Publication date:
May 2025
Author:
Roy Illsley

Publication date:
May 2025
Author:
Roy Illsley

From VMware to Distributed Cloud: A Practical Guide for Enterprise Virtualization Transformation

Commissioned by:

Commissioned by:

Contents

contained in the white paper for any purpose. This white paper has not been reviewed, approved or disapproved by regulatory authorities of any jurisdiction. Any reliance you place on such information in this white paper is therefore strictly at your own risk.

YOU SHOULD CONSULT YOUR OWN TECHNICAL, LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION WITH THE INFORMATION PROVIDED IN THE WHITE PAPER.

Catalyst

The acquisition of VMware by Broadcom in 2023 and the subsequent changes made to VMware's licensing and products have seen increased speculation about customers' plans to migrate off VMware. Omdia was asked by Tencent Cloud to conduct an independent survey of VMware customers to understand the customer sentiment and propensity for any such migration.

Omdia view

VMware has been the dominant vendor in the software virtualization market for the past 20 years. However, it was acquired by Broadcom in 2023 for $69bn. Since the acquisition closed, Broadcom has made some significant changes to the pricing, product packaging, and partner network. The response from VMware customers was vocal and loud, and according to Omdia's survey, 73% of VMware customers are considering moving away from a VMware solution in the next three years. Many believe that making the shift from virtual machines (VMs) to a Kubernetes environment will be the path taken by these disgruntled VMware customers. However, while 66% of VMware customers are currently running Kubernetes, 79% of these Kubernetes deployments are run on VMs. Therefore, Omdia believes VMs will remain a critical part of an organisation's software environment for the foreseeable future—meaning any decision to move away from VMware technology represents a solid market opportunity for those competitor solutions.

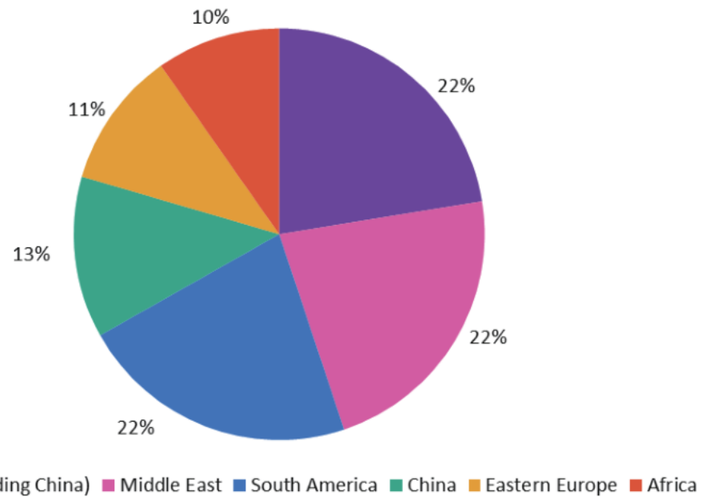
Key messages

- The move to a subscription model is the biggest influence on the decision to move off VMware.
- Customers are looking for any VMware alternative to deliver superior TCO compared to VMware.
- VMware customers looking to perform a like-for-like migration want integrated security features.
- Barriers to moving away from VMware differ depending on migration intention.
- Fully integrated hybrid cloud solutions are the most popular choice for moving away from VMware.
- It's crucial to provide solutions that enable customers to adopt public cloud flexibility on-premises, which delivers data privacy.
- Tencent's approach to adopting cloud native technology offers customers choice.
- Customers want improved security, better reliability and increased performance.

Survey demographics

The survey asked VMware customers from Asia and Oceania, the Middle East, South America, China, Eastern Europe and Africa (see **Figure 1** for the distribution of these customers) about their motivations and expectations from any VMware alternative provider. The survey only selected those respondents who indicated they are seriously considering, planning or in the process of migrating off VMware after the acquisition of VMware by Broadcom in 2023.

Figure 1: Regions and countries covered in the survey



Source Omdia

The survey was restricted to decision-makers in organisations with an annual revenue of over $250m in the banking and financial services, retail, manufacturing and government sectors.

Survey results

Understanding the VMware environment in organisations

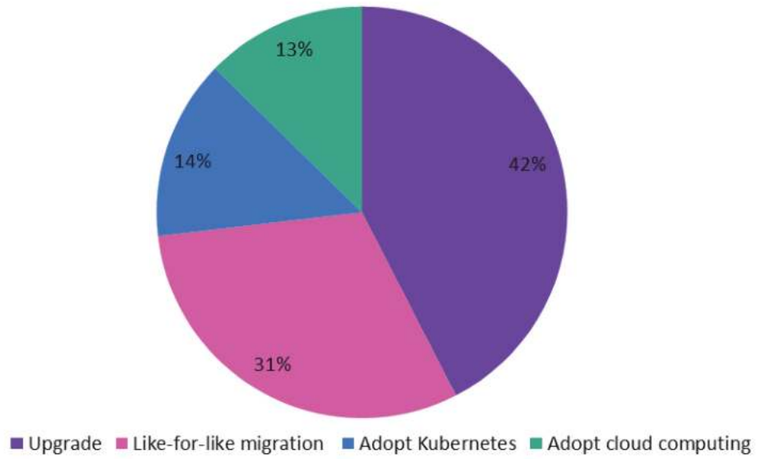
Over 37% of the respondents stated they spent over $1m per year on VMware, with 34% spending between $500,000 and $1m. The average cost per VM was $313,000, and the majority of organisations (41%) run between 500 and 999 virtual machines (VMs), with 26% running more than 1,000 VMs. The density of VMs per host is evenly distributed, with 41% reporting running between 10 and 24 VMs per host, and the same number reporting running between 25 to 49 VMs per host, with 12% running less than 10 VMs per host. Most commonly, 45% of organisations reported using between 100GB and 999GB of vSAN storage in production environments, with 36% having between 1TB and 99TB. Overall, 52% of respondents stated that VMware VMs accounted for between 25% and 49% of their production workloads, with 35% noting that 50% to 74% of production workloads are run on VMware VMs.

The move to a subscription model is the biggest influence on the decision to move off VMware

Overall, the decision by VMware to mandate customers to adopt a subscription model was the biggest reason respondents gave for considering a move off VMware. Interestingly, there was no direct correlation between the amount of spending on VMware and the most important factor that caused customers to move off VMware. Analysis shows the responses by amount of spend with VMware differed between these groups. For those spending less than $499,000 and those spending more than $5m, they identified the move to a subscription model as the most important reason. However, for those spending between $500,000 and $999,000, concerns about Broadcom's future intentions was the top reason, with subscription a close second. However, for the group of those spending between $1m and $4.99m, the shift from CPU licensing for vSphere and vSAN was the biggest reason, with the increased cost to run the same number of VMs second and subscription third.

Figure 2 shows the intentions of those planning to move away from VMware.The most common migration was to upgrade the VM technology used and adopt the latest capabilities, with 42% of all respondents stating this was their intended migration plan. The second most common intention was to perform a like-for-like migration, with 31% of respondents. The third option is to shift to Kubernetes (14%) or adopt public cloud services (13%).

Figure 2: Migration plans of respondents planning to move away from VMware

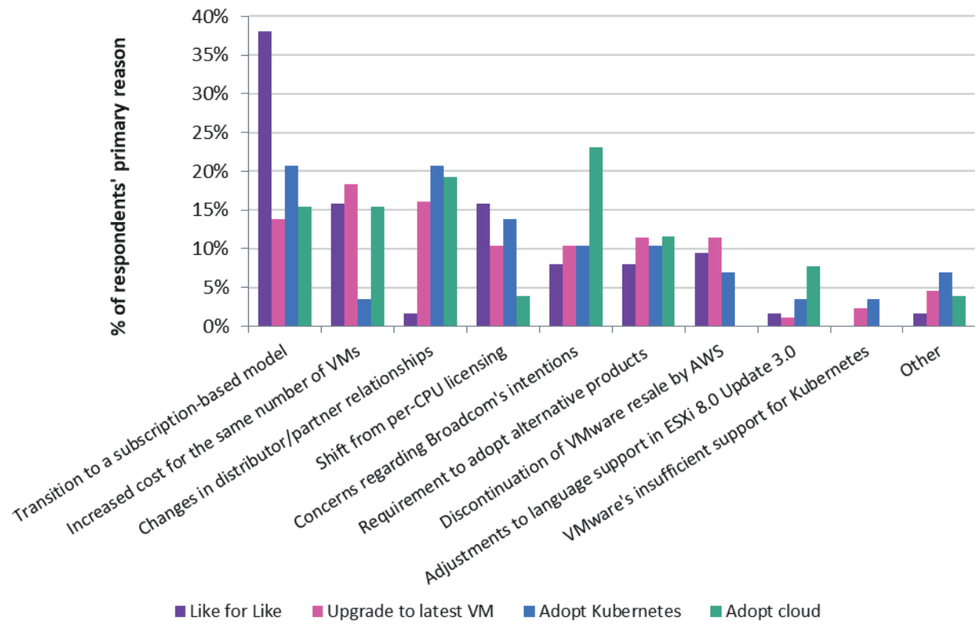


Source Omdia

Figure 3 shows the motivation to move off VMware by the intended type of migration. The impact of the mandate to adopt a subscription model is the main reason given by those adopting a like-for-like move off VMware, with 38% putting it as the most important reason, 22 percentage points more than the second most important reason—the shift from a per CPU licensing model for vSphere and vSAN. For those looking to upgrade their virtualization environment as part of the move from VMware, the primary reason is less clear. The most common reason for this group was the increased price for the same number of VMs, 18%, with changes to the partner network second, 16%, and subscription pricing third, 14%. This lack of a clear reason why this group is considering moving from VMware can be attributed to the fact that any upgrade of VM capabilities is likely to be more complex and require assistance from partners. Also, the need to adopt the newer packages from VMware will increase the cost.

For those planning to adopt Kubernetes or move to the cloud, the reasons for considering moving off VMware were also different. For the group adopting the cloud, concern over Broadcom's future intentions was the top reason for them moving away from VMware and virtualization in general. For those adopting Kubernetes, the joint most important reason was the change to subscription and the changes to the partner network—both at 21%. This reason changed for those already running Kubernetes, where the subscription model was the top incentive (23%).

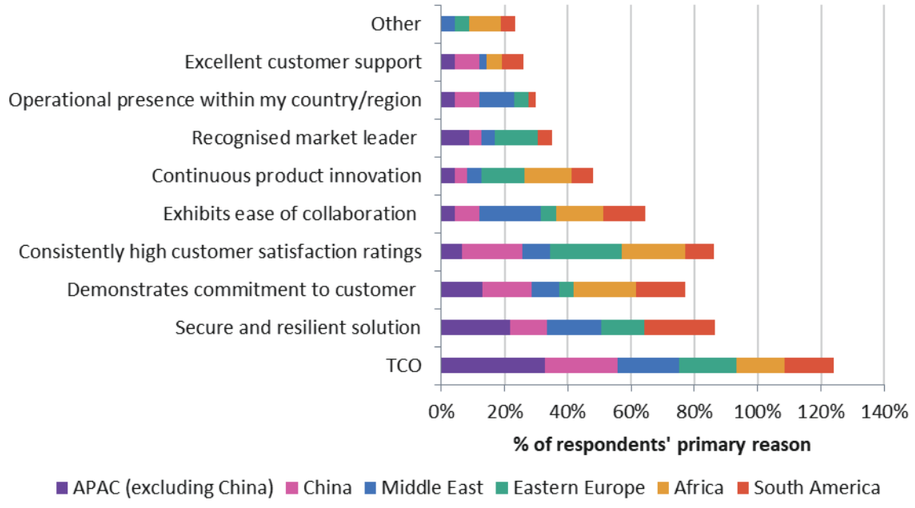
Figure 3: Primary reason to move off VMware by type of migration



Customers are looking for any VMware alternative to deliver superior TCO compared to VMware

Overall, 22% of respondents put superior TCO as the most important characteristic of any VMware alternative provider, with security and resilience as the second most important, at 17%. However, the characteristics customers are looking for change when viewed by country/region (see **Figure 4**). In Asia & Oceania (excluding China), China, and the Middle East, TCO was the most important characteristic, with 33%, 23%, and 20%, respectively. Whereas in Eastern Europe and Africa, customer satisfaction rating was the most important, with 21%; in South America, security and resilience was the most looked-for characteristic (22%).

Figure 4: Most important characteristic of any VMware alternative provider by country/region



Source Omdia

TCO is the most essential characteristic for all categories of spending on VMware, except for the $500,000 to $999,000 group, which accounts for 34% of the survey, where TCO was joint top with security and resilience. This compares to those that spend more than $1m per year with VMware, where TCO was the most important consideration (at 22%), demonstrating a commitment to the customer was second with 16%, and security and resilience and customer satisfaction were joint third, at 13%. These expectations from any VMware alternative provider are a result of how the customers rate VMware after the acquisition. For example, of those spending more than $1m per year, only 9% rated VMware as excellent, while 23% rated VMware as poor or inadequate in terms of TCO.

Tencent Cloud VMware alternative solution can offer an improved TCO. For example, with 5,000 vCPUs, the three-year total cost of ownership on Tencent Cloud is approximately 70% of VMware's. As the scale increases, the total cost of ownership will become even lower.

