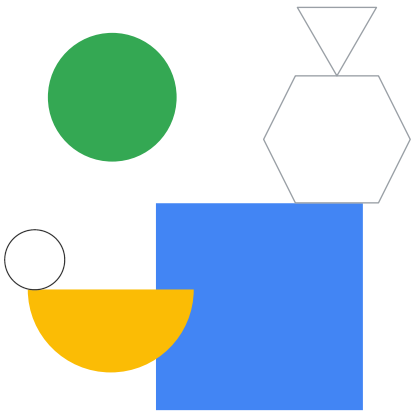
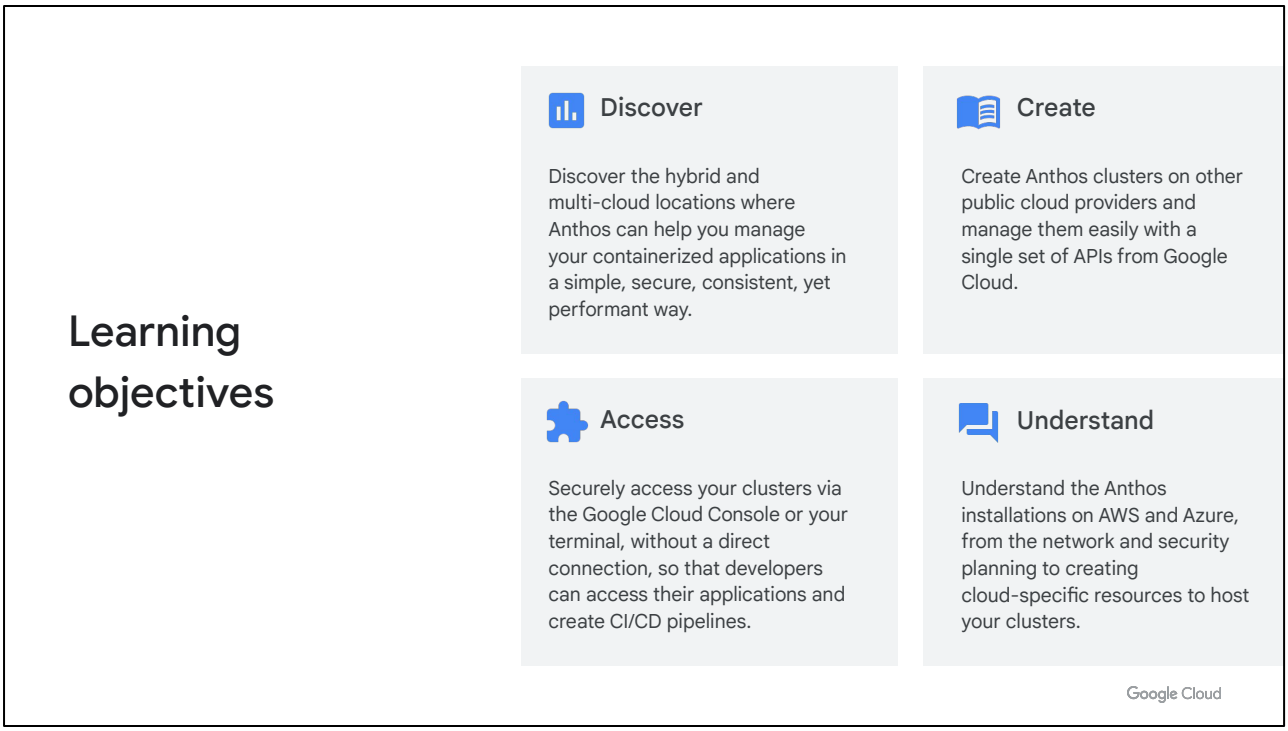
Google Cloud

Anthos Environments (multi-cloud focus)

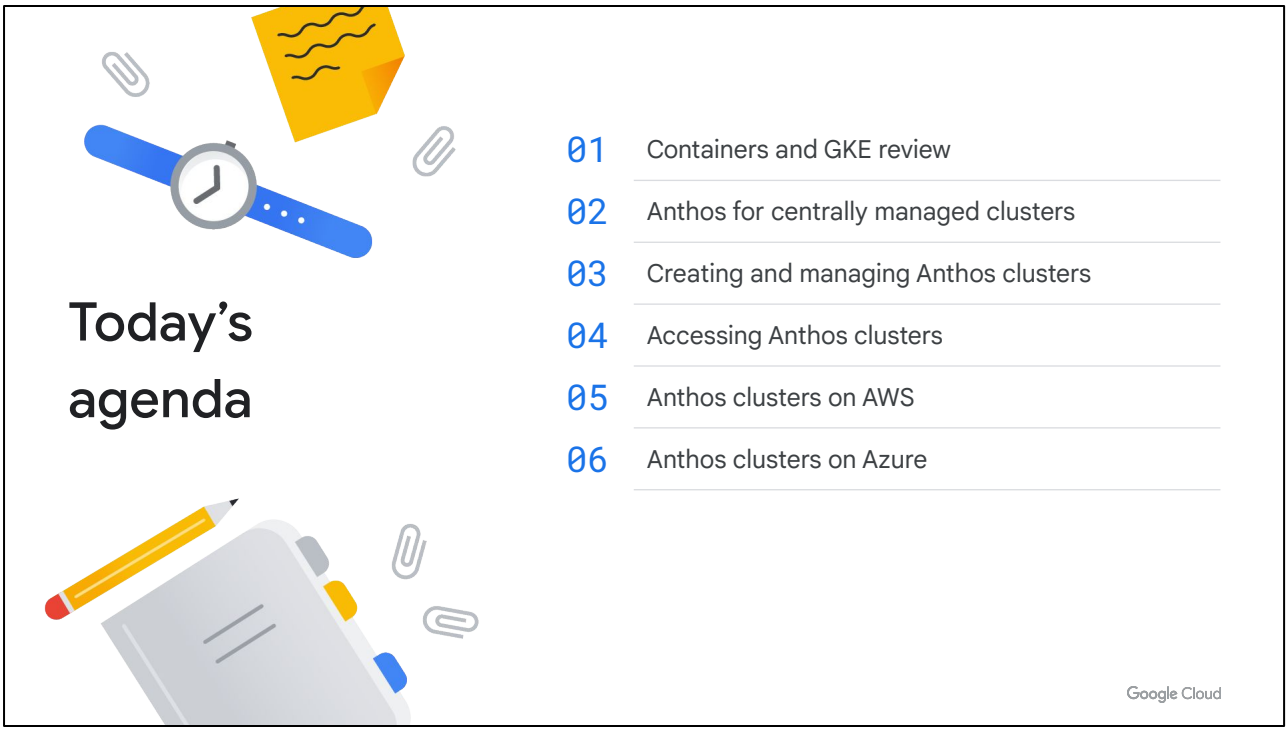


Welcome to the Anthos Environments module. In this module, we will discuss Anthos environments, with a focus on multi-cloud.



In this module, you learn how to:

- Discover the hybrid and multi-cloud locations where Anthos can help you manage your containerized applications in a simple, secure, consistent, yet performant way.
- Create Anthos clusters on other public cloud providers and manage them easily with a single set of APIs from Google Cloud.
- Securely access your clusters via the Google Cloud Console or your terminal, without a direct line-of-sight, so that developers can access their applications and create CI/CD pipelines.
- Understand the Anthos installations on AWS and Azure from the network and security planning to creating cloud-specific resources to host your clusters.



This is the agenda for the day.

Today's agenda

01 Containers and GKE review

02 Anthos for centrally managed clusters

03 Creating and managing Anthos clusters

04 Accessing Anthos clusters

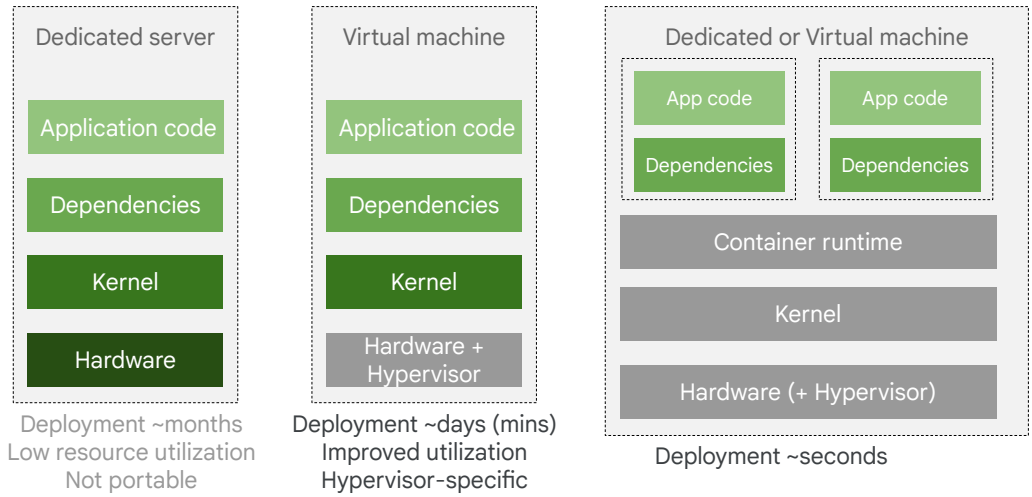
05 Anthos clusters on AWS

06 Anthos clusters on Azure

Google Cloud

Let's start with a review of containers and Google Kubernetes Engine.

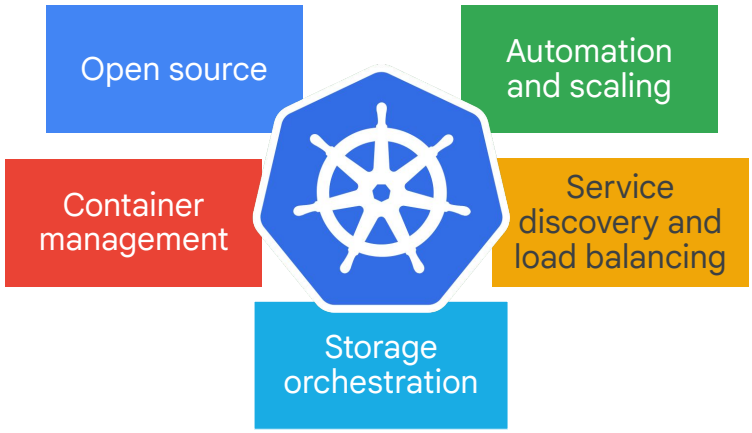
Containers enable you to run workloads anywhere



Google Cloud

Running your workloads on separate environments has many challenges. Fortunately, containers solve most of the consistency issues on the level of the application and its dependencies. Developers consider containers the best abstraction layer because they can package their application, test it locally, and be sure that it will consistently perform on any platform. DevOps also enjoy working with containers because they offer millisecond latencies for deploying, moving, and scaling workloads, which was impossible with virtual machines or bare metal servers.

Kubernetes makes container orchestration easier



Google Cloud

However, managing containers at scale is difficult. Placing containers in compute environments, distributing traffic across containers, managing new application releases, and rolling back deployments to a previous working version are common tasks involved in managing applications.

As a response to those challenges, Google helped launch Kubernetes.

So what is Kubernetes? It's a container-centric management environment. Google originated it and donated it to the open source community. Now it's a project of the vendor-neutral Cloud Native Computing Foundation.

