Transitioning from VMware to the AWS Cloud

AWS Prescriptive Guidance

AWS Prescriptive Guidance: Transitioning from VMware to the AWS Cloud

Table of Contents

Transitioning from VMware to the AWS Cloud

Phurba Sherpa and Phani Lingamallu, Amazon Web Services

> **Note**
>
> As of April 30, 2024, VMware on AWS is no longer resold by AWS or its channel partners. The service will continue to be available through Broadcom. We encourage you to reach out to your AWS representative for details.

The transition from VMware to the AWS Cloud represents a significant organizational transformation that extends beyond technology. Although chief technology officers (CTOs) recognize the operational benefits of cloud adoption, they often face two primary challenges: the technical learning curve and organizational change management. The journey requires strategic workforce development and cultural transformation.

This shift demands careful attention to upskilling existing teams, adapting operational processes, and implementing comprehensive change management strategies to ensure successful cloud adoption.

For organizations that are beginning their cloud journey to AWS, this guide examines the transition in three key sections:

- On-premises operational analysis – Perform a systematic evaluation of existing infrastructure, operational practices, and business requirements to create a transformation baseline.
- Transition to the AWS Cloud – Create a comprehensive migration blueprint that transforms VMware workloads to the AWS Cloud while ensuring business continuity and security.
- Operational transformation – Evolve traditional IT operations into cloud-optimized practices that maximize agility, efficiency, and innovation.

Objectives

This guide provides a comprehensive blueprint for organizations transitioning from VMware to the AWS Cloud. It delivers a structured framework to help you:

- Map VMware workloads to AWS cloud-native services

- Maintain operational stability during transformation
- Implement cloud-optimized practices for long-term success

Intended audience

This guide is intended for technology leaders, cloud architects, and operations teams who are embarking on a journey to migrate their enterprise IT infrastructure to AWS. The guide assumes that you have knowledge and experience with VMware technologies, tools, and services for managing on-premises infrastructure.

Attachments

To access additional content that is associated with this document, download and unzip the following file:

attachment.zip

On-premises operational analysis

On-premises VMware environments encompass multiple components and can be broadly classified as virtualization, storage, networking, security, and operations. VMware environments require management of several key functions including:

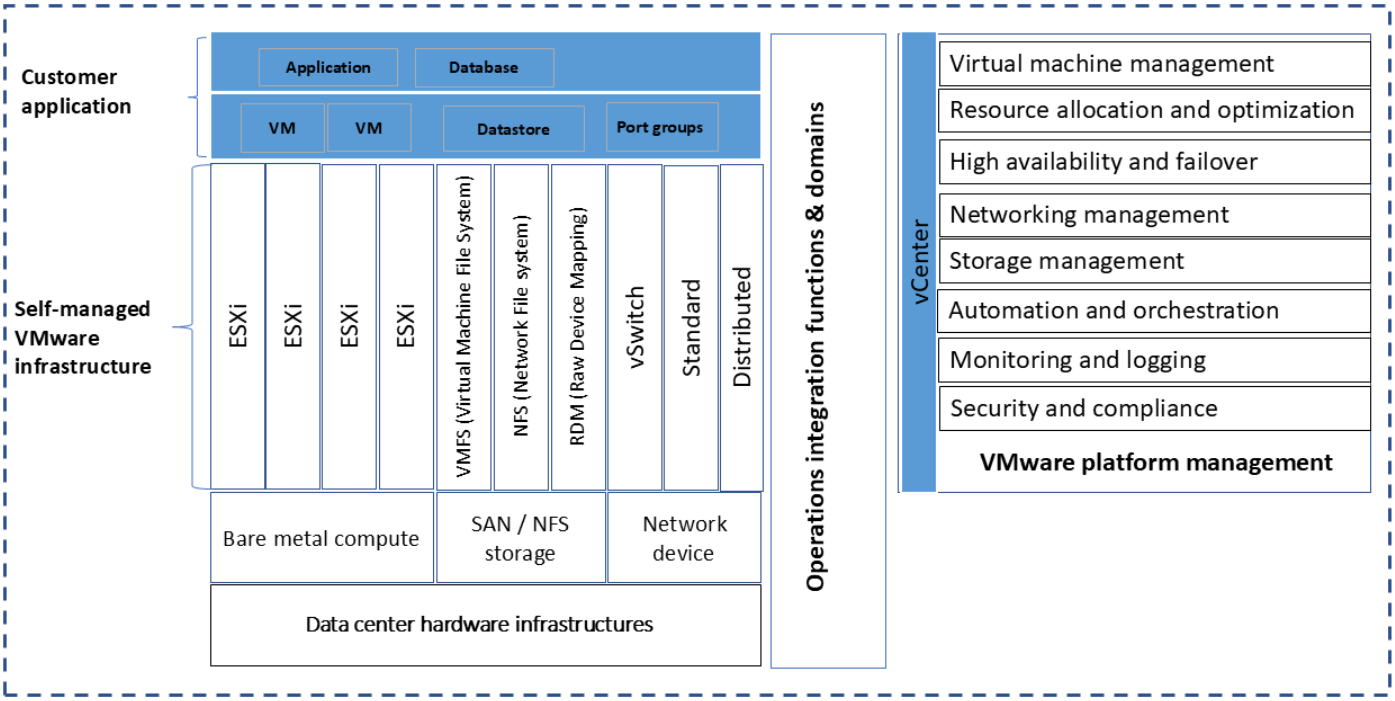
- Provisioning and managing virtual machines (VMs)
- Implementing data protection strategies
- Configuring virtual networks
- Automating operational tasks
- Ensuring compliance with organizational policies and industry regulations

