AWS vs Azure: A VMWare based Hybrid Cloud Comparison

Rutwik Ghag
Departement of Information Systems
Syracuse University
Syracuse, NY, USA
rutwik.ghag21@gmail.com

Puneet Shetty
Department of Information Systems
Syracuse University
Syracuse, NY, USA
puneetjpshetty@gmail.com

***Abstract*— This paper details the specifics that entail the setups of using VMWare Aria in conjunction with AWS IoT Core and Azure IoT Hub.**

Keywords—AWS, IoT Core, Azure, IoT Hub, VMWare, Aria, Multicloud, Edge IoT, hybrid cloud.

I. INTRODUCTION (*HEADING 1*)

The term "edge computing" refers to the practice of locating data storage and processing closer to the devices that generate data and the people who use that data[1]. Typically, data collected by sensors and cellphones is sent to a server farm for analysis via an application. However, the network's capacity has been overwhelmed by the data's unprecedented complexity and scale. Edge computing solutions greatly enhance application performance, reduce bandwidth requirements, and provide faster real-time insights by moving processing capabilities closer to consumers and devices.

Multi-cloud to edge computing refers to the use of multiple cloud platforms and edge computing resources to support a wide range of applications and services. Cloud computing refers to the delivery of computing services, including storage, processing power, and applications, over the internet. Multi-cloud computing involves using multiple cloud service providers to meet different requirements, such as performance, scalability, and cost-effectiveness.

On the other hand, edge computing involves processing data closer to where it is generated, rather than sending it to a central cloud data center for processing. This can help reduce latency, improve data security, and save on bandwidth costs.

Multi-cloud to edge computing combines these two approaches to create a hybrid infrastructure that can support a variety of workloads and use cases. This can include using edge devices such as sensors and IoT devices to collect and process data, then leveraging multiple cloud platforms to store, analyze, and act upon that data.

By using a combination of cloud and edge computing resources, organizations can optimize their infrastructure to meet specific business needs and ensure high performance and availability for their applications and services. However, this approach can also create challenges in terms of managing and integrating multiple systems, ensuring data security and compliance, and maintaining operational consistency across different environments.

Companies can save time and money on data collection and analysis by using edge computing. Today, more than ever, businesses require immediate access to their data in order to make educated decisions regarding the effectiveness of their operations and other business functions. Organizations can boost security and performance, automate operations, and enhance the user experience with the help of edge computing if it is used correctly.

A hybrid cloud is a type of cloud computing in which resources (such as servers, databases, and applications) are spread across many cloud types and locations (such as public clouds, private clouds, and on-premises data centers or "edge" locations)[4]. Nearly everyone uses multiple public clouds rather than just one, so hybrid cloud computing strategies are common.

Cloud computing solutions that may be used with several cloud service providers is called a multicloud solution[2]. All public cloud providers back open-source, cloud-native technologies like Kubernetes, the backbone of most multicloud solutions. Features for coordinating operations in several cloud environments from a single control panel ('single pane of glass') are also common. Multicloud solutions for computing infrastructure, development, data warehousing, cloud storage, AI/ML, disaster recovery/business continuity, and more are offered by several of the top cloud providers and cloud solution providers like VMware.

AWS IoT Core and Azure IoT Hub are cloud-based services offered by AWS and Azure respectively that provide a centralized relay for messages between IoT gadgets and software. Connecting, managing, and keeping tabs on millions of devices is now possible in a safe and dependable manner. Data, commands, and policies can all be transmitted to and from the devices over the cloud. Azure IoT Hub is accessible and manageable via numerous interfaces and tools.

VMware Aria is a multi-cloud management portfolio that includes tools for controlling expenses, optimizing resources, and streamlining the rollout of software and hardware [3].

By installing a hypervisor on the physical server, VMware server virtualization makes it possible to host numerous virtual machines (VMs) on a single host computer [8]. Virtual machines (VMs) allow for the installation of several operating systems (OS) on a single host machine. Virtual machines (VMs) hosted on a single physical server share system resources like memory and network bandwidth. VMware, a popular hypervisor, now has built-in support for deploying containerized workloads to a Kubernetes cluster. DevOps teams can deploy containers as usual, and the infrastructure team can manage these workloads in the same manner they handle virtual machines.

Customers using VMware Cloud on AWS can deploy and operate a vSphere host cluster on Amazon Web Services (AWS), complete with vSAN and NSX, and run their workloads in the cloud using their existing VMware knowledge and expertise.