VMware customers looking to perform a like-for-like migration want integrated security features

The survey asked existing VMware customers to name the top three most important attributes of the product they consider when selecting a VMware alternative. For those planning a like-for-like alternative, 37% put integrated security as part of the core offering as the top requirement, followed by delivering the best price/performance, with 33%. However, for those looking to upgrade their virtualization capability as part of any move away from VMware, price/performance was the most important attribute (33%) and flexible pricing models was second, at 31%.

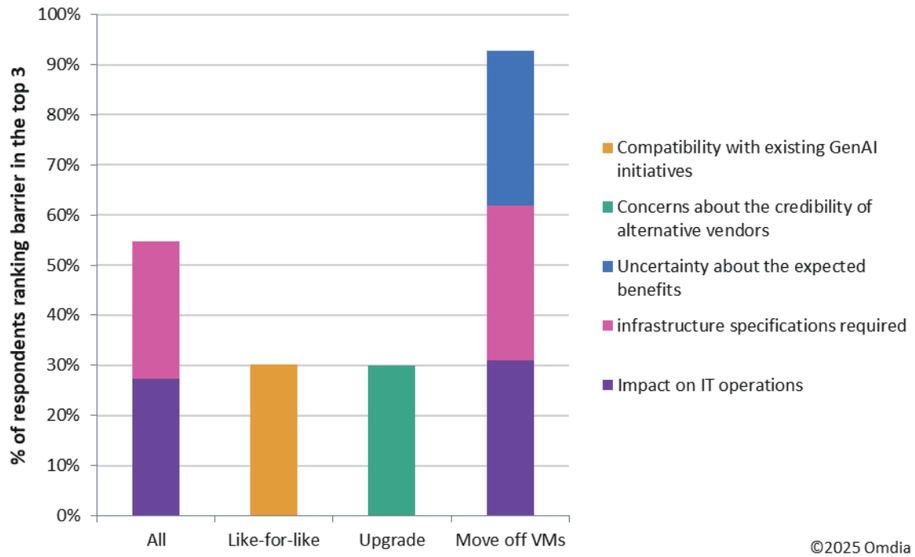
Customers looking to adopt a like-for-like alternative to VMware reported that integrated security was a priority; this finding was supported by how this group of customers rated VMware in terms of security breaches. For the like-for-like group, 19% reported security breaches all or most of the time, compared to the group looking to upgrade, where only 9% reported security breaches all or most of the time. These different experiences with VMware also depend on how much of the production workload is run on VMware. For example, of those that run more than 75% of their workload on VMware, 21% reported security-related issues all or most of the time, compared to 12% who run less than 50% of their production workloads on VMware. The clear implication is that the greater the scale of use of VMware, the more unhappy customers are with the security aspects.

Tencent Distributed Cloud (CDC/CDZ)/Tencent Cloud Enterprise (TCE/TCS) provides a one-stop service in terms of security, which includes host security, container security, web application firewall (WAF), cloud firewall, threat traffic analysis, network intrusion protection, data security auditing, security posture awareness, key management services, credential management systems, bastion hosts and more. These capabilities can help customers better defend against security issues.

Barriers to moving away from VMware differ depending on migration intention

Figure 5 shows respondents' top barriers to moving away from VMware by the migration intention. Across all respondents, the joint top barriers were the impact on IT operations and understanding the infrastructure requirements to support any move. VMware competitors can easily mitigate these concerns; vendors could provide VMware customers with the information needed about infrastructure requirements by offering a migration assessment tool. Any alternative technology must have a similar look and feel and include automation to mitigate the impact on IT operations. For those customers looking to adopt a like-for-like alternative to VMware, the top barrier was ensuring no impact on the current investment in GenAI. Omdia considers that this must be a key aspect of any like-for-like alternative solution: it must support the same hardware and software packages that VMware supports.

Figure 5: Top barriers to adopting VMware alternatives by intended migration strategy



Source Omdia

The top concern for those planning to upgrade the existing VMware estate to include the latest virtualization capabilities is focused on the credibility of the alternative vendors. This concern is exemplified by the response to questions asking customers to rate VMware post-acquisition on several different attributes. VMware scored well for product performance, where 60% of respondents rated VMware as good or excellent, and 57% rated VMware's product innovation as good or excellent. The concerns of those planning to move away from VMs or adopt Kubernetes or cloud are related to a lack of knowledge about the benefits, the infrastructure needed and the impact on operational skills and processes.

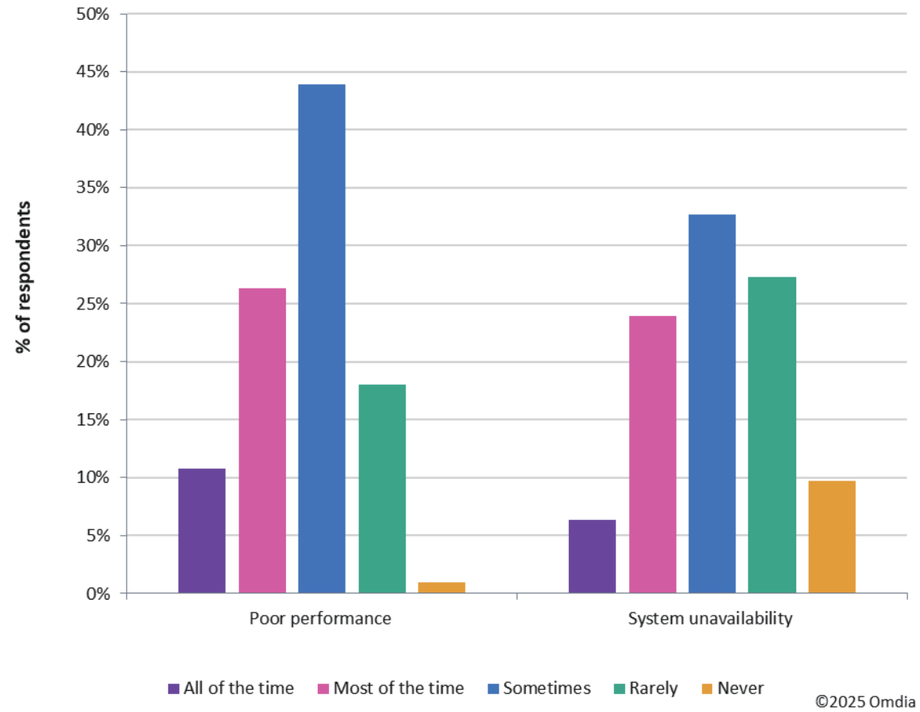
Tencent Distributed Cloud (CDC/CDZ)/Tencent Cloud Enterprise (TCE/TCS) provides a comprehensive product catalogue, enabling support for the migration and upgrade of existing VMware environments. It also offers tools such as go2TencentCloud to migrate business systems from VMware to Distributed Cloud/TCE via hot migration/cold migration methods. In a case study involving a city commercial bank, TCE successfully migrated hundreds of VMware virtual machines running 130 business systems to the cloud within 8 hours.

Security and reliability are the top two benefits customers are expecting from a move away from VMware

The top two reported benefits customers are expecting from any move away from VMware are improved security posture and fewer incidents (35%) and enhanced reliability and increased up-time

(33%). These expectations are supported by the rating customers gave VMware for performance and reliability after Broadcom's acquisition (see **Figure 6**). In terms of performance, 37% of respondents stated they experienced performance issues with VMware all or most of the time. In fact, only 1% reported never experiencing a performance issue, while 30% of respondents stated they experienced system unavailability issues with VMware all or most of the time, and only 10% reported never having any availability issues.

Figure 6: Customer's rating of VMware

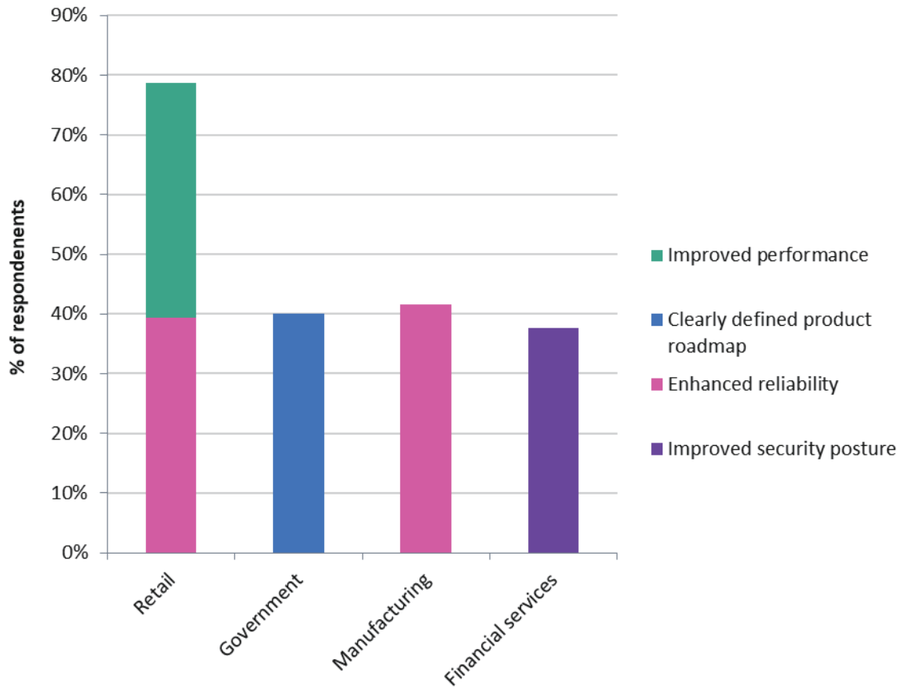


Source Omdia

The expected benefits of moving away from VMware differ by industry (see **Figure 7**). Retail reported that reliability and performance were the joint top benefits, which is supported by retail's experience of VMware for these two attributes. Retail reported poorer than the survey average, with 0% never experiencing poor performance and 41% reporting that performance was an issue all or most of the time. Retail customers' experience of VMware for reliability was also poorer than the survey average, with 5% reporting never having reliability issues and 38% reporting reliability was an issue all or most of the time. Manufacturing reported that reliability was the top benefit, and for

financial services, improved security was the top benefit. These results further indicate that VMware customers are unhappy with security, reliability, and performance. However, government customers' top benefit was having a clearly defined roadmap for the product.

Figure 7: Top benefits of moving away from VMware by industry



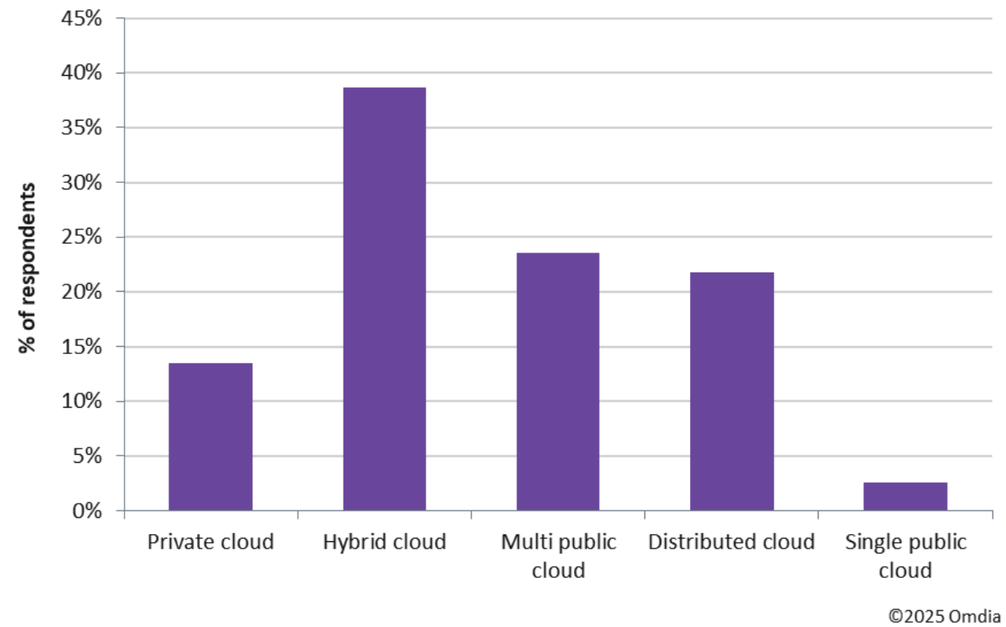
Source Omdia

Tencent Distributed Cloud (CDC/CDZ)/Tencent Cloud Enterprise (TCE/TCS) adopts a fully distributed architecture, supporting online horizontal scalability for performance expansion. Its architecture design decouples the control plane from the data plane, ensuring uninterrupted service even in the event of a single-node failure.

Fully integrated hybrid cloud solutions are the most popular choice for moving away from VMware

Currently, VMware customers report that 39% of their production workloads are run in a hybrid cloud environment, and this will increase to 42% once these customers have migrated to VMware alternatives. The survey showed that the driver for hybrid cloud solutions was customers prioritizing a vendor with a local presence for data sovereignty reasons. In fact, 63% of respondents agreed or strongly agreed with that statement. Even more respondents (79%) agreed or strongly agreed with the option to choose a VMware alternative that provides a fully integrated hybrid cloud solution. When it comes to selecting the alternative vendor, the need for a local presence and a fully integrated hybrid cloud solution becomes obvious. **Figure 8** shows that, currently, hybrid cloud is the cloud architecture of choice for the survey respondents.