This management approach helps organizations maintain control over their virtualized infrastructure while meeting security and operational requirements.

The following diagram shows a typical on-premises VMware environment and operational activities:

- Customer applications can encompass VMs, datastores, port groups, and databases.
- The self-managed VMware infrastructure supports bare metal compute, SAN and NFS storage, and network devices, all part of the data center hardware infrastructures.
- During a migration to AWS, organizations need to establish new or modify existing operational functions. The AWS operations modernization framework encompasses 21 operational domains. These domains are grouped into four main functions: Core operations, security and control functions, business management functions, and supporting functions. For more information about these functions, see Modernizing operations in the AWS Cloud.
- VCenter provides VMware platform management of multiple activities including:
  - VM management
  - Resource allocation and optimization
  - High availability and failover
  - Networking management
  - Storage management
  - Automation and orchestration
  - Monitoring and logging

- Security and compliance



These functions can be categorized into multiple workstreams and tasks, each designed to support business operations within on-premises VMware infrastructures. Following are the common VMware operational workstreams and related tasks:

- **Backup management** – Implement comprehensive backup and recovery operations. Tasks include daily virtual machine (VM) backups for critical systems, backup monitoring and troubleshooting, and retention policy management. Also includes the establishment of restore procedures with defined recovery point objectives (RPOs) for different workloads.
- **Storage management** – Oversee storage infrastructure management. Tasks include vSAN datastore provisioning and administration for VM workloads, while maintaining robust data protection and disaster recovery measures to ensure business continuity.
- **Network management** – Manage comprehensive network operations. Tasks include vSwitch configuration (standard and distributed), traffic management (vMotion, VM, and management), and virtual network administration.
- **Virtualization and compute** – Oversee comprehensive VMware operations, such as VM provisioning, ESXi, and vCenter management. Also included are tasks such as performance

monitoring, resource optimization, and capacity planning to maintain optimal infrastructure efficiency.

- **Automation and management** – Streamline infrastructure operations through automated provisioning and lifecycle management processes, incorporating self-service capabilities to empower users.
- **Monitoring** – Oversee centralized monitoring system for events and logs throughout the VMware environment. Tasks include implementing proactive troubleshooting measures across the infrastructure stack to ensure continuous operational efficiency.
- **Security and compliance** – Oversee the security posture of the on-premises VMware infrastructure. Tasks are achieved through comprehensive identity and access management, while ensuring compliance with industry regulations and organizational security policies for the virtualized environment.
- **Data center infrastructure** – Oversee the data center infrastructure that hosts the VMware environment through comprehensive management of physical components, ensuring optimal functioning and regular maintenance of critical systems. Examples of components include blade chassis systems, power supply units, and rack enclosures.
- **Application support** – Maintain and support the full stack of virtualized workloads, while optimizing their performance and ensuring continuous availability. Examples of virtualized workloads are applications, operating systems, and databases operating within the VMware environment.
- **Capacity planning** – Oversee hardware capacity management by monitoring and optimizing critical resources such as storage, CPU, RAM, and network infrastructure. Ensure efficient resource allocation while maintaining sufficient capacity for both planned operations and emergency requirements.
- **Asset/vendor and license management** – Oversee hardware refreshment initiatives, maintain comprehensive inventory management, and track licensing requirements for the VMware infrastructure and related components. The purpose is to help ensure operational continuity and that compliance standards are met.
- **Hardware management** – Manage and maintain the physical infrastructure that supports the VMware environment. Tasks include comprehensive hardware support, regular maintenance, and prompt issue resolution to support continuous optimal performance of the underlying systems.
- **IT operations** – Function as the primary support interface for the VMware environment. Tasks include addressing business IT requirements and resolving technical queries while ensuring operational continuity and maintaining alignment between IT services and business needs.

