

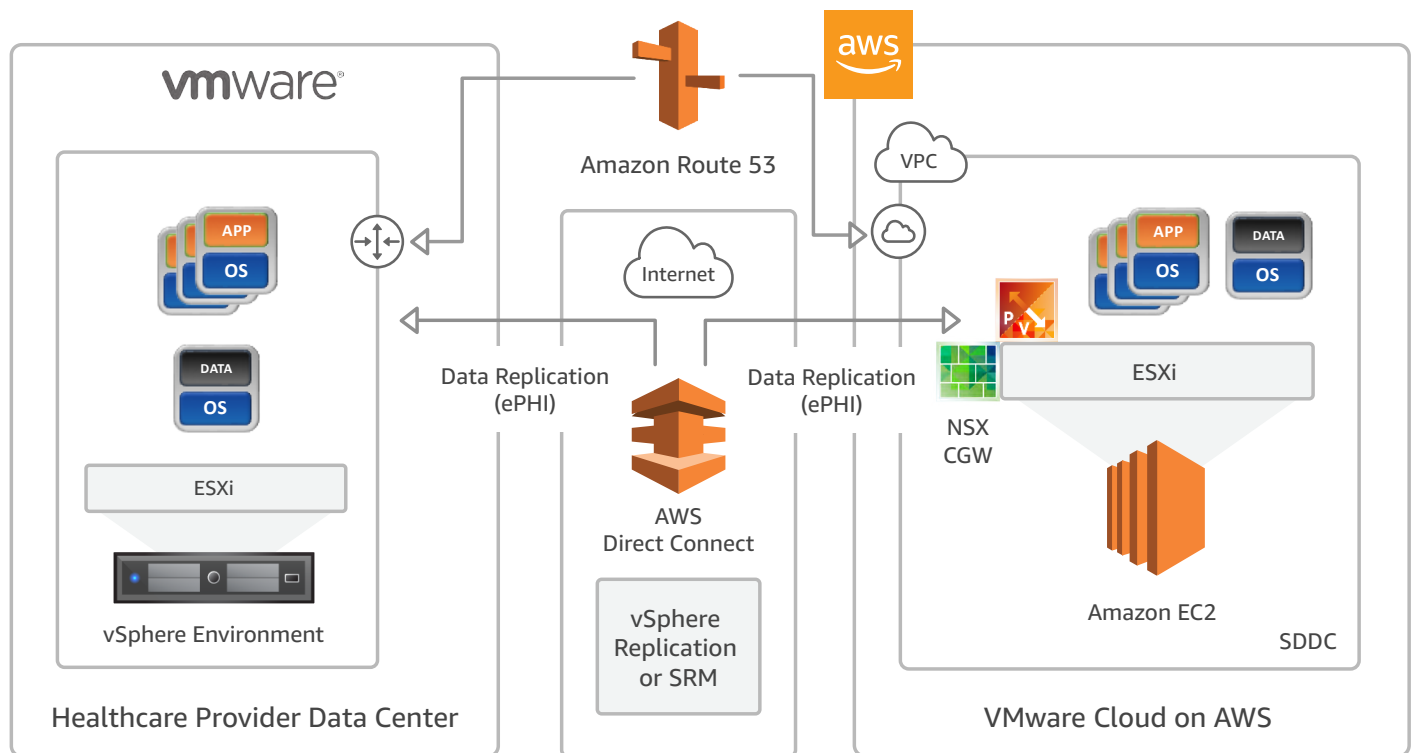
VMware on Amazon Web Services (AWS) simplifies the administrative tasks of cloud adoption by leveraging a familiar operational framework and providing a simple, fast way for healthcare organizations to port applications to AWS with accessibility to the growing list of storage, compute, networking, and artificial intelligence and machine learning (AI/ML) HIPAA-eligible services on AWS.

Healthcare companies are leveraging VMware on AWS to:

- Consolidate healthcare data assets
- Enable population healthcare analytics
- Shift non-clinical productivity and Tier 2&3 applications to the cloud
- Improve patient and member experiences with SaaS applications
- Enhance image radiology with machine learning

In order to help customers, the following diagrams are healthcare reference architectures for VMware on AWS environments. They address common disaster recovery, availability, migration, and backup scenarios along with Virtual Desktop Infrastructure (VDI) using VMware Horizon 7.