Built into the ESXi hypervisor and fully integrated with vSphere, VMware vSAN is a software-based storage feature

that pools disk space from multiple ESXi hosts and provisions it, using smart policies like protection limits, thin provisioning, and erasure coding. Integrating with vSphere High Availability, it provides more reliable access to both computing resources and data storage.

VMware vSphere is VMware's suite of virtualization products. VMware vSphere, known as VMware Infrastructure prior to 2009, includes the following: ESXi, vCenter Server, vSphere Client, and vMotion.

If a disaster were to occur, an administrator might set up recovery procedures in VMware Site Recovery Manager (SRM) that would be carried out automatically. With Site Recovery Manager, IT staff can easily automate the failover and failback of virtual machines. Virtual machine (VM) network and security rules are maintained after a migration thanks to SRM's integration with NSX.

The vRealize Suite is a suite of programs that lets you set up and control your own personal hybrid cloud. The vRealize Suite's four main components are vRealize Operations for monitoring, vRealize Log Insight for centralized logging, vRealize Automation for data center automation, and vRealize Business for Cloud for expense management.

With this package, a system administrator can deploy and manage virtual machines (VMs) across multiple hypervisors or cloud platforms without leaving the centralized management console. VMware Tanzu, which was released in 2019, helps businesses create containerized apps, run enterprise Kubernetes, and manage Kubernetes from a developer and IT perspective.

All these components play a vital role in letting a client distinguish between vendors when making a choice.

II. Comparing IoT Cloud Platforms

There are three top vendors in the IoT Cloud Platforms, Amazon AWS, Microsoft Azure, and Google Cloud Platform [5]. There are certain commonalities among the various cloud providers' IoT offerings, but there are also key distinctions. The ways in which cloud providers like AWS, Google Cloud, and Microsoft Azure bundle and collaborate with IoT technologies vary widely. Additionally, a business may find that a smaller, less established rival outside the big three is a better fit for its requirements.

The AWS platform provides solid foundations for scalable, dependable, and secure IoT applications. The AWS IoT platform takes care of the boring stuff so developers can concentrate on making their app or feature stand out. Amazon's AWS IoT Core service, which is dedicated to connectivity and ingestion, allows devices to connect securely to the cloud infrastructure and route communications. Even as recently as 2018, some industry professionals thought that Google Cloud Platform (GCP) was behind AWS and Azure in IoT functionality. In that same year, Forrester Research released research on industrial IoT and cloud that analyzed the offerings of a dozen or more service providers, including AWS and Azure but excluding Google. AWS IoT Core supports MQTT, HTTP, and WebSockets protocols, while Azure IoT Hub supports these protocols plus AMQP and MQTT-SN. The protocol support is important because it can impact the way the IoT devices and cloud services interact and transfer data. Although both services provide safe communication between devices and the cloud, the underlying security mechanisms that they employ are distinct. In order to provide end-to-end security, AWS IoT Core makes use of the AWS IoT Device SDK. On the other hand, Azure IoT Hub makes use of both the Azure IoT SDK and a Certificate Authority (CA) in order to authenticate devices and secure communication.

Both of these services provide integration with a variety of different cloud services, including storage, analytics, and machine learning. On the other hand, AWS IoT Core [12] is well-known for its integration with AWS Lambda and other AWS services, whereas Azure IoT Hub interfaces with other Azure services such as Azure Stream Analytics [13] and Azure Functions.

Both services have different pricing models based on the amount of data transferred, the number of devices, and other factors. Azure IoT Hub charges customers per device per month based on the number of messages transferred. AWS IoT Core has a pricing model based on five factors, which are as follows; number of connections purchased, the messaging protocol used to transfer messages to the cloud, the registry pricing, the rules used for messages (pay per operation, e.g. AWS Lambda or arithmetic functions), and location solving required. However, AWS IoT Core tends to be slightly cheaper for small and medium-sized deployments, while Azure IoT Hub may be more cost-effective for large-scale deployments.

