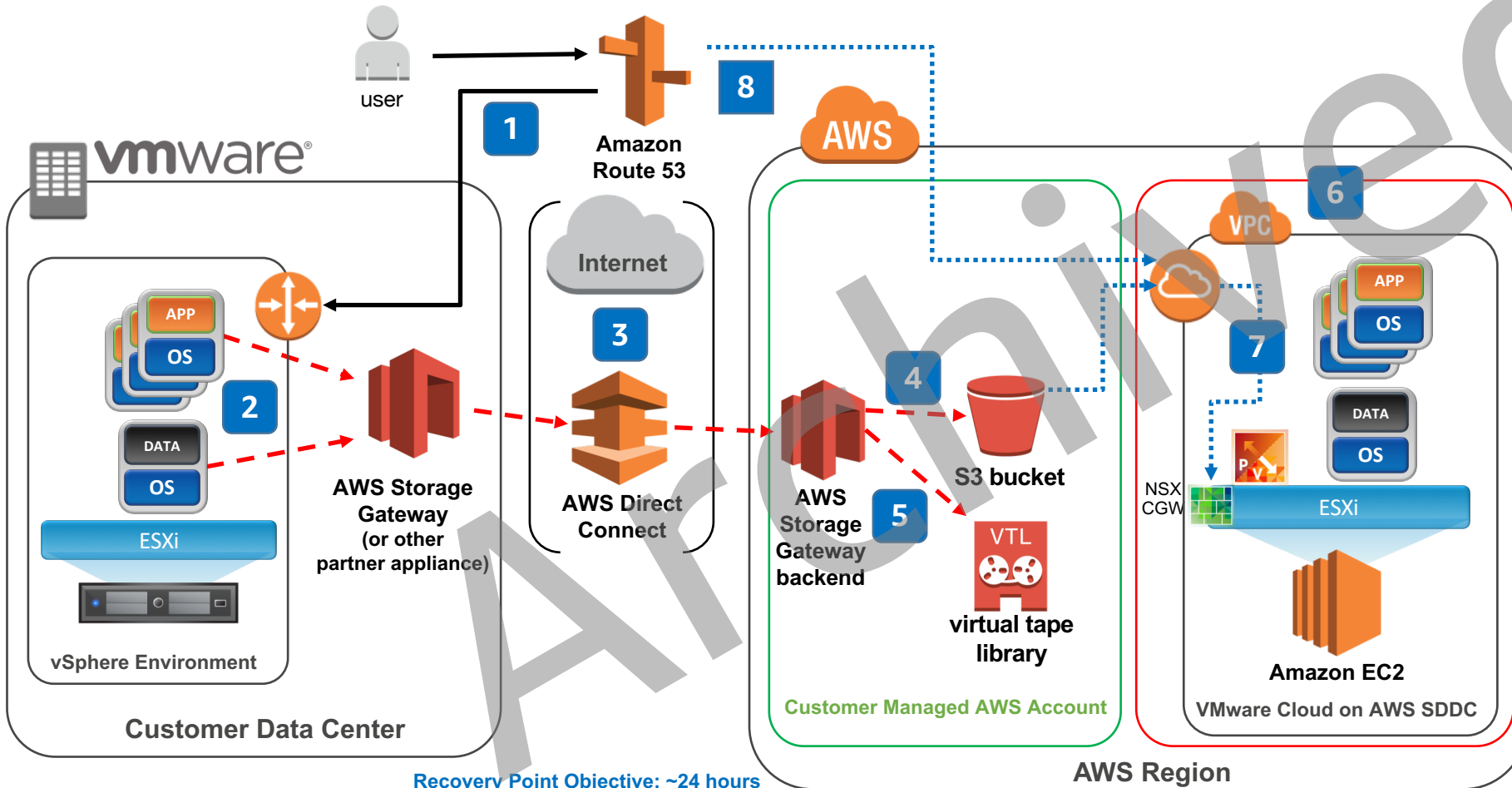


# Backup and Restore to VMware Cloud on AWS

## Native Services Integration: Storage Gateway, S3, Direct Connect, and Route53



Recovery Point Objective: ~24 hours  
 Recovery Time Objective: ~4 - 6 hours  
 Cost: \$