## Data Recovery as a Service with Site Recovery Manager

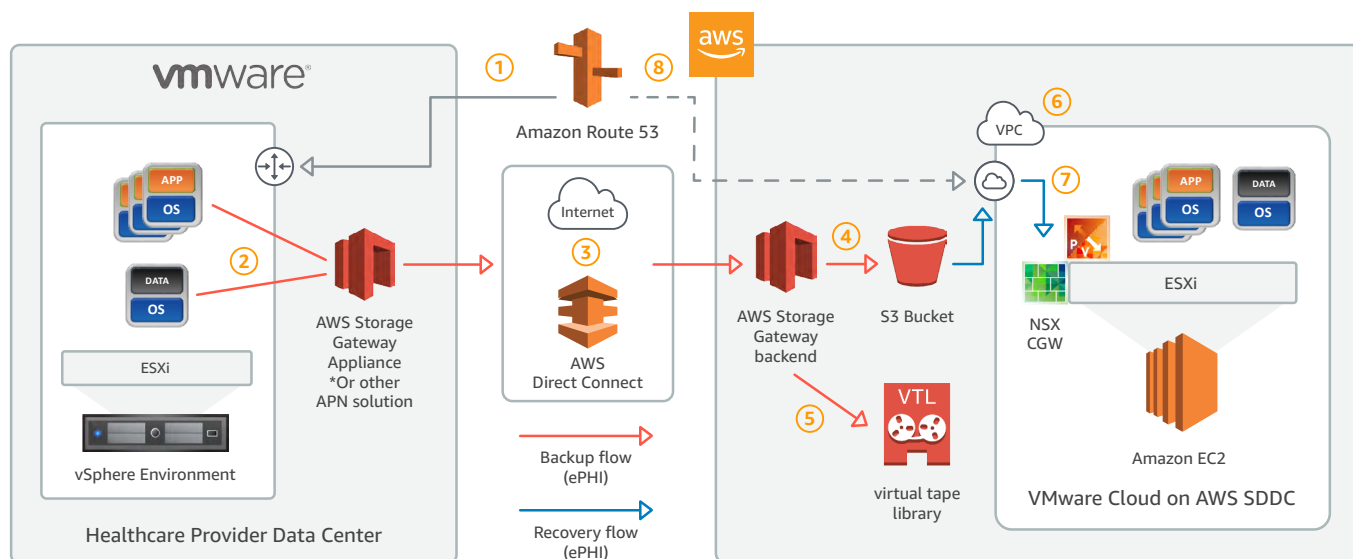


- Deliver Data Recovery as a Service built on VMware's established Data Recovery Solutions
- Remove the need for a dedicated disaster recovery data center
- Leverage AWS services you already know such as AWS Direct Connect to establish a dedicated network and Amazon Route 53, a highly available Domain Name System (DNS) service
- Quickly backup and restore your environment on AWS using tools you are already familiar with on VMware, such as vSphere Replication
- All services are HIPAA-eligible if you have an executed business associate agreement (BAA) with VMware and AWS for ePHI data

## Backup and Restore to VMware Cloud on AWS

Native Services Integration: AWS Storage Gateway, Amazon Simple Storage Service (Amazon S3), AWS Direct Connect, and Amazon Route 53

- Lower capital expenditures by eliminating the need for a disaster recovery data center
- Lower overall cost to implement, despite being the longest Recovery Time Objective (RTO)
- Quickly backup and restore your environment on AWS using tools you are already familiar with on VMware
- All services are HIPAA-eligible if you have an executed business associate agreement (BAA) with VMware and AWS for ePHI data



