

# VMware Cloud™ on AWS - Reference Architecture

## Horizon 7 on VMware Cloud™ on AWS

This reference architecture illustrates a minimal viable product to start Horizon 7 on VMware Cloud™ on AWS. This reference architecture shows all the components required for a hybrid cloud environment utilizing Horizon Cloud Pod Architecture.

- 1 On-Prem connectivity**  
IPsec VPN (preferably route-based) or Amazon Direct Connect between on-prem datacenter and VMC on AWS.
- 2 Firewall rules for vCenter Access.**
  - If On-Prem connectivity is configured, allow infrastructure on-prem subnets to access vCenter & ESXi for management.
- 3 On-Prem Firewall**  
Access from on-prem subnets to VMC Management segment (or at least vCenter and ESXi).  
Access from VMC vCenter to on-prem infrastructure services (Active Directory, DNS, Content Library, ...)  
Access from VMC DMZ to virtual desktops hosted on-premises
- 4 Routed Network Segments**  
One Infrastructure segment with privileged access to Management component (vCenter, NSX, ...)  
Multiple workload segments including:
  - Segment for Horizon infrastructure
  - Segment for Virtual Desktops or RDSH Servers
  - Two DMZ Segments
- 5 Firewall rules for Network segments**
  - Allow connectivity between Infra & Management
  - Allow connectivity between Infra & on-prem infrastructure subnet
  - Allow connectivity between workload segment, AWS VPC Subnets and on-prem application subnets
  - For Horizon Specific requirements, see the Horizon network ports diagram at <https://techzone.vmware.com/resource/network-ports-vmware-horizon-7>
- 6 DMZ**  
Horizon utilizes the Unified Access Gateway for remote access. This appliance can support 1, 2, or 3 network interfaces. A two NIC deployment is recommended.  
Two DMZ are needed for a two NIC deployment
  - One external-facing DMZ that will be exposed to the Internet via NAT
  - One internal-facing DMZ that will connect to Horizon resources in VMC or on-premises
- 7 Virtual Desktops and Published Apps**  
These are the subnets that Horizon virtual desktops and Published Apps Servers will be deployed into.
- 8 VPC connectivity**  
This will allow to create hybrid applications leveraging Cloud-Native Services and traditional Virtual Machines
  - Allow access from/to VPC subnets and Workload segments in the Compute Gateway and through Security Groups.
  - Utilize services like RDS for Horizon and App Volumes databases in place of virtual machines
- 9 Horizon Cloud Service**  
Horizon Cloud Service is a cloud-based management plane for Horizon 7 environments. It can manage on-premises and cloud-based Horizon 7 environments and provides licensing, desktop brokering, and monitoring services from the cloud.