- **Account management** – Oversee financial management of the VMware infrastructure. Tasks include billing administration, cost allocation, and expenditure tracking, while providing accurate reporting and transparency of IT costs to respective business units and stakeholders.

Although specific workstream activities may differ across organizations, the fundamental objectives remain consistent. By transitioning from on-premises VMware to the AWS Cloud, organizations can capitalize on cloud advantages, achieving enhanced agility, improved scalability, and optimized cost management.

This guide discusses AWS services that align with your VMware workstreams. With this background, you can make informed decisions and develop comprehensive migration plans for a confident transition to the AWS Cloud.

Transition to the AWS Cloud

Moving to the AWS Cloud unlocks new opportunities for innovation, cost optimization, and business agility. Organizations can move beyond physical infrastructure constraints and leverage an extensive array of cloud-native services and capabilities. These range from highly scalable compute and storage resources to advanced analytics, machine learning, and serverless computing, providing a comprehensive platform for digital transformation.

Organizations migrating from VMware environments to AWS can realize significant benefits from the AWS flexible, pay-as-you-go approach that aligns IT costs with business demands. Traditional infrastructure requires substantial upfront capital expenditure for hardware, licensing, and maintenance. However, the AWS consumption-based pricing model helps organizations pay only for the resources that they actually use, eliminating overprovisioning and underutilization concerns.

Comprehensive cost optimization tools, including AWS Cost Explorer and AWS Budgets, enable effective cloud spending management through detailed usage insights and resource allocation optimization. Furthermore, AWS manages the underlying infrastructure maintenance, software updates, and patching, reducing the operational overhead typically associated with on-premises environments. This approach not only reduces costs but also allows IT personnel to focus on strategic initiatives that drive business value.

Through the AWS Migration Acceleration Program and other initiatives, AWS provides a structured path for migrating VMware workloads to the AWS Cloud. Begin with a complimentary AWS Migration Assessment that evaluates your organization's current on-premises environment, explores cloud opportunities, and helps build a comprehensive business case for AWS migration.

Key advantages of transitioning to the AWS Cloud

Key advantages of transitioning from VMware to the AWS Cloud include the following:

- **Rapid migration** – Rehosting VMware workloads provides the fastest and most straightforward approach to AWS Cloud migration. This approach minimizes the need for extensive application refactoring or redevelopment, enabling quick workload transition to the cloud environment.
- **Cost savings** – Moving infrastructure to AWS allows organizations to shift to a pay-as-you-go pricing structure. This transition can deliver significant cost savings compared to maintaining on-premises infrastructure and licenses, particularly for workloads with fluctuating resource demands.

- **Scalability and elasticity** – The AWS Cloud provides robust scalability and elasticity, enabling organizations to adjust resources based on demand. This capability ensures optimal resource utilization, eliminates over-provisioning or under-provisioning concerns, and removes the burden of managing extra capacity for dynamic requirements.
- **Reduced operational overhead** – Offloading infrastructure management to AWS reduces operational overhead associated with maintaining on-premises hardware, software, and data centers.
- **Improved reliability and availability** – The AWS Cloud offers robust service-level agreements (SLAs) and high availability (HA) configurations, which helps to achieve superior uptime and reliability compared to traditional on-premises environments.
- **Disaster recovery and backup** – The AWS Cloud provides built-in disaster recovery and backup solutions, which helps to support data integrity and business continuity during unforeseen circumstances.
- **Access to cloud-native services** – By migrating to the AWS Cloud, organizations can leverage various cloud-native services and tools, including managed databases, serverless computing, and advanced analytics capabilities.
- **Faster time to market** – Rehosting accelerates cloud migration, enabling rapid deployment of new features and services to meet evolving business requirements and customer demands.