Figure 8: Distribution of current cloud architecture



Source Omdia

Tencent Cloud's architectural approach to VMware alternative

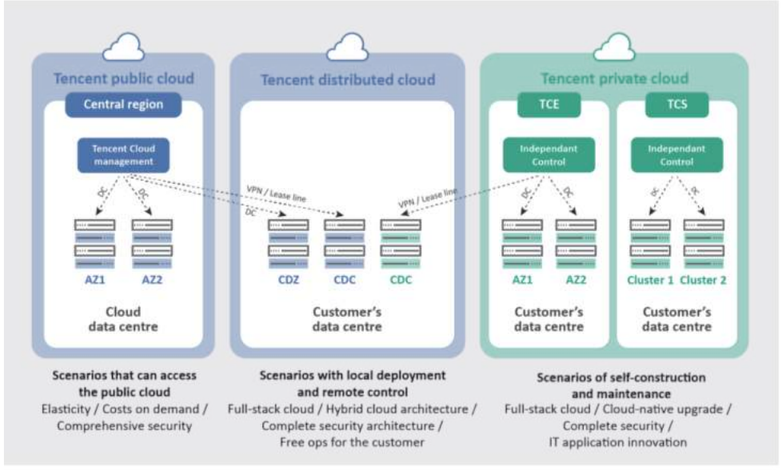
Tencent Cloud solution overview

Tencent Cloud offers a wide array of consistent products and features that provide customers with choice, enabling customers to migrate to the public cloud or migrate and remain on-premises. This choice extends beyond just the infrastructure and covers operational models such as retaining any current self-built operational capabilities or transitioning to a cloud service model. Tencent Cloud can cater to their needs.

Tencent Cloud's diverse product architecture stems from a robust public cloud system architecture that has been refined over a decade of operations. During this time, it has built a reputation for its stability and reliability. Beyond basic IaaS capabilities, Tencent Cloud provides additional container, security, database, and middleware products that can be integrated with its IaaS offerings. This integration provides customers with an improved TCO, along with integrated security and PaaS capabilities.

Tencent Cloud provides a variety of product offerings, including public cloud, distributed cloud (CDC+CDZ) and private cloud (TCE+TCS), to cater to VMware alternatives and upgrade needs across multiple dimensions (see **Figure 9**). Customers can mix and match different cloud services to create a hybrid cloud environment, leveraging public clouds for services featuring ubiquitous accessibility and elasticity, while running stable-state services in distributed or private clouds. This approach capitalizes on the strengths of each cloud option and fosters synergy through a unified control platform. The survey (see **Figure 8**) clearly showed that customers prefer a hybrid cloud environment, making Tencent's offering well aligned with current architectural choices.

Figure 9: Tencent Cloud Solutions for VMware Migration

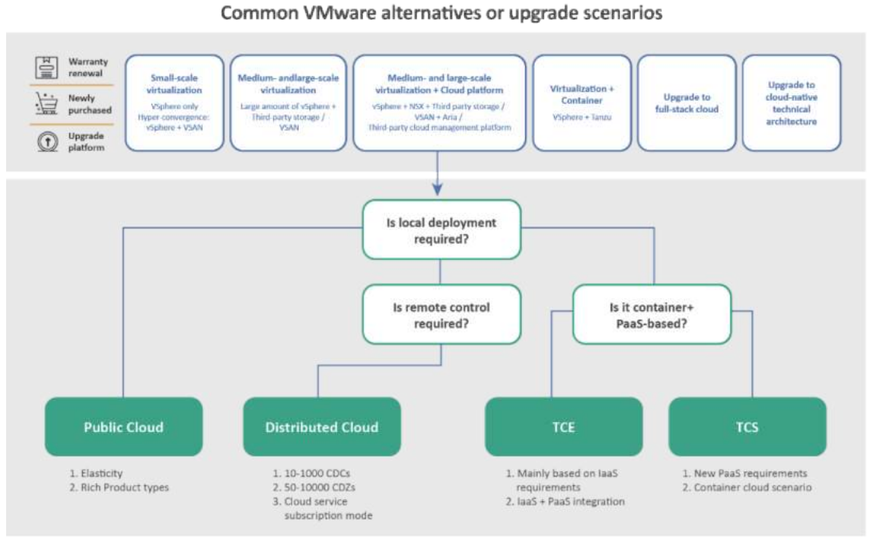


Source Tencent

Decision tree reference for adopting Tencent Cloud alternatives and upgrades

Tencent Cloud offers a decision tree (see **Figure 10**) to help customers quickly identify products and solutions they need for VMware alternative or upgrade.

Figure 10: Tencent's decision tree for VMware alternatives



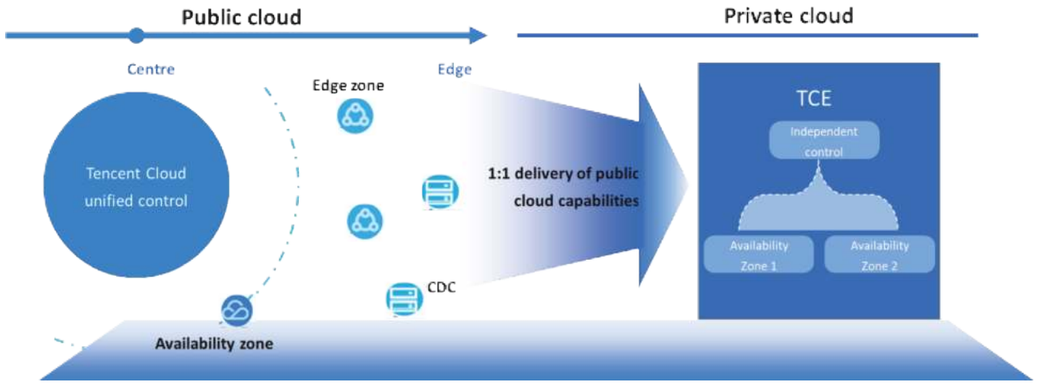
Source Tencent

Introduction to Tencent Cloud products

Product overview: Private cloud (TCE)

Tencent Cloud Enterprise (TCE) is a private cloud solution derived from Tencent's public cloud. It offers seamless alternative and upgrade for enterprises migrating from VMware to a full-stack cloud environment (see **Figure 11**).

Figure 11: Architecture for public cloud to private cloud migration



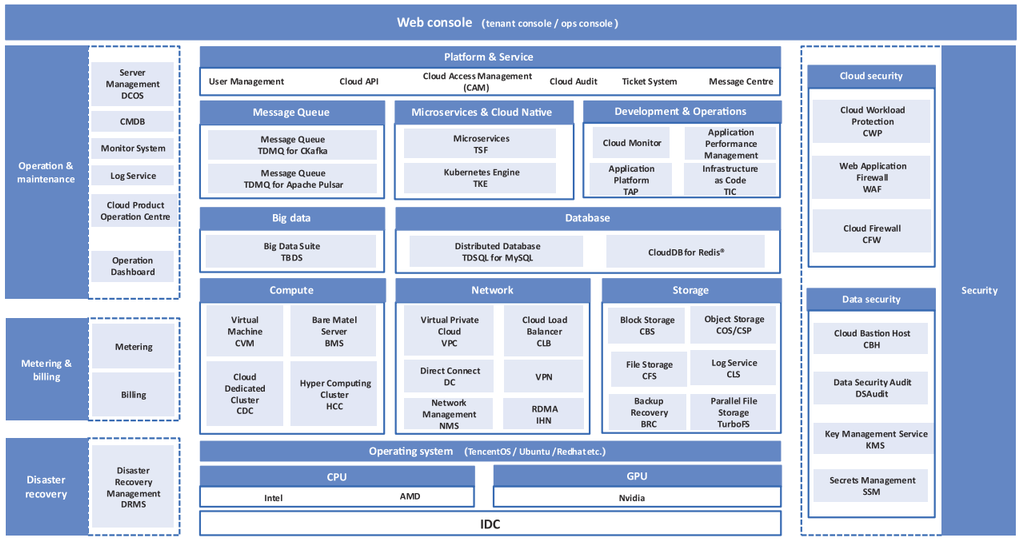
Source Tencent

TCE is an exact 1:1 replication of Tencent's public cloud capabilities, offering a full-stack cloud solution for enterprises on their own premises. Both TCE and Tencent's public cloud share the same architecture and codebase, enabling them to cater to a wide range of infrastructure needs. This includes self-service clouds for internal government and enterprise users, as well as industry clouds for enterprise tenants. In addition, TCE offers management capabilities, including operations, and high availability. It offers more granular management, operability, and maintainability compared to public clouds and comes with comprehensive documentation and tools for customers to manage their own clouds.

Service catalogue

TCE provides a full stack of IaaS and PaaS products (see **Figure 12**), including compute, storage, network, security, database and middleware services. The extensive product portfolio is designed to adapt flexibly to a wide range of user needs.

Figure 12: TCE platform service catalogue



Source Tencent

TCE supports the following three go-to-market models:

1. One-off software authorization: permanent software authorization and software maintenance
2. Software subscription: subscriptions based on product type, usage and duration
3. Unlimited license agreements (ULA): unlimited use for a limited period within the agreed-upon product categories

These go-to-market options can be flexibly combined to meet customer needs in a variety of scenarios, including VMware alternative, new construction and scale-out.

Product overview: Private cloud PaaS platform (TCS)

Tencent Cloud-native Suite (TCS) is an integrated software solution designed to facilitate enterprise cloud-native transformation. This on-premises solution shares the same codebase and architecture

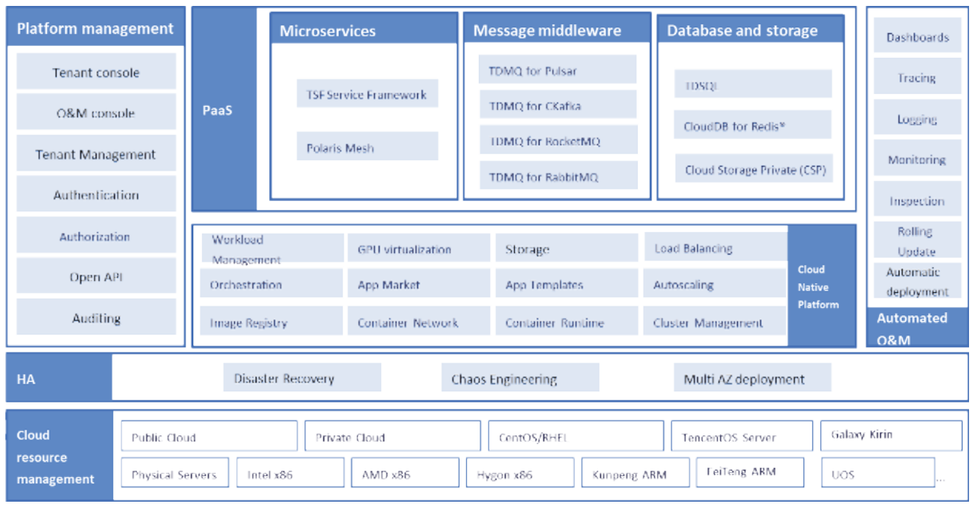
as Tencent's public cloud. Proven through large-scale deployment in the public cloud, TCS delivers essential features such as stability and reliability, as well as independent controllability.

Typical application scenarios of TCS include cloud-native PaaS platforms, container and microservice platforms, AI platforms and edge computing.

Service catalogue

TCS offers PaaS capabilities, including containers, microservices, message middleware and databases (see **Figure 13**). Its extensive product portfolio enables flexible combinations to precisely meet customer needs.

Figure 13: TCS platform service catalogue



Source Tencent

TCS supports the following three go-to-market models:

1. One-off software authorization mode: permanent software authorization and software maintenance
2. Software subscription mode: subscriptions based on product type, usage and duration
3. Unlimited license agreements (ULA) mode: unlimited use for a limited period within the agreed-upon product categories

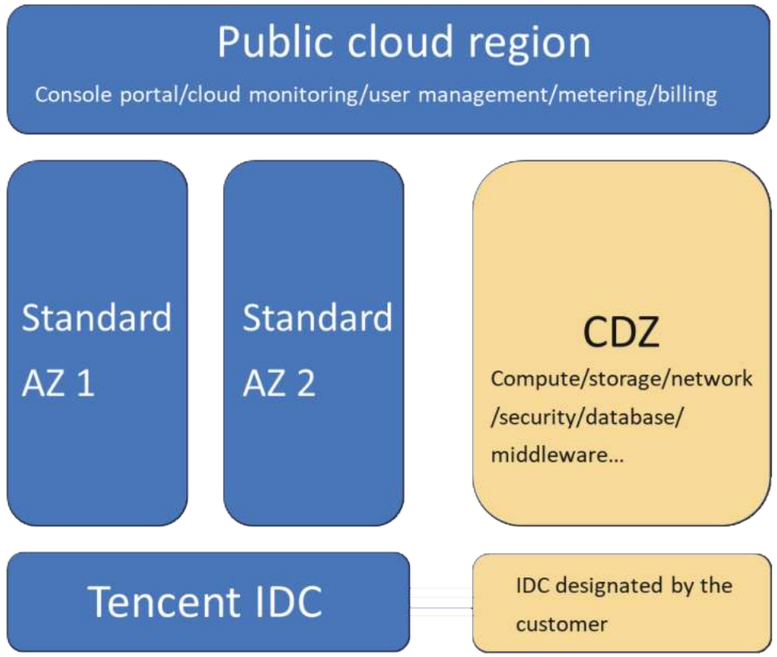
These go-to-market options sales modes can be flexibly combined to meet customer needs in a variety of scenarios, including new construction, expansion, and alternative projects.

