Google Cloud

Organizational policy constraints, inheritance, and violation

So far, you've learned that cloud organizational policies are restrictions or constraints on cloud services for security, risk management, and compliance purposes. Cloud organizational policies prevent security violations from happening by restricting actions that pose security risks. Google Cloud's **Organization Policy Service** gives you centralized control over organization policies throughout your resource hierarchy. In this reading, you'll learn more about organizational policy constraints, inheritance, and violations.

Policy constraints

A **constraint** is a restriction against a Google Cloud service, or a list of services. Once you apply a constraint to an organization, folder, or project, the Google Cloud service mapped to the constraint will enforce the restrictions you've configured.

Every constraint has these attributes:

- A unique **name,** which might be something like: `constraints/compute.disablePortAccess`
- A **display name** that is reader user friendly, for example: 'Disable Port Access Constraint"
- A **description** that details the enforcements that are put in place by applying the constraint
- A **default behavior** that explains what will happen in the absence of user defined configurations within a policy

List constraints and **boolean constraints** are two common types of constraints used to enforce policy.

Policy inheritance

A constraint acts like a blueprint that defines which behaviors are controlled. This blueprint is then applied to a 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.

During the hierarchy evaluation, the organization policy set on the current resource hierarchy node takes effect. During evaluation, you can also disallow inheritance, reconcile policy conflicts, and even reset to default policy.

Policy violation

A violation occurs when a Google Cloud service does not follow policy restrictions set up in the resource hierarchy. Google Cloud services will enforce constraints to prevent violations, but the application of new organization policies is usually not retroactive. This means that once a new policy is in place, actions that occurred previously may be in violation of the new policy.

Key takeaways

Organizational policy constraints and inheritance help you automate and enforce policies across an organization. Knowing when and how violations can occur can help you to stop or correct policy violations.

Resources for more information

These resources provide more information on policy constraints:

- This Google cloud resource includes a variety of constraints that are supported by Google Cloud services.
- The constraints for specific services outline different constraints for services like BlgQuery, App Engine,or Cloud Deploy.
- Review the how-to guides to learn more about how to use individual constraints.