

# Google Distributed Cloud air-gapped racks

---

## At a glance

Google Distributed Cloud air-gapped (GDC) delivers a fully managed cloud experience with a rich set of IaaS services to enable lift and shift workloads and cloud native workloads. The system is designed from the ground up for organizations that require complete isolation to meet stringent sovereignty and regulatory requirements.

GDC air-gapped does not require connectivity to Google Cloud (public cloud) or the public internet to manage the infrastructure services and is built to operate in a persistent disconnected mode.





## Benefits



Optimized IaaS with fully integrated compute, storage and networking services for a wide range of enterprise and modern workloads, requiring sovereign security controls.



Extends Google Cloud IaaS patterns to deliver Google managed services like VertexAI, AlloyDB etc. with consistent developer experience.



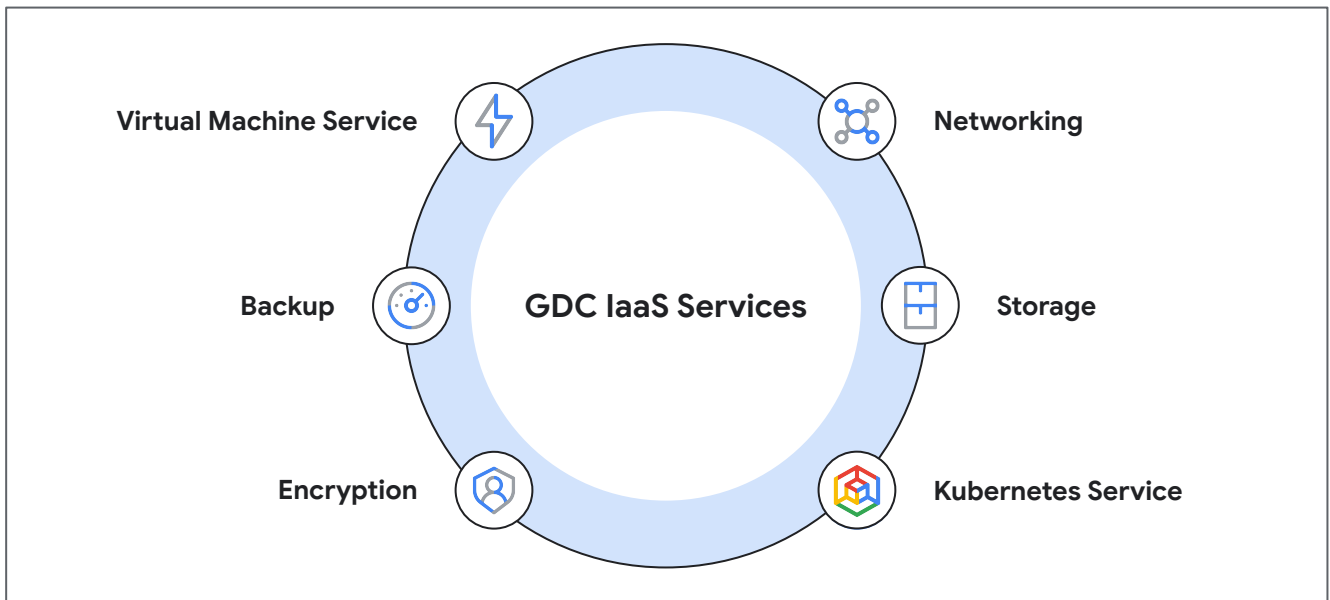
Industry leading application modernization platform for AI-led applications and container-native workloads.



IaaS services with multiple VM and storage types to adapt to optimize the workload needs.



Scales seamlessly from as low as 3 racks to hundreds of racks and supports Infra-as-a-code/GitOps style operations.