Product overview: Distributed cloud (CDZ)

Cloud Dedicated Zone (CDZ) is a dedicated availability zone (AZ) in Tencent's public cloud, extending the standard cloud services to a customer-designated data centre. This setup provides on-premises cloud platform capabilities, addressing the need for local data processing, storage and minimal business latency, while ensuring a seamless user experience and consistent APIs with the public cloud.

In the CDZ, a customer can deploy standard public cloud products as needed (see **Figure 14**), and the resources within the CDZ are exclusively available to the customer or its authorized users. Customers can use CDZ to build their own enterprise cloud platforms or establish industry cloud platforms to provide services externally.

Figure 14: Architecture of public cloud to CDZ

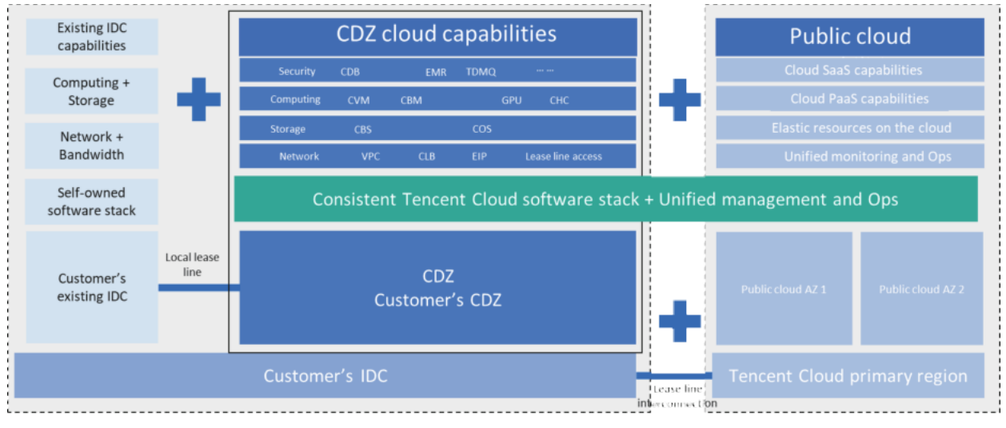


Source Tencent

Service catalogue

CDZ provides more than 80 cloud offerings (see **Figure 15**), including IaaS and PaaS products such as CPU-based computing, GPU-based computing, container, storage, network, security, database and middleware. Customers can mix and match these products on demand for seamless integration with public cloud services. All public cloud services remain accessible while mission-critical data is stored locally to meet diverse customer needs.

Figure 15: CDZ Service catalogue



Source: Tencent

CDZ supports sales through cloud service subscriptions with options for down payments and monthly instalments, minimising the one-time expenditure.

Product overview: Distributed cloud (CDC)

Cloud Dedicated Cluster (CDC) is a new managed infrastructure offering of Tencent Cloud (see **Figure 16**) that extends centralised public cloud services to on-premises environments for nearby access, catering to applications such as AI quality inspection in production lines, university research stations, medical film reading rooms and oil platforms. It combines the benefits of public clouds with on-premises data centres, offering extensive cloud features with low latency and enhanced security.

Deployed in the form of intelligent integrated cabinets, CDC delivers computing power directly from a customer's data center, enabling resource access through a nearby public cloud region for unified management. Customers can easily manage CDC resources using existing public cloud tools such as consoles and APIs.

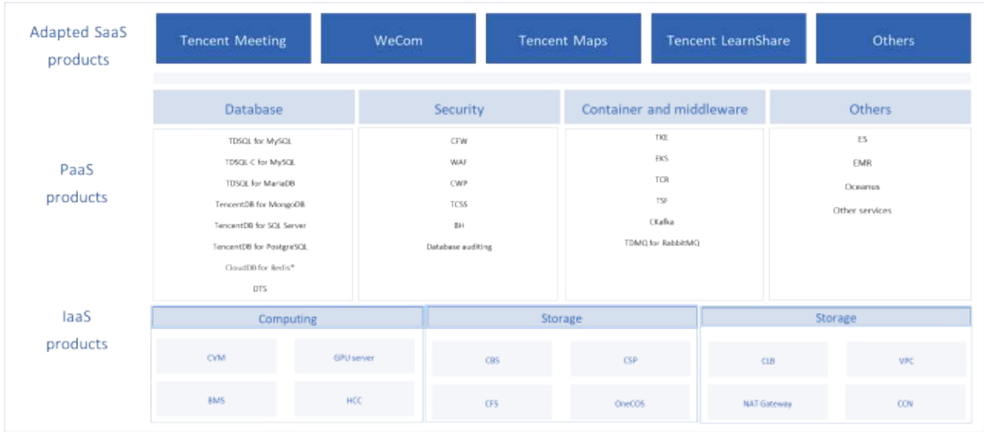
Figure 16: CDC all-in-one machine

Source Tencent

Service catalogue

CDC provides a wide range of offerings (see **Figure 17**), including IaaS and PaaS products such as CPU-based computing, GPU-based computing, container, storage, network, security, database and middleware. Customers can mix and match these products on demand for seamless integration with public cloud services to meet diverse needs.

Figure 17: Catalogue of CDC all-in-one machine services



Source Tencent

CDC supports sales through cloud service subscriptions with options for down payments and monthly instalments, minimizing the one-time expenditure.

Classification and analysis of Tencent Cloud alternatives to VMware and upgrade scenario

Scenario 1: IaaS layer alternatives to VMware

IaaS layer alternatives to VMware are the most common scenario among VMware customers. In this scenario, there can be:

- A small-scale hyper-converged architecture consisting of more than a dozen servers, vSphere and vSAN.
- A medium-scale storage-compute separated architecture consisting of more than a hundred servers, vSphere and IP SAN/FC SAN.
- A multi-tenant self-service cloud platform consisting of more than a thousand servers, IP SAN/FC SAN, physical networks and cloud management platforms.

In this scenario, the IaaS layer, comprising compute, storage, and network resources, establishes the foundational infrastructure of an enterprise IT system. The stability and reliability of IaaS are critical decision-making factors for customers. Moreover, changes to the IaaS infrastructure can significantly affect business operations, making the sustainable supply of products a key consideration for customers when choosing suppliers. Finally, intrinsic security capabilities rank among the most common customer requirements.

More significantly, in its sub-scenarios, customers with multiple branches will focus on achieving centralized operational management between headquarters and branches. Small and medium-sized enterprises emphasise the availability of comprehensive IaaS product capabilities and solutions, rather than procuring and assembling hardware and virtualization software on their own. Large enterprises may value self-service, metering, and billing capabilities for tenants. Additionally, customers planning for IPOs may underscore the need for asset ownership management.

Challenges

1. **Lack of an integrated security system:** In traditional VMware architecture, security solutions are often built from third-party vendor products, resulting in a lack of unified perception and protection capabilities.

2. **Lack of a software-hardware integrated solution:** Small and medium-sized enterprises, often limited by insufficient technical personnel, face further challenges when hardware and software are procured and maintained separately. These customers tend to prefer integrated solutions that provide both software and hardware as a package. Since VMware supplies only software, customers are required to manage hardware procurement and maintenance on their own, which increases operational expenses.

3. **Lack of refined operations capability:** For medium and large-sized enterprises with multiple branches, IT decision-makers prioritize key capabilities such as unified management of branch IT facilities, self-service tools for internal users, and usage-based allocation of internal IT costs. However, the current VMware management platform requires customers to perform secondary development to meet these demands, which can lead to increased costs.

4. **Subscription mode only:** Listed companies or those planning for IPOs may face strict financial management regulations and prefer to retain ownership of software and hardware assets. VMware's shift to subscription mode has exacerbated challenges for these customers.

5. **Lack of a domestic alternatives solution:** Enterprises with stringent domestic alternative and compliance requirements demand the software to support domestic hardware, which VMware is unable to support in all geographies—in China, for example.

Tencent Cloud "IaaS Layer alternatives to VMware" solution

In the scenario of IaaS layer alternative (see **Figure 18**), Tencent's distributed cloud solution (CDZ+CDC) and private cloud solution (TCE) share the same technical architecture as its public cloud, ensuring stable and reliable product performance. Both solutions can provide comprehensive compute, storage and network capabilities as alternatives to VMware's vSphere, vSAN and NSX. In addition, they provide tenant self-service capabilities out of the box. Moreover, the distributed cloud solution integrates software, hardware and operational management into a unified framework, delivering cloud-based services that reduce both the operational complexity and costs for customers.

Figure 18: IaaS layer alternatives to VMware diagram

Source Tencent

Key capabilities of Tencent Cloud's solution

- **Integrated security system:** Tencent's distributed cloud solution (CDZ+CDC) and private cloud solution (TCE) provide comprehensive security capabilities, encompassing network security, application security and data security.
- **One-stop solution:** The distributed cloud solution or TCE integrates compute, storage and network capabilities into a comprehensive IaaS solution, offering a wide range of models, storage options and built-in distributed firewall (DFW) capabilities.
- **Refined operations capability:** The distributed cloud solution or TCE has its own tenant platform and ops platform to support multi-tenancy and self-service, meeting the enterprise's need for refined operations from aspects of the group account, metering and billing.

- **Support for multiple go-to-market options:** TCE supports multiple go-to-market options, including resale, subscription, and ULA, to flexibly meet users' needs for their assets.
- **Adaptation to mainstream domestic chips:** compatible with common domestic software and hardware such as Hygon, Kunpeng and Phytium chips, as well as domestic operating systems such as Kylin OS and UOS.

Case study 1: A university in Macao (China)

Background

A university in Macao (China) realised its traditional siloed IT infrastructure could no longer meet the flexible demands for running multiple applications within the institution. To improve resource utilisation, reduce operational costs, enable flexible resource scaling and allocation, and transition to a software-defined data centre architecture, the university decided to upgrade its existing VMware platform to better meet development requirements.

Business challenges

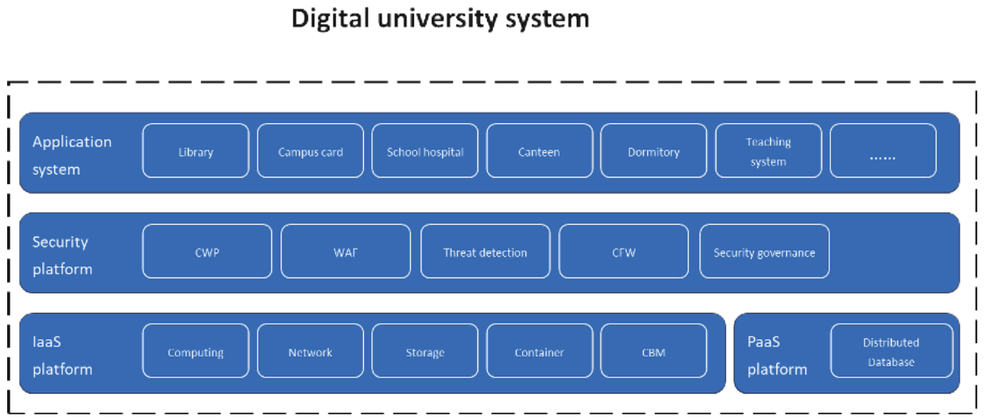
1. Lack of scaling elasticity: The original VMware architecture lacks elasticity, preventing the library, card, hospital, canteen, dormitory and teaching management systems from being quickly scaled to meet usage demands.

2. Lack of refined operations capability: The original VMware architecture lacks multi-tenancy and quota capabilities to support the logical isolation required by the teaching and experiment platform.

Solution

Based on the Tencent private cloud solution TCE (see **Figure 19**), the university in Macao (China) has built an exclusive IaaS cloud platform that integrates IaaS, database, security and management capabilities into a one-stop solution. The platform comprises cloud servers, bare metal servers, containers, block storage, object storage, file storage, SDN networks, TDSQL databases, host security, threat detection, security centres, security governance (NIPS), bastion hosts, cloud firewalls, WAF and operational platforms. These offerings fulfil the operational needs of the university's business systems and student experiment platforms. Furthermore, the university has migrated its existing VMware environments to the cloud using an offline migration process.

Figure 19: Digital university system of the university in Macao, China



Source Tencent

Customer benefits

1. Elastic IT architecture: The TCE cloud platform has created a unified infrastructure for all teaching and research systems at the university. Workloads from 50 VMware hosts have been migrated to the cloud, resulting in reduced management and maintenance costs. The cloud platform's distributed architecture and auto-scaling capabilities facilitate elastic scaling, allowing for the rapid accommodation of the expansion needs of teaching and research systems.

2. Refined operations: The TCE cloud platform supports all business systems of the university and incorporates multi-tenancy, permission management and quota management features to offer students a unified experimental platform with logical isolation capabilities. Additionally, it facilitates the university's pursuit of research innovations.

Case study 2: Midea (Brazil)

Background

Midea, a leading global home appliance manufacturer, has established a local factory in Brazil to support its overseas expansion and meet local business needs. Its IT support also needs to be extended to this factory. At the same time, as a large group customer, the customer has multiple infrastructures around the world and hopes to achieve unified management of all IT infrastructures as much as possible to reduce operation and maintenance costs.