The AWS global infrastructure is built with industry-leading security measures and compliance standards to support customer workloads that require various regulatory compliance certifications. For more information about these security responsibilities, see the AWS Shared Responsibility Model documentation.

Application rehosting

Organizations can rehost their existing VMware virtual machines, datastore storage, and virtual networks to the AWS Cloud, where business applications can operate efficiently. The following topics provide guidance for rehosting your existing VMware workloads to AWS services across compute, storage, and network components.

Rehosting virtual machines to the AWS Cloud

Amazon Elastic Compute Cloud (Amazon EC2) instances and VMware vSphere virtual machines (VMs) differ fundamentally in their architecture and storage approach. vSphere VMs store data as file sets such as Virtual Machine Disk (VMDK). Amazon EC2 instances use Amazon Machine Images (AMIs) and Amazon Elastic Block Store (Amazon EBS) volumes.

Organizations can migrate to AWS by using AWS Transform MGN, which supports VM migration from any supported operating system to Amazon EC2.

The following key elements highlight the architectural and operational differences between vSphere VMs and Amazon EC2 instances:

- **File format** – In vSphere, virtual machines are organized as a collection of files. These files include the .vmx file that handles configuration settings and .vmdk files that contain the virtual disk data. Also included are various auxiliary files (.nvram, .vmsd, .vmsn, and .vmss) that manage different VM states and functions. In contrast, Amazon EC2 doesn't rely on specific file formats. Instead, Amazon EC2 uses Amazon Machine Images (AMIs) as templates that contain all the necessary information and configurations needed to launch instances.
- **Storage** – In vSphere, the complete virtual machine environment—including the operating system, applications, and data—is consolidated within .vmdk virtual disk files. The .vmdk files are stored in datastores and managed through vSAN volumes. Amazon EC2, however, uses a more modular approach where the instance's root volume is created from an AMI snapshot and stored as an Amazon EBS volume. This approach provides the flexibility to attach additional EBS volumes or instance store volumes as needed.
- **Portability** – AMIs from the existing instance can be copied or shared across different AWS Regions or AWS accounts.
- **Scalability** – Amazon EC2 offers dynamic scaling capabilities. Its auto scaling features can automatically adjust the number of instances based on demand, enabling seamless scaling up or down in response to workload requirements.
- **Snapshots and backups** – Amazon EC2 takes a volume-centric approach, allowing for independent creation of EBS volume snapshots, which can then be used to create new volumes or AMIs. Integrated AWS services complement this Amazon EC2 capability, such as AWS Backup for comprehensive backup management.
- **Management** – AWS provides multiple management options including the graphical AWS Management Console, the AWS Command Line Interface (AWS CLI), AWS SDKs, and infrastructure as code (IaC) through AWS CloudFormation. These options offer greater flexibility in how users interact with and manage their resources.

For containerized workloads, VMware provides vSphere with Tanzu Platform, which enables you to run and manage containerized applications alongside traditional virtual machines in your existing infrastructure. AWS provides multiple container services that help you deploy, manage, and scale containers in the cloud.

The following recommendations can help you identify which AWS container service aligns most closely with your workload requirements:

- **Amazon Elastic Container Registry** – Use Amazon ECR with any AWS container orchestration service to store your container images. For more information, see the Amazon ECR documentation.
- **Amazon Elastic Container Service** – Use Amazon ECS to break monolith apps into microservices, migrate to the cloud, or run batch processing workloads. For more information, see the Amazon ECS documentation.
- **Amazon Elastic Kubernetes Service** – Use Amazon EKS to run Kubernetes on AWS, build hybrid applications across the cloud and on premises, or deploy machine learning (ML) models. For more information, see the Amazon EKS documentation.
- **AWS Fargate** – Use Fargate with Amazon ECS to launch serverless containers or build a platform as a service (PaaS). For more information, see the Fargate documentation.
- **Amazon Elastic Compute Cloud** – Use Amazon EC2 with any of the AWS management services for the maximum control over your launch type. For more information, see the Amazon EC2 documentation.

For more detailed information about AWS containers and suitable options for your organization, see Containers on AWS.

Rehosting datastores to the AWS Cloud

You can migrate VMware vSphere datastores, which function as storage repositories for virtual machine files and other data, to AWS storage services.

