Introduction to Virtualization

What is virtualization

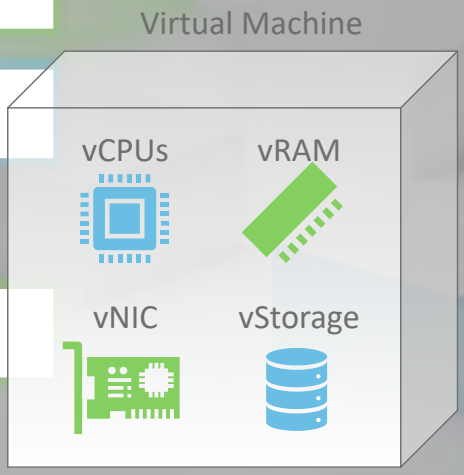
Allows you to deploy datacenter recourses using software that usually associated with hardware

Virtualized compute

vCPU
vNIC
vRAM
vStorage

Virtualized networking

vSwitch
DVS
NSX



Why Virtualize the Datacenter

Cost savings

Hardware utilization

vSphere clustering services

DRS
HA

Software Defined Datacenter vs Cloud Infrastructure

Software defined datacenter

Your hardware
You are responsible for infrastructure patching and upgrades
You will need to plan for growth when purchasing

Cloud infrastructure

Cloud vendor provides that hardware
Cloud vendor will patch and upgrade the infrastructure
You pay for the resources you need/use

Demo

Tour vSphere and a software defined datacenter

VDI Deployment On-Premises vs Cloud

On-premises

More configurable / customizable
You have greater control of security
Data on premise

Cloud

Cost per desktop may be high
Vendor will be responsible for patching
Can deploy new desktops as needed, even if sudden growth was not planned
Data will be in the cloud

Conclusions

Introduction to virtualization

What is virtualization
Why virtualize the datacenter
Software defined datacenter vs cloud infrastructure
VDI deployment on-premises vs cloud

Introduction to VMware Horizon

Introduction to VMware Horizon

- Features and Benefits
- Horizon 8 Architecture
- Use Cases
- vSphere in VMware Horizon

Features and Benefits

Flexible Deployments

On-premises deployment

Cloud-hosted deployment

Hybrid deployment

Connecting Horizon 8 Deployments to Horizon Control Plane

Requires SaaS subscription license

Allows connecting Horizon 8 pods to the control plane for Horizon Cloud Service - next gen with Horizon Edge for Horizon 8

Allows for the managing of on-premise and multi-cloud from a single pane of glass

Provides a single workflow to enable VMware JMP technologies

Features and Benefits

Just-in-Time Management Platform (JMP)

- Instant clones
- VMware App Volumes
- VMware Dynamic Environment Manager

Reliability and Security

- Data Access
  - Sensitive data can be prevented from being copied onto a remote systems
- RADIUS support
- Integration with VMware Workspace ONE
- Unified access gateway
- Active Directory (ADDDS) integration
- Datacenter up time

Features and Benefits

Integration with the VMware Ecosystem

VMware vSphere
vSAN
NSX

Rich User Experience

Familiar and personalized desktop environment
Able to access USB and other devices connected to their local computer
Real-time audio/video features
Unified access gateway
Multiple monitor support
3D graphics support