It automates the deployment, scaling, load balancing, logging, monitoring, and other management features of containerized applications. These are the features that are characteristic of typical platform-as-a-service solutions.

Managing Kubernetes infrastructure can be hard

Kubernetes is powerful, but managing the infrastructure is a full-time job.

Is there a managed service for Kubernetes within Google Cloud?

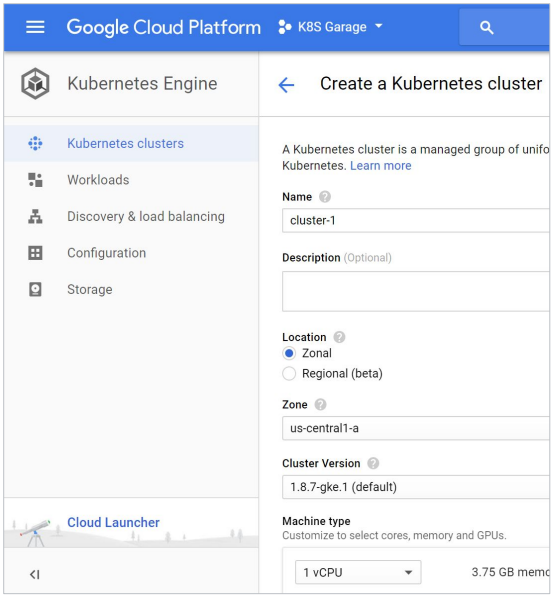
Yes! Google Kubernetes Engine

Google Cloud

However, managing Kubernetes infrastructure can be difficult. You are still responsible for the underlying provisioning of compute, setting up the network, bringing external load balancers, and managing Kubernetes security, identity, and upgrades. To solve all of that, Google Cloud provides Google Kubernetes Engine, or GKE, a managed service that takes care of all the heavy lifting for you so that you can focus on running containers.

GKE is Kubernetes the easy way

- Start a cluster with one click and scale up to 15,000 nodes.
- View your clusters and workloads in a single unified interface.
- Access dashboards for monitoring, logging, and error reporting.
- Google keeps your cluster up and running.



Google Cloud

GKE is Kubernetes the easy way.
With Google Cloud's GKE console, you can start a cluster with one click and scale up to 15,000 nodes.
You can intuitively view your clusters and workloads in a single unified interface and seamlessly access dashboards for monitoring, logging, and error reporting.
All that while Google keeps your cluster up and running.

Google Kubernete Engine manages clusters at scale

- Leverage a high-availability control plane including multi-zonal and regional clusters.
- Eliminate operational overhead with industry-first four-way auto scaling.
- Secure by default, including vulnerability scanning of container images and data encryption.
- Per second billing means paying only for the compute time that you use.

Google Cloud

Google Kubernete Engine manages clusters at scale.
You can leverage a high-availability control plane including multi-zonal and regional clusters.
Eliminate operational overhead with industry-first four-way auto scaling.
GKE is secure by default, including vulnerability scanning of container images and data encryption.
All that with a per second billing model, which means paying only for the compute time that you use.

Today's agenda

01 Containers and GKE review

02 Anthos for centrally managed clusters

03 Creating and managing Anthos clusters

04 Accessing Anthos clusters

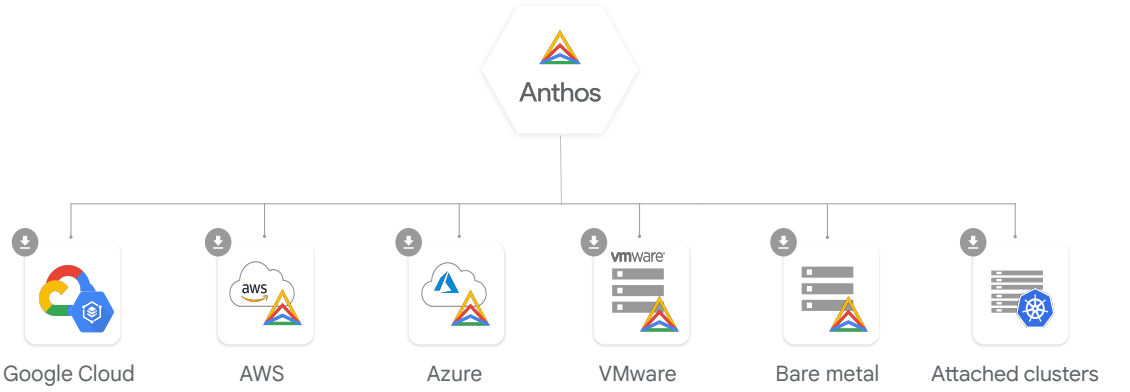
05 Anthos clusters on AWS

06 Anthos clusters on Azure

Google Cloud

Customers love using GKE on Google Cloud, but they also need help when running their Kubernetes clusters on platforms. That's where Anthos comes into place.

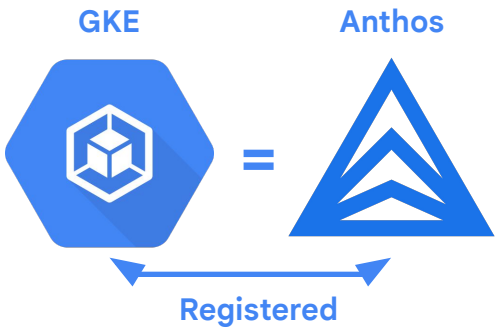
Anthos manages Kubernetes clusters anywhere



Anthos manages Kubernetes clusters anywhere. From running in Google Cloud together with GKE clusters, to being installed in other clouds, such as Anthos on AWS or Anthos on Azure, Anthos provides a fully managed Kubernetes experience. You can also run Anthos on-premises and in edge locations with the Anthos on VMware and Anthos on bare metal offerings. The idea is that Anthos leverages different infrastructure but uses the same management software to provide consistency across environments. Finally, if you already use a supported distribution of Kubernetes, such as Openshift or Rancher, you can connect them—as well as attached clusters—and manage them centrally from Google Cloud. Let's look closer at the specific offerings.

Anthos on Google Cloud uses GKE clusters

- Not every GKE cluster is an Anthos cluster.
- You must register a GKE cluster with Anthos Hub, using:
  - Workload Identity
  - Service account
- Anthos clusters benefit from additional features such as Anthos Service Mesh or Anthos Config Management.
- More details on Anthos Connect follow later in the module.



Google Cloud

The first option is running Anthos on Google Cloud, which uses GKE clusters.
However, not every GKE cluster is an Anthos cluster.
To convert a GKE cluster into an Anthos cluster, you must register a GKE cluster with Anthos Hub, using either:

- Workload Identity
- Or Service account

You might choose to register GKE as Anthos clusters to benefit from additional features such as Anthos Service Mesh or Anthos Config Management.
More details on Anthos Connect and how to use it follow later in the module.

Anthos clusters on AWS bring GKE to Amazon

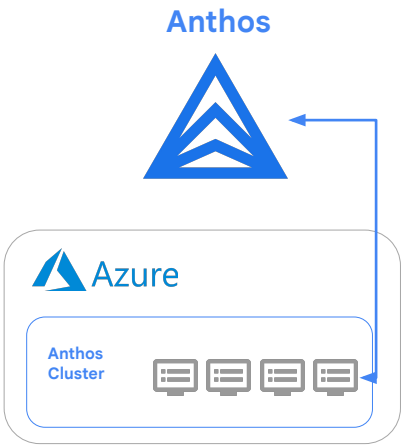
- Anthos uses regular AWS resources such as EC2 VMs, EBS volumes, ELB load balancers, and VPC networks.
- Anthos provides Kubernetes advanced management features such as node autoscaling.
- Anthos offers operational consistency, a unified interface, and easy Kubernetes upgrades.
- Anthos clusters on AWS integrate with Anthos Config Management policies, Anthos Service Mesh controls and observability, Cloud Run, and Cloud Logging.

Google Cloud

Anthos clusters on AWS bring GKE to Amazon Web Services. Google Cloud runs the Anthos management software to create, update, manage, and upgrade Kubernetes clusters in AWS.
Anthos uses regular AWS resources such as EC2 VMs, EBS volumes, ELB load balancers, and VPC networks, providing the same native performance.
Additionally, it provides Kubernetes advanced management features such as node autoscaling.
Anthos offers all features expected from a managed service, such as operational consistency, a unified interface, and easy Kubernetes upgrades.
Finally, Anthos clusters on AWS integrate with the rest of Anthos components, including Anthos Config Management policies, Anthos Service Mesh controls and observability, serverless Cloud Run containers, and Cloud Logging and Cloud Monitoring to observe your clusters.

Anthos clusters on Azure bring GKE to Microsoft Azure

- As with AWS, operators can create, manage, and upgrade GKE clusters in Azure.
- Anthos uses regular Azure resources such as Azure VMs, Azure managed disks, Azure Load Balancers, and Azure Virtual Networks.
- Continue to manage identity with your Azure Active Directory, using those credentials to authenticate to your clusters from the Google Cloud Console.
- Anthos clusters on Azure integrate with the same additional Anthos components as discussed before.

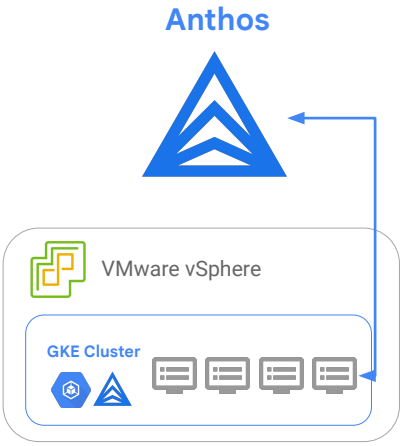


Google Cloud

As with AWS, operators can leverage Anthos to create, manage, and upgrade GKE clusters in Azure.
Anthos uses regular Azure resources such as Azure VMs, Azure managed disks, Azure Load Balancers, and Azure Virtual Networks running with native performance.
You can continue to manage identity with your Azure Active Directory, using those credentials to authenticate to your clusters from the Google Cloud Console.
Anthos clusters on Azure integrate with the same additional Anthos components we discussed previously.

Anthos clusters on VMware provide on-premises functionality

- Turnkey, production-grade, conformant Kubernetes with best practice configuration and upgrades working as a managed service.
- Anthos provides node management functionality and integration with the vSphere environment:
  - Node autoscaling, auto-resizing, auto-repair
  - Support for Linux and Windows nodes and containers
- Anthos packages load balancer software with Seesaw and deep integrations with other providers such as F5.
- Anthos also leverages the Container Storage Interface (CSI) to provide native integrations with vSphere drivers and other third-party storage solutions.



Google Cloud

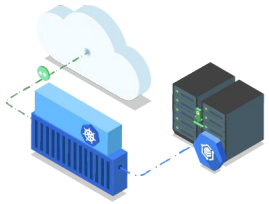
Anthos clusters on VMware is a software that brings Google Kubernetes Engine (GKE) to your data center in a vSphere environment.
Use turnkey, production-grade, conformant Kubernetes with best practice configuration working as a managed service.
Anthos provides node management functionality and integration with the vSphere environment:

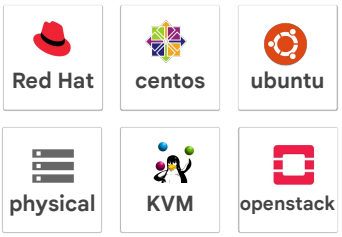
- That way, it can work with VMs the same way as in the cloud, providing node autoscaling, auto-resizing, and auto-repairs
- Additionally, it provides support for Linux and Windows nodes and containers

Anthos packages load balancer software with Seesaw and deep integrations with other providers such as F5 to offer an end-to-end solution that leverages your existing enterprise software.
Anthos also leverages the Container Storage Interface (CSI) to provide native integrations with vSphere drivers and other third-party storage solutions.

