White Paper

VMware Cloud on AWS: Facilitating Agile Datacenter Extension and Virtual Desktop Infrastructure in the Public Cloud

Sponsored by: VMware

Shannon Kalvar Deepak Mohan

December 2020

IDC OPINION

The COVID-19 pandemic is the first crisis to hit the market since the emergence of public cloud IaaS as a major component of the enterprise IT landscape. The cloud's promises when it comes to elastic consumption, Agile development, and global reach are being put to the test. IDC research shows that IaaS platforms have, after some initial issues, met this test and played a critical role in both business continuity and the emergence of business resilience.

The cloud's benefits of elasticity and automation, allowing businesses to scale and shift service delivery points as needed with minimal manual intervention, are proving invaluable in today's environment. Cloud has expanded beyond being the underlying IT system for niche ecommerce segments. The use of cloud now spans a much broader swath of digital activities. Of particular note, datacenter extension and virtual desktop infrastructure (VDI) have emerged as resilient use cases of the public cloud during the COVID-19-related disruption.

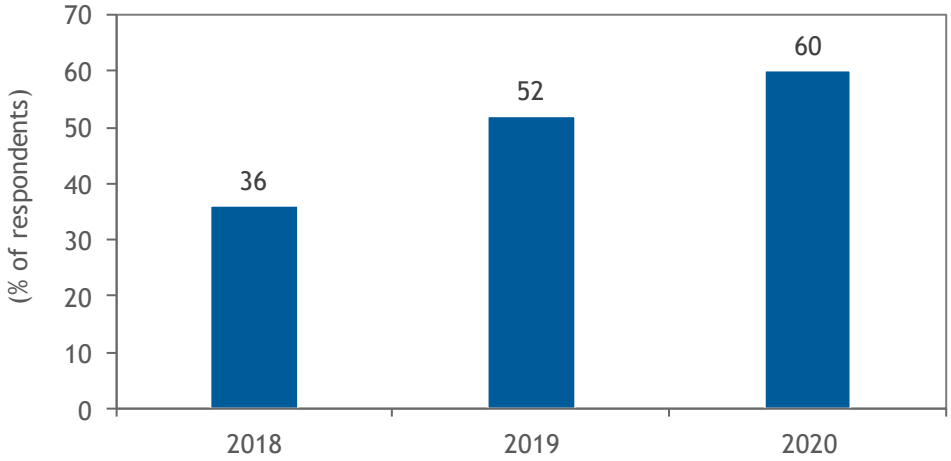
Realizing these benefits is dependent on achieving environmental consistency within a technical service, using consistent operations platforms/tools across environments, and achieving consistency across the enterprise's technology ecosystem. In particular, virtual desktop infrastructure is heavily impacted by data gravity and latency, while datacenter extension beyond momentary bursts requires careful management and a high degree of operational automation/flexibility.

HYBRID CLOUD ARCHITECTURES ENABLE AGILITY

Over the past decade, public cloud has transitioned from the realm of developers and secondary use cases and gained acceptance as a viable alternative for nearly all IT infrastructure needs. The use of public cloud alongside on-premises infrastructure is growing rapidly. IDC research shows that spending on public cloud infrastructure services will exceed spending on traditional on-premises infrastructure systems by enterprises within the next five years and that a majority of enterprises are already using public cloud in one form or another for their IT needs (see *Worldwide Public Cloud Infrastructure as a Service Forecast, 2019-2023,* IDC #US44178519, July 2019). This disruptive trend has further underscored the importance of agility and flexibility for IT, and cloud has emerged as a de facto way to enable both agility and flexibility. At the same time, enterprises tend to continue to have a certain level of traditional or private cloud infrastructure footprint on premises for total cost of ownership (TCO), compliance, or sunk investment reasons. This dichotomy of needs — combined with the reality that public cloud adoption is rarely a step function transition — has resulted in the growing prevalence of hybrid cloud environments (see Figure 1).

FIGURE 1

Growth of Hybrid Cloud Environments, 2018-2020



n = 1,500 (representing North America = 60%, EMEA = 20%, and Asia/Pacific = 20%)

Note: Respondents included IT decision makers (85%), provider selection owners (40%), and influencers (36%). (Respondents could select more than one.)

Source: IDC's *IaaSView Survey,* 2018, 2019, and 2020

The transformation of IT to a hybrid cloud environment involves a myriad of components such as emerging technologies, open source standards, cloud-native stack, modular applications built with containers and microservices, APIs, orchestration tools such as Kubernetes, DevOps best practices, automation, and stringent governance/compliance. These components must be built around a hybrid cloud architecture, which offers cost efficiency, access to cutting-edge technologies, better risk management, optimal placement of workloads, freedom from data gravity, on-demand infrastructure scalability, and so forth. This is especially true for broad use cases that impact a large portion of the enterprise's operations and user communities. Commonly seen hybrid cloud use cases, which are also common use cases used for an initial move to the cloud, are datacenter extension and virtual desktop infrastructure. In fact, these two use cases are linked. The COVID-19 pandemic has made the cloud more critical to IT transformation as enterprises are forced to reimagine their business models more drastically than before. The shift of employees to work from home (WFH) has been the top impact to businesses and has accelerated the move to extend datacenters and workspaces to a hybrid cloud environment.

IN THIS WHITE PAPER

The holy grail in cloud computing, sought by IT decision makers and practitioners alike, is a frictionless, hybrid cloud that provides consistent infrastructure and operations and unified management across public and private clouds and traditional on-premises infrastructure that will drive insights, innovation, and growth. This white paper outlines key considerations for enterprises as they pursue these hybrid cloud benefits and provides an overview of VMware Cloud on AWS and its capabilities in two common hybrid cloud use cases.

Note: All numbers in this document may not be exact due to rounding.