RESTful APIs Support

Horizon 8 Architecture

Core Infrastructure

vSphere, SQL, ADDS

Connection Server

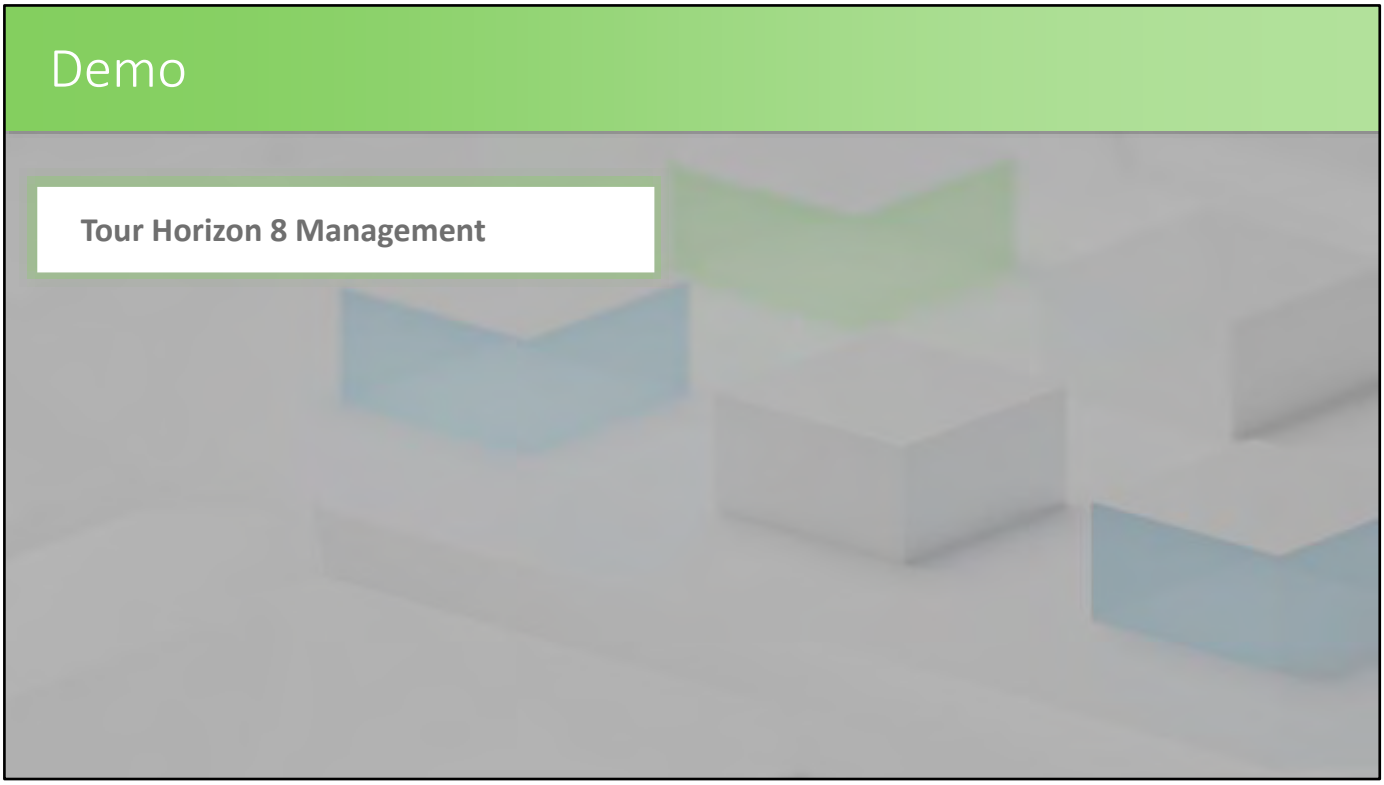
Unified Access Gateway

VMware Horizon Agent

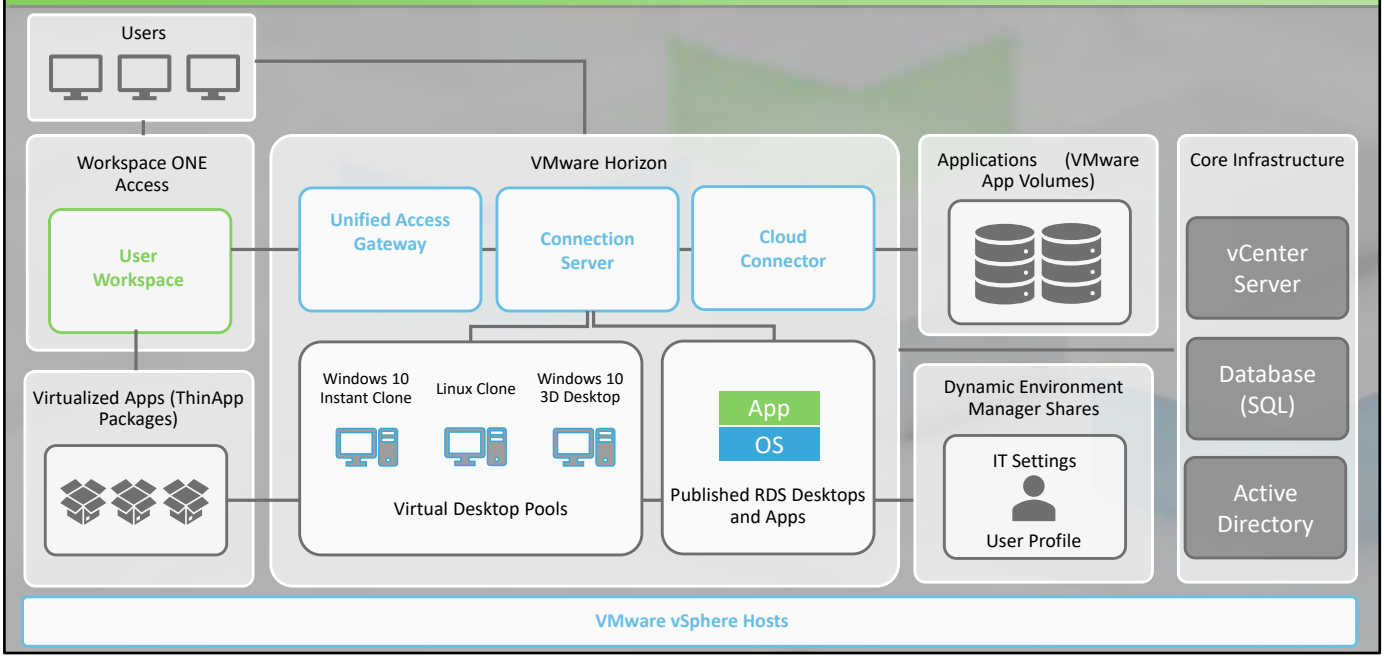
Dynamic Environment Manager

Thin App Packages

Demo



Horizon 8 Architecture



Conclusions

Introduction to VMware Horizon

Features and Benefits

Architecture

Use Cases

- In office desktops
- Remote user's desktops
- IT users jump boxes
- Special applications (graphic intensive applications)
- Kiosks
- Healthcare workers
- Education (Student Systems)
- Working from multiple locations/stations

Customer requirements

- Security of data
- Security of user environment
- User mobility
- Special application or hardware needed
- Customized desktop needed in secure or limited access environment
- Regulations or governance

Matching customer requirements to use cases

Use Cases	Customer Requirements
In Office Desktops	Security of data
IT Users jump boxes	Security of user environment
Kiosks	Customized desktop secure or limited environment
Education (Student Systems)	User Mobility
Remote Users Desktops	Special application or hardware needed
Special Applications (Graphic Intensive Applications)	Regulations or governance
Healthcare workers	
Working from multiple locations/stations	

Match VMware products with use cases

Use Cases
In Office Desktops
Remote Users Desktops
IT Users jump boxes
Special Applications (Graphic Intensive Applications)
Kiosks
Healthcare workers
Education (Student Systems)
Working from multiple locations/stations

Horizon
Horizon Cloud Service

Horizon with Workspace ONE

User authentication

Device management

BYOD

Application management/deployment

DR and HA

- VMware Horizon can be a part of your DR plan
  - Can provide users remote desktops in case of a disaster
- VMware Horizon makes your user's desktops part of the datacenter
  - VDI environment can be protected as part of your datacenter DR plan
  - VDI environments can take advantage of vSphere HA features
  - Users profiles and data are not detached from a desktop and able to be portable to other VDI sessions insuring a consistent experience

Conclusions

Use Cases

Use cases

Customer requirements

Matching customer requirements to use cases

Workspace ONE

VDI DR and HA

vSphere in VMware Horizon

- vSphere Introduction
- Using vSphere Client, vCenter Server, and ESXi
- Creating, provisioning, and deleting virtual machines

vSphere Introduction

- **vSphere is the foundation of VMware's virtualized datacenter**
- **Provides datacenter virtualization services**
  - ESXi clustering
  - DRS
  - HA
  - vMotion
  - Virtual machine templates
- **Many other VMware solutions build off vSphere**
  - NSX
  - Horizon
  - SRM

Using vSphere Client, vCenter Server, and ESXi

vSphere Client

HTML based client for managing vSphere environment

Central place to manage your vSphere environment such as storage, virtual networking, vm provisioning, services configuration and more.

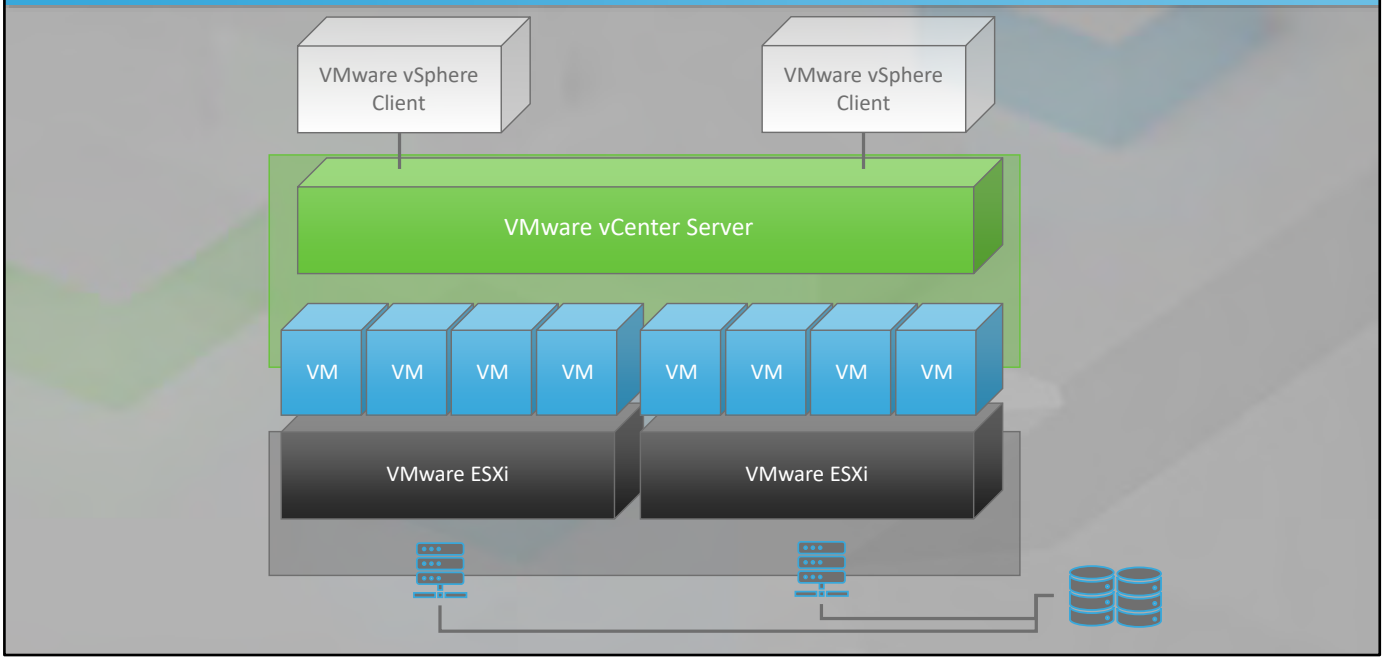
vCenter Server

Virtual appliance that is the central management location for a vSphere environment

ESXi

VMware's enterprise type 1 hypervisor for vSphere

vSphere Client, vCenter Server, and ESXi



Creating, Provisioning, and Deleting Virtual Machines

Creating a virtual machine

If there is no VM or template in your environment that has the base configuration you need, a VM can be created from scratch

Provisioning a virtual machines

A VM can also be provisioned by coping another VM or template and adding customizations if required

Deleting virtual machines

A VM can be removed from inventory only

A VM can also be removed from inventory and deleted from disk/storage

Demo

- Creating, provisioning, and deleting virtual machines

Conclusions

- vSphere Introduction
- Using vSphere Client, vCenter Server, and ESXi
- Creating, provisioning, and deleting virtual machines

Installing the Horizon Environment

Connection Server

Installation Types (Windows Server)