Anthos clusters on bare metal run directly on your hardware

- You own the hardware environment, so you have direct control over scale, security, latency, etc.
- Anthos provides out-of-the-box overlay network, load balancing, in-place upgrades, etc.
- You don't have as much node management capabilities as with other Anthos environments such as autoscaling, but you can run on a range of platforms and operating systems.
- Anthos on bare metal provides the same level of management, security, networking, and add-ons as other Anthos installations.



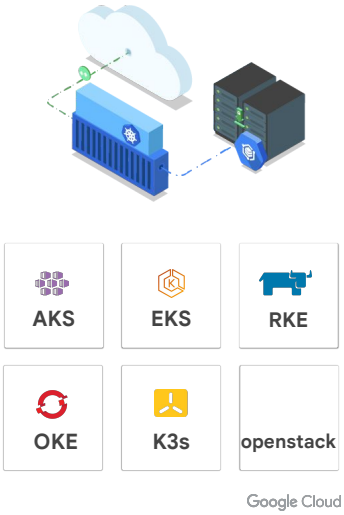


Google Cloud

Anthos clusters on bare metal clusters run directly on your hardware, getting the best performance and enabling you to deploy them in your data centers and edge locations.
You own the hardware environment, so you have direct control over scale, security, latency, etc.
Anthos on bare metal provides an out-of-the-box overlay network, load balancing with MetalLB, and in-place upgrades for Kubernetes, among other features.
You don't have as much node management capability as with other Anthos environments, but you can run on a range of platforms, such as openstack or KVM, and operating systems such as Red Hat, CentOS, or Ubuntu.
Anthos on bare metal provides the same level of management, security, networking, and add-ons as other Anthos installations.

You can attach non-Anthos managed clusters

- Connected clusters support a subset of Anthos features, including:
  - Anthos Service Mesh
  - Anthos Config Management
- Anthos supports connecting these cluster types:
  - Amazon Elastic Kubernetes Service (EKS)
  - Microsoft Azure Kubernetes Service (AKS)
  - Red Hat OpenShift Kubernetes Engine (OKE) and Container platform (OCP)
  - Rancher Kubernetes Engine (RKE)
  - KIND
  - K3s
  - K3d



Finally, you can also attach non-Anthos managed clusters that might be running in other clouds, platforms, or data centers.
In this case, you are responsible for the Kubernetes cluster management and administration, while Anthos provides the centralized workload, operations, and configuration management.
You can use a subset of Anthos components—such as Anthos Service Mesh or Anthos Config Management—and the GKE console and Google Cloud Logging and Monitoring capabilities.
It allows you to work with existing supported clusters such as:

- Amazon Elastic Kubernetes Service (EKS)
- Microsoft Azure Kubernetes Service (AKS)
- Red Hat OpenShift Kubernetes Engine (OKE) and Container platform (OCP)
- Rancher Kubernetes Engine (RKE)
- KIND
- K3s
- K3d

Today's agenda

01 Containers and GKE review

02 Anthos for centrally managed clusters

03 Creating and managing Anthos clusters

04 Accessing Anthos clusters

05 Anthos clusters on AWS

06 Anthos clusters on Azure

Google Cloud

Now that we have seen the different Anthos offerings, let's look at how to create such clusters. We will focus on multi-cloud in this module. If you are interested in learning more about running Anthos on VMware or bare metal, we recommend the one-day specialization courses.

Enable services to manage Anthos clusters in other public clouds

```
gcloud services enable \
    gkemulticloud.googleapis.com \
    gkeconnect.googleapis.com \
    connectgateway.googleapis.com \
    cloudresourcemanager.googleapis.com
\
    anthos.googleapis.com \
    logging.googleapis.com \
    monitoring.googleapis.com
```

Google Cloud

The first thing, as always when you want to use a new service in Google Cloud, is enabling services.

Google Cloud management regions

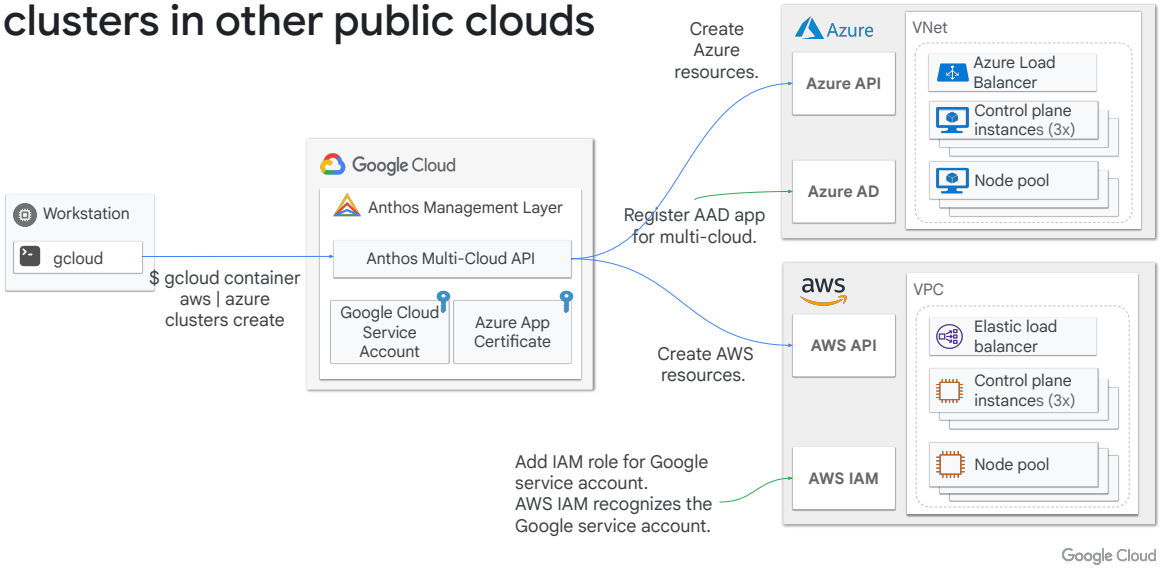
- AWS and Azure regions are associated with Google Cloud regions for management purposes.
- Anthos stores all cluster resource data and keys in the specified Google Cloud region to comply with your geographic requirements.

Google Cloud Region	Associated AWS Region	Associated Azure region
europe-west1	eu-central-1 eu-north-1 eu-south-1 eu-west-1 eu-west-2 eu-west-3	francecentral germanywestcentral northeurope uksouth westeurope
us-west1	us-west-1 us-west-2	westus2
us-east4	ca-central-1 us-east-1 us-east-2	canadacentral centralus eastus eastus2 southcentralus
asia-southeast1	ap-southeast-1	southeastasia australiaeast

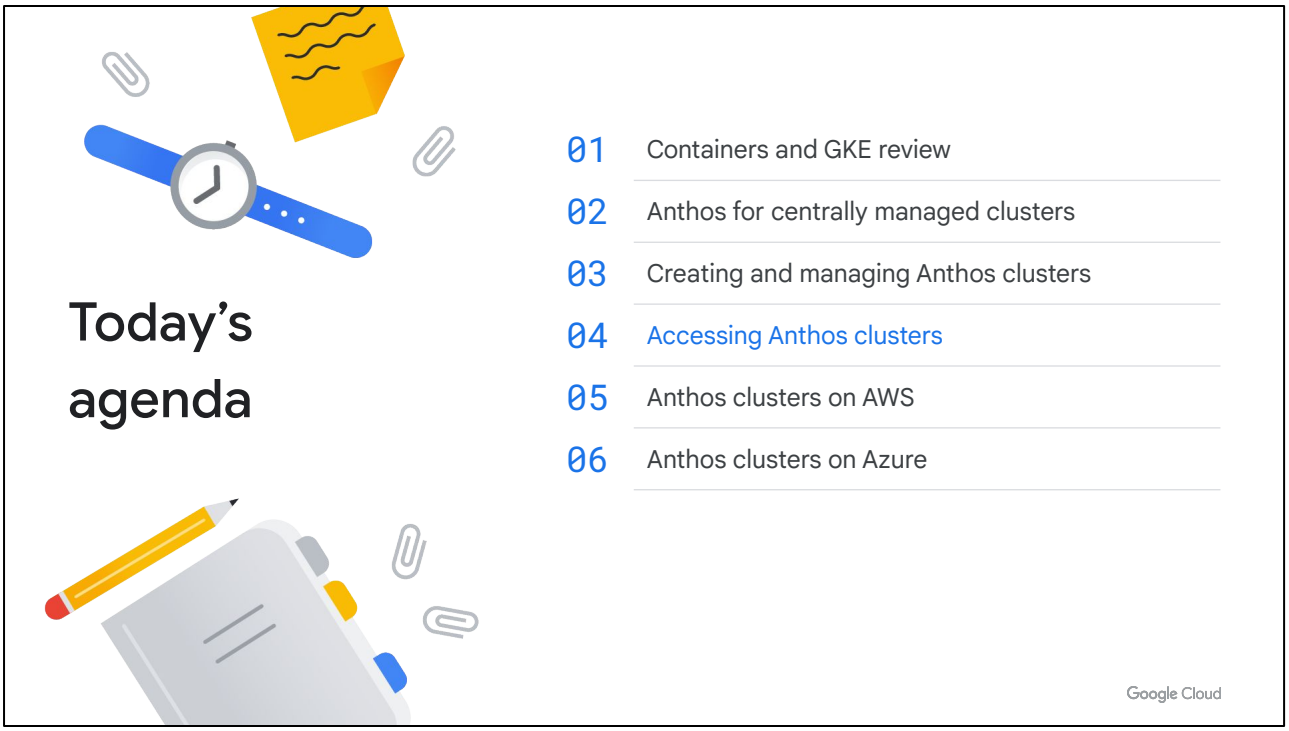
Google Cloud

Second, you must decide where to run your clusters and where to host the management services in Google Cloud.
Here is a list of AWS and Azure regions that are associated with Google Cloud regions for management purposes.
Anthos stores all cluster resource data and keys in the specified Google Cloud region to comply with your geographic requirements.
For example, if you want to keep all your data in Asia and run your cluster in AWS, you would choose the asia-southeast1 region in Google Cloud and the ap-southeast-1 in AWS.
Take a moment to observe the association between Google Cloud and the other public cloud providers.

