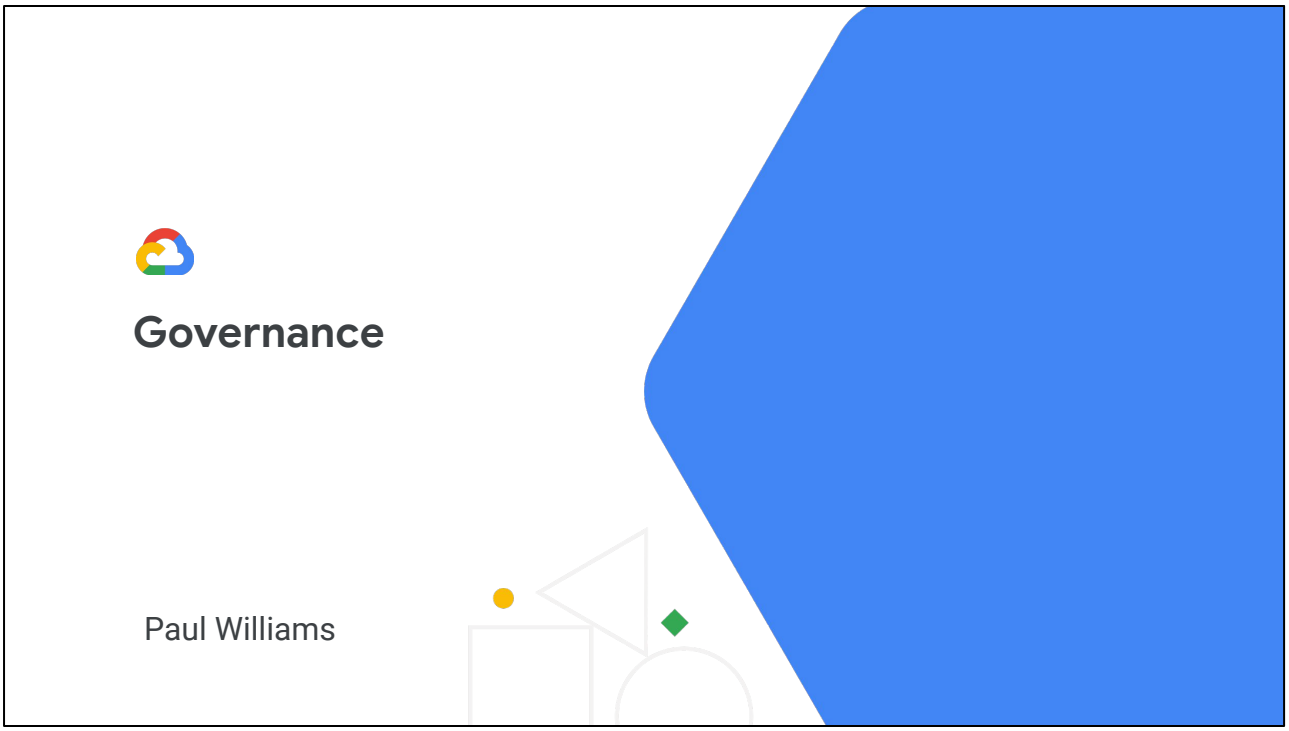


Welcome to the Governance module.

Learn how to...

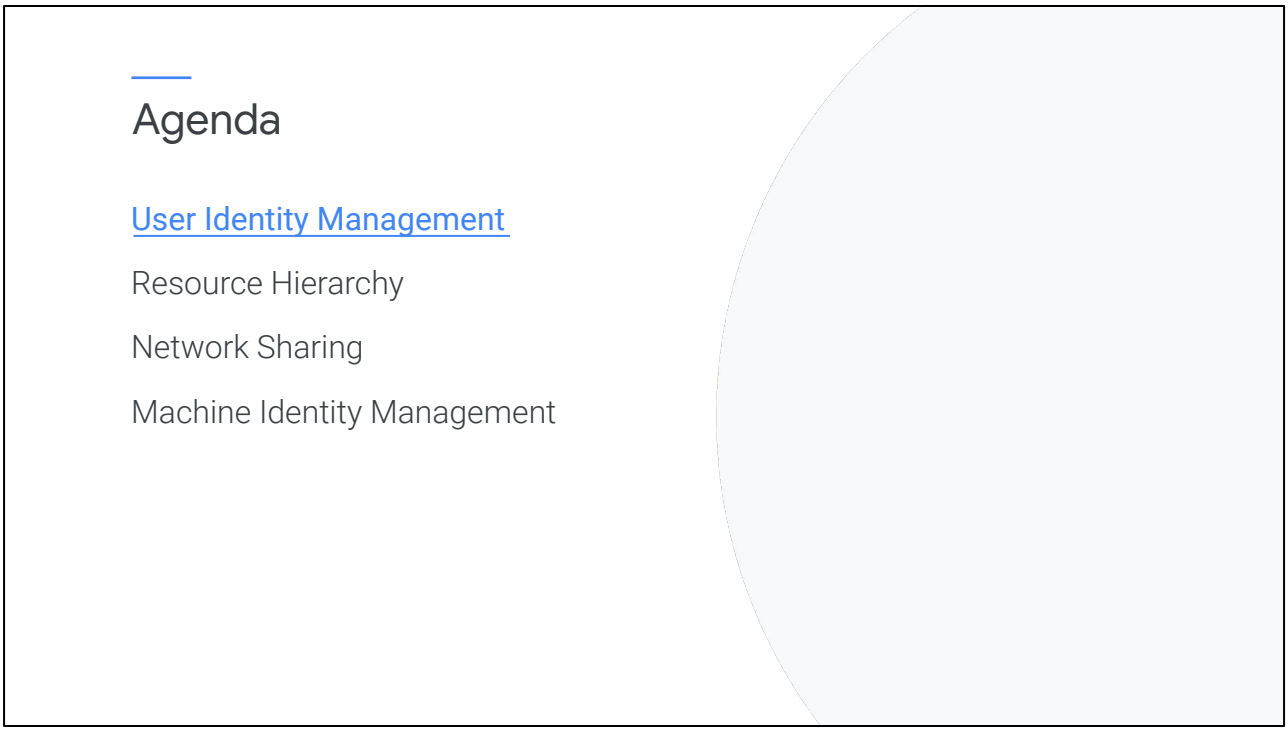
Manage and sync user accounts

Create a resource hierarchy

Centrally manage and share a network

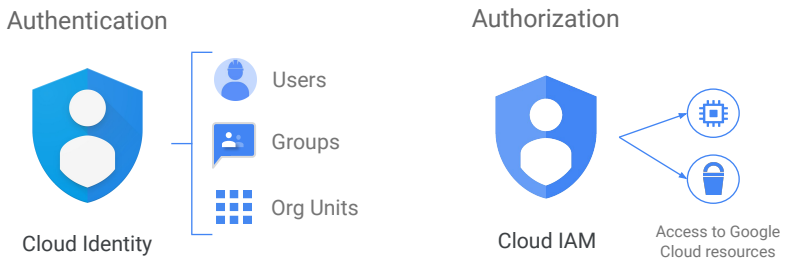
Manage identity provider across environments

In this module, you will learn how to create and manage user identities in the cloud using Cloud Identity. You will also learn how to sync your current users and groups from your on-premises environment to the cloud using an automation tool. In addition, you will learn best practices on how to structure your resource hierarchy as your cloud footprint grows in size. You will then learn how to centrally manage a single network across multiple projects, known as Shared VPC. Lastly, you will learn how to manage an identity provider across environments.



In this video you will learn how to create a Cloud Identity account, manage the user accounts lifecycle, and sync users from your on-premises environment to the cloud.

