

JSON key file (Google ServiceAccount)

A user-managed key-pair that you can use as a credential for a service account. Because the credential is long-lived, it is the least secure option of all the available authentication methods.

A service account key is a long-lived key-pair that you can use as a credential for a service account. Unlike the OAuth access token, a service account key does not expire. You are responsible for security of the private key and other key management operations, such as key rotation.

Anyone who has access to a valid private key for a service account will be able to access resources through the service account. For example, some service accounts automatically created by Google Cloud, such as the Container Registry service account, are granted the read-write [Editor](#) role for the parent project. The Compute Engine default service account is configured with read-only access to storage within the same project.

In addition, the lifecycle of the key's access to the service account (and thus, the data the service account has access to) is independent of the lifecycle of the user who has downloaded the key.

Use the following guidelines to limit access to your container images:

- Create dedicated service accounts that are only used to interact with Container Registry.
- Grant the specific [role](#) for the least amount of access that the service account requires.
- Follow [best practices for managing credentials](#).

To create a new service account and a service account key for use with Container Registry repositories only:

1. Create a new service account that will interact with Container Registry. From gcloud console

The screenshot shows the Google Cloud Platform (GCP) web interface. The left sidebar is open, showing the 'IAM & Admin' section under 'APIS & SERVICES'. The main content area is titled 'Service Accounts' and shows three existing projects: 'devops25', 'test', and 'My First Project'. The 'devops25' project card provides details: Project ID: devops25-338512, Organization: No organization, Accessed 2 hours ago. Below the projects, there is a link to 'Create a Project'. The top navigation bar includes tabs for Home, Recent, View all products, IAM, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts, Workload Identity Federation, Labels, Tags, Settings, Privacy & Security, Identity-Aware Proxy, Roles, Audit Logs, Manage Resources, Create a Project, Asset Inventory, Essential Contacts, Groups, and Early Access Center. A search bar at the top right is empty. The URL in the address bar is <https://console.cloud.google.com/iam-admin/serviceaccounts?supportedpurview=project>.

Select Your Project

The screenshot shows the Google Cloud Platform interface for managing service accounts. The left sidebar is titled "IAM & Admin" and includes links for IAM, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts (which is selected), Workload Identity Federat..., Labels, Tags, Settings, Privacy & Security, Manage Resources, and Release Notes. The main content area is titled "Service Accounts" and displays a message: "To view this page, select a project." Below this, there is a section titled "Select a recent project" showing five recent projects: "naresh" (Project ID: naresh-342705, Organization: No organization, Accessed 2 hours ago), "devops25" (Project ID: devops25-338512, Organization: No organization, Accessed 2 hours ago), "test" (Project ID: argon-key-342705, Organization: No organization, Accessed 1 day ago), "corp" (Project ID: corp-342307, Organization: No organization, Accessed 1 day ago), and "My First Project" (Project ID: zippy-chain-338512, Organization: No organization, Accessed Jan 17, 2022). There are also buttons for "SELECT PROJECT" and "CREATE PROJECT".

The screenshot shows the Google Cloud Platform Service Accounts page for the project "naresh". The left sidebar is identical to the previous screenshot. The main content area is titled "Service accounts" and includes buttons for "+ CREATE SERVICE ACCOUNT", "DELETE", "MANAGE ACCESS", and "REFRESH". Below this, there is a section titled "Service accounts for project "naresh"" with a brief description: "A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts.](#)" and a note: "Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account organization policies.](#)".

