USDC TECHNOLOGY
Smart Data Center

VMware Horizon Introduction

Cuong Le Sy

vmware®

What’s in This Session for You?

Knowledge

Demonstrate the value of Horizon solutions

Expand adoption

Solve use cases - blueprints

Take all the products and design for use cases

Reference Architecture

Lots of pretty pictures

Understand design guidance and what is involved

- Architectural principles and how to design components
- Scaling, availability, multi-site, etc

Lots of tips and tricks - use as a reference

Links to relevant documentation sections

Agenda

Overview and Approach

Horizon 7

Unifed Access Gateway

App Volumes

User Environment Manager

Integration

Reference Architecture

Objective and Methodology

Framework intended to provide guidance on how to architect and deploy Workspace ONE and Horizon solutions

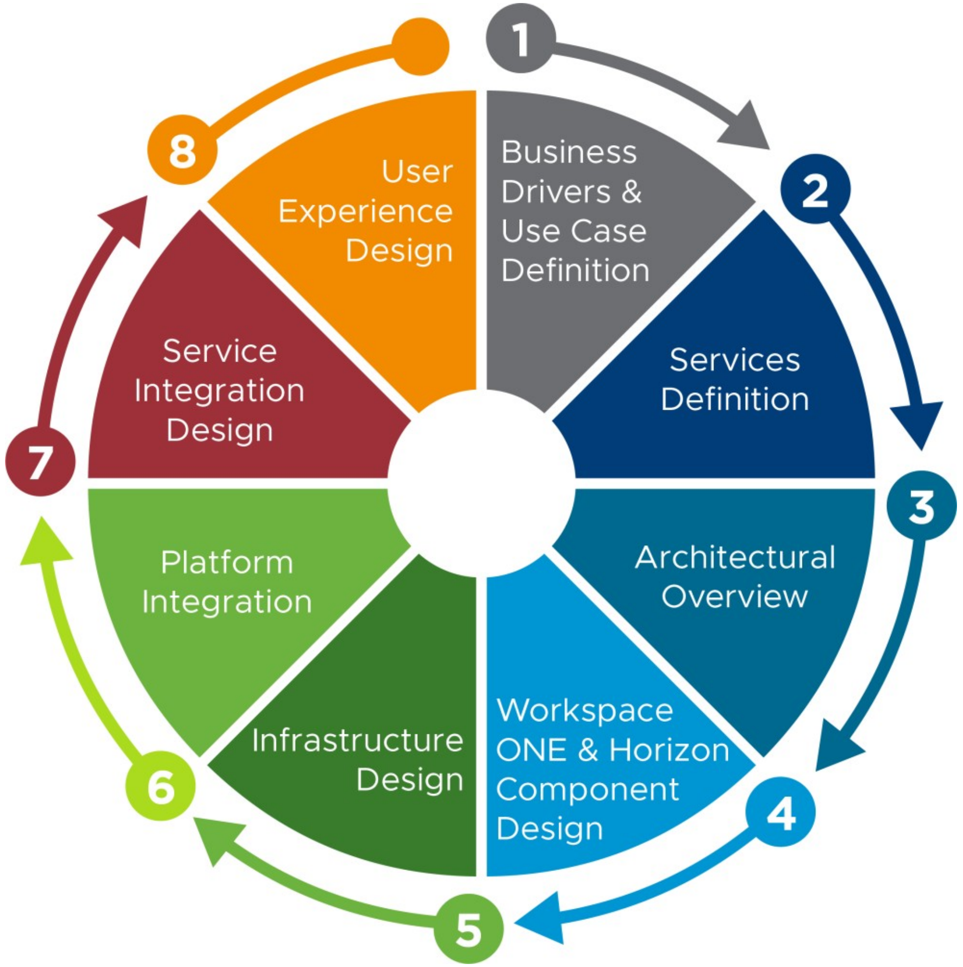
Gives an example architecture for deploying all products in an integrated manner

Focus

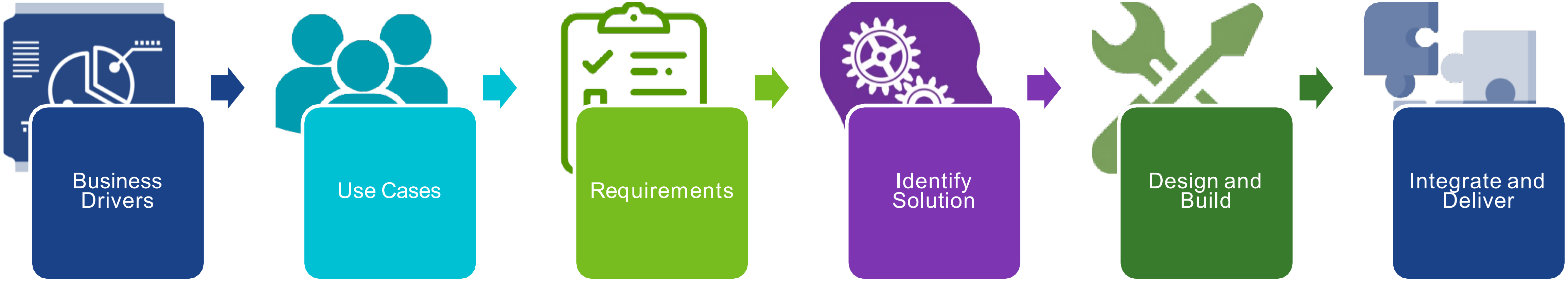
- Document design for the deployment, highlighting integration points
- Deploy all components as a customer would
- Test and validate key features

Scale and sizing

- Provide design methodology for scaling and sizing recommendations
- Does not validate load, scale or performance of components or hardware



Solving Business Drivers and Identifying a Solution



Business Drivers → Use Cases → Requirements → Identify Solution → Design and Build → Integrate and Deliver

Horizon Service Blueprints

Customize and combine asrequired

Horizon Service

Published Application

GPU-Accelerated Application

Desktop

Desktop with User Installed Applications

GPU-Accelerated Desktop

Linux Desktop

+

Recovery Service

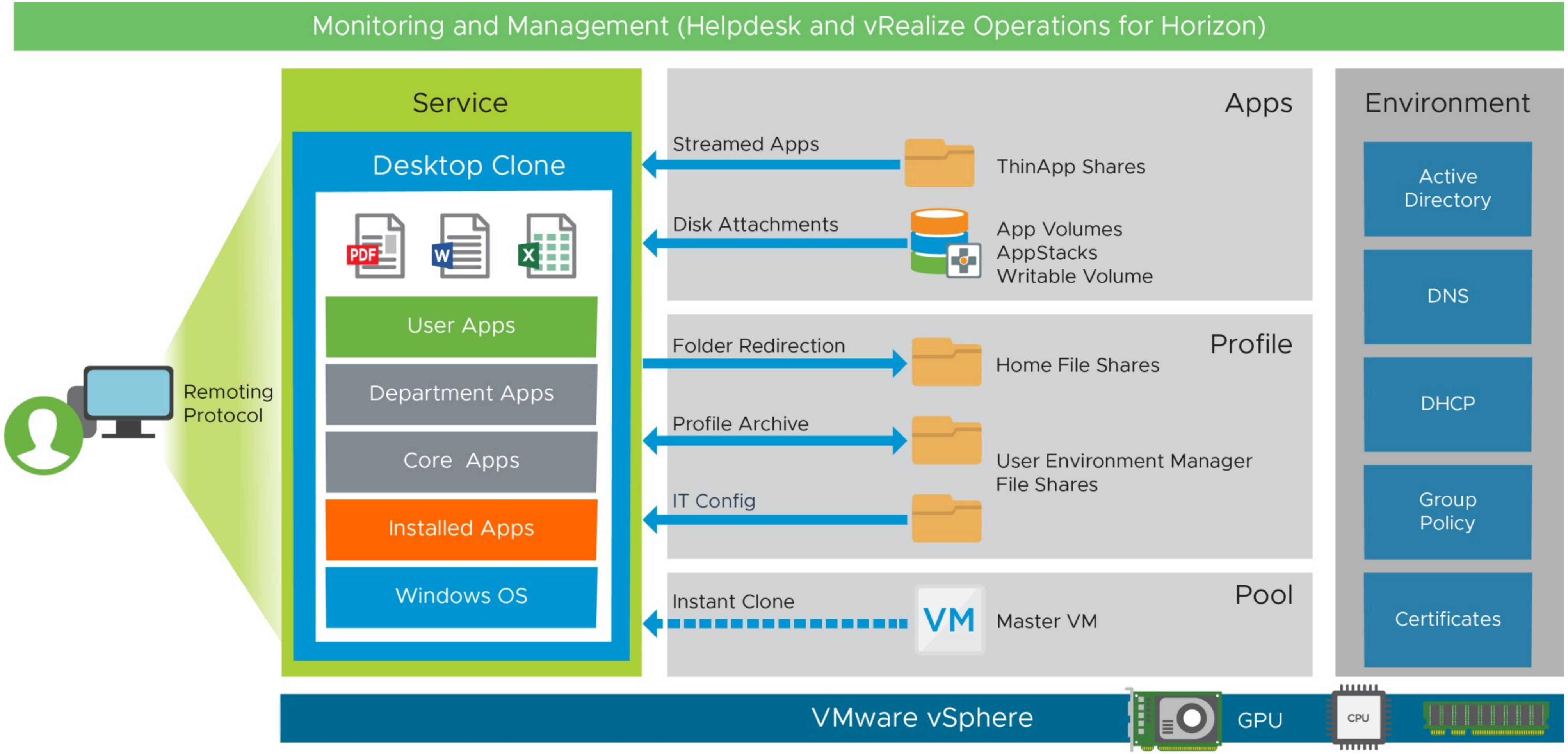
Horizon 7 Active/Passive Recovery

Horizon 7 Active/Active Recovery

Horizon Cloud Service Active/Passive Recovery

Service Blueprint Sample

GPU-Accelerated Desktop



Monitoring and Management (Helpdesk and vRealize Operations for Horizon)

Remoting Protocol

Service

Desktop Clone

User Apps

Department Apps

Core Apps

Installed Apps

Windows OS

Apps

Streamed Apps

ThinApp Shares

Disk Attachments

App Volumes AppStacks Writable Volume

Profile

Folder Redirection

Home File Shares

Profile Archive

User Environment Manager File Shares

IT Config

Pool

Instant Clone

Master VM

Environment

Active Directory

DNS

DHCP

Group Policy

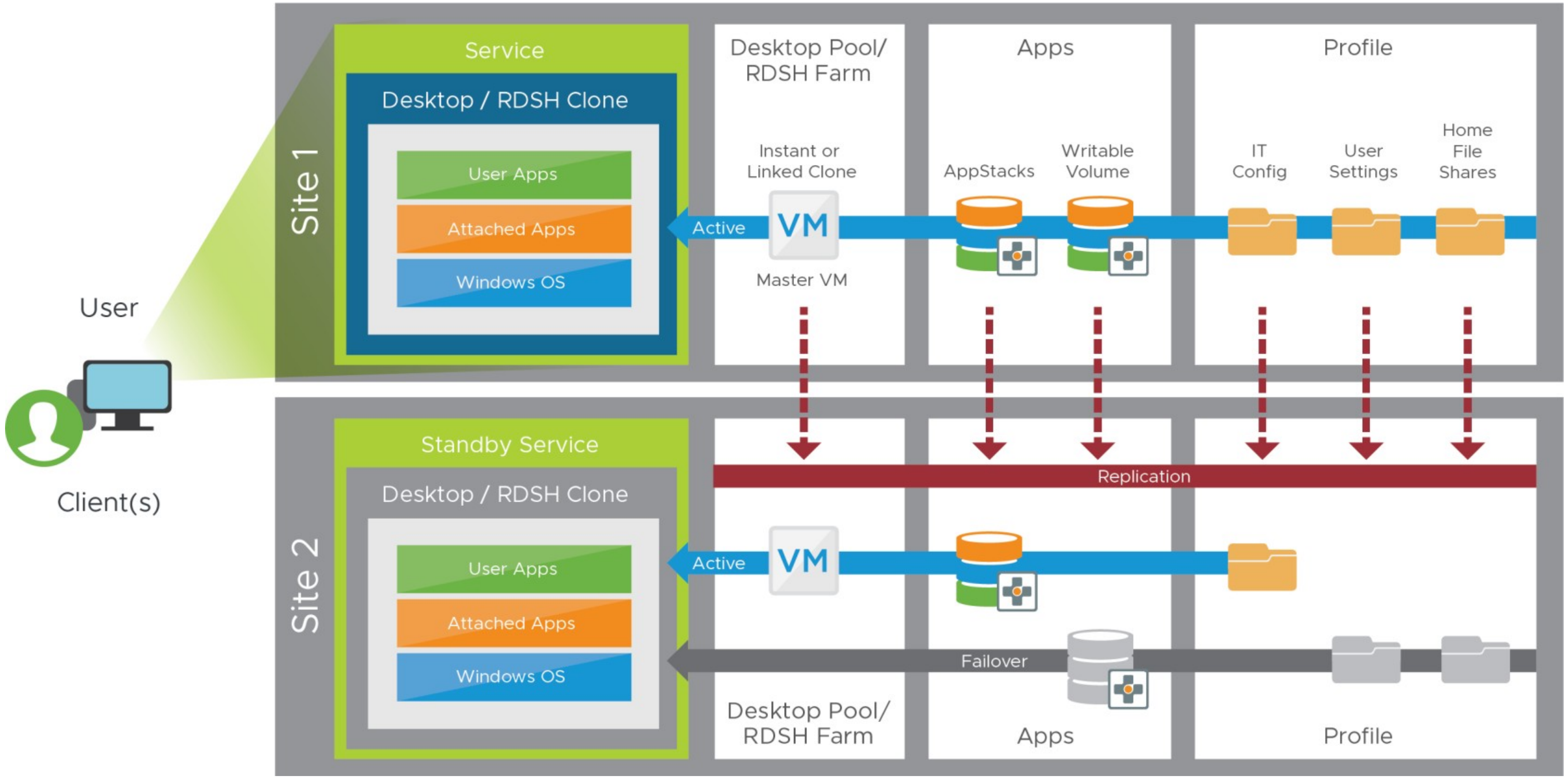
Certificates

VMware vSphere

GPU

Recovery Service Blueprint Sample

Active/Passive Horizon 7



Component Design

Architecting VMware products

Design Considerations

The “Empty” Desktop

Talk User Experience –
NOT Desktop

RTO / RPO

Huge impact to design

User Placement

User <> Datacenter alignment
And initial placement.