Datacenter Extension

Datacenter extension is the expansion of the infrastructure capacity of an existing datacenter by leveraging additional infrastructure resources in the public cloud. This is typically planned and executed by the central IT stakeholders who operate the primary datacenter, often in consultation with the application stakeholders who develop, deploy, and maintain the application.

An enterprise's IT decision makers see the value of cloud-native and higher-layer services. Running applications on public cloud IaaS makes it easy for the enterprise, whether central IT or lines of business (LOBs), to leverage technologies such as artificial intelligence (AI), machine learning (ML), and dynamic scaling. Yet creating an integrated hybrid IT environment involves several areas of particular focus.

Use Case Scenarios

The journey to leverage public cloud infrastructure is well underway in all types of businesses. Typical scenarios driving datacenter extension include:

- **Datacenter footprint expansion** to prepare for growth, without taking on additional facilities leases
- **Gradual datacenter evacuation** that involves incrementally moving workloads from the customer datacenter to the cloud
- **Temporary increases in capacity needs** to accommodate for seasonal or event-driven IT capacity increases
- **Geographic separation** of primary and secondary data and resource locations to meet disaster recovery or regulatory requirements (e.g., GDPR and HIPAA)

Key Considerations in the Datacenter Extension

Consistency of Experience

IT organizations and practitioners require a consistent usage experience for applications and operations across the infrastructure. To this end, there is an increasing level of partnerships between public cloud providers and traditional enterprise IT and services companies to deliver a seamless transition between environments. Such integration partnerships focus on providing public cloud environments that are environmentally consistent with their respective private cloud offerings at enterprises, highlighting the emphasis and prioritization of hybrid infrastructure and the demand for a coherent experience across public cloud and on-premises infrastructure. This consistency, or lack thereof, is both a top priority and an ongoing challenge.

When IDC's 2020 IaaSView Survey asked enterprises about the top considerations in their hybrid cloud environment, 58% of respondents cited consistent management workflows, and 45% of respondents cited consistent environments between on premises and cloud.[1]

---

[1] For more details, see *IaaSView 2020: Survey Findings* (IDC #US46783620, August 2020).

Flexibility and Speed

Flexibility via best-fit compute resources allows enterprises to reap the benefits of extending their datacenters to the public cloud. On-demand infrastructure provides instant access to hardware, software, and services; deployment and provisioning can be done in minutes rather than days or weeks. Cloud resources can be quickly scaled up or down based on workload requirements. High-availability (HA) resources provide built-in robust solutions for disaster recovery, backup, and archiving. Access to emerging technologies, cloud services, and a vast array of tools and platforms is the flagship of public cloud. In addition, execution time benefits from cloud infrastructure come from the wide array of virtual machine (VM) configurations and processor speeds offered by cloud providers.

Cost

Cost savings continue to be a top objective in extending datacenters to the cloud, with TCO being the most cited (53%) factor[2] in the selection of a public cloud provider, according to IDC's 2020 *IaaSView Survey.* The cloud itself brings cost savings in moving costs from fixed capex to flexible opex. 60% of the organizations surveyed reported realizing cost savings from adopting public cloud infrastructure – savings due to the cost of cloud infrastructure itself as well as the cost of operations. On the other hand, enterprises must also consider the costs associated with the migration of applications and/or data to the cloud. To minimize the effort of migration, enterprises require consistency between their on-premises and cloud environments for DevOps as well as the runtime experience.

Current Challenges with Datacenter Extension

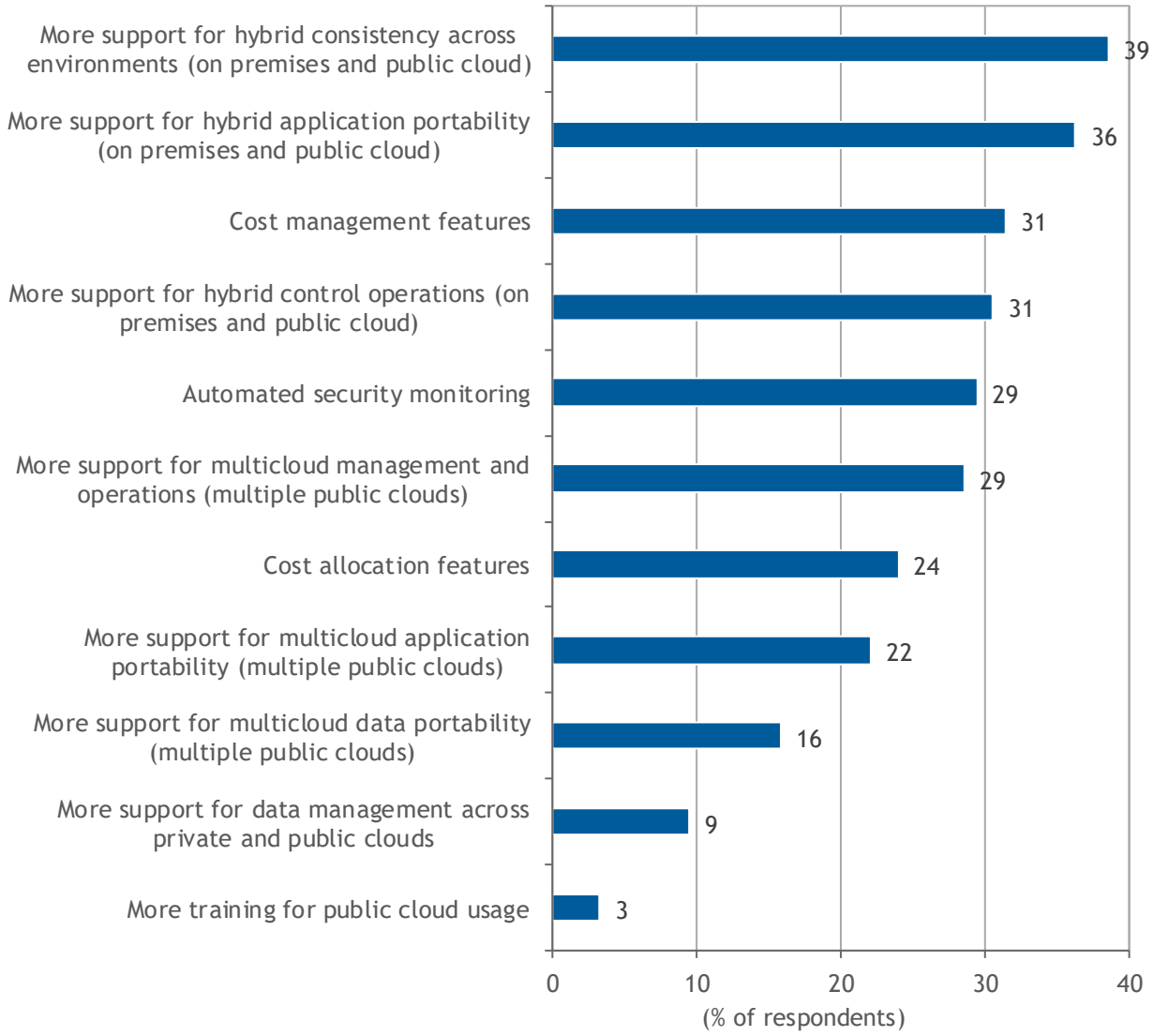
While the vision of a seamless hybrid IT environment is compelling, in practice, there are challenges in achieving this. Enterprises are demanding greater hybrid cloud enablement services from their cloud partners, with consistency of environments and application portability topping the list (see Figure 2). One important aspect to note is that these are the considerations during the early adoption phase of hybrid cloud. As customers mature and gain confidence in their hybrid cloud environment, the focus often shifts to areas such as automated resource optimization and application modernization.