Chrome File Edit View History Bookmarks Profiles Tab Window Help

labs/hpa Creating Use IAM How to P Installing How to P gcloud cr Authenti Create S Releases

Govt eSign PDF Downloads Imported github My Portal terraform Ansible python CKA CKS devops25

Google Cloud Platform naresh Search Products, resources, docs (/)

IAM & Admin

- IAM
- Identity & Organization
- Policy Troubleshooter
- Policy Analyzer
- Organization Policies
- Service Accounts**
- Workload Identity Federat...
- Labels
- Tags

Create service account

1 Service account details

Service account name Display name for this service account

Service account ID *

Service account description

Describe what this service account will do

CREATE AND CONTINUE

Chrome File Edit View History Bookmarks Profiles Tab Window Help

labs/hpa Creating Use IAM How to P Installing How to P gcloud cr Access Create S Releases

Govt eSign PDF Downloads Imported github My Portal terraform Ansible python CKA CKS devops25

Google Cloud Platform naresh Search Products, resources, docs (/)

IAM & Admin

- IAM
- Identity & Organization
- Policy Troubleshooter
- Policy Analyzer
- Organization Policies
- Service Accounts**
- Workload Identity Federat...
- Labels
- Tags
- Settings
- Privacy & Security
- Manage Resources
- Release Notes

Create service account

1 Service account details

2 Grant this service account access to project (optional)

Grant this service account access to naresh so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Select a role Condition

All Platform service agent can act as log writer, Cloud Storage admin, Artifact Registry Reader, BigQuery writer, and service account access token creator.

Storage Admin
Full control of GCS resources.

Storage HMAC Key Admin
Full control of GCS HMAC Keys.

Storage Object Admin
Full control of GCS objects.

DONE

Chrome File Edit View History Bookmarks Profiles Tab Window Help

labs/hpa Creating Use IAM How to P Installing How to P gcloud Access Create S Releases

Govt eSign PDF Downloads Imported github My Portal terraform Ansible python CKA CKS devops25

Google Cloud Platform naresh Search Products, resources, docs (/)

IAM & Admin Create service account

IAM Identity & Organization Policy Troubleshooter Policy Analyzer Organization Policies Service Accounts Workload Identity Federat... Labels Tags Settings Privacy & Security Manage Resources

Service account details

Grant this service account access to project (optional)

Role: Storage Admin Condition: Add condition

Full control of GCS resources.

+ ADD ANOTHER ROLE

CONTINUE

Grant users access to this service account (optional)

DONE CANCEL

Chrome File Edit View History Bookmarks Profiles Tab Window Help

labs/hpa Creating Use IAM How to P Installing How to P gcloud Access Create S Releases

Govt eSign PDF Downloads Imported github My Portal terraform Ansible python CKA CKS devops25

Google Cloud Platform naresh Search Products, resources, docs (/)

IAM & Admin Service accounts + CREATE SERVICE ACCOUNT DELETE MANAGE ACCESS REFRESH

IAM Identity & Organization Policy Troubleshooter Policy Analyzer Organization Policies Service Accounts Workload Identity Federat... Labels Tags Settings

Service accounts for project "naresh"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts.](#)

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account organization policies.](#)

Filter Enter property name or value

Email	Status	Name	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
945973218273-compute@developer.gserviceaccount.com	✓	Compute Engine default service account	No keys		1092926987808639738		
gcr-login@naresh-342705.iam.gserviceaccount.com	✓	gcr-login	No keys		1160341642286100634		

Obtain a key for the service account that will interact with Container Registry.

The screenshot shows the Google Cloud Platform interface for managing service accounts. The left sidebar is titled 'IAM & Admin' and includes sections for IAM, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts (which is selected), Workload Identity Federation, Labels, Tags, Settings, Privacy & Security, and Manage Resources. The main content area is titled 'gcr-login' and shows the 'KEYS' tab selected. A warning message states: 'Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the [Workload Identity Federation](#). You can learn more about the best way to authenticate service accounts on Google Cloud [here](#).' Below this, there are buttons for 'ADD KEY' (with options 'Create new key' or 'Upload existing key'), 'Key creation date', and 'Key expiration date'. The 'DETAILS', 'PERMISSIONS', 'METRICS', and 'LOGS' tabs are also visible at the top of the main content area.