Standard

Replica

Enrollment

Three node cluster

Best Practice for stability and availability

Hardware

4 CPU

1 Gbps NIC

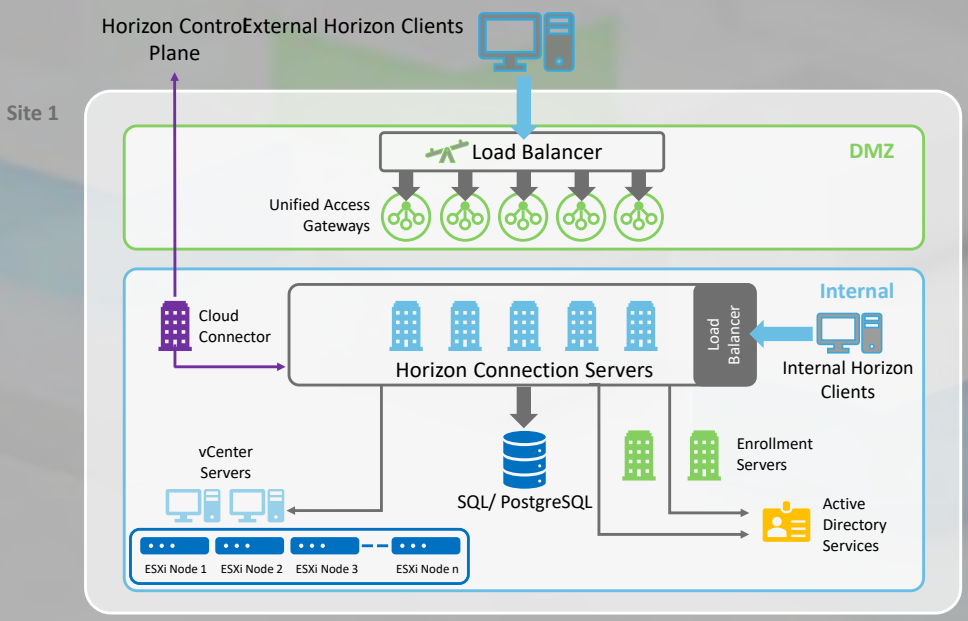
10 GB RAM

Connection Server cont.

Horizon agent

Must be installed on all virtual machines, physical systems, and RDS hosts

Horizon Installation



Installing Connection Server

- Run Connection Server installed on Windows Server
- Click “Yes” when prompted to allow the app to make changes
- On the Installation Options page select
  - Horizon Standard Server
  - IPv4
- Enter the password for recovering data backups
- On the Firewall Configuration page accept default
  - Configure Windows Firewall automatically

Installing Connection Server

Initial Horizon Administrators page chose either…

- Authorize the local Administrators group
- Authorize a specific domain user or domain group

User Experience Improvement Program page you can deselect « **Join the VMware Customer**”

On the Ready to Install page select “General” for a local (Not cloud) installation

On the Installer Completed page, click Finish

Demo

Installing Horizon Connection server

Pre Connection Server Configuration

- Create the Domain Admin User
- Create OUs for Instant-Clone Desktops and RDSH Servers
- Delegate Control to the OU's
- Add the Product License Key

Demo

Pre Connection Server Configuration

After Installation of Connection Server

- SSL Server certificates
- Perform initial configuration on connection server
- Deploy replicated connection server instances (3 node cluster)
- Before you add vCenter Server to VMware Horizon in a production, make sure that vCenter Server uses certificates signed by a CA
- Configuring the PSG (PCoIP Secure Gateway) service to use a CA-signed certificate
- Blast Server uses the connection server certificate

Connection Server Configuration

Add the Product License Key

Add a vCenter Server Instance

Add an Instant-Clone Domain Administrator

Create and Configure the Events Database

Prerequisites for Setting Up the Events Database

SQL Server instance

Microsoft SQL Server Management Studio

Microsoft SQL Server Configuration Manager

SA credentials

Configure TCP/IP Properties for the Database Server

Configure the Events Database in the Horizon Console

Demo

Connection Server Configuration

Connection Server User Rights

Before deploying instant clones create a user or group account that has the permissions to perform certain operations in Active Directory

Apply permissions to the correct container (OU) and to all child objects

- Create computer objects
- Delete computer objects
- Write all properties
- List contents
- Read all properties
- Write all properties
- Read permissions
- Reset password
- Create computer objects
- Delete computer objects

Configuring User Account in vCenter Server for Horizon and Instant Clones

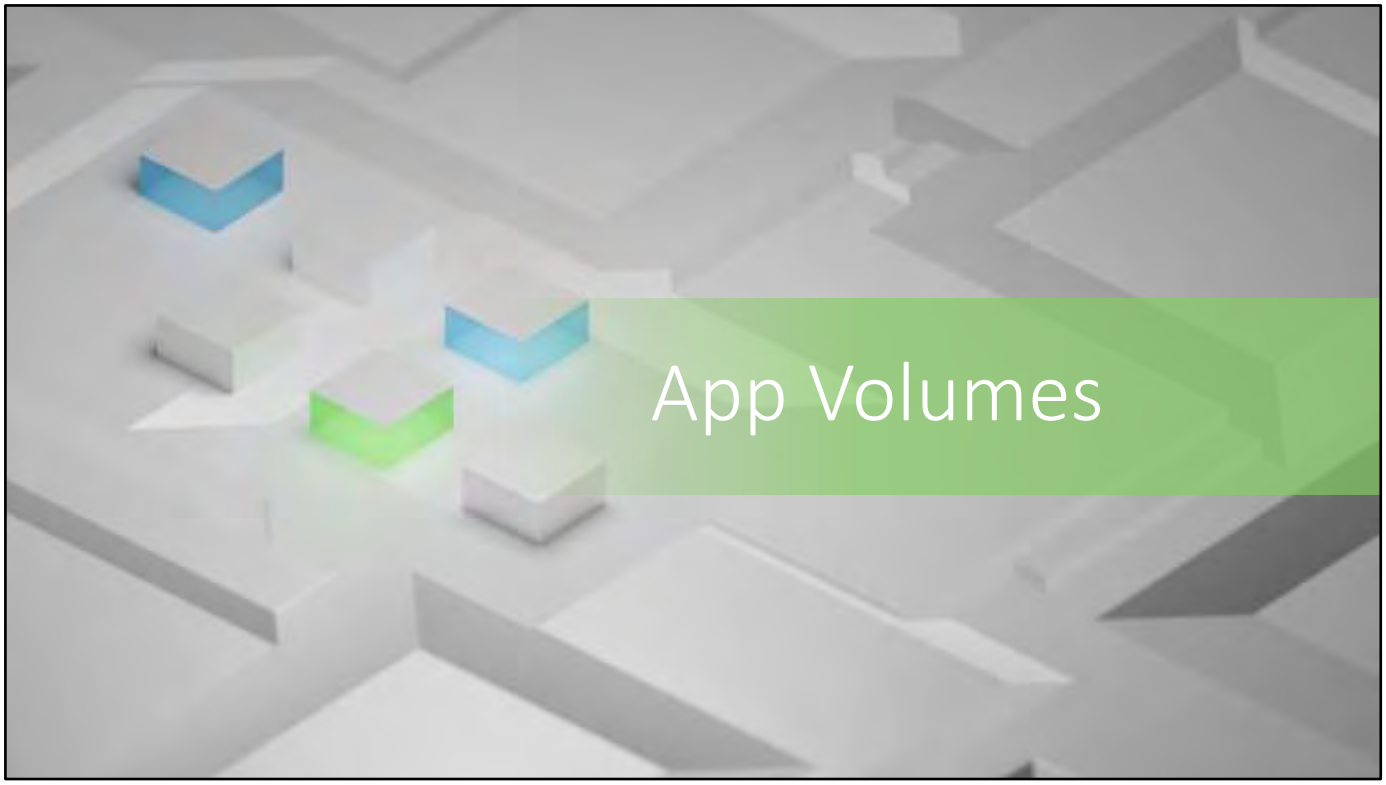
Create a role with the minimum privileges needed by Connection Server to perform vCenter operations and instant-clone operations