Pick a Site

Non Multi-Master
One site has to be “primary”

Non-VMware Software

SQL Cluster / AlwaysOn
Business Critical Apps
Other dependencies

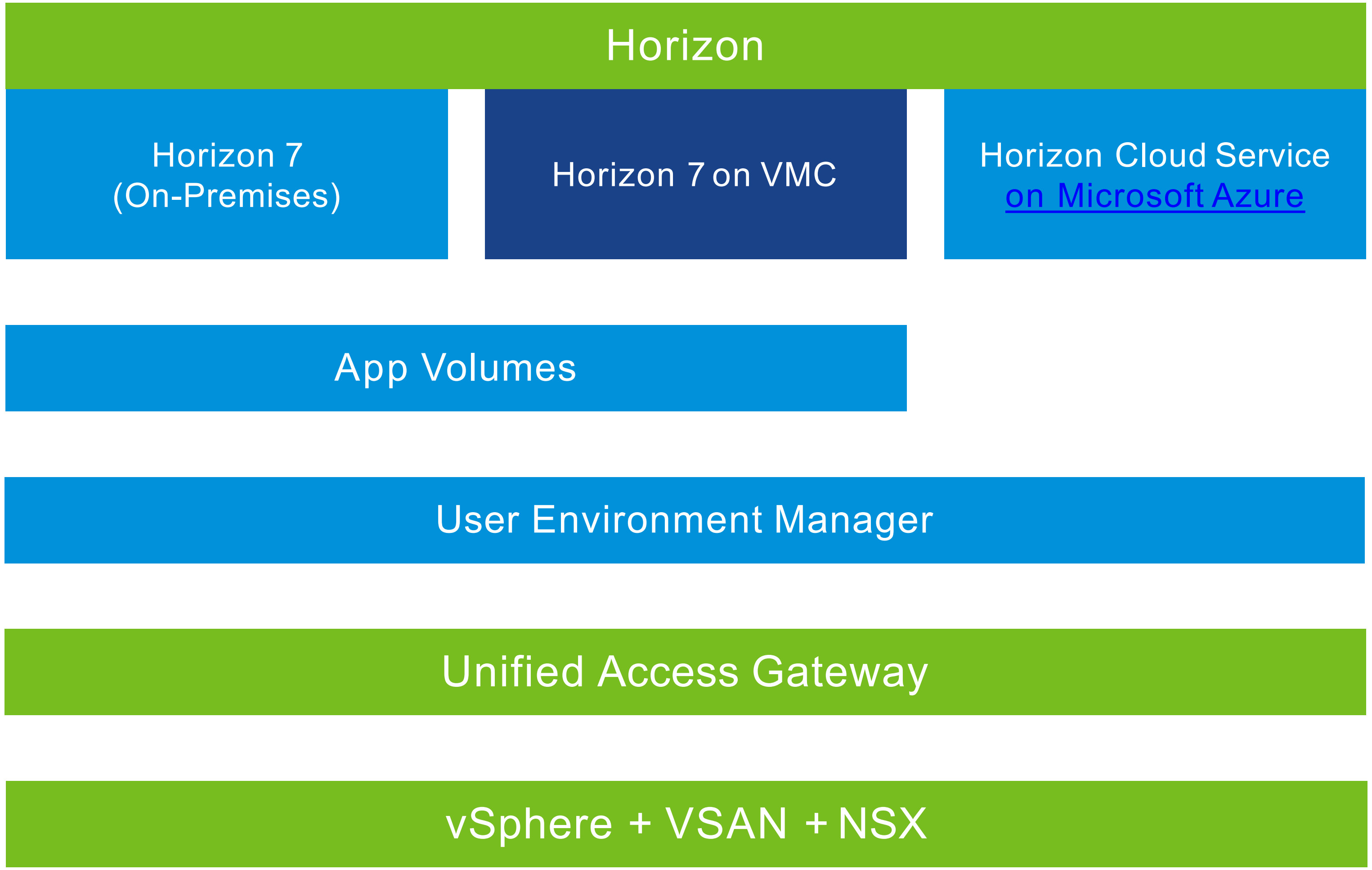
Design of Solution Components

Not an exhaustive list

Considerations

- On-premises or Cloud
- Version
- Scalability
- Availability
- Disaster recovery
  - (multi-site)
- Replication
- Load balancing
- Database
- Authentication
- Networking
- Storage
- VM build and OS choice

List design decisions



Horizon

Horizon 7 (On-Premises)

Horizon 7 on VMC

Horizon Cloud Service on Microsoft Azure

App Volumes

User Environment Manager

Unified Access Gateway

vSphere + VSAN + NSX

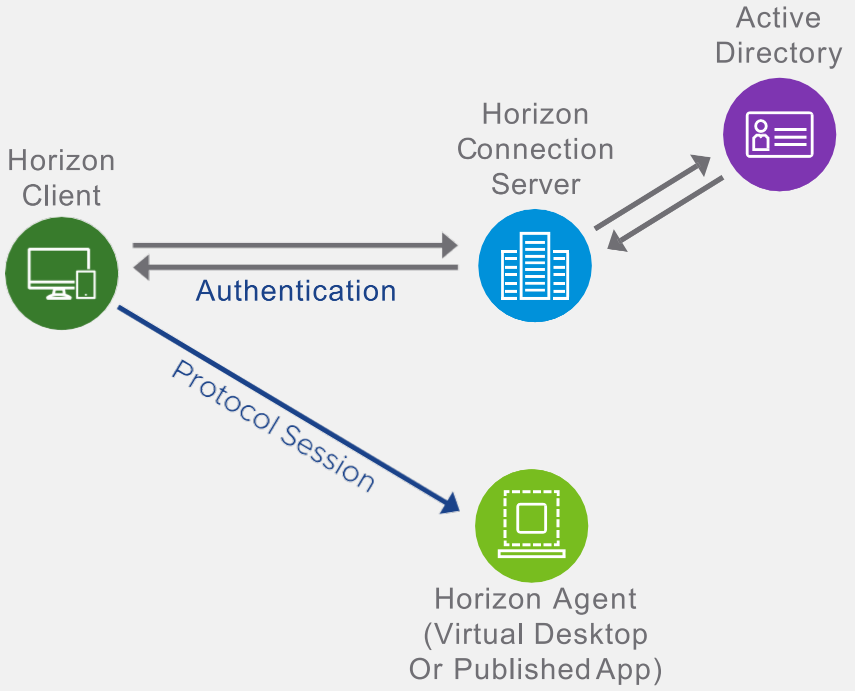
Horizon 7

Architecture and design

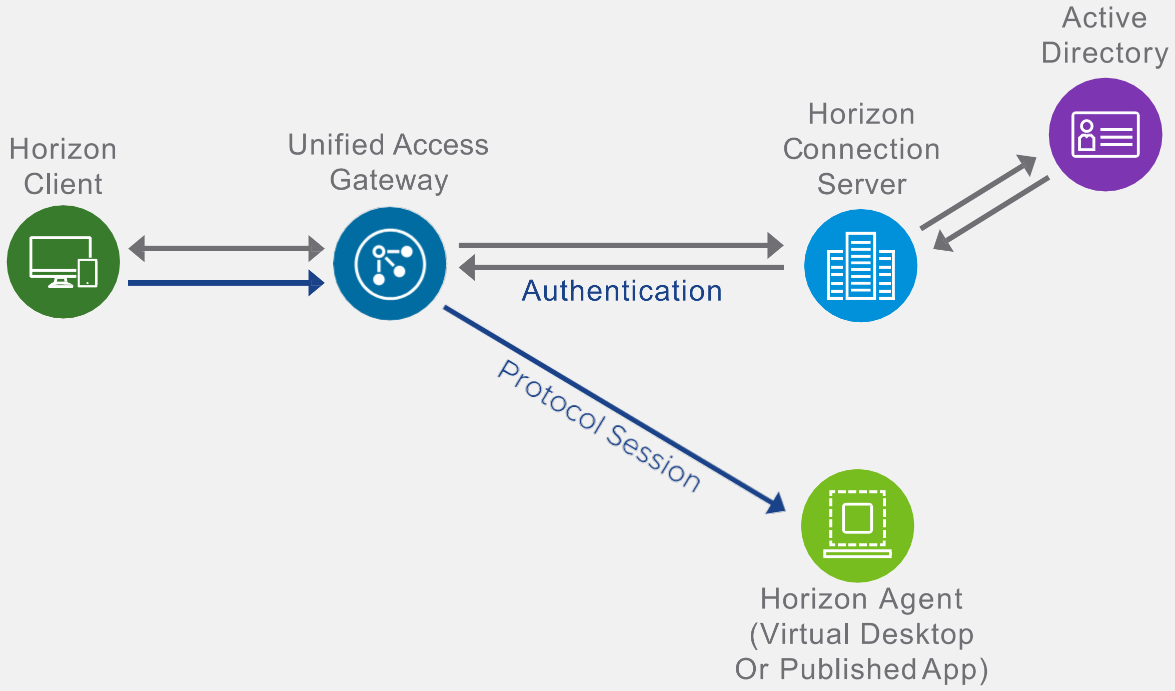
Horizon Core Components – Logical View

https://techzone.vmware.com/blog/understanding-horizon-connections

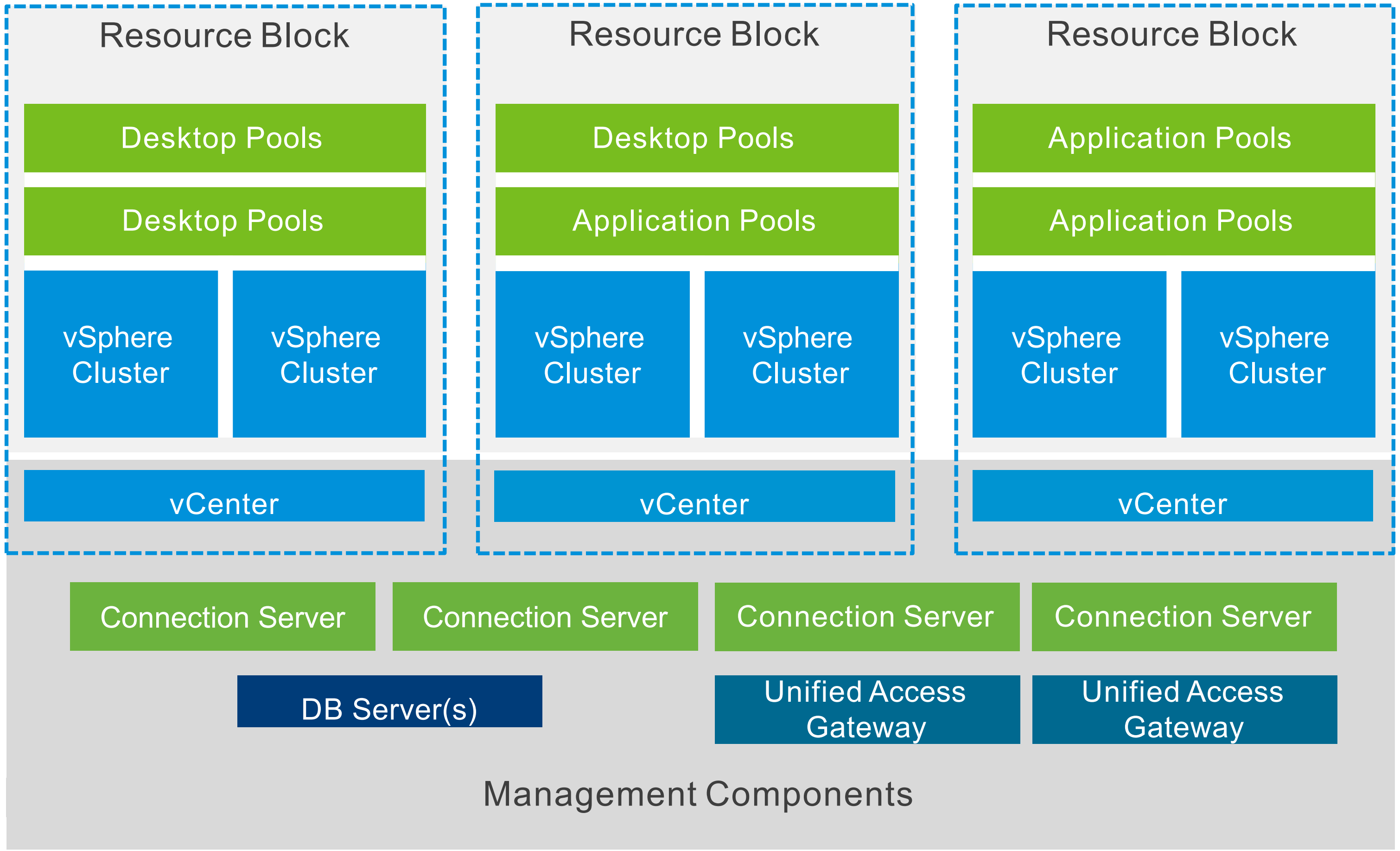
Internal Connection


Active Directory
Horizon Connection Server
Horizon Client
Authentication
Protocol Session
Horizon Agent (Virtual Desktop Or Published App)

External Connection



Horizon 7 Pod and Block Design



Sizing Best Practice

https://kb.vmware.com/s/article/2150348

Block

Bound by the vCenter Server

- Number of virtual machines

The number depends on the type used:

8,000 instant-clone VMs

4,000 linked-clone or full-clone VMs

Pod

Bound by the Connection Servers.

- Number of total connections

Each Connection Server = 2,000 connections

Max 7 Connection Servers per Pod.

- All Connection Servers active
- Require N+1

10,000 per Pod best practice

Cloud Pod Architecture

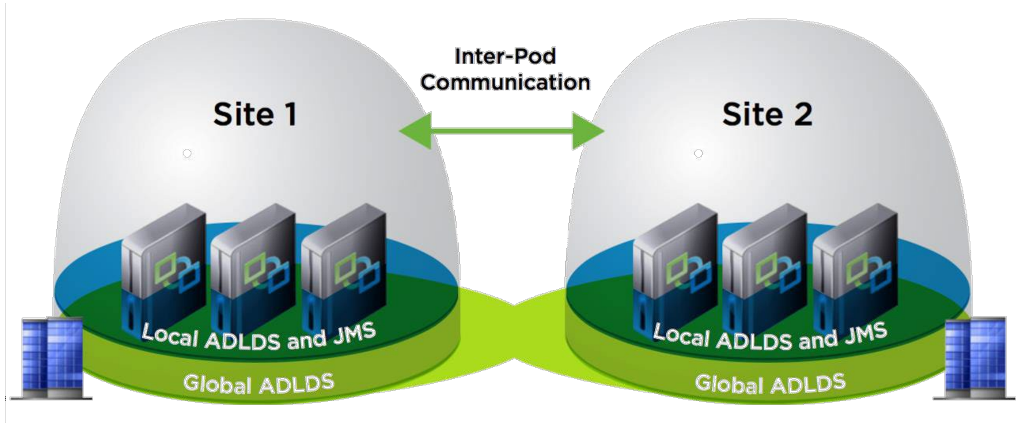
CPA

Makes Horizon 7 truly scalable

Joins multiple View pods together into a ***federation***

Able to be deployed across multiple locations/sites

Can also be pods from the same site



Concepts

Global entitlement (GE).