The screenshot shows a modal dialog box titled 'Create private key for "gcr-login"'. The dialog contains instructions: 'Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.' It includes a 'Key type' section with two options: 'JSON' (selected) and 'P12'. A note under 'P12' says: 'For backward compatibility with code using the P12 format'. At the bottom of the dialog are 'CANCEL' and 'CREATE' buttons. The background of the main interface is dimmed, and the 'KEYS' tab is still highlighted in blue.

Finder File Edit View Go Window Help

labs/hpa Creating Use IAM How to P Installing How to P gcloud cr Authenti gcr-login Releases

console.cloud.google.com/iam-admin/serviceaccounts/details/116034164228610063433/keys?project=naresh-342705&supportedpurview=project

Govt eSign PDF Downloads Imported github My Portal terraform Ansible python CKA CKS devops25

Google Cloud Platform naresh Search Products, resources, docs (/)

IAM & Admin

DETAILS PERMISSIONS KEYS METRICS LOGS

Keys

Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the [Workload Identity Federation](#). You can learn more about the best way to authenticate service accounts on Google Cloud [here](#).

Private key saved to your computer

naresh-342705-28c48e6d4d8d.json allows access to your cloud resources, so store it securely. [Learn more best practices](#)

CKAD_Curriculum.pdf docker-cred...-4-2.1.0.tar.gz edufeb21.pem Elec-Bill-min.jpg iCloud Photos.zip Istio myprojec-1.5.tar.gz naresh-3427..6d4d8d.json PTRReceiptDetails.pdf SBI-Kanduko...updated.pdf SBI-Kanduko.pdf SBI-latest-updated.pdf SBI-latest.pdf Statement_Feb 2022.pdf terraform.docx Training Pres...mplate.pptx