[2] For more details, see *IaaSView 2020: Survey Findings* (IDC #US46783620, August 2020).

FIGURE 2

Services That Are Delivered in Hybrid Clouds

Q. What additional services would you like to see delivered into the ecosystem?



n = 1,500

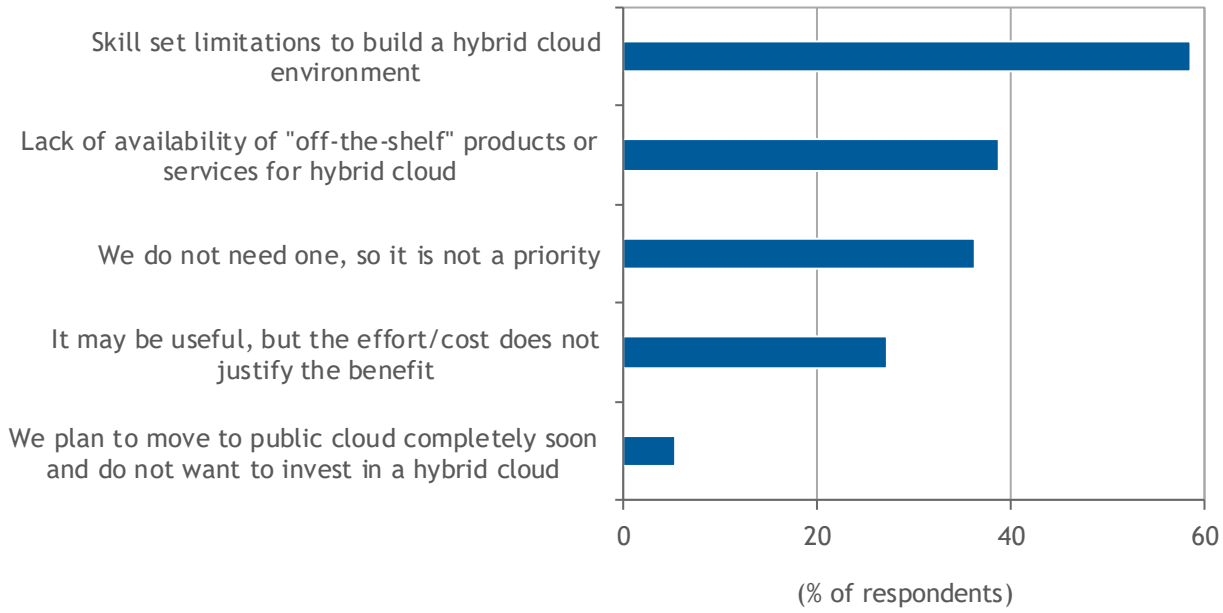
Note: Respondents included IT decision makers (85%), provider selection owners (40%), and influencers (36%). (Respondents could select more than one.)

Source: IDC's *IaaSView Survey,* 2020

The biggest perceived barrier to achieving a seamless hybrid environment is the limited skill sets to implement and operate an effective hybrid environment (see Figure 3). As enterprises develop their hybrid cloud infrastructure to extend their datacenter environment, they must proceed with a gradual skill set transition from their existing infrastructure ecosystem to cloud infrastructure and services for their enterprise IT needs. Examples include building workflows that offer a consistent experience and planning value-added adjacencies that minimize the friction in transitioning workflows and skill sets. Of course, consistent environments will minimize skill disparity, but training and development will be required to leverage the new technologies in the public cloud.

FIGURE 3

Obstacles to a Successful Hybrid Cloud Implementation



n = 242

Source: IDC's *IaaSView Survey,* 2020

Virtual Desktop Infrastructure in the Cloud

Virtual desktop infrastructure is the combination of server, storage, and network components required to provide computing resources to run virtual desktops or applications, in addition to providing those virtualized desktops with their resources. This nexus of network-enabled interface devices connected to compute, storage, and display "wraps around" the user (who is at the center of this workspace paradigm), allowing for a fluid hybrid digital-physical service that adapts to and enables multiple styles of work. This "wrapper" of components is device independent and designed to abstract applications and desktops away from the client device, allowing for additional layers of control and security.