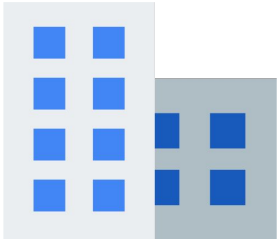
Controlling access



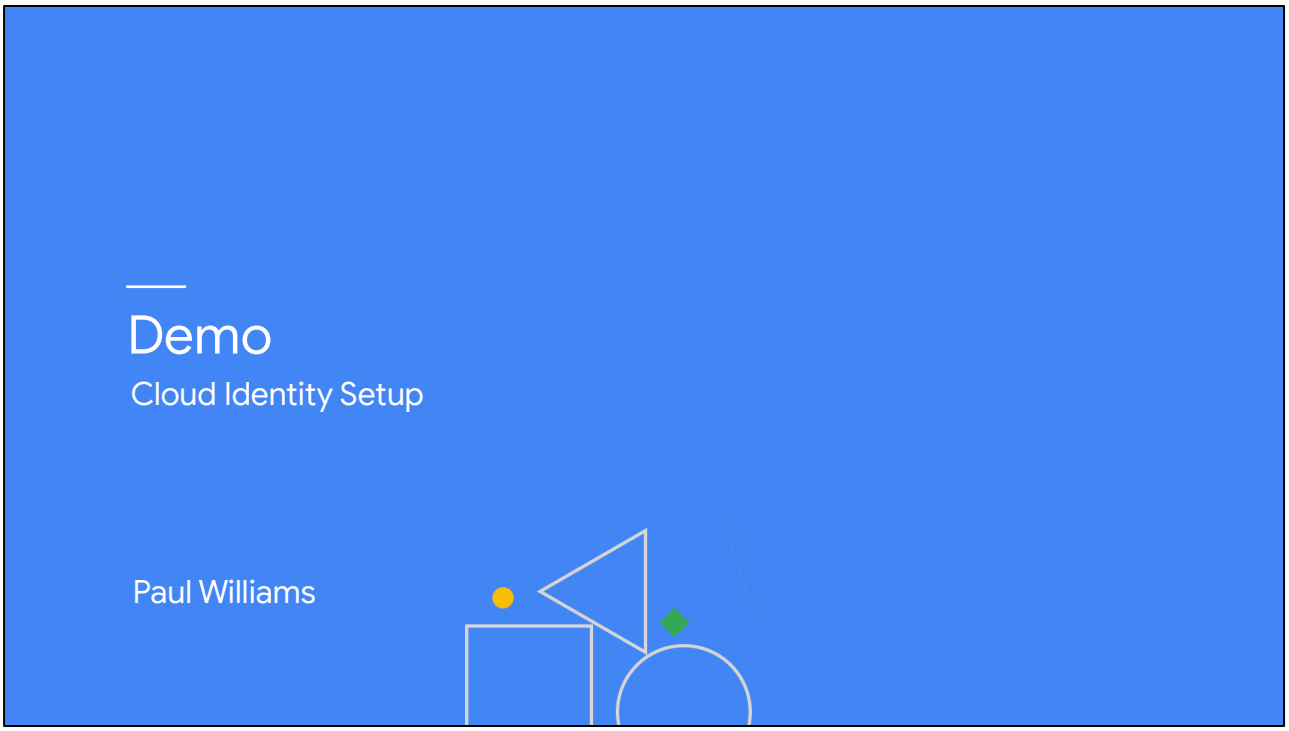
In Module 3 we introduced Cloud IAM in detail and we touched on Cloud Identity. Cloud Identity handles authentication, which handles identifying a user, typically through a private form of verification like a password and a key. Cloud Identity is managed outside of Google Cloud in admin.google.com.

IAM, in contrast, is responsible for Authorization, which is a set of permissions that a user is allocated post authentication. Permissions are managed directly inside the Cloud Console at console.cloud.google.com under the IAM section.

The Organization node



The Organization resource represents an organization (for example, a company) and is the root node in the Google Cloud resource hierarchy. The Organization resource is the hierarchical ancestor of project resources and Folders. The Cloud IAM access control policies applied on the Organization resource apply throughout the hierarchy on all resources in the organization.



[Presenter]
In this demo, you will learn how to set up cloud identity and the organization node.

[Demo - screencast]

[Presenter]
Now that you have learned how to set up cloud identity, you will learn how to manage your cloud users lifecycle in the next video.

User provisioning options

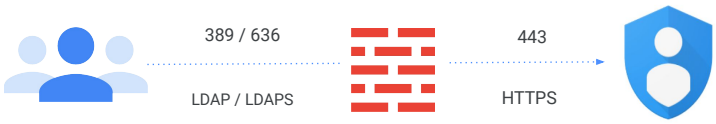
	Method	Effort	Staff involved	Notes
	Manual provisioning	High	Cloud Identity admin	Easiest method, but not scalable
	CSV upload via Admin Console	Medium	Cloud Identity admin	More flexibility, but not scalable
Best Practice	**Google Cloud Directory Sync**	**Medium**	**LDAP Admin**	**Integrates with LDAP, scalable, requires no programming**
	Third party tools (Okta, Ping, ...)	Medium	LDAP admin	Scalable, may incur additional cost
	Admin SDK Directory API	High	LDAP Admin Development staff	Scalable, flexible, requires in-depth programming

When you migrate to Google Cloud, there are many options to choose from for managing the users lifecycle.

You can start by manually creating a few users in your cloud environment, but that can be tedious, error-prone, and not scalable. You can also import a CSV file into Cloud Identity, but after that operation, the users lifecycle does not sync with your source environment, meaning that if a user changes a password or leaves the company, their user profile in Cloud Identity will not be affected.

There is a way to create a trust relationship between your directory services and Cloud Identity called Google Cloud Directory Sync, which is the recommended approach.

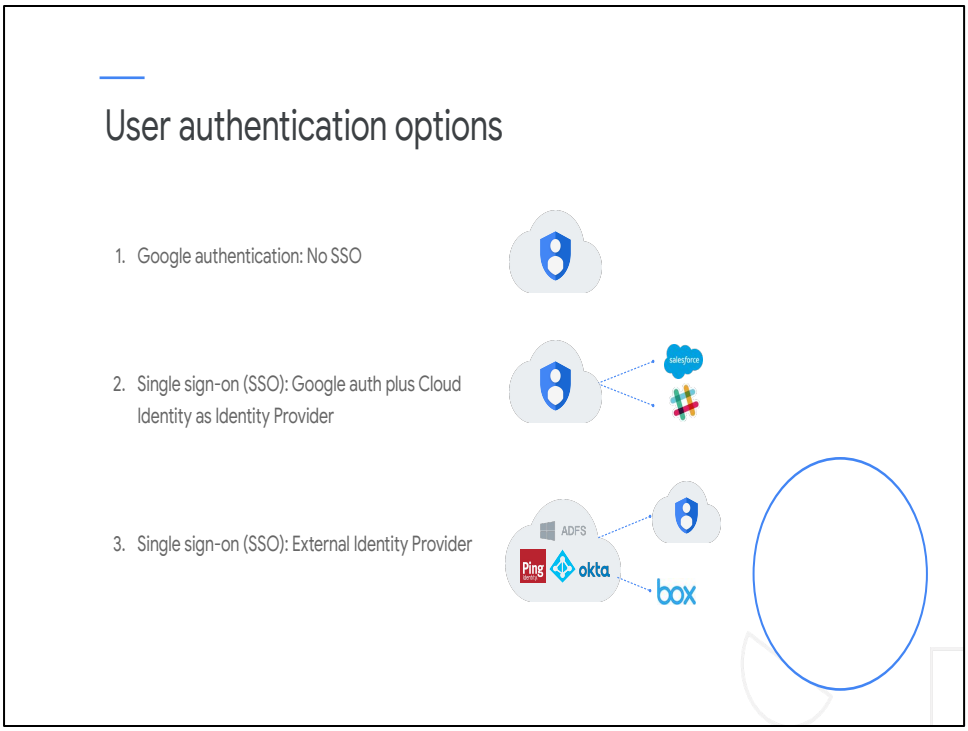
Google Cloud Directory Sync (GCDS)



- One-way synchronization
- Only synchronizes deltas for fastest possible provisioning
- Configure which users accounts to sync

Google Cloud Directory Sync is a Google-provided connector tool that integrates with most enterprise LDAP management systems and synchronizes identities on a schedule. It runs in a dedicated machine on-premises and communicates with Cloud Identity via well-established protocols.

Google Cloud Directory Sync is a one-way synchronization tool, which keeps your on-premises Active Directory as the single point of truth. It synchronizes the users and groups in order for them to use cloud environment. This gives you granular control over corporate users that you want to grant direct Google Cloud resource access to.



Google Cloud Directory Sync only syncs objects like users and groups, without their passwords. Once a user is synced to Cloud Identity, it needs to also have a password or a means of authentication. There are a few options to choose from.

The first option is to create a password for the users in Cloud Identity's Admin Console. The users will authenticate against Cloud Identity, and their cloud password doesn't sync back to Active Directory.

A recommended alternative is to set up SSO using SAML2. Here, there are 2 options: the first is to use Cloud Identity, which is a managed, highly available service, as your main identity provider.

