A Technical Guide to running VMware based applications in Google Cloud

Google Cloud

Contents

Executive summary

Moving your VMware based applications to the cloud is often a complex and costly process. IT has to grapple with re-architecting applications, changes to networking and tools, and in many cases, app modification for those that are not able to run in the cloud.

Google Cloud VMware Engine simplifies cloud migration and frees IT from the operational overhead of managing physical infrastructure, helping reduce the operational burden and costs of migrating and managing VMware applications. By migrating your VMware applications to Google Cloud, you can continue to leverage your existing investments in VMware, utilize the same tools, processes, and policies, while increasing business agility, security and availability.

This paper provides deeper insights into how VMware Engine facilitates migrating your applications to Google Cloud and helps you understand the impact on networking, security, monitoring, and maintenance.

Introducing Google Cloud VMware Engine

Google Cloud VMware Engine is a fully managed VMware-as-a-Service product that enables businesses running on-premises VMware workloads to seamlessly migrate to Google Cloud without needing to re-architect or refactor their applications. Your VMware environment – including its components vSphere, vCenter, vSAN, NSX-T, and corresponding tools – continues to run natively in a dedicated and private, software-defined data center stack on Google Cloud's bare metal infrastructure located in Google Cloud data centers. Essentially, you get to leverage your existing VMware investments, tools, processes, and skills to maintain operational continuity, while avoiding data center management, hardware refreshes, and procurement cycles. Vmware Engine is sold and supported by Google and is VMware 'Cloud Verified'.

Because VMware Engine is 100% compatible with your VMware workloads, many of your typical applications can be migrated without change or having to use a new application in the cloud. Common workloads include Virtual Desktop Infrastructure (VDI) to enable employees to work from anywhere, and moving DR and Backup targets to the cloud to reduce TCO. In addition to the ease of migration, you can also benefit from bringing your existing data to Google Cloud and leveraging high speed access to native Google Cloud Services such as AI, ML, Anthos and BigQuery.

This paper provides a technical overview of VMware Engine, covering key features and capabilities, in addition to highlighting areas of consideration before you take positive steps towards modernizing your IT infrastructure.

Architecture overview

VMware Engine provides a dedicated private cloud, composed of a hyperconverged compute, storage, and networking stack deployed on Google Cloud infrastructure in various Google Cloud locations worldwide.

Each private cloud contains one instance of the vCenter Server, which manages multiple ESXi nodes contained in one or more vSphere Clusters, along with the corresponding Virtual SAN (vSAN) storage. VMware Engine is sold by the node, with the minimum configuration of three nodes up to a maximum of 64 nodes per private cloud and you can create any number of private clouds.

By running your workloads on a native VMware environment running in a dedicated VMware software stack on Google Cloud, you can migrate and run any of your on-premise virtualized workloads in Google Cloud with no changes. You use the same VMware tools you are already familiar with – including vSphere, vCenter, vROPS and vMotion, for example. All the VMware licenses needed to run the service are included: ESXi, vCenter, vSAN, NSX-T, and HCX.

Each node consists of all the compute, memory, and storage you need. The initial node configuration is:

- CPU: Intel Xeon Gold 6240 (Cascade Lake), 2.6 GHz (x2), 36 Cores, 72 Hyper-Threads
- Storage: 2 × 1.6 TB (3.2 TB) NVMe (Cache), 6 × 3.2 TB (19.2 TB) NVMe (Data)
- Hyperconverged design using vSAN

The all-flash NVMe-based storage can support the speed and performance required for demanding workloads, such as Oracle, SQL Server, SharePoint, Microsoft Exchange Server, and VDI running on VMware. VMware Engine also has the ability to reduce the core count in the nodes to align with licensing restrictions of third party software.

Customers have various service options for storage targets, including:

Local storage on the hyper-converged platform (vSAN)

It offers low-cost storage due to compression and dedupe abilities of vSAN (dependent on data redundancy) while providing single location high availability

Multiple storage options (e.g. Elastifile Cloud Files, NetApp Cloud Volumes)

These are good for primary or secondary (backup) storage due to single location availability and lower costs

Google Cloud Storage

This is best for secondary storage, image files, ISOs, and so forth. It can offer the lowest cost and largest variety of storage options across multiple regions

Networking

Networking is a key feature of the service, providing high speed, secure access to your applications as well as secures all traffic between your applications and Google Cloud Services. You can provision NSX-T network overlays (and their subnets), create firewall tables, and assign public IP addresses that map to a virtual machine running in your private cloud.

Google supports the following connectivity options to connect to your VMware Engine region network, multiple of which can be used at the same time:

Direct Interconnect connection from your on-premises data center to VMware Engine on Google Cloud region network

This is a high-speed, low-latency, secure private connection that bridges your on-premises circuit to your Google Direct Interconnect circuit.