Both services have analytics capabilities that can assist users in analyzing the data produced by Internet of Things (IoT) devices. AWS IoT Core interfaces with Amazon Kinesis Data Analytics and Amazon QuickSight, both of which enable real-time data analysis and give features for data visualization and report generation, respectively. Azure IoT Hub connects with Azure Stream Analytics and Azure Time Series Insights, both of which give historical data analysis. Real-time data analysis is enabled via Azure Stream Analytics, and Azure IoT Hub provides access to it. Both services offer device management features, such as remote setting of the device and firmware updates, as part of their offerings. A virtual representation of a physical device can be created using the Device Shadow feature of AWS IoT Core. This enables software programs to communicate with the device even when it is not connected to the internet. Device twin is one of the features offered by Azure IoT Hub. Device twin not only delivers a virtual version of a device but also enables device management and setup.

Both services offer a collection of development tools and application programming interfaces (APIs) to assist developers in the process of building and deploying Internet of Things applications. AWS IoT Core is comprised of the AWS IoT Device SDK and AWS Greengrass. Both of these components enable local processing and data caching. A range of programming languages and operating systems are supported by both of these components. Azure IoT Hub offers the Azure IoT Software Development Kit (SDK), which is compatible with a variety of operating systems and programming languages. Additionally, it offers Azure IoT Edge, which enables edge processing and local analytics. Both of these services are part of a huge ecosystem of partners and third-party integrations that can supply additional tools, services, and support for Internet of Things (IoT)-related

solutions. Both AWS IoT Core and Azure IoT Hub have formed relationships with a variety of hardware vendors and system integrators respectively. Additionally, Azure IoT Hub has formed partnerships with a variety of software vendors and providers of IoT platforms. Both of these services include the option of customization, which gives developers the ability to modify their solutions to satisfy a variety of special requirements. AWS IoT Core is responsible for providing AWS IoT Greengrass, which enables developers to execute Lambda functions on IoT devices at the edge of the network. This paves the way for local processing and data caching. Azure IoT Hub provides Azure IoT Edge, which makes it possible for developers to execute individualized code and services on IoT devices located at the edge of the network.

Both of these services include monitoring and alerting features to assist in ensuring that IoT solutions continue to function properly and remain in good health. AWS IoT Core is included with AWS IoT Device Defender, which enables continuous monitoring and auditing of IoT device fleets to verify compliance with established security standards. IoT solutions can benefit from Azure Monitor's real-time monitoring and alerting capabilities, which are made available through Azure IoT Hub. Developers and consumers of both services have access to varying levels of support, documentation, and training materials provided by both services. A variety of support options are available through AWS IoT Core. These support tiers include basic, developer, business, and enterprise support. Documentation, tutorials, and community forums are some of the other features offered by Azure IoT Hub in addition to standard and professional support plans. Both of these services are in accordance with a variety of industry standards and regulations, including GDPR, HIPAA, and ISO 27001. AWS IoT Core offers compliance reports and certifications appropriate for a variety of geographical areas and business sectors. Compliance certifications are available through Azure IoT Hub for a variety of locations and sectors. These certifications include the Azure HIPAA Compliance Blueprint as well as the Azure IoT Device Security Baseline.

Both services are interoperable with a comprehensive selection of Internet of Things devices and protocols. This enables software developers to connect and manage devices produced by a wide variety of businesses and sectors. A large number of IoT device platforms are supported by AWS IoT Core. These include AWS IoT Device SDKs, MQTT, HTTP, and CoAP. Additionally, a large number of third-party devices and protocols can be supported using AWS IoT Greengrass connectors. Azure IoT Hub is compatible with a wide variety of IoT device platforms, including MQTT, AMQP, HTTP, and Azure IoT SDKs. Additionally, Azure IoT Hub supports a wide variety of third-party devices and protocols via IoT Edge modules and IoT Plug and Play. Both services are available in many regions worldwide, enabling customers to deploy IoT solutions closer to their users and data centers. AWS IoT Core is available in many regions, including North America, Europe, Asia, and South America, as well as in GovCloud regions for US government customers. Azure IoT Hub is available in many regions, including North America, Europe, Asia, and Australia, as well as in Azure Government regions for US government customers.

Both services are consistently adapting to meet the ever-shifting requirements of IoT clients and markets, which results in the introduction of new features and capabilities across the board. A number of new features have recently been added to AWS IoT Core. These new features include AWS IoT Greengrass v2, which offers enhanced edge computing and machine learning capabilities, and AWS IoT SiteWise, which offers capabilities for the collection and analysis of industrial data. Azure IoT Hub has recently launched new features, such as Azure IoT Central, which offers a platform for cloud based IoT applications, and Azure Digital Twins, which offers a digital representation of physical assets and settings. Both of these features were developed by Microsoft.