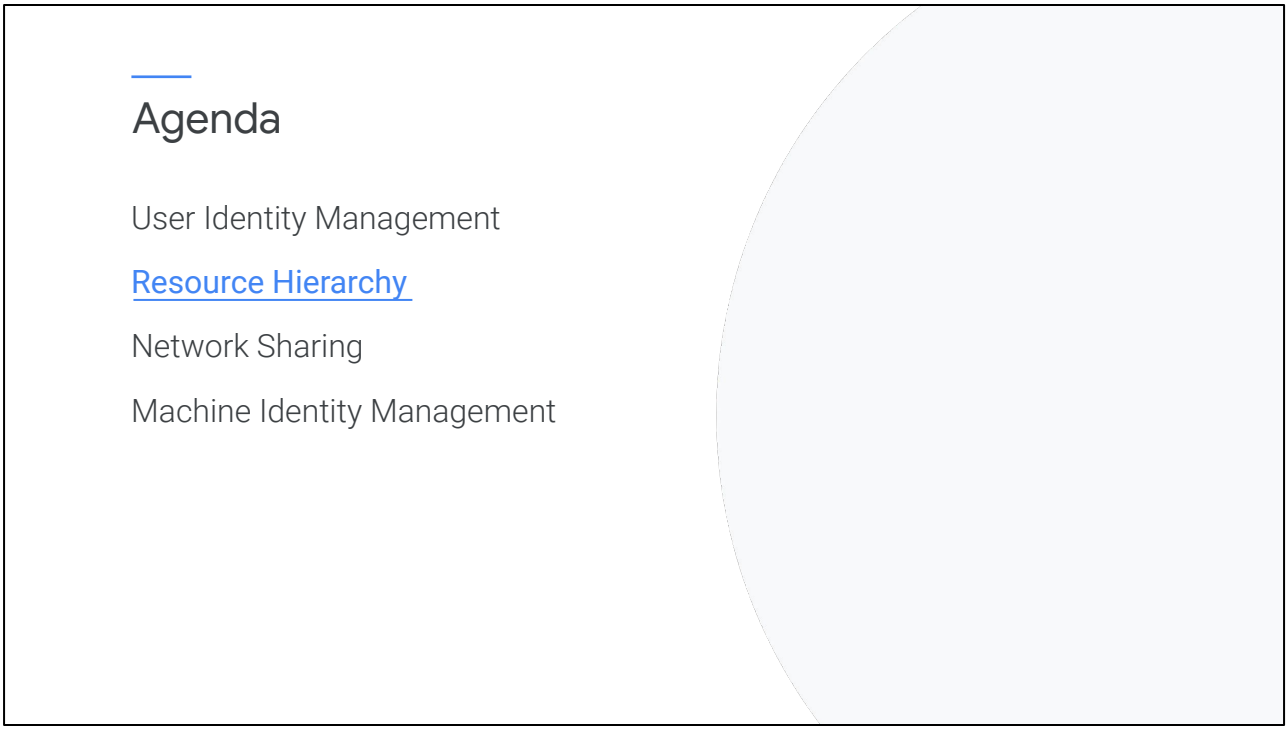
Alternatively, you can federate the authentication of your synced cloud users back to on-premises. When you configure SSO, the user will be authenticated directly against your on-premises identity provider, which eliminates the need to manually manage passwords in the cloud. That also means that your on-premises identity provider must be highly available so that users will be able to access cloud resources.

G Suite Password Sync (GSPS)

- Synchronizes user passwords from Active Directory to Cloud Identity as they are changed (in real time).
- GSPS intercepts the raw password and applies a salted SHA512 hash.
- Encrypted via TLS, the salted hash is sent to Cloud Identity using the Directory API.

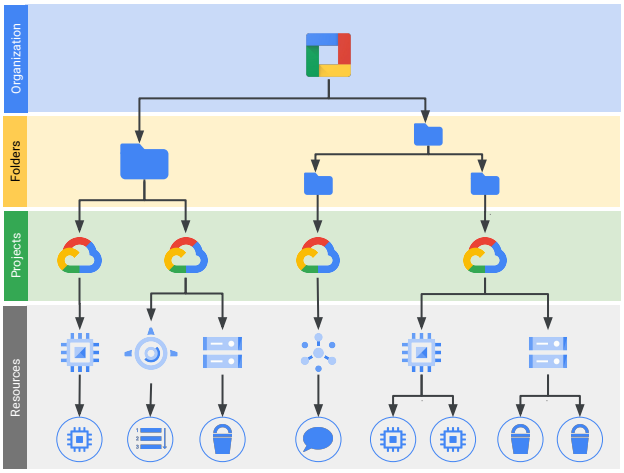
If you are do not use SSO and would like to sign in to Google Cloud with the same passwords you use on-premises, G Suite Password Sync will synchronize user passwords from Active Directory to Cloud Identity in real time.

GSPS intercepts the raw passwords and applies a salted SHA512 hash before they are transmitted over an encrypted TLS tunnel, and only the salted version is sent to Cloud Identity using native APIs.



In this video you will learn about the resource hierarchy, and explore different methods to organise your resources.

Organization hierarchy



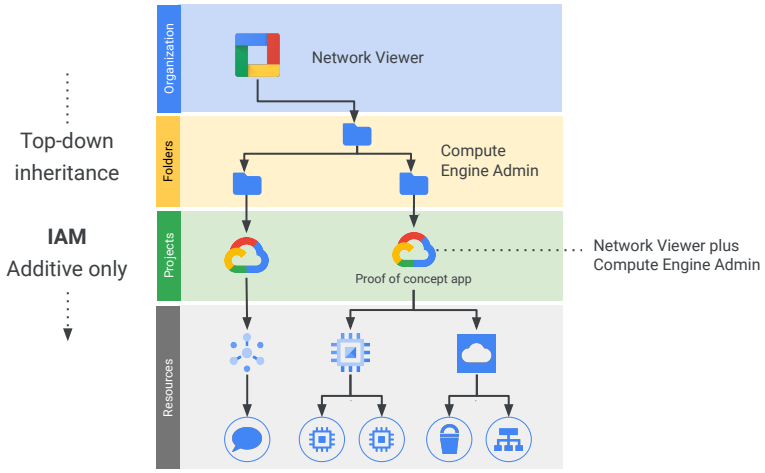
Top-down inheritance

IAM
Additive only

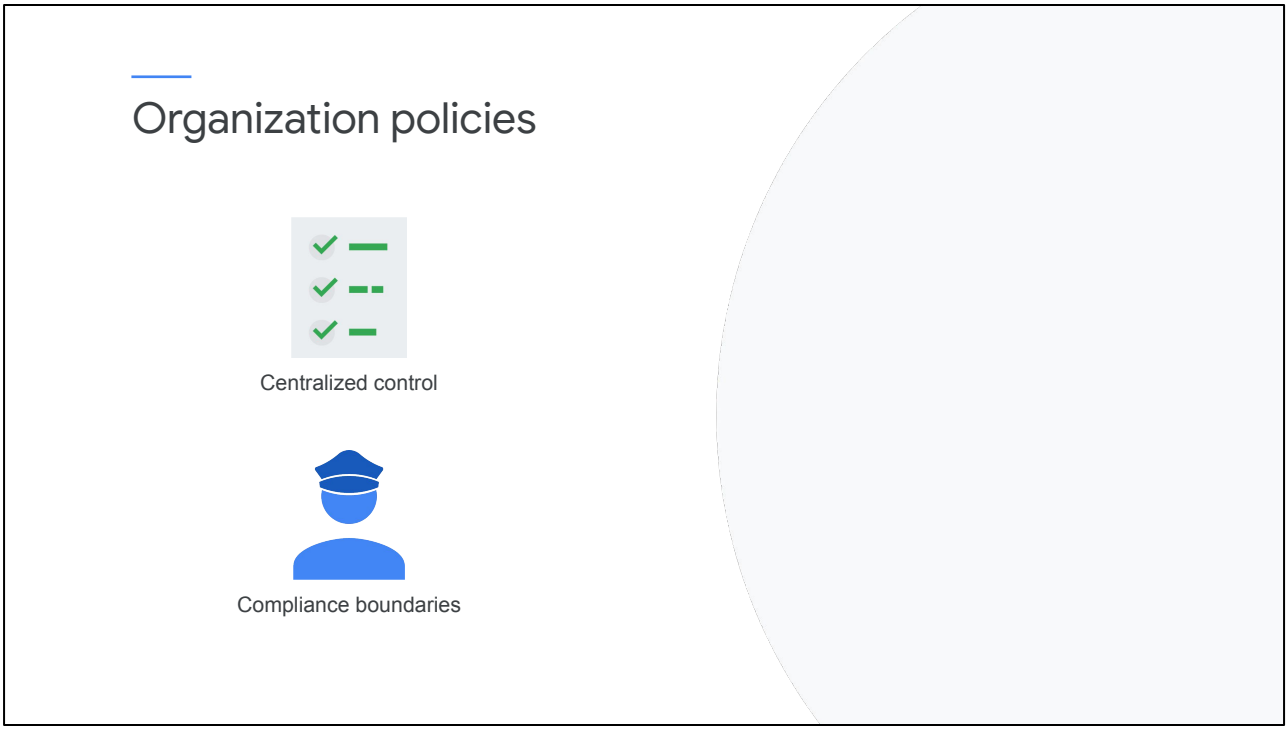
Org Policy
Exceptions supported

As the scale of your Cloud footprint increases, the need to organize your resources into folders and projects increases for billing, administrative, and security reasons. Segregating your resources in a way that makes sense for your organization will help you put policies in place, separate administrative boundaries, and have finer-grained control over consumption. The role of a well-defined resource hierarchy is to give you the flexibility and convenience to distribute permissions in a straightforward manner, while maintaining important security principles like granting the least privilege to your staff to minimize accidental disruption.

Organization hierarchy



Remember that permissions trickle down from top to bottom and it'll always be a union of permissions. For example, if you want to give your Networks Operations Control group Network View access at the organization level, that permission with trickle down to all VPC networks in the resource hierarchy, and you won't be able to remove that permission on a particular project below in the hierarchy tree. Since IAM permissions are additive, you can add permissions to that specific group on a specific project, for example if they need to create a virtual machine to test a new appliance. The union of the permissions means that in that particular project, they will be granted both the inherited Network Viewer role and a Compute Engine Admin. This concept ensures that you give your staff the least privilege to do their job effectively, which helps minimize accidental or malicious potential.



The only exception to the additive permissions rule is organization policies. The Organization Policy Service gives you centralized and programmatic control over your organization's cloud resources, for instance, you can restrict where resources can be provisioned to only one country. It is applied at the root of the resource hierarchy and restricts access to resources across all descendants. The constraints you can impose define and establish guardrails for your development teams to stay within compliance boundaries and help project owners and their teams move quickly without fear of breaking compliance.