naresh-342705-28c48e6d4d8d.json

JSON file - 2 KB

Information

CLOSE

Show all

iTerm2 Shell Edit View Session Scripts Profiles Toolbelt Window Help

ssh ssh -zsh

```
root@test:~# cat keyfile.json
{
    "type": "service_account",
    "project_id": "naresh-342705",
    "private_key_id": "28c48e6d4d8d107602e338952037898b746d3c35",
    "private_key": "-----BEGIN PRIVATE KEY-----\nMIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwgSjAgEAAoIBAQD\nm0bVjaw/sQ5Nb/nTfDh/mM16VhcReBxuYHdjWmlJPm1yw1SwFxCQH4cuH+FQhgJSXX777jF7TM/dGz\nnzSqr2IKCglm81G0omPMVwXZAlmrSmrA90EHwgb0lo9mJHKSB5c1JGH\nmra90EHwGs0io8m2HHKS5c1JGH9JcDZ8/nEI9k6ytFY9uiwlhXvYx1Ns9k3xq142sbAWc3Msq9AdALks2c3QFMoN7HMh3P1V\nnp1sIZy7ufEM3NRcU9ctp0Jd1NtMKC7xmrh+Gb283vb0hKGEdmS8\noapEhqCf1ypnJ4mEyIGzXDRlx50Dzkow5jTT4+CjRq7NhLrGvCFGmpaa\nxsylZobpLL+64pV994cLESAgBAEAEcgEAY70App\nUJ1ffGbbADkhQbeUMnh79tn8H7r0F3G1WrkG\nn7IFsBIM+1XjDDTz/R0X9xdZewYuspBBSMVol\njCetqJ5L1eDi13FbWMztL9xibhn\nn+UyQiuhfsRnPk3d/wMxNyMj1Q7G3FLdohSsrtpmMeA0FP1artsvbBvtNwIWFFR2Wv\\n9pZZEcWEpn2Qn4JX\nD5sErc0/0fUP3sDdaU2KH+ftc/LjxSlc/7BLBn3X8gVptmc\\nVmseWTKi\npgZmebrjq16NVVAP/kINjHFhr3NG0GRiwKHth3vQDYdHXVFKNJsGCX\ns\\nE2jhBht8LTkbmENHt1KA3njP/fffYK6ImUu49nZCkQKbgD2xz4uH/ew+z1Vd1kx\\njmAvpPo+pfHC5YWyThXbymRp2wkE2gIu30y06oi1IR\nLZyrsYGC3rxFWpPKxbvA\\nwGjaoyV83iL3k64T6fc4m6nXlU5CdC8grji1Lv4Prxx0+D+SdJhQISZH8XH2QcTn\\nZSPMCXn499aYQY2+Emkwra\ndMwKBgQDvccu6o69EhDnxiU/MZ3MbR7zTQuL7Ad2M\\n0LcTs1PS2W4M7iNit4d9WBXcacuuMLH7jFloCkp/+txYK8//m/wLntG3YEfMDTz\\nF6Q\nJLN/05eCbNdPxYo27LW8DJx5gVrJa/n7V4au1cd2WF/HOUYDWArjWkmrlrWok\\nNPPM+f2qyQKbgCx1gtd0frJ0gSm0VY73Bop/uXHv9bNWJHznA\nvshAGiKDCqHsIN6\\n0gLPSvyRavAmuw3w4xvUl3wX+GMFGKLGQN267MMNRiFyYrdFvHtfV/718C56vg7W\\nNHM37x+mPaRghxt81ABDqKdnd8+Ui\nf1LwA0n8HxRimi++B6pjQnFTQUPAoGBA0jI\\ntwnyTFj00/WVuUfxzbZ3ft9UXIS9AwMdY/ZgjGu2Wt1TQy+bwatIUY86j3v/d21\\nYnysXEbtu\nRX2qyoJ0QWuCsdxWRiQLo0N7172RcbzWrXv/8ykxvgJcbo5w09/B0e\\ny+xfgzHZs1W3QmMK+VgS5jL1+heKkmCc41Dq0YSRAoGAU/gphR2/z1k\nODciympzQ\\na80DR3eG1VHpxuG/08ZjkBBmLFKeIFT7HuC1o4kV820ASDysSwqfz3cRaou0e1\\nYVWh7z5Fz3bcB5oMXQ0zjyLTx043qVXA18\nFDT9Cs1S0N+fCxIfr3U+sHfZqljlJ\\n9XBewf7yzlIF6faXwsf9DQ=\n-----END PRIVATE KEY-----\n",
    "client_email": "gcr-login@naresh-342705.iam.gserviceaccount.com",
    "client_id": "116034164228610063433",
    "auth_uri": "https://accounts.google.com/o/oauth2/auth",
    "token_uri": "https://oauth2.googleapis.com/token",
    "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
    "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/gcr-login"
}
root@test:~#
```

iTerm2 Shell Edit View Session Scripts Profiles Toolbelt Window Help

ssh ssh -zsh

```
root@test:~# 
root@test:~# 
root@test:~# docker login -u _json_key -p "$(cat keyfile.json)" https://gcr.io
WARNING! Using --password via the CLI is insecure. Use --password-stdin.
WARNING! Your password will be stored unencrypted in /root/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
root@test:~# 
```

Chrome File Edit View History Bookmarks Profiles Tab Window Help

labs/hp Creatin Use IAM How to Installi How to gcloud Authen gcr-log Release VM inst

console.cloud.google.com/compute/instances?project=devops25-338512

Govt eSign PDF Downloads Imported github My Portal terraform Ansible python CKA CKS devops25

Google Cloud Platform devops25 Search Products, resources, docs (/)

Compute Engine VM instances

Virtual machines VM instances Instance templates Sole-tenant nodes Machine images TPUs Committed use discounts Migrate for Compute Eng...

Storage Disks Snapshots Marketplace Release Notes

Select a project

NEW PROJECT

RECENT STARRED ALL

Name	ID	Connect
devops25	devops25-338512	SSH
naresh	naresh-342705	SSH
test	argon-key-342705	SSH
corp	corp-342307	SSH
My First Project	zippy-chain-338512	SSH

CANCEL OPEN