- Entitle users and groups
- Can contain desktop pools or RDSH-published applications
- From multiple different View pods

Home Site

- Global – Assigned to user or group
- Per-global entitlement (home site override)

Scope Policy

- Search local Pod, site, or any

Multi-site Design

Each site has separate Horizon Pods

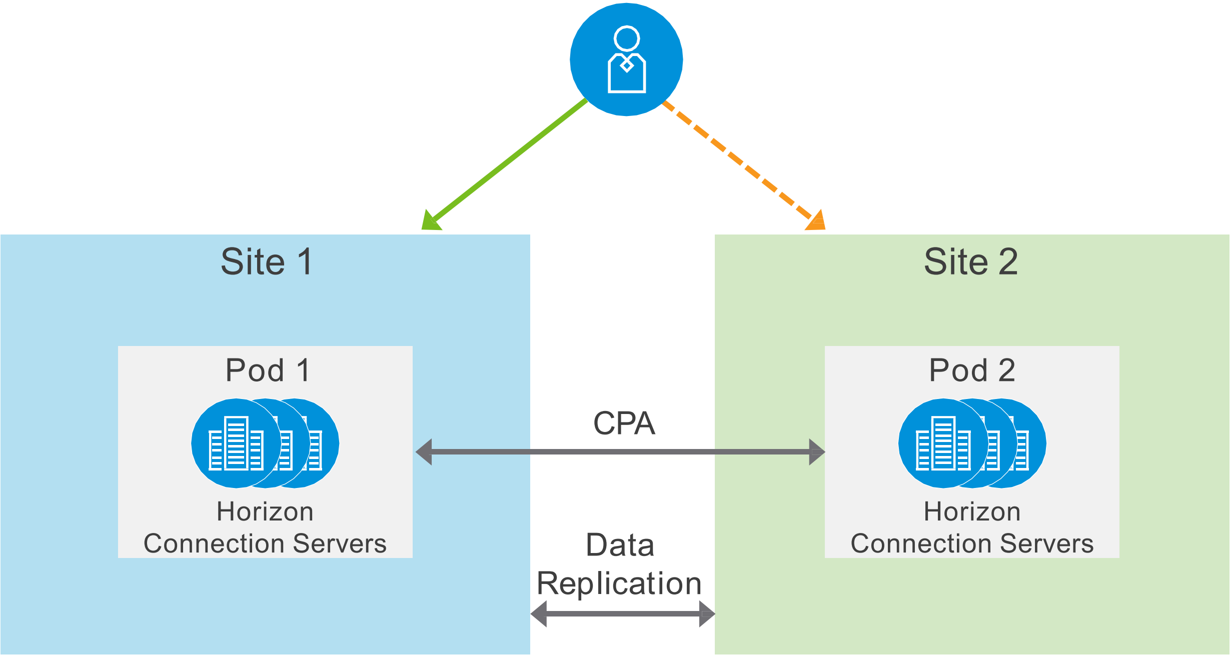
Each pod has own set of Horizon Connection Servers

Pods are federated with CPA

User can consume resources:

- Active/passive - from primary site
- Active/active - from either site

Data replication is usually a big consideration



vSAN Stretched Cluster

Connection Servers:

- One common set
- All pinned to the same site

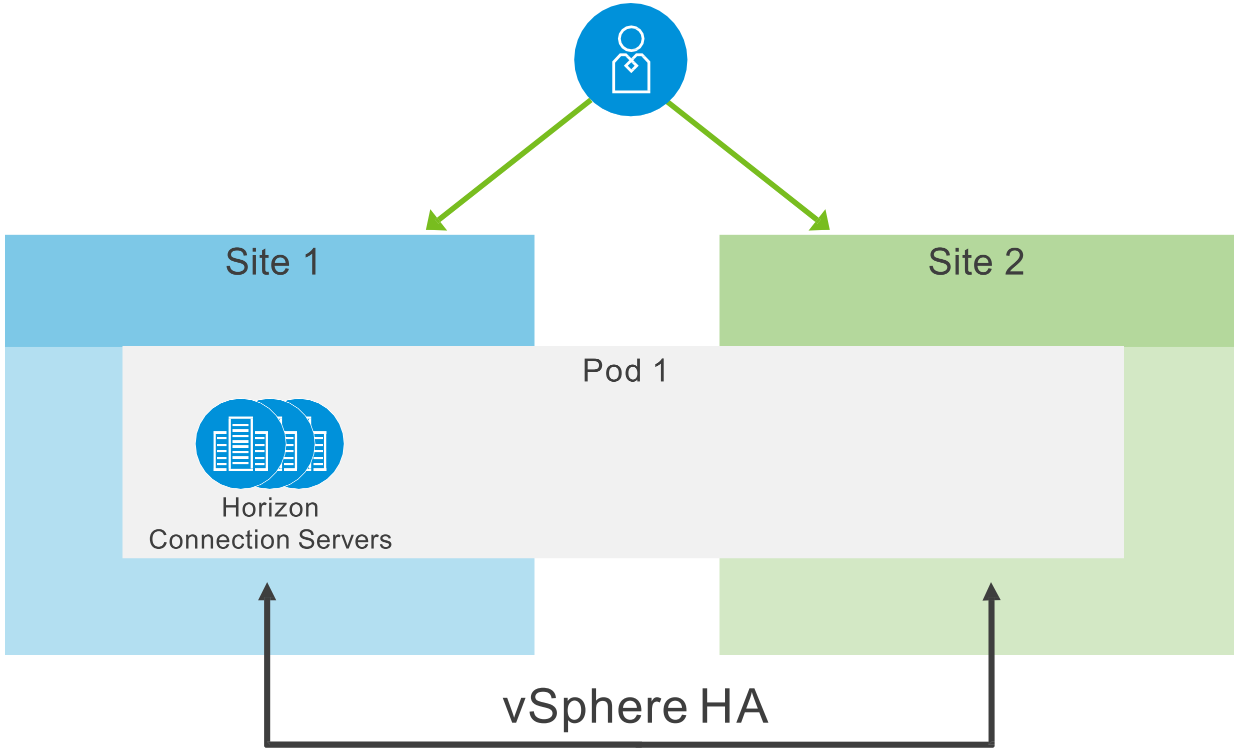
Must failover together

Control with

- vSphere HA
- vSphere Host/ VM Groups
  - Group Hosts by Site
  - Group Connection Servers
- vSphere Host/ VM Rules
  - Pin VM group to Host Group

Target Use Cases

- Full clones & persistent desktops



Unified Access Gateway

Architecture and design

vmware

USDC TECHNOLOGY
Smart Data Center

Unified Access Gateway

Providing external access for Horizon 7

Unified Access Gateway

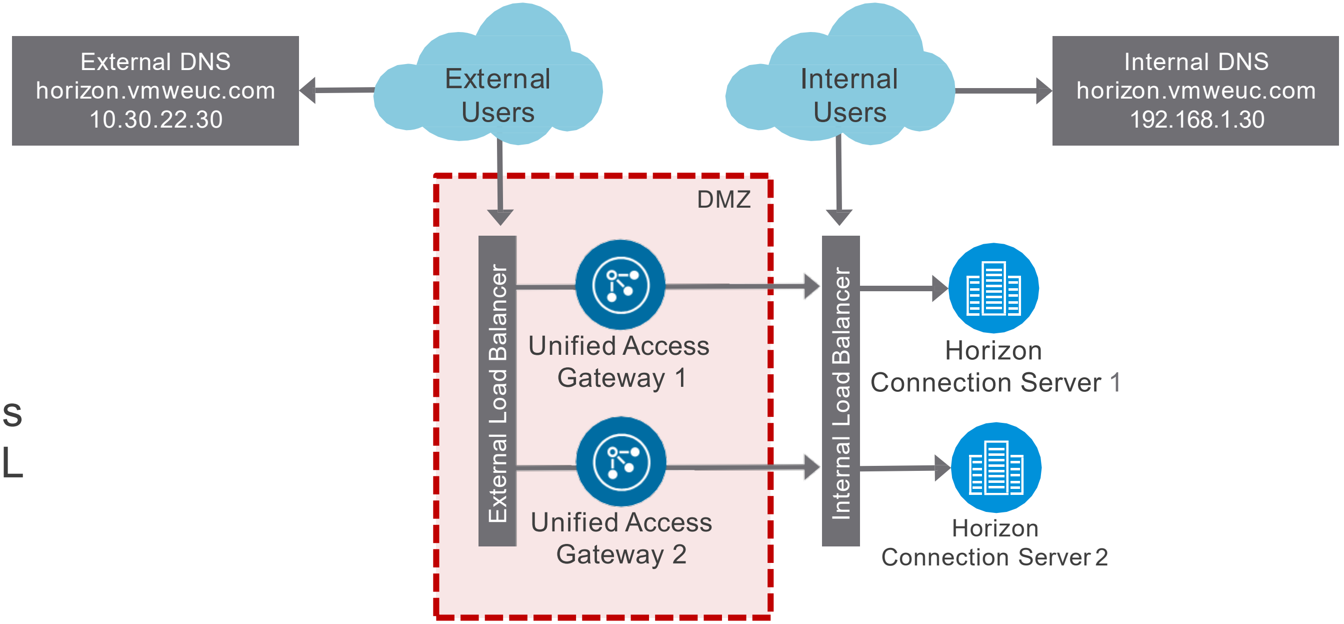
- No 1-1 mapping with Horizon Connection Servers
- Same Connection Server can handle internal and external connections
- Scale separately
- Allows DMZ Authentication.
  - Smartcard, Cert, RSA SecurID, RADIUS, SAML

Load Balancing

- Only the initial XML API connection is load-balanced
  - Authentication, authorization, and session management
- Protocol connects directly to the Unified Access Gateway appliance that brokered the initial XML API connection
  - Blast Extreme, PCoIP, or RDP connections

Split DNS is optional

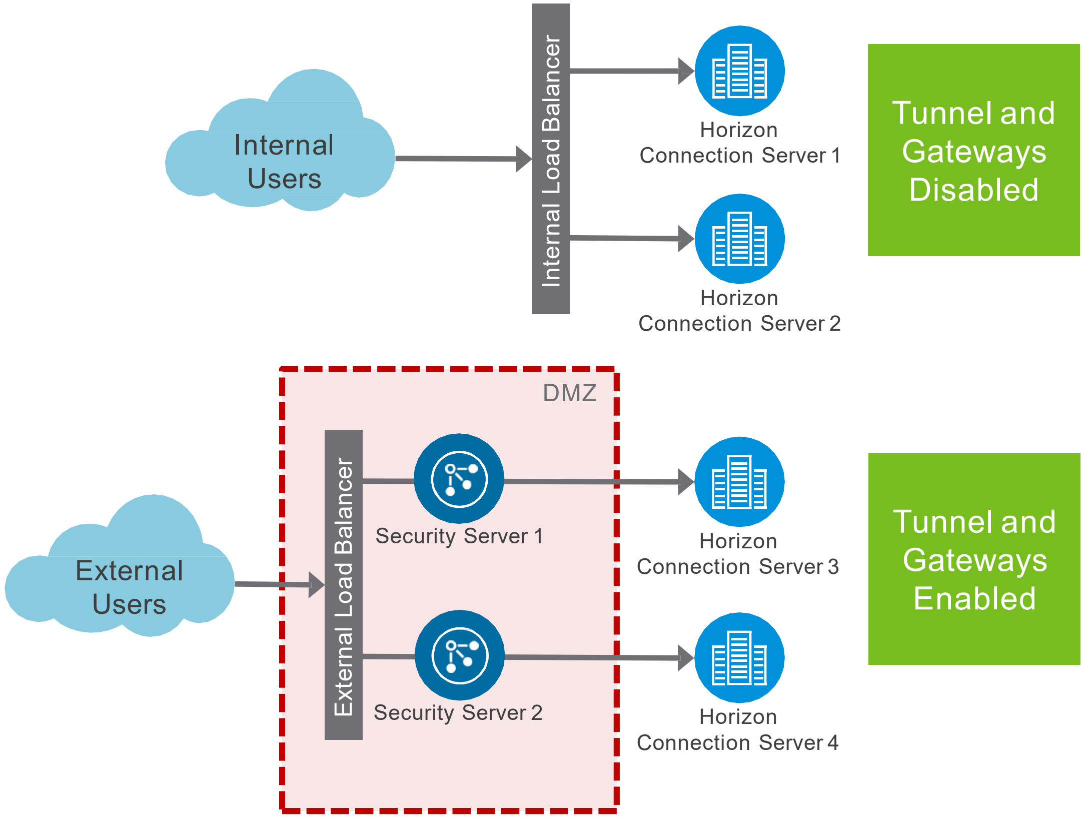
- E.g. when resolving horizon.vmweuc,com
  - External clients get 10.30.22.30
  - All internal components and clients use 192.168.1.30