Business challenges

1. Low latency demand: Production services are sensitive to network latency and require less than 3ms. If the Brazilian public cloud is used, the latency requirement cannot be met.

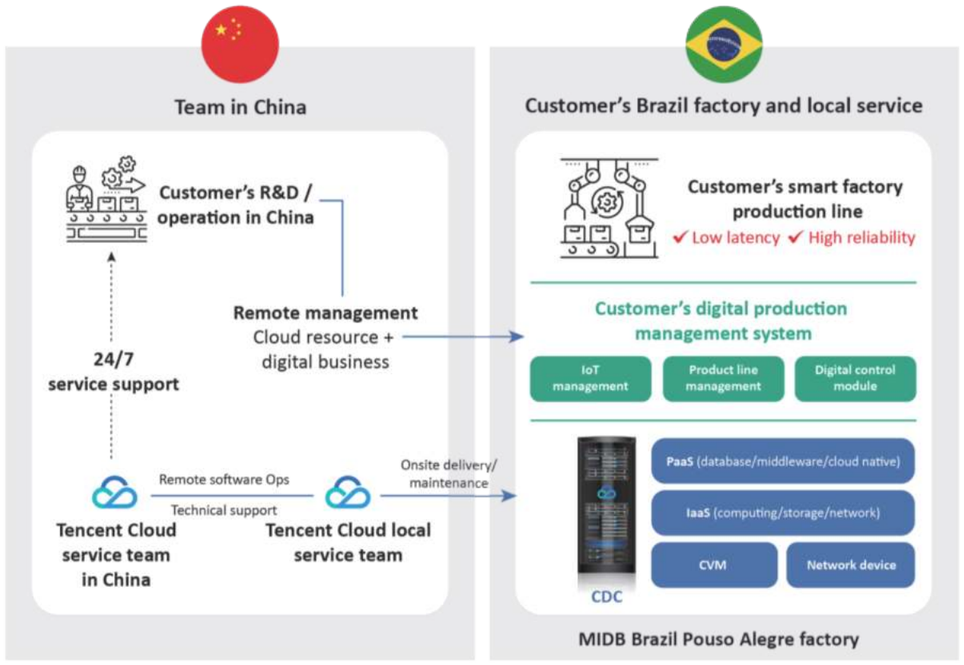
2. Low investment demand: The construction scale of overseas factories is small in the early stage. If the mode of self-purchased VMware software, hardware equipment, self-manpowered construction and operation and maintenance is adopted, the initial investment will be heavy, and the operation and maintenance costs will also be relatively high.

3. Unified management demands: With the gradual development of business, customers have more and more IT environments around the world. They hope that headquarters and branches and centres and edges can be managed in a unified manner to reduce management difficulties.

Solution

Tencent Cloud's distributed cloud product CDC (see **Figure 20**) provides customers with localised, low-latency cloud services in the computer room of their Brazilian factory, including cloud host, cloud hard disk, cloud network, host security and other related products that meet the customer's access latency requirement of less than 3ms. Secondly, the ability to deploy cloud services in CDC is consistent with that of the public cloud and performs unified operation, maintenance and upgrades with the public cloud. Finally, the CDC software and hardware deployed in the customer's computer room is maintained by Tencent, which reduces the customer's operation and maintenance costs.

Figure 20: CDC built localised cloud services for Midea's factory in Brazil



Source Tencent

Customer benefits

1. **Localized low-latency IT platform:** CDC is deployed in the customer's factory computer room to achieve low-latency access to cloud services for production lines.

2. **Unified management infrastructure:** The IT platform of the Brazilian factory is operated and managed in a unified manner with the domestic public cloud platform, realizing the unification of the centre and the edge.

3. **Lower operational costs:** The customer no longer needs to purchase VMware software and hardware devices to build and maintain an IT platform by themselves. Instead, they can directly use cloud services, which reduces the costs of operations outside the Chinese mainland.

Scenario 2: Upgrading from IaaS to full-stack cloud

Medium-sized and large enterprises are usually involved in this scenario. Such enterprises have many business departments, various IT business types and many employees using IT systems. In addition to providing basic IaaS products and capabilities, the IT department also needs to provide PaaS products, such as databases, middleware, big data products, and containers, as well as comprehensive security capabilities. Moreover, due to the large number of employees and teams, multi-tenant/self-service capabilities and internal measurement cost amortization or billing capabilities are also required.

If VMware product solutions are used, customers need to purchase a large number of servers and network devices and build IaaS platforms with VMware software products. In terms of PaaS products, they usually use open-source products or purchase commercial software. For example, they may use the open-source version of MySQL as the database or purchase commercial Oracle. In terms of security products, DFW products of VMware are usually used together with commercial products such as WAF, DDoS protection, endpoint security and security centre. Self-developed products or VMware products that have undergone secondary development are usually used to provide multi-tenant management and self-service capabilities.

Challenges

1. Patchwork solution: Software and hardware are purchased separately, open-source products and commercial products are used together, and self-development and secondary development are combined. The built enterprise cloud platform is non-standardised and customised, rather than standardised with SLA metrics. As a result, operational boundaries are not clear, troubleshooting is complex and it is hard to carry out product upgrades and iterations.

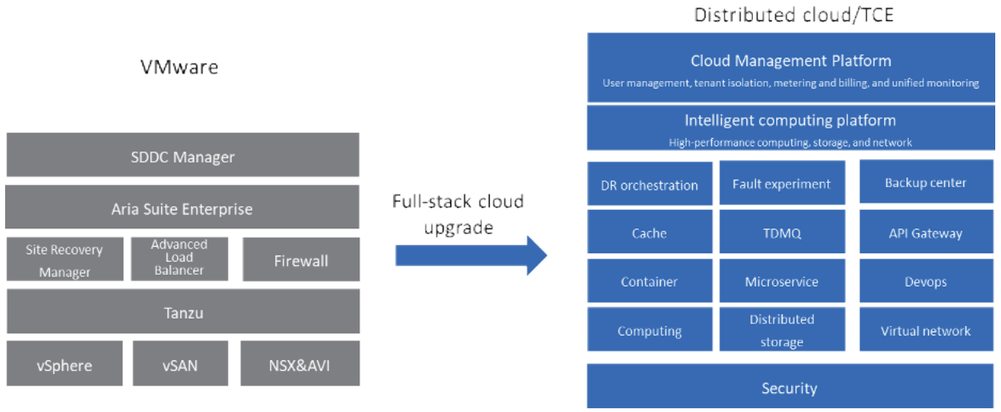
2. Incomplete self-service capabilities: The multi-tenant self-service capabilities are incomplete because the products from different vendors need to be integrated for orchestration and process-based transformation, which requires more workforce. Therefore, self-service features are usually relatively simple and few. They even require certain processes and manual operations.

3. No AI-computing integration solution: Under the wave of AI, VMware cannot manage GPU computing power and cannot provide an AI-computing integration solution.

Tencent Cloud Solution: Upgrading from IaaS to full-stack cloud

In upgrading from IaaS to full-stack cloud (see **Figure 21**), distributed cloud products of Tencent Cloud (CDZ, CDC and TCE) can provide IaaS, PaaS, overall security, multi-tenant management and self-service capabilities. They can serve as alternative to VMware's basic IaaS and container capabilities. They can also provide capabilities required by modern applications, including various databases and middleware, AI infrastructure that supports AI business, comprehensive one-stop security and comprehensive operational management covering disaster recovery orchestration. With these capabilities, the products can provide comprehensive cloud services for large and medium-sized enterprises.

Figure 21: Full-stack cloud upgrade diagram



Source Tencent

Key capabilities

Full-stack unified solution: Provides a complete full-stack solution covering IaaS, PaaS and security to achieve unified management and technical support of infrastructure technology stacks.

Complete operation and ops capabilities: Provide a complete operational platform to meet users' needs of one-stop operational management. Observable and automated operations capabilities at the hardware, cloud service, cloud instance, application and business layers are provided.

Support for AI-computing integration solutions: Provide both general computing and AI-computing integration solutions that support high-performance computing, high-performance storage, high-performance networks and high-performance training/inference acceleration frameworks. In this way, enterprise AI applications are provided with high-efficiency underlying computing power support.

Case study 1: A major commercial bank

Background

A major commercial bank hopes to support the new core system and various online business systems through new cloud infrastructure to achieve unified integration of business and technology platforms.

Business challenges

1. Improve the architecture stability: The original application systems adopt a centralized technology architecture to run open-source middleware products. No technical support guarantee from product vendors is provided for important systems, and components are not stable enough.

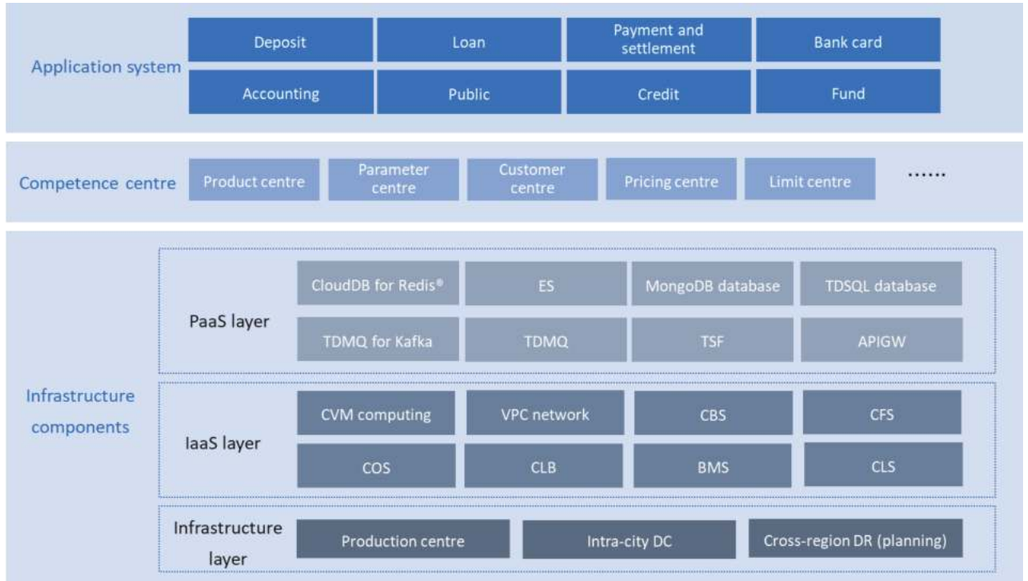
2. Achieve automated operations: One-stop monitoring and automated operations capabilities that match the cloud infrastructure need to be built to achieve automated, data-based and intelligent operations.

3. Ensure smooth migration: The business systems of the bank can be shut down for a short time. All business systems must be migrated from VMware to the cloud platform within this period.

Solution

The bank has built a full-stack cloud by using TCE (see **Figure 22**), which provides Cloud Virtual Machine (CVM), Bare Metal Server (BMS), Tencent Kubernetes Engine (TKE), Cloud Block Storage (CBS), Cloud File Storage (CFS), Cloud Object Storage (COS), Software-Defined Networking (SDN) gateway, CloudDB for Redis®, Tencent Distributed Message Queue (TDMQ) for Kafka, Tencent Service Framework (TSF), TDMQ, TencentDB for MongoDB, TDSQL, Elasticsearch (ES) and a variety of security products. It meets the production needs for cloud-based business systems and has passed level 3 cybersecurity classified protection 2.0. The bank managed to migrate 130 systems running on VMs to the cloud within eight hours.

Figure 22: Technical architecture diagram of the bank



Source Tencent

Customer benefits

High stability: The bank adopts the TCE full-stack solution and uses TCE PaaS services, such as TDMQ, TSF and CRedis. Tencent Cloud provides technical support. As a result, the requirement of high middleware stability is met.

Automated operations: The native Cloud Monitor, CMDB, CLS, TAP and other components of TCE are used to achieve one-stop automated operations covering hardware, cloud service, cloud instance, application and businesses.

Efficient migration solution: The Tencent Cloud tool go2tencentcloud is used to migrate hundreds of VMware VMs to the cloud within eight hours. The virtual machines run stably after migration.

Case study 2: GRM's Industry Cloud Platform in Malaysia

Background

Global Resources Management SDN. BHD. (GRM) is a well-known local ICT vendor in Malaysia. With the increasing demand for local enterprises to migrate to the cloud and the increasingly high requirements of local regulations on data localization, the customer hopes to build a localised cloud platform to provide localised industry cloud services for local enterprises.

Business challenges

For the technical route of building a localised cloud platform, there are several solutions, including the solution based on commercial VMware software, the solution based on open-source OpenStack and self-developed capabilities, and the distributed cloud solution applying the public cloud to customer sites. The customer hopes that the localized cloud platform can provide a variety of product capabilities covering IaaS, PaaS and security. The customer wants to choose a technical route that supports long-term iterations and updates to minimise the operational burden so that the customer can focus on the business.

1. The customer is familiar with the solutions of using commercial VMware software and adopting the open-source OpenStack capabilities. However, they can only provide IaaS product capabilities but cannot provide PaaS and security product capabilities.