Direct Interconnect connection from your virtual private cloud to your VMware Engine region network

This is a high-speed, low-latency, secure private connection that uses virtual network gateways to bridge your virtual network on Google Cloud to your VMware Engine circuit.

Cloud VPN securely connects your peer network to your virtual private cloud (VPC) network through an IPsec VPN connection

Traffic traveling between the two networks is encrypted by one VPN gateway, and then decrypted by the other VPN gateway. This protects your data as it travels over the internet. You can also connect two instances of Cloud VPN to each other.

Google Direct Interconnect or VPN are supported for communicating with and migrating workloads to your dedicated cloud. Point-to-Site VPN is supported for remote/quick access to VMware Engine and you can control which users can access the VMware environment.

The service provides fully redundant networking (via multiple TORs) and direct integration into your dedicated cloud, enabling the use of Cloud Interconnect and Cloud VPN. Further, it is integrated in Google Cloud billing, identity management, and access control to simplify management.

Each node includes four NICs operating at 25 Gbps throughput each for a total of 100 Gbps, providing high-speed, low-latency access to services via VPC peering. For example, you can deploy your customer database in a dedicated cloud and access the application servers in Google Cloud with millisecond response times.

Questions to consider

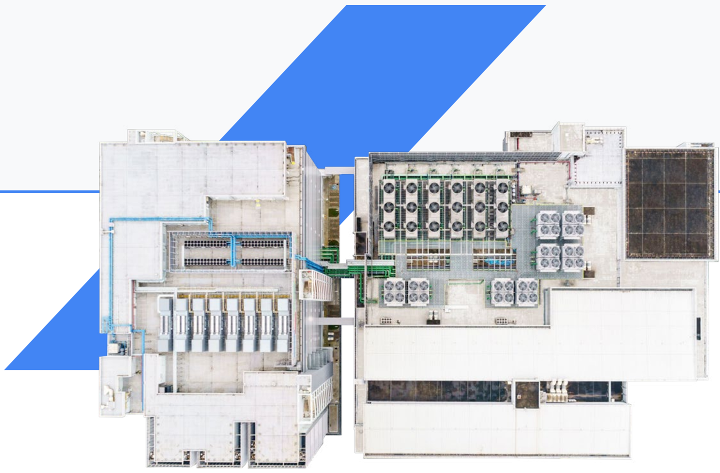
1. How do you intend to connect your applications to Google Cloud; via Direct Interconnect or VPN?
2. Do you want high-speed, low-latency access to these innovative products and services?

Leverage innovative tools by Google, VMware and trusted third-parties

Another powerful advantage of VMware Engine is that it enables access to the entire vSphere ecosystem of trusted third-party IT management tools, as well as the complete core vSphere platform and its default interface, vCenter.

You can leverage a wide array of capabilities – including provisioning, monitoring, support, inventory management, backup and disaster recovery, security, network and IP address management, identity management – all of which are managed through a single pane of glass. For backup and disaster recovery, we're currently working with the following partners to integrate their offerings with the service: Cohesity, NetApp, Veeam, and Zerto.

VMware Engine offers privilege elevation, which allows you to install and manage third party applications which require administrative access to vCenter. At your request, your privileges can be upgraded for up to a 24-hour period to make limited configuration changes to the vCenter, after which the environment is automatically locked for security. Applications like Zerto for DR are fully supported with this feature.



On-boarding and migrating workloads via VMware HCX and vMotion

The service supports all standard VMware migration tools like vMotion and HCX. vMotion is best for migrating individual workloads without interrupting the service. In this deployment scenario, you connect your private cloud to your on-premises environment using a dedicated interconnect tunnel that allows on-premises management and vMotion subnets to communicate with the private cloud management and vMotion subnets. This allows for Cross vCenter vMotion (xVC-vMotion).

A full HCX license is also included, allowing you to migrate workloads en masse, while enabling L2 connectivity and vMotion or Storage vMotion workflows without changing the IP address. The time to execute migrations is based on the number and size of your workloads, as well as the speed and bandwidth of your connectivity.

Questions to consider

1. Do you want to take advantage of the most innovative products and services in the market that are fully compatible with your infrastructure?
2. Do you want high-speed, low-latency access to these innovative products and services?

Continuous monitoring while you focus on what matters

For IT teams, monitoring the performance and availability of operating systems, middleware, and applications running across physical, virtual, and cloud environments internally is complex and time-consuming, making it unfeasible to innovate.

