Custom constraint

Simulation history

Enforcement state ?	Name	ID
Active	Disables Subscription Single Message Transforms (SMTs)	pubsub.managed.disableSubscriptionMessageTransforms
Active	Disables Topic Single Message Transforms (SMTs)	pubsub.managed.disableTopicMessageTransforms
Active	Disable creation of Cloud Armor security policies	compute.disableGlobalCloudArmorPolicy
Active	Google Cloud Platform - Resource Location Restriction	gcp.resourceLocations
Active	Restrict Resource Service Usage	gcp.restrictServiceUsage
Active	Restrict TLS Versions	gcp.restrictTLSVersion
Active	Restrict which services mav	gcp.restrictNonCmekServices

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.

The screenshot shows the Google Cloud IAM & Admin console. The breadcrumb trail is: IAM & Admin / Organization policies / Policy details for constraint: gcp-resourceLocations. The left sidebar shows the 'Organization Policies' section selected. The main content area is titled 'Policy details' and shows the 'Policy for "Google Cloud Platform - Resource Location Restriction"'. It indicates the policy applies to the folder 'folder-pa-acn-italy' and its source is 'Override parent's policy'. Below this, the 'Effective policy for folder "folder-pa-acn-italy"' is shown, stating it is a computed policy across multiple resources. A table lists the allowed locations: europe-west8-b, europe-west8-c, europe-west8-locations, europe-west8-a, and europe-west8. The 'Configured policy' section shows the policy enforcement is set to 'Replace parent' and lists a rule with allowed values 'in:europe-west8-locations' and no conditions.

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."

Google Cloud folder-pa-acn-italy Search (/) for resources, docs, products, and more Search

IAM & Admin / Organization policies / Policy details for constraint: gcp-resourceLocations / Edit policy

Overview Preview

IAM

PAM

Principal Access Bound...

Organizations

Identity & Organization

Policy Troubleshooter

Policy Analyzer

Organization Policies

Service Accounts

Workload Identity Feder...

Workforce Identity Fed...

Labels

Tags

Settings

Privacy & Security

Manage Resources

Release Notes

<1

Edit policy

Edit rule

Policy values

Custom

Policy type

Allow

Custom values

Enter one or more custom values. Custom values require specific formatting to work. [Learn more about formatting.](#)

To make sure your custom value works, test your policy after it's created. [Learn more.](#)

in:europa-west8-locations

in:europa-west12-locations

+ Add value

Add condition

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.



Search (/) for resources, docs, products, and more

New Project

Project name *
?

Project ID: project-pa-acn-italy. It cannot be changed later. [Edit](#)

Billing account *
▼

Any charges for this project will be billed to the account you select here.

Organization *
▼
?

Select an organization to attach it to a project. This selection can't be changed later.

Location *
Browse

Parent organization or folder

Create

Cancel

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.

☰

Google Cloud

project-pa-acn-italy

Search (/) for resources, docs, products, and more

←

Create an instance

⚡ Create VM from...

! Machine configuration

Some form fields are incorrect

• OS and storage

Debian GNU/Linux 12 (bookworm)

• Data protection

Snapshot schedules

! Networking

Some form fields are incorrect

• Observability

• Security

• Advanced

Machine configuration

Name *
instance-20250730-165118

Region *
Europe
europe-west12 (Turin)
europe-west8 (Milan)
now in Preview

Zone
Zone is permanent

Local SSD and Xeon 6 (Granite Rapids)

✕

✓ Try new C4 machine types, including local SSD and bare metal variants, on the latest

Try now

✓ General purpose

Compute optimized

Memory optimized

Storage optimized

GPUs

Machine types for common workloads, optimized for cost and flexibility

	Series ?	Description	vCPUs ?	Memory ?	CPU Platform
○	C4	Consistently high performance	2 - 288	4 - 2,232 GB	Intel Emerald
○	C4A	Arm-based consistently high performance	1 - 72	2 - 576 GB	Google Axion
○	C4D	Consistently high performance	2 - 384	3 - 3,072 GB	AMD Turin
○	N4	Flexible & cost-optimized	2 - 80	4 - 640 GB	Intel Emerald
○	C3	Consistently high performance	4 - 192	8 - 1,536 GB	Intel Sapphire
○	C3D	Consistently high performance	4 - 360	8 - 2,880 GB	AMD Genoa

