VMWARE CLOUD ON AWS AND AMAZON WEB SERVICES IS THE NEW ENTERPRISE ARCHITECTURE

Using the VMware Cloud and AWS clouds to transform your VMware enterprise to modernize your VMware workloads

Contributors:

Vince Montalbano AWS Principal SHI International

Contents

Executive Summary

SHI International Corp.'s, (SHI) Cloud and Innovative Solutions (CIS) group, and Amazon Web Services (AWS) have collaborated to jointly develop this solution based white paper, "VMware Cloud and Amazon Web Services is the New Enterprise Architecture". SHI is an AWS and VMware Premier partner that develops enterprise solutions that identifies and delivers VMC and AWS solutions that align to the business vision and goals of your IT organization. This white paper defines a unique business vision for VMC and illustrates how the integration of your existing VMware enterprise environment with VMC and the AWS platform will allow your IT organization to keep up with the pace of change required to deliver modern enterprise workloads.

This whitepaper is an overview of the SHI International Corp.'s approach to the adoption and integration of VMC into an IT organization's enterprise, and the benefits of the capabilities to modernize VMware workloads by utilizing AWS native services. There have been many blogs and whitepapers published that discuss the many values of VMC and how VMC has been used in the traditional sense. This whitepaper will explore an approach to what we feel delivers the greatest value from the integration of VMC into your IT enterprise:

VMC integration with your existing VMware enterprise environment provides SHI customers solutions to the following business visions and technology challenges:

1. The capability for the IT organization to adopt to a modern operating model that uses known technologies, tools, and existing infrastructure, allowing for a less disruptive transition to a modern IT operating model.
2. A platform that provides workload portability, that utilizes a common virtual machine format and operational consistency between the on-premises environment and the AWS platform.
3. The ability to consume specific technologies in each infrastructure component without disruption to other workloads or environments in the IT enterprise.
4. Allowing for different IT organizational teams to each work on their own areas of expertise on a hybrid platform that is integrated with their current IT organization and enterprise.
5. Providing your IT organization, the ability to manage your IT infrastructure as code, (IaC) and develop modern IT workloads that utilize modern AWS services to provide high-availability and workloads that natively scale.
6. The integration of the existing on-premises VMware environment with VMC and AWS delivers VMware based workloads that take full advantage of the benefits of public, private and hybrid cloud architectures and solutions.
7. The capability to utilize and deploy to a variety of database technologies instead of being locked into one particular technology of software solution.

This whitepaper also provides insights on the benefits of adopting VMC and AWS, to create what we are now calling the "the new enterprise architecture". The new enterprise architecture contains the following 3 in-line components; the customer's existing on-premises VMware environment running in their data center, VMC, and the customer's AWS organization.

Introduction

VMware Cloud on Amazon Web Services – VMC

VMware Cloud (VMC) on Amazon Web Services (AWS), is an integrated cloud offering jointly developed by AWS and VMware that delivers a highly scalable, secure, and innovative infrastructure service allowing organizations to seamlessly migrate and extend their on-premises VMware vSphere-based environments to the AWS Cloud. The VMC runs on the next-generation of Amazon Elastic Compute Cloud (Amazon EC2) bare metal infrastructure. VMware Cloud on AWS is ideal for enterprise IT infrastructure organizations looking to migrate their on-premises vSphere-based workloads to the public cloud, consolidate and extend their data center capacities, and to modernize their VMware workloads with AWS native services. VMware Cloud on AWS is delivered, sold, and supported globally by VMware.

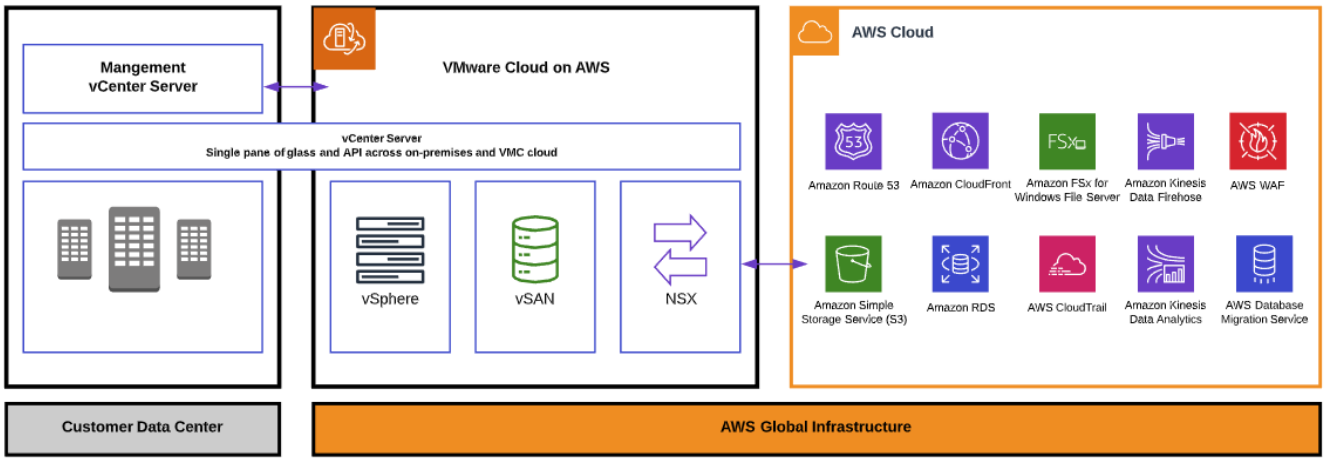
Transformation, Not Disruption

VMware vSphere ESXi is by far the most adopted hypervisor used to run virtual machines in the IT enterprise. When you provision a Software Defined Data Center (SDDC) from VMC, the ESXi hypervisors are automatically deployed onto bare metal Amazon Elastic Compute Cloud (Amazon EC2) with Amazon Elastic Network Interfaces (ENI) that connects to the customer managed Amazon Web Services account. This SDDC allows our SHI customers to establish a VMC SDDC on AWS global infrastructure and quickly begin deploying their enterprise workloads to the VMC cloud. VMC customers can migrate workloads between their on-premises data center and the VMC cloud using VMware vSphere® StoragevMotion®, and with Hybrid Linked Mode (HLM), administrators can manage both the on-premises environment vCenter, and the VMC from one centralized location, easily migrating workloads between the different vCenter sites.