Anthos Multi-Cloud API manages clusters in other public clouds



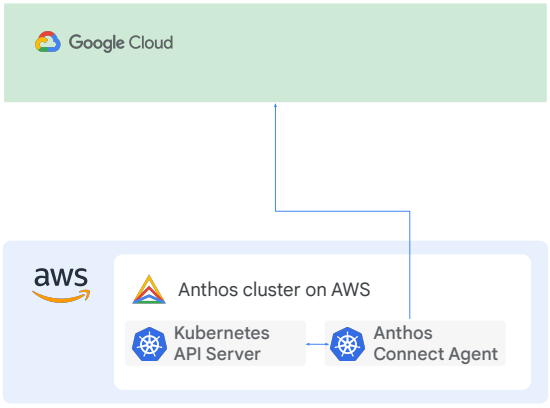
Third, you can create the Anthos clusters on other clouds by leveraging the Multi-Cloud API.
The Multi-Cloud API manages the setup, update, and teardown of clusters in each cloud.
All those actions are available via the gcloud CLI tool, so everything can be programmatically configured and automated.
Notice that certain permissions will be needed in the cloud providers. Later we'll discuss this in a higher level of detail, but you will use an application client in Azure and a service account in AWS.
The Anthos Multi-Cloud API then creates your cluster control planes, worker nodes, and associated storage and load balancers in the target cloud provider.
You then view your clusters in the Google Cloud console.



Let's look at how to connect and interact with a cluster.

Anthos Connect Agent enables connectivity to Google Cloud

- Anthos Connect Agent is installed in your cluster.
- No public IP address is required for your cluster.
- Connection from the Kubernetes cluster to Google Cloud is authenticated and encrypted with TLS.
- Connections can traverse NATs and firewalls.
- User interactions with clusters are visible in Kubernetes Audit Logs.

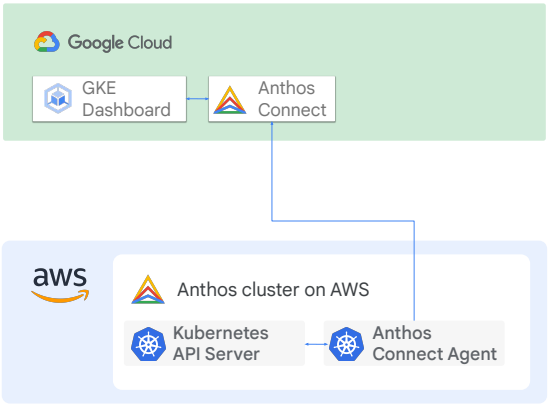


Google Cloud

We'll first discuss the Anthos Connect Agent, a Kubernetes Deployment running in your Anthos cluster. This agent is either deployed in the installation process when you run a managed Anthos offering, or you must install it on your own when working with attached clusters. We will see how to do so in a couple of slides.
The Anthos Connect Agent performs an authenticated and encrypted connection from the Kubernetes cluster to Google Cloud using TLS. This outbound connection traverses any NATs and firewalls in the network and does not require a public IP address in your cluster.
This connection is used to communicate with the control plane. Any user interactions with clusters are then visible in Kubernetes Audit Logs.

Anthos Connect enables the management of Anthos clusters from Google Cloud

- Perform requests from Google Cloud to each cluster's API server.
- Use the GKE management pages to observe and manage your cluster, workloads, and services in other environments.
- Anthos components such as Anthos Config Management and Usage Metering are also managed through Anthos Connect.



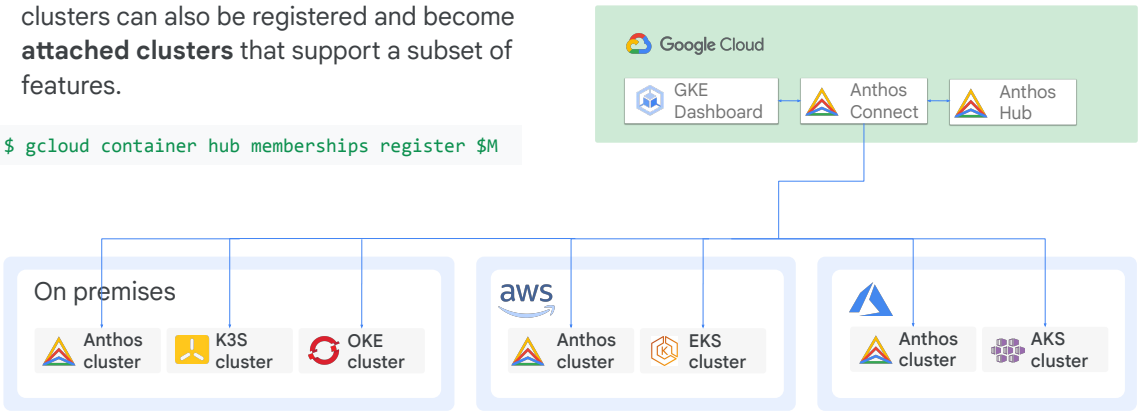
Google Cloud

The Anthos Connect Agent in the cluster establishes a connection with Anthos Connect, which enables the management of Anthos clusters from Google Cloud. You can access the Google Console GKE dashboard to observe and manage your cluster, workloads, and services.
Additional Anthos components, such as Anthos Config Management or Usage Metering, are also managed through Anthos Connect.

Register any Kubernetes cluster to Anthos Hub

- Conformant, but non-Anthos distribution, clusters can also be registered and become **attached clusters** that support a subset of features.

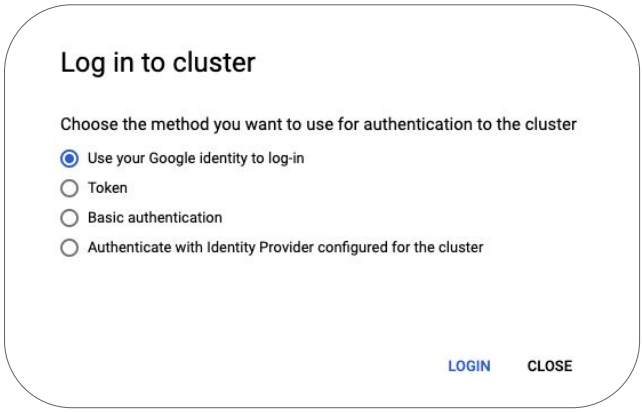
```
$ gcloud container hub memberships register $M
```



Google Cloud

If you want to manage an existing Kubernetes cluster with Anthos, you must register it with Anthos Hub. That way, you can access and control all your clusters from the same unified management interface. To do so, run the “gcloud container hub memberships register” command, which installs and configures the Anthos Connect Agent in your cluster.

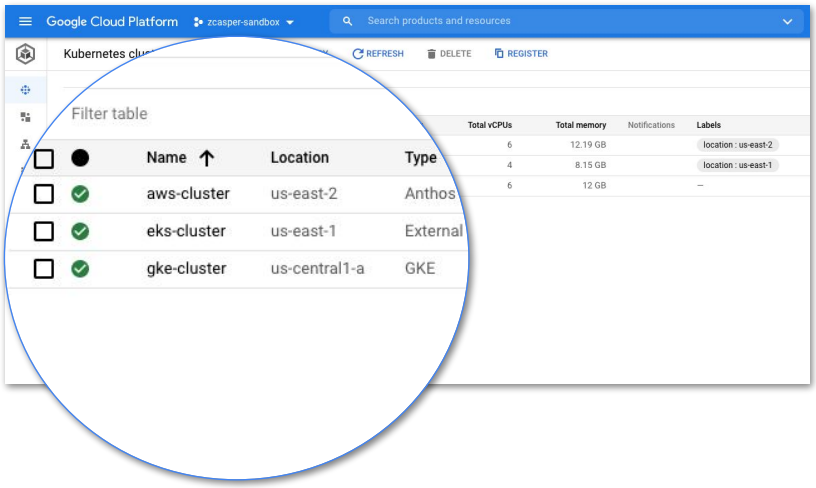
Users can log in to the cluster using various credentials



Google Cloud

You must log in to your cluster from the Google Cloud Console to operate it. Users can log in to the cluster using several types of credentials: Google Accounts, Kubernetes Service Account tokens, basic username/password combinations, or credentials associated with a third-party Identity Provider.

Registered and authenticated clusters can be managed via Google Cloud GKE Dashboard

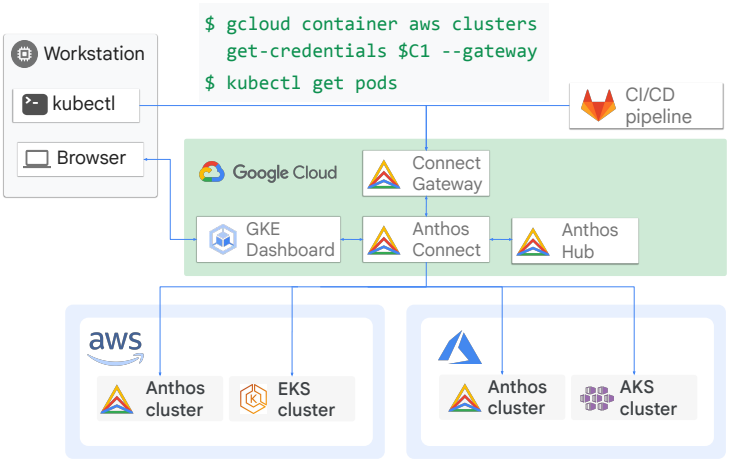


Google Cloud

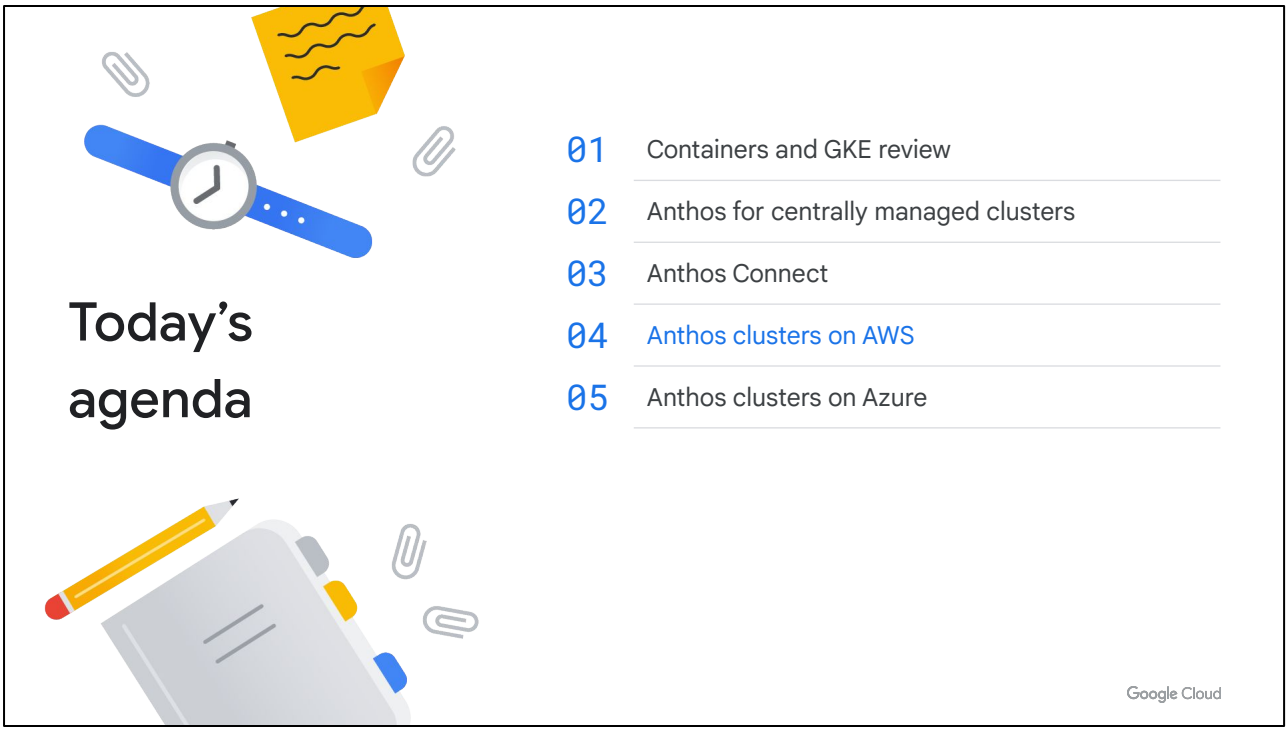
After you log in to the cluster, you can manage your cluster via the Google Cloud GKE Dashboard.