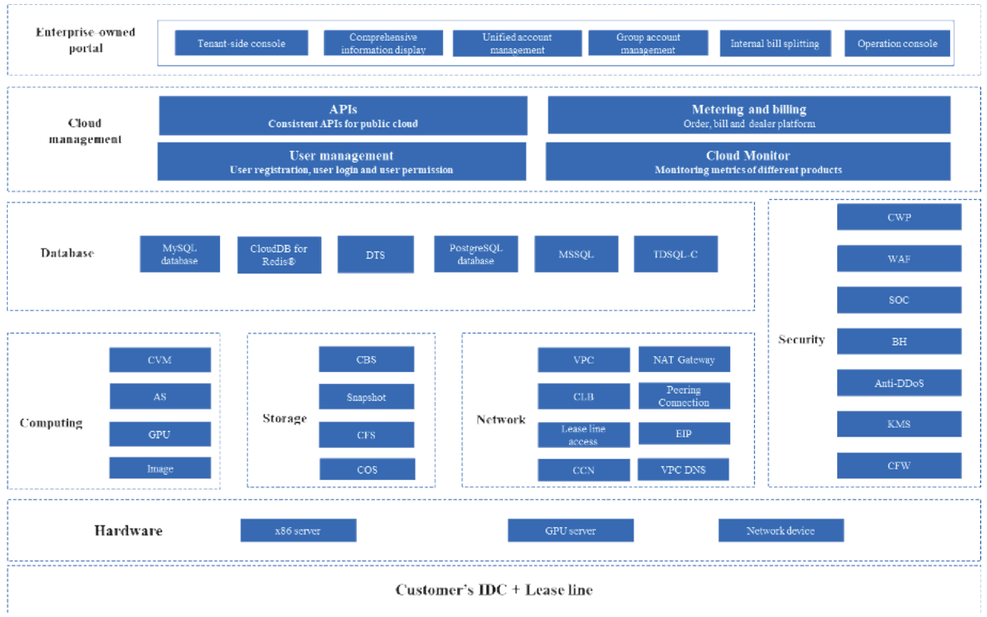
2. The customer needs to purchase software and hardware, build a platform and perform operational management This requires huge initial human resources and device investment, and the business cannot run quickly.

3. The solutions of using commercial software and open-source capabilities require secondary development of multi-tenant and self-service capabilities, which is complex and difficult.

Solution

By adopting the distributed cloud product CDZ, the customer officially released Alto Cloud (see **Figure 23**), hosted in its own data centre. Common IaaS/PaaS/security cloud products are deployed in the local data centre in Malaysia. At the same time, a comprehensive multi-tenant and self-service platform was provided to meet the needs of Malaysian enterprises requiring cloud migration. The distributed cloud product CDZ also provides operational management capabilities for the entire cloud platform, which greatly reduces the management costs for the customer.

Figure 23: Architecture of Alto Cloud released by GRM



Source Tencent

Customer benefits

Localized cloud platform: A localized cloud platform is provided in Malaysia to meet the country's requirements for data localization.

Quick business running and low ops costs: By using the distributed cloud product CDZ, the business can run quickly with no large initial investment.

Scenario 3: Evolution from VMware to cloud native

In the early stages of the cloud computing industry, some customers chose to start cloud transformation at the IaaS layer. Customers using VMware mainly use the vSphere, vSAN and NSX IaaS layer. Most applications run on VMs, and PaaS-layer applications such as middleware and databases are usually built by using open-source products. The traditional monolithic application architecture is usually used.

As cloud-native PaaS technologies represented by Kubernetes become mature, customers are considering evolving to a cloud native architecture for VMware upgrades. This cloud native architecture can help build more resilient application systems, improve resource utilization, and respond more agilely to corresponding business changes. The upgrade to a cloud native architecture

can also meet the demand for cloud migration of PaaS-layer applications, such as middleware and databases. TCS operates on third-party IaaS platforms or physical servers, serving as a flexible alternative to VMware during cloud-native migration upgrades.

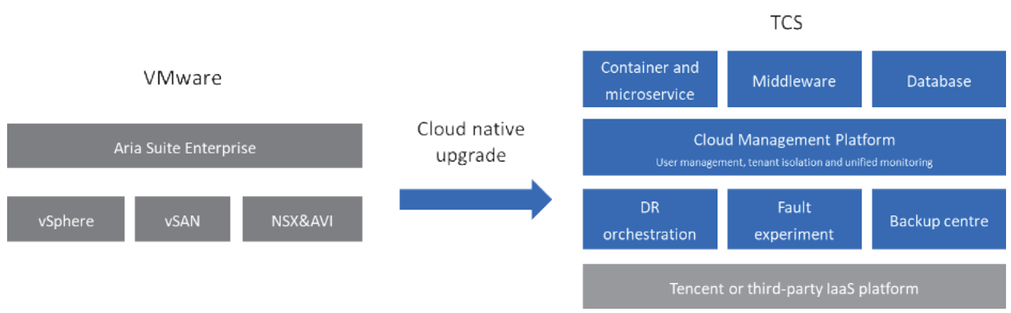
Challenges

- More resilient systems are needed to improve stability and reduce TCO: Compared with VMs, container applications have a shorter deployment cycle and higher resource utilization. They can automatically scale more quickly to handle burst traffic, which improves business stability during peak hours and reduces resource waste during off-peak hours.
- Lack of unified management of PaaS components: Different teams use different technologies and PaaS component versions. The lack of unified and standardized management leads to ineffective repeated construction and also causes difficulties for operations.
- Lack of operational management capabilities at the PaaS layer: It is difficult for customers to employ technical experts in multiple PaaS fields simultaneously. Professional vendors are needed to provide operational services and best practices to ensure business stability.
- System architecture evolution along with the AI ecosystem: The core technology stacks of the industry's AI ecosystem (such as training frameworks, inference services and data pipelines) have widely adopted containerised deployment. Containerisation has become a de facto standard, and customers urgently need stable and reliable container and PaaS services.

Tencent Cloud's solution: Evolution from VMware to cloud native

TCS integrates many of Tencent's mature PaaS products, such as containers, microservices, databases and middleware (see **Figure 24**). It provides unified capabilities such as operational management, disaster recovery and backup, which can meet a customer's cloud native architecture upgrade demands in one go.

Figure 24: Cloud native upgrade diagram



Source Tencent

Key capabilities

The key strengths of the TCS solution can be summarized as follows:

1. Unified management and easy maintenance: TCS provides mature and reliable operational management and high availability capabilities that have been tested by users of Tencent's public cloud and other private clouds. Customers' operational efficiency and system stability can be improved greatly.

2. Low application transformation cost: TCS provides mature application management, deployment and orchestration capabilities together with out-of-the-box database and middleware services to help customers efficiently build cloud native applications.

3. Flexible construction with low investment: TCS requires few initial resources for deployment and supports on-demand scale-out according to business volume, which will reduce the initial costs of resources used by customers. At the same time, it supports various heterogeneous computing resources and many PaaS services that can be selected on demand to flexibly adapt to different scenarios and effectively lower the threshold for customers to migrate to the cloud.

4. Openness and compatibility: TCS supports integration with third-party IaaS platforms and is compatible with mainstream domestic processors and IT application innovation. It adheres to mainstream open-source specifications, thus protecting any customers' existing IaaS investments and avoiding technical lock-in.

Case study 1: Pacific Insurance

Background

The Life Insurance Department of Pacific Insurance wants to build a standardized architectural design framework, a unified development platform and a delivery pipeline. By doing so, it aims to adopt a cloud native transformation to improve the efficiency, system stability and resource utilisation of its R&D system.

Business challenges

The customer faces technical and operational challenges in their existing R&D system.

1. Technical perspective:

   a. Lack of full-stack dynamic elasticity with business-optimised scheduling.
   b. Low automation and observability, with non-standardised monitoring and logging.
   c. Weak self-healing and service governance, leading to slow handling of single points of failures.
   d. Fragmented foundational capabilities in services such as containers and microservices without integration of public cloud resources.
   e. Need to enhance business continuity through active-active architecture and elastic scale-out.

2. Business perspective:

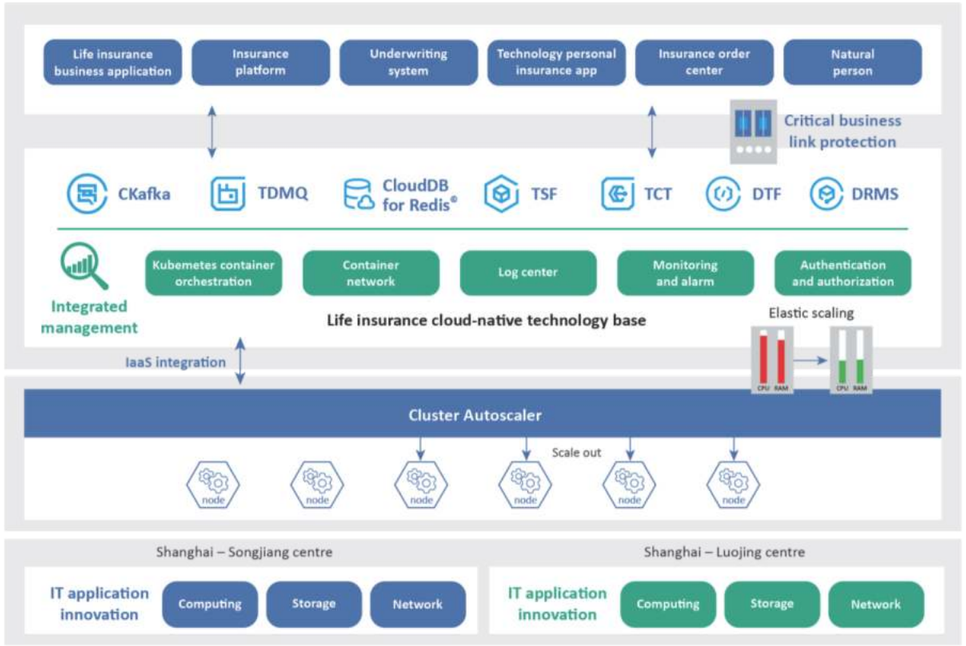
   a. Accelerate market responsiveness by shortening delivery cycles.
   b. Reduce resource waste caused by fragmented technology stacks through platform unification and standardization.

c. Leverage cloud native technologies for dynamic resource allocation, cost reduction and rapid innovation.

Solution

The Life Insurance Department of Pacific Insurance deploys TCS alongside its existing third-party IaaS platform (see **Figure 25**). TCS integrates PaaS services such as containers, microservices, cache and message queues, enabling centralised management and resolving platform and pipeline challenges to achieve cloud-native transformation.

Figure 25: Architecture of the CPIC life insurance cloud native system



Source Tencent

Customer benefits

1. TCO optimisation: 80% of systems are migrated to TCS's service framework, which reduces application resource allocation by 30%.

2. R&D efficiency: Integration of internal CI/CD with TCS improves the release efficiency of cloud-based applications by 85% and delivery speed by 20%.

3. Ops efficiency: TCS's unified observability increases the issue-detection rate by 20% and reduces troubleshooting time by 20%.

4. Industry recognition: Pacific Insurance's cloud native project won the 2023 to 2024 "Trusted Cloud User Case Best Practice" award in July 2024.

Comparison of three major scenario alternatives and upgrade solutions

Table 1 provides an overall comparison between VMware and Tencent.

Table 1: General comparison of VMware and Tencent Cloud Alternatives

Customer IT Needs	VMware	Tencent Cloud product portfolio	Tencent Cloud strengths
Long-term product supply for supply chain security Comprehensive security schemes and product capabilities Lower TCO	After the acquisition, the product has undergone major adjustments, and its continuous supply capacity is worrying. Incomplete security capability. After the acquisition, prices generally rise 3 to 5 times.	TCE CDC CDZ TCS	Public cloud-aligned architecture for supply chain security Comprehensive IaaS, PaaS and security capabilities Superior TCO

Source Tencent

Tables 2, 3 and 4 show the comparison for each of the scenarios discussed in the report.

Table 2: Scenario 1 comparison: IaaS layer alternatives

Customer IT needs	VMware	Tencent Cloud product portfolio	Tencent Cloud strengths
Diversified computing power needs with the emergence of AI applications Unified management of headquarters and branches	No GPU, object storage support and other product capabilities. Weak overall unified management	TCE CDC CDZ	Diverse computing power solutions Centre and edge, group and branch unified management

Source Tencent

Table 3: Scenario 2 comparison: Upgrading from IaaS to full-stack cloud

Customer IT needs	VMware	Tencent Cloud product portfolio	Tencent cloud strengths
Business upgrades require more product capabilities, such as cache libraries and middleware. Large customers have self-service and billing requirements.	Only IaaS capabilities, no PaaS or comprehensive security capabilities. Multi-tenant and self-service capabilities require secondary development.	TCE CDC CDZ	Complete IaaS, PaaS and security product capabilities. Complete cloud management platform capabilities, including multi-tenancy, self-service and metering capabilities.

Source Tencent

Table 4: Scenario 3 comparison: Evolution from VMware to cloud native

Customer IT needs	VMware limitations	Tencent Cloud product portfolio	Tencent Cloud strengths
Unified PaaS standards and vendor-supported operations. The PaaS layer runs on a third-party IaaS platform, and the two layers are built independently and flexibly. When adopting VMware alternatives, upgrade from the traditional virtualization-dominated architecture to a more elastic cloud-native architecture, enhancing business stability and resource utilization.	The PaaS product matrix is incomplete. Customers need to purchase other commercial middleware and databases or build them based on open-source products. Heavy virtualization limits elasticity and resource utilization. From the perspective of GPU computing power management capabilities, container solutions are weaker than the industry's AI ecological integration.	TCS	Provides a complete commercial PaaS product matrix, including containers, microservices, middleware and databases to support platform-based unified management. Proven cloud native expertise and use cases accumulated from customers. Tencent Cloud empowers customers to make good use of cloud native technology to maximise their benefits. Provide GPU virtualization and computing power scheduling capabilities, which can be well integrated with the AI ecosystem to meet the needs of AI application construction.