With VMware Engine, the level of probes and error logs best-suited for your business is established automatically. The solution has a continuous performance monitoring subsystem so that issues can be detected and resolved quickly. For example, if a hardware failure is detected, a new node is added to your private cloud and the failed node is removed.

Maintenance, Patches, Upgrades, and Change Windows

As with any cloud service, taking time to patch and upgrade the underlying software is critical to ensuring security and access to the latest features. Google Cloud has a standard process we are committed to for patching the underlying VMware software. All of the patching for applications and software running on the VMware environment is the user's responsibility.

Questions to consider

1. Do you want the ability to increase or decrease capacity on demand?
2. Do you want to optimize capacity expenditure?

Backend/internal maintenance

System maintenance typically involves reconfiguring physical assets or installing software patches. It doesn't affect normal consumption of the assets being serviced. With redundant NICs going to each physical rack, normal network traffic and private cloud operations aren't affected. You might notice a performance impact only if your organization expects to use the full redundant bandwidth during the maintenance interval.

Portal maintenance

Some limited service downtime is required when the control plane or infrastructure is updated. Currently, maintenance intervals can be as frequent as once per month. The frequency is expected to decline over time. Notification is provided for portal maintenance and efforts are made to keep the interval as short as possible. During a portal maintenance interval, the following services continue to function without any impact:

- VMware management plane and applications
- vCenter access
- All networking and storage

VMware infrastructure maintenance

Occasionally it's necessary to make changes to the configuration of the VMware infrastructure. Currently, these intervals can occur every 1-2 months, but the frequency is expected to decline over time. This type of maintenance can usually be done without interrupting normal private cloud consumption. During a VMware maintenance interval, the following services continue to function without any impact:

- VMware management plane and applications
- vCenter access
- All networking and storage

Updates and upgrades

Google is responsible for lifecycle management of VMware software (ESXi, vCenter, vSAN, PSC, and NSX) in the private cloud.

Software updates include:

Patches	Updates	Upgrades
Security patches or bug fixes released by VMware.	Minor version change of a VMware stack component.	Major version change of a VMware stack component.

Critical security patches are tested as soon as they become available from VMware. Per our SLA, the security patch is rolled out to private cloud environments within a week.

Quarterly maintenance updates apply VMware software components. When a new major version of VMware software is available, we work with customers to coordinate a suitable maintenance window for upgrade.

Questions to consider

1. Do you want to ensure your applications and hardware performance are continuously monitored while you focus on more important business initiatives?
2. Do you want to ensure issues are detected and resolved quickly and comprehensively?

Secure by design

Since all the edge-type networking services of VMware Engine – including VPN, public IP, and internet gateways – run on Google Cloud, they inherit the baseline network security and DDoS protection provided by Google Cloud. This applies to both Google Cloud and the dedicated private VMware environment.

In particular, VMware Engine has separate Layer-2 networks that restrict access to your own internal networks in your private cloud environment. You can easily define east-west and north-south network traffic control rules for all network traffic, including intra-private cloud traffic, inter-private cloud traffic, general traffic to the internet, and network traffic to on-premises.

Security is additionally delivered at the hardware level. As part of the service, all customers get dedicated bare metal hosts with local attached disks that are physically isolated from other hardware. An ESXi hypervisor with vSAN runs on every node and the nodes are managed through customer-dedicated VMware vCenter and NSX.

Questions to consider

1. Do you want a service that guarantees multiple layers of network security?
2. Do you want the ability to manage network security easily, efficiently, and reliably?

Protecting critical data

With VMware Engine, you can ensure data at rest and data in transit are protected.

Data at rest in the private cloud environment can be encrypted using vSAN software-based encryption. This type of encryption works with certified third-party key management servers located in your own network or on-premises, and you can easily control and manage the encryption keys yourself.

For data in transit, applications are expected to encrypt their network communication within the internal network segments. vSphere supports encryption of data over the wire for vMotion traffic.

To protect data that moves through public networks, you can create IPsec and SSL VPN tunnels for your private clouds. Common encryption methods are supported, including 128-byte and 256-byte AES. Data in transit – including authentication, administrative access, and customer data – is encrypted with standard mechanisms, such as SSH, TLS 1.2, and Secure RDP.

Questions to consider

1. Do you want to ensure data at rest and data in transit across your cloud environments can be reliably protected?
2. Do you want access to best-in-class security capabilities from VMware and Google Cloud?

Take the next step

Regardless of what your "why" is, it is important that any technology you adopt is aligned with the goals, needs, and objectives of the business. There is no one-size-fits-all model that can be implemented across the board. This is why you need a comprehensive solution that can adapt to and grow with your business.

So, tell us what you're solving for and one of our experts will help you find the best solution.

For detailed specifications, visit the Google Cloud VMware Engine website or contact sales.