Anthos Connect Gateway enables management through kubectl

- Run commands against registered Anthos clusters in a simple, consistent, and secured way.
- Access clusters on Google Cloud, other public clouds, or on-premises.
- Authenticate and authorize using the same identities you use with Google Cloud services.
- Automate DevOps processes across all your clusters.

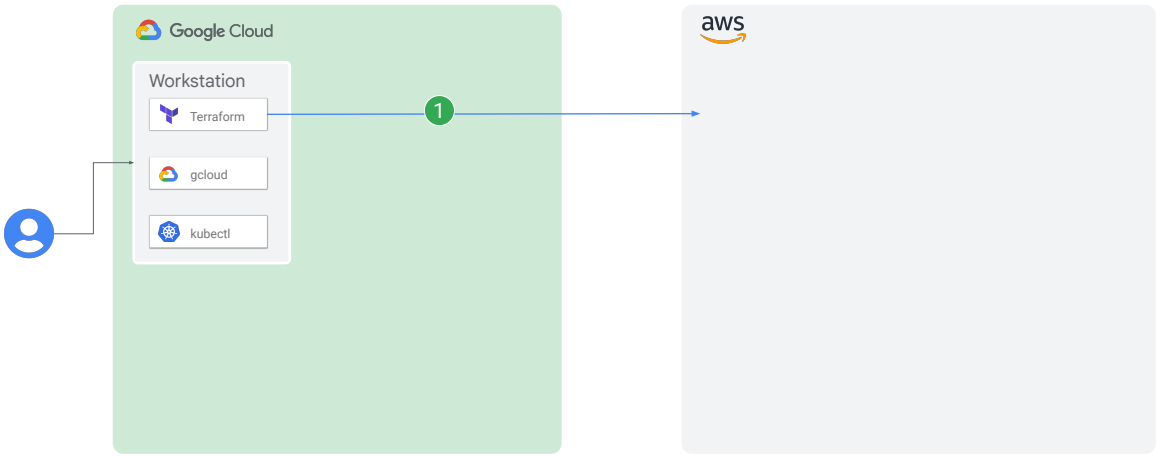


You can also run commands against registered Anthos clusters in a simple, consistent, and secured way, using Anthos Connect Gateway. This option is only available for Anthos managed clusters and changes slightly in every Anthos version. To obtain the kubeconfig credentials for Anthos installations in AWS or Azure, run the “gcloud container aws (or azure) clusters get-credentials” command.
That way, you can communicate with clusters on other locations without being in the same network. You perform an authenticated kubectl command against the Connect Gateway, and this authorizes it and forwards it via the connect agent to your Anthos cluster. You can have a unified CI/CD process across Anthos clusters in different environments and networks.



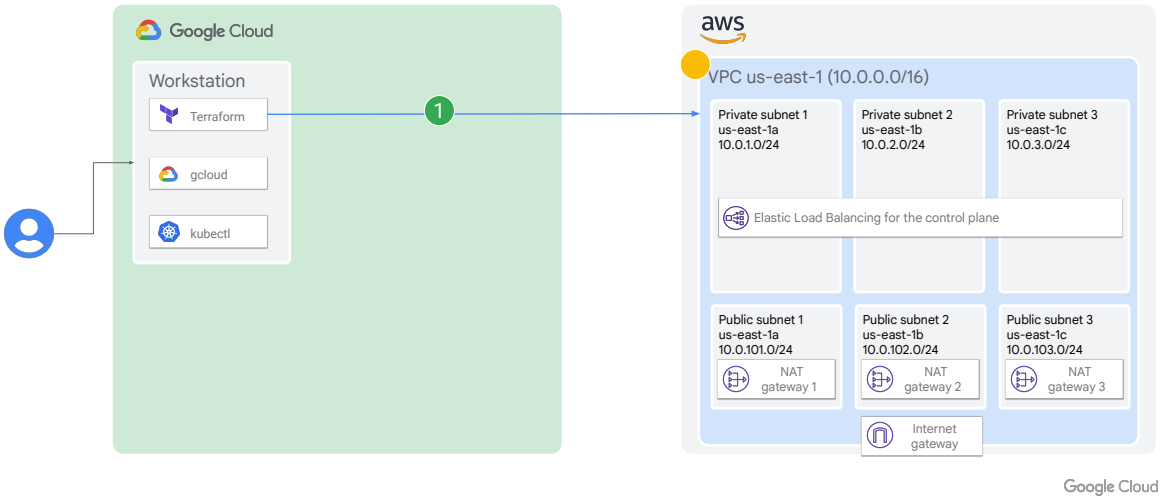
Let's do a deep dive on AWS and provide a more detailed overview of the entire process.

Use Terraform to create the AWS infrastructure



First, you must create the AWS Infrastructure. This can be done using a variety of methods such as Terraform, the AWS CLI, or the AWS Console. The AWS Infrastructure required includes the following components: Networking, Encryption Keys, and Identity and Access Management roles.

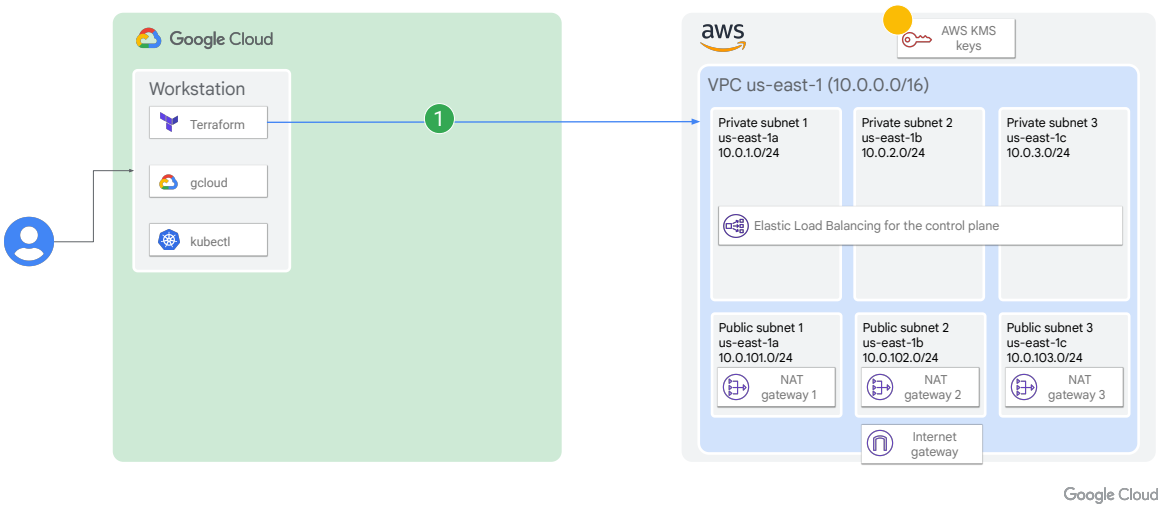
Create AWS networking components



Let's look at the AWS networking components, which include:

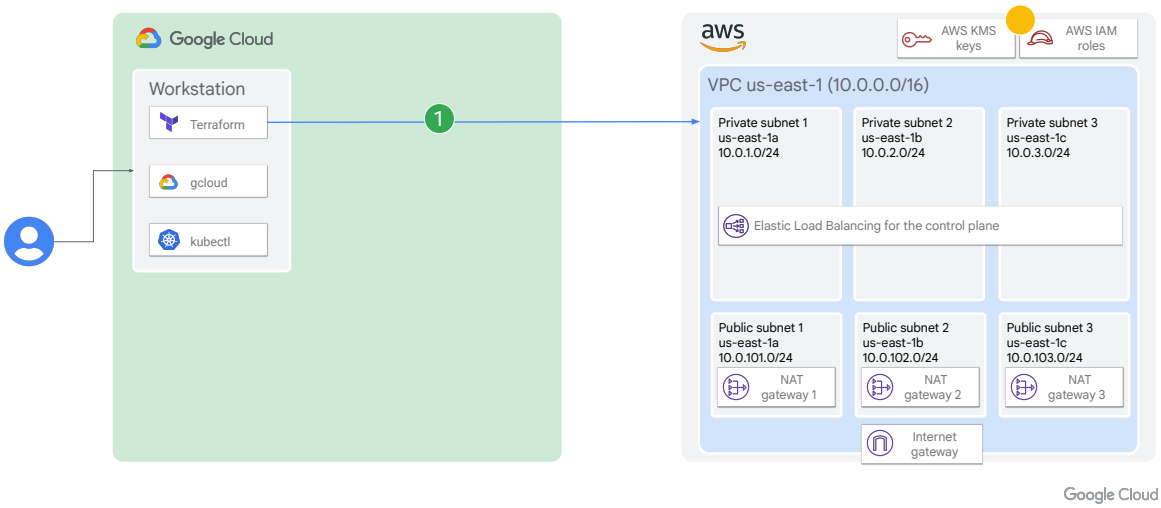
- A Virtual Private Cloud, or VPC, with a CIDR range big enough to host IP addresses for load balancers, gateways, cluster nodes, pod and services IP addresses.
- One or multiple private subnets to host the worker and control plane nodes.
- One or multiple subnets to host NAT gateways to allow outbound connectivity on the nodes that are hosted on the private subnets.
- Networking tags on the subnets so that Anthos clusters on AWS can discover the type of AWS load balancers to create.
- An Internet gateway that enables internet connectivity to the public networks.

Create AWS Key Management Service encryption keys



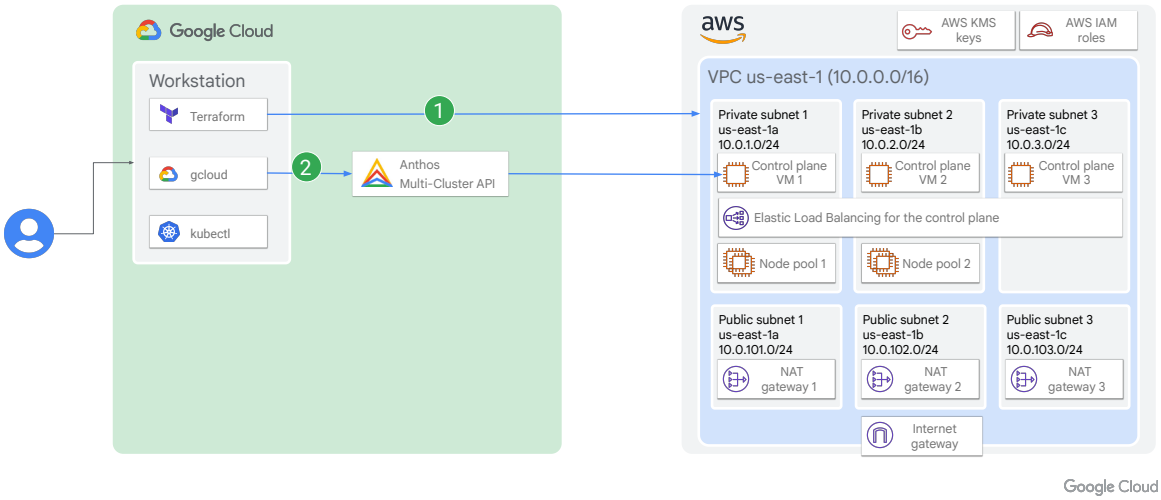
Create AWS Key Management Service encryption keys. Anthos clusters on AWS uses a customer-managed KMS symmetric key to encrypt Kubernetes state data in etcd and customer user data. You can use a separate key for your etcd and user data or use the same key for both.