This enterprise architecture provides following additional benefits to your IT organization:

1. No refactoring of your current IT enterprise, as we are adding a VMC site to our existing environment. The VMC account and target AWS accounts are connected via NSX and AWS Elastic Network Interfaces (ENI)s providing the ability to extend VMC providing high bandwidth and low latency to AWS services.
2. The current VMware enterprise administrators in your organization will use the existing VMware management tools that they know and understand, to support the workloads that will be deployed into the VMC. This approach will minimize the changes that our SHI customers have to go through to adopt the VMware on AWS and AWS native services.
3. SHI customers can start using their enterprise VMware with a cloud first approach by aligning specific VMware workloads to a specific IT organization business vision and specific use cases for adopting AWS native services to modernize their workloads.
4. The ability to use your current IT support staff to support wokloads that are hosted on the AWS cloud, allowing your staff to smoothly transition with minimal disruption to your day-to-day operations.
5. Accelerate datacenter modernization with VMware HCX hybrid interconnect to rebalance your cloud and on-premises application footprint by easily migrating VMs within and across data centers and clouds. VMware HCX also provides additional protection to workloads by replicating data across common VMC infrastructure in two or more places allowing our customer to fulfill high-availability and disaster recovery requirements for their VMware workloads.

The New Enterprise Architecture



The new enterprise architecture is a 3-component modern hybrid operating model that provides IT organizations the following benefits to their business visions and IT organizational goals:

1. A cloud transformation solution that allows the IT organization to provide Infrastructure-as-Code (IaC) enterprise workloads that can run on multiple platforms that provide a scalable, high-available, and compliant solutions that utilizes their existing VMware enterprise operational teams, VMware tools, and VMware management interfaces.
2. The ability to modularize and segment their enterprise environments for IT organizational teams to develop and run workloads on the platform that is the most appropriate for the use case. This approach presents the ability to consume on-premises VMware, VMC and AWS public cloud services to provide the most cost-effective solution for the use case or workload.
3. Transforming their IT enterprise by receiving the benefits of consuming cloud platform services by adopting emerging technologies for data storage, content delivery, and micro services. This will allow IT organizations to reduce their dependency on traditional infrastructure constructs and proprietary software to modernize their workloads.
4. VMware Cloud on AWS allows organizations to take immediate advantage of the scalability, availability, security, and global reach of the AWS infrastructure.
5. Additionally, customers can access native AWS services from the VMware Cloud on AWS SDDC without incurring any ingress or egress charges.

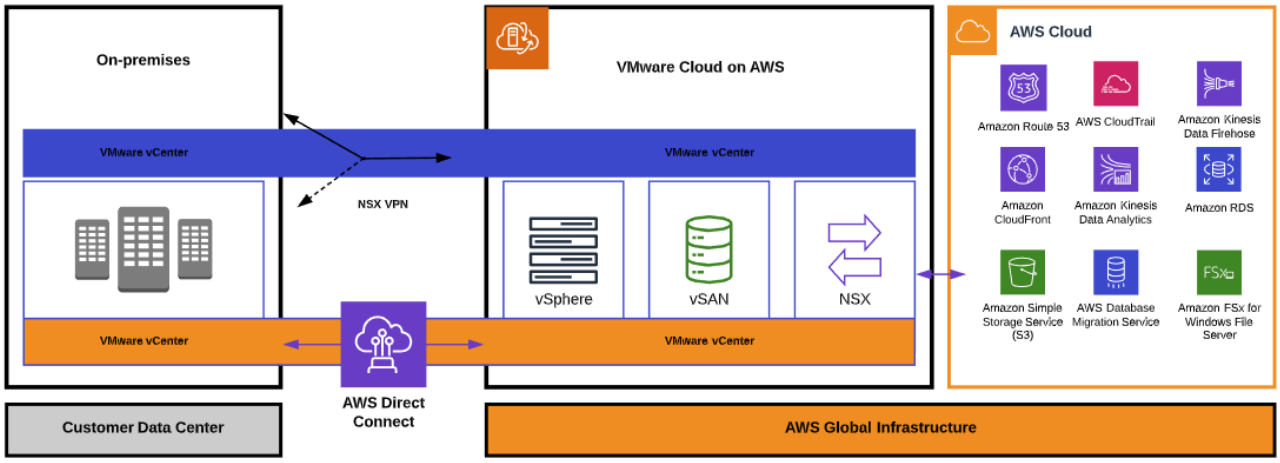
VMC and AWS is a solution that provides portability, operational consistency and supports a common virtual machine format and the required infrastructure constructs. The new enterprise architecture will provide your IT organization with the required solutions allowing your enterprise to transform to a modern operating model that utilizes your existing VMware enterprise environment and the Amazon Web Services (AWS) cloud.

