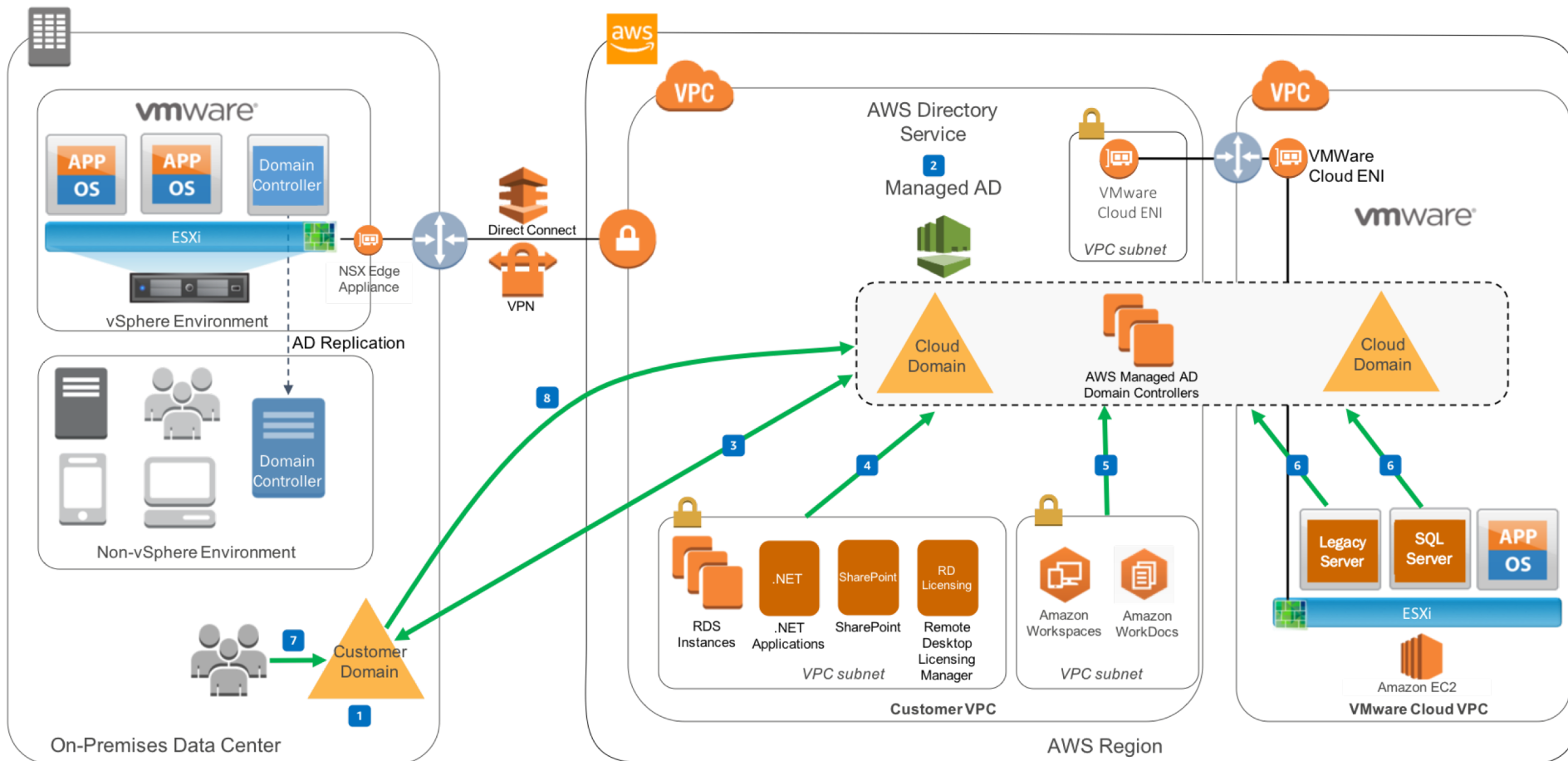


# Hybrid Active Directory Trusted Domains

## Using AWS Directory Service Managed AD

This architecture demonstrates AD Trusted Domains in which a *Customer Domain* is configured in a 1-way or 2-way trust relationship with *Cloud Domain*. Cloud Domain provides managed AD services for both Amazon Elastic Compute Cloud (Amazon EC2) instances and VMware Cloud on AWS VMs. Cloud Domain is provisioned through AWS Directory Service *Managed AD* to provide multiple domain controllers, high availability, automated patching, and automatic backups.



- | # | Description  |
|---|--|
| 1 | Customer Domain is deployed on-premises with Users, Computers, and Group Policy as the single source of identity.  |
| 2 | Customer Domain is provisioned as a separate domain on AWS with the AWS Managed Microsoft AD.  |
| 3 | Cloud Domain is configured in a 1-way or 2-way trust with Customer Domain enabling on-premises Users and AD Security Groups to access cloud instances and VMs. |
| 4 | AWS Instances are seamlessly domain-joined to the Cloud Domain at launch.  |
| 5 | AWS enterprise apps users are domain-joined to Cloud Domain.   |
| 6 | VMware Cloud VMs are domain-joined to Cloud Domain with access through VMC Compute Gateway Firewall Rules.   |
| 7 | Users are authenticated to Customer Domain through on-premises domain controllers.   |
| 8 | On-premises users access AWS or VMC resources through the 1-way or 2-way trust relationship and AD Global Security Group permissions.                          |



AWS Reference Architecture