Create AWS Identity and Access Management (IAM) policies and roles



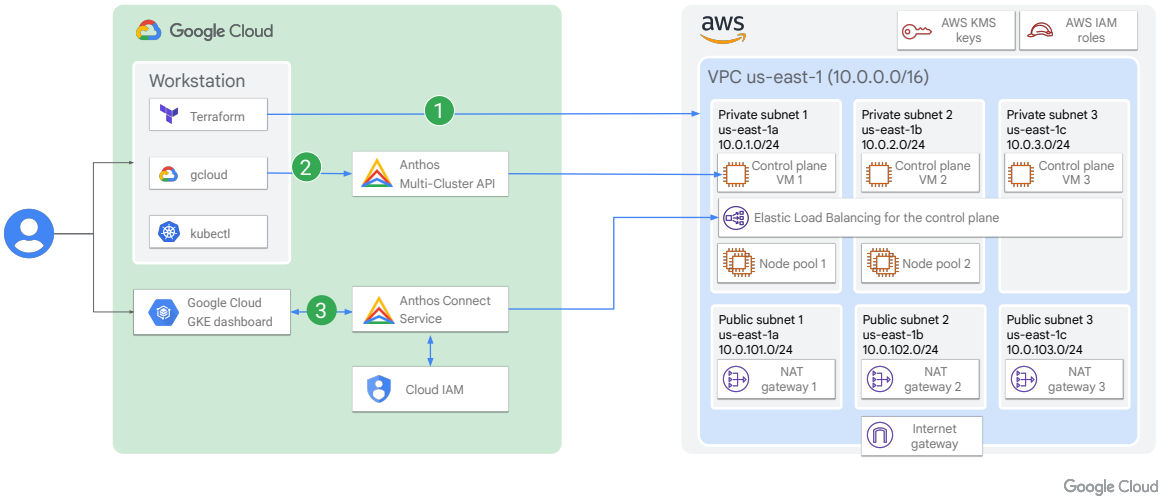
Create AWS Identity and Access Management roles and associated policy with permissions to manage AWS Key Management Service (KMS), Elastic Compute Cloud (EC2), Autoscaling, Elastic Load Balancing (ELB), and Identity and Access Management (IAM). These are used by the Anthos Multi-Cluster API to create, update, and delete the Anthos clusters on AWS.

Create your AWS cluster and node pools using gcloud



Create your AWS cluster and node pools using gcloud. You can specify the control plane to be located in one or multiple Availability Zones. Node pools are created in one Availability Zone only and therefore, if you want high availability of your workloads, you must spread them across multiple pools. Although the control plane always creates three nodes, you can specify a minimum and maximum number of nodes for autoscaling your node pools.

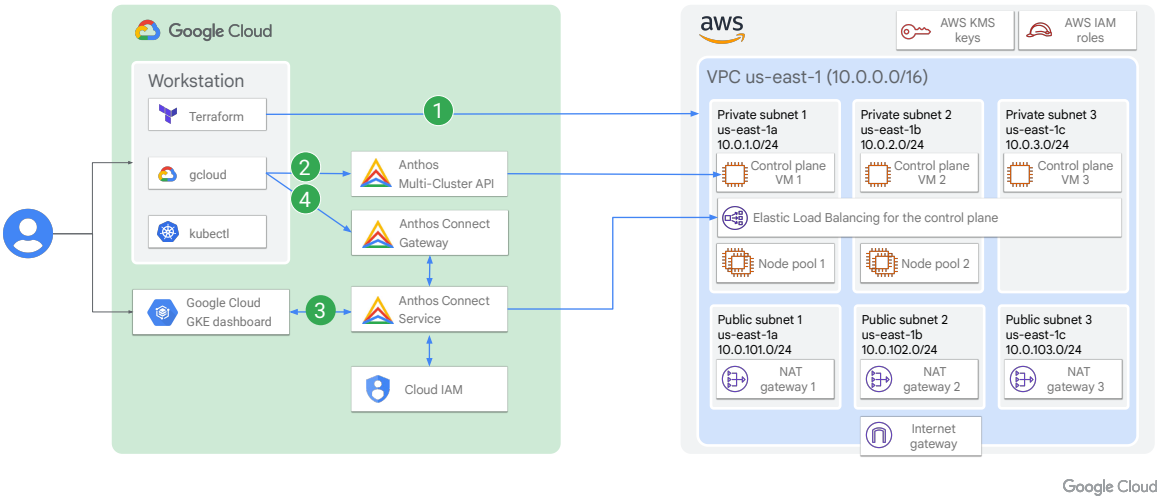
Authenticate to your Anthos cluster on AWS to manage it from the Google Cloud Console



Now that the cluster has been created, you can log in to your cluster to perform operations through the Google Cloud Console. You can use several different types of credentials such as Google Accounts, Kubernetes Service Account tokens, basic username/password combinations, or credentials associated with a third-party identity provider.

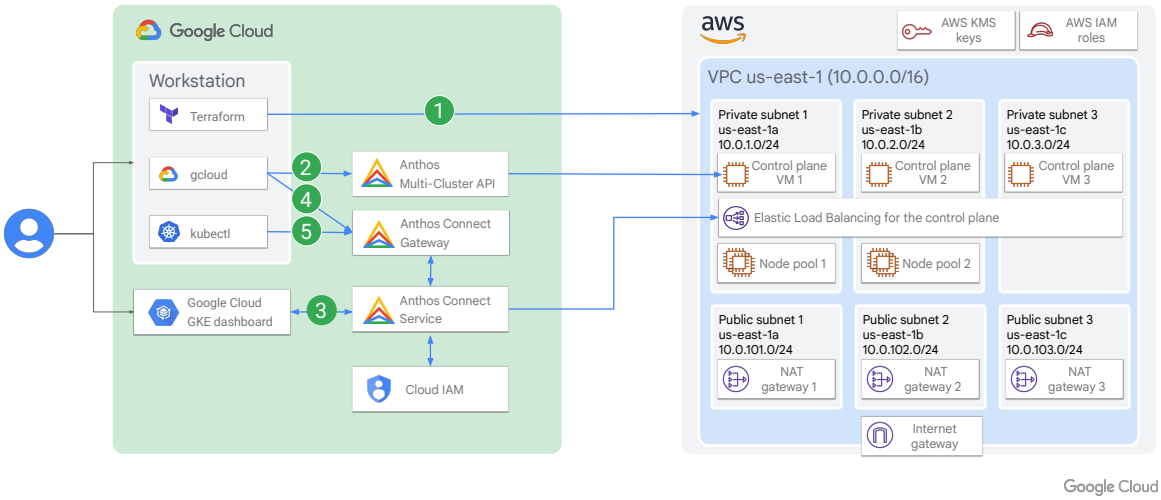
Obtain credentials with:

"gcloud container hub memberships get-credentials aws-cluster"



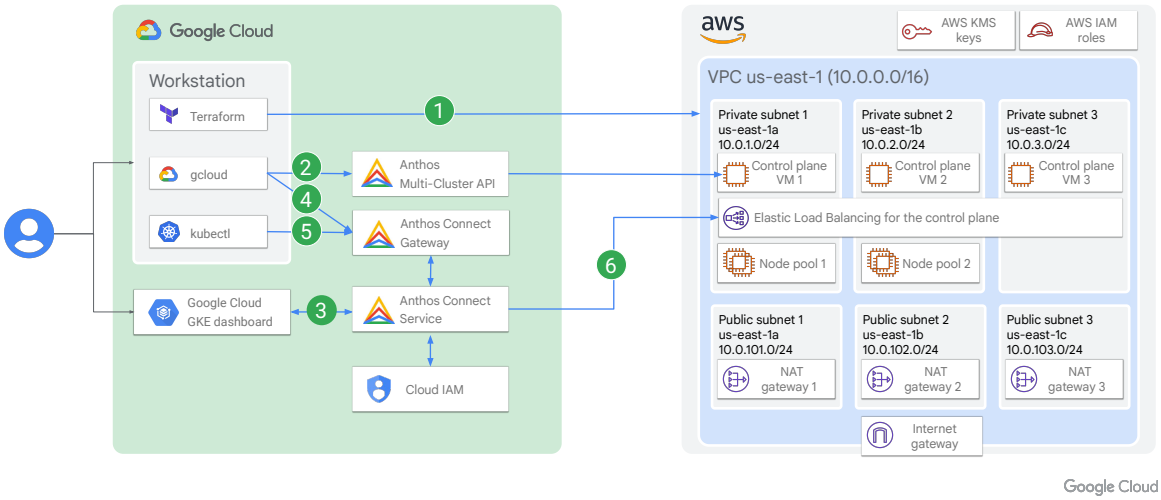
You can also interact with your cluster using kubectl. To do so, download the kubeconfig with the credentials for the Connect Gateway by running the "gcloud container hub memberships get-credentials" on your AWS cluster.

Perform operations with kubectl



Use the new kubeconfig file with kubectl that way, connecting to the Anthos Connect Gateway, and initiate an operation.

Connect Gateway forwards the requests via the agent on the cluster to the API server



The Connect Gateway forwards the requests via the agent on the Anthos cluster on AWS to the API server. That way you can communicate with your cluster without being in the same network.

