Restricting Service Account Usage

The Resource Manager provides constraints that can be used in organization policies (https://cloud.google.com/resource-manager/docs/organization-policy/understanding-policies) to limit the usage of Cloud Identity and Access Management service accounts (https://cloud.google.com/iam/docs/).

When you set these constraints, they apply to future creation of and modifications to service accounts. These constraints are not retroactive and will not affect previously created and configured service accounts.

Disable service account creation

You can use the `iam.disableServiceAccountCreation` boolean constraint to disable the creation of new service accounts. This allows you to centralize management of service accounts while not restricting the other permissions your developers have on projects.

Disable service account key creation

You can use the `iam.disableServiceAccountKeyCreation` boolean constraint to disable the creation of new external service account keys. This allows you to control the use of unmanaged long-term credentials for service accounts. When this constraint is set, user-managed credentials cannot be created for service accounts in projects affected by the constraint.

Setting the policy

The service account restriction constraint is a type of boolean constraint (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#boolean-constraint)
.

You must have permission to modify organization policies (https://cloud.google.com/resource-manager/reference/rest/v1/Policy) to set this constraint. For example, the `resourcemanager.organizationAdmin` (https://cloud.google.com/resource-manager/docs/access-control-org) role has permission to set organization policy constraints. Read the Using Constraints (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#add-org-policy-admin) page to learn more about managing policies at the organization level.

CONSOLE GCLOUD

To set an organization policy including a constraint to disable service account key creation:

1. Go to the **Organization policies** page in the Google Cloud Console.

   GO TO THE ORGANIZATION POLICIES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/IAM-ADMIN

2. Click the **Organization** drop-down list at the top of the page and then select your organization.
3. Click **Disable Service Account Creation** or **Disable Service Account Key Creation**.
4. Click the **Edit** button.
5. Under **Applies to**, select **Customize**.
6. Under **Enforcement**, select **On**.
7. Click **Save**. A notification will appear to confirm that the policy has been updated.

To learn about using constraints in organization policies, see Using Constraints (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#boolean-constraint)
.

Example policy

The following code snippet shows an organization policy including the disable service account creation constraint:

```
resource: "organizations/842463781240"
policy {
  constraint: "constraints/iam.disableServiceAccountCreation"
  etag: "\a\005L\252\122\321\946\334"
  boolean_policy {
```

```
  enforced: true
  }
}
```

The following code snippet shows an organization policy including the disable service account key creation constraint:

```
resource: "organizations/842463781240"
policy {
  constraint: "constraints/iam.disableServiceAccountKeyCreation"
  etag: "\a\005L\252\122\321\946\334"
  boolean_policy {
  enforced: true
  }
}
```

Restrict service account key upload

You can use the `iam.allowedPublicCertificateTrustedRootCA` list constraint to restrict the public keys that can be uploaded to service accounts. This constraint allows you to define a set of trusted certificate authorities from which the issued public certificates can be uploaded to Cloud Identity and Access Management service accounts. Additionally, you can also fully disable service account key upload by setting this list constraint to `Deny All`.

Setting the policy

The service account upload restriction constraint is a type of list constraint (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#list-constraint).

You must have permission to modify organization policies (https://cloud.google.com/resource-manager/reference/rest/v1/Policy) to set this constraint. For example, the `resourcemanager.organizationAdmin` (https://cloud.google.com/resource-manager/docs/access-control-org) role has permission to set organization policy constraints. For more information about managing policies at the organization level, see Using Constraints (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#add-org-policy-admin)

.

CONSOLE GCLOUD

To set an organization policy including a constraint to service account key upload:

1. Go to the **Organization policies** page in the Google Cloud Console.

   GO TO THE ORGANIZATION POLICIES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/IAM-ADMIN

2. Click the **Organization** drop-down list at the top of the page and then select your organization.
3. Click **Define allowed root certificate authority**.
4. Click the **Edit** button.
5. Under **Applies to**, select **Customize**.
6. Under **Policy Values**, select **Custom**.
7. Enter a Certificate Authority (#certificate_authority) into the **Custom values** text box.
   a. To enter multiple values, click **New policy value** and enter one certificate authority per line.
8. Click **Save**. A notification will appear to confirm that the policy has been updated.

To learn about using list constraints in organization policies, see Using Constraints (https://cloud.google.com/resource-manager/docs/organization-policy/using-constraints#list-constraint).

Example organization policy

The following code snippet shows an organization policy including an allowed certificate authority:

```
resource: "organizations/842463781240"
policy {
  constraint: "constraints/iam.allowedPublicCertificateTrustedRootCA"
  etag: "\a\005L\252\122\321\946\334"
  list_policy {
  allowed_values: "issuer=C = AU, ST = Some-State, O = Internet Widgits Pty Ltd"
  }
}
```

Retrieve certificate authority from a public key certificate

The certificate authority of a public key certificate can be obtained using following command:

```
openssl x509 -noout -in $PUBLIC_KEY_CERT_PATH -issuer
```

Please note that this command only works for public key certificates that are in X509 PEM format.

Error Messages

Disable service account creation

If `iam.disableServiceAccountCreation` is enforced, creating a service account will fail with the error:

```
FAILED_PRECONDITION: Service account creation is not allowed on this project.
```

Disable service account key creation

If `iam.disableServiceAccountKeyCreation` is enforced, creating a service account will fail with the error:

```
FAILED_PRECONDITION: Key creation is not allowed on this service account.
```

Troubleshooting Known Issues

Default service accounts

Applying the `iam.disableServiceAccountCreation` constraint will prevent the creation of service accounts in that project. This limitation also affects Google Cloud services that, when enabled, automatically create default service accounts in the project, such as:

- Compute Engine
- GKE
- App Engine
- Dataflow

If the `iam.disableServiceAccountCreation` constraint is applied, attempting to enable these services will fail because their default service accounts cannot be created.

To resolve this issue:

1. Temporarily remove the `iam.disableServiceAccountCreation` constraint.
2. Enable the desired services.
3. Create any other desired service accounts.
4. Finally, re-apply the constraint.

Last updated December 4, 2019.