Create

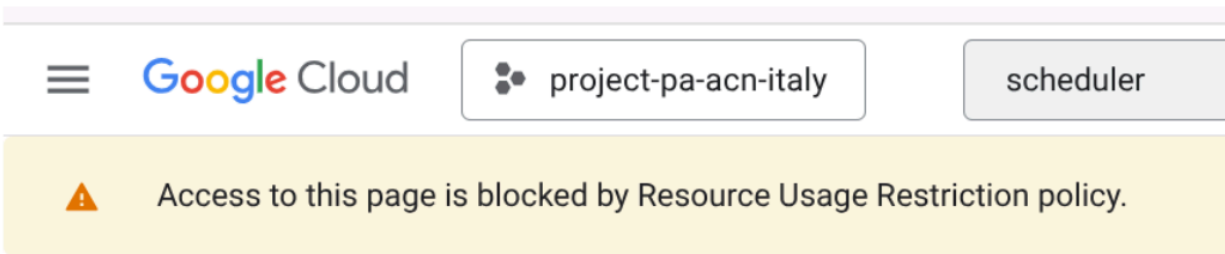
Cancel

⚡ Equivalent code

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.



There was an error while loading

[https://\[redacted\].google.com/cloudscheduler?referrer=search&authuser=2&inv=1&inv=Ab4Jow&orgonly=true&project=project-pa-acn-italy&supportedpurview=project](https://[redacted].google.com/cloudscheduler?referrer=search&authuser=2&inv=1&inv=Ab4Jow&orgonly=true&project=project-pa-acn-italy&supportedpurview=project).

Your administrator has activated the Resource Usage Restriction policy. This policy restricts access to selected GCP services and APIs.

[Learn more about Resource Usage Restriction](#) 

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.

Google Cloud | folder-pa-acn-italy | Search (/) for resources, docs, products, and more | Search

IAM & Admin / Organization policies / Policy details for constraint: gcp-resourceLocations / Edit policy

Overview **Preview** | **Edit policy**

Allow

Custom values

Enter one or more custom values. Custom values require specific formatting to work. [Learn more about formatting.](#)

To make sure your custom value works, test your policy after it's created. [Learn more.](#)

in:eu-west8-locations X

in:eu-west12-locations X

in:us-east1-locations X

+ Add value

Add condition

Add a rule

Set policy Cancel Done

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."

Compliance / Assured Workloads

Assured Workloads

Monitoring

Audit Manager

Assured Workloads folders

CREATE

SHOW INFO PA

Introducing Resource Violation Monitoring

NEW

Monitor your environment for resource violations in real time and get alerts when issues are detected. Enable this feature for your disabled folders in the selected organization to stay compliant.

LEARN MORE

2 unresolved

1 exceptions

View

18 unresolved

1 exceptions

View

All regions

Filter

Enter property name or value

☐	Name	Creation time	Control package	Resource location	Org policy violations	Resource violations	
☐	folder-pa-acn-italy	Jul 30, 2025,	EU Data Boundary	Italy	1 unresolved	0 violations	▼
☐	EUDataBoundary30luglio	Jul 30, 2025,	EU Data Boundary	Italy	0 violations	0 violations	▼
☐	TestLZPSN	Jul 29, 2025,	EU Data Boundary	Italy	0 violations	0 violations	▼
☐	Cartella Boundary Dati UE	Jul 23, 2025,	EU Data Boundary...	europe-west1	0 violations	0 violations	▼
☐	RCPartnerWebinarF	May 14, 2025,	EU Data Boundary	Italy	1 unresolved 1 exception	18 unresolved 1 exception	▼
☐	RegionalControlDestFolder	May 13, 2025,	EU Data Boundary	europe-west12	0 violations	0 violations	▼

Release Notes

Compliance / Violation: e886052e-9bf8-4d7b-881e-f381dc647d31

Assured Workloads

Monitoring

Audit Manager

Organization policy violation detail page

This compliance violation is currently unresolved. Follow the steps toward remediation below to resolve this violation or input a business justification to mark it as an exception.