Organization policies

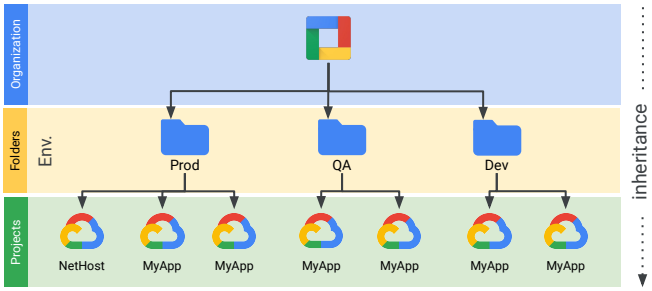
Services	Constraints	Description	Useful for
Compute Engine	High	Cloud Identity admin	Ensuring **minimal external surface**. VMs should normally get internal IPs only.
	Skip default network creation	Skips the creation of the default network and related resources during project creation.	Enforcing usage of **centrally managed and secured VPC networks.**
Cloud IAM	Domain restricted sharing (Beta)	Defines the set of members (domains) that can be added to Cloud IAM policies.	Protect against **malicious acts and human mistakes** by **ensuring access** only to users in **whitelisted domains.**
Google Cloud	Resource location restriction (Beta)	Defines the set of locations where location-based Google Cloud resources can be created.	**Compliance with regulations** that restrict resources location.

Another good example is to restrict the use of external IP addresses for virtual machines or disable the use of default networks that are created with each new project, forcing the use of a centrally controlled network like a shared VCP, which will be introduced later in this module. There are many more to choose from, so we added a link to this video with the full list.

Environment-oriented hierarchy

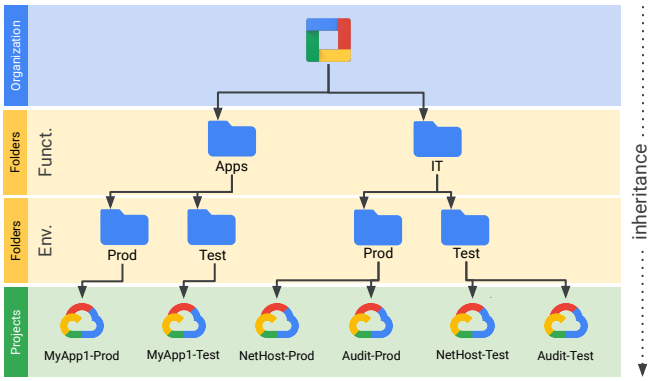
As your resource hierarchy grows, more and more projects and folders accumulate. Here are a few common resource hierarchies we recommend using. When you start using Google Cloud, you may start with a single project, and as more teams or products areas start using cloud resources, the number of projects you own will grow.

Environment-oriented hierarchy



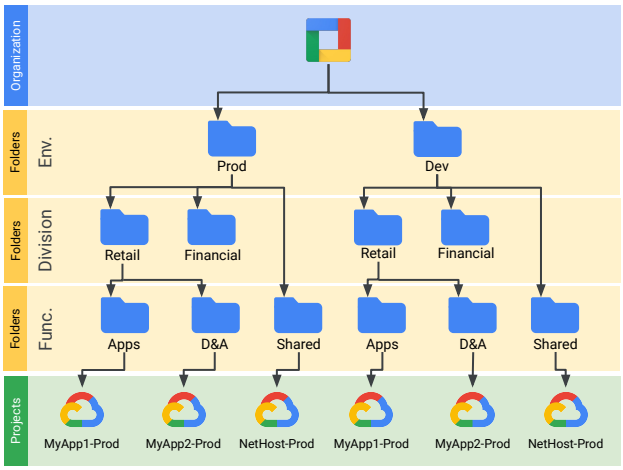
We recommend using folders to organize these resources, which help simplify access and permissions patterns. For example, in this hierarchy, an organization decided to segregate their resources based on the environment. A folder for production, QA and dev. Some engineers in the company will have full control over the Dev folder and therefore all the project and resources under it, while having view-only access to Production.

Example: Function-oriented hierarchy

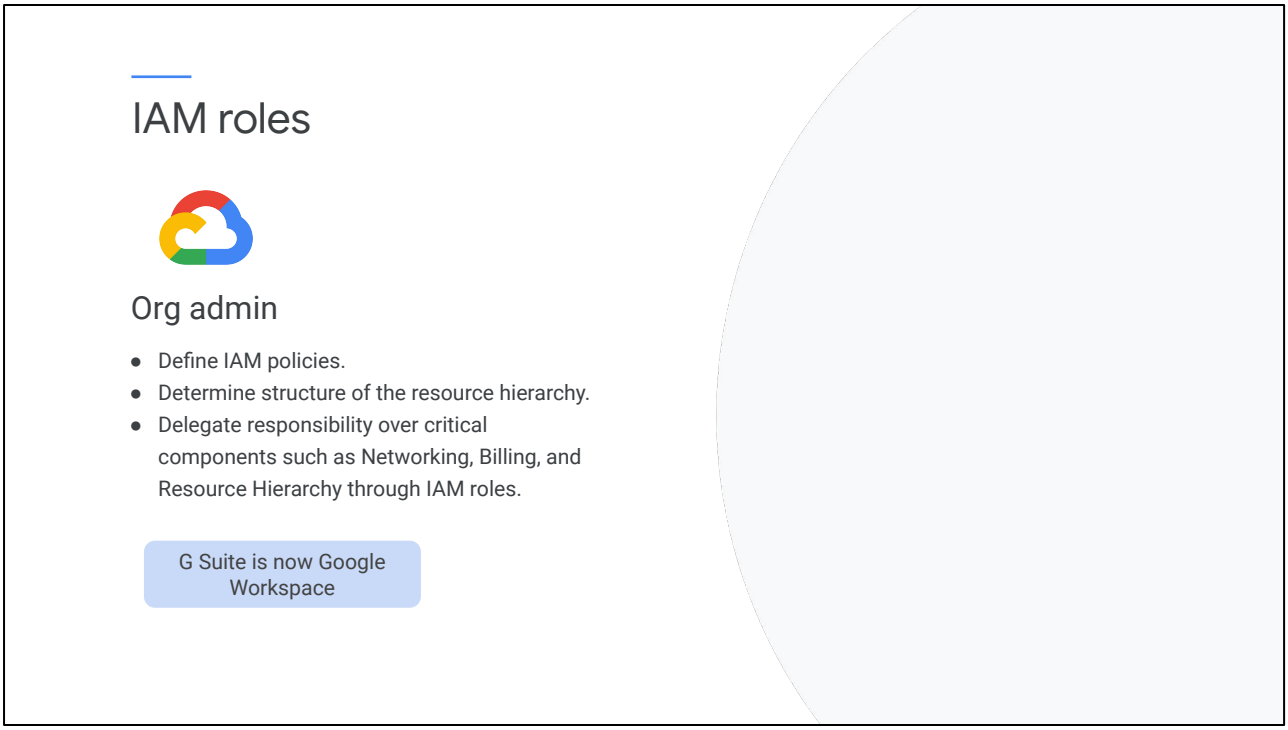


A more complex example is a function-oriented hierarchy, which has 2 layers of folders: one for the environment and one for the function of the business. That makes access and permissions more granular. As your cloud environment grows and you change your resource hierarchy, it's important to keep in mind that permissions are inherited.

Example: Environment-oriented hierarchy



Another common pattern is segregating resources based on the operating environment. This is **beneficial** from a **security standpoint** because it allows **centrally applying policies** on all projects of a **specific operating environment**. For example, disabling external IPs on all VMs in production.

