Introduction to the Organization Policy Service

The Organization Policy Service gives you centralized and programmatic control over your organization's cloud resources. As the organization policy administrator (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#add-org-policy-admin), you will be able to configure restrictions across your entire resource hierarchy (https://cloud.google.com/resource-manager/docs/cloud-platform-resource-hierarchy).

Benefits

- Centralize control to configure restrictions on how your organization’s resources can be used.
- Define and establish guardrails for your development teams to stay within compliance boundaries.
- Help project owners and their teams move quickly without worry of breaking compliance.

Common use cases

See the list of all Organization Policy Service constraints (https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints).

Differences from Cloud Identity and Access Management

Cloud Identity and Access Management (https://cloud.google.com/iam/) focuses on **who**, and lets the administrator authorize (https://cloud.google.com/resource-manager/docs/access-control-org) who can take action on specific resources based on permissions.

Organization Policy focuses on **what**, and lets the administrator set restrictions on specific resources to determine how they can be configured.

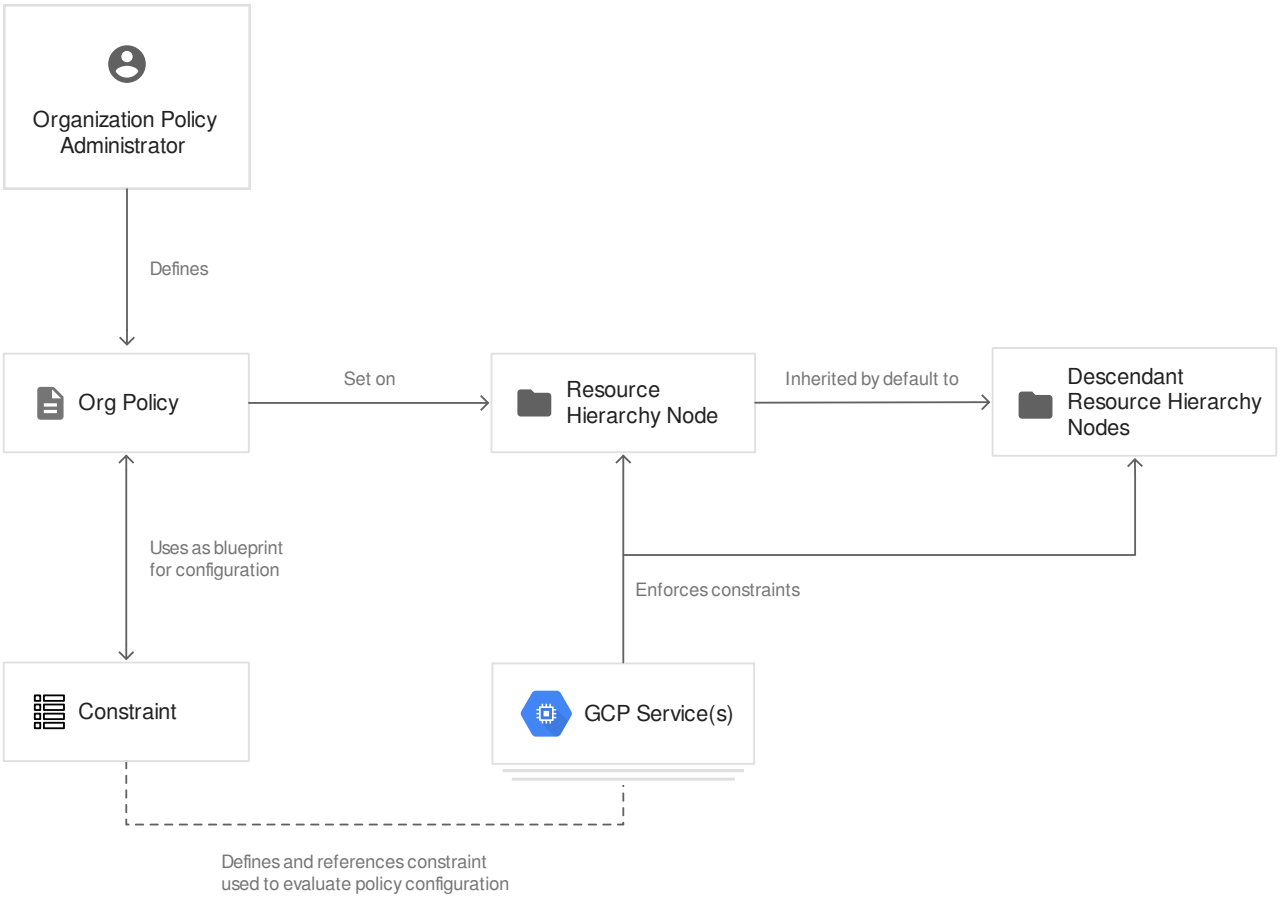
Key Concepts

Organization policy

An organization policy is a configuration of restrictions. You, as the organization policy administrator (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#add-org-policy-admin), define an organization policy, and you set that organization policy on a resource hierarchy node in order to enforce the restrictions on that resource hierarchy node and its descendants.