Violation overview

The organization policy 'gcp.resourceLocations' for the folder **folder-pa-acn-italy** has been modified to allow resources to be located in non-compliant regions. This folder is no longer **EU Data Boundary** compliant.

Violation ID

e886052e-9bf8-4d7b-881e-f381dc647d31

Violation time

Jul 30, 2025, at 7:26:09 PM GMT+02:00

Folder name

folder-pa-acn-italy

Violation status

Unresolved

Audit log

Access the record of all actions taken in this folder in the audit log.

VIEW AUDIT LOG

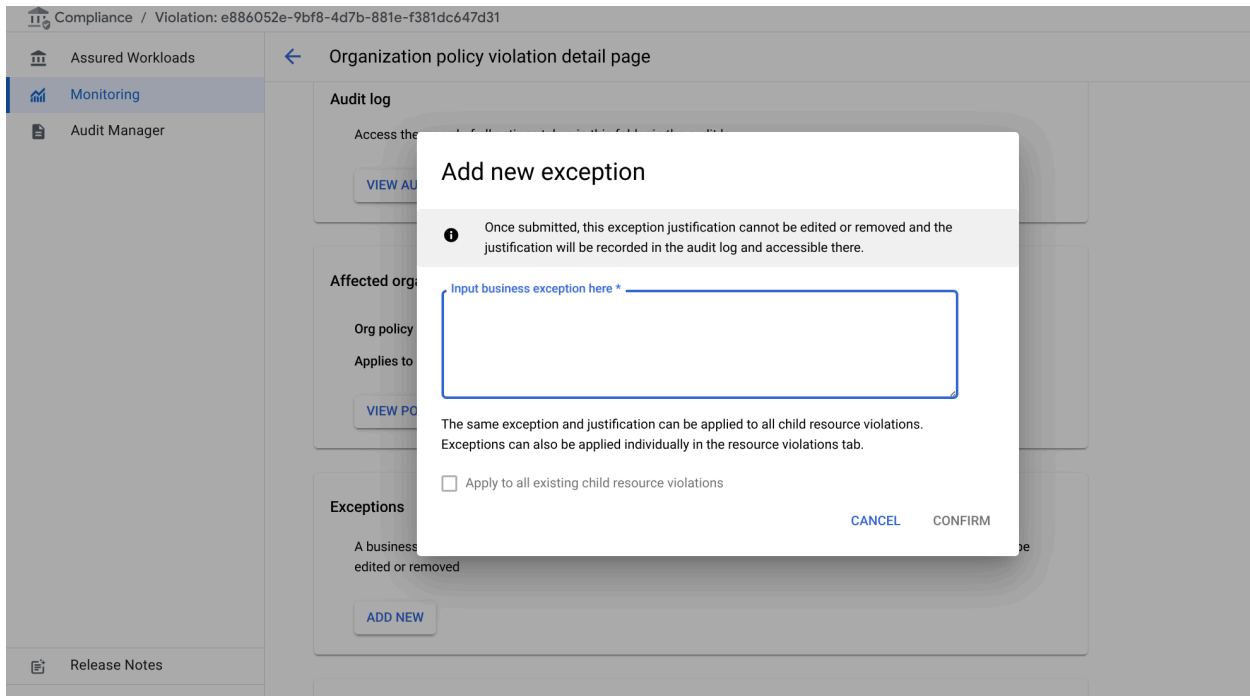
Affected organization policy

Org policy constraint

gcp.resourceLocations

Release Notes

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.

Google Cloud

project-pa-acn-italy

Search (/) for resources, docs, products, and more

Create an instance

Create VM from...