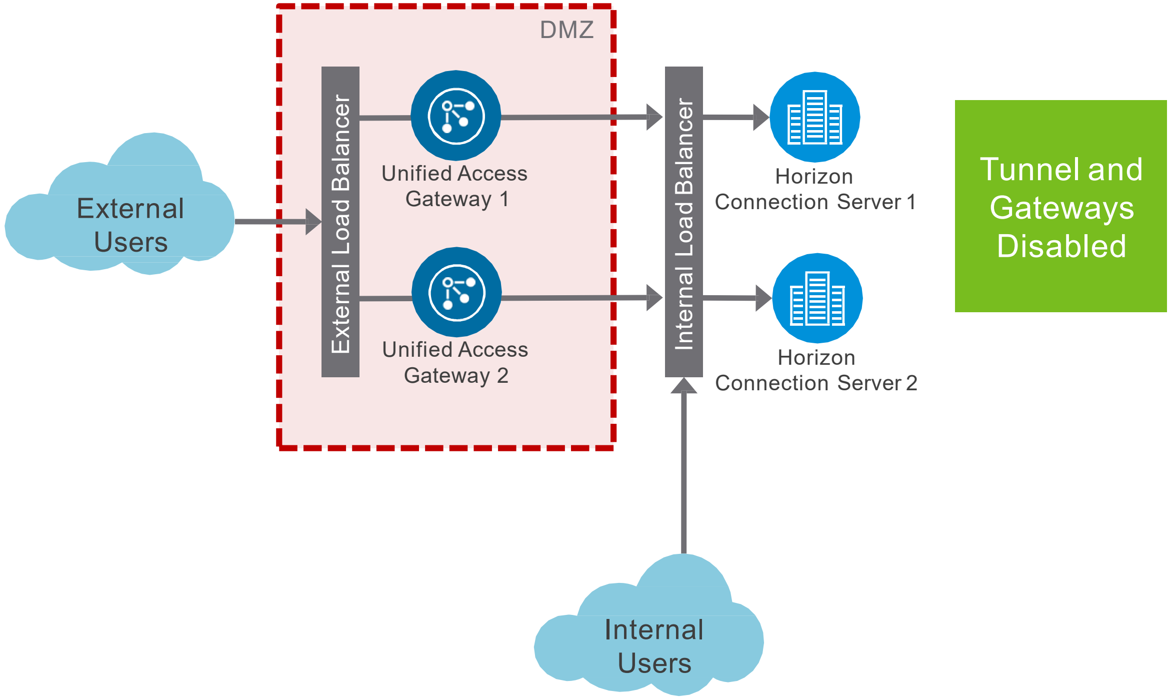
Architectural Comparison

Security Server vs. Unified Access Gateway

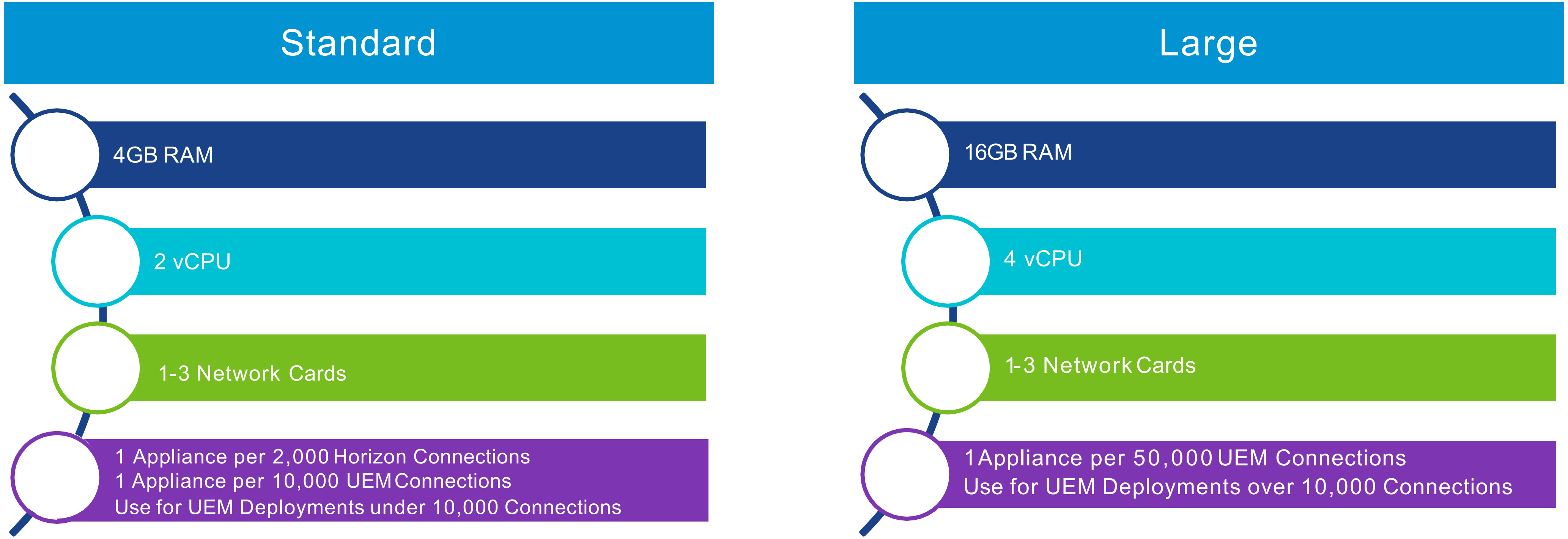
With Security Server


Internal Users
Internal Load Balancer
Horizon Connection Server 1
Horizon Connection Server 2
Tunnel and Gateways Disabled
DMZ
External Users
External Load Balancer
Security Server 1
Security Server 2
Horizon Connection Server 3
Horizon Connection Server 4
Tunnel and Gateways Enabled

With Unified Access Gateway



Standard and Large UAG Sizes



Standard

- 4GB RAM
- 2 vCPU
- 1-3 Network Cards
- 1 Appliance per 2,000 Horizon Connections
  1 Appliance per 10,000 UEM Connections
  Use for UEM Deployments under 10,000 Connections

Large

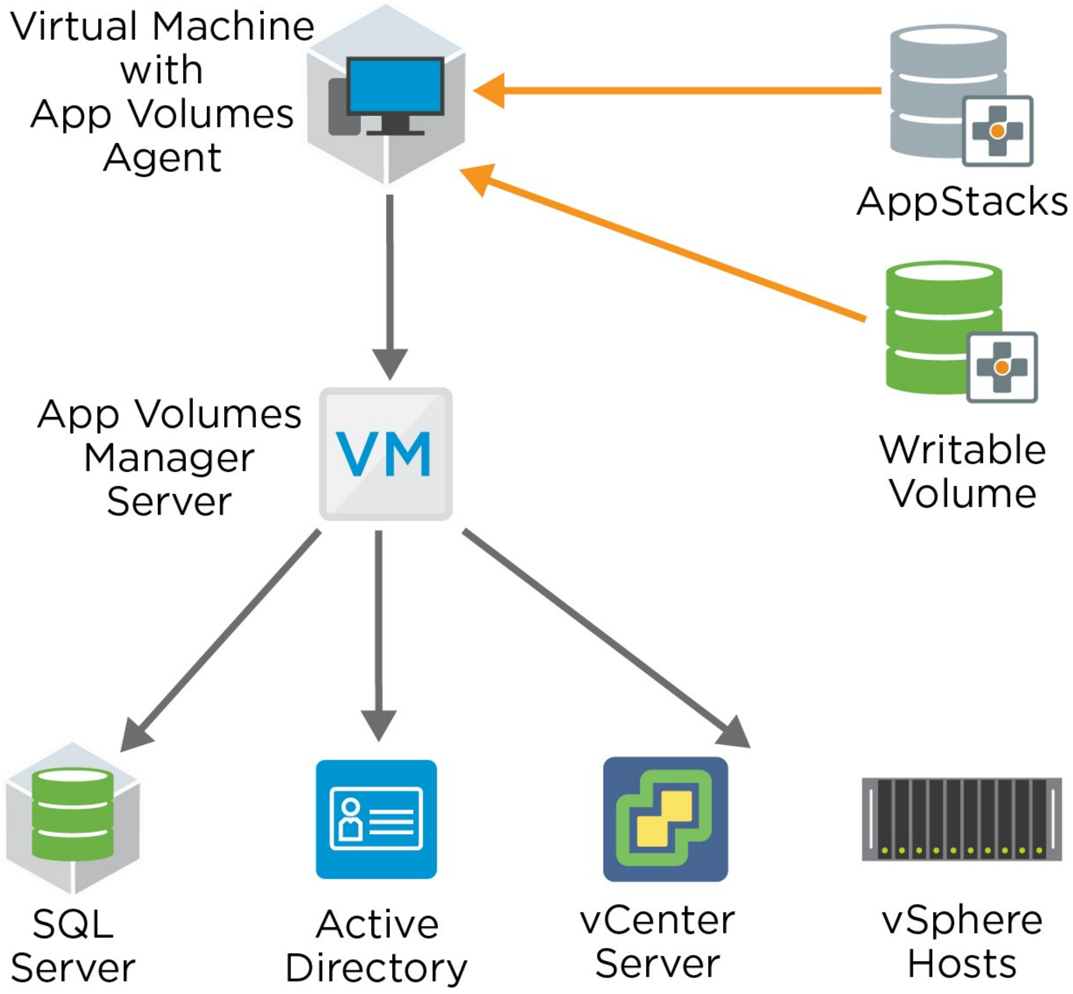
- 16GB RAM
- 4 vCPU
- 1-3 Network Cards
- 1 Appliance per 50,000 UEM Connections
  Use for UEM Deployments over 10,000 Connections

App Volumes

Architecture and design for Horizon 7

App Volumes Logical Architecture

Horizon 7 (not Horizon Cloud)



App Volumes Sizing Limits and Recommendations

https://kb.vmware.com/s/article/67354

Each AVM has been tested for

- 2,000 concurrent logins
- One per second login rate

Concurrent logins determines:

Number of AVM

- And CPU and memory

Size of block

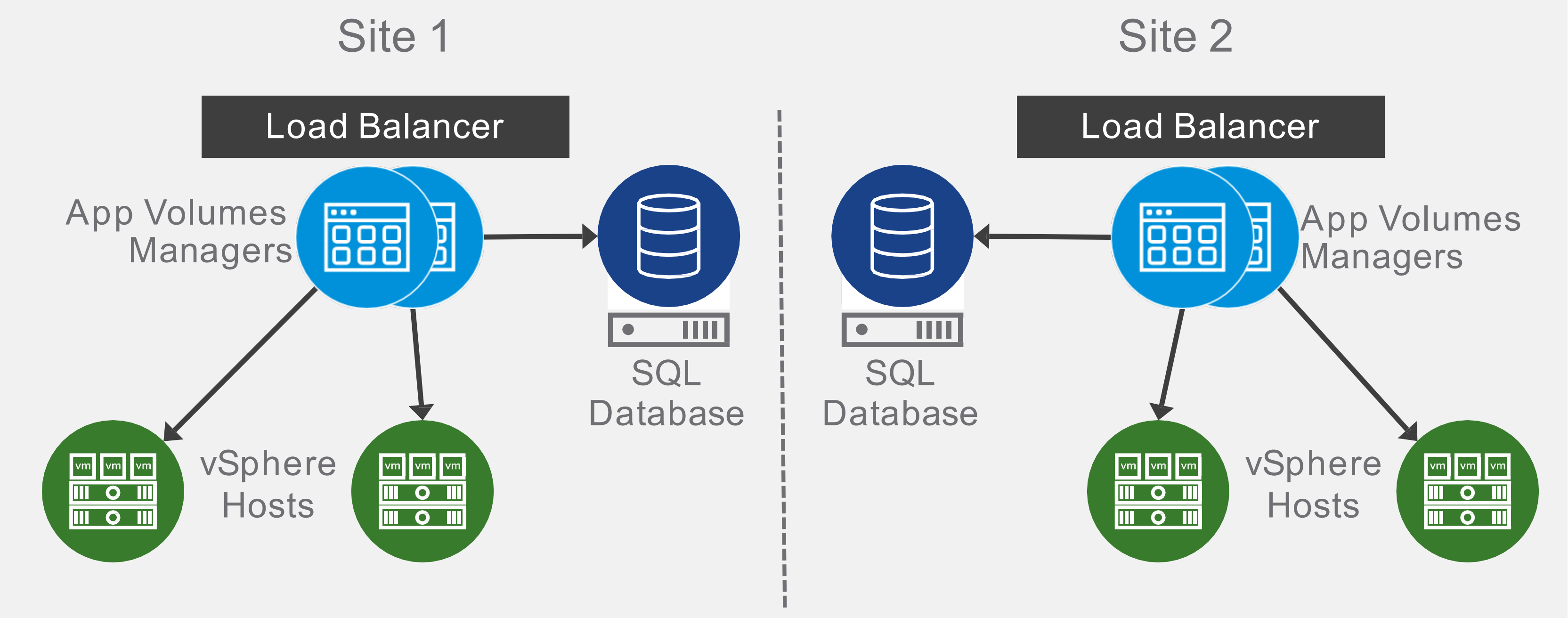
- Number of VMs per vCenter Server

Concurrent Logins	<=2000	2001 to 5000	5,001 to 7,500	>7,500
AVMs per Pod	2	3	4	4+1 for every 2,500 users
CPU per AVM	4	6	8	8
Memory per AVM	4 GB	8 GB	16 GB	16 GB
vCenters per Pod	2	3	4	4+1 for every 2,000 VMs
Logins per second (tested)	2/sec	3/sec	4/sec	4/sec+1 for each AVM

For deployments with 5,000 or more users, consider tuning App Volumes background jobs timing values for optimal performance

Multi-site Architecture

Separate Instances and Databases Option



AppStack Entitlements will need to reproduced in the other site

https://blogs.vmware.com/euc/2017/07/app-volumes-automated-entitlement-replication.html

Separate deployments of App Volumes

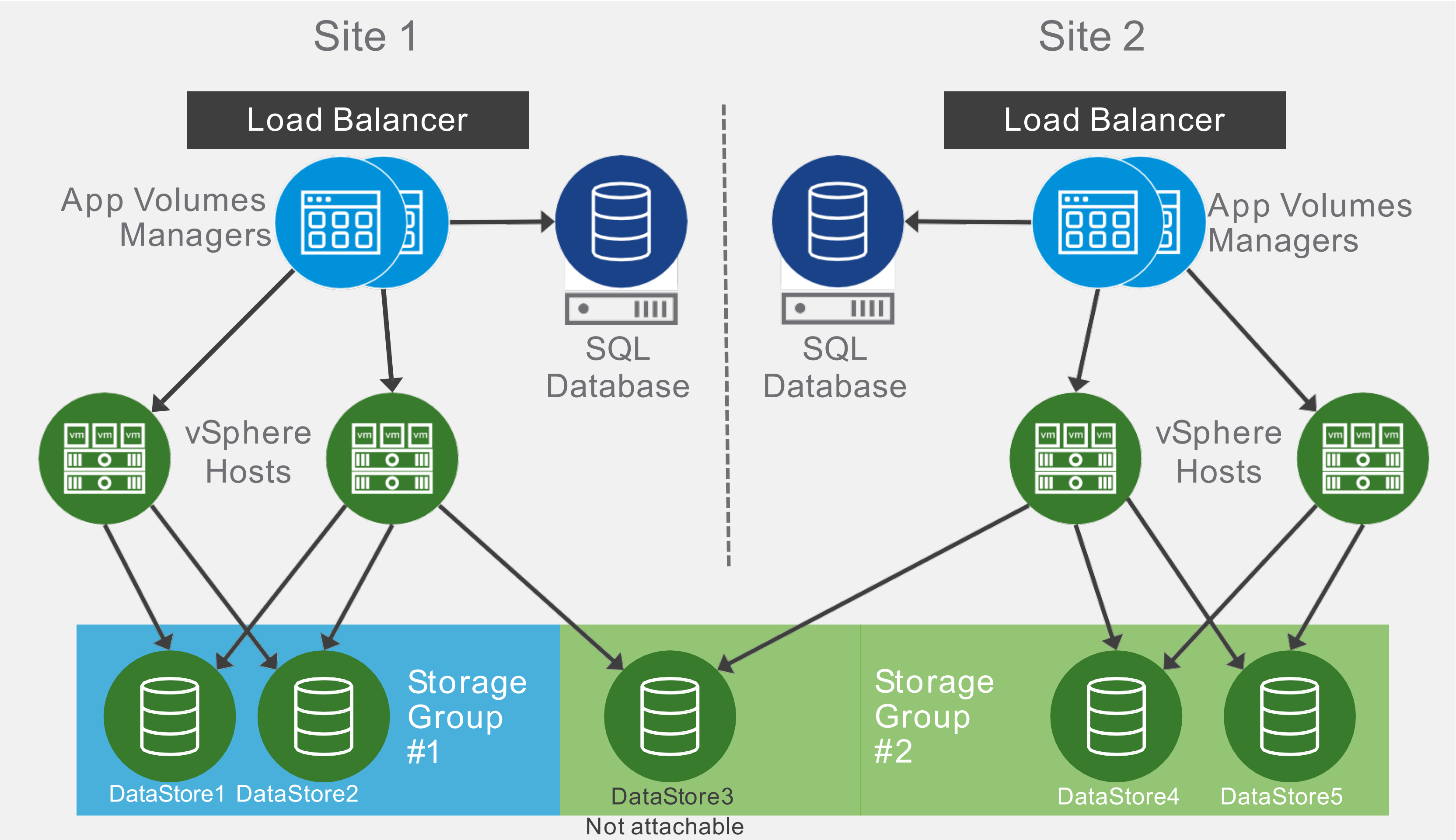
- An App Volumes instance is defined by the database
- Each site has multiple Managers