## Compute - VM

### Machine Families

N2 VM instances (Intel 4th Gen)  
A2 and A3 VM instances (Nvidia GPU enabled)

### Guest OS & Image Management

Linux & Windows VM instances  
BYO image pipeline

### Instance Operations

VM instance CRUD and power operations  
via API/UI  
UEFI Seca  
VM Observability



## Storage

### Block Storage

Balanced block Storage  
Local snapshots  
FIPS compliant encryption at rest and in-transit

### Object Storage

Standard object storage  
FIPS compliant encryption at rest and in-transit  
Object and bucket level encryption keys  
WORM buckets and retention lock

### Backup

VM and container backup & restore



## Compute - GKE Cluster

GKE Enterprise - Multi tenancy modes  
GPU & CPU capable node/node pools  
Network policy controls (Cilium CNI)

### Operations

Observability Dashboards



## Networking

### Interconnects

Shared & Dedicated Org Connectivity

### VPC Networking

Egress NAT  
VPC Flow Logs  
Managed VPN Gateway  
Firewall



## Service category: Compute - VM

| Services        | Key features                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VM families     | <p>GDC offers different Virtual Machine Families to suit different use cases covering a variety of general workload and specialized workload demands</p> <ul style="list-style-type: none"><li>• GDC <a href="#">N2</a> machine family (Intel 4th Gen)   general purpose compute <a href="#">N-series</a></li><li>• GDC A2 (Nvidia A100 GPUs) and <a href="#">A3</a> machine family for GPU-optimized workloads (Nvidia H100 GPUs)</li></ul> |
| VM guest images | <p>GDC VM Instances offer a wide range of Linux and Windows images to support diverse customer workloads:</p> <ul style="list-style-type: none"><li>• <a href="#">Linux</a> : GDC provided - Linux VM instances [Ubuntu 20.x, Rocky 8.x]</li><li>• BYO image [Ubuntu 20.x, RHEL 8.x, Rocky 8.x, <a href="#">Windows</a> server datacenter 2019]</li></ul>                                                                                    |
| VM security     | <p>Security and access mechanisms within the GDC architecture ensure secure boot and access:</p> <ul style="list-style-type: none"><li>• Guest BIOS   <a href="#">UEFI secured boot</a></li><li>• Guest access <a href="#">authentication</a> with user provided SSH keys</li></ul>                                                                                                                                                          |



## Service category: Compute - GKE Cluster

| Services                | Key features                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GKE Enterprise Clusters | <p>GDC empowers users to deploy modern applications using industry-leading GKE enterprise capabilities. GDC enables the deployment of Kubernetes-native container applications to air-gapped environments:</p> <ul style="list-style-type: none"><li>• <a href="#">GKE Enterprise</a> with single &amp; multi tenancy modes</li><li>• Cilium based CNI and network policy controls</li><li>• CPU &amp; <a href="#">GPU-enabled node pools</a></li></ul> |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cluster management</b>  | <p>GDC offers a comprehensive suite of services and features for deploying and managing GKE clusters:</p> <ul style="list-style-type: none"> <li>• <a href="#">Pod Autoscaling</a> : Horizontal pod autoscaler changes the shape of your Kubernetes workload by automatically increasing or decreasing the number of Pods in response to the workload's CPU or memory consumption.</li> <li>• Pre-built dashboards for cluster <a href="#">observability</a></li> <li>• <a href="#">Upgrade orchestrations</a> &amp; automated rollback</li> </ul> |
| <b>Container security</b>  | <p>GDC offers vulnerability scanning tools to help you detect and mitigate security vulnerabilities in your container images:</p> <ul style="list-style-type: none"> <li>• Vulnerability <a href="#">scanning</a> for container images</li> </ul>                                                                                                                                                                                                                                                                                                  |
| <b>Workload management</b> | <ul style="list-style-type: none"> <li>• Marketplace service Integration</li> <li>• Integrated <a href="#">container registry service</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                               |



## Service category: **Storage**

GDC air-gapped provides a comprehensive suite of managed storage services, equipped with data security, protection, and management features. These services are designed to cater to the diverse requirements of both enterprise and public sector workloads. GDC's current storage portfolio encompasses the following managed services and capabilities:

- Block storage Service
- Object storage Service
- Data security
- Data protection Services

| Services              | Key features                                                                                                                                                                                                                                                                                           |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Block storage</b>  | <p>GDC air-gapped offers durable block storage for VM and container workloads that provide:</p> <ul style="list-style-type: none"> <li>• GDC balanced (3 IOPS/GiB) block storage for <a href="#">VMs</a> and <a href="#">containers</a></li> <li>• Organization level storage multi-tenancy</li> </ul> |
| <b>Object storage</b> | <p>GDC air-gapped offers a scalable and durable managed object storage service that provides:</p> <ul style="list-style-type: none"> <li>• <a href="#">GDC standard object storage class</a></li> <li>• Organization level storage multi-tenancy</li> </ul>                                            |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data security</b>   | <p>GDC air-gapped storage offers zero-trust security that aligns with the most rigorous data security and compliance standards. Key benefits include local data storage, encryption key management, and data access control:</p> <ul style="list-style-type: none"> <li>• FIPS compliant encryption at <a href="#">rest</a> and in <a href="#">transit</a></li> <li>• Object and bucket level encryption   <a href="#">CMEK</a></li> <li>• Client side encryption (block storage)</li> <li>• WORM buckets   bucket retention lock</li> </ul> |
| <b>Data protection</b> | <p>GDC air-gapped storage offers advanced data protection, including backup, and data transfer capabilities, ensuring durability and availability:</p> <ul style="list-style-type: none"> <li>• Snapshot-based <a href="#">backup and restore</a> - VM &amp; containers</li> <li>• <a href="#">Online storage data transfer service</a></li> </ul>                                                                                                                                                                                           |



## Service category: **Networking**

GDC air-gapped networking delivers secure, high-performance networking for both compute services and cloud storage. It incorporates:

### Physical Networking

Comprising dataplane and management networks, it connects all cloud components including ingress/egress connectivity and provides network isolation between organizations.

### Cloud Networking

Facilitates VPC connectivity between workloads within a single organization. Additionally, it offers VPC networking services, including load balancers, NAT, and flow logs.

| Services                           | Key features                                                                                                                                                                                                                                                                                                                        |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Physical dataplane network</b>  | <p>The physical dataplane network is used to carry traffic for all customer workloads and GDC software components:</p> <ul style="list-style-type: none"> <li>• Two-tier, non-blocking fabric.</li> <li>• Up to 1.6 Tbps uplink bandwidth per rack.</li> <li>• Redundant switches and connections for high availability.</li> </ul> |
| <b>Physical management network</b> | <p>The physical management network is a completely separate physical network for out-of-band management connectivity to the physical nodes.</p>                                                                                                                                                                                     |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Interconnect</b>  | <p><a href="#">Interconnects</a> provide redundant external connectivity to customer networks, other GDC zones, and operations infrastructure rack (OIR) via a dedicated set of switches:</p> <ul style="list-style-type: none"> <li>• <b>Customer networks:</b> Flexible 10, 100, 400 Gbps connectivity to dedicated or shared external networks.</li> <li>• <b>Multi-zone:</b> Connectivity to external routers with speeds up to 400 Gbps. Optional, third-party high-grade crypto device integration.</li> <li>• <b>Operations infrastructure rack (OIR):</b> 100 Gbps connectivity to OIR for connectivity to operations suite facility (OIF).</li> </ul> |
| <b>Egress NAT</b>    | <p><a href="#">Egress NAT</a> allows customers to control how instances with private IP addresses can communicate with the internet or other networks. This feature provides egress NAT configurations to both virtual machine and containerized workloads.</p>                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>VPC flow logs</b> | <p><a href="#">VPC</a> flow logs allow customers to capture and save network traffic metadata for analysis and troubleshooting. By leveraging the flow logs feature, you can effectively monitor and manage your network environment in GDC, ensuring the smooth and secure operation of your applications and workloads.</p>                                                                                                                                                                                                                                                                                                                                  |
| <b>VPN</b>           | <p><a href="#">VPN</a> securely extends a peer network to a user's virtual machine (VM) in an organization of a GDC zone through an internet protocol security (IPsec) VPN connection. Customers can configure gateways, dynamic routing, and tunnels, while also controlling egress and ingress traffic to their VPN tunnel.</p>                                                                                                                                                                                                                                                                                                                              |
| <b>Firewall</b>      | <p><a href="#">Firewall (project network policies)</a> provides a security control over network traffic flow at the project level. They determine how workloads and services within a project can communicate with each other and with external resources. Policies define either ingress (incoming) or egress (outgoing) rules, but not both in the same policy.</p>                                                                                                                                                                                                                                                                                          |