Machine configuration

Some form fields are incorrect

- OS and storage
Debian GNU/Linux 12 (bookworm)
- Data protection
Snapshot schedules
- Networking
Some form fields are incorrect
- Observability
- Security
- Advanced

Machine configuration

Name *

instance-20250730-173646

Region *

Americas

us-east1 (South Carolina)

Europe

europa-west12 (Turin)

europa-west8 (Milan)

Zone

Zone is permanent

General purpose

Compute optimized

Memory optimized

Storage optimized

GPUs

Machine types for common workloads, optimized for cost and flexibility

Series	Description	vCPUs	Memory	CPU Pla
C4	Consistently high performance	2 - 288	4 - 2,232 GB	Intel Eme
C4A	Arm-based consistently high performance	1 - 72	2 - 576 GB	Google A
C4D	Consistently high performance	2 - 384	3 - 3,072 GB	AMD Tur
N4	Flexible & cost-optimized	2 - 80	4 - 640 GB	Intel Eme
C3	Consistently high performance	4 - 192	8 - 1,536 GB	Intel Sap
C3D	Consistently high performance	4 - 360	8 - 2,880 GB	AMD Ger

Create

Cancel

Equivalent code

Google Cloud

project-pa-acn-italy

Search (/) for resources, docs, products, and more

Search

3

Compute Engine

VM instances

Create instance

Import VM

Refresh

Overview

Security risk overview

Virtual machines

VM instances

Instance templates

Sole-tenant nodes

Instances

Observability

Instance schedules

VM instances

Filter

Enter property name or value

Status	Name	Zone	Recommendations	In use by	Internal IP	External IP	Connect
✓	vmuseast1	us-east1-d			10.142.0.2 (nic0)		SSH

Step 4: Viewing the Resource Creation Violation

- Return to the "MONITORING" tab of Assured Workloads.
- After another scan (it may take several minutes), a second violation will appear.
 - Violation Type: RESOURCE_VIOLATION
 - 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.

Compliance / Assured Workloads

Assured Workloads

Monitoring

Audit Manager

Assured Workloads folders

CREATE

SH

Introducing Resource Violation Monitoring

NEW

Monitor your environment for resource violations in real time and get alerts when issues are detected. Enable this feature for your disabled folders in the selected organization to stay compliant.

LEARN MORE

All regions

Filter

Enter property name or value

☐	Name	Creation time	Control package	Resource location	Org policy violations	Resource violations
☒	folder-pa-acn-italy	Jul 30, 2025, 4:54:22 PM	EU Data Boundary	Italy	1 exception	3 unresolved
☐	EUDataBoundary30luglio	Jul 30, 2025,	EU Data Boundary	Italy	0 violations	0 violations
☐	TestLZPSN	Jul 29, 2025,	EU Data Boundary	Italy	0 violations	0 violations
☐	Cartella Boundary Dati UE	Jul 23, 2025,	EU Data Boundary...	europe-west1	0 violations	0 violations
☐	RCPartnerWebinarF	May 14, 2025,	EU Data Boundary	Italy	1 unresolved 1 exception	18 unresolved 1 exception
☐	RegionalControlDestFolder	May 13, 2025,	EU Data Boundary	europe-west12	0 violations	0 violations
☐	EU Regional Control Webinar	May 13, 2025,	EU Data Boundary	Italy	-	-
☐	PSN Regional Control 25-03	Mar 25, 2025,	EU Data Boundary	Italy	-	-

Release Notes

Release Notes

Release Notes

Release Notes

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

Compliance / Resource Violation

Assured Workloads

Monitoring

Audit Manager

Assured Workloads Monitoring

ORGANIZATION POLICY VIOLATIONS

RESOURCE VIOLATIONS

Your folders and projects are scanned in real time for potential resource violations which may have resulted due to organization policy violations to ensure compliance. Currently scanning 3 Organization Policies