Virtual desktops, long a feature accounting for 1 in 10 of client deployments in an enterprise, have almost doubled in average utilization. The COVID-19 pandemic has accelerated this growth, with 2020 being the "year of VDI" — enterprises saw 50–60% of employees work from home during 2020.[3] And while enterprises have been able to advance their capabilities for supporting a remote workforce, 2021 may see a "return to work." IDC research indicates that enterprises expect 30% of their workforces to work from home during 2021.

Traditional VDI was limited to drawing resources from the device or the bespoke hyperconverged systems established for their use; modern cloud-enabled systems draw on resources from bespoke systems, the enterprise's private cloud, third-party hosted environments, public clouds, and increasing the edge near the user to create complex digital workspaces.

This shift from traditional datacenter-specific VDI to a broader implementation of services across computing environments has brought both new capabilities and exposed fundamental challenges. These new capabilities have enriched the traditional use cases with accessibility, intelligence, and versatility; the fundamental challenges of access control and latency, however, are even more pronounced.

Use Case Scenarios

VDI in both traditional and cloud-enabled environments is used to address the following issues:

- **Remote work,** where individuals, teams, or entire enterprises no longer work within the enterprise workplace but instead can function wherever they are, whenever they need to
- **Compliance** with industry standards, legal requirements, or government regulations (e.g., HIPAA, ISO certifications, DOJ, DOE, and DISA), which affects the company's business and requires specific controls on specific devices, users, and digital work environments
- **Compatibility,** where aged applications that either cannot be rewritten at an affordable cost or cannot be maintained are offered in a customized environment so they can run on any device
- **Control,** where the organization uses virtualization to manage installation and entitlement to expensive or high-value applications
- **Recovery/continuity,** where the organization uses virtualization to provide functional working environments for short durations, often in bursts, to account for specific time-limited disruptive events

The Cloud Unlocks Use Cases That Traditional VDI Could Not Deliver

The cloud not only *addresses and expands* on these use cases, making them possible at scale, but also unlocks use cases the industry has considered for decades but has been unable to address, including:

- **Intelligent workspaces.** Combine virtualization with artificial intelligence to organize an individual's work, enhance collaboration, manage entitlements, and embed security. Intelligence requires access to amounts of parallel processing only affordable to the largest enterprises at scale if purchased privately; public cloud providers make this capability broadly affordable.

---

[3] For more details, see *Worldwide Virtual Client Computing Software Forecast, 2020–2024: Accelerated Adoption Offset by Economic Instability* (IDC #US46516219, June 2020).

- **Virtual-first workspaces.** Beyond remote work, a virtual-first workspace assumes that the workspace exists first in the cloud and expresses itself on the devices. Unlike a traditional remote work scenario, where resources are drawn from the datacenter regardless of the user's location, a virtual-first workspace draws resources from the nearest available cloud, which is simultaneously closest to the data and applications it needs to function.

  The virtual-first workspace allows for the long spoken about but rarely achieved ideal of instant provisioning, where any enabled worker in the company can log in to any available endpoint, including one direct from a manufacturer, and access their workspace within seconds.

Key Considerations in VDI in the Cloud

VDI, whether traditional or cloud enabled, is highly dependent on the following:

- **Latency.** The aggregate of the speed with which a virtualized application, desktop, or workspace responds to the user's request is the single most important factor in whether the deployment will be perceived as a success or a failure. Optimization and management of latency, in a wide range of ways, lie at the heart of VDI operations and approaches.
- **Data gravity.** The key to latency, especially in cloud-enabled environments, is data gravity; the design idea is that VDI should reside as close as possible to the location where data and applications live.

  Data gravity in traditional VDI scenarios is limited to the enterprise datacenter. However, in the cloud-enabled era, it is radically more complex, with the data and applications needed for the workspace existing in multiple locations, often dynamically assigned by the underlying algorithms rather than static architectures. Meeting this consideration requires more than just careful design and reference architectures; it requires a radical rethinking of how VDI operations and management software handles resources in complex environments.
- **Heterogeneous compatibility.** Modern enterprises, with their diversity of geographic and demographic distribution, must adapt to the requirements of latency and data gravity across a wide range of devices, configurations, and network capabilities, simultaneously and synchronously. It is possible that the largest enterprises might invest in the datacenter and network infrastructure to do this; however, most enterprises will use a combination of network virtualization and public cloud infrastructures to meet this need while relying on cloud-enabled workspace providers to handle device compatibility.
- **Interoperability.** The diversity of resources described previously brings with it an intricate tapestry of interconnections and interoperability requirements — APIs and data flows, data formats, and AI models, which must coordinate seamlessly at low latency, with the best data gravity to present a workspace in a way that is compatible with a heterogeneous environment. These challenges must be resolved seamlessly, without user intervention, or the deployment will fail.
- **Security in depth.** A zero-trust security model for the virtual workspace is just the beginning of protecting a VDI system in the cloud era. With resources distributed across everything from the edge to the private datacenter, every element must be part of a single, unified security scheme, which is monitored and adapted in real time without impacting interoperability, heterogeneous compatibility, data gravity, and latency.
- **Consistent operations.** Where possible, virtualization should fall into the operational tools and framework used for other aspects of the enterprise.

Evolution to Virtual-First, Cloud-Enabled VDI Accelerated by the COVID-19 Pandemic

Going into the pandemic, the IT architecture in many organizations was still a jumble of 2nd Platform (client/server era) tools mixed with some 3rd Platform technologies (cloud, mobile, and social). Digital transformation (DX) efforts were stalled or slow rolling, with long "time horizons" and limited impact on the virtualization environment except in the most forward-thinking organizations.