When moving data to the cloud, it's important to understand where you're moving it, the potential use cases, the type of data you're moving, and the network resources available. Your organization can choose from among several AWS services, based on your storage needs and workload characteristics:

- For persistent block storage, consider Amazon Elastic Block Store (Amazon EBS).
- For scalable file storage, consider Amazon Elastic File System (Amazon EFS).
- For object storage, consider Amazon Simple Storage Service (Amazon S3).

For block-level storage, you can migrate VMware VMFS and vSAN datastores to Amazon EBS, which provides persistent storage volumes for EC2 instances. You can migrate existing Server Message

Block (SMB) or Network File System (NFS) servers to Amazon FSx to reduce operational overheads, take advantage of elastic scaling, and increase availability. Amazon FSx is compatible with NetApp ONTAP, Windows File Server, Lustre, and OpenZFS. For modern file sharing services that don't require configuration of SMB or NFS, Amazon EFS is a serverless, fully elastic, fully managed file storage solution.

The following table highlights storage options that are optimized for specific circumstances. Use it to help determine the option that's appropriate for your use case.

Storage type	What is it optimized for?	AWS storage services or tools
Block	Applications that require low-latency, high-performance durable storage attached to single Amazon EC2 instances or containers, such as databases and general-purpose local instance storage.	Amazon EBS Amazon EC2 instance store
File system	Applications and workloads that require shared read and write access across multiple Amazon EC2 instances or containers or from multiple on-premises servers. Examples include team file shares, highly available enterprise applications, analytics workloads, and ML training.	Amazon EFS Amazon FSx Amazon FSx for Lustre Amazon FSx for NetApp ONTAP Amazon FSx for OpenZFS Amazon FSx for Windows File Server Amazon S3 File Gateway Amazon FSx File Gateway
Object	Read-heavy workloads such as content distribution, web hosting, big data analytics,	Amazon S3

	and ML workflows. Well-suited for scenarios where data needs to be stored, accessed, and distributed globally over the internet.	
Cache	Fully managed, scalable, and high-speed cache on AWS for processing file data that's stored in disparate locations. Examples include on-premises NFS file systems, and/or in cloud file systems (FSx for OpenZFS or FSx for ONTAP), and Amazon S3.	Amazon File Cache
Hybrid/Edge	Deliver low-latency data to on-premises applications and provide on-premises applications access to cloud-backed storage.	AWS Storage Gateway Tape Gateway AWS Storage Gateway Volume Gateway

The following table provides a detailed look at your online and offline options.

Migration options	When speed is the priority	When bandwidth is important	AWS storage services or tools
Online	Online is optimized for frequent updates to data. Use it for time-critical or ongoing workloads.	Consider scheduling your transfer during off hours when you have sufficient bandwidth.	AWS DataSync AWS Transfer Family FSx for ONTAP SnapMirror Storage Gateway
Offline	Suitable for one-time or periodic uploads—	This choice makes sense when you	AWS Snowball

	and when data can be static in transit.	need to use only the minimum available bandwidth—and you prefer the predictability of physical moves.

For more information about storage options, see the AWS Decision Guide Choosing an AWS storage service.

Rehosting virtual networks to the AWS Cloud

VMware virtual networking capabilities can be redesigned for AWS by using Amazon Virtual Private Cloud (Amazon VPC). You can manage the IP address usage of the resources running in your VPCs by using Amazon VPC IP Address Manager (IPAM). Amazon VPC provides logically isolated virtual networks with configurable subnets, routing tables, and security groups for traffic control and additional protection through AWS Network Firewall and Web Application Firewall. Amazon VPC doesn't require configuration of port groups or VLAN tagging unlike existing on-premises VMware vSwitch. The AWS approach makes management simpler while maintaining functionality. For more information, see How Amazon VPC works.

With AWS Transit Gateway, you can connect VPCs, AWS accounts, and on-premises networks to a single gateway. Transit Gateway acts as a cloud router, managing traffic between VPCs and on-premises networks through a central hub. With this capability, you can design and implement networks at scale.

AWS offers services and tools to help organizations maintain network monitoring and visibility, such as Amazon CloudWatch, AWS CloudTrail, Reachability Analyzer, Amazon VPC Lattice, and VPC Flow Logs. Organizations can use these integrated services and tools to get the required insights from application networking.

For VMware NSX specific use cases, AWS offers a different approach by managing the underlying network infrastructure, eliminating the need for complex network virtualization management. To address sophisticated networking requirements, you can deploy AWS networking and security services either individually or in combination. With this flexibility, organizations can redirect their focus from infrastructure maintenance to business-driven objectives.