Unresolved 22

Exception 1

Resolved 0

Quick filters

CLEAR ALL

Violation status

☒ Unresolved 22
 ☐ Exception 1
 ☐ Resolved 0

Project

☐ RCPartnerWebinarP 18
 ☐ project-pa-acn-italy 4

Violation ID	Project	Resource type	Compliance type	Violation type
0cb3b437-92...46ebc8	project-pa-acn-italy	compute.../ResourcePolicy	EU Data Boundary	Location
70f8e8e2-e9...cb919d	project-pa-acn-italy	compute.../Instance	EU Data Boundary	Location
22b2a764-51...fb4aed	project-pa-acn-italy	compute.../Disk	EU Data Boundary	Location
b83619f7-89...3aba30	project-pa-acn-italy	compute.../Subnetwork	EU Data Boundary	Location

Release Notes

Release Notes

Release Notes

Release Notes

16

© 2024 Google LLC. All rights reserved.

Compliance / Violation: 0cb3b437-9220-4dbe-8ab7-45c96146ebc8

Assured Workloads

Monitoring

Audit Manager

Resource violation detail page

This compliance violation is currently unresolved. Follow the steps toward remediation below to resolve this violation or input a business justification to mark it as an exception.

Violation overview

The resource `//compute.googleapis.com/projects/project-pa-acn-italy/regions/us-east1/resourcePolicies/default-schedule-1` is created in a restricted location. This has resulted in a compliance violation.

Violation ID: `0cb3b437-9220-4dbe-8ab7-45c96146ebc8`

Folder name: [folder-pa-acn-italy](#)

Project ID: [project-pa-acn-italy](#)

Resource name: `//compute.googleapis.com/projects/project-pa-acn-italy/regions/us-east1/resourcePolicies/default-schedule-1`

Resource type: `compute.googleapis.com/ResourcePolicy`

Violation time: Jul 30, 2025, at 7:52:50 PM GMT+02:00

Violation status: Unresolved

Audit log

Access the record of all actions taken in this folder in the audit log.

Release Notes

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

Google Cloud

project-pa-acn-italy

Search

Logs Explorer

Query library

Share link

Preferences

7:52 PM - Now

CEST

Project logs

Faster

Run query

All resources

All log names

All severities

Correlate by

1 SEARCH("default-schedule-1")

2 compute.googleapis.com

Example queries

Query language guide

Fields

Search fields and values

System Metadata

Severity

Showing top 1 of 1 value

Notice

Resource type

JSON payload (most frequent)

Preview

No results found

Timeline

3 results

SEVERITY	TIME	SUMMARY
Notice	2025-07-30 19:52:50.348	compute.googleapis.com v1.compute.resourcePolicies.insert _ast1//resourcePolicies/default-schedule-1

Explain this log entry

Copy

Expand nested fields

Hide log summary

```

{
  insertId: "klhzffdbu0k"
  labels: {1}
  logName: "projects/project-pa-acn-italy/logs/cloudaudit.googleapis.com%2Factivity"
  operation: {3}
  protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog"
    authenticationInfo: {1}
    authorizationInfo: [1]
  }
}

```

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.

The screenshot shows the Google Cloud IAM & Admin console. The breadcrumb trail is: IAM & Admin / Organization policies / Policy details for constraint: custom-createOnlyN2DVMss. The left sidebar shows the 'Organization Policies' section selected. The main content area displays the 'Policy details' for 'Policy for "N2D Only"'. It shows the policy is 'Live' and 'Not enforced'. Below this, the 'Effective policy for folder "folder-pa-acn-italy"' is shown, indicating it is a computed policy. The 'Constraint details' table lists the following information:

Constraint details	
Constraint ID	custom.createOnlyN2DVMss
Enforcement method	Enforce on create
Description	
Resource type	compute.googleapis.com/Instance
Condition	resource.machineType.contains('/machineTypes/n2d')
Action	Allow
Display name	N2D Only
Last updated	March 25, 2025 at 11:21:53 AM UTC+1

At the bottom of the constraint details, there is a link to 'Show constraint YAML'.

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.