Each site has a separate database

- No DB replication between sites

Can expand for more than 2 sites

AppStack Replication



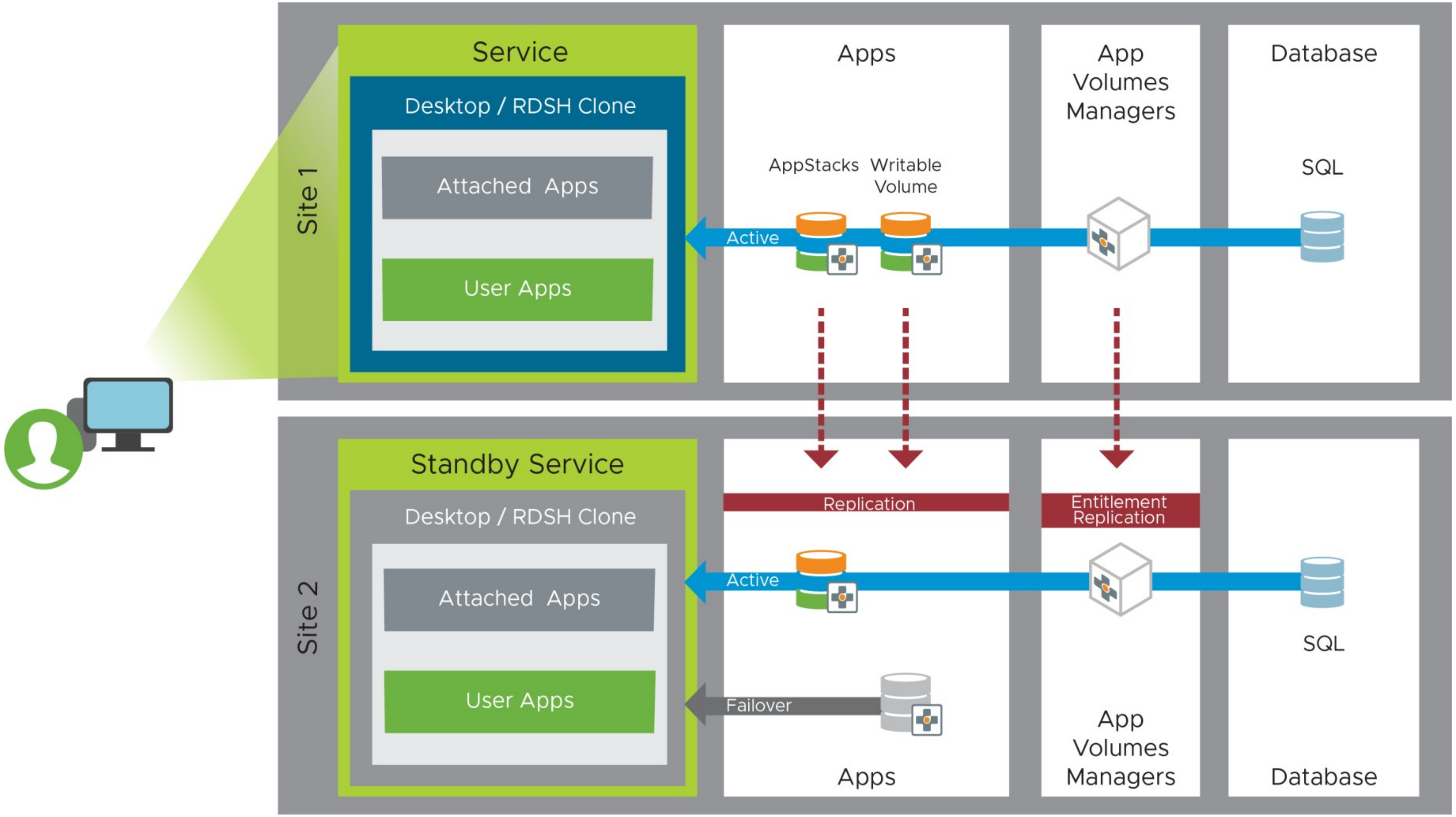
Storage Groups replicate AppStacks

1overlapping Datastore marked as non-attachable

Replication across sites when Datastore is visible by one or more vSphere hosts in both sites

Could manually export and import AppStacks from one site to the other

App Volumes Multi-Site Service



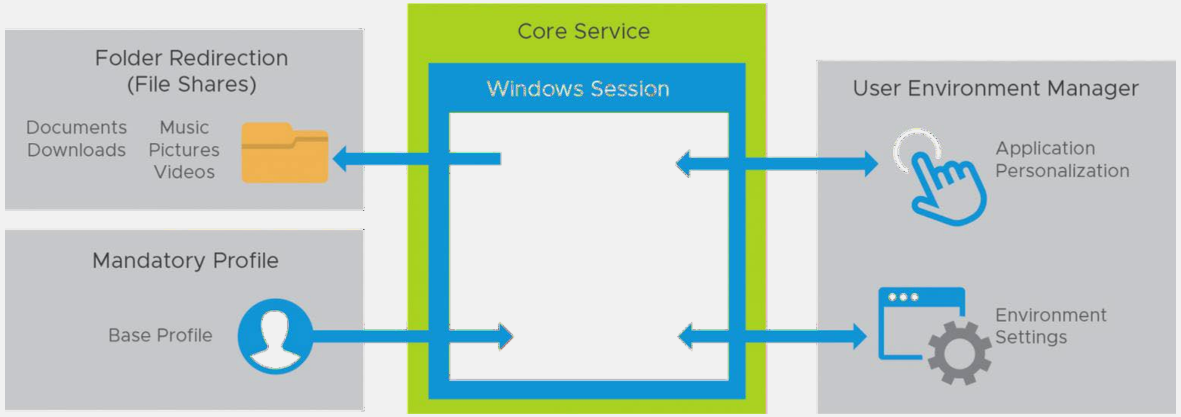
User Environment Manager

Architecture and design

User Environment Manager

Approach and infrastructure

User Profile Strategy

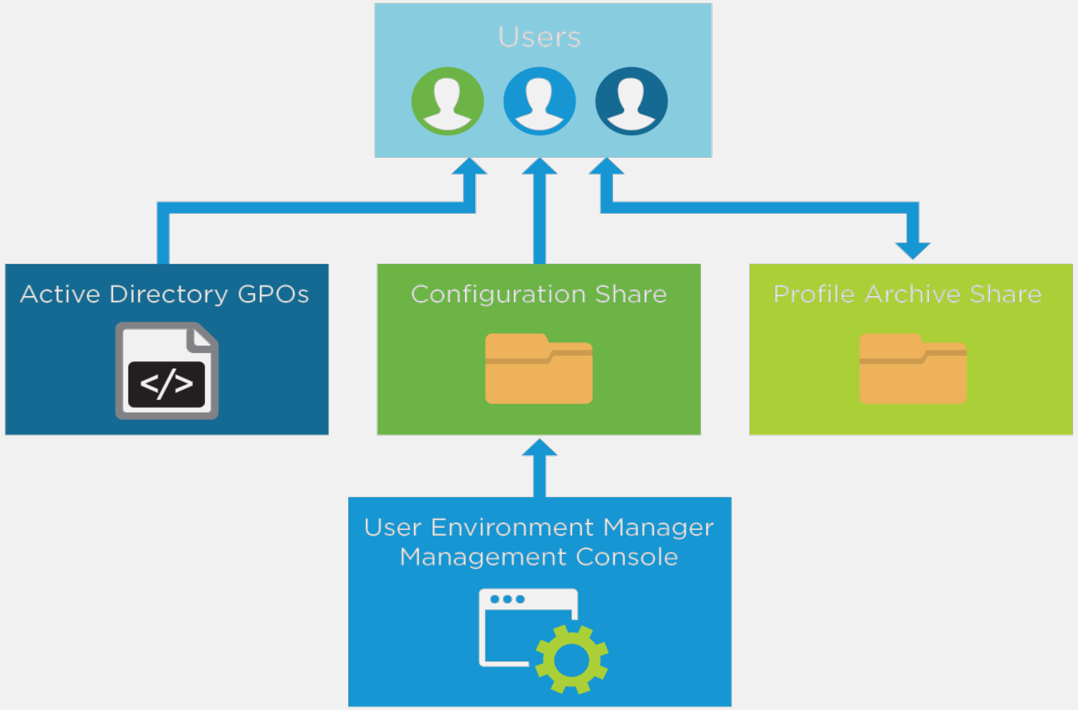


Folder Redirection

Abstract user data from the guest OS

Mandatory Profiles - Blog and How-To

Infrastructure



Profile Archive Share

Replication and availability

User can read and write

Profile data is sensitive to conflicts

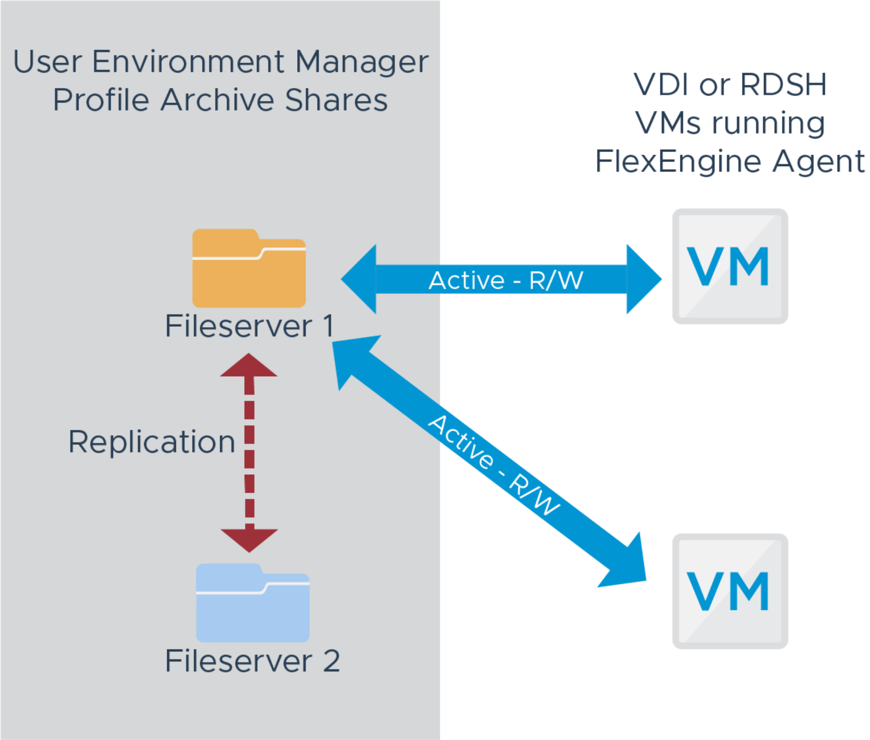
- See support statement and blog from Microsoft

DFS-R does not have conflict resolution

- DFS-Replication in an Active-Active setup is not supported

Setup DFS-R, and disable the referral to the replicated DFS-N Folder Target(s)

- That way active-passive replication topology is created



IT Configuration Share

Replication and availability

Only admins make changes

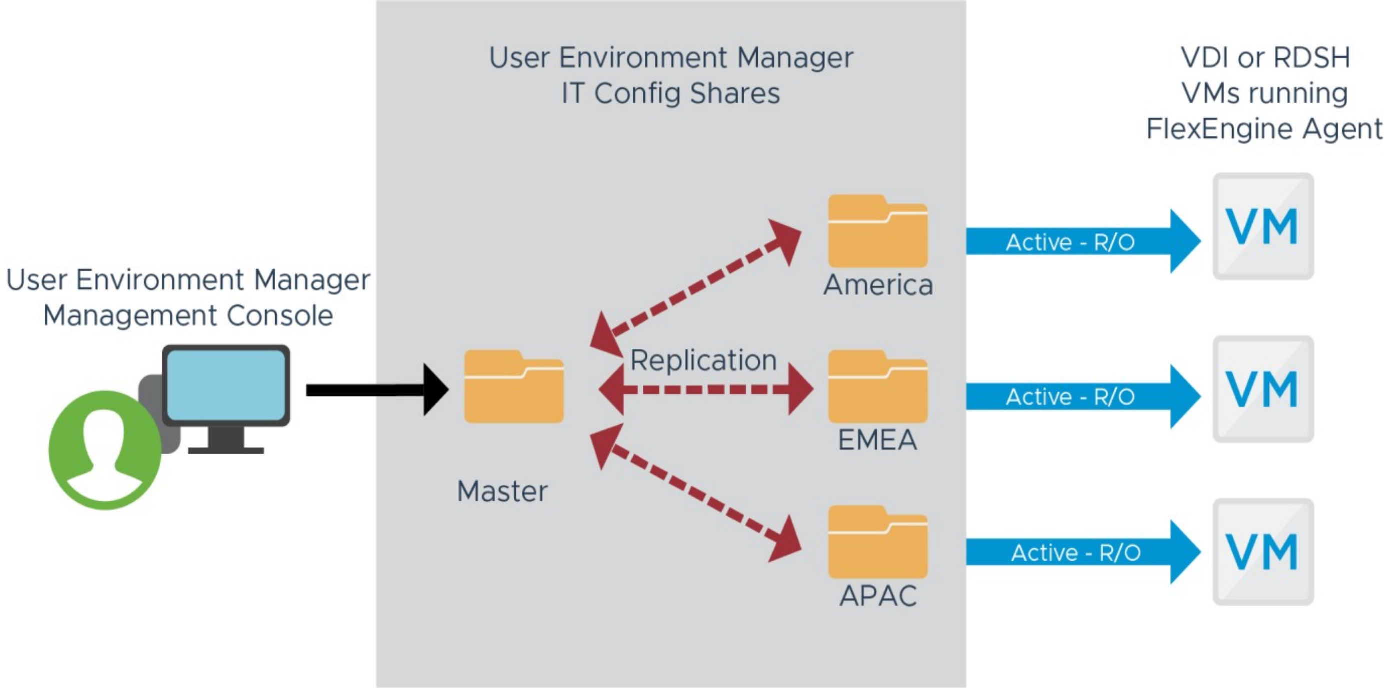
Users have read-only rights

DFS-Namespace (DFS-N) is fully supported:

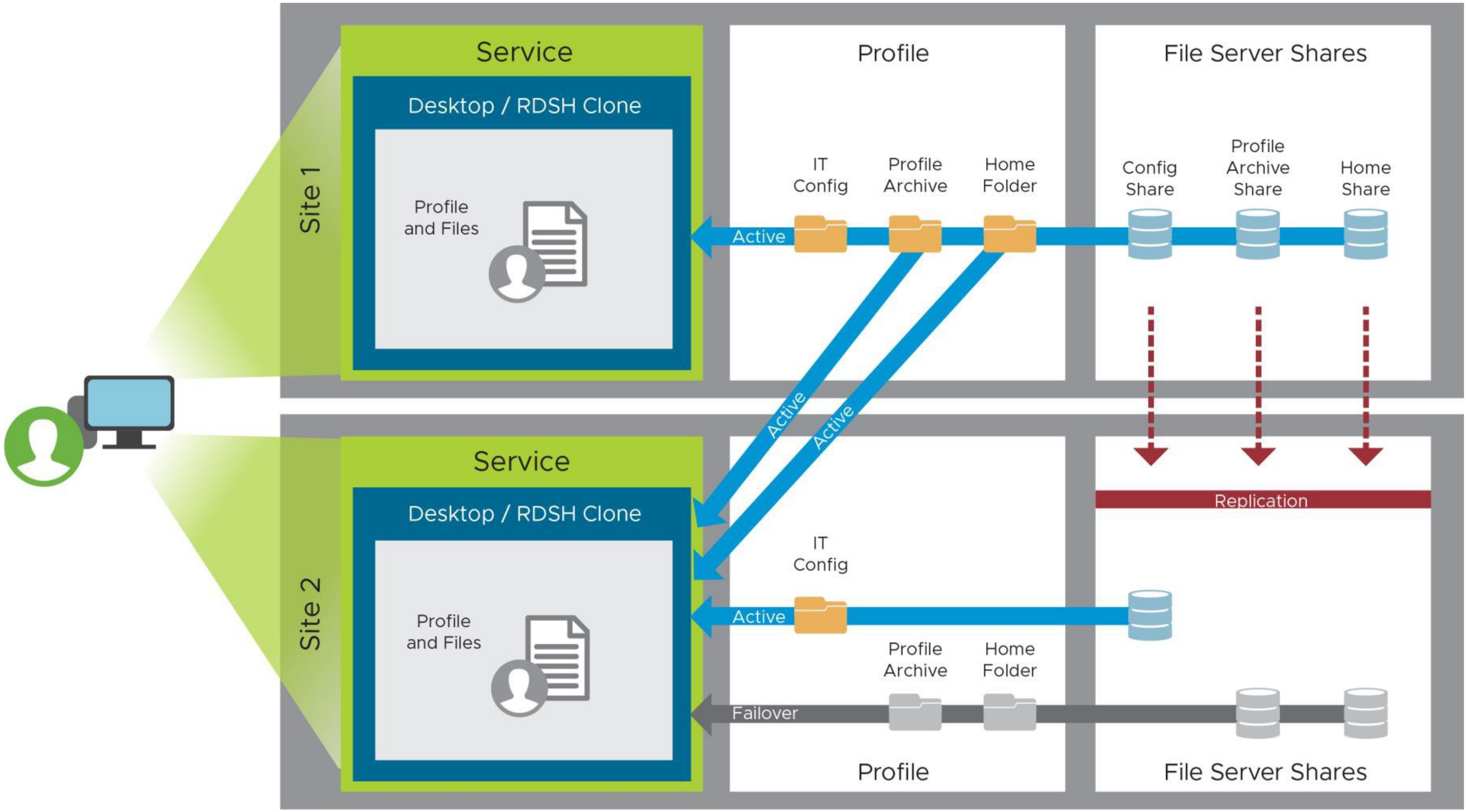
- In a hub and spoke replication topology

Connect the Management Console only to the hub master to make changes

- Let DFS-R replicate those changes to the spoke members



User Environment Manager Multi-Site Service



Environment Design

Physical Environment Considerations

Outside of Workspace ONE and Horizon products

- But required to deliver a complete solution

Some of these may already be present

Considerations:

- Supported versions
- Highly available
- Expected load
  - Compute
  - Disk load and space
  - Frequency of events
- Particular configuration needed

Site availability

- Active Directory
- Group Policy
- DNS
- DHCP
- Certificate Authority
- Key Management Service
- Database
- Load Balancer
- Firewall
- RDS Licensing
- File Servers
- Profiles

Service Integration

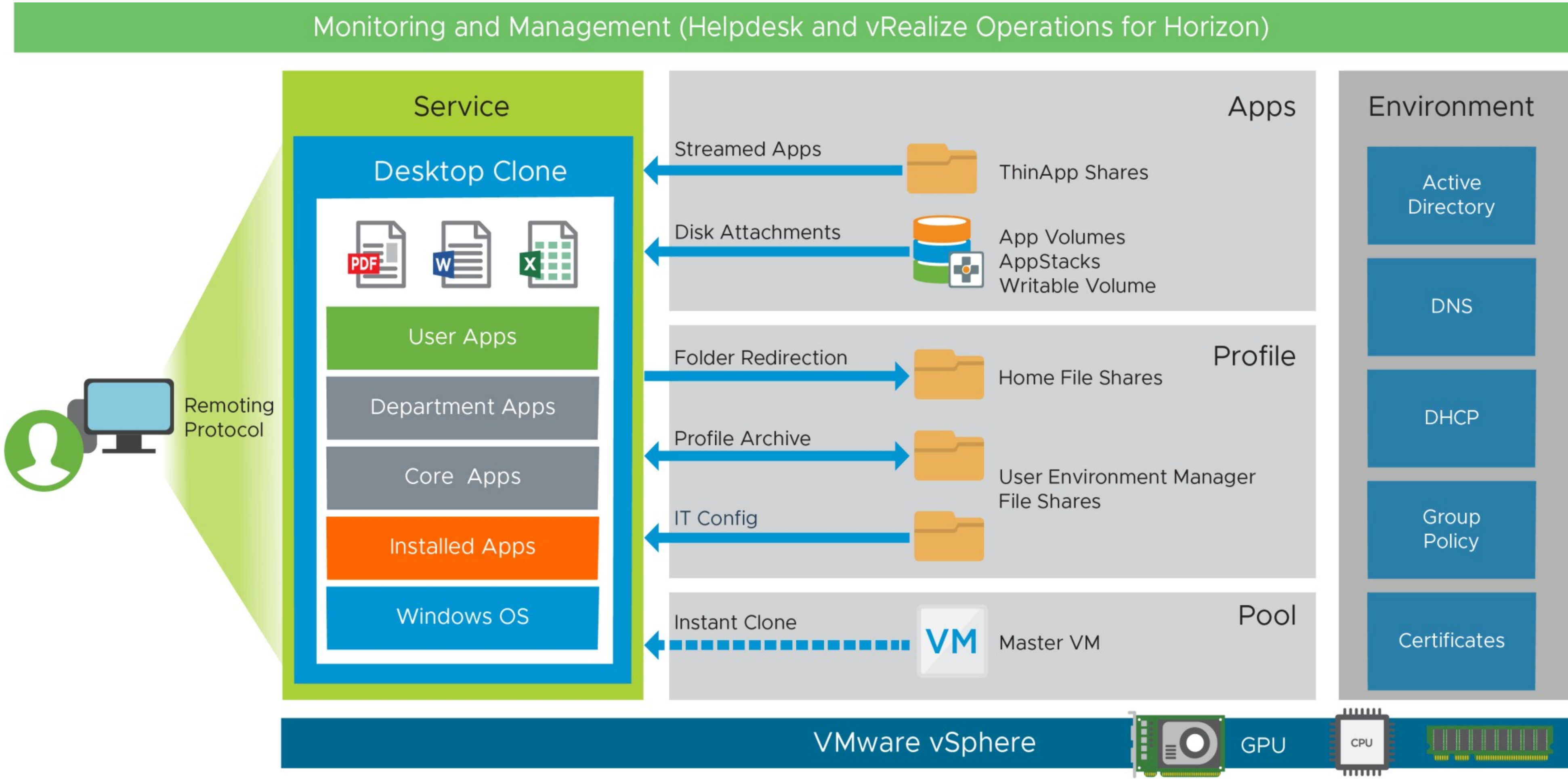
Constructing the services

Integrate and Deliver the Service

Create the required parts from each of the components

Assemble and integrate them into the end service that will be delivered to the users

Reference the blueprint for the use case

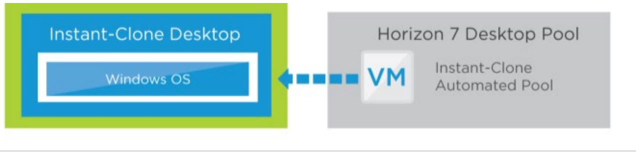


Build the Required Parts and Integrate

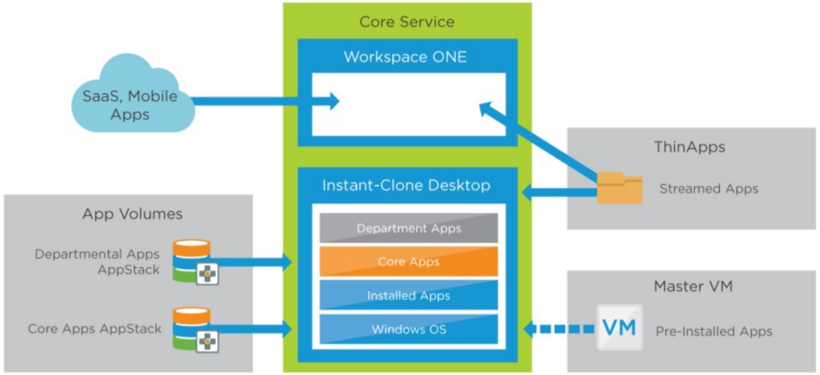
Horizon 7 Service Example

Part Required	Dedicated Power Workspace Service
Windows 10 instant clone	P
RDSH instant clone	
Linux clone	
App Volumes AppStack	P
App Volumes writable volume	P
User Environment Manager	P
Smart Policies	P
Application blocking	P
Folder redirection	P
Mandatory profile	P
GPO	P
Virtual printing	P
ThinApp Packages	P
SaaS apps	P
Unified Access Gateway	P
True SSO	P
vGPU	
NSX Firewall	Optional

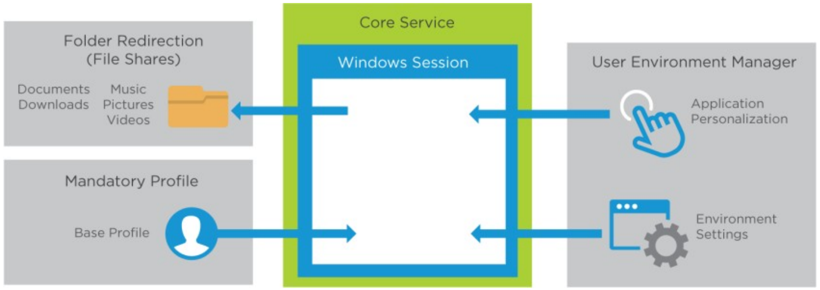
Desktop OS



Applications



Profile



Desktop OS

- Create Master VM
- OS install & tuning
- Create pool

Applications

- Install some in Master VM
- Create AppStacks
- Assign Writable Volume
- Create ThinApps

Profile

- Mandatory profile
- User Environment Manager configuration
- Folder redirection

Resource Block Considerations

Just because there is a maximum doesn't mean we should design to it

How many virtual machines per vCenter Server?

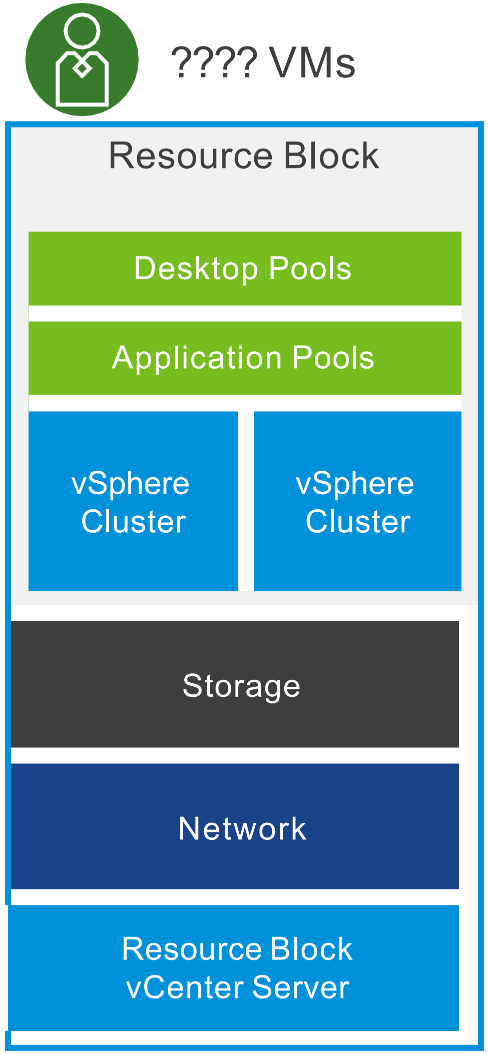
- Size of failure domain
- What is affected when vCenter is unavailable?
- Different concerns for Instant Clones vs. Linked Clones?

Sizing for:

- Normal operations
- Provisioning tasks, frequency, etc
- Time to provision, refresh, instant clone, etc

What about other products?

- App Volumes

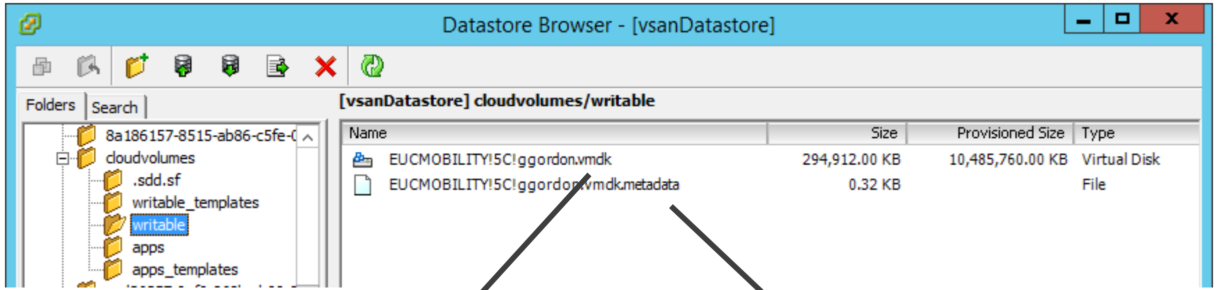


Cloud Pod Architecture Scale

Current recommendations as of Horizon 7.8

250,000	Total sessions
50	Pods
10,000	Sessions per pod
15	Sites
350	Connection Server instances

Writable Volumes



Datastore Browser - [vsanDatastore]

[vsanDatastore] cloudvolumes/writable

Name	Size	Provisioned Size	Type
EUCMOBILITY!5C!ggordon.vmdk	294,912.00 KB	10,485,760.00 KB	Virtual Disk
EUCMOBILITY!5C!ggordon.vmdk.metadata	0.32 KB		File

```
:protected: false
:writable: true
:name: EUCMOBILITY\ggordon
:block_login: false
:defer_create: false
```

Black boxes - Use them sparingly

Consider not protecting them at all

- Where content can be easily recreated – OSTs, etc

Virtual Disks not Virtual machines

Protection Options

- Backup through GUI = manual or scheduled
- LUN replication
- Manual file copy
- App Volumes Backup fling: https://labs.vmware.com/flings/app-volumes-backup-utility

Considerations

- Data Integrity and Consistency
- Recovery Point Objective (RPO) – How long will it take to recover them?
- Recovery Time Objective (RTO) – How much data might be lost?

Multi-Site Deployment Considerations

UEM Environment = UEM *Instance*

- Defined by Config share

Multiple models available

Choose based on customer requirements and infrastructure performance

- End users roam between sites or pinned to one?
- Latency between sites?
- Centralized or regional IT management of UEM?