During the COVID-19 pandemic, as more workers have shifted to "remote work" solutions, the last-mile problem of residential network infrastructure has become increasingly problematic. Even if WFH requirements fall from an estimated 60% to an estimated 30%, the numbers of WFH employees still represent an opportunity for improvement. As Windows 10 and later generations become the client computing standard, systems will have to deal with increasing graphical burdens across a range of applications. This issue can be addressed by integration within the hyperconverged stack, integration of AI-dedicated chips to manage cognitive workflows, and integration of graphics processors to accelerate rendering. If such issues are not properly managed, the VDI market in the cloud will remain impeded by network performance.

Current Challenges with Traditional and Cloud VDI

The current challenges driven by both the rapidly accelerated transformation and the corresponding architectural shifts are discussed in the sections that follow.

The Shift from Business Continuity to Business Resilience

Virtualization is one of many approaches and techniques that deliver the remote work experience. Many of those approaches, including using VPNs or remote desktop technology, provide immediate business continuity relief, but they do not set up the enterprise for the shift to long-term resilient operations in an uncertain environment.

Return to Work and Ideal Remote Work Ratio

While 2020 saw a ramping up of desktop virtualization, enterprises may soon experience the challenges of "ramping down" these virtual environments. Organizations may attempt to return to "normal" too quickly, where normal is what they originally perceived as their ideal remote work ratio, rather than building the technical and cultural infrastructure required to become an agile, digital company. This can lead to problems in recruitment, retention, and resilience as the pace of disruption accelerates.

Unpredictable Shifts

As described previously, the most significant market development in the past 18 months has been the marked upshift in the percentage of users in the enterprise environment who consistently use application and/or desktop virtualization. IDC surveys indicate that this percentage had hovered at 10–20% in recent years, and it has upticked to 20–30% in enterprises and new businesses.[4] The COVID-19 pandemic and associated economic disruptions will continue for at least 24 months, forcing periodic and unpredictable shifts in WFH arrangements, varying the percentage of the workforce working from home at least one day a week from 20% to as high as 70% during regional WFH lockdowns. This will likely stabilize to 30–40% during the pandemic period and retreat to 20% afterward.

[4] For more details, *see Worldwide Virtual Client Computing Software Forecast, 2020–2024: Accelerated Adoption Offset by Economic Instability* (IDC #US46516219, June 2020).

Maintaining Operational Readiness Across the Changing Environment

In addition to the leadership, social, and practical challenges this shifting environment brings, the organization must maintain operational readiness across its technical estate to respond to security threats and interoperability issues. Many organizations were not operationally ready before the crisis; the increasing complexity of heterogeneous environments has exacerbated this situation. The steps taken to reduce the complexity of a solution, including reducing the number of vendors and the number of operational tools/frameworks related to the issue, may help with this challenge.

HYBRID CLOUD IMPLEMENTATION HAS ITS CHALLENGES

Hybrid cloud is not always the silver bullet solution for IT challenges. Hybrid cloud implementation and operations come with their own challenges, as revealed by IDC's 2020 *IaaSView Survey* results (refer back to Figure 3). Obstacles to the "holy grail" ideal of a frictionless hybrid cloud IT environment center around the three areas, which are described in the sections that follow.

Lack of Environmental Consistency

Migration to a cloud environment can range from basic rehosting ("lift and shift") to refactoring to rearchitecting of applications. The effort required will be determined in part by the level of consistency (or inconsistency) between the on-premises and cloud environments, along with the level of skills available within the migration team. The "team" may include support from the cloud provider to assist in the migration. Legacy inertia and the lack of access to skill sets or effective skill set transition frameworks will inhibit public cloud infrastructure adoption at enterprises. These fundamental difficulties in migration are a common impediment to successful hybrid cloud infrastructure.

Limited Operational Consistency

Enterprise IT organizations ranked the consistent management of workflows (provisioning, terminating, monitoring, etc.) as the most important attribute in their hybrid cloud environments. A lack of operational consistency between environments makes it difficult to monitor and automate processes, especially when building automations that span premises. This could include monitoring tasks, such as monitoring resources on premises and in public cloud in a consistent manner, or scaling tasks, where organizations may wish to expand into public cloud in a seamless manner as needed using the same underlying provisioning mechanisms.

Dissimilar Tools and Frameworks

High among the top inhibitors to hybrid cloud adoption were the limited skills to build a hybrid cloud environment and the lack of off-the-shelf products or services for the hybrid cloud. The perceived effort and cost to govern and audit hybrid environments are seen as outweighing the benefit. Each public cloud IaaS provider has different workflow and management tools. IT organizations cite concerns with the lack of unified tools, especially in security monitoring and management across all providers, and regulatory constraints were seen as the second most cited reason *not* to host workloads in a public cloud environment.

Despite these challenges, organizations' abilities to master a multicloud or hybrid cloud environment will be a key contributor to company success or failure. The ability to integrate and manage such cloud environments will be a fundamental requirement for operating — not just as an IT organization but as a business.

VMWARE CLOUD ON AWS: A NONDISRUPTIVE PATH TO HYBRID CLOUD

VMware Cloud on AWS delivers to customers a ready-to-use VMware environment, completely managed and delivered as a service by VMware, within the Amazon Web Services (AWS) public cloud. VMware Cloud on AWS is based on VMware Cloud Foundation (VCF), which includes vSphere, vSAN, and NSX, built on Amazon Elastic Compute Cloud (EC2) bare metal servers featuring second-generation Intel Xeon Scalable processors. Customers can provision virtual machines and manage their infrastructures on VMware Cloud on AWS using the same VMware tools and process workflows that are used for the rest of their VMware environment. This includes access to services such as vSphere HA for high-availability workloads, vSphere vMotion to move workloads to and from a VMware Cloud on AWS environment, and NSX networking to build a common private network across deployments.

