VMware Cloud on AWS

Practitioners quick reference for cloud migration and modernization

WHAT IS VMWARE CLOUD ON AWS?

VMware Cloud on AWS is a unified SDDC platform that integrates VMware vSphere®, VMware vSAN™, and VMware NSX® on top of bare metal hardware from AWS. Utilizing the same trusted, enterprise-grade VMware products and tools, customers can tap into the broad range of AWS services while taking advantage of the functionality, elasticity, and security they expect to gain in the cloud.

Migrating workloads to the cloud can be complex and time-consuming. Organizations need to address varying Virtual Machine (VM) formats, disparate hardware, network connectivity, and application dependencies — all while keeping downtime to a minimum. They also need to be assured that the destination is capable of supporting the transformation of their applications over time to cloud native frameworks. Maintaining operational consistency while minimizing learning curves and re-tooling can seem impossible. VMware Cloud™ on AWS can dramatically simplify workload migration. This quick reference guide provides practitioners with key considerations to keep in mind prior to, during, and after a cloud migration.

Key considerations when migrating to the cloud

Key consideration 1: Map your application dependences

Before an environment can be effectively sized, application dependencies must be understood in order to determine the scope of the migration. This process can be simplified significantly by utilizing automated tools such as VMware Network Insight™ to identify network communication patterns between applications. This can also be used to gain insight into data volume between systems and estimate data egress charges, if the dependent system remains on-premises.

Analyzing network traffic patterns can help determine application dependencies, however interviews with the application owners should also be considered. This will enable you to discover the unique constraints for each application being migrated. This may not always be possible, but time spent on discovery will lead to a smoother migration to the cloud.
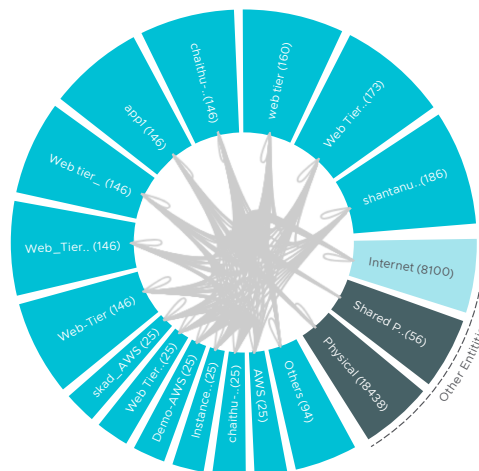

FIGURE 1: Analyze network traffic patterns to understand application dependencies

CLOUD MIGRATION TEAM

• Infrastructure administrators and architects

– Compute, storage, network and data protection

• Networking and security

– Security and compliance

• Application owner

– Applications, development, lifecycle

• Support and operations

– Automation, lifecycle, change management

FURTHER RESOURCES

Attend the *VMware Cloud on AWS Deploy and Manage course* from VMware Education to learn more about architecture and deployment.

Key consideration 2: Design requirements

Build a cross-functional migration team consisting of infrastructure administrators and architects, network and security, support and operations, application owners and other stakeholders.

FIGURE 2: Recommended cross-functional migration team

Design requirements are informed by the needs of the workload. For example, consider the availability requirements for the workloads that will be migrated. For these workloads, consider opting for Stretched Clusters for VMware Cloud on AWS. Stretched clusters facilitate zero Recovery Point Objective infrastructure availability for mission-critical applications. This enables customers to failover workloads with zero RPO within clusters spanning two AWS Availability Zones. Developers might also want to consider planning for their applications to make use of native AWS services for more advanced capabilities in areas such as networking and data analytics. Other considerations include storage, networking and security needs.
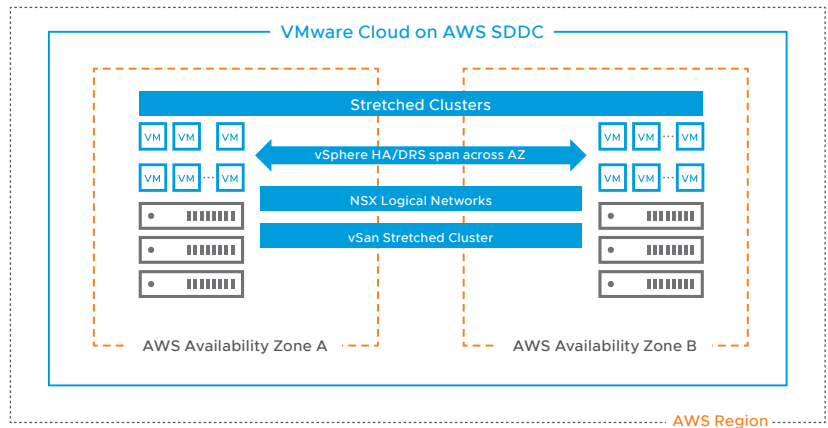

FIGURE 3: Stretched Clusters for VMware Cloud on AWS enable failover of workloads with zero RPO within clusters spanning two AWS Availability Zones

Key consideration 3: Sizing the environment

After completing the application dependency mapping and initial design, create an inventory of the workloads that are planned to be migrated to VMware Cloud on AWS.

If there are specific Independent Software Vendor (ISV) licensing requirements that would require special clusters or isolated environments, separate out those workloads for sizing purposes.

When thinking about future growth, the usage of AWS native services could reduce the resources needed in the SDDC. For example, modifying an application to use Amazon S3 for large-scale object storage could mean that they will not need as much storage and CPU within their SDDC.

