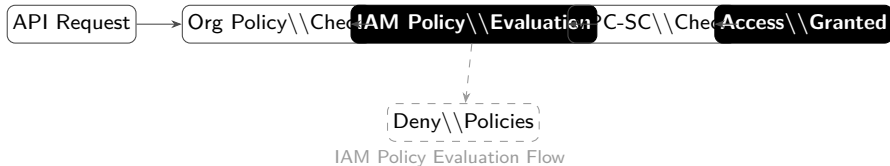




# Identity & Access Management

GCP Professional Cloud Security Engineer | IAM, Workload Identity, Org Policies & BeyondCorp

## IAM Deep Dive



|                                  |                                                                                                                                                             |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IAM deny policies</b>         | Explicit deny rules that override allow policies. Attached at org, folder, or project. Use for hard guardrails (e.g., deny deletion of specific resources). |
| <b>IAM Conditions</b>            | Conditional role bindings using CEL expressions. Conditions on: request time, resource type, resource name, IP address. Temporal access: grant until date.  |
| <b>Policy Troubleshooter</b>     | Debug why a member can or cannot access a resource. Shows effective policy from entire hierarchy.                                                           |
| <b>IAM Recommender</b>           | ML-based suggestions to reduce permissions. Analyzes 90 days of access patterns. Replace overly broad roles with scoped ones.                               |
| <b>Principal Access Boundary</b> | Restrict which resources a principal (user/SA) can access, regardless of IAM policies. Added security layer.                                                |

### Role Best Practices

- Never use basic roles (Owner/Editor/Viewer) in production — too broad
- Predefined roles cover 99% of use cases — review before creating custom
- Custom roles: use permissions from predefined roles, test in dev first
- Grant roles at the narrowest scope (resource > project > folder > org)
- Use groups instead of individual users for role assignments



Identity & Access Layers

## Service Accounts & Workload Identity

|                                     |                                                                                                                                                                     |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Service account types</b>        | Default (auto-created, over-privileged), user-managed (you create with specific roles), Google-managed (internal to Google services).                               |
| <b>SA key management</b>            | Avoid downloading keys. If required: enforce rotation (90 days max), use org policy constraints/iam.managed.disableServiceAccountKeyCreation to block key creation. |
| <b>Short-lived credentials</b>      | Generate OAuth2 tokens or signed JWTs valid for 1 hour. Use impersonation (roles/iam.serviceAccountTokenCreator) instead of keys.                                   |
| <b>Workload Identity (GKE)</b>      | Map K8s ServiceAccount to GCP ServiceAccount. Pod authenticates as GCP SA without keys. Required for secure GKE workloads.                                          |
| <b>Workload Identity Federation</b> | External identities (AWS IAM, Azure AD, OIDC, SAML) get GCP SA tokens. No key exchange. Attribute mapping and conditions.                                           |
| <b>Service Account Insights</b>     | Identifies unused service accounts and keys. Shows last authentication time. Recommends cleanup.                                                                    |

- One SA per application/microservice — never share SAs across services

- Disable or delete unused SAs — they are attack surface
- Use SA impersonation chain: user > SA-A > SA-B for delegated access

Workload Identity security

SA key convenience

Impersonation security

WIF flexibility

●●●●●

●●●●●

●●●●●

●●●●●

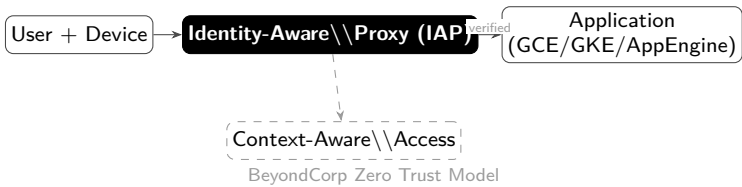
Organization Policies & Resource Hierarchy

Organization Policy Service enforces constraints across the resource hierarchy. Constraints are boolean (allow/deny) or list-based (allowed/denied values). Custom constraints use CEL expressions for flexible rules.