VMware Cloud on AWS is built with a deep level of technical integration across the VMware and Amazon Virtual Private Cloud (VPC) networking, allowing customer VMs within VMware Cloud on AWS to be on the same private network as Amazon EC2 instances and other AWS services launched within the customer's Amazon VPC. Customers can thus easily provision and use AWS public cloud services such as databases and analytics services alongside their VMware environment. Customers can also add and remove hosts on demand and benefit from the flexibility and agility features of public cloud.

VMware Cloud on AWS was launched in 2017 and is now available in over 17 AWS regions worldwide, including a special controlled instance running in AWS GovCloud, called VMware Cloud on AWS GovCloud (US).

Benefits of VMware Cloud on AWS

IDC highlights that inconsistent operational workflows and limited transferability of skill sets continue to be challenges to effective movement of applications and ongoing operation of hybrid cloud environments. VMware Cloud on AWS is designed to address this consistency gap by delivering a hybrid cloud environment that is consistent with and manageable by the familiar VMware tools and workflows that are used in many private cloud environments. Its use can facilitate faster adoption of cloud while lowering operating costs and increasing business value for enterprises. According to IDC research,[5] organizations that have deployed VMware Cloud on AWS have lowered three-year operating costs by 44% and have achieved three-year ROI of 351%.

VMware Cloud on AWS for Datacenter Extension

VMware Cloud on AWS allows the datacenter infrastructure to be extended into the public cloud in an on-demand manner, using the same tools and operations framework used for expanding the physical datacenter. VMware Cloud on AWS clusters can be managed from within the same vRealize Suite of management and operations tools to create a consistent operating environment within the public cloud identical to the one in which applications would operate within the on-premises datacenter. Popular vSphere features such as vMotion for load balancing, upgrades, and migrations between on premises and the cloud are also available.

Moreover, if enterprises are already running VMware on premises on Intel Xeon servers, their applications will benefit from the same Intel software optimizations and robust testing in VMware Cloud for AWS, leading to consistent and predictable application performance.

[5] For more details, see *The Business Value of Running Applications on VMware Cloud on AWS in VMware Hybrid Cloud Environments* (IDC #US46919520, October 2020).

Customer Benefits

IDC sees three categories of benefits for organizations extending their datacenters with VMware Cloud on AWS: migration, operations, and innovation enablers.

Migration

- **Consistent security framework.** Security is increasingly intertwined with cloud platform services and is an implicit priority in enterprise use cases. VMware Cloud on AWS allows for common security protocols across the hybrid cloud. Providing intrinsic security that is built into the infrastructure, VMware NSX uses software-defined networking to abstract the network and apply security policies to applications wherever they run – on premises (e.g., in VMs, in Kubernetes containers with VMware Tanzu, and on bare metal), on the AWS cloud infrastructure, or on edge devices. This environment consistency reduces security risk in migration of applications to the cloud.
- **Environmental consistency.** VMware Cloud on AWS was architected for that "holy grail" of hybrid cloud environments discussed previously. It provides multidirectional workload migration between on-premises VMware environments and the AWS cloud. In a recent study of organizations running important business applications on VMware Cloud on AWS,[6] IDC calculated that, on average, organizations incurred total migration-related costs that were 57% lower than those of another public cloud solution, including needing 59% less staff time. Completing faster migrations to the public cloud with VMware Cloud on AWS – 46% faster (or 4.5 months earlier) on average – helped those organizations start realizing the benefits of public cloud adoption at an earlier time, allowing them to capture these productivity- and business-related benefits sooner.
- **Capabilities of VMware HCX.** VMware HCX provides services for migrating, rebalancing, and replicating workloads (e.g., for business continuity or workload protection). These services facilitate private network connectivity and can support a gradual migration of components and safe failover. VMware HCX prepares the sending and receiving environments and initiates the migration or replication operations from the source. VMware HCX services can be accessed from an HCX Manager, via a plug-in vSphere, or via command line interface (CLI).

  VMware HCX extends the migration enablement framework on vSphere to enable multiple migration paths for customer VMs to and from public cloud. These services include VMware HCX vMotion, an extension of the familiar live migration capability delivered through vMotion; VMware HCX Cold Migration, for migration of virtual machines that are powered off; and VMware HCX Bulk Migration, for programmatic live migration of batches of virtual machines. Bulk Migration, in particular, has emerged as an extremely valuable feature, enabling practitioners to easily move multi-VM applications into the public cloud and back as needed without any downtime for the application.

Operations

- **Tooling consistency.** With consistent VMware infrastructure on both traditional and AWS environments, there is no need for retraining staff on new tools to manage the expanded datacenter infrastructure. Practitioners access the same VMware vCenter dashboard to manage the broader datacenter; vRealize products similarly manage the heterogeneous datacenter environment. This allows practitioners to rapidly avail themselves of the benefits of the hybrid cloud environment. It's a case of ROI – if organizations are going to invest valuable staff time on learning new tools, those tools should add corresponding value to operations rather than merely perform the same functions as existing tools.

[6] For more details, see *The Business Value of Running Applications on VMware Cloud on AWS in VMware Hybrid Cloud Environments* (IDC #US46919520, October 2020).