In order to define an organization policy, you choose a constraint (#constraints), which is a particular type of restriction against either a Google Cloud service or a group of Google Cloud services. You configure that constraint with your desired restrictions.

Descendants of the targeted resource hierarchy node inherit (#inheritance) the organization policy. By applying an organization policy to the root organization node, you are able to effectively drive enforcement of that organization policy and configuration of restrictions across your organization.



Constraints

A constraint is a particular type of restriction against a Google Cloud service (https://cloud.google.com/docs/overview/cloud-platform-services) or a list of Google Cloud services. Think of the constraint as a blueprint that defines what behaviors are controlled. This blueprint is then applied to a resource hierarchy (https://cloud.google.com/resource-manager/docs/cloud-platform-resource-hierarchy) node as an organization policy, which implements the rules defined in the constraint. The Google Cloud service mapped to that constraint and associated with that resource hierarchy node will then enforce the restrictions configured within the organization policy.

A constraint has a type, either list (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#list-constraint) or boolean (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#boolean-constraint)

. List constraints evaluate the constraint with a list of allowed or denied values that you provide, such as a whitelist of IP addresses that can connect to a virtual machine. Boolean constraints are either enforced or not enforced for a given resource, and govern a specific behavior, such as whether external service accounts can be created.

Constraint type	Business need	Constraint configuration

List (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#list-constraint)	Restrict configuration of external IPs to a list of instances	`resource: "organizations/ORGANIZATION_ID"`
		`policy: {`
		`constraint: "constraints/compute.vmExternal`
		`listPolicy: {`
		`allowedValues: [`
		`projects/PROJECT_NAME/zones/ZONE_ID/insta`
		`projects/PROJECT_NAME/zones/ZONE_ID/insta`
		`]`
		`}`
		`}`

Boolean (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#boolean-constraint)	Disable service account creation	`resource: "organizations/ORGANIZATION_ID"`
		`policy: {`
		`constraint: "constraints/iam.disableService`
		`booleanPolicy: {`
		`enforced: true`
		`}`
		`}`

Each Google Cloud service evaluates constraint types and values to determine what should be restricted. To learn more about constraints, see the Understanding Constraints (https://cloud.google.com/resource-manager/docs/organization-policy/understanding-constraints) page.

Inheritance

When an organization policy is set on a resource hierarchy node, all descendants of that node inherit the organization policy by default. If you set an organization policy at the root organization node, then the configuration of restrictions defined by that policy will be passed down through all descendant folders, projects, and service resources.

A user with the **Organization Policy Administrator** role can set descendant resource hierarchy nodes with another organization policy that either overwrites the inheritance, or merges them based on the rules of hierarchy evaluation. This provides precise control for how your

organization policies apply throughout your organization, and where you want exceptions made.

To learn more about hierarchy evaluation, see the Understanding Hierarchy (https://cloud.google.com/resource-manager/docs/organization-policy/understanding-hierarchy) page.

Violations

A violation is when a Google Cloud service acts or is in a state that is counter to the organization policy restriction configuration within the scope of its resource hierarchy. Normally, GCP services will enforce a constraint to prevent the violation, but the application of a new organization policy is **not retroactive**.

If a new organization policy sets a restriction on an action or state that a service is already in, the policy is considered to be in violation, but the service will not stop its original behavior. You will need to address this violation manually. This prevents the risk of a new organization policy completely shutting down your business continuity.

Next steps

- Read the Creating and Managing Organizations (https://cloud.google.com/resource-manager/docs/creating-managing-organization) page to learn how to acquire an organization resource.
- Read about how to create and manage organization policies (https://cloud.google.com/resource-manager/docs/organization-policy/creating-managing-policies) with the Google Cloud Console.
- Learn how to define organization policies using constraints (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints).
- Explore the solutions you can accomplish (https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints) with organization policy constraints.

Last updated December 9, 2019.