- Use a more limited role than the predefined Administrator role in vCenter Server and with instant clones
- In vSphere Client, click Home > Roles > Add Role
- Enter a role name such as Horizon Instant Clone Administrator, and select privileges for the role

Privileges for the vSphere role for Connection Server

VMware Horizon 2103 Installation Guide page 73 abbreviate

Folder	Crate folder Delete folder
Datastore	Allocate space Browse datastore
Virtual Machine	In Configuration (all) In Interaction (Abbbreviated)
Resource	Assign virtual machine to resource pool
Global	Act as vCenter Server
Cryptographic Operations	
Host	In Inventory - Modify Cluster In Configuration - Advanced settings



App Volumes

- Application virtualization
- Install and configure App Volumes
- Create an App Volumes Application Packaged
- Manage, assign and provision an App Volumes Application Packaged
- Update an App Volumes Application Package
- Create, manage, and assign a writable volume
- Move, backup, restore a writable volume

Application Virtualization

Application virtualization

A user access's an application installed on a remote system as if it were installed locally.
A horizon RDS server farm has the application installed
A client running the VMWare Horizon Client connects to a VMWare Horizon Connection Server
The user is then presented with published applications that they are given entitlements to

Install and configure App Volumes

Create an App Volumes Application Packaged

Manage, assign and provision an App Volumes Application Packaged

Install and Configure App Volumes

Install and configure App Volumes

Create and set up the required user accounts and Active Directory credentials

Install App Volumes Manager

- Used to administer and configure App Volumes and assignment of Application Packages and Writable Volumes

Install App Volumes Agent

- Install the App Volumes agent on the packaging computer and target desktops

Verify License

- Enter the App Volumes license information

Create an App Volumes Application Packaged

Manage, assign and provision an App Volumes Application Packaged

Demo

Install and Configure App Volumes

Create an App Volumes Application Package

Create an App Volumes Application Packaged

In App Volumes Manager

- INVENTORY > Applications

Select an application and click Create Package

On the Create Package page provide package detail

Select the package Delivery mode

- Default mode is Classic

Click Create

Update an App Volumes Application Package

Create, manage, and assign a writable volume

Demo

Create an App Volumes Application Package

Update an App Volumes Application Package

Update an App Volumes Application Package

In App Volumes Manager

- INVENTORY > Applications

Select an application and click Create Package

On the Create Package page provide package detail

Select the package Delivery mode

- Default mode is Classic

Click Create

Demo

Update an App Volumes Application Package

Writable Volumes

- Per-user volumes where users can install and configure their own applications and keep the data that is specific to their profile
- Is assigned to a specific user and becomes available to the user from any machine
- An empty VMDK or VHD file that is assign to a specific user
- Mounts to the VM when the user authenticates to the desktop
- Mounts to the VM when the user authenticates to the desktop

If a user logs into Workstation1 and Workstation2 simultaneously one volume is attached to the user on Workstation1 and a second on Workstation2

App Volumes and Writeable Volumes

Assign a Writable Volume

- Can be assigned to a user, group, computer, or organizational unit
  - When created for a user, it is assigned to the user immediately
  - When assigned to a group, it is created when a user belonging to the assigned group logs in to the machine the first time
- A user can have more than one Writable Volume attached at the same time
  - The volume is OS-specific
  - Created for a computer with a specific prefix
- Can have only one writable volume attached to the virtual machine at a given time

Demo

Assign a Writable Volume

Backup a Writable volume

From App Volumes Manager
- INVENTORY > Writables

Select the Writable Volume you want to back up
Click Backup
On the Backup Writable Volume page choose
- Destination Storage
- Destination Path

Select Delete writable volumes after backup (Optional)
Click Backup
On the Confirm Backup Writable Volumes window choose
- Backup volume in the background
- Backup volume immediately

Click Backup
To check the status of the backup

Demo

Backup a Writable Volume

Restore a Writable volume

From the App Volumes Manager

- INVENTORY > Writables.

Chose which entity you want to restore

Click Restore.

On the Restore Writable page, provide the following information

- Source Storage
- Source Path

Click Restore

On the Confirm Restore Writable Volumes window choose

- Restore volume in the background
- Restore volume immediately

View Backup or Restore Logs

To see detailed information about the operation progress

ACTIVITY > Activity Log

To see any warnings or error messages

ACTIVITY > System Messages

Demo

Restore a writable volume

View Backup or Restore logs

Move a Writable volume

In App Volumes Manager
- INVENTORY > Writables

A list of entities is displayed.

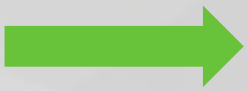
Select the entity whose Writable Volume you want to move

Click Move

On the Move Writable Volume page
- Destination Storage
- Destination Path

Click Move
- Move volumes in the background
- Move volumes immediately

Click Move



Demo

Move a writable volume

Conclusions

App Volumes

Application virtualization

Install and configure App Volumes

Create an App Volumes Application Packaged

Manage, assign and provision an App Volumes Application Packaged

Update an App Volumes Application Package

Create, manage, and assign a writable volume

Move, backup, restore a writable volume

Creating a Windows and Linux VM in vSphere

- Configure Virtual Hardware
- Choose OS
- Install Guest Operating System

Demo

- Creating a Windows and Linux VM in vSphere

Optimizing VMs for Horizon desktop

Automate VM image optimization

- Use Microsoft Deployment Toolkit (MDT)

Manual VM image optimization

- Follow the guide “Manually Creating Optimized Windows Images for VMware Horizon VMs”

https://techzone.VMware.com/resource/manually-creating-optimized-windows-images-VMware-horizon-vms#introduction

Reason to Optimizing Horizon Desktops

- To reach a higher consolidation ratio, increasing the number of VMs per hosted turning off features that are not needed
- One-time system actions must be configured in the base image
- One-time user actions must be configured in the default user profile

Optimizing Tasks

- Creating a vSphere-Based VM
  - Use a Volume License Key
- Install VM operating system
- Install VMware tools, de-selecting un-needed components
  - Carbon Black Helper Component
  - Service Discovery
  - Volume Shadow Copy Services Support
- Install .Net Framework 3.5
- Install any Windows Updates

Optimizing Tasks

- Install Horizon Agent (usually)
  - Desktop Mode
  - Core
  - VMware Horizon Instant Clone Agent
  - VMware Audio
  - VMware Integrated Printing
- Install the Dynamic Environment Manager Agent
- Run Windows OS Optimization Tool to…
  - Optimize
  - Generalize
  - Finalize the OS