The following table provides an overview of AWS networking and content delivery services that are optimized for specific scenarios.

Service category	What is it optimized for?	AWS networking and content delivery services
Network foundations	Getting started with AWS networking services and connecting your VPCs securely.	Amazon VPC AWS PrivateLink AWS Transit Gateway
Global and hybrid connectivity	Help to ensure private, secure, and global network connectivity.	AWS Client VPN AWS Cloud WAN AWS Direct Connect AWS Site-to-Site VPN
Edge networking and content delivery	Low latency, reliable traffic routing to and from your workloads.	Amazon CloudFront AWS Global Accelerator Amazon Route 53 AWS Data Transfer Terminal
Application networking	Help to ensure that your workloads are highly available, adapt to demand, and can communicate with each other.	Amazon API Gateway Amazon VPC IPAM Amazon VPC Lattice Elastic Load Balancing
Network security and remote access	Protect your workloads against malware, DDoS, SQL injection, and cross-site scripting attacks.	AWS Firewall Manager AWS Network Firewall AWS Shield AWS Verified Access

AWS WAF

For more information, see the AWS Decision Guide Choosing an AWS networking and content delivery service.

Resource management

This section covers how to transition the following VMware resource management functions to AWS cloud-native services:

- vSphere resource allocation and optimization
- vSphere HA

vSphere resource allocation and optimization

VMware vSphere Distributed Resource Scheduler (DRS) automatically monitors and balances workload resources across ESXi hosts in a cluster. When in AWS, the hypervisor host and the underlying infrastructure are managed by AWS. With this approach, you can focus on application and business outcomes, reducing your operational overhead.

AWS automated resource management solutions including the following:

- Amazon EC2 Auto Scaling dynamically adjusts Amazon EC2 instance numbers based on demand.
- Elastic Load Balancing (ELB) distributes incoming traffic across multiple instances.
- AWS Compute Optimizer analyzes and recommends optimal instance configurations.
- Instance Scheduler on AWS enables automated scheduling of instance operations.

Collectively, these AWS solutions deliver resource optimization capabilities without the operational overhead associated with on-premises infrastructure management.

vSphere HA

High availability (HA) in VMware vSphere HA and AWS follow fundamentally different approaches. vSphere HA provides automatic failover and restart of virtual machines across ESXi hosts for on-premises workloads. AWS manages infrastructure-level availability through its underlying platform, backed by service-level agreements (SLAs) and service-level objectives (SLOs) for all paid, generally available services.

AWS services such as AWS Transform MGN and AWS Database Migration Service (AWS DMS) facilitate migrations between different environments. The AWS approach provides your organization with more flexibility and control of your resources.

To help guide your approach for resource management, following are key specifications:

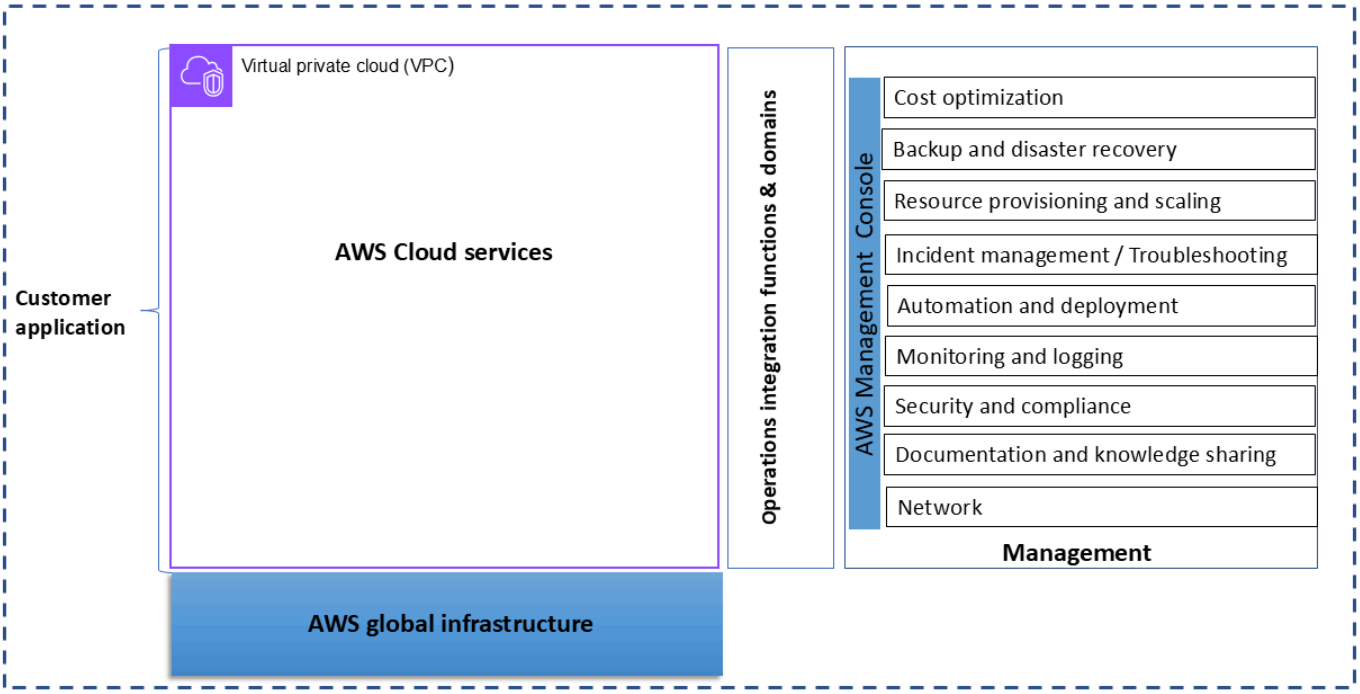
- **Virtual machine management** – The AWS Management Console serves as a central management resource for managing EC2 instances.
- **Automation and orchestration** – AWS provides multiple automation services such as AWS CloudFormation and the AWS CDK for IaC and AWS Systems Manager for resource management. These AWS services support comprehensive automation of resource provisioning and management within the cloud environment.
- **Monitoring and logging** – AWS offers Amazon CloudWatch for resource and application monitoring, and AWS CloudTrail handles logging and auditing of AWS account activities. AWS monitoring combines VPC Flow Logs for network traffic analysis and AWS X-Ray for application request tracking, providing complete visibility into network and application performance. These integrated services enable organizations to maintain visibility and track operational metrics across their respective environments.
- **Security and compliance** – AWS integrated security services include AWS Security Hub CSPM for centralized security management, AWS WAF for web application protection, AWS Shield for DDoS protection, and AWS Identity and Access Management (IAM) for access control. These AWS services provide multi-layered security and compliance capabilities across the cloud infrastructure.
- **Management and governance** – To optimize cloud operations, AWS Systems Manager enables centralized management of AWS resources. Cost management is addressed through AWS Budgets and AWS Cost Explorer. AWS Organizations helps manage multiple AWS accounts. Amazon EC2 Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. AWS License Manager makes it easier to manage licenses in AWS and on-premises servers. These services collectively enable efficient resource management, cost optimization, and operational excellence in AWS environments.

Implementing IT operations in the AWS Cloud

AWS can help reduce the operational overhead that organizations incur from their infrastructure maintenance responsibilities. As a result, IT teams can redirect their focus from routine operational tasks to strategic business initiatives, improving overall organizational efficiency and innovation capacity.

The following diagram provides an overview of an AWS Cloud environment:

- Customer applications can access AWS services in the AWS Cloud using a virtual private cloud (VPC). AWS global infrastructure supports the AWS Cloud.
- AWS offers multiple services to automate your IT operations, combining both core functionalities and AI-powered operations (AIOps) capabilities. For more information about the AWS services that support automation, see AWS services for automation. Understanding these services can facilitate your smooth transition from on-premises infrastructure to AWS native solutions.
- The AWS Management Console supports multiple operational tasks including:
  - Cost optimization
  - Backup and disaster recovery
  - Resource provisioning and scaling
  - Incident management and troubleshooting
  - Automation and deployment
  - Monitoring and logging
  - Security and compliance
  - Documentation and knowledge sharing
  - Network management



To effectively transition from VMware to the AWS Cloud, organizations should use the following steps:

1. Identify key AWS operational tasks.
2. Assess existing on-premises processes for potential reuse.
3. Adopt adopt cloud-native operations gradually where appropriate.
4. Align current workflows with AWS best practices.
5. Develop skills in tools and services that are specific to AWS.
6. Implement a phased approach to minimize disruption.

This approach helps to provide a smooth migration while leveraging existing expertise and gradually embracing cloud-native capabilities. Teams can leverage AWS capabilities quickly while maintaining operational continuity. The following table provides guidance to help you get started with AWS operational tasks.