VMC Software Defined Data Center (SDDC)

The AWS network is a full layer 3 network and is itself, an overlay of the compute, storage and networking that comprises the AWS global infrastructure. VMware and AWS jointly developed the VMC SDDC solution, where the native VMware vSphere Distributed Switch (VDS) VLANs are mapped to AWS

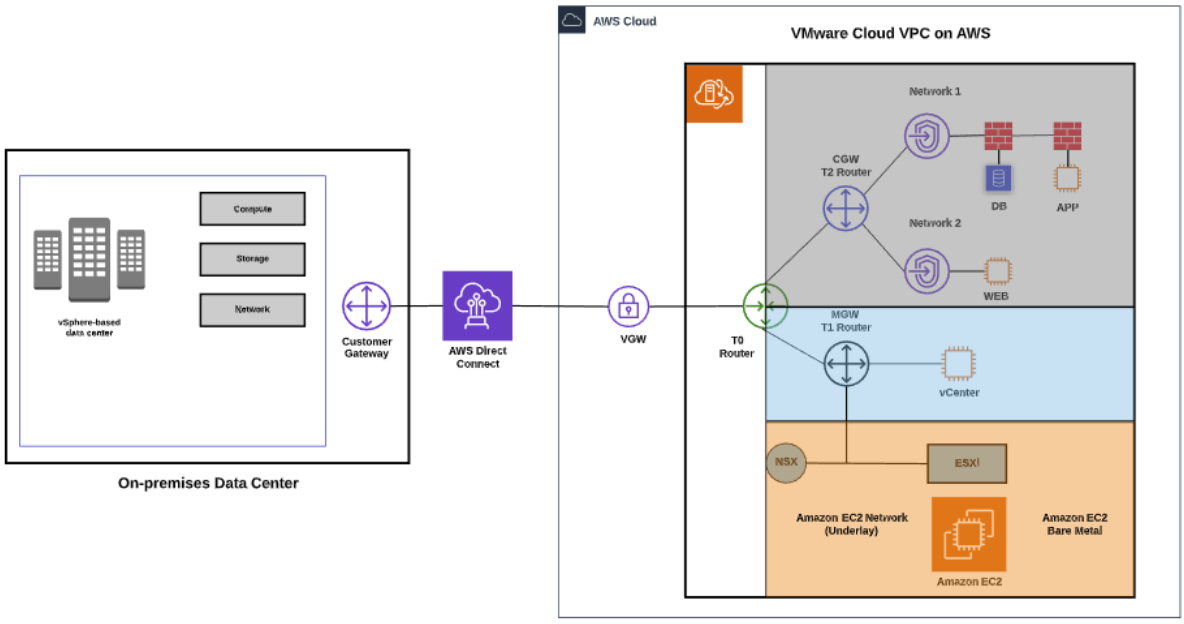
ENIs in your AWS account. This VLAN-to-ENI mapping is what allows the VDS and ESXi hosts to communicate and run in the SDDC VMC on the AWS infrastructure.

Once the VMC on AWS SDDC is deployed, SHI customers have multiple connectivity options between on premises and the VMC SDDC. These connectivity options include policy-based IPSEC VPN, route-based IPSEC VPN, L2VPN, and AWS Direct Connect. The AWS Direct Connect can carry all traffic from on-premises to a VMC, and vice-versa. This traffic and communication includes all ESXi management, vMotion, cold migration, vSphere management appliance, and workload traffic. The traffic over Direct Connect is not natively encrypted and it is a recommended best practice to encrypt traffic by using an IPSEC VPN over the AWS Direct Connect Connection.



VMware and VMC VPC Connectivity - NSXT

In the reference architecture example below, we illustrate a hybrid environment with an on-premises VMware vSphere environment that is connected to the VMC via an AWS Direct Connect. The routing from the on-premises environment to the VMC VPC is provided by VMware NSX-T. NSX-T provides the connectivity via an AWS Direct Connect for all traffic types providing access to the VMware management network appliance and ESXi access to and from the overlay networks and AWS VPC. The architecture also illustrates the Amazon cloud platform control plane and how it integrates into the customer VMC VPC. In middle layer of this architecture in the customer's vCenter instance in their VMC account. vCenter uses it's native NSX service to control all of the routing and VMware communications in the VMC environment, sending communications up to the third level VMware instances in the VMC VPC.



VMC Tx Routers

In the illustration the T0 router provides access to workloads on compute network segments that are connected to the VMC Compute Gateway (CGW) providing access to components on the management network that is connected to the Management Gateway (MGW). The T0 router is also where connectivity to the external environment (Internet Gateway (IGW), AWS Direct Connect, IPSEC VPN, and Amazon ENIs to the customer AWS account VPC takes place. This architecture illustrates that the compute, network segments, and management network are overlays and all traffic entering and exiting the SDDC must traverse the T0 router. The T1 MGW router is used to communicate with the customer's vCenter instance and the underlying VMC infrastructure, vCenter, NSX Manager, ESXi servers and the T0 router. The CGW T2 router is used to send traffic and native VMware communications to the VMware virtual machines that reside on subnets in the VMC VPC.

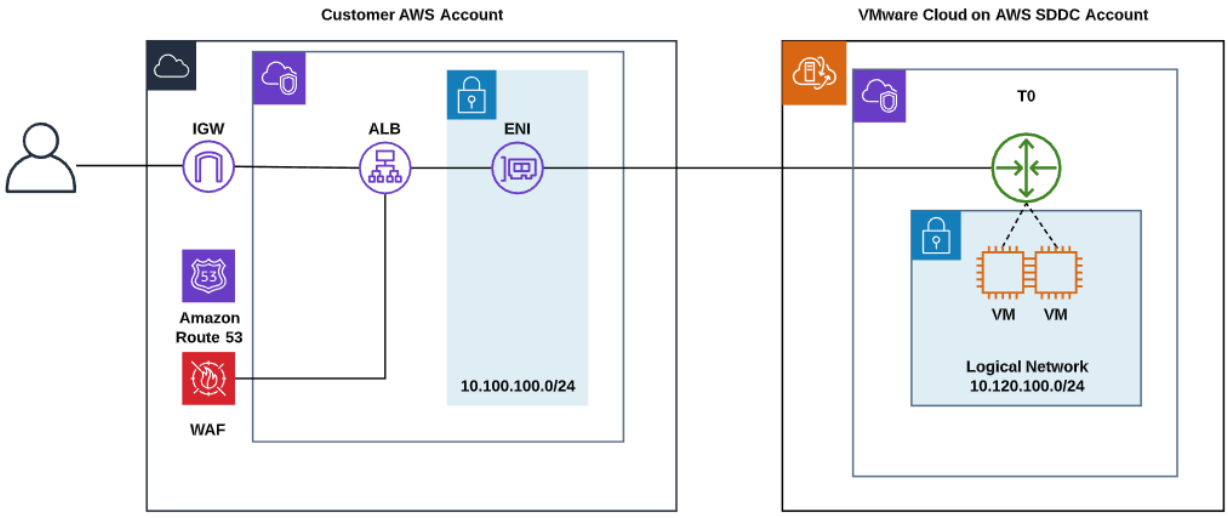
True High-Availability for VMware using AWS Global Infrastructure