| Constraint                           | Purpose                                        |
|--------------------------------------|------------------------------------------------|
| iam.disableServiceAccountKeyCreation | Block SA key downloads org-wide                |
| compute.vmExternallpAccess           | Control which VMs can have public IPs          |
| compute.restrictVpcPeering           | Limit VPC peering targets                      |
| gcp.resourceLocations                | Restrict regions for data residency            |
| iam.allowedPolicyMemberDomains       | Limit IAM to specific domains only             |
| storage.uniformBucketLevelAccess     | Force uniform bucket access                    |
| compute.requireShieldedVm            | Enforce Shielded VM features                   |
| compute.trustedImageProjects         | Restrict boot disk images to approved projects |

|                               |                                                                                                                                        |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Custom org policy constraints | Write CEL expressions for rules not covered by built-in constraints. E.g., enforce labels, restrict machine types, require encryption. |
| Tag-based policies            | Apply org policies conditionally based on resource tags. Different rules for dev vs prod tagged resources.                             |
| Dry-run                       | Test org policy changes by simulating enforcement. View would-be violations before enabling.                                           |

BeyondCorp & Zero Trust



|                            |                                                                                                                                       |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Identity-Aware Proxy (IAP) | Verify user identity and context before granting access to apps/VMs. Replaces VPN. Supports HTTPS and TCP forwarding (SSH, RDP).      |
| Context-Aware Access       | Access levels based on: identity, IP/network, device security posture, location, time. Combine with Cloud Identity device management. |
| Access Context Manager     | Define access levels used by IAP and VPC-SC. Conditions: IP ranges, device policy (OS version, encryption, screen lock), region.      |
| Endpoint Verification      | Chrome extension collecting device signals: OS, encryption, screen lock, password status. Feeds into Access Context Manager.          |
| Certificate-Based Access   | Require mTLS certificates on devices. Stronger device identity than Endpoint Verification alone.                                      |

- Zero trust principle: never trust, always verify. Access is per-request, not per-network
- IAP + VPC-SC = defense in depth: identity-based + perimeter-based protection
- IAP TCP forwarding replaces VPN for SSH/RDP to VMs: `gcloud compute ssh --tunnel-through-iap`

Cloud Identity & Directory

|                                    |                                                                                                                                          |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Cloud Identity                     | Identity as a Service. Manage users, groups, devices. Free tier available. Links to GCP org. Federation with external IdP via SAML/OIDC. |
| Google Workspace                   | Superset of Cloud Identity with productivity tools. Same identity management for GCP.                                                    |
| SSO with external IdP              | SAML 2.0 federation with Active Directory, Okta, Azure AD. Google as SP, external IdP as identity source.                                |
| GCDS (Google Cloud Directory Sync) | One-way sync from Active Directory/LDAP to Cloud Identity. Syncs users, groups, OUs. Does not sync passwords.                            |
| Password Sync                      | Google Password Sync tool for AD. Syncs password changes from AD to Cloud Identity in real-time.                                         |
| MFA/2SV                            | Enforce 2-step verification org-wide. Support: security keys (FIDO2), phone prompts, TOTP. Mandate security keys for admins.             |

- Step 1 Cloud Identity Setup
- Step 2 SSO Federation
- Step 3 IAM Policy Config
- Step 4 MFA Enforcement
- Step 5 Continuous Monitoring

Identity Security Rollout

## Zero Trust

BeyondCorp security model

Access based on identity + device trust, not network location

### Official resources

#### ⚠ Check the current exam guide

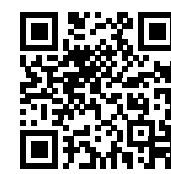
Google Cloud is updating its exams to the products announced at Google Cloud Next '26 (Gemini Enterprise Agent Platform, the data and analytics stack), per the certification hub checked 2026-10-05: read the current exam guide before these sheets.



Professional Cloud Security Engineer exam...  
[services.google...english.pdf](#)  
domains and topics



Professional Cloud Security Engineer...  
[cloud.google...y-engineer](#)  
format, price, sample questions link, renewal



Professional Cloud Security Engineer...  
[skills.google/paths/15](#)  
Google Skills (ex Cloud Skills Boost)



gcloud CLI cheat sheet  
[cloud.google...cheatsheet](#)  
the commands on one page



IAM documentation  
[cloud.google.com/iam/docs](#)



Security Command Center  
[cloud.google...enter/docs](#)



Cloud KMS documentation  
[cloud.google.com/kms/docs](#)



VPC Service Controls  
[cloud.google...trols/docs](#)