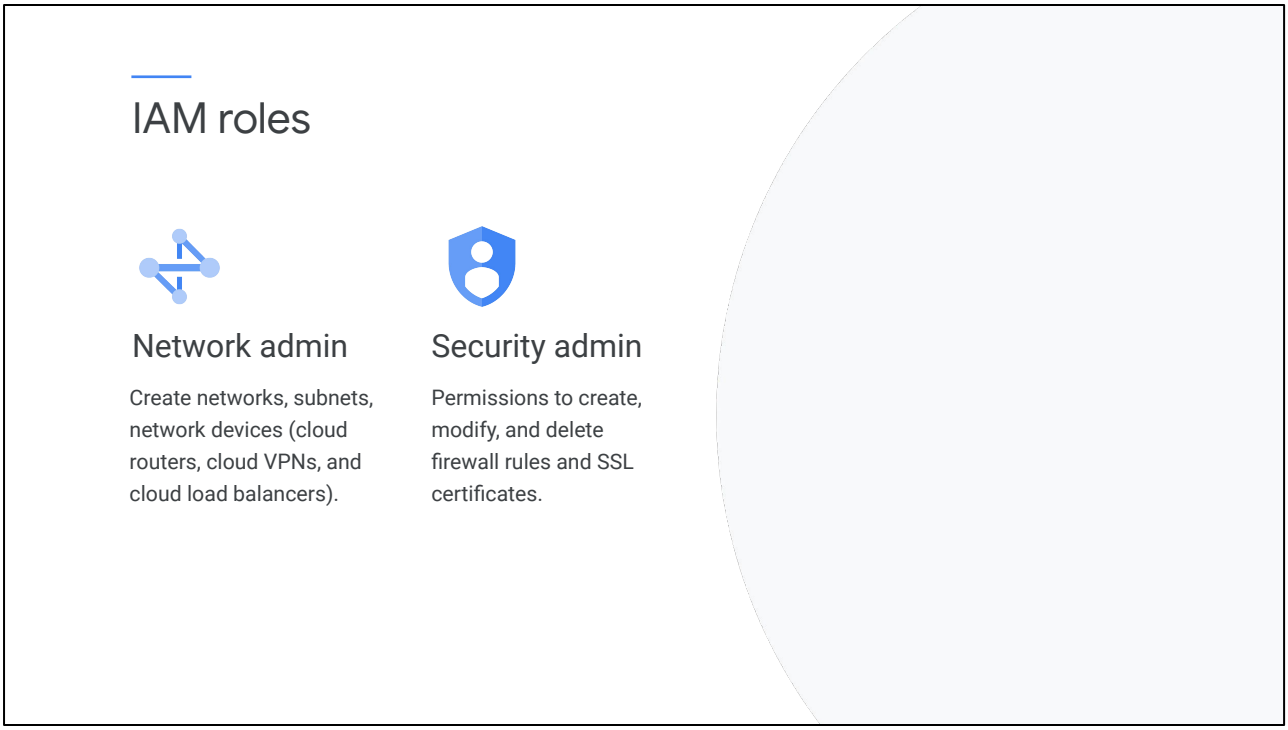


When you start creating your cloud environment, you need to establish who in your company can have permission to create, access, modify, and destroy cloud resources.

There are a few key IAM roles that we recommend paying close attention to.

The organization Admin role is responsible for defining IAM policies, determining the resource hierarchy, and delegating responsibilities over critical components.

It's worth mentioning that you only get an Organization node, folder structure, and an Organization Admin if you import your domain to Cloud Identity or Workspace. Having an Organization in Google Cloud is not mandatory for virtual machine migration: however it is recommended for scalability reasons.

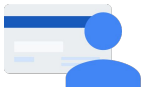


The network admin role equips your network engineer with permissions to create, modify and delete network topologies and resources like whole VPCs, subnets, and network resources like Cloud Router, Load Balancers, etc. Because firewall and SSL certificates are sensitive and security-related, the Network Admin only has read access to these resources.

The Security Admin role contains permissions to create, modify, and delete firewall rules and SSL certificates.

For example, if your company has a security team that manages firewalls and SSL certificates and a networking team that manages the rest of the networking resources, then grant the networking team's group the Network Admin role and the security team the Security Admin role. You can also grant a single entity both permissions.

IAM roles



Billing Account Admin

- Set up a billing account.
- Monitor usage.

This role is an owner role for a billing account. Use it to manage payment instruments, configure billing exports, view cost information, link and unlink projects, and manage other user roles on the billing account.

Agenda

User Identity Management

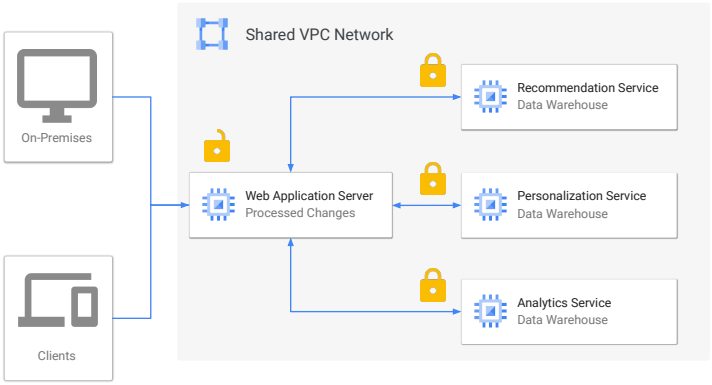
Resource Hierarchy

Network Sharing

Machine Identity Management

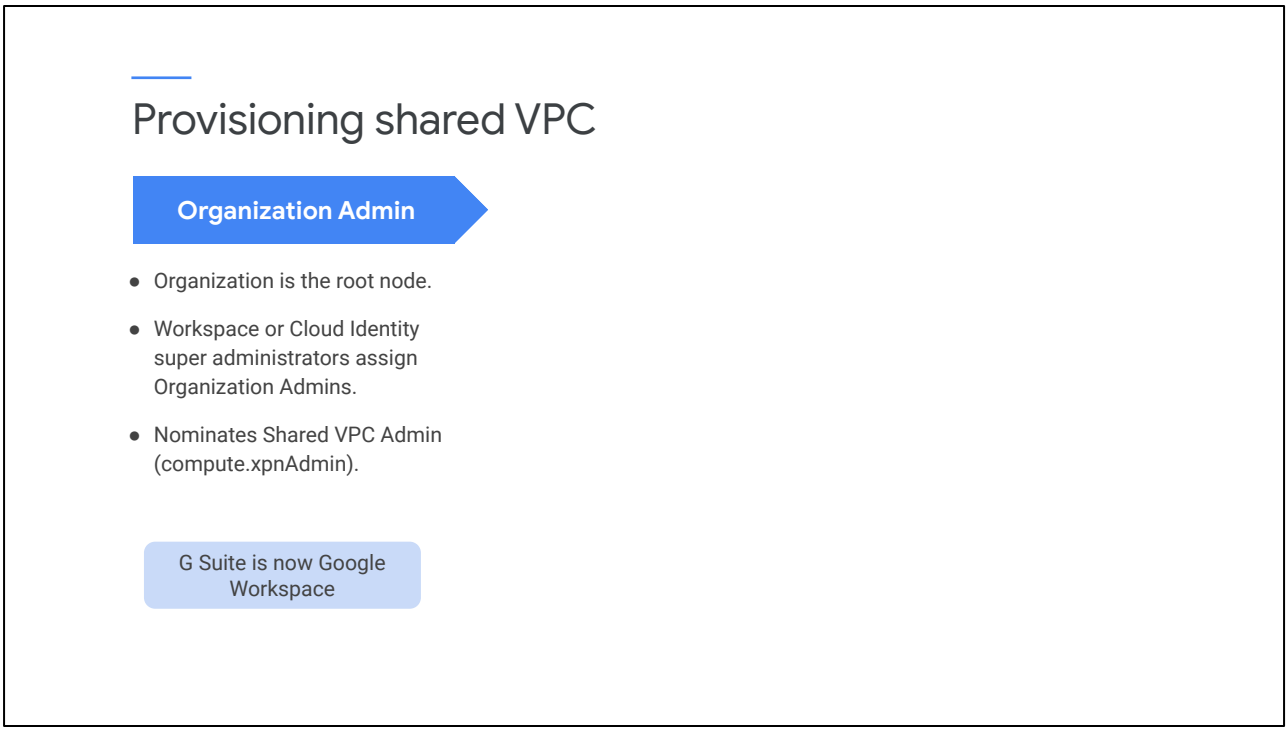
In this video you will learn how utilise the Shared VPC network, which provides a single network that is shared across different projects in your organization.

Shared VPC



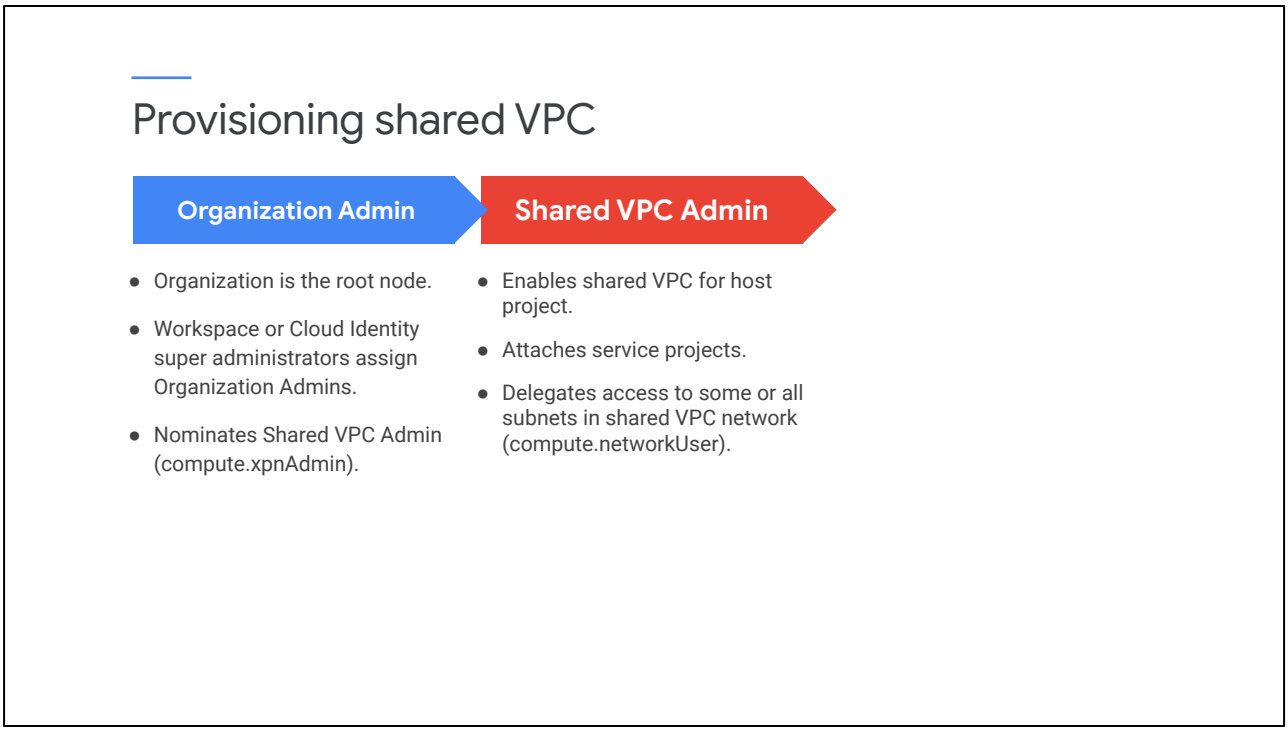
As a reminder, a standard VPC network is confined to a single project. That means that when 2 machines from 2 different projects want to communicate with each other, they will have to use their external IP addresses. Shared VPC allows an organization to connect resources from multiple projects to a common VPC network. This allows the resources to communicate with each other securely and efficiently using internal IPs from that network. The biggest advantage to such a design is that it allows virtual machines to be in different projects, governed by different parts of the organization, but communicating over one centrally managed VPC.