Source Tencent

TCE vs. VMware feature& technical comparison

Feature	VMware	TCE
Virtualization	Based on proprietary ESXi technology, scalability is limited	Based on open-source KVM with deep optimization, scalability is unrestricted
Computing	VMware vSphere only supports compute resources at the virtual machine level and does not support bare metal servers	TCE CVM supports cloud-edge integration, provides bare metal servers, and virtualization with zero loss. It also supports virtual machine rescue mode, deletion protection, placement groups, and full-link task-level monitoring and alerting capabilities
storage	Only support block storage and file storage	Comprehensively support block storage,file storage and object storage
Network platform	Centralized management by platform administrators ,with high technical thresholds	Supports multi-tenant management (tenant portal and operations portal), allowing users to self-manage network instances via the tenant portal

Security	Cybersecurity products are mainly self-owned cloud firewalls,while host security products mainly rely on third-party offerings	Self-developed security products cover Web Application Firewall, Cloud Firewall, Host Security, Bastion Host (BH), and Key Management System (KMS), etc
Container	Supports container capabilities through VKS, tightly locked in vSphere; dependent on ESXi at the underlying layer，high resource overhead; complex deployment and management	Natively integrated with TKE(Tencent Kubernetes Engine) (including Containers/Clusters/Monitoring/Image Registry), Ready to Use Out of the Box
Distributed database **Message queue**	A large number of open source databases or middleware are integrated through the application catalog, but no backup support is provided. In fact, for commercial customers, it cannot be used in production	Tencent Public Cloud's pravite deployment with full-stack cloud capabilities, including integrated middleware and databases, etc
High availability	Only provides traditional virtualization-level disaster recovery through SRM (Site Recovery Manager), lacking a chaos engineering drill system	Provides DRMS (Disaster Recovery Management System) with support for 2AZ, 2AZ+arbitration, 3AZ, and cross-region disaster recovery, along with a chaos engineering drill system
Unified Operations and Maintenance	Supports monitoring, alarm, log management, automation &orchestration, health diagnosis, etc	Supports monitoring,alerting, log management, automation & orchestration, health diagnosis, etc., and also supports application performance monitoring

Platform Operations	User management, quota management	User Management,Product Management(Tenant-specific product catalogs+Product quota allocation (tenant/project level)), Resource Management(Quota administration+Resource request & approval workflows),Operations Tools (Documentation management+Portal administration+Announcements & messaging+Ticketing system), Industry-cloud-ready operational capabilities
Metering and billing system	Administrators can use VCF-operations to calculate resource costs,but the metering and billing capabilities are limited	Provides billing capabilities for tenant business resource usage, meeting the needs of industry cloud operations, group clou multi-tenant account splitting, and department and group separate billing scenaos; supports account splitting by resource tags, projects, tenants, etc., accurately counting resource usage in each cycle to the second, and setting discounts by tenant and product, etc
Licensing	Bundled products annual software subscription	Individual product annual software subscription
Supported hardware types	Officially certified servers, storage, and networking equipment	Supports standard x86/ARM architecture servers and generic hardware,and also supports legacy hardware reuse
Support software integration	Supports third-party product integration, but the access is complex, requires strict review, and is only open to strategic partners	Supports third-party product integration with convenient access, forming a unified system with the cloud platform for account management, permissions, resource management, monitoring, and metering/billing capabilities

Hybrid Cloud	Cooperate with third-party public cloud, and after being acquired, cooperation with the public cloud provider was terminated, and customers need to complete it themselves	Build a single-cloud hybrid with Tencent Public Cloud, with the same architecture; also supports multi-cloud hybrid
Cloud-Edge Co-operation	Implementing a cloud-edge architecture through SDE	Support Distributed IT infrastructure with co-operation of Clou(TCE)+ edge(CDC)
Industry Cloud	Unable to support	Possess full-stack cloud capabilities tailored for industry clouds, including billing and metering capabilities, etc
AI & Intelligent Computing	Support AI computing capabilities through PrivateAI with a focus on underlying GPU resource optimization, but cannot independently provide an end-to-end, out-of-the-box AI comput-ing solution	Supports high-performance computing and task scheduling platform based on GPU, ASIC and other computing power integrated with RDMA networks,while providing comprehensive training/inference acceleration suite and collective communication library, all available out-of-the-box
Ecosystems	Self-developed products focus on the IaaS layer,while at the PaaS layer relying more on third-party partners	Self-developed products cover IaaS, PaaS, security, backup, operation, and maintenance.Fully opens 10,000+ APIs covering tenants and operations, and supports Terraform for easy integration. Also has the ability to access third-party products

Migration

1. Migration overview

Through cloud migration, customers can seamlessly migrate from VMware environments to distributed cloud (CDC+CDZ) and private cloud (TCE+TCS) environments. The migration tasks can be completed without service interruption to ensure minimal impact on business operations.

2. Four key elements of cloud migration

Migration objects: Specify the objects to be migrated, such as images, databases, files and VMs.

Migration tools: Corresponding migration tools are available for different cloud resources. They are as follows:

- CVM migration: The go2tencentcloud tool enables full migration from VMware to target cloud servers in the distributed cloud (CDC+CDZ) and private cloud (TCE+TCS).
- Container application migration: Use application deployment YAML files, such as the Velero tool.
- Container image migration: Tencent recommends using CI/CD for direct version deployment to the cloud.
- Database migration: Use tools such as Data Transfer Service (DTS), MongoShake and RedisShake.
- Storage migration: Support resource migration for cloud object storage (COS Migration and COSDistCp) and cloud file storage (Filetruck).
- Middleware migration: Provide different migration solutions according to scenarios with high or low requirements for message ordering.
- Big data migration: Support tools such as Logstash, Elasticsearch-dump and Mysqldump.

Migration plans: Support cold migration (offline migration, see **Figure 26**) and live migration (hitless migration), which can be selected based on scenarios.

Figure 26: Cold migration vs. hot migration

Source Tencent

Cold migration (offline migration): Suspend the services and perform migration during off-peak hours. Compared with hitless migration, offline migration is less complex to implement, and the process is simple and clear. During the service suspension period, businesses can be switched at one time or in batches by product or business line.

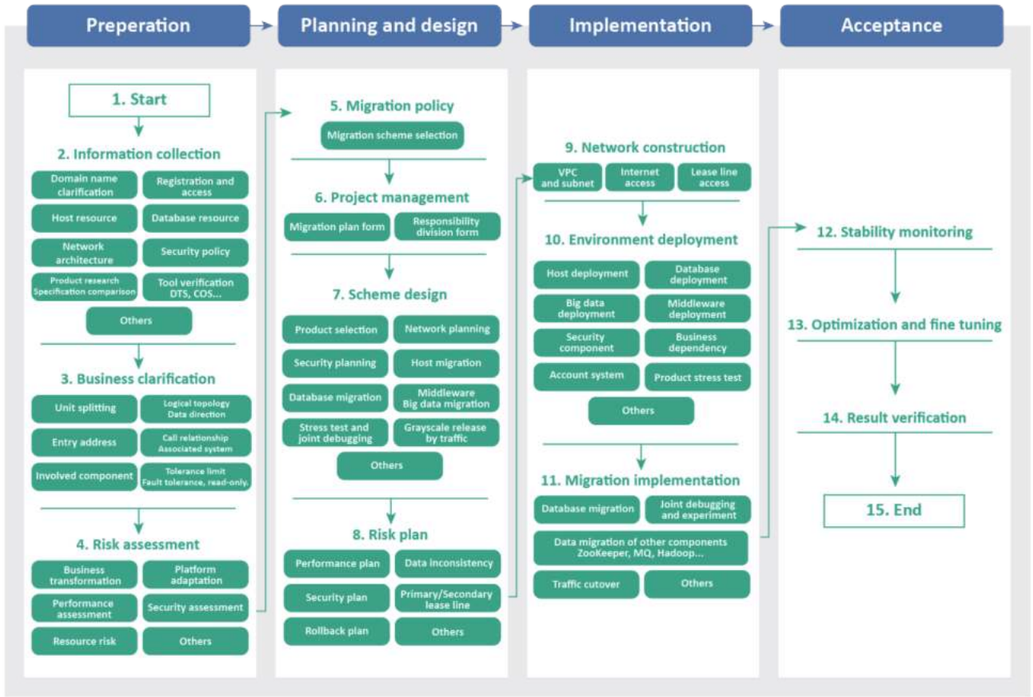
Live migration (hitless migration): Analyse the coupling of businesses and decouple the businesses. Businesses are switched in batches by module or product line to minimise the impact on businesses and realise a quick switch.

Migration teams: Migration can be performed by Tencent Cloud's migration service team or self-managed by the customer.

3. Cloud migration process

Figure 27 shows the general cloud migration process adopted by Tencent as best practice.

Figure 27: Cloud migration flowchart



Source Tencent

3.1. Preparation

Assess the following items:

1. Domain name analysis: Identify domain names required for business system access. Determine if domain name filing is needed.

2. Account system: Tenant account permissions and enterprise organisation management, including separation of ops and finance, login restrictions and project management.

3. Network architecture: VPC, IP range, subnet design, IP address planning, network architecture review and business subnet division.

4. Security rules: Security control implementation, network interconnection requirements and isolation policies.

5. Resource analysis: Distributed cloud, TCS, TCE product selection, resource usage and quotas. Identify special components or performance requirements.

6. Business analysis: Analyse coupling degree and call relationships between businesses. Identify special components or compatibility requirements.

3.2. Planning and design

1. Cloud migration assessment: Classify and assess the business systems on the original VMware to see which are suitable for cloud migration and which are suitable for cloud modification (see **Table 5**).

Table 5: Cloud migration options

Migration type	Feature
Cloud migration	▪ Involve only IaaS-layer alternatives by migrating VMware VMs to cloud VMs. ▪ It is suitable for scenarios with high application modification complexity.
Cloud modification	▪ Transform tightly coupled architectures into loosely coupled or distributed architectures. ▪ Enable cloud native capabilities such as containers, microservices and DevOps. ▪ Upgrade self-built open-source components to enterprise-grade cloud PaaS.

Source Tencent

2. Migration strategy: Confirm the migration plan (suspension or hitless migration) based on customer requirements, costs and complexity.

3. Project management: Establish a migration team, define the migration plan and assign responsibilities.

4. Detailed design: Develop a detailed plan, including SOW and operational manuals.

5. Emergency plan: Ensure migration robustness and define rollback procedures to reduce business impact. Common risks and mitigation measures are as follows (see **Table 6**).

Table 6: Cloud migration emergency plan

Risk	Measure
IP change	▪ Check business access. If the IP address is fixed, keep the private IP address unchanged during migration, if possible.

	▪ Register a public IP address 20 days before migration to ensure normal business access.
Business interruption	▪ Migrate at off-peak hours.
	▪ Keep the source online during migration and stop original businesses only after the last incremental synchronisation and business switch are completed.
	▪ Build a primary/secondary environment for the source and target.
	▪ Make sure that each migration step supports rollback.
Network instability	▪ Use direct connect for migration, which can ensure network stability and greatly accelerate migration.
	▪ Import images of source virtual hosts to reduce dependencies on the network during migration. In this case, incremental synchronization is required.
Data inconsistency	▪ Use full synchronization together with multiple incremental synchronizations, and stop data write to the source before the last synchronisation.
	▪ Stop data write to the source before migration to ensure that the data to be migrated is full data.
	▪ Back up the source data before migration by the customer.

Source Tencent

6. Risk management: Mitigate uncontrollable factors that may cause project failure. If unavoidable, minimize losses. For common risks, a rollback plan is required. The common triggering conditions for rollback are as follows:

(a) The data synchronization task is interrupted unexpectedly, and the incremental data cannot be totally synchronized during the migration.

(b) Data inconsistency exists after verification. The data synchronization mode and service write status need to be checked.

(c) Businesses are unstable after migration, which is difficult to solve quickly. Rollback is required for re-assessment and migration experiments.

In the first two cases, stop the migration, find out the cause, and conduct the migration again.

In the third case, re-assess the migration scheme, and conduct migration experiments and verification for the adjusted scheme.

3.3. Implementation

The implementation phase for cloud migration adheres to the following principles:

1. Parallel migration: Maintain identical environments and component versions to avoid compatibility issues caused by environmental discrepancies.

2. Downward compatibility: If no exact version counterpart exists, follow downward compatibility principles or evaluate self-built solutions.

3. Data consistency: Ensure data consistency before and after migration for disk-stored data.

4. Comprehensive testing: Because a single component may have multiple migration approaches or adjacent versions, fully consider business scenarios and conduct compatibility tests.

In addition to environment deployment and data synchronisation, implementing the migration is the key step. During off-peak business hours, migrate predefined services at appropriate time points according to the pre-designed scheme.

Strictly follow the migration steps to avoid migration failures caused by premature or delayed operations.