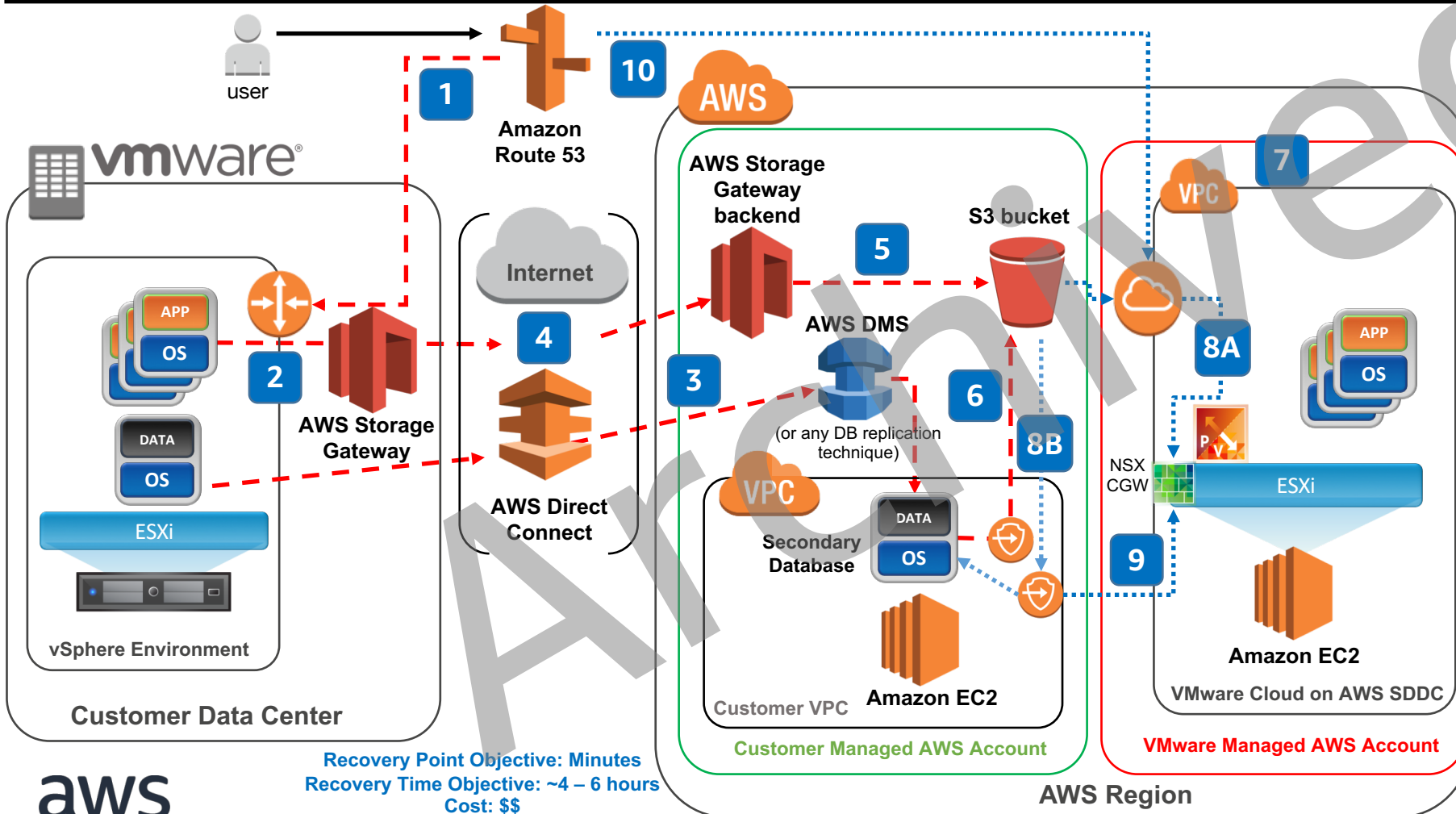
Backup flow - - - - ->  
 Recovery flow .....>

- | # | Description  |
|---|--|
| 1 | Amazon Route 53 routes DNS requests to the primary domain controller on-premises.  |
| 2 | VM and application backups are stored in Amazon S3 using an AWS Storage Gateway or other storage appliance using a partner-integrated solution or application-level backup software.   |
| 3 | The on-premises Storage Gateway securely transfers the backup data to the Storage Gateway backend using Direct Connect or through an SSL Internet connection.                          |
| 4 | File gateway uses an AWS Identity and Access Management role to access the customer backup data and securely store it in Amazon S3.  |
| 5 | Use the virtual tape library configuration in the Storage Gateway for long term data archiving to AWS Glacier or other archive service.  |
| 6 | The recovery process starts by launching and configuring a VMware SDDC cluster in AWS with the web portal or through automation scripts using AWS CloudFormation, VMware vRA, or vCLI. |
| 7 | After VMware Cloud on AWS SDDC is ready, deploy the software to restore the backed up application and VM data from Amazon S3.  |
| 8 | The final recovery step is updating the Route 53 DNS records to route new requests to secondary domain controller in AWS.  |

### AWS Reference Architecture

# Pilot Light on VMware Cloud on AWS

## Native Services Integration: Storage Gateway, EC2, S3, DMS, Direct Connect, and Route53



Recovery Point Objective: Minutes  
 Recovery Time Objective: ~4 – 6 hours  
 Cost: \$\$

Backup flow - - - - -  
 Recovery flow ······

- | #  | Description  |
|----|--|
| 1  | Amazon Route 53 routes DNS requests to the primary domain controller at the customer data center.  |
| 2  | VM and application backups are stored in Amazon S3 using an AWS Storage Gateway or another storage appliance or software backup solution.  |
| 3  | AWS Database Migration Service (DMS) replicates data from primary database to secondary database in AWS.   |
| 4  | Storage Gateway and DMS connect to the backend AWS services endpoints over Direct Connect or the Internet.   |
| 5  | File gateway uses an AWS Identity and Access Management role to access the customer backup data and securely store it in Amazon S3.  |
| 6  | Single point-in-time backups can be created on the secondary database using EBS snapshots stored in S3.  |
| 7  | The recovery process starts by launching and configuring a VMware SDDC cluster in AWS with the web portal or through automation scripts using AWS CloudFormation, VMware vRA, or vCLI. |
| 8  | After VMware Cloud on AWS SDDC is ready, retrieve backed up data using (A) public S3 endpoint or (B) VMware endpoint using S3 VPC endpoint.  |
| 9  | Recovered applications in VMware SDDC directly connect to the secondary database through VMware endpoints.   |
| 10 | The final recovery step is updating the DNS records to route new requests to the secondary domain controller in AWS.   |

## AWS Reference Architecture