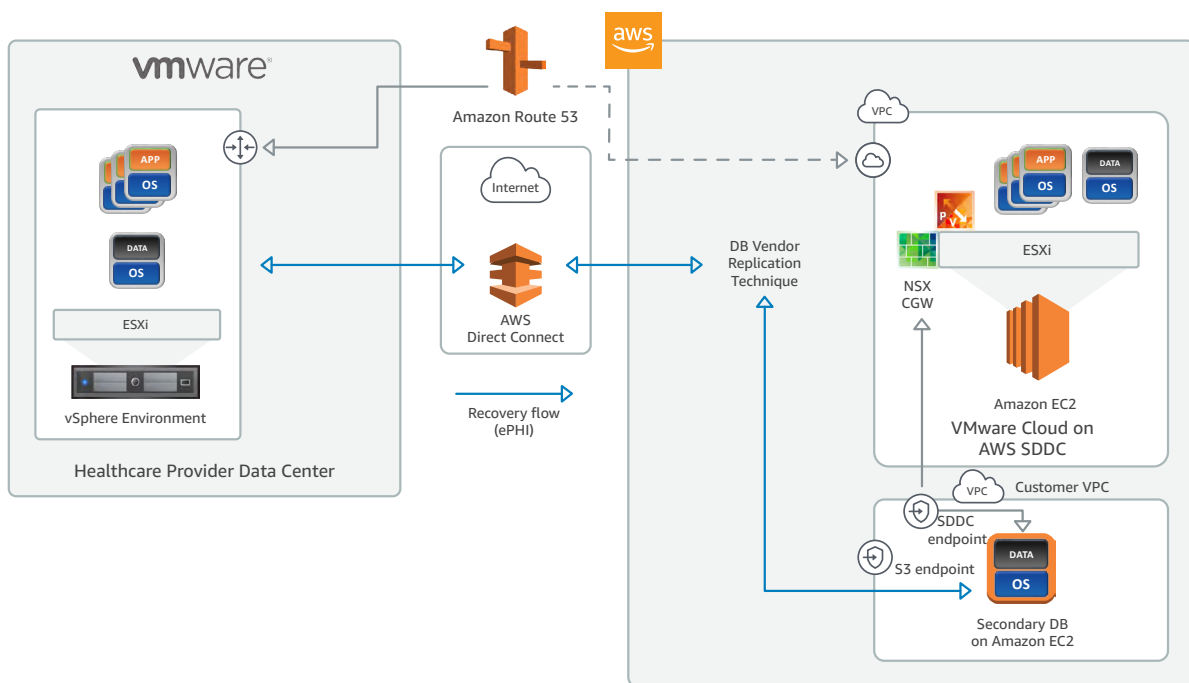
1. DNS requests are handled by Amazon Route 53, to resolve requests to your primary data center (DC) on-premises.
2. Application and data level backups are stored on the file-based AWS Storage Gateway (or any other AWS Partner Network (APN) solution) using a partner integrated solution or application-level backup software.
3. AWS Storage Gateway connects to the backend Amazon S3 either over AWS Direct Connect for optimized network experience or via the public Internet. Data destined to Amazon S3 is encrypted in transit using transport layer security (TLS).
4. File gateway, AWS Storage Gateway for files, uses an AWS Identity and Access Management (IAM) role to access the customer's Amazon S3 bucket to store backed up data as objects in Amazon S3.
5. For long-term archiving, AWS Storage Gateway, when combined with a virtual tape library configuration, can be used to store data in Amazon Glacier, an extremely low-cost cloud storage service on AWS.
6. The recovery process starts by launching and configuring a VMware software-defined data center (SDDC) cluster in the designated AWS recovery region through a web portal or automation script using VMware vRealize Automation (vRA), AWS CloudFormation, or VMware vSphere Command-Line Interface (vSphere CLI).
7. Once the VMware SDDC is ready, deploy the backup software data mover to restore backed up VMs and application data from Amazon S3, using either a public Amazon S3 endpoint or a Virtual Private Cloud (VPC) endpoint for Amazon S3.
8. Final recovery step is to update the Amazon Route 53 record setting to resolve requests to the new secondary DC on the cloud.



## Active/Active on VMware Cloud on AWS

Native Services Integration: Amazon EC2, AWS Direct Connect, and Amazon Route 53

- This architecture provides you the ability to extend your on-premises VMware environment to AWS using VMware Cloud on AWS in an active/active architecture
- Migrate to VMware Cloud on AWS with minimal downtime
- Use any database replication technique that you are already familiar with
- All services are HIPAA-eligible if you have an executed BAA with VMware and AWS for ePHI data