VMC is the middle tier in the new enterprise architecture as it sits between your enterprise VMware services and the AWS cloud. One of the most compelling and exciting benefits of this architecture is the ability to easily extend VMC to your AWS account resources, to take advantage of the Amazon global platform and AWS services to provide modern capabilities to your VMware workloads. As an AWS Solution Architect, I always ensure that we account for high-availability in our envisioning and planning sessions to deliver solutions that are scalable, resilient and well-architected. In this section of this white paper we will discuss how using AWS native services will allow your IT organization to integrate AWS native services for true high-availability, and to transforming your VMware workloads to modern applications.

AWS Application Load Balancer

In the reference architecture below we are looking at 2 components of the new enterprise architecture. The diagram on the right depicts VMware web server virtual machines running in a VPC in the VMC

cloud. On the right we have our customer AWS account and AWS VPC, and an external user that needs to access a typical web-based application that is running in the VMC cloud.



The reference architecture illustrates a VMware virtual machine web server workload that is running in VMC. Our solution uses Amazon native services to provide a solution for DNS name resolution, web traffic filtering, DDoS protection and load balancing.

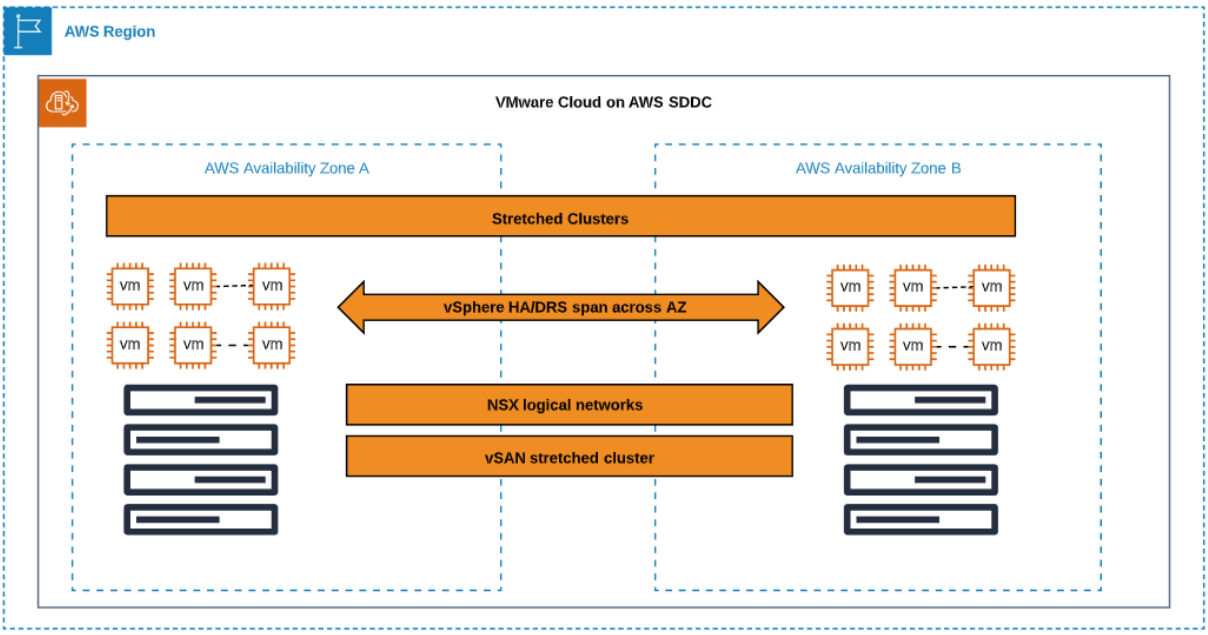
1. The web site consumer connects to the VMware web servers through an endpoint in the customer's AWS account VPC Internet Gate Way, (IGW)
2. The request is then routed to an application load balancer instance in the customer's AWS VPC
3. The load balancer sends the request to the VMC and the request is routed to the VMware web server virtual machines in the VMC VPC
4. This solution provides a highly-available solution for DNS name resolution, a layered security perimeter for protection against network based and application DDoS attacks by using AWS native services

VMC Stretched Clusters on Amazon Availability Zones

This is probably the most intriguing feature that is now available on the VMC cloud. Running workloads in multiple AWS Availity Zones (AZ) is one of the most advantageous benefits of using the AWS cloud. As you probably already know, AZs are a group of data centers in an Amazon region. These data centers are strategically placed in the region with each data center segmented from the other. The data centers that make up an AZ do not share power, they are also separated by flood plains and earthquake faults to ensure reliability. Architecting your workloads that span across data centers in a Amazon Region is something that is very native to AWS, and almost impossible to replicate in your enterprise environment. The VMC SDDC now provides solution architects to ability "stretch" VMware clusters across AWS AZs to take advantage of the native high availability of the AWS cloud. VMC Stretched clusters facilitate zero RPO infrastructure availability for mission-critical applications enabling your organization the ability to failover workloads with zero RPO within clusters spanning two AWS Availability Zones (AZs). The vSAN's stretched cluster feature also extends workload logical networks to support vMotion between AZs, and in the case of an AZ failure, vSphere HA will restart your VMs on the

surviving AZ. This solution provides a architecture pattern that is suitable for VMware production workloads and is not recommended as a Disaster Recovery strategy.