Today's agenda

01 Containers and GKE review

02 Anthos for centrally managed clusters

03 Anthos Connect

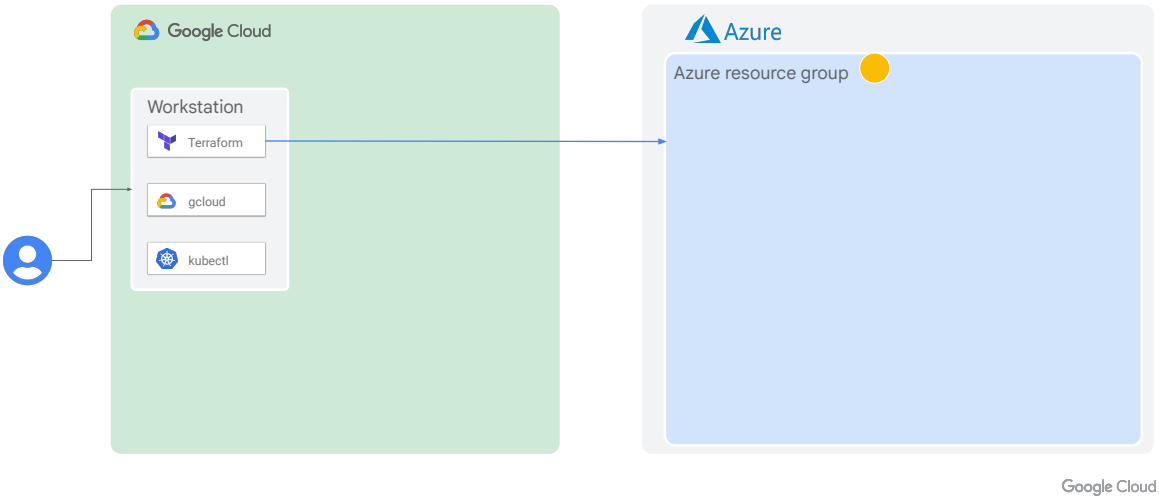
04 Anthos clusters on AWS

05 Anthos clusters on Azure

Google Cloud

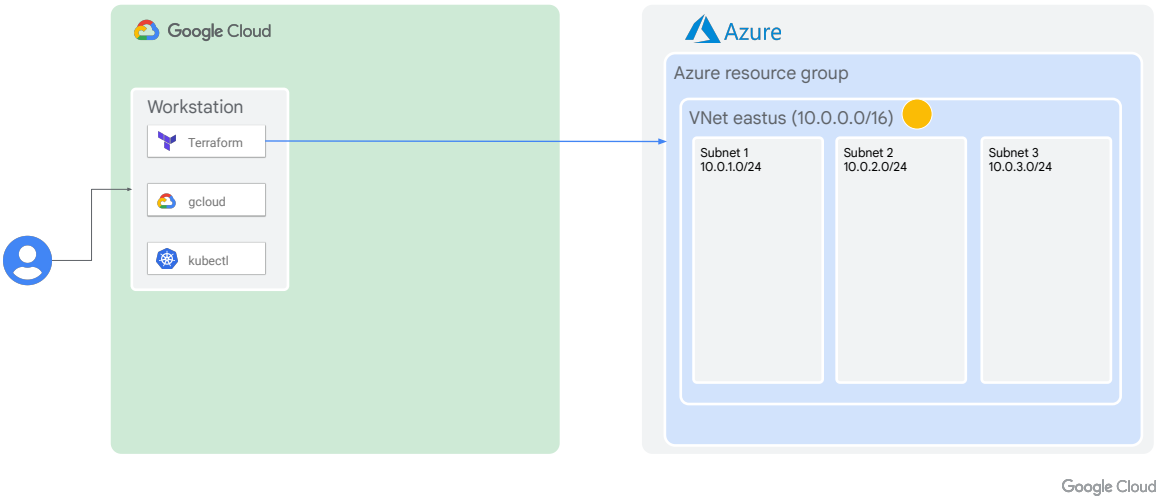
Let's dive deep now.

Create a new resource group for the Anthos cluster on Azure solution



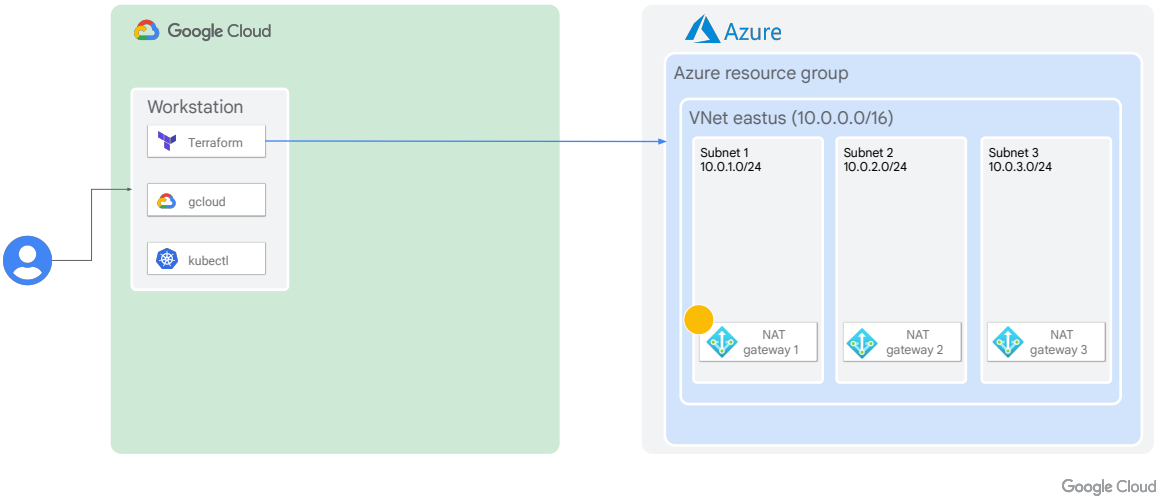
(1) Create a new resource group for your Anthos clusters on Azure. Here, you will place all Azure resources, from networking and security, on the clusters themselves.

Create an Azure virtual network (VNet) and subnets



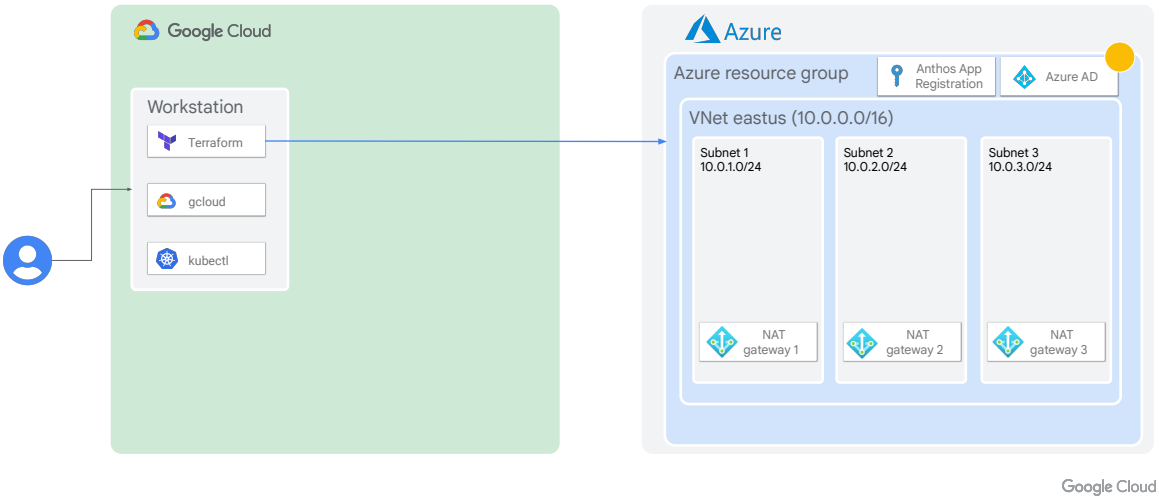
(2) Create an Azure virtual network (VNet) and add as many subnets as you want. The control plane nodes will be distributed across your subnets.

Create Nat Gateway for outbound communication of the Anthos Connect Agent



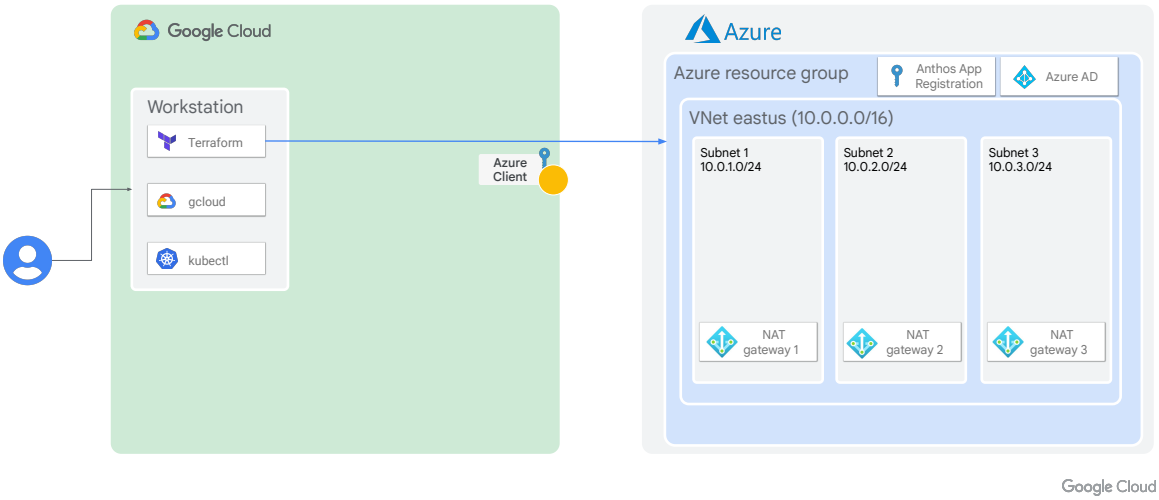
(3) Create and attach a NAT gateway per subnet and an IP address per NAT gateway. The NAT gateway enables the outbound communication from the Anthos Connect Agent inside the Anthos cluster on Azure to Google Cloud.

Create an Azure Active Directory (Azure AD) to store configuration information in Azure



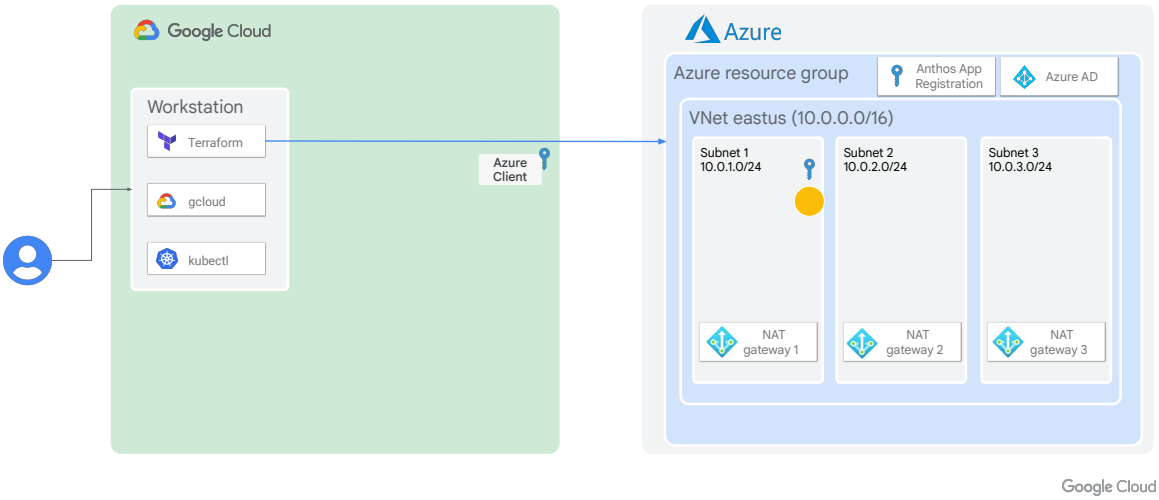
(4) Create an Azure Active Directory (Azure AD) application and service principal. Anthos clusters on Azure use these to store configuration information on Azure. For Anthos to access the Azure APIs, assign the following permissions to your Azure subscription or resource group: Contributor, User Access Administrator, and Key Vault Administrator roles.