AWS IoT core features high connectivity, numerous SDKs for development, ease of scalability, advanced AI and ML capabilities, multiple device qualification partners, but has a learning curve to setup and use. Azure IoT Hub boasts of an OS for IoT management, tools for edge and IoT support, digital twins, OTA updates, and a reliable security system while restricting the number of services for free users.

There is a lot of cross-over between AWS, Google Cloud, and Microsoft Azure. Some popular IoT cloud platforms are Azure IoT Hub, Amazon Web Services IoT Core, and Google Cloud IoT Core. In many cases, the components are the same even if the presentation is different. Azure's IoT Central is one such environment, boasting built-in support for message queuing, device management, and event-based triggers. While similar capabilities exist in GCP and AWS, developers using those platforms would have to implement them manually.

Each cloud IoT setting also has its own set of analytics capabilities, including streaming and in-place options as well as visualization technology. Azure has Power BI and Streaming Analytics while Google has Cloud Machine Learning and Data Studio. Although there are differences in platform functionality, most businesses will find it simpler to stick with the cloud they are already familiar with. For instance, Azure's IoT Central simplifies things, but it can only handle so many different types of issues.

Azure has made it a priority to bundle their IoT solutions with a wide range of partners. However, proficiency with the AWS platform is required to use AWS IoT, making it a distant second. A rising player in the IoT space, Google is utilizing BigQuery and TensorFlow, two of the company's machine learning tools, to fuel and differentiate the company's IoT offerings.

III. AWS VS AZURE: VMWARE BASED COMPARISON

Though hybrid cloud has been discussed by experts in the field for quite some time, it is only in the last few years that businesses have been able to successfully combine on-premises and public cloud infrastructures. Much of this change has been driven by VMware. Its user community is eager to move their vSphere environments to many public clouds, and it has become the de facto standard for virtualizing business software stacks. VMware abandoned plans to operate its own private cloud service and instead began work on hybrid connectors with leading public cloud providers [6].

Together with Amazon Web Services (AWS), VMware created a service that could be deployed on AWS's platform. Since its release in 2017, VMware Cloud on AWS has expanded to include additional regions and capabilities including vSAN support and enhanced workload migration instruments.

As of April 2019, VMware and Microsoft have an agreement in place to support businesses running workloads on Microsoft Azure. Azure VMware Solutions was a service package that comprised a CloudSimple-managed VMware environment. CloudSimple is a leading provider of secure, high performance, dedicated environments to run VMware workloads in the cloud. CloudSimple makes it easier for large companies to run applications in public clouds.

Within minutes, VMware workloads may be adapted by CloudSimple and made available on public cloud platforms. By utilizing Azure's CloudSimple service, you may set up VMware in its native environment. You can rest assured that your deployment will be hosted on Azure and will work seamlessly with the rest of the Azure cloud [7].

Since both solutions (by AWS and Azure) are built on the same underlying software and are intended to work in tandem with VMware infrastructures, it should come as no surprise that they share many similarities. Because they both use public cloud infrastructure to implement private clouds in accordance with the VMware Cloud Foundation's software-defined data center (SDDC) definition, they provide the same core VMware services. In the event that there is a catastrophic incident, VMware Site Recovery can be utilized to protect the workloads that are housed within AWS SDDC and on-premises vSphere Clusters. It enables failover and failback functionality, in addition to providing Disaster Recovery as a Service, which can be activated with a single click.

Microsoft Azure's Azure Site Recovery (ASR) is a disaster recovery as a service (DRaaS) offering that supports a variety of different kinds of environments. ASR offers disaster recovery capabilities for on-premises VMware, Hyper-V, and bare metal physical infrastructure in addition to workloads hosted in public clouds such as AWS, in contrast to proprietary disaster recovery solutions, which are tailored to a particular technology [9]. ASR enables the protection of virtual machines (VMs) operating within VMware vSphere settings beginning with version 5.5. Integration with vCenter Server is also supported, and once again, version 5.5 must be the bare minimum need. Using replication settings that can be written and maintained via the Azure interface, virtual machines (VMs) can be continually backed up to Azure.