Utilize the *VMware Cloud on AWS sizer* to build a configuration for the environments to be migrated. This also includes a TCO analysis to build the business case for migration.
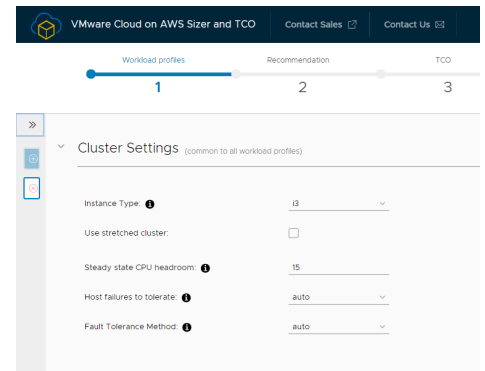

FIGURE 4: VMware Cloud on AWS Sizer and TCO

Key Consideration 4: Pilot the migrations

After dependencies are discovered and mapped, it is best to separate workloads and applications into one of three categories according to downtime tolerance:

1. Prolonged downtime

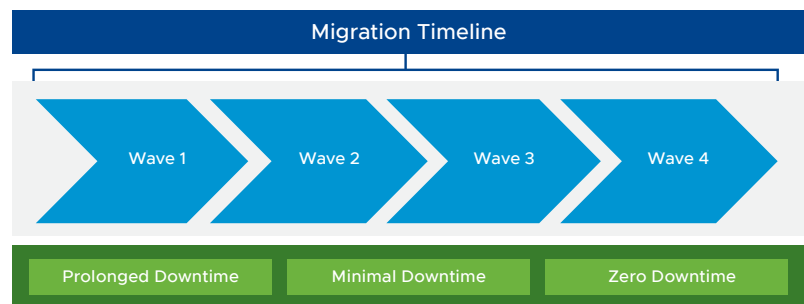2. Minimal downtime

3. Zero downtime

FIGURE 4: Plan to migrate workloads in waves by how you categorize them according to downtime tolerance

Once these workloads are separated and categorized, we recommend ranking into groups of migration waves starting with the greatest amount of downtime allowance for the business.

The first set of waves should be used to validate the run books for the migration, as well as test the monitoring and management of the applications and workloads during the migration itself. Ensure that the pilot migrations include validation of change control, user acceptance testing, and documentation updates.

Key consideration 5: Sequence your migrations

Staging the majority of the migrations within the next waves will rely on the application dependencies, downtime allowance, and change windows. Ensure that the waves are as small as possible by leveraging the appropriate available technologies: Live Migration, Bulk Migration, VMware HCX® vMotion® with VMware vSphere® Replication™, etc.

During the migrations ensure that monitoring tools are integrated with both environments and that cloud monitoring and management are integrated with external toolsets as required. Networking considerations such as stretched network terminations, load balancers reconfigurations, and 3rd party security appliances should be documented and optimized for workload placements. Data Protection and Disaster Recovery re-tooling will be required after all user acceptance testing is completed.

Key consideration 6: Automate migration and management

VMware Cloud on AWS has a full set of automation capabilities that can help improve cloud migrations by making them repeatable, integrated into existing DevOps flows, and able to work with popular automation tools and frameworks. PowerCLI, long a standard for automation of VMware products, can be used to deploy and manage SDDCs and clusters with the benefits that scripting provides, such as being repeatable and self-documenting. PowerCLI can also be used to perform migrations with HCX. VMware Data Center Command Line Interface™ (DCLI) is a multi-platform simple python based CLI which provides both an interactive and scriptable mode for working with VMware Cloud on AWS and the vSphere Automation API (REST API for vSphere).

VMware vRealize® Automation™ can deliver Infrastructure as Code-based automation for VMware Cloud on AWS. Blueprints created in vRealize Automation Cloud are written declaratively in YAML. Blueprints describe a desired end-state of virtual machines, networking, load balancers and other infrastructure components that are satisfied by the various Cloud Accounts and Integrations. With GitLab and GitHub integration the YAML blueprints can be subject to source control management, with versioning synchronised between blueprints and the source control system.

Terraform from Hashicorp is a tool for building, changing, and versioning infrastructure safely and efficiently. The Terraform provider for VMware Cloud on AWS enables users (cloud admins and DevOps engineers) to declaratively define and provision their VMware Cloud on AWS environments and simplify the management of their hybrid infrastructure through automation. This provider can be used with the existing Terraform providers for vSphere and NSX to manage end-to-end hybrid infrastructure from SDDC networking to VM lifecycle.

Key consideration 7: Modernize with Kubernetes

VMware Tanzu™ Kubernetes Grid™ Plus support for VMware Cloud on AWS enables customers to deploy their SDDC in the cloud, with the required components needed to architect and scale Kubernetes to fit their needs. Tanzu Kubernetes Grid Plus is an enterprise-ready Kubernetes distribution that packages open source technologies and automation tooling to help get you up and running quickly with a scalable, multi-cluster Kubernetes environment. Customers deploying Tanzu Kubernetes Grid Plus on VMware Cloud on AWS can benefit from 24x7 break-fix support for Kubernetes and key open source ecosystem technologies, along with proactive architectural guidance from VMware's Customer Reliability Engineering team. Additionally, customers can also engage with VMware Pivotal Labs for help transforming applications, leveraging modern application development and delivery methodologies. This establishes a reliable foundation for cloud native application management and application modernization.

Migrations with VMware Cloud on AWS are simple, fast and safe. Learn more by reviewing the available resources and participating in a *Hands-On Lab*.

Get started now with VMware Cloud on AWS
https://cloud.vmware.com/vmc-aws/get-started