- **Flexibility and speed.** VMware Cloud on AWS provides for the rapid provisioning of additional resources. VMware reports the average time to deploy and provision additional hosts is on the order of minutes and the average time to deploy full software-defined datacenters is under two hours. Not atypical for public cloud providers, VMware Cloud on AWS offers automatic on-demand infrastructure scaling for best-fit compute, showing the value of having a scale-out cloud system that can be managed on a granular basis. VMware's Elastic DRS allows for automatic scaling of workloads to add (or remove) compute or storage resources seamlessly as needed.
- **On-demand pricing.** VMware Cloud on AWS offers consumption-based pricing for "pay-as-you-go flexibility." This allows organizations to optimally manage the cost of infrastructure, eliminating idle capacity while ensuring the availability of required resources on demand.

Innovation Enablers

- **Access to broader capabilities in AWS.** Public cloud continues to be the easiest accessible source for emerging technologies such as AI, ML, analytics, and IoT for most enterprises to support their digital transformation. With VMware Cloud on AWS, practitioners can take vendor tools that run on vSphere and move them to the breadth of compute power in the AWS cloud. They can also access all the advanced technologies and tools in AWS in a virtualized environment. Because of the environmental and operational consistency, they can easily move these between environments for development and test or runtime. Alongside this consistency, customers gain access to 175+ cloud services available within AWS to accelerate their modernization and transformation initiatives.
- **Managed service for focus on higher layer.** The consistency of environments and operations delivered in VMware Cloud on AWS reduces staff time spent on maintaining and operating the stack. This allows organizations to focus their time and talent on higher levels of digital transformation and application modernization, which delivers much higher payoff to the business.
- **Access to Intel software optimizations and special instructions.** VMware has partnered with AWS and Intel to test and tune VMware Horizon virtual desktop configurations on Intel Xeon Gold 6258R processor-based servers and Intel Optane Persistent Memory for improved performance of hyperconverged infrastructure.
- **Support for Kubernetes and containers.** Embedding Kubernetes into vSphere has broad accessibility and manageability advantages for application modernization in support of full-stack, multicloud, and hybrid cloud operations and automation. Tanzu Kubernetes Grid (TKG) delivers core Kubernetes technology available in VMware Cloud on AWS and helps customers deploy, scale, and manage containerized workloads within VMware Cloud on AWS. Tanzu Mission Control provides Kubernetes management that can be extended across any Kubernetes distro using open standard Kubernetes APIs, regardless of where it runs.

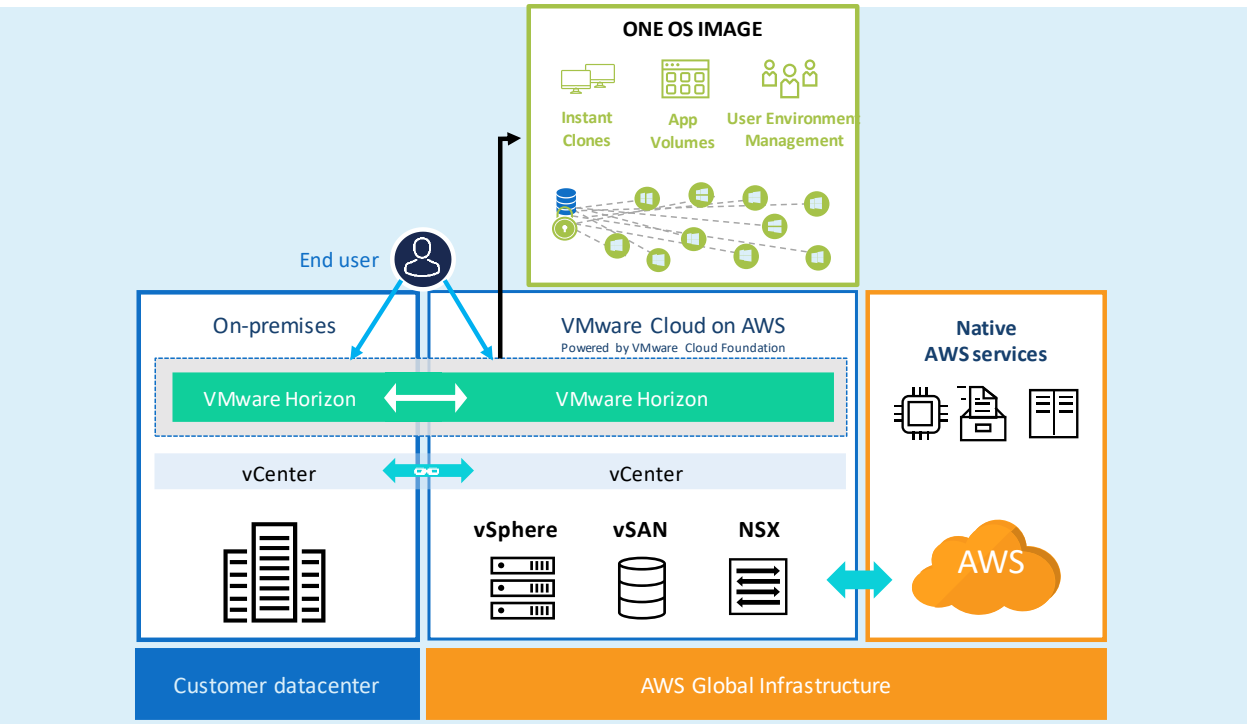
VMWARE HORIZON ON VMWARE CLOUD ON AWS FOR VDI

VMware posits that "if you've moved workloads to the cloud, it makes sense for your desktops to follow." VMware Horizon on VMware Cloud on AWS provides VDI capabilities for unifying physical desktop device management, digital workspace creation/operations, and client workspace security into the overall VMware Cloud platform. It is especially well suited to the use cases described previously, such as workloads with high data gravity, where moving the desktop to the data (rather than the reverse) results in increased performance. As described previously, 2020 has been the "year of VDI" because of the global pandemic, but this expansion will decline as organizations move their workforces back to the office (return to work). This should play to VMware's strength with the ease of bidirectional movement across on-premises and VMware Cloud infrastructures.