For example, in this diagram there is one network that belongs to the Web Application Server's project. This network is shared with three other projects, namely the Recommendation Service, the Personalization Service, and the Analytics Service. Each of those service projects has instances that are in the same network as the Web Application Server, allowing for private communication to that server using internal IP addresses. The Web Application Server communicates with clients and on-premises using the server's external IP address. The backend services, in contrast, cannot be reached externally because they only communicate using internal IP addresses. When you use shared VPC, you designate a project as a host project and attach one or more other service projects to it. In this case, the Web Application Server's project is the host project, and the three other projects are the service projects. The overall VPC network is called the shared VPC network.



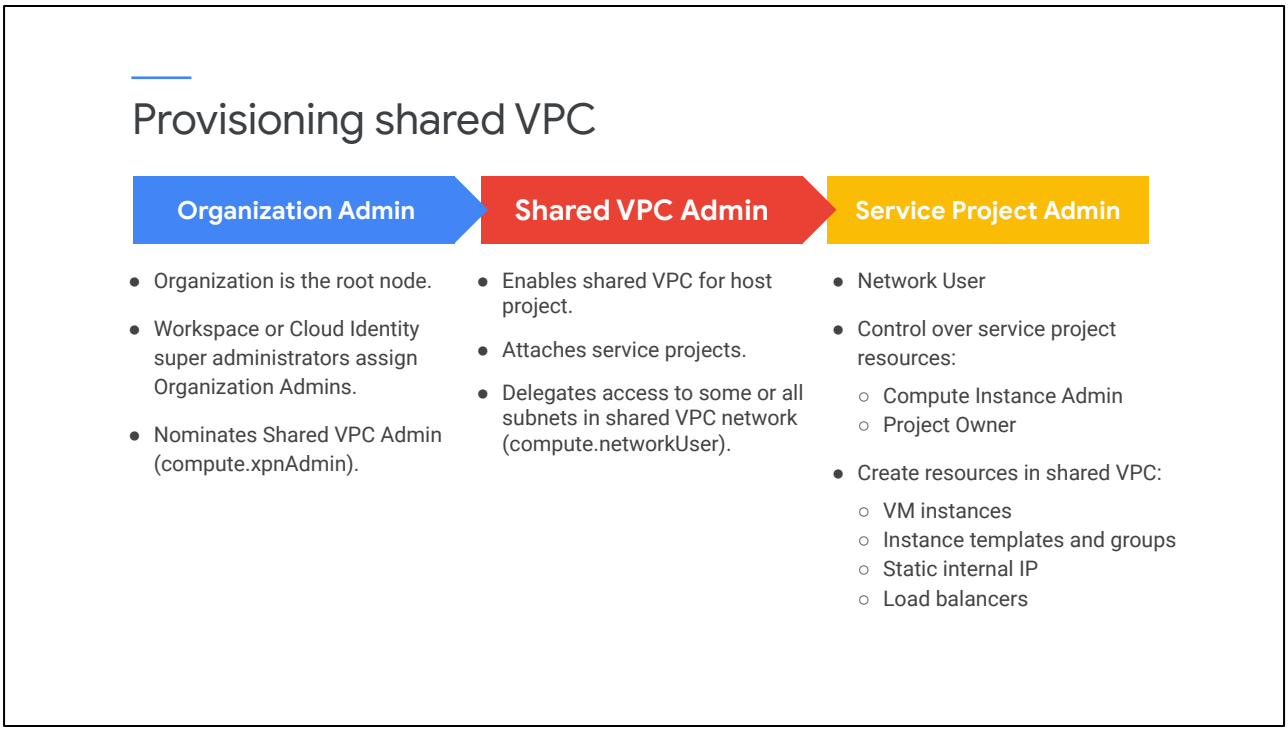
Shared VPC makes use of Cloud IAM roles for delegated administration. Let me walk through how to provision shared VPC by focusing on the required administrative roles.

The first required role is the organization admin. The Organization resource represents an organization, for example, a company, and is the root node in the Google Cloud resource hierarchy. The Workspace or Cloud Identity super administrators are the first users who can access the organization, and they assign the organization admin role to users. The organization admin's role in provisioning shared VPC is to nominate Shared VPC Admins by granting them appropriate project creation and deletion roles, and the compute.xpnAdmin role for the organization. Note that shared VPC is also referred to as "XPN" in the API and command-line interface.



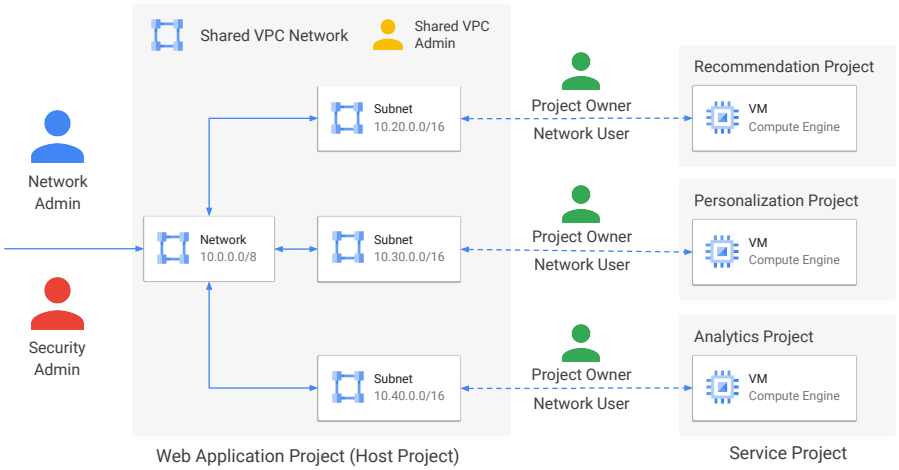
Next, the Shared VPC Admin performs various tasks necessary to set up shared VPC. This includes enabling shared VPC on the host project, attaching service projects to the host project, and delegating access to some or all of the subnets in shared VPC networks to Service Project Admins. Access is provided by granting the compute.networkUser role.

Typically, a Shared VPC Admin is also the project owner for a given host project.



Now, in addition to being Network Users, Service Project Admins also maintain ownership and control over resources defined in their service projects. The Service Project Admins must at least have the compute.instanceAdmin role to the corresponding service project. However, typically, the Service Project Admins are project owners of their service projects. This allows them to create and manage resources in the shared VPC. These resources could be VM instances, Instance templates and groups, static internal IP addresses, and load balancers.