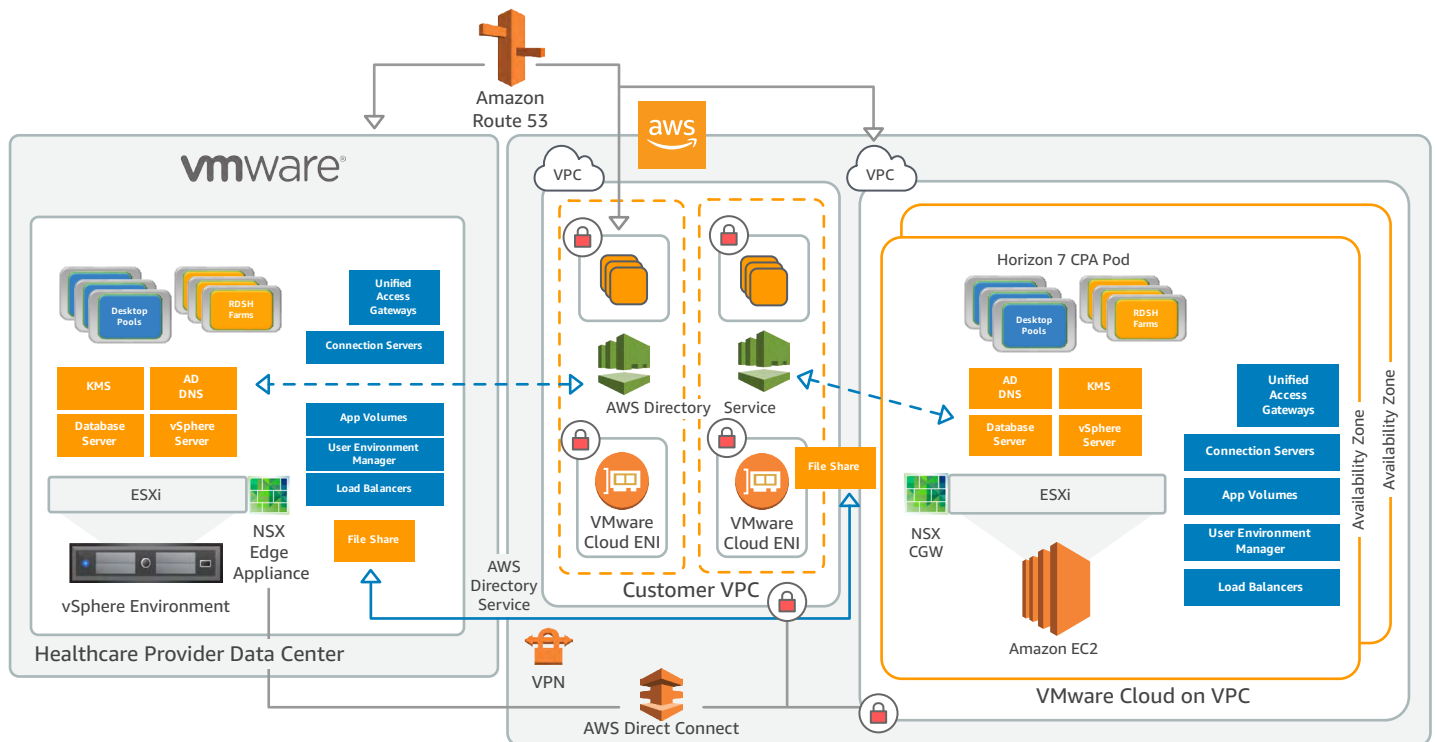


1. New or existing services are built on VMware Cloud on AWS
2. DNS requests are handled by Amazon Route 53.
3. Database replication is handled using database vendor specific replication techniques

## Expand your on-premises VMware environment to AWS using Cloud Pod Architecture

Native Services Integration: Amazon Route 53, AWS Direct Connect, VPN, Amazon VPC, Amazon EC2, and AWS Directory Service

- Architecturally, the Horizon 7 Platform is the same on-premises as on AWS. Traditional on-premises Virtual Desktop Infrastructures (VDIs) are often limited in how quickly they can scale as well as how cost-effectively they respond to business needs
- Horizon 7 Healthcare and Life Science customers are using VMware Cloud on AWS to elastically scale on-premises Horizon 7 infrastructures and to expand capacity for existing workloads
- VMware Cloud on AWS makes it easy to add desktop services without managing additional data center infrastructure
- All services are HIPAA-eligible if you have an executed BAA with VMware and AWS for ePHI data



1. Horizon 7 is built in VMware Cloud on AWS.
2. DNS requests are handled by Amazon Route 53, to resolve requests to primary on-premises DCs or VMware Cloud on AWS.
3. Data on the file share is kept in sync using an APN Partner solution to replicate the data between AWS and on-premises.
4. End-user VDI is easily scaled up or migrated to VMware Cloud on AWS.