AWS operational alignment strategy	AWS operational tasks	Existing on-premises processes to assess for potential reuse
Monitoring and logging	• Review and analyze Amazon CloudWatch logs, metrics, and alarms for any issues or anomalies. • Monitor the health and performance of EC2 instances, load balancers, databases, and other AWS services. • Analyze log data from services like AWS CloudTrai l for security and complianc e purposes.	• Monitoring and observabi lity
Security and compliance	• Review and apply necessary security patches and updates to EC2 instances and other AWS services. • Verify that security groups, network access control lists (ACLs), and IAM policies are configured correctly and follow best practices. • Check for any security vulnerabilities or misconfig urations using AWS Security Hub CSPM or third-party security tools. • Ensure compliance with industry standards and regulations (for example, Payment Card Industry	• Security and compliance management

	Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and System and Organization Controls SOC)..	
Cost optimization	• Monitor and analyze AWScost and usage reports using AWS Cost Explorer or third-party cost management tools. • Identify and terminate unused or underutilized resources (for example, idle EC2 instances or unattached EBS volumes). • Implement cost-saving strategies such as Reserved Instances, Spot Instances, or AWS Auto Scaling.	• • Capacity planning and forecasting
Backup and disaster recovery	• Create and verify backups of critical data, including EBS volumes, Amazon RDS databases, and Amazon S3 buckets. • Test and validate disaster recovery plans and procedures using services like AWS Backup and AWS Elastic Disaster Recovery.	• Availability and business continuity management

Resource provisioning and scaling	• Provision new AWS resources (for example, EC2 instances, Amazon RDS databases, or load balancers) as needed for new projects or workloads. • Scale existing resources up or down based on demand, using services like AWS Auto Scaling.	• Provisioning and configuration management
Automation and deployment	• Leverage IaC tools like AWS CloudFormation or HashiCorp Terraform to automate resource provisioning and configuration management. • Implement continuous integration and continuous deployment (CI/CD) pipelines for application deployments using services like AWS CodePipeline, AWS CodeBuild, and AWS CodeDeploy.	• Provisioning and configuration management

Incident management and troubleshooting	• Monitor and respond to any alerts, incidents, or service disruptions. • Troubleshoot and resolve issues related to AWS resources, networking, or application performance. • Collaborate with development teams and other stakeholders to investigate and resolve complex issues.	• Event and incident management
Documentation and knowledge sharing	• Maintain up-to-date documentation for AWS infrastructure, configura tions, and processes. • Conduct knowledge-sharing sessions or training for team members on AWS best practices.	• IT operations • Application support

Network	• Define your IP address ranges, subnets, routing tables, and network gateways. • Enable secure communica tion between AWS resources and your on-premises network. • Maintain route tables, security groups, ACLs, and network connectiv ity by using AWS Direct Connectand Transit Gateway.	• Network management

Develop skills in AWS services and tools

Through AWS training programs, certifications, documentation, and best practice guides, teams can continuously enhance their cloud expertise. Organizations can become proficient with the latest AWS services and capabilities, enabling them to design, implement, and maintain effective cloud solutions that drive business success.

AWS provides a wide range of resources and programs to help individuals and organizations build their skills and capabilities on the AWS Cloud such as:

- AWS Training and Certification
- AWS Skill Builder
- AWS Partner Training and Certification
- AWS Events and Webinars

Resources

For additional information, see the following AWS resources.

AWS Blogs

- Accelerate the modernization of Mainframe and VMware workloads with AWS Transform

AWS Prescriptive Guidance

- AWS Enterprise Transformation Framework
- Backup and recovery approaches on AWS
- Designing and implementing logging and monitoring with Amazon CloudWatch
- Modernizing operations in the AWS Cloud

Other AWS resources

- AWS Cloud Adoption Framework (AWS CAF)
- AWS Migration Acceleration Program
- AWS Migration Assessment
- Operational Excellence Pillar – AWS Well-Architected Framework

Contributors

Contributors to this guide include:

Authors

- Phurba D Sherpa, Senior Partner Solutions Architect, Migration and Modernization, AWS
- Phani Lingamallu, Senior Partner Solutions Architect, AWS

Reviewer

- Sahan Celikag, Senior Partner Solutions Architect, VMware, AWS

Document history

The following table describes significant changes to this guide.

Change	Description	Date
Initial publication	—	August 28, 2025