Create an Azure Client resource that Anthos clusters use to authenticate to Azure



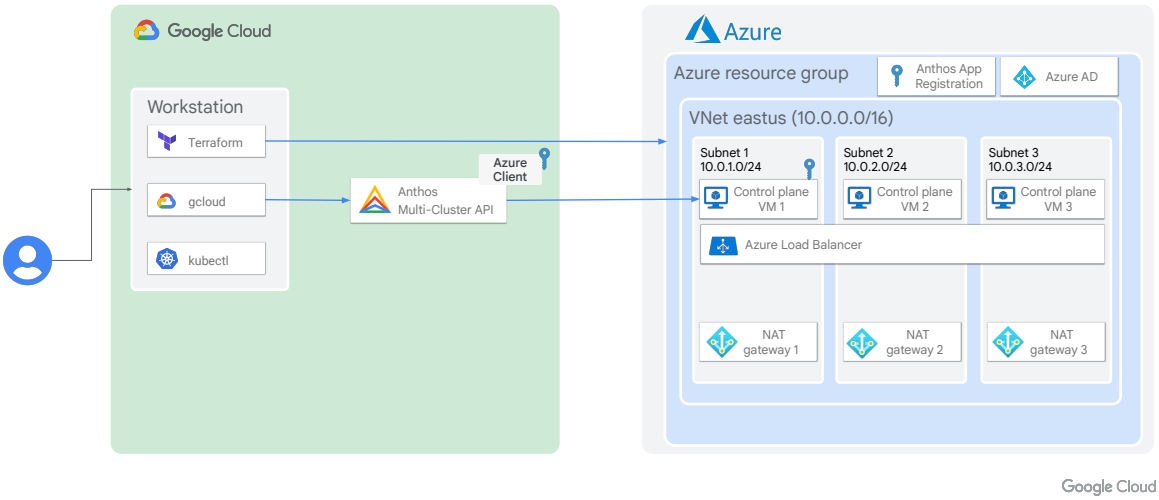
(5) Create an *AzureClient* resource that Anthos clusters on Azure use to authenticate to Azure. When you create a client, Google generates a key pair. You upload the public key to Azure Active Directory (Azure AD). You can use the same Azure Client to create multiple clusters in the same Google Cloud project.

Create an SSH key pair to enable encrypted communications with your cluster

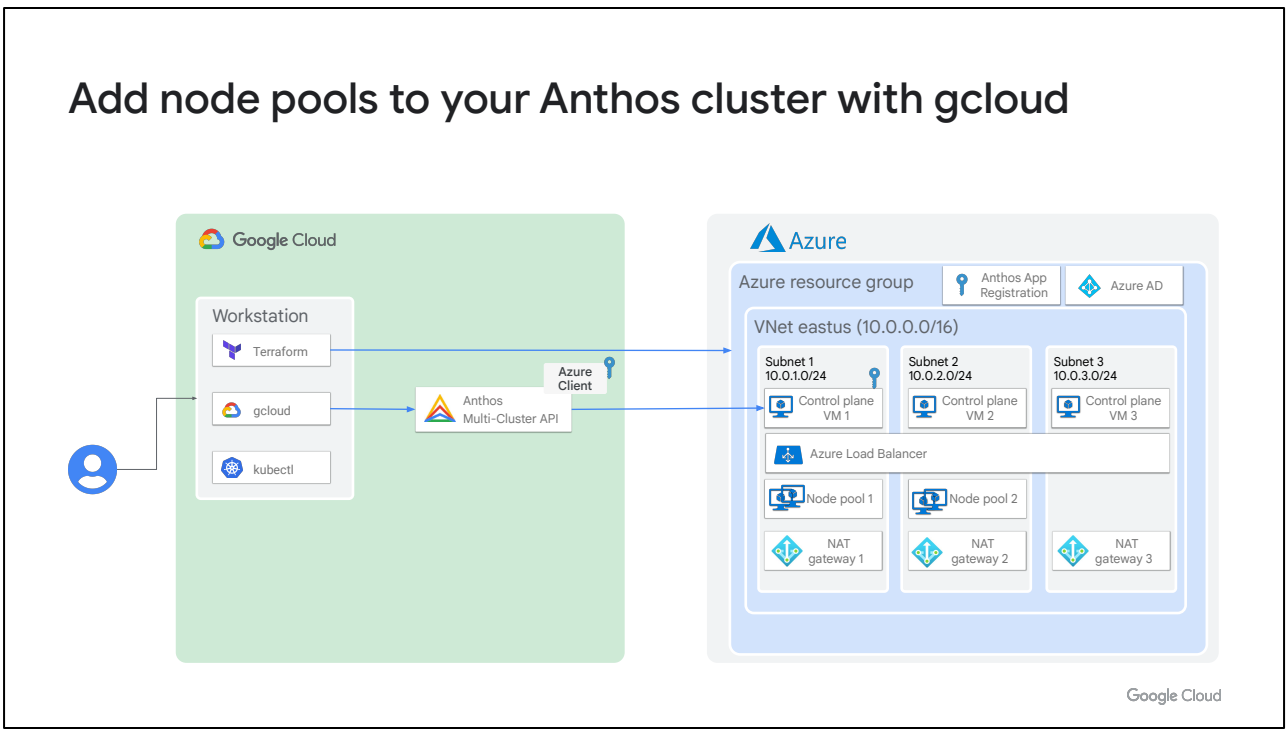


(6) Create an SSH key pair to enable encrypted communications with your cluster. In the cluster creation process, associate it with your control plane and node pool virtual machines.

Use gcloud to create your Anthos cluster on Azure

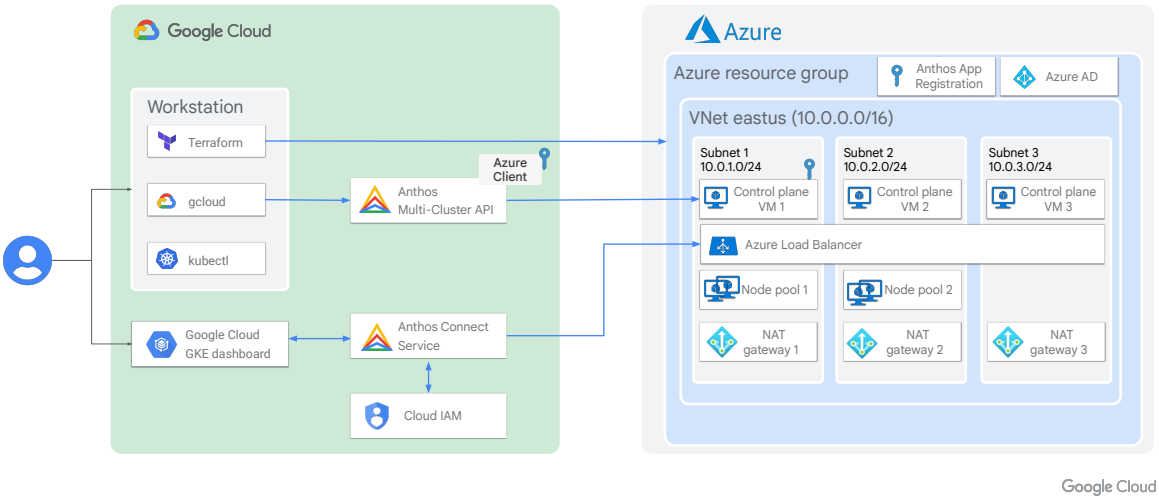


Use gcloud to create your Anthos cluster on Azure.



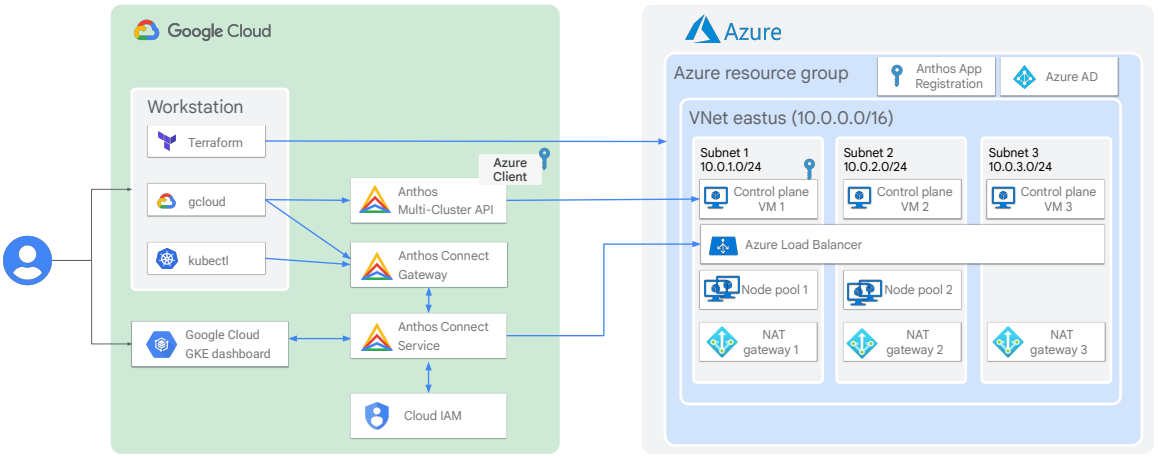
Add node pools to your Anthos cluster with gcloud.

Leverage Anthos Connect to view the cluster in the GKE console



To view the cluster in the GKE Console, leverage Anthos Connect.

Use Anthos Connect Gateway to work with your cluster using kubectl

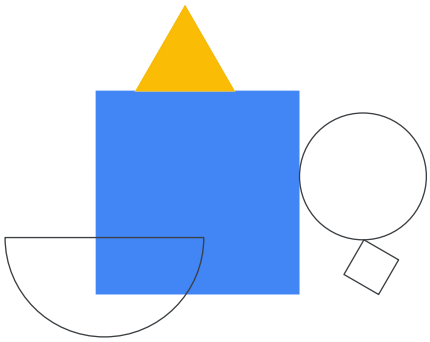


To work with your cluster using kubectl, use Anthos Connect Gateway.

Lab intro

45 min

Lab 021: Building Anthos Clusters on Google Cloud and AWS



In this lab, you deploy a GKE cluster and an Anthos cluster on AWS and register them to Anthos Hub. You access them from the Google Cloud Console and the terminal, and deploy an application to both clusters to experience the consistency across environments.

Questions and answers

1. What component is used to get cluster credentials to access the cluster through Google Cloud?

1. Anthos Identity Service
2. Anthos Connect Gateway
3. Anthos Connect Agent
4. Cloud Identity
5. IAM

1. What component is used to get cluster credentials to access the cluster through Google Cloud?

1 Anthos Identity Service	2 Anthos Connect Gateway
3 Anthos Connect Agent	4 Cloud Identity
5 IAM	

2. Anthos clusters on AWS install Anthos Service Mesh automatically.

1 True

2 False

2. Anthos clusters on AWS install Anthos Service Mesh automatically.

1 True

2 False

Google Cloud

False, it only installs an Ingress controller using the envoy proxy. This Ingress is composed of a deployment of Envoy proxy pods and a LoadBalancer Service for that istio-ingress deployment on the user cluster's ingress VIP specified on creation.

3. What tool is used to create Anthos clusters on Azure?

1. azurecli
2. gcloud
3. anthosgke
4. All tools above are needed

3. What tool is used to create Anthos clusters on Azure?

1. azurecli
2. gcloud
3. anthosgke
4. All tools above are needed