The reference architecture below illustrates how the SDDC deploys a VMware cluster that spans two availability zones. The VMC stretched cluster uses vSAN technology to provide a single datastore for the SDDC and replicates the data across both availability zones. If service in one availability zone is disrupted, workload VMs in the SDDC are brought up in the other availability zone.



VMC and AWS Services – VMware Workload Modernization

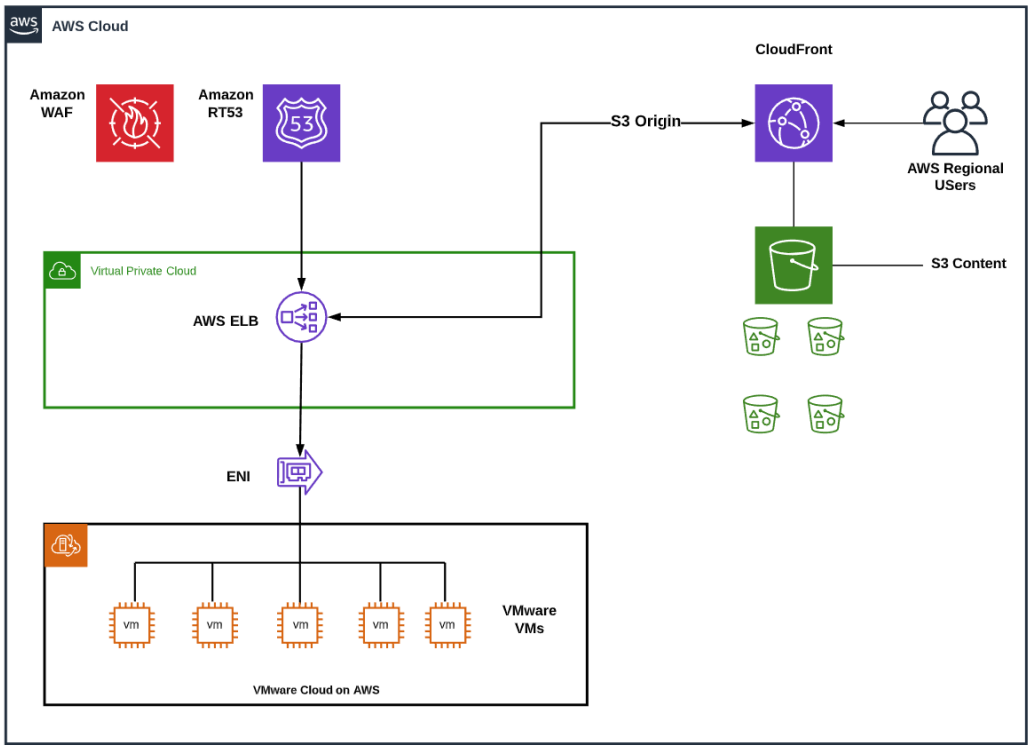
VMC and AWS Native Services

The most intriguing use cases for using VMC is to modernize your workloads by presenting AWS native services to your VMware VMC virtual machines. This integration provides your IT organization the capability to develop modern next-generation applications. In the section below we will illustrate 4 examples of how to integrate AWS native services to the VMC, and the benefits and value of using VMC and native AWS services to modernize your VMware virtual machine workloads.

Amazon CloudFront

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds using a global network of Points of Presence, located in AWS Regions across the globe. Amazon CloudFront is tightly integrated with AWS Shield, AWS WAF and Amazon Route53 (RT53) services to creating a flexible, layered security perimeter against multiple attacks that includes network based and application DDoS attacks. Amazon CloudFront delivers content, APIs and applications via SSL/TLS and provides the restriction of content by restricting access based on geo-locations, signed URLs, signed cookies, and origin of access controls. CloudFront's integration with AWS services provides IT enterprises the ability to distribute their content behind a highly secure, scalable, and resilient perimeter that provides advanced layer 7 protections to their web- based content using these Amazon fully managed services.

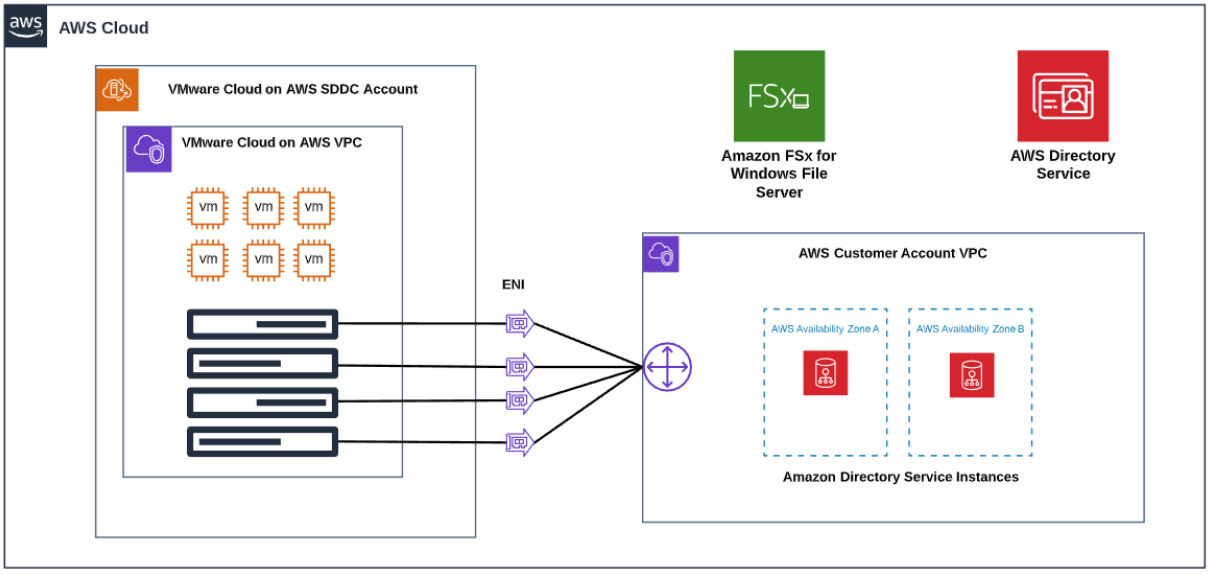
The reference architecture below illustrates VMware virtual machine web servers that are running in the VMC that are connected to a customer AWS account VPC via the VMC Elastic Network Interface (ENI). Amazon RT53 is providing the DNS resolution for the CloudFront distribution and the AWS WAF service is providing network and DDoS protections to the VMware virtual machines that are hosting that website. Amazon CloudFront uses an "origin" that describes the Amazon Simple Storage Service (S3) content that is to be distributed, the access controls to that content, and aligning that content to the closest CloudFront CDN to the user that is requesting the hosted content.