Demo

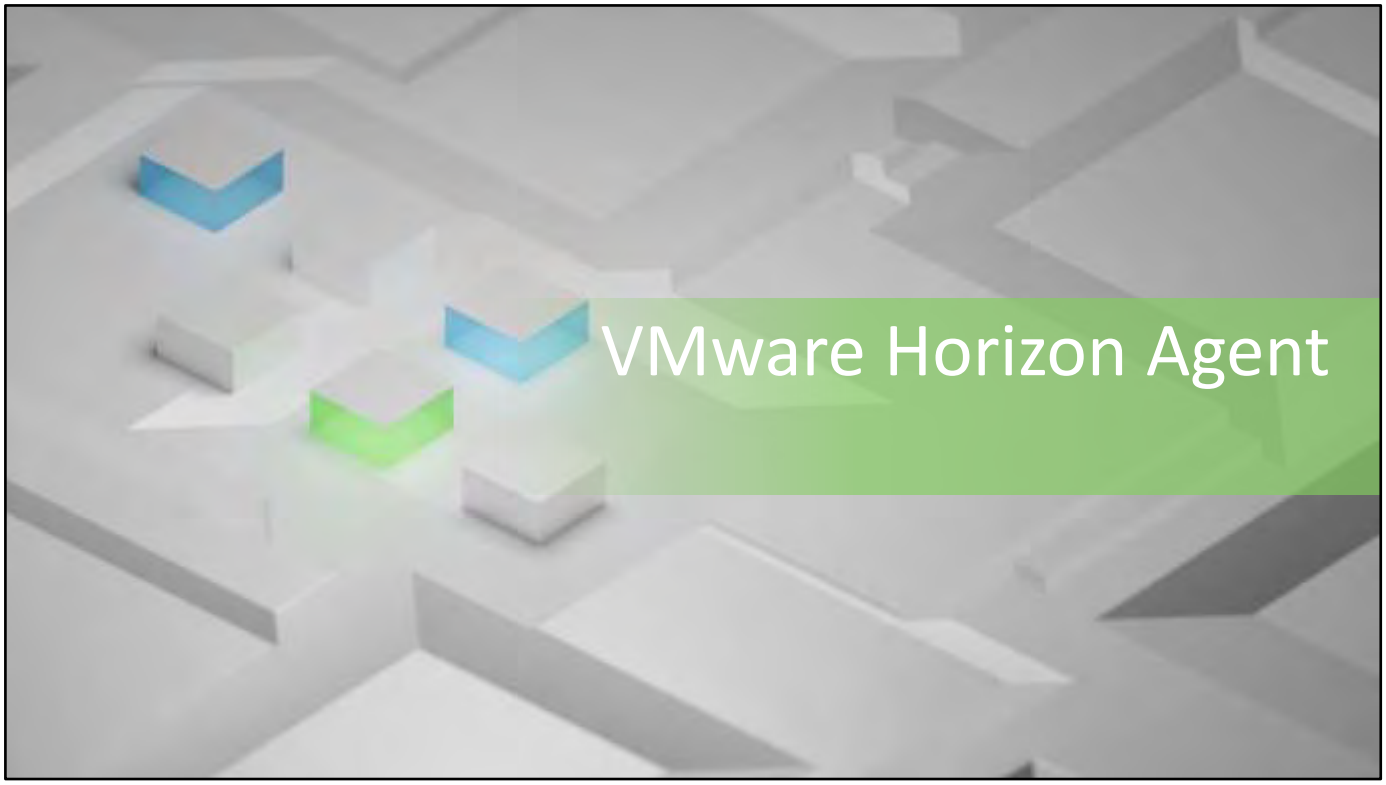
- Optimizing VMs for Horizon desktop

Conclusions

VMware Horizon Desktops

Creating a Windows and Linux VM in vSphere

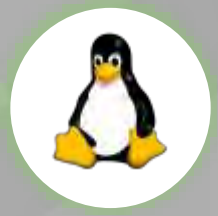
Optimizing VMs for Horizon desktop



VMware Horizon Agent

- Create a golden image for Windows Horizon desktops

- Create a golden image for Linux Horizon desktops



Configuration choices when installing Horizon agent on Windows

- A local use account with administrative privileges
- Horizon Agent installer
- VM with supported Windows OS
- Choose RDS Mode or Desktop Mode
- IPv4 or IPv6
- Select the features that will be used, for most environments
  - Core
  - VMware Horizon Instant Clone Agent
  - VMware Audio
  - VMware Integrated Printing
- Enable Remote Desktop support

Demo VMware Horizon Agent

Create a golden image for Windows Horizon desktops

Installing Horizon agent on Windows VMs

Prerequisites when installing Horizon agent on Linux VM

- Verify that the Linux guest operating system is prepared for desktop use

  See “Prepare a Linux Machine for Remote Desktop Deployment”

- Familiarize yourself with the Horizon Agent installer script for Linux.

  See install_viewagent.sh Command-Line Options.

Configuration Procedure when installing Horizon agent on Linux VMs

- Download the Horizon Agent for Linux installer file from the VMware download site
  - https://my.vmware.com/web/vmware/downloadsCreate a golden image for Windows and Linux Horizon desktops
  - VMware-horizonagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz for 64-bit Linux
  - y.y.y is the version number
  - xxxxxxx is the build number.
- Unpack the tarball
  - tar -xzvf VMware-horizonagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz
- Navigate to the tarball folder

Configuration Procedure when installing Horizon agent on Linux VMs

Run the install_viewagent.sh script as a superuser

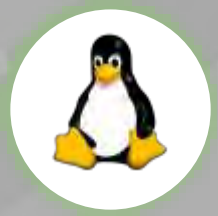
- See install_viewagent.sh Command-Line Options for a list of the optional parameters available for this script

Accept the EULA

Restart the Linux VM

Create a golden image for Windows and Linux Horizon desktops

- Create the Windows or Linux VM
- Optimize the VM
- Install Horizon Agent
- Install the Dynamic Environment Manager Agent or Microsoft FSLogix
  - Microsoft FSLogix for Office 365 Activation on Windows Desktops
- Script to optimize and shutdown Golden Image

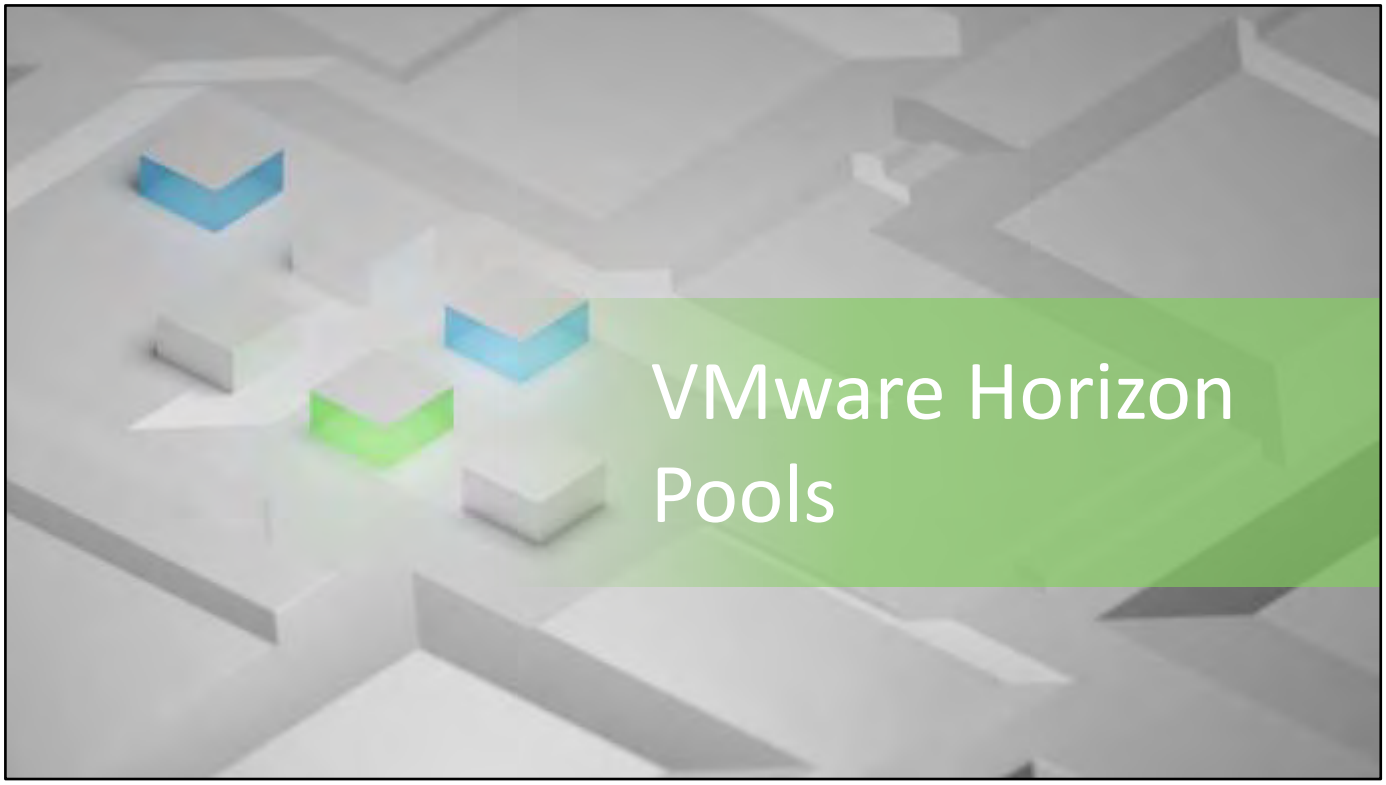


Conclusions

VMware Horizon Agent

Configuration choices when installing Horizon agent on Windows and Linux VMs

Create a golden image for Windows and Linux Horizon desktops



VMware Horizon Pools

Steps to set up a template for Instant-Clone desktop pool deployment

Steps to add desktops to the Horizon Connection Server inventory

Dedicated vs. floating-assignment pools

User entitlement

Hierarchy of global, pool, and user-level policies

Steps to Set Up an Instant-clone Template for Desktop Pool Deployment

Create a Golden Image VM

VM snapshot the Golden Image VM

Run the Add Pool Wizard

Entitling Users

Launching Remote Desktops

Demo

Set up an Instant-Clone template for desktop pool deployment

Steps to Add Desktops to the Horizon Connection Server Inventory

You will need the desktop (Endpoint) PC you wan to connect to

Install Horizon Client

- Will need user account with Administrator privileges to install

Address of the Connection Server to register the Endpoint PC to

Desktop pool

Dedicated vs. floating-assignment Pools

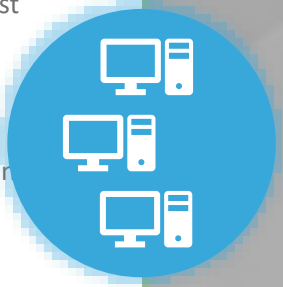
Dedicated Assignment

Desktops are statically assigned to a user, and that user gets the same desktop at each login.