Shared VPC

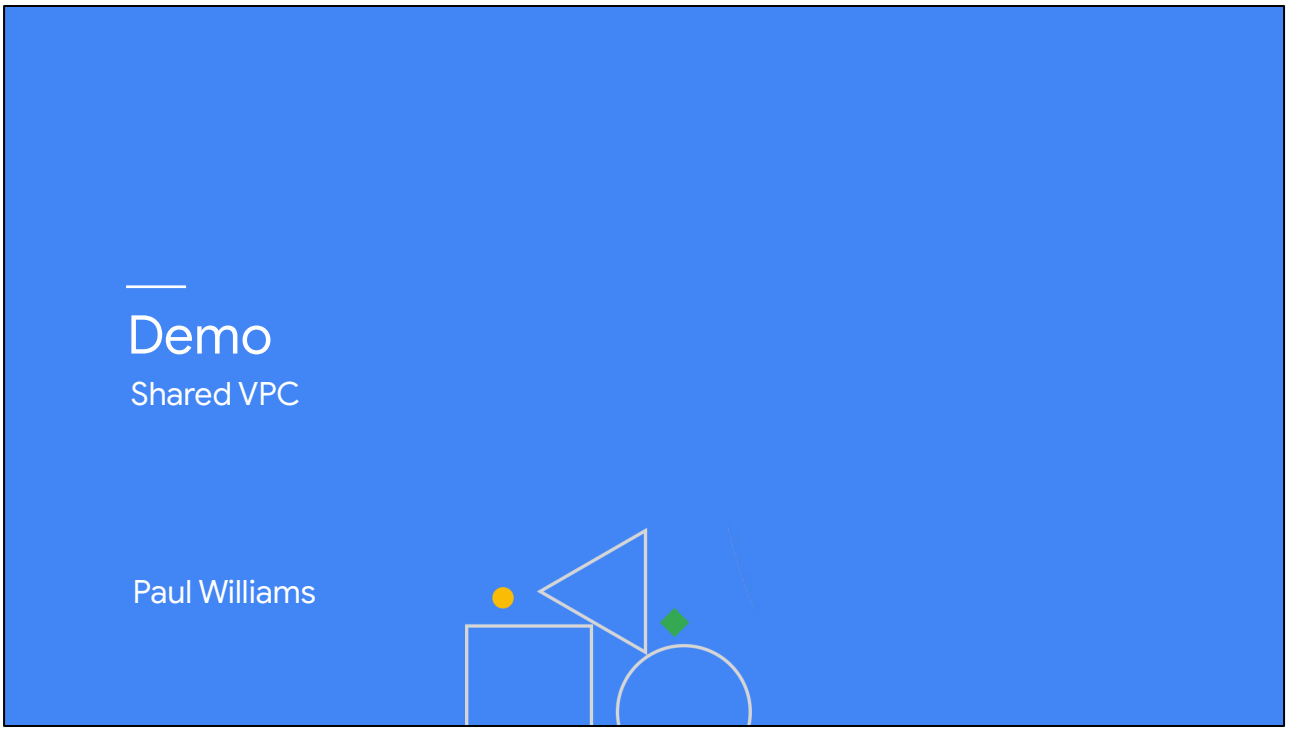


Let me come back to our original example that had one host project and 3 service projects:

In this diagram, the Shared VPC Admin, which was nominated by an organization admin, configured the Web Application Project to be a host project with subnet-level permissions. Doing so allowed the Shared VPC Admin to selectively share subnets from the VPC network.

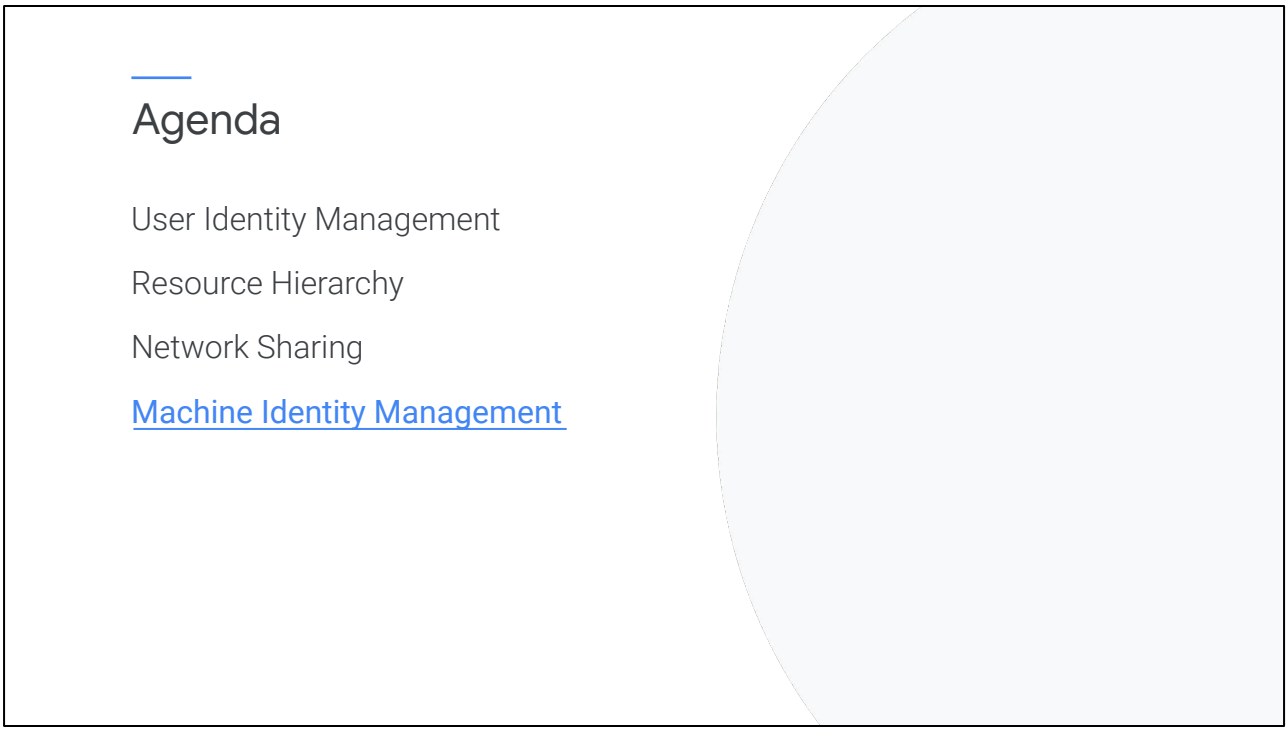
Next, the Shared VPC Admin attached the three service projects to the host project and gave each project owner the Network User role for the corresponding subnets. Each project owner then created VM instances from their service projects in the shared subnets.
By the way, billing for those VM instances is attributed to the projects where the resources are created, which are the service projects.

Shared VPC Admins have full control over the resources in the host project, including administration of the shared VPC network. They can optionally delegate the Network Admin and Security Admin roles for the host project. Overall, shared VPC is a centralized approach to multi-project networking because security and network policy occurs in a single designated VPC network.



[Presenter]
In this demo, you will learn how configure a shared vpc network topology

[Demo - screencast]
https://www.youtube.com/watch?v=4MtfyViH9t0



In this video, you will learn how to handle machine authentication against an Active Directory for machines hosted in the cloud.

Machine authentication

We introduced a way to manage the lifecycle of users. Virtual machines on-premises tend to authenticate against an Active Directory server or similar Directory Services platforms like LDAP or NIS+.

When you migrate virtual machines to Google Cloud, your virtual machines still need to authenticate against an identity provider. There are a few choices to choose from; each has its own benefits.

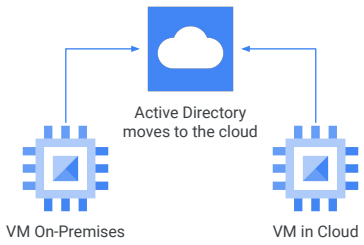
Connect back to on-premises AD

- Suitable for small cloud footprint
- Requires little to no application/VM changes
- Trust boundary for Active Directory extended to include the cloud

As you migrate your virtual machines to Google Cloud, these machines can authenticate against your Active Directory on-premises or Azure AD server. It is suitable in situations when your cloud footprint is relatively small in comparison to the source environment. The advantages of this strategy are little to no application or virtual machine changes, and it saves time because you don't have to move your identity provider. The disadvantages are that the trust boundary of your Active Directory is now extended to include your cloud environment, which needs to be hardened. You are also dependent on the interconnectivity between the two environments, whether the connection is a VPN tunnel or a physical Cloud Interconnect. If you choose this approach, make sure the DNS entry resolves correctly, and remember that only global domains are allowed.

[https://cloud.google.com/solutions/patterns-for-using-active-directory-in-a-hybrid-environment]

Migrating to Google Cloud



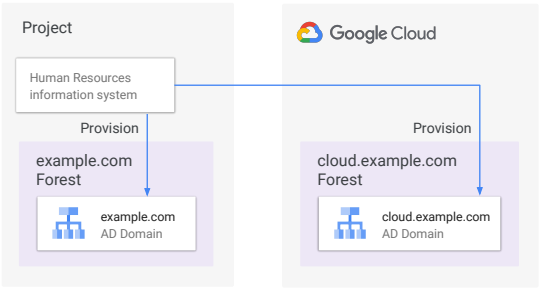
- Suitable when most or all virtual machines migrate to the cloud.
- Apps and users left on-premises need to connect to the cloud.
- Still need to maintain your own server.

If you move all or most of your workloads to the cloud, you can simply move your Active Directory server also.

The benefits of this approach is that it's usually a simple process, unless you have a high availability configuration in place, which can make it slightly more challenging. In addition, if you do have worloads that stay on-premises, these workloads need to authenticate against a remote server in your cloud environment, so latency, connectivity and configuration become a consideration.

Moving your Active Directory to the cloud can be a viable solution; however, you still need to maintain it.

Synchronized forest pattern



- Sync accounts
- Keeps a trust boundary clear between on-premises and cloud

In the synchronized forests pattern, you deploy a separate Active Directory forest to Google Cloud. You use this forest to manage any resources deployed on Google Cloud and the user accounts required to manage these resources.

Instead of creating a trust between the new forest and an existing, on-premises forest, you synchronize accounts. If you use an HRIS as the leading system to manage user accounts, you can configure the HRIS to provision user accounts in the Google Cloud-hosted Active Directory forest. Or you can use tools such as Microsoft Identity Manager to synchronize user accounts between environments.