When it comes to a direct comparison, both, AWS and Azure provide on-demand services and capacity provisioning. Both run vSphere to manage VMs, vSAN to run storage, and NSX-T to run Virtual Networking. Private WAN circuit support is given by AWS Direct Connect and Azure ExpressRoute respectively. AWS has vCenter Server and vRealize installed on the machines by default, whereas Azure has vCenter, but no vRealize. However, Azure supports the installation of vRealize on demand, privately. AWS has a Site Recovery Manager (SRM) pre-installed whereas Azure does not, but, once again, it supports the private installation of an SRM on demand. Both support Hybrid Cloud Extensions and integration with native cloud services, like AWS IoT Core and Azure IoT Hub (the two relays in question).

Amazon Web Services (AWS) provides two different services for integrating VMware: VMware Cloud on AWS and Amazon EC2 Bare Metal. VMware Cloud on AWS is a solution that was collaboratively developed by the two companies to deliver a cloud service that is based on vSphere and runs on AWS infrastructure. Customers using Amazon EC2 Bare Metal are able to execute VMware workloads directly on dedicated bare-metal instances hosted by Amazon Web Services. Azure provides its customers with a fully managed VMware solution known as the Azure VMware Solution (AVS). This service enables users to run VMware workloads in their native environment on Azure infrastructure. Amazon Web Services (AWS) provides support for VMware vSphere, a well-known virtualization platform that can be used to create and manage virtual machines. vSphere versions 6.5, 6.7, and 7.0 may all be run on VMware Cloud on AWS. vSphere versions 6.7 and 7.0 can be used with Amazon EC2 Bare Metal. AVS is built on VMware Cloud Foundation, which is an integrated software stack that comprises vSphere, vSAN, and NSX. Azure also supports VMware vSphere, but AVS is built on VMware Cloud Foundation. AVS is compatible with vSphere versions 6.5, 6.7, and 7.0.

Both Amazon Web Services and Microsoft Azure provide users with management tools that make it easier to deploy and maintain VMware workloads in the cloud. A single point of control for administering VMware workloads in the AWS Cloud can be attained through the use of the VMware Cloud on AWS Console, which is made available by AWS. AWS now supports VMware vCenter Server, which enables clients to manage the VMware workloads they have on AWS with the same VMware tools they are already accustomed with. A single management experience may be obtained for AVS and the other Azure services by utilizing the Azure portal, which is offered by Azure. Customers are able to administer their AVS setup by utilizing VMware tools because to the fact that Azure also supports VMware vCenter Server [10].

Customers of Amazon Web Services and Microsoft Azure can link their VMware workloads to other cloud resources and on-premises infrastructure thanks to the networking services offered by both companies. Amazon Virtual Private Cloud (Amazon VPC) is a service provided by AWS that enables clients to compartmentalize and safeguard the VMware workloads they run. AWS additionally provides services such as AWS Direct link and VPN in order to link the VPC to networks located on customer premises. Azure has a service known as Azure Virtual Network, which operates in a manner analogous to that of AVS's virtual private cloud. In addition, Azure provides the capability to connect the virtual network to on-premises networks using Azure ExpressRoute and VPN [11].

Both Amazon Web Services and Microsoft Azure provide customers with hybrid cloud capabilities that enable them to extend their VMware workloads from on-premises to the cloud in a seamless manner. Customers have the ability to run AWS infrastructure locally using the same application programming interfaces (APIs) and tools that are available in the AWS Cloud if they use a service called AWS Outposts, which is offered by AWS. AWS Outposts also supports VMware Cloud on AWS, which enables users to execute VMware workloads on-premises or in the cloud utilizing the same VMware tools and APIs. This is made possible by the fact that AWS Outposts supports VMware Cloud on AWS. Customers may manage their resources across on-premises, multi-cloud, and edge settings with the help of Azure Arc, which is a hybrid cloud management service offered by Azure. Azure Arc is also known as Azure Stack. AVS, which enables users to operate VMware workloads on-premises and in the cloud using the same VMware tools and APIs, is supported by Azure Arc as well. users may find more information here.

AWS vs. Azure: a comparison of VMware hybrid cloud features

FEATURE	VMWARE CLOUD ON AWS	AZURE CLOUDSIMPLE
On-demand service, capacity provisioning	Yes	Yes
VMs	vSphere	vSphere
Virtual storage	vSAN	vSAN
Virtual networking	NSX-T	NSX-T
Private WAN circuit support	AWS Direct Connect	Azure ExpressRoute
Management	vCenter Server, vRealize	vCenter, supports private vRealize installation, but not included
Replication and disaster recovery	Site Recovery Manager (SRM)	Supports private SRM installation with CloudSimple as a DR target, but not included
HCX support (hybrid cloud extensions)	Yes	Yes
Global cloud regions	16	2
Integration with native cloud services	Yes	Yes
Virtualization model	Bare metal	Bare metal
Host configuration (standard)	EC2 i3.metal instance: ■ Dual 2.3 GHz Intel Xeon Processor E5-2686 v4 CPU package with 36 cores total ■ 512 GiB RAM ■ 15.2 TB NVMe raw storage	CS28 node: ■ Dual 2.2 GHz processor with 28 cores total ■ 256 GB RAM ■ 1.6 GB NVMe cache storage ■ 5.7 GB data storage CS36 node: ■ Dual 2.3 GHz processor with 36 cores total ■ 512 GB RAM ■ 3.2 GB NVMe cache storage ■ 11.5 GB NVMe data storage
Storage node	EC2 R5.metal instance (beta): ■ Dual 3.1 GHz Xeon Platinum 8000 series (Skylake) processors with 48 cores total ■ 768 GiB RAM ■ 15 TB to 35 TB on Elastic Block Store	N/A
Software-defined data center per region (SDDC)*	5	Not specified
Maximum ESXi cluster size	16	16
Maximum hosts, VMs per SDDC	300	64
Maximum VMs per SDDC	4000	Not specified

There is a huge gap between the two services in terms of delivery and maintenance. While AWS is used for the underlying infrastructure of VMware Cloud on AWS, the service itself is provided, supported, and billed for by VMware. In contrast, Microsoft's Azure VMware Cloud Solution is based on CloudSimple technology but is invoiced and supported as an Azure service. In conclusion, when working with AWS, VMware retains ownership of the client relationship, while Microsoft does so when working with Azure [6].

VMware Cloud on AWS pricing

NODE/HOST SIZE	ON-DEMAND	1-YEAR SUBSCRIPTION*	3-YEAR SUBSCRIPTION**
i3.metal	$8.368/hour	$5.935/hour	$4.162/hour
R5.metal	$10.138/hour	$6.637/hour	$4.706/hour

Azure VMware Solution by CloudSimple pricing

NODE/HOST SIZE	ON-DEMAND	1-YEAR SUBSCRIPTION*	3-YEAR SUBSCRIPTION**
CS28	$6.444/hour	$4.511/hour	$3.222/hour
CS36	$9.205/hour	$6.444/hour	$4.603/hour

The AWS i3.metal and Azure CS36 instances both provide 36 total cores with 512 GB RAM and a similar amount of storage. However, the Azure service is 10% more expensive across the board.

Therefore, the typical applications for VMware Cloud on AWS and Azure VMware Solution by CloudSimple are identical, for example: workload migration to the cloud infrastructure, data center extension using the cloud infrastructure, or on-demand capacity expansion or workload localization to different global regions, virtual desktop infrastructure that either supplements or replaces on-premises systems yet is available via high-performance private network links using AWS Direct Connect or Azure ExpressRoute, disaster recovery using the cloud as a backup site for on-premises workloads, and next-generation, cloud-native applications that can tap into native AWS or Azure services while also accessing legacy databases.

IV. Results and Conclusion

Both offerings are tailored to businesses that have chosen to standardize on VMware's line of virtualization products and management software for their servers, storage, and networks.

While using VMware cloud on AWS, customers can choose between an on-demand (hourly) pricing or reserved up-front pricing for one to three years per host. It is possible to combine reserved pricing with a hybrid loyalty program in order to further lower total cost of ownership (TCO). Reserved pricing is helpful for long-term savings. Customers that already use VMware can receive a discount of up to 25 percent off each host, based on the number of qualified on-premises product licenses they purchase. Licenses for VMware vSphere, VSAN, or NSX can each receive a discount of 10 percentage points per product, with the overall benefit being capped at a discount of 25 percentage points per host. VMware is in charge of handling billing for both VMware components and AWS, and it provides the customer with a consolidated bill for both services. Customers should explore license mobility options in order to make the most of their existing licenses and lower total cost of ownership (TCO) when it comes to licensing for workloads that are hosted in a VMware cloud for AWS. For instance, the Microsoft License Mobility program can be utilized for software licenses as well as licensing for the Windows operating system [9].

In addition to the price of the Azure storage used for the replicated data, the flat pricing that Azure Site Recovery charges for its service is calculated on a per-instance, per-month basis. The Block Blob storage that ASR uses for the purpose of storing the data is relatively inexpensive, and the customer is billed on the basis of the amount of used storage on a per-GB per month basis. Only in the event of a failover will the charges for the virtual machines become active, and they will be billed on an hourly basis based on the type of VM instance that was used. By combining Azure Hybrid Benefit with ASR, it is possible to cut costs further for Windows VMs that are failed over to Azure. This will result in a lower monthly bill. By enabling customers to use Windows licenses that they already possess on-premises, it is possible to achieve cost savings of up to forty percent.

Because many of the same technologies are deployed in AWS, providing a nearly seamless extension of existing infrastructure, VMware cloud on AWS may be more useful for organizations that require a tighter integration with their existing VMware infrastructure. However, it is important to keep in mind that organizations will still be required to pay for

VMware licenses on AWS. On the other hand, if the primary use cases that are being targeted are workload migration and disaster recovery, then the solution that will be most cost-effective will be Microsoft Azure.

Given the similarities between the two services, picking between Amazon Web Services and Microsoft Azure for VMware depends on the following factors:

- Previous vendor relationships and whether AWS or Azure are currently being used for production workloads. For businesses using Windows Server, the CloudSimple service's support for Azure Hybrid Benefit means lower license costs.
- Whether a business would rather handle billing and support inquiries directly with VMware (as is the case with VMware Cloud on AWS) or the cloud provider (as is the case with CloudSimple).
- Application workloads that require access to external data sources should be deployed on AWS, where the high-capacity vSAN storage nodes are accessible, rather than on Azure, which are not on the bleeding-edge of tech in the vSAN space.
- How feature rich you want your service to be. AWS has all VMWare features pre-installed whereas Azure has the essential ones pre-installed and supports the installation of the remaining features on demand, privately. If a business has an exact idea of how it is going to use the resources provided, this is a crucial factor as Azure gives you more storage space accounting for the fact that it is less bloated.

REFERENCES

[1] Amazon Web Services. (n.d.). What is Edge Computing? Retrieved May 2, 2023, from https://aws.amazon.com/what-is/edge-computing/#:~:text=%20Edge%20computing%20is%20running%20workloads%20at%20the,cloud%20service%20providers%20also%20provide%20edge%20computing%20services.

[2] IBM. (n.d.). Multicloud. Retrieved May 2, 2023, from https://www.ibm.com/topics/multicloud

[3] VMware. (2022, August). Introducing VMware Aria [Blog post]. Retrieved from https://blogs.vmware.com/management/2022/08/introducing-vmware-aria.html

[4] Google Cloud. (n.d.). What is hybrid cloud? Retrieved May 2, 2023, from https://cloud.google.com/learn/what-is-hybrid-cloud.

[5] TechTarget. (n.d.). AWS vs. Azure and Google: An IoT cloud platform comparison. Retrieved May 2, 2023, from https://www.techtarget.com/searchaws/feature/AWS-vs-Azure-and-Google-An-IoT-cloud-platform-comparison

[6] TechTarget. (n.d.). AWS vs. Azure: Compare VMware-based hybrid clouds. SearchCloudComputing. https://www.techtarget.com/searchcloudcomputing/tip/AWS-vs-Azure-Compare-VMware-based-hybrid-clouds.

[7] Microsoft. (n.d.). CloudSimple private cloud. Microsoft Learn. https://learn.microsoft.com/en-us/previous-versions/azure/vmware-cloudsimple/cloudsimple-private-cloud

[8] TechTarget. (n.d.). VMware. Retrieved from https://www.techtarget.com/searchvmware/definition/VMware

[9] Navisite. (2021, April 29). Azure or AWS: Which to Choose If Running vSphere On-Premises? [Blog post]. Retrieved from https://www.navisite.com/blog/azure-or-aws-which-to-choose-if-running-vsphere-on-premises/

[10] Microsoft. (n.d.). Azure VMware Solution. Retrieved May 4, 2023, from https://azure.microsoft.com/en-us/products/azure-vmware/

[11] Amazon Web Services. (n.d.). VMware on AWS - Run VMware workloads on AWS. Retrieved May 4, 2023, from https://aws.amazon.com/vmware/

[12] Amazon Web Services. (n.d.). AWS IoT Core - Secure and Reliable IoT Communication and Management. Retrieved May 4, 2023, from https://aws.amazon.com/iot-core/

[13] Microsoft. (n.d.). Azure IoT Hub. Retrieved from https://azure.microsoft.com/en-us/products/iot-hub