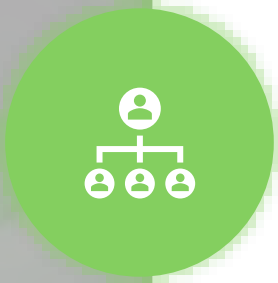
Dedicated Desktops can be assigned automatically the first time a user logs in or manually by an administrator

Floating Assignment

Desktops are assigned from the pool at login and then returned when the user signs out again



User Entitlement



Controls which remote desktops and applications users can access

Configure restricted entitlements feature

- Control desktop access based on the Horizon Connection Server instance
- Restrict access to a set of users outside the network from connecting to remote desktops and published applications within the network.

Hierarchy of global, pool, and user-level policies

- Global level policies
  - Affects all client sessions and users
- Pool level policies
  - Affects specific desktop pools
  - Takes precedence over global policy settings
- User level policies
  - Affects specific users
  - Takes precedence over global and desktop pool level policy settings
- Lower-level policy settings can be more or less restrictive than the equivalent higher-level settings.
  - Can set a global policy to Deny and the equivalent desktop pool-level policy to Allow, or vice versa

Demo

Configure user entitlement

Conclusions

VMware Horizon Pools

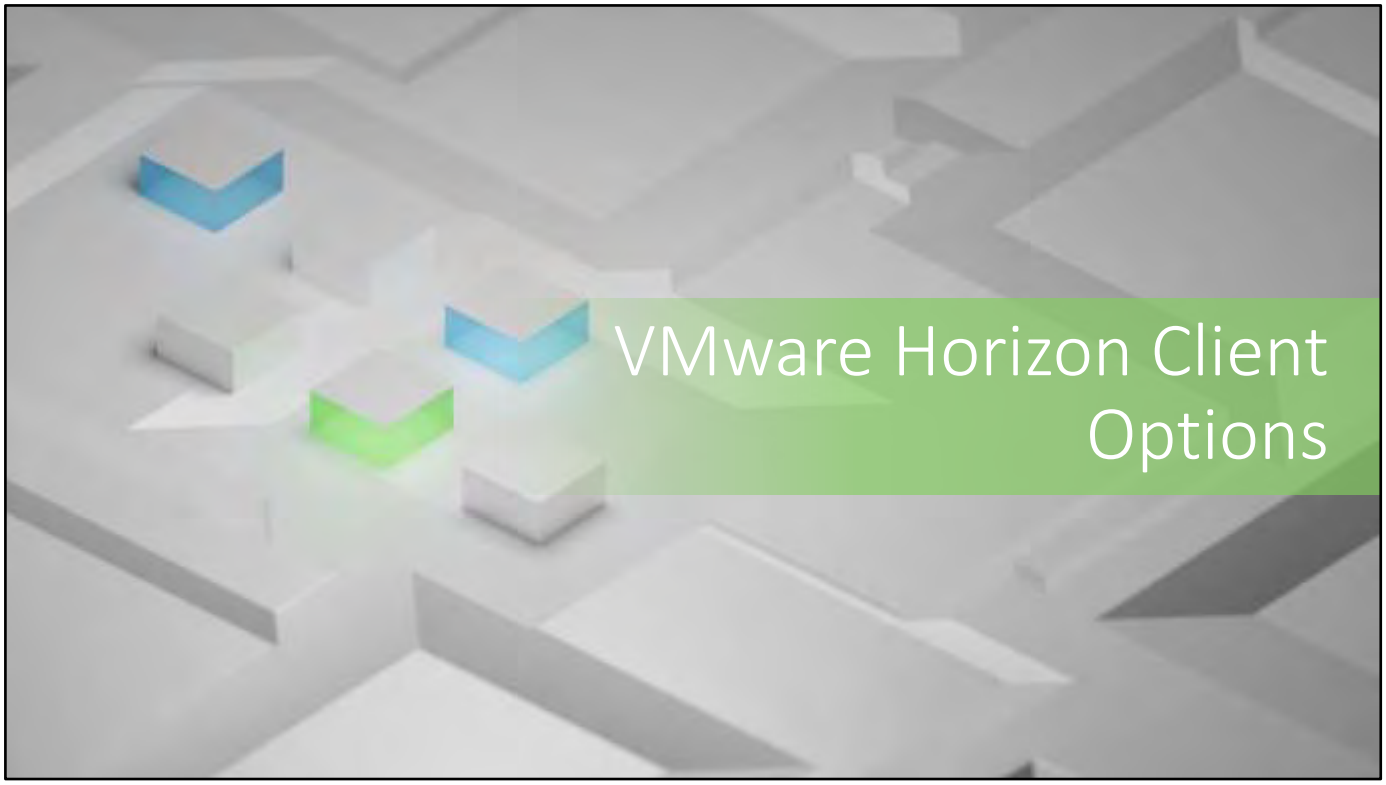
Steps to set up a template for Instant-Clone desktop pool deployment

Steps to add desktops to the Horizon Connection Server inventory

Dedicated vs. floating-assignment pools

User entitlement

Hierarchy of global, pool, and user-level policies



VMware Horizon Clients

- **Allows connection to your VMware Horizon virtual desktop from your chosen device**
- **Allows access from any were with internet access**
- **VMware Horizon Clients**

Windows	Chrome
Linux	Android
Mac	Thin clients
iOS	Zero clients

Comparing Different Clients

Horizon Client

Client software installed on a thick client to access VMware Horizon desktops

Thin clients

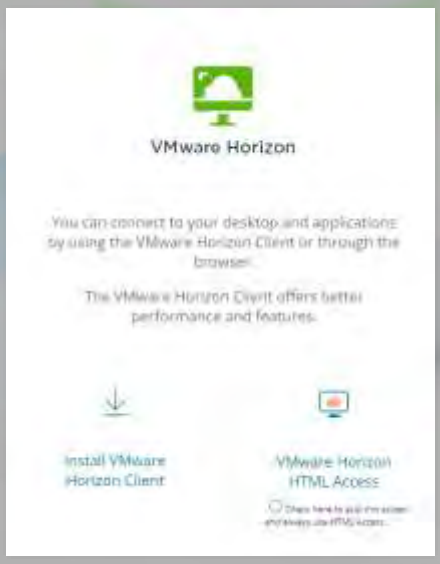
Minimal operating system

Zero clients

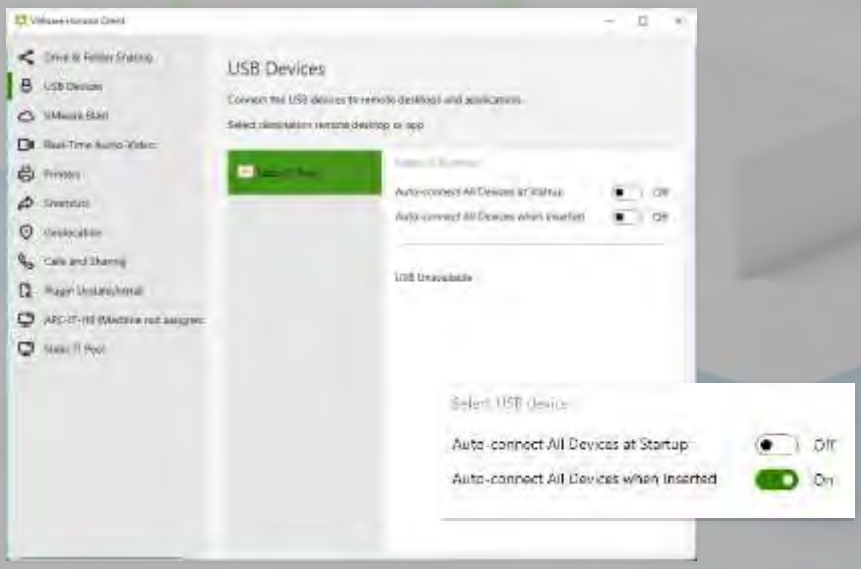
Configured to connect to one connection broker type.
- For example, VMware horizon or Citrix.