Building on the capabilities for a software-defined datacenter extension, VMware Horizon provides the means for organizations to manage desktops across cloud infrastructures using established skills and tools – familiar tools such as Cloud Pod Architecture for scaling across pods and sites, unified dashboards for health monitoring, and help desk services across the hybrid cloud, as well as the VMware stack of advanced features such as vSphere, vSAN storage, and NSX for security (see Figure 4). Practitioners will value the consistency of having all tools in one "basket," managed in a vCenter console server rather than having a cloud management solution and a VDI solution. They can manage both on-premises and VMware Cloud on AWS deployments in a single federated space as the Horizon architecture is the same for all environments.

FIGURE 4

VMware Horizon on VMware Cloud: On Premises and on AWS



Source: VMware, 2020

CITRIX ON VMWARE CLOUD ON AWS FOR VDI

Given Citrix's presence in VDI and virtualized Windows applications for desktops, both VMware and Citrix are committed to offer compatibility with their hypervisors. An example of "coopetition," VMware and Citrix both offer a guide to operating and managing the other's VM desktop environments. VMware has published a guide to VMware Horizon 7 for Citrix Administrators.

Customer Benefits

Monitor and Manage

Users can monitor and manage the entire user experience from the device behavior through the cloud using VMware Horizon modern management capabilities. The Horizon Cloud Management Console dashboard is the same for both on-premises and cloud environments and allows health monitoring of resources.

Security

Carbon Black's machine learning (ML)-based security technology is used to identify and resolve security issues in a single cloud fabric. Designed for security for virtual machines, this technology is more efficient and delivers better performance than security tools designed for physical desktops. For example, with nonpersistent desktops and applications in a cloud environment, if a user logs off, the instance can be removed immediately, reducing both costs and exposure to malware and threats.

Generic Capabilities

VMware Horizon on VMware Cloud on AWS allows the spinning up of AWS resources (GPU, CPU, storage) quickly and in a variety of configurations on demand. These resources include access to the latest AWS compute resources such as the Intel Xeon processor-based servers described previously. This access provides specialized workstation capabilities for intensive compute or graphics processing without purchasing the physical devices.

Amazon-Specific Capabilities

AWS offers a broad portfolio of cloud application platform components for building cloud environments across Amazon's EC2 base infrastructure, Elastic File System (EFS), EC2 Container Service, Availability Zones (AZs), and serverless functions. In addition, AWS offers access to an ecosystem of 650+ VMware Cloud on AWS competency partners as well as access to 175+ native AWS services and tools such as AWS Lambda, Alexa, and SageMaker applications without cross-cloud platform delays.

Flexibility

VMware Horizon on VMware Cloud on AWS provides the ability to expand application virtualization on demand, particularly for applications that were originally housed in the datacenter and now need additional resources, as in the dispersed "new normal."

CHALLENGES AND OPPORTUNITIES

Challenges

- **Complexity of cloud infrastructure.** The rapid diversification of cloud resources and footprints in multicloud environments creates extremely complex scenarios where the data and applications live in one cloud, but the capabilities required live in another cloud.

- **Shift in usage patterns.** The most significant market development in the past 18 months has been the marked upshift in the percentage of users in the enterprise environment who consistently use application and/or desktop virtualization. IDC surveys indicate that this percentage had hovered in the range of 10–20% in recent years, and it has ticked up to 20–30% in enterprises and new businesses. These developments coming into 2020 were further accelerated by the pressures of the dual pandemic and economic events. IDC expects upticks and downticks over the next four-year time frame. It is one thing to say "put this all in the cloud"; it is another thing to deliver on that promise over an extended period of time.

Opportunities

- **Continued datacenter expansion to cloud.** IDC sees a broad shift of work from "in-house" within the physical space of the office (and its associated network boundaries) to commonly used data and applications in hybrid cloud environments, which then become the target for shifting the location of the client.
- **Guidance and education.** To communicate its value, VMware should educate the global VMware partner community to be prescriptive in how VMware Cloud on AWS supports the wide variety of use cases.
- **Back to work.** As the COVID-19 pandemic wanes, businesses will recall remote workers. There will be opportunities to build on the benefits achieved during the wider desktop virtualization and remote work of 2020 while successfully shutting down excess remote deployments. This shift will continue to drive the opportunity to shift to "virtual first" end-user experiences, with the increased flexibility and operational complexity these experiences bring.

CONCLUSION

The events of the COVID-19 era have forced enterprises to adapt, first by ensuring business continuity by any means necessary and then more thoughtfully to evolve resilience and the ability to adapt their technology infrastructures to rapidly changing circumstances. The public IaaS companies stumbled briefly under increased demand but rose to the challenge; for their part, enterprise IT operations have begun to more consistently manage their internal operations and environments while consolidating their management tools. Vendors such as VMware and Amazon have responded to this need for consistency and consolidation by expanding and integrating their products to offer complete technical solutions intended to deliver business outcomes rather than incremental technical outcomes.

This accelerated evolution will continue as business resilience is tested over the next 24–36 months. Enterprises that partner with integrated ecosystems of IaaS and software vendors with evolving technical solutions will be better positioned to adapt to these changes than their competitors that attempt to stitch together their own bespoke solutions. This trend will become particularly apparent in "intelligent" operations and workspace products, where the development cost of the intelligence is higher than its value to a single enterprise, but trivial when looked at across the entire user ecosystem.

As highlighted throughout this document, the underlying pace of change is not likely to decelerate in the foreseeable future. IT operations have already accelerated to meet this change. Agile, AIOps, DevOps, and SecOps are the first wave of these adaptations, but they will ultimately fall short of the need. Software vendors, public cloud providers, and enterprises will need to reimagine how the technical underpinnings of ecosystems of value are created, curated, adapted, and operated over time.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com