Migration is categorised into offline migration and hitless migration.

The offline migration (cold migration) process is as follows:
The cold migration process is shown in **Figure 28** and consists of six main process stages.

Figure 28: Cold migration process

Source Tencent

1. Prepare the environment.

    a. The source environment is deployed 1:1 on distributed cloud, TCS and TCE (or minimise deployment according to the business unit with elastic scaling later).

    b. Establish DC tunnel and confirm intranet connectivity.

    c. Configure monitoring and alarm rules for all products.

2. Prepare the migration.

    a. Disable frontend traffic ingress during the migration.

    b. Synchronize data files.

3. Verify consistency.

    a. Enable read-only for source databases.

    b. Perform incremental synchronization and consistency checks.

c. Modify the read-write address of business databases.

4. Forward the traffic: Add the distributed cloud, TCS or TCE environment to the forwarding queue at the source access layer.

5. Switch DNS.

a. Switch DNS entry addresses.

b. Maintain traffic forwarding at the source environment.

c. Monitor business metrics and metric data.

d. Observe service stability after completing all entry address modifications.

6. Conduct the rollback plan.

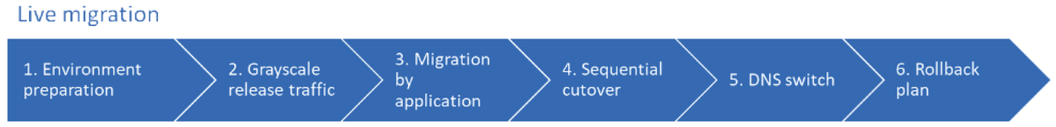
a. Disable Cloud Load Balancer (CLB) traffic.

b. Revert DNS to the source environment.

c. Inspect and rectify source environment data.

The hitless migration (live migration) process is as follows:
Figure 29 shows the live migration process, consisting of five stages.

Figure 29: Live migration process



Source Tencent

1. Prepare the environment.

a. The source environment is deployed 1:1 on distributed cloud, TCS and TCE (or minimise deployment according to the business unit with elastic scaling later).

b. Establish DC tunnel and confirm intranet connectivity.

c. Configure monitoring and alarm rules for all products.

2. Conduct the grayscale test.

a. Configure business data read/write on distributed cloud, TCS or TCE environment to be directed to the source environment.

b. Add distributed cloud, TCS or TCE business layer to forwarding queue and adjust weight.

c. Observe business status and log monitoring.

d. Track monitoring, databases and big data synchronization status.

3. Migrate applications sequentially.

a. Enable read-only for source databases.

b. Perform incremental synchronization and consistency checks.

c. Modify the read-write address of business databases.

d. Sequential migration: Migrate applications progressively until all database migration is completed.

4. Switch DNS.

a. Switch DNS entry addresses.

b. Maintain traffic forwarding at the source environment.

c. Monitor business metrics and metric data.

d. Observe service stability after completing all entry address modifications.

5. Conduct the rollback plan.

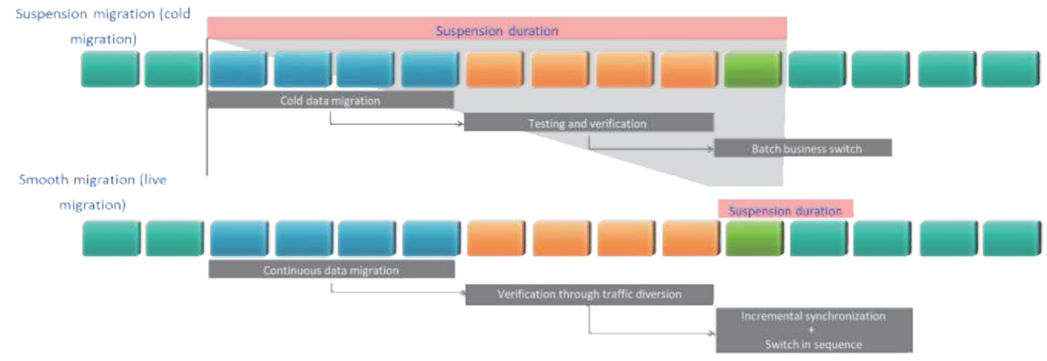
a. Redirect CLB traffic and application databases to the source environment.

b. Revert DNS to the source environment.

c. Inspect and rectify data.

Comparing the service downtime of the two migration strategies
Figure 30 shows the comparison of service downtime between the two approaches to cloud migration.

Figure 30: Downtime comparison: Suspension migration vs. smooth migration

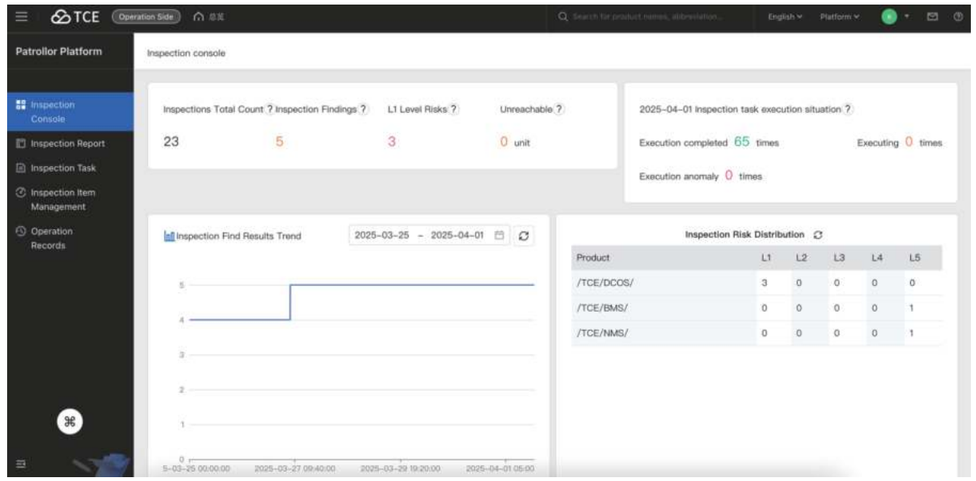


Source Tencent

3.4 Acceptance

The acceptance phase, focusing on verifying migration outcomes, is shown in **Figure 31**. Post-migration observation should last 48 to 72 hours, covering business peak and off-peak periods to monitor business stability and cloud product performance metrics for optimisation. After confirming business stability through observation and completing system checks, finalise documentation, hand over outstanding items and ensure business continuity.

Figure 31: Cloud platform monitoring dashboard



Source Tencent

Conclusion

The evidence from the survey clearly showed that the majority of VMware customers have been unhappy with the changes made since Broadcom's acquisition of VMware. The other clear observation is that the majority of VMware customers are considering migrating away from VMware but remaining on a virtualisation platform (73%). The second most popular option is to migrate to adopt cloud computing (14%), with the adoption of cloud native (Kubernetes) a close third at 13%. These customers are looking for an alternative vendor/solution to deliver an improved TCO and be secure and resilient. Tencent Cloud has focused its development on three main approaches to delivering a VMware alternative that match the survey findings.

Firstly, for the remaining-on-VMs scenario, Tencent Cloud has developed its offering based on its public cloud operating environment, which has been tried and tested over many years as a reliable and secure virtualisation platform. Furthermore, this platform supports a wide selection of services that Tencent Cloud and third parties have developed for the platform. An example of Tencent's capability in this scenario is the Tencent Cloud Local Dedicated Cluster (CDC), which is a newly launched managed infrastructure product aiming to extend the centralized public cloud service to a near-field service that can be implemented in the user's own facility. CDC deploys local computing power in the user's data center in the form of an integrated cabinet. Resources are connected to nearby public cloud regions for unified management. Users can manage CDC resources through existing public cloud tools (console, API, etc).

Secondly, Tencent Cloud is a global public cloud provider and has developed a mature and tested process for migrating VMs from on-premises to a cloud environment. Tencent Cloud supports the standard approach to private and public cloud management and procurement by offering flexible payment methods and the ability for its offerings to be used by enterprise and service providers to deliver cloud services to internal customers or external customers. For example, Tencent Cloud Dedicated Zone (CDZ) is a dedicated availability zone deployed on the customer's on-premises infrastructure. Customers can purchase Tencent Cloud resources, such as compute, storage and database, and use them in the same way as they would in Tencent's public cloud. CDZ provides a full set of services with integrated hardware and software, which makes deployment fast and simple.

For scenarios requiring full physical isolation, Tencent Cloud offers the Tencent Cloud Enterprise (TCE) solution. This enables the complete privatisation of public cloud technologies, allowing on-premises deployment to deliver localised cloud computing services.

Finally, Tencent's Distributed Cloud for cloud native applications solution is based on a multi-layer model. The core base layer is the infrastructure that supports compute, network and storage. This layer must be common across all approaches, cloud native or virtualised. The second layer provides the choice of cloud-native architecture to the customer, TKE or TCS. The third layer delivers integrated capabilities such as database, security, middleware, etc. Tencent, in this layer, also supports third-party offerings. Next, is the integrated security layer, which includes a series of security protection capabilities—for example, a cloud firewall (CFW), which supports active firewall access control lists (ACL), real-time intrusion blocking, virtual patching, and malicious code detection. The final layer is where multi-cloud management and customisations can be applied.

Appendix

Tencent Cloud's product portfolio demonstrates advantages compared to OpenStack and hyperconverged infrastructure systems (HCI) in alternative and upgrade scenarios beyond VMware alternatives (see **Table 7** and **Table 8**).

Table 7: Comparison of OpenStack and Tencent Cloud solutions

	OpenStack	Tencent Cloud
Technical architecture	Focuses on IaaS with a lightweight foundation and lacks PaaS solutions. Requires vendor-specific integration on an open-source framework with prolonged integration cycles and an unstable product roadmap.	Complete IaaS and PaaS capabilities with financial-grade high availability (HA) and unified ops system. Delivers sustainable iteration based on public cloud architecture, offering full-stack cloud solutions.
Availability	Only IaaS-layer HA is available. PaaS requires self-build or vendor dependency with inconsistent availability across layers.	IaaS and PaaS-integrated HA design follows public cloud standards with industry-leading business continuity.
Elastic scalability	Elastic scalability is limited by the overall maximum scale and generally, a single cluster does not exceed 500 nodes.	A cluster supports 10,000+ nodes, and can be scaled out across data centres. Supports hybrid cloud architecture and access to Tencent's public cloud through DC for enhanced responsiveness.
Sustainability	OpenStack's market share is gradually decreasing and there are community continuity risks because vendors are exiting the OpenStack ecosystem.	Provides a self-controlled cloud platform with full code ownership, consistent architecture with public cloud and continuous feature updates, representing mainstream private cloud development.
Security	Relies on third-party security products with high integration complexity and costs.	Offers cloud native security solutions with elastic scaling, a comprehensive protection system and level 3 cybersecurity classified protection 2.0 certification.
Easy to use	Focuses on IaaS-layer ops. Additional products require separate ops system development.	Delivers a unified ops portal integrating authentication, monitoring, Configuration Management Database (CMDB), logs and third-party platform connectivity for unified operations.

Source Tencent

Table 8: Comparison of HCI and Tencent cloud solutions

	Hyperconverged infrastructure system (HCI)	Tencent Cloud
Scalability	Compute-storage integrated architecture limits large-scale expansion.	Flexible compute-storage separation architecture enables superior scalability.
PaaS capability	Focuses on IaaS, with open-source PaaS deployment requiring self-management.	Provides full-stack cloud with comprehensive PaaS capabilities.
Operational availability	Offers a basic management console lacking advanced ops capabilities.	Delivers full-stack cloud with built-in monitoring, logging, CMDB, capacity management, approval management and multi-tenant support for automated ops.
Security	Provide fragmented security capabilities and rely on third-party products.	The full-stack cloud provides comprehensive security capabilities and has successfully supported customers like UnionPay Cloud and CCB Cloud in secure cloud migration.
Availability	Only provides resources without the intra-city active-active and 2-region-3-DC architecture.	Supports the intra-city active-active and multi-site multi-active architecture with complete disaster recovery capabilities.

Source Tencent

Methodology

Omdia conducted a double-blind survey on behalf of Tencent: the survey respondents did not know it was being undertaken by Omdia or on behalf of Tencent, and Omdia and Tencent did not know who the respondents were. The key criteria of the survey was the respondents must be current VMware customers; a secondary selection for participation was made on only those with plans to move away from VMware. Tencent provided Omdia with a deep dive technical briefing on its solutions and processes so the analysis of its capabilities could be written.

Further reading

Understanding the People and Process Challenges with Deploying Data Center Automation Technologies (March 2021)

About Tencent Cloud

Tencent Cloud, one of the world's leading cloud companies, delivers advanced technology solutions worldwide. Its capabilities encompass cloud computing, AI, and big data services customized for enterprises, organizations, institutions, and individual developers globally. Currently, Tencent Cloud's infrastructure spans 21 regions, operates in 56 zones, and covers over 1 million global servers and 3200+ global acceleration nodes, aside from 200T global bandwidth reserve and 400+ authoritative certifications. Tencent Cloud develops comprehensive industry-specific solutions, fosters an open and collaborative cloud ecosystem, and empowers diverse sectors in their digital transformation journeys.

Author

Roy Illsley
Chief Analyst, Cloud and Data Center Practice
askananalyst@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together “Informa TechTarget”) or its third party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.