Start with Profile Archive share design

- Users connect either to Profile Archives share at their respective sites, or to one share at a single site
- Profile Archives share replicated between sites
- Provides DR and/or (manual) HA
- Latency of >20ms between sites will affect user performance, and should be considered when architecting the solution

Finish with Config share design

- Single Config share for centralized management
- Multiple Config shares (multiple UEM instances) for regional management

Multi-Site Deployment Considerations

Example Deployment Models

Roaming users
Less than 20ms latency
Centralized management

- VMs from both sites point to Profile Archives share at one active site
  - Configure DFS-R/DFS-N for active-passive replication topology
- Single Config share replicates to remote sites
- Benefits
  - Centralized management
  - Active-passive with minimal RTO

Pinned users
Greater than 20ms latency
Centralized management

- Unique Profile Archives share at each site, replicated for DR
  - VMs from each site point to Profile Archives share at the same site
- GPO to segment users
- Single Config share replicates to remote sites
- Benefits
  - Centralized management
  - Good user experience despite higher latency between sites

Pinned users
Greater than 20ms latency
Regional management

- Unique Profile Archives share at each site, replicated for DR
  - VMs from each site point to Profile Archives share at the same site
- GPO to segment users\
- Multiple Config shares for distributed management
- Benefits
  - Regional management
  - Good user experience despite higher latency

Platform Integration

Horizon and VMware Identity Manager

Integration

Overview

Horizon resources available in Workspace ONE catalog

Provides access, authentication and launch

Benefit

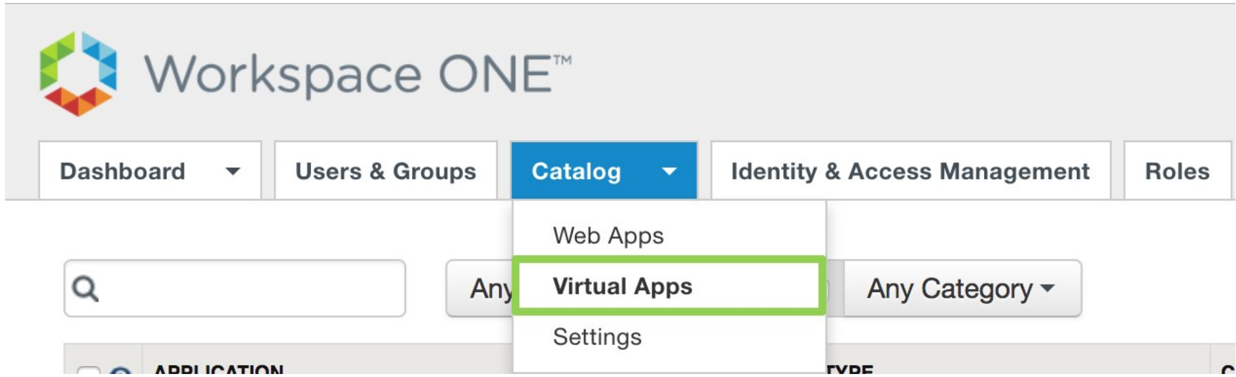
Simple, easy and consistent for users

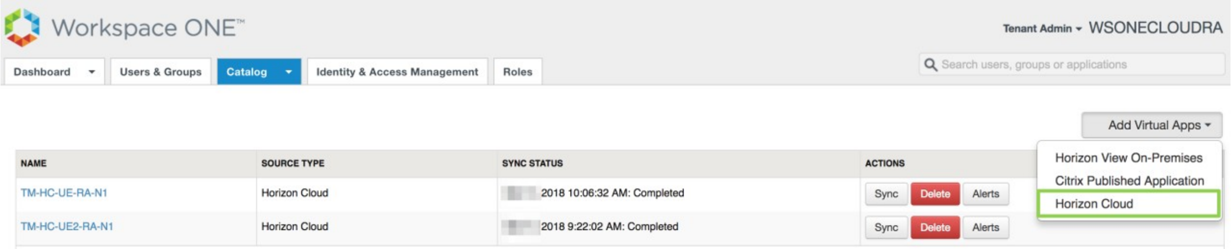
Enhance security with multi-factor authentication, and control conditional access

Detail

Register Horizon pod in VMware Identity Manager console

- Catalog > Virtual Apps > Horizon View or Cloud





NAME	SOURCE TYPE	SYNC STATUS	ACTIONS
TM-HC-UE-RA-N1	Horizon Cloud	[redacted] 2018 10:06:32 AM: Completed	Sync Delete Alerts
TM-HC-UE2-RA-N1	Horizon Cloud	[redacted] 2018 9:22:02 AM: Completed	Sync Delete Alerts

Horizon 7 and On-Premises VMware Identity Manager

Integration

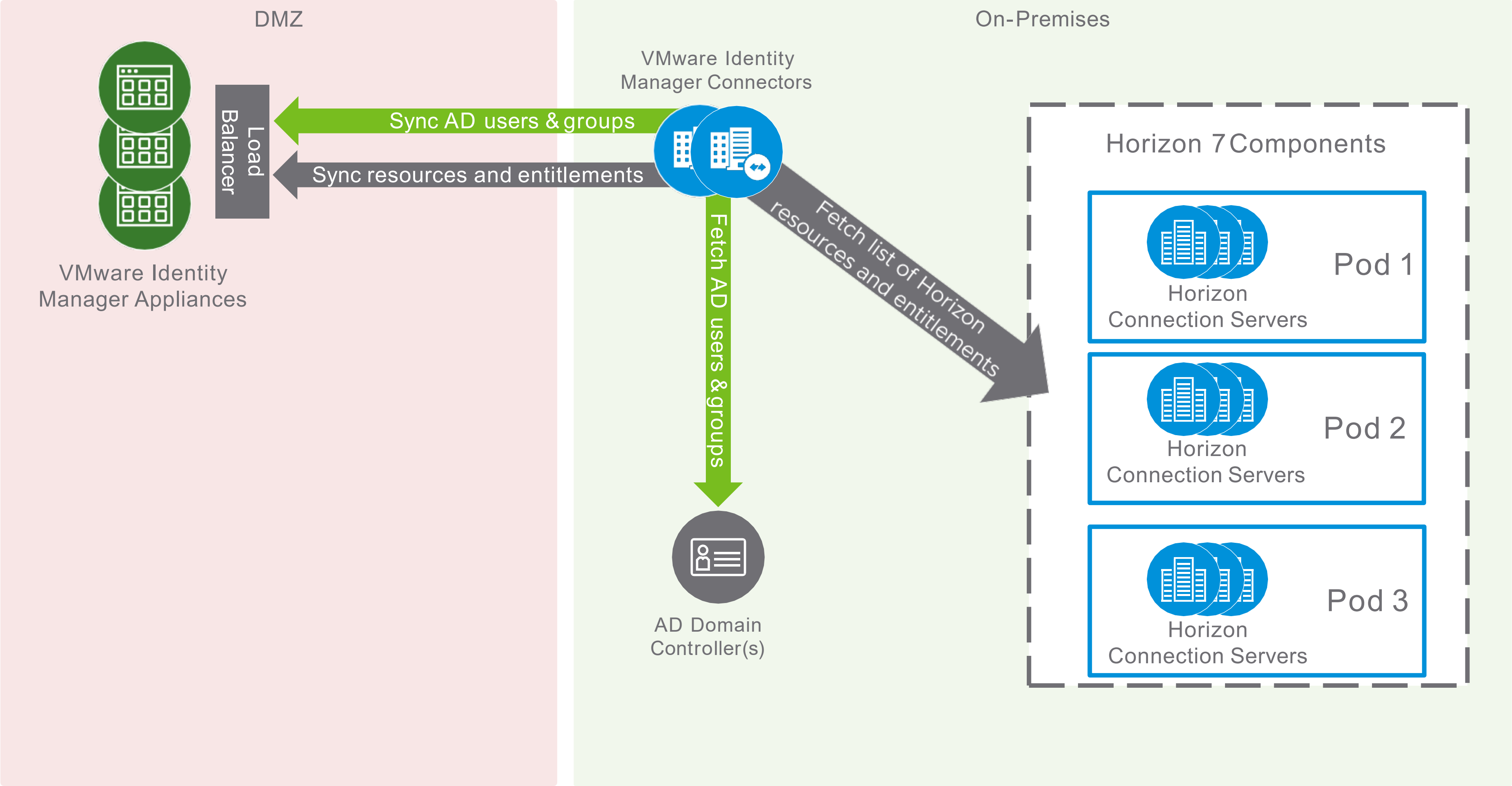
USDC TECHNOLOGY
Smart Data Center

AD users & groups

- Synced to vIDM service
- Using vIDM connector

Horizon resources and entitlements

- Synched from the connection server
- To the vIDM service
- Using vIDM connector


DMZ
On-Premises
VMware Identity Manager Appliances
Load Balancer
VMware Identity Manager Connectors
Sync AD users & groups
Sync resources and entitlements
Fetch AD users & groups
Fetch list of Horizon resources and entitlements
AD Domain Controller(s)
Horizon 7 Components
Pod 1
Horizon Connection Servers
Pod 2
Horizon Connection Servers
Pod 3
Horizon Connection Servers

vmware

Horizon 7 and Cloud-Based VMware Identity Manager

Integration

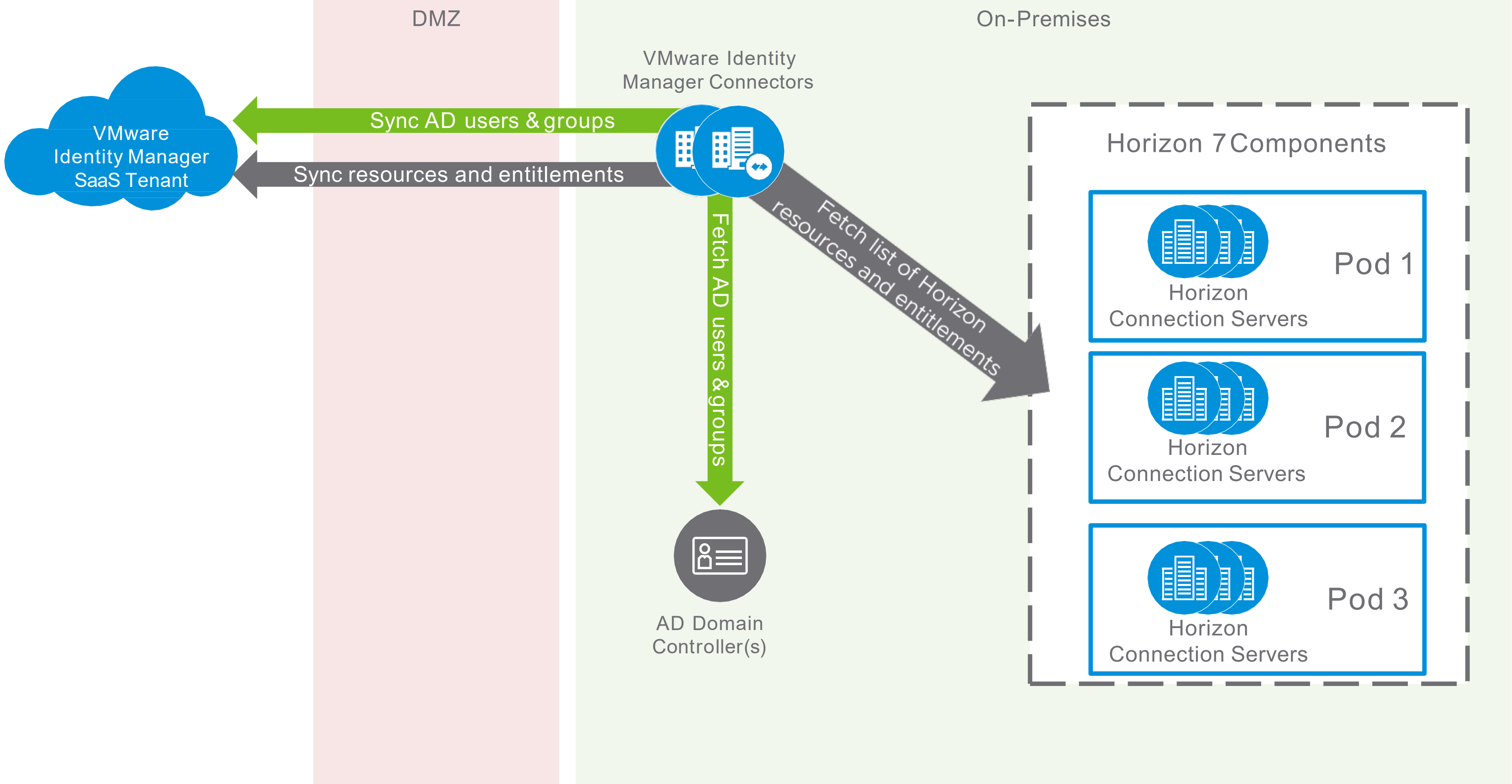
USDC TECHNOLOGY
Smart Data Center

AD users & groups

- Synced to vIDM service
- Using vIDM connector

Horizon resources and entitlements

- Synched from the connection server
- To the vIDM service
- Using vIDM connector


DMZ
On-Premises
VMware Identity Manager SaaS Tenant
Sync AD users & groups
Sync resources and entitlements
VMware Identity Manager Connectors
Fetch AD users & groups
Fetch list of Horizon resources and entitlements
AD Domain Controller(s)
Horizon 7 Components
Pod 1
Horizon Connection Servers
Pod 2
Horizon Connection Servers
Pod 3
Horizon Connection Servers