This pattern is a good choice if you want to maintain a trust boundary between your on-premises Active Directory environment and the Google Cloud-hosted Active Directory environment—either as a defense-in-depth measure or because you trust one environment more than the other.

[https://cloud.google.com/solutions/patterns-for-using-active-directory-in-a-hybrid-environment#integration_patterns]

Managed Service for Microsoft Active Directory

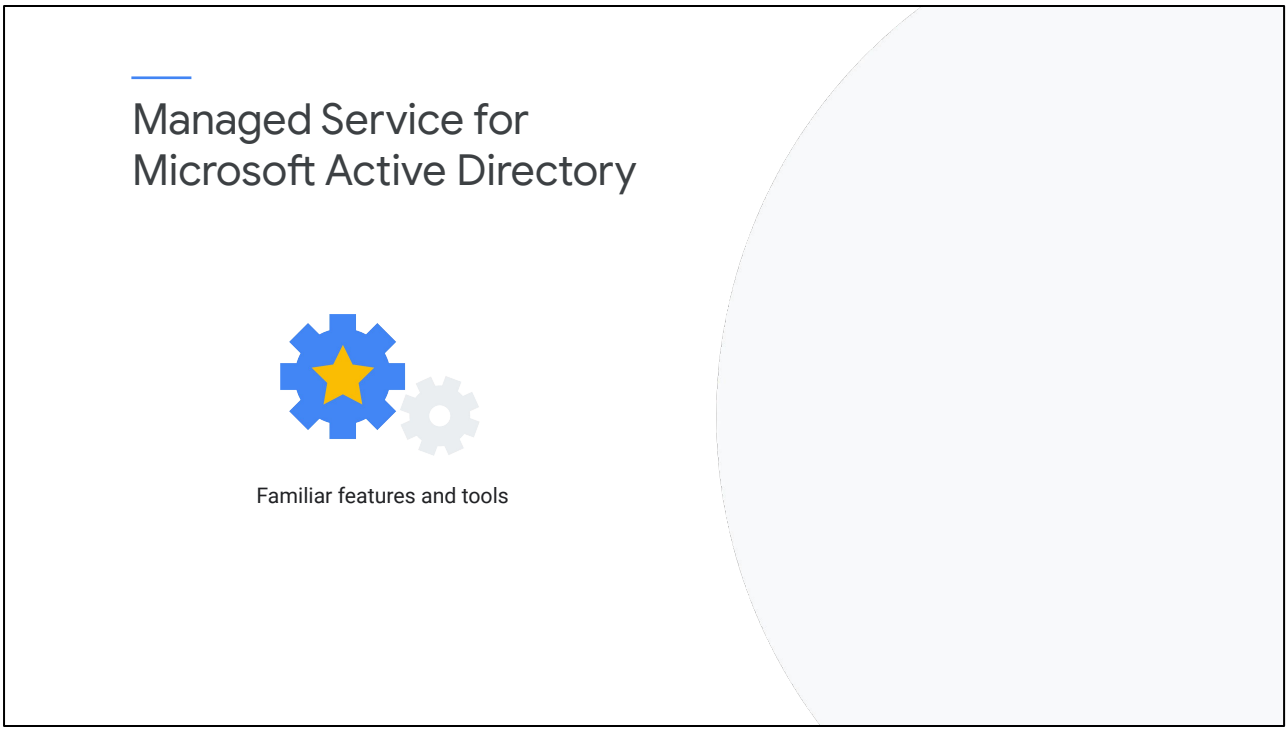
So far, we have demonstrated a few options for running Active Directory. For running Active Directory in Google Cloud, you have 2 options: manage it yourself, or use a managed service called Managed Service for Microsoft Active Directory.

Managed Service for Microsoft Active Directory (AD) is a highly available, hardened Google Cloud service running actual Microsoft AD that enables you to manage your cloud-based AD-dependent workloads, automate AD server maintenance and security configuration, and connect your on-premises AD domain to the cloud.

Managed Service for Microsoft Active Directory

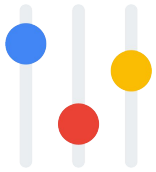
Virtually maintenance-free

Enable your IT and security teams to focus on higher-value tasks, knowing that the service is highly available, automatically patched, configured with secure defaults, and protected by appropriate network firewall rules.



In addition, there's no need to learn new tools. Your organization can still use Active Directory features, such as Group Policy, and familiar administration tools, such as Remote Server Administration Tools (RSAT), to manage the domain.

Managed Service for Microsoft Active Directory



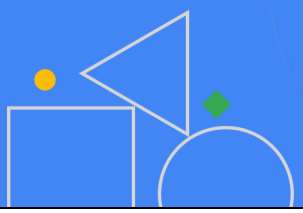
Versatile Configuration

With Managed Service for Microsoft Active Directory, you can connect your on-premises Active Directory domain to Google Cloud and create various trust relationships between your environments. You can also deploy a cloud-based standalone domain in multiple regions for your cloud-based workloads, including VMs and applications.

Demo

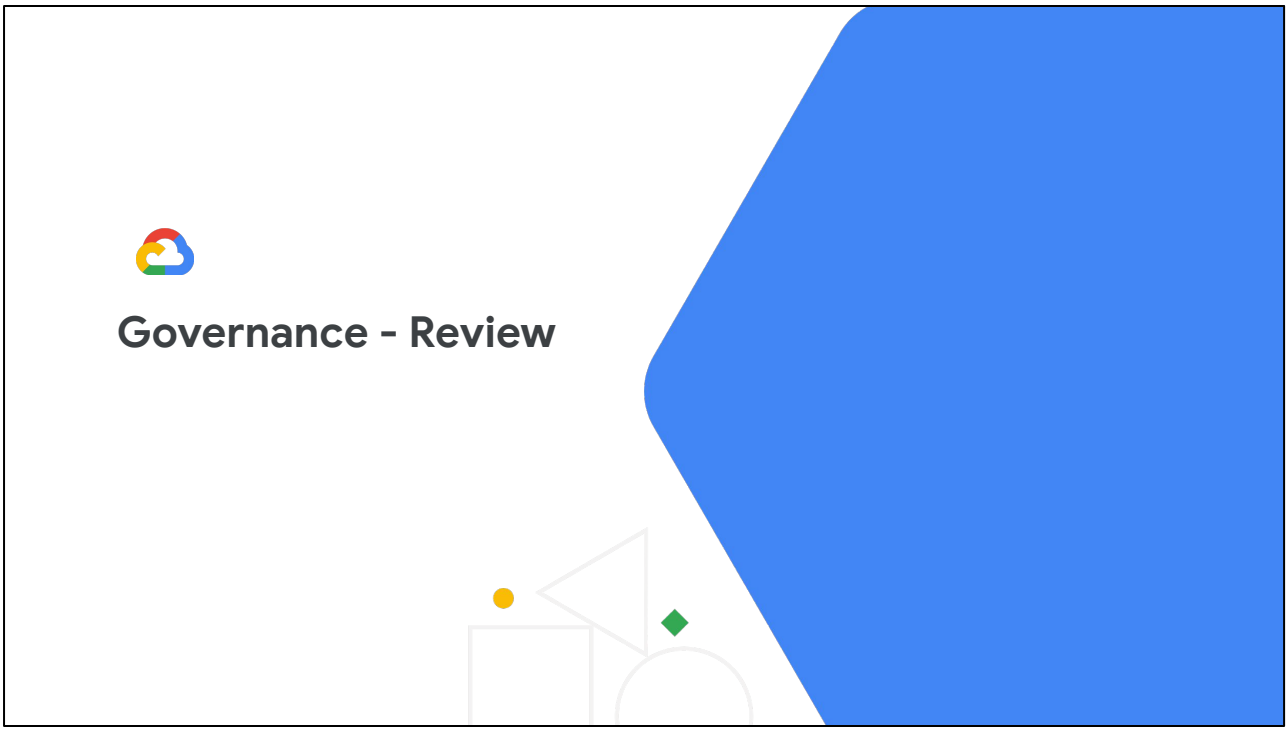
Installing Managed Active Directory

Paul Williams



[Presenter]
In this demo, you will learn how configure a shared vpc network topology

[Demo - screencast]
https://www.youtube.com/watch?v=4MtfyViH9t0



In this module, you learned how to create and manage user identities in the cloud using Cloud Identity. You also learned how to sync your current users and groups from your on-premises environment to the cloud using an automation tool. You were introduced to some best practices on how to structure your resource hierarchy as your cloud footprint grows in size. You also learned how to centrally manage a single network across multiple projects and how to manage an identity provider across environments.

Following your migration, you will want an efficient and effective way to observe your cloud environment. In the next module, we will introduce you to some of the tools that make up Google Cloud's operations suite. Cloud Monitoring provides visibility into the performance, uptime, and overall health of cloud-powered applications. Cloud Logging allows you to store, search, analyze, monitor, and alert on log data and events from Google Cloud.

We will also explain how to use managed instance groups, which are automated groups of virtual machines that can scale up and down based on metrics. You will use our global load balancer to frontend a group of virtual machines, which allows you to scale applications on Compute Engine from zero to full throttle without the need for pre-warming.

Move on to the next module to learn more.