No hard disk or operating system

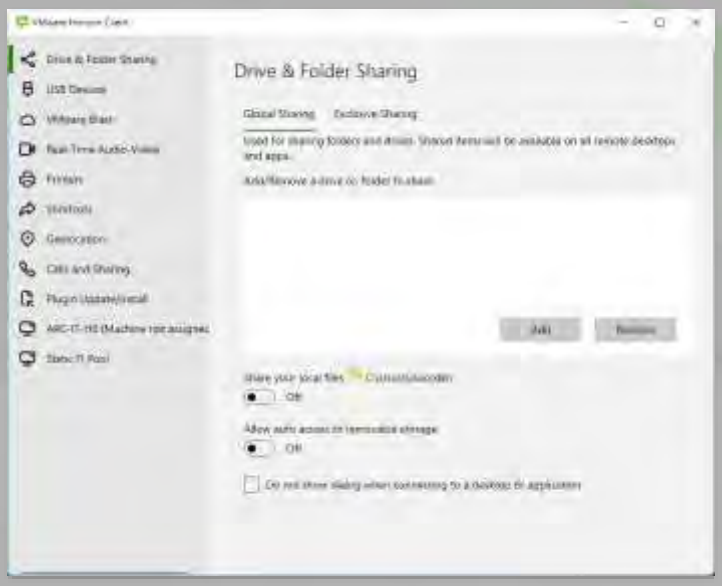
Access Horizon desktops using Horizon Clients or HTML



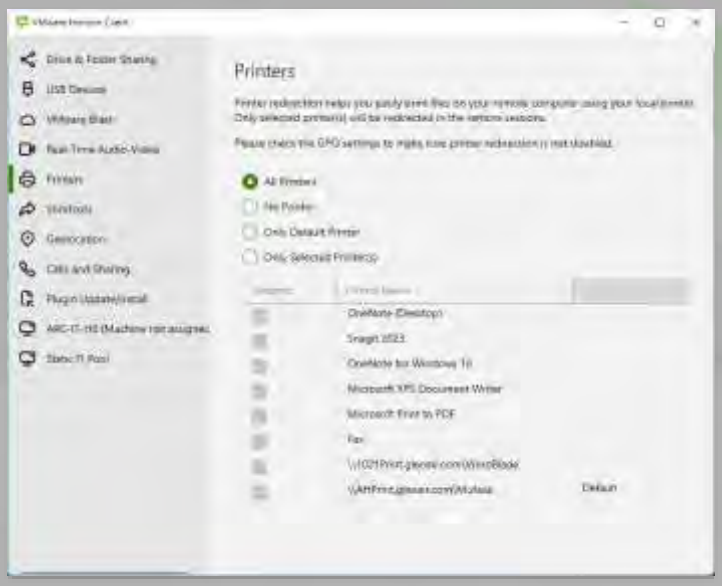
Setup USB Redirection



Setup Shared folders



Setup Integrated Printing



Demo

- Access Horizon desktops using Horizon Clients
- Setup USB Redirection
- Setup Shared folders
- Setup Integrated Printing

Microsoft Teams Session Optimization

Downside of making a video call from a virtual desktop

User's microphone and camera send the user's voice and image to the virtual desktop.

VMware Horizon® sends that data compressed, using our real-time audio-video (RTAV) feature

RTAV feature still sends a lot of data across the wire

The virtual desktop has to process the data and send it over the network to complete the call

The virtual desktop captures the video feed and sends it back over the network using the VMware Blast display protocol

Microsoft Teams Session Optimization cont.

VMware, with Microsoft, supports Media Optimization for Microsoft Teams

- Works with Horizon 8 (2006 and later) and Horizon 7 version 7.13
- When using a supported Horizon Agent and VMware Horizon Client versions
  - When a user starts a call inside the virtual desktop, a channel to the local physical device is opened and the call is started there

Horizon Client draws over the Microsoft Teams window in the virtual desktop VM

Gives users the impression that they are still in the VM

- The media is actually traveling directly between the local endpoint and the remote peer
- The load disappears from the network, and the processing moves from the data center to the endpoint
- The end-user experience can improves as well because the data has one less hop to make
- This process avoids using RTAV

Media Optimization for Microsoft Teams

Redirects audio calls, video calls, and viewing desktop shares

Provides a seamless experience between the client system and the remote session

Doesn’t negatively affecting the virtual infrastructure or overloading the network

Takes place on the client machine instead of in the virtual desktop

Does not rely on Real-Time Audio-Video (RTAV).

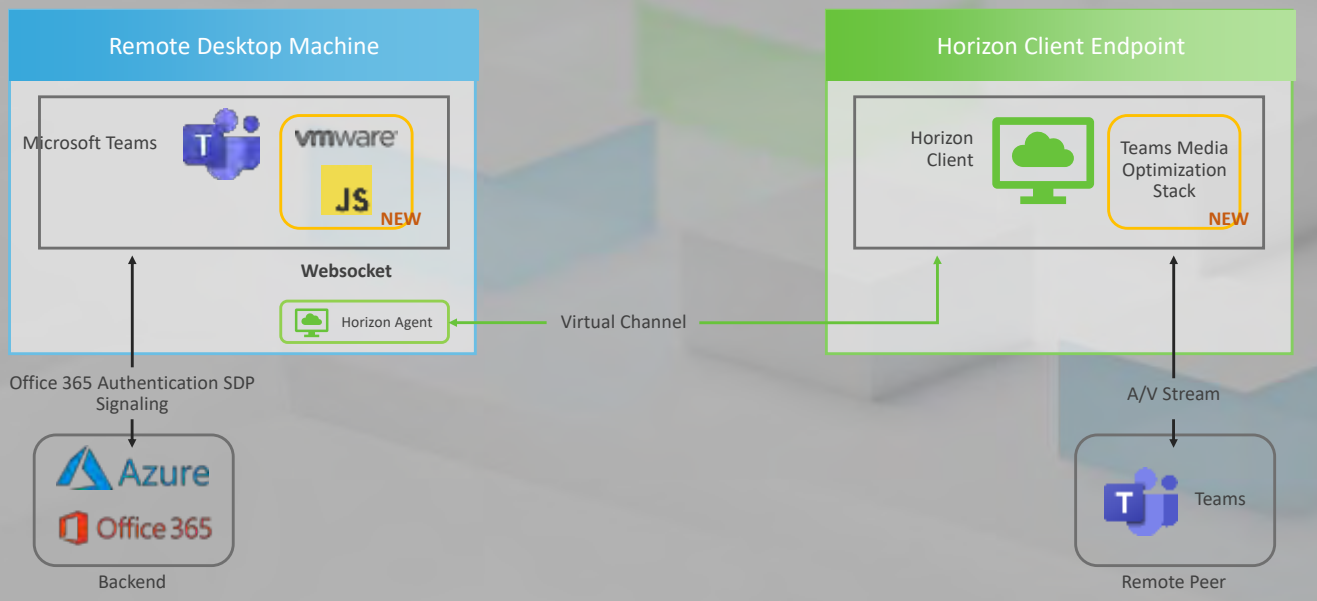
Media Optimization for Microsoft Teams

Horizon Client for Windows 2203 and earlier

Can see the setting if you select Customize installation in the installer

Horizon Client for Windows 2206 and later the feature is always installed

Media Optimization for Microsoft Teams



Conclusions

VMware Horizon Client Options

Comparing Different Clients

Access Horizon desktops using Horizon Clients or HTML

Setup USB Redirection

Setup Shared Folders

Setup Printer Redirection

Microsoft Teams Session Optimization

Media Optimization for Microsoft Teams

What Is VMware Dynamic Environment Manager

- Previously VMware User Environment Manager
- A software solution for configuring and deploying end-user desktop settings
- Provides personalization and dynamic policy configuration across any virtual, physical, or cloud-based Windows desktop environment
- Simplifies end-user profile management by giving you a lightweight, yet scalable solution that leverages your existing infrastructure
- Optimizes performance by replacing roaming profiles and eliminating complex difficult to maintain login scripts

Install VMware Dynamic Environment Manager

Login using an account with administrator privileges

Download and extract the MSI file package for your operating system

Run the MSI for your operating system

Read and accept the End User License Agreement and click Next

Select the destination folder where you want to install the application and click Next.