vmware

Horizon Cloud and VMware Identity Manager

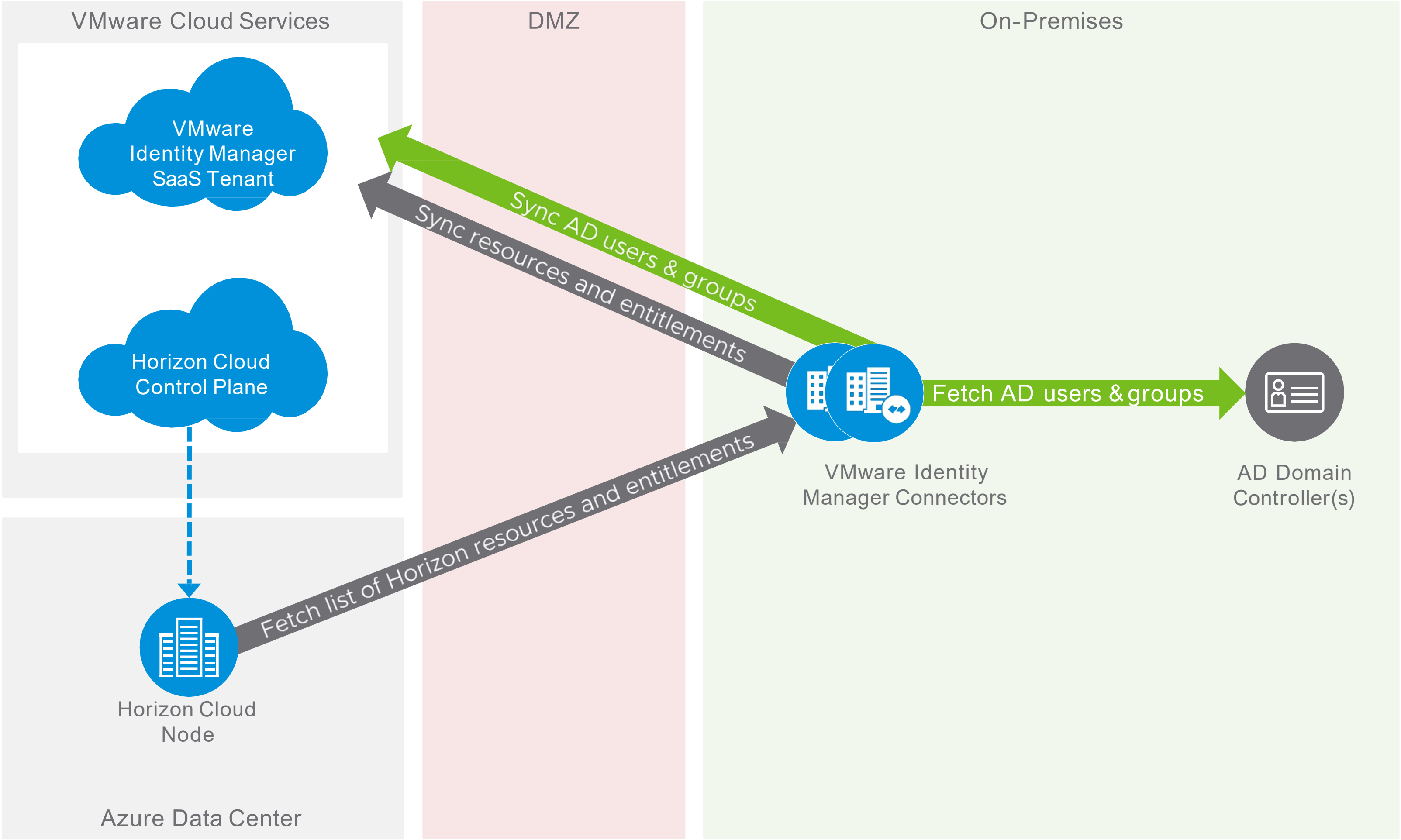
Integration

AD users & groups

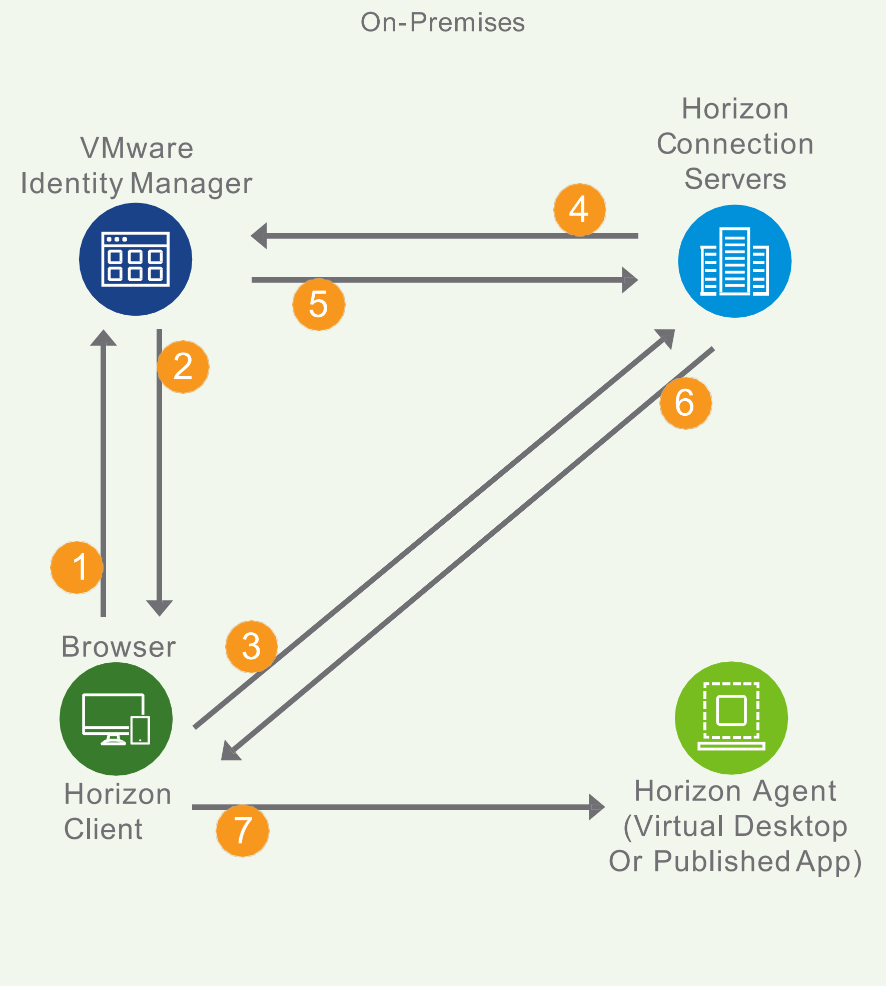
- Synced to vIDM service
- Using vIDM connector

Horizon resources and entitlements

- Synched from the Horizon Cloud Node
- To the vIDM service
- Using vIDM connector


VMware Cloud Services
DMZ
On-Premises
VMware Identity Manager SaaS Tenant
Horizon Cloud Control Plane
Sync AD users & groups
Sync resources and entitlements
Fetch AD users & groups
VMware Identity Manager Connectors
AD Domain Controller(s)
Fetch list of Horizon resources and entitlements
Horizon Cloud Node
Azure Data Center

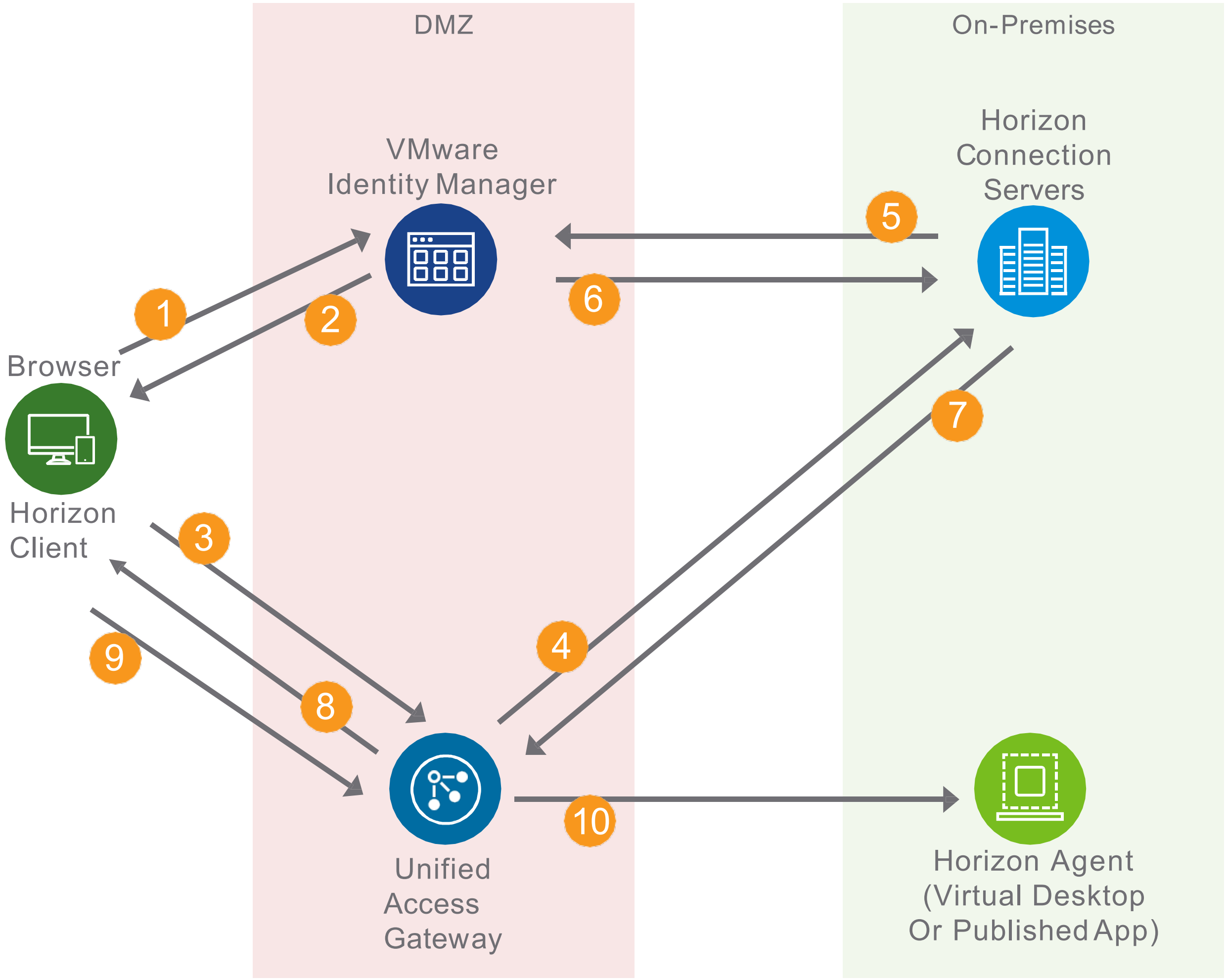
Launch Horizon 7 Resource from VMware Identity Manager


On-Premises
VMware Identity Manager
Horizon Connection Servers
4
5
2
6
1
3
Browser
Horizon Client
7
Horizon Agent (Virtual Desktop Or Published App)

1. In Browser, user launches Horizon resource from Identity Manager.
2. Identity Manager generates SAML assertion and artifact.
   - Generates view URL containing artifact and returns to Browser: vmware-view://URL SAMLArt=<saml-artifact>
3. Horizon Client is launched from view URL.
   - XML-API request do-submit-authentication <saml-artifact>
4. Broker performs SAML resolve against Identity Manager.
   - <saml-artifact>
5. Identity Manager validates artifact and returns assertion.
   - <saml-assertion>
6. Broker returns successful authentication.
   - XML-API OK response submit-authentication
7. Remote protocol client launches session with parameters returned.

External Launch Horizon 7 Resource

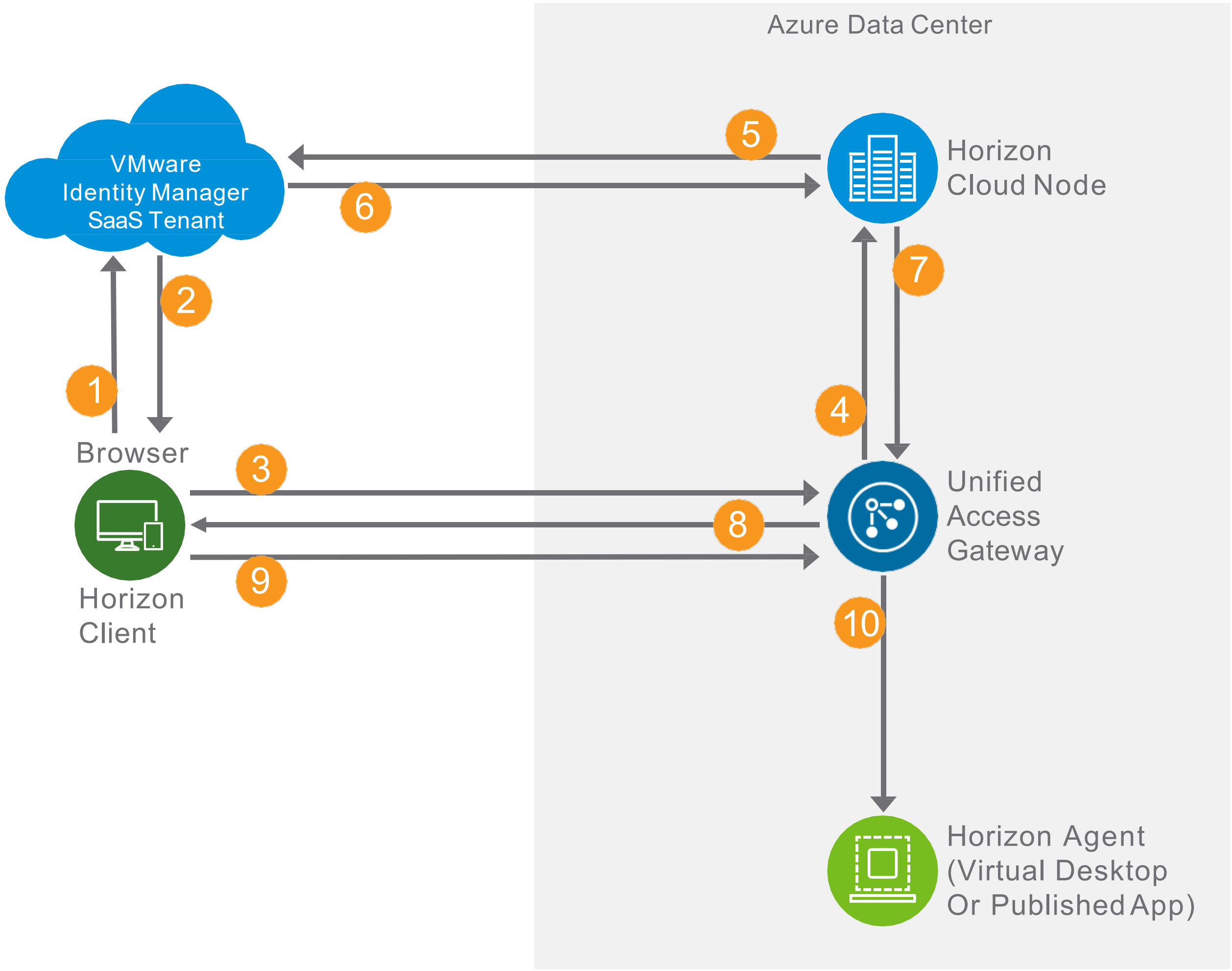
from On-Premises VMware Identity Manager



1. In Browser, user launches Horizon resource from Identity Manager.
2. Identity Manager generates SAML assertion and artifact.
   - Generates view URL containing artifact and returns to Browser: vmware-view://URL SAMLArt=<saml-artifact>
3. Horizon Client is launched from view URL.
   - XML-API request do-submit-authentication <saml-artifact>
4. Unifed Access Gateway (UAG) proxies the authentication to the Horizon Broker
5. The Broker performs SAML resolve against Identity Manager.
   - <saml-artifact>
6. Identity Manager validates artifact and returns assertion.
   - <saml-assertion>
7. Broker returns successful authentication.
   - XML-API OK response submit-authentication
8. UAG returns the successful authentication to the Client
9. Remote protocol client launches session with parameters returned.
10. UAG proxies the protocol session to the Horizon Agent.

USDC TECHNOLOGY
Smart Data Center

Launch Horizon Cloud Resource from VMware Identity Manager



1. In Browser, user launches Horizon resource from Identity Manager.
2. Identity Manager generates SAML assertion and artifact.
   - Generates view URL containing artifact and returns to Browser: vmware-view://URL SAMLArt=<saml-artifact>
3. Horizon Client is launched from view URL.
   - XML-API request do-submit-authentication <saml-artifact>
4. Unifed Access Gateway (UAG) proxies the authentication to the Horizon Cloud Node
5. The Broker performs SAML resolve against Identity Manager.
   - <saml-artifact>
6. Identity Manager validates artifact and returns assertion.
   - <saml-assertion>
7. Broker returns successful authentication.
   - XML-API OK response submit-authentication
8. UAG returns the successful authentication to the Client
9. Remote protocol client launches session with parameters returned.
10. UAG proxies the protocol session to the Horizon Agent.

vmware

Thank You!