Policy

Defines an Identity and Access Management (IAM) policy. It is used to specify access control policies for Cloud Platform resources.

A `Policy` is a collection of `bindings`. A `binding` binds one or more `members` to a single `role`. Members can be user accounts, service accounts, Google groups, and domains (such as G Suite). A `role` is a named list of permissions (defined by IAM or configured by users). A `binding` can optionally specify a `condition`, which is a logic expression that further constrains the role binding based on attributes about the request and/or target resource.

JSON Example

```
{
  "bindings": [
    {
      "role": "roles/resourcemanager.organizationAdmin",
      "members": [
        "user:mike@example.com",
        "group:admins@example.com",
        "domain:google.com",
        "serviceAccount:my-project-id@appspot.gserviceaccount.com"
      ]
    },
    {
      "role": "roles/resourcemanager.organizationViewer",
      "members": ["user:eve@example.com"],
      "condition": {
        "title": "expirable access",
        "description": "Does not grant access after Sep 2020",
        "expression": "request.time <
        timestamp('2020-10-01T00:00:00.000Z')",
      }
    }
  ]
}
```

YAML Example

```
bindings:
- members:
```

```
  - user:mike@example.com
  - group:admins@example.com
  - domain:google.com
  - serviceAccount:my-project-id@appspot.gserviceaccount.com
  role: roles/resourcemanager.organizationAdmin
- members:
  - user:eve@example.com
  role: roles/resourcemanager.organizationViewer
  condition:
    title: expirable access
    description: Does not grant access after Sep 2020
    expression: request.time < timestamp('2020-10-01T00:00:00.000Z')
```

For a description of IAM and its features, see the <u>IAM developer's guide</u>
 (https://cloud.google.com/iam/docs).

JSON representation

```
{
  "version": number,
  "bindings": [
    {
      object (Binding (https://cloud.google.com/vision/automl/docs/reference/rest/v1beta1/Policy#B
    }
  ],
  "etag": string
}
```

Fields

Fields

version	**number** Specifies the format of the policy. Valid values are 0, 1, and 3. Requests specifying an invalid value will be rejected. Operations affecting conditional bindings must specify version 3. This can be either setting a conditional policy, modifying a conditional binding, or removing a conditional binding from the stored conditional policy. Operations on non-conditional policies may specify any valid value or leave the field unset. If no etag is provided in the call to `setIamPolicy`, any version compliance checks on the incoming and/or stored policy is skipped.

bindings[]	`object (`<u>`Binding`</u>
	`(https://cloud.google.com/vision/automl/docs/reference/rest/v1beta1/`
	`Policy#Binding)`
	`)`
	
	Associates a list of `members` to a `role`. Optionally may specify a `condition` that determines when binding is in effect. `bindings` with no members will result in an error.

etag	`string (`<u>`bytes`</u> `(https://developers.google.com/discovery/v1/type-format)` `format)` `etag` is used for optimistic concurrency control as a way to help prevent simultaneous updates of a policy from overwriting each other. It is strongly suggested that systems make use of the `etag` in the read-modify-write cycle to perform policy updates in order to avoid race conditions: An `etag` is returned in the response to `getIamPolicy`, and systems are expected to put that etag in the request to `setIamPolicy` to ensure that their change will be applied to the same version of the policy. If no `etag` is provided in the call to `setIamPolicy`, then the existing policy is overwritten. Due to blind-set semantics of an etag-less policy, 'setIamPolicy' will not fail even if either of incoming or stored policy does not meet the version requirements. A base64-encoded string.

Binding

Associates `members` with a `role`.

JSON representation
```{   "role": string,   "members": [string   ],   "condition": {   object (Expr (https://cloud.google.com/vision/automl/docs/reference/rest/v1beta1/Policy#Expr))   } }```

Fields	
`role`	**string** Role that is assigned to `members`. For example, `roles/viewer`, `roles/editor`, or `roles/owner`.
`members[]`	**string** Specifies the identities requesting access for a Cloud Platform resource. `members` can have the following values: • `allUsers`: A special identifier that represents anyone who is on the internet; with or without a Google account. • `allAuthenticatedUsers`: A special identifier that represents anyone who is authenticated with a Google account or a service account. • `user:{emailid}`: An email address that represents a specific Google account. For example, `alice@example.com`. • `serviceAccount:{emailid}`: An email address that represents a service account. For example, `my-other-app@appspot.gserviceaccount.com`. • `group:{emailid}`: An email address that represents a Google group. For example, `admins@example.com`. • `domain:{domain}`: The G Suite domain (primary) that represents all the users of that domain. For example, `google.com` or `example.com`.

Fields	
condition	object (Expr (https://cloud.google.com/vision/automl/docs/reference/rest/v1beta1/Policy#Expr)) The condition that is associated with this binding. NOTE: An unsatisfied condition will not allow user access via current binding. Different bindings, including their conditions, are examined independently.

Expr

Represents an expression text. Example:

```
title: "User account presence"
description: "Determines whether the request has a user account"
expression: "size(request.user) > 0"
```

JSON representation
| ```
{
  "expression": string,
  "title": string,
  "description": string,
  "location": string
}
``` |

Fields	
expression	string Textual representation of an expression in Common Expression Language syntax. The application context of the containing message determines which well-known feature set of CEL is supported.

Fields	
title	**string** An optional title for the expression, i.e. a short string describing its purpose. This can be used e.g. in UIs which allow to enter the expression.
description	**string** An optional description of the expression. This is a longer text which describes the expression, e.g. when hovered over it in a UI.
location	**string** An optional string indicating the location of the expression for error reporting, e.g. a file name and a position in the file.