Best practice, install VMware Dynamic Environment Manager in the default folder

What Is VMware Dynamic Environment Manager

Select an installation option for VMware Dynamic Environment Manager

Typical

Custom

Complete

Click Install

After the installation is complete, click Finish.

Demo

Install VMware Dynamic Environment Manager

Configure VMware Dynamic Environment Manager

Configure FlexEngine by creating an Active Directory Group Policy Object (GPO) via VMware Dynamic Environment Manager administrative templates that are provided

Multiple FlexEngine configurations can be used by configuring multiple GPOs

- Test Dev
- Production

VMware Dynamic Environment Manager Flex Configuration Files

A Flex configuration file is created and manage by Management Console

Contains content specific for User Environment Manager

Each application has a separate Flex configuration file that contains the locations of the settings that are managed with User Environment Manager

VMware Dynamic Environment Manager Flex Configuration Files

Configuration templates are pre-configured Flex configuration files for popular applications

- Can download the available templates directly from VMware marketplace

Custom configuration files can be

- Created with Application Profiler
- Use Windows Common Settings
- Use an application template
- Only a single application template can be selected for a Flex configuration file, unless you use a Microsoft Office template
- Microsoft Office template select multiple application-specific templates simultaneously

Demo

Manage Dynamic Environment Manager Profiles in the DEM Console

- Download Configuration Templates
- Create a Flex Configuration File by Using an Application Template
- Create a Flex Configuration File by Using Windows Common Settings
- Export a Flex Configuration File to Another Location or Environment
- Import a Flex Configuration File From Another Location or Environment
- Create a Custom Flex Configuration File

Use the DEM Application Profiler

- Install the application you want to configure on your profiling system
- Log in to your profiling system as an administrator
- Start Application Profiler and click Start Session
- Browse to and select the application for which you want to create a Flex configuration file, Click OK
- The application is opened, and the Analyzing Application dialog box appears
- Change the application settings as necessary and close the application
- The locations for the application settings are saved as a Flex configuration file

Conclusions

VMware Dynamic Environment Manager

- What Is VMware Dynamic Environment Manager
- Install VMware Dynamic Environment Manager
- Configure VMware Dynamic Environment Manager
- VMware Dynamic Environment Manager Flex Configuration Files
- Demo - Manage Dynamic Environment Manager Profiles in the DEM Console
- Use the DEM Application Profiler

FSLogix

Enables a consistent experience for Windows user profiles in VDI environments

Can be used on physical desktops as well where a more portable user experience is needed

FSLogix provides:

- Roam user data between remote computing session
- Minimize sign in times for virtual desktop environments.
- Optimize file I/O between host/client and remote profile store.
- Provide a local profile experience, eliminating the need for roaming profiles.
- Simplify the management of applications and 'Gold Images'.

FSLogix cont.

Redirect user profiles to a “storage provider” or network share.

- Mounting and using the profile from a storage provider eliminates delays often associated with solutions that copy profiles to and from a network location.

Can redirect only the portion of the profile that contains Office1 data by using an ODFC container.

- The ODFC container allows the use of an alternate profile solution, such as vmware Dynamic Environment Manager, to enable Microsoft 365 applications in multi-session desktop environments

FSLogix cont.

- Many applications use the user's profile as if it were on the local disk.
  - FSLogix uses a filter driver to virtualize and redirect the profile at the file system level
  - Applications are unaware the profile is on the network
  - Obscuring the redirection is important because many applications wont work correctly with a profile stored remotely
- Profile containers used with Cloud Cache to provide high availability and disaster recovery profile solutions.
- Office application activation needs to happen only once for a user using an FSLogix ODFC container.
  - This is very useful in environments with dynamic Quick Clone desktop pools

FSLogix Eligibility

Users are eligible to use FSLogix if they have one of the following licenses:

- Microsoft 365 E3/E5
- Microsoft 365 A3/A5/ Student Use Benefits
- Microsoft 365 F1/F3
- Microsoft 365 Business
- Windows 10 Enterprise E3/E5
- Windows 10 Education A3/A5
- Windows 10 VDA per user
- Remote Desktop Services (RDS) Client Access License (CAL)
- Remote Desktop Services (RDS) Subscriber Access License (SAL)
- Azure Virtual Desktop per-user access license

FSLogix and Antivirus

Antivirus products are known to conflict with FSLogix containers and requires that specific files and folders are excluded from any type of scanning or heuristic

Check FSLogix documentation for the long list of directories and files to be excluded from your antivirus monitoring

Configure FSLogix Profile Containers

- Install FSLogix on the golden image for the Horizon Desktop
- Sign into the Horizon Desktop as a user with administrator privileges
- On the Horizon Desktop open Registry Editor and navigate to
  - HKEY_LOCAL_MACHINE\SOFTWARE\FSLogix\Profiles
- Make the needed changes to the Registry (on the following slide)
- Log out and sign back in as a standard user
- Open a Windows command prompt
- Change directory to C:\Program Files\FSLogix\Apps
  - Type “frx list-redirects”

Configure FSLogix Profile Containers cont.

Open file Explorer

In the address bar type the path from “VHDLocations” returned from running the command “frx list-redirect” at the command prompt

Double click the folder “%username%-%sid%”

Locate the VHDX container

Example Registery Changes for FSLogix Profile Container

Key Name	Data Type	Value	Description
Enabled	**DWORD**	**1**	**REQUIRED**
DeleteLocalProfileWhenVHDShouldApply1	DWORD	1	Recommended
FlipFlopProfileDirectoryName2	DWORD	1	Recommended
LockedRetryCount3	DWORD	3	Recommended
LockedRetryInterval3	DWORD	15	Recommended
ProfileType4	DWORD	0	Default
ReAttachIntervalSeconds3	DWORD	15	Recommended
ReAttachRetryCount3	DWORD	3	Recommended
SizeInMBs	DWORD	30000	Default
VHDLocations	**MULTI_SZ or REG_SZ**	**\\<storage-account-name>.file.core.windows.net\<share-name>**	**Example**
VolumeType5	REG_SZ	VHDX	Recommended

Configure FSLogix ODFC Containers (For Office Activation)

Install FSLogix on the golden image for the Horizon Desktop

Sign into the Horizon Desktop as a user with administrator privileges

On the Horizon Desktop open Registry Editor and navigate to

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\FSLogix\ODFC

Make the needed changes to the Registry (on the following slide)

Log out and sign back in as a standard user

Open a Windows command prompt

Change directory to C:\Program Files\FSLogix\Apps

Type “frx list-redirects”

Configure FSLogix ODFC Containers cont.

Open file Explorer

In the address bar type the path from “VHDLocations” returned from running the command “frx list-redirect” at the command prompt

Double click the folder “%username%-%sid%”

Locate the Profile and ODFC VHDX containers

Example Registery Changes for FSLogix ODFC Container

Key Name	Data Type	Value	Description
Enabled	**DWORD**	**1**	**REQUIRED**
FlipFlopProfileDirectoryName	DWORD	1	Recommended
IncludeTeams	DWORD	1	Recommended
LockedRetryCount	DWORD	3	Recommended
LockedRetryInterval