Amazon FSx for Windows File Server

Amazon FSx for Windows File Server is a fully managed native Microsoft Windows file system built on Windows Server that provides shared file storage with full support for the SMB protocol, NTFS, Active Directory (AD) integration, and Distributed File System (DFS). Amazon FSx allows your organization to connect your enterprise file system via an Amazon ENI to your VMware virtual machines running in the VMC, that provides a Microsoft NTFS file system that complies with PCI DSS, SOC 1, 2 and 3, and HIPPA standards. Amazon FSx natively encrypts data at rest and eliminates the typical administrative overhead of managing Windows file servers' virtual machines, (Microsoft Windows operating system updates and the associated operational cost to manage file server storage) in the traditional IT enterprise.

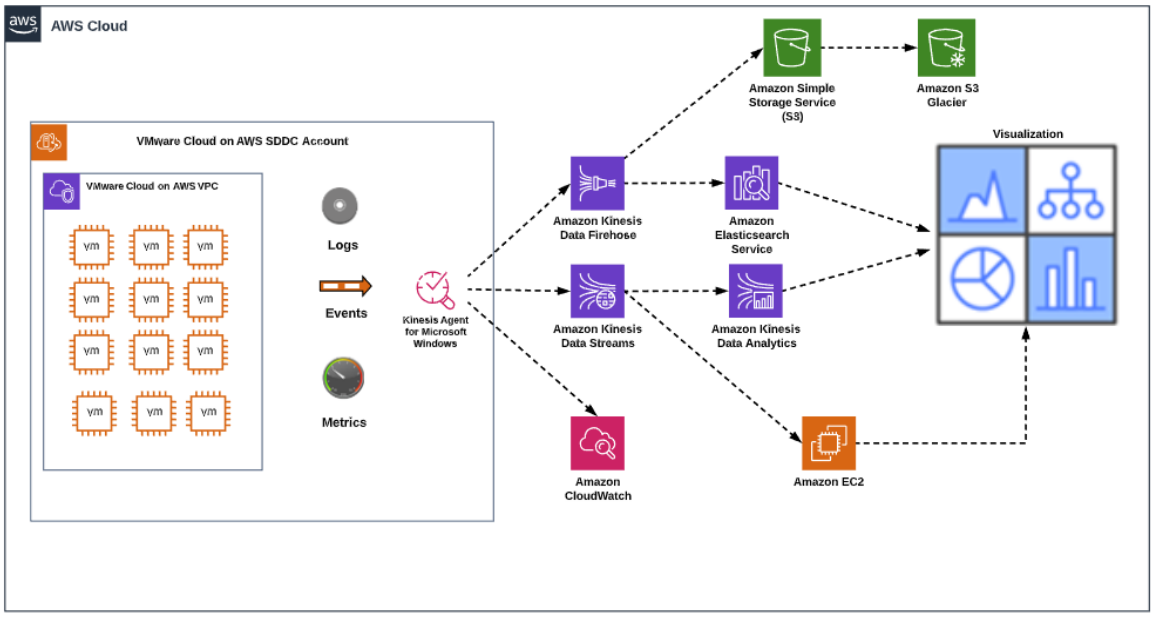
In the example architecture below we illustrate Microsoft Windows virtual machines running in the VMC that is connected to a customer managed AWS VPC. In the AWS VPC we have a customer managed Active Directory domain to provide Active Directory authentication, AD group policies, authorization and NTFS permissions to the Amazon FSx Windows file servers running on the AWS cloud.



Amazon Kinesis

Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service that can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events. The streaming data that is collected is presented in milliseconds providing your IT organization the capability to provide real-time analytics use cases such as real-time dashboards and real-time anomaly detection. KDS applications are built by capturing data using the AWS SDK, the Kinesis Client Library (KCL), and Kinesis agents that process data and provide options for built-in integrations to AWS Lambda, Amazon Kinesis Data Analytics, and Amazon Kinesis Data Firehose. In the example illustrated below, we use the Amazon Kinesis Agent for Windows that is installed on our Microsoft Windows virtual machines on the VMC. The Kinesis agent efficiently and reliably streams logs, events, and metrics, sending this data to the Kinesis Data Streams, Kinesis Data Firehose, Amazon CloudWatch, Amazon S3 services.

In our example KDS is configured to send real-time VMware virtual machine log data to the Kinesis stream-processing frameworks. This solution allows your enterprise to stream data for storage on Amazon S3, to Amazon CloudWatch to track metrics and analyze logs, to Amazon EC2, and to Amazon Kinesis Data Analytics and the Amazon ElasticSearch Service to provide real-time analytics for dashboards or visualizations. This reference architecture provides your VMware enterprise a framework to provide real-time reporting on VMware virtual machine workloads, the capability to send specific VMware virtual machine data in Amazon S3 for further processing, the ability to store data at rest with encryption, and to provide a lifecycle storage policy for data that needs to be retained in a data archive.



AWS Cloud Native Databases

Amazon Relational Database Services (RDS)

Amazon Relational Database Service (Amazon RDS) provides cost-efficient and resizable capacity for database instances that are optimized for memory, performance or I/O. Amazon RDS provides the capability for automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups, reducing the operational overhead that is necessary to provide database instances to your VMware based virtual machines running in the VMC. Amazon RDS runs in a subnet in the customer AWS VPC, providing several advanced native capabilities for database infrastructure patterns that include, automation via the AWS API, running database instances across AWS Availability Zones (AZ), real-only database instances, and database instance backups using the AWS native services.

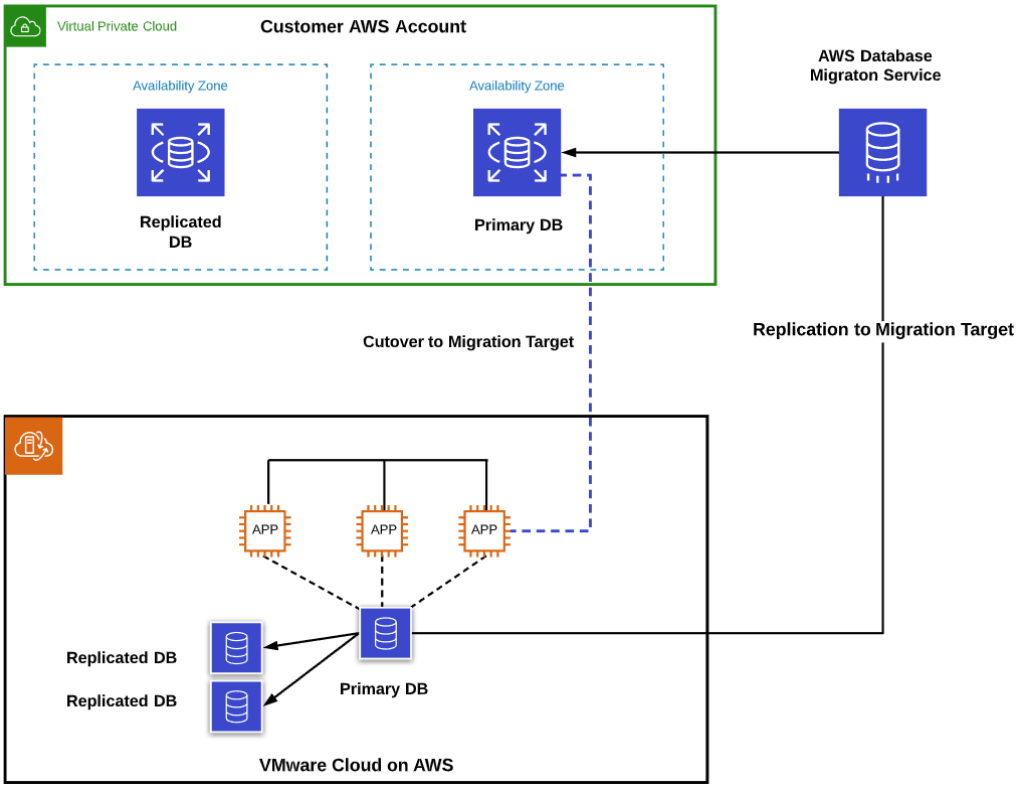
VMware Virtual Machines Database Server Migrations to Amazon RDS

In the example reference architecture below we illustrate a common pattern of a VMware database server providing database instances to VMware virtual machines. The VMware database server is configured in a “one-to-many” architecture to provide primary and secondary database instances to virtual machines.

AWS Database Migration Service (DMS)

Our Amazon RDS solution illustrates the use of the AWS Database Migration Service, (DMS). AWS DMS allows your IT Organization to migrate databases to AWS quickly and securely. AWS DMS migrations allows the source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from most widely used commercial and open-source databases. Using AWS DMS to migrate your databases provides your IT organization the ability to decouple the one-to-many database server patterns, (monolithic database servers), and migrate the workload database instance to a one-to-one database pattern on an Amazon RDS instance. The AWS DMS service uses the existing database as the database source and replicates the database source to a target instance running on AWS RDS. When the AWS DMS replication is complete the database administrators can cut-over and point the VMware

virtual machines on VMC to the RDS instance. This reference architecture pattern also provides additional database instance redundancy by using the AWS Multi-AZ instance type that provides read only copies of the database across AWS AZs. The AWS RDS Multi-AZ instances provide additional redundancy benefits as the replicated database instances are synchronously replicated to different data centers in the Amazon region on independent infrastructure. AWS Multi-AZ instances provide additional redundancy using the native RDS automated failover feature that will failover a primary database instance to the secondary database instance in the case of primary database instance failure.



Converting Microsoft SQL to AWS Native Databases

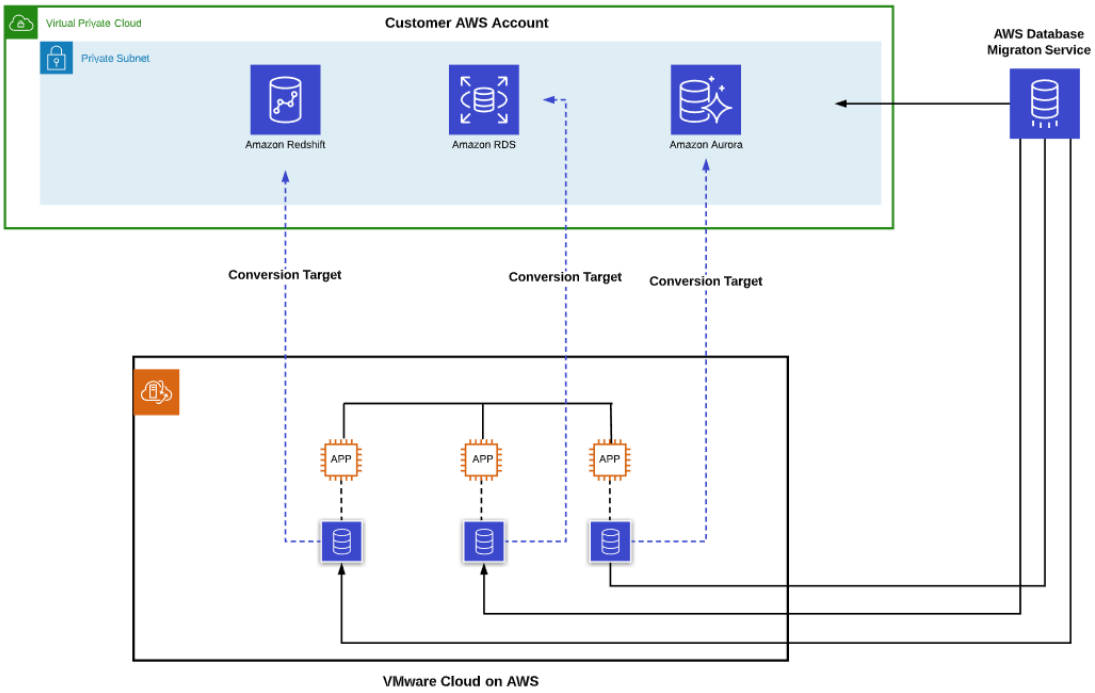
The AWS DMS service supports homogenous migrations such as Microsoft to Microsoft, as well as heterogeneous migrations between different database platforms, such as Microsoft SQL Server to MySQL. AWS DMS also allows you to stream data to Amazon Redshift enabling data warehouse consolidation and easy analysis of data in a petabyte-scale data warehouse. The next section of this whitepaper will discuss how we can use the AWS DMS service for heterogeneous migrations between Microsoft SQL Server to AWS native database services. AWS DMS migrations form Microsoft SQL Server to AWS native database services will help you reduce the cost of commercial database engines by moving them to open-source and Amazon-managed databases, therefore reducing your IT organization's dependency on proprietary software, and also providing your enterprise with several database choices for your applications.

MS SQL Database Conversion to Amazon Database Engines - AWS Schema Conversion Tool

The AWS Schema Conversion Tool, (SCT) makes heterogeneous database migrations predictable by automatically converting the source database schema and a majority of the database code objects, to a format compatible with the target database. Any objects that cannot be automatically converted by

AWS SCT are clearly marked so that they can be manually converted to complete the migration. AWS SCT can also scan your application source code for embedded SQL statements and convert them as part of a database schema conversion project.

During this process, AWS SCT performs cloud native code optimization by converting legacy Microsoft SQL Server functions to their equivalent AWS service to further modernize the applications at the same time of database migration. The diagram below illustrates a similar pattern that we used to migrate VMware database instances to Amazon RDS. In this illustration we are still using the AWS DMS service along with AWS SCT to convert the source Microsoft SQL database to a variety of AWS database service targets. The process is similar as the database is first converted to the target schema, then cutover to the new instance.



VMC and Microsoft Licensing

Updated Microsoft Licensing

Starting October 1, 2019, Microsoft has modified their licensing terms related to outsourcing rights and how their licenses are applied to dedicated hosted cloud services. The new licensing term will not impact the use of existing licensing and software, and all existing perpetual software licenses are "grandfathered" in and retain the same rights, and also have transfer rights unless purchased from an OEM that explicitly prohibits it.

1. Microsoft's licensing change means on-premises software that is not eligible for License Mobility can no longer be used on AWS Dedicated Hosts if the licenses are purchased after October 1, 2019 or running a version released after that date.
2. Customers with existing Microsoft software listed above which is purchased before October 1, 2019 can continue to use all of those existing licenses with dedicated hosts on AWS through BYOL.

3. This license change does not impact the use of AWS license included (LI) Windows Server and Microsoft SQL server instances. It also does not impact upgrades to existing versions of software, including Windows Server 2019 of SQL Server 2017

What does this mean for AWS Customers

1. Any licenses purchased before October 1, 2019 can be used with AWS Dedicated Hosts on AWS, as long as the licenses are not upgraded to a version released after the October 1, 2019 date.
2. Products that are eligible for License Mobility can still be brought to AWS Dedicated Hosts regardless of when the products were purchased. There are no changes to License Mobility terms and customers can continue to bring SQL Server, Remote Desktop, and System Center to shared EC2 tenant EC2 as long as the products have an active Software Assurance (SA).
3. All new licenses purchased after October 1, 2019, as well as any future version of Microsoft software, (Windows Server 2019), will not be permitted to run on the AWS Dedicated Hosts offering, (also announced on August 1, 2019), unless authorized under the new terms. The authorized software must now also be purchased with Microsoft Software Assurance (SA).
4. The primary benefit of Software Assurance (SA) is version upgrade rights, but Microsoft is now forcing customers to pay the annual premium to have Software Assurance (SA) to use a dedicated cloud offering but cannot take advantage of the primary benefit, without violating terms and being forced to move back on-premises or to Azure Dedicated Host, or face litigation.
5. Since new Windows Server licenses cannot be applied in dedicated clouds, new Core Infrastructure Suite (CIS), Remote Desktop Services, SharePoint, Skype for Business, and Exchange Server instances cannot be provisioned unless there is an existing Windows Server license available since there isn't a version available for Linux like SQL Server on Linux. Also, SQL Server on Linux is not at feature parity with the SQL Server editions for Windows.
6. The Unlimited Virtualization feature of Windows Server Datacenter will allow customers to continue to deploy new VMs up to the limit of the capacity of the licensed compute.
7. SQL Server Enterprise also offers the Unlimited Virtualization feature but has an additional stipulation that requires Software Assurance (SA), and without Software Assurance, the number of SQL Server instances deployed on that compute host cannot exceed the number of licensed physical CPU cores excluding hyperthreading. For example, on a VMC i3.metal host, that would mean the customer could deploy up to 36 SQL Server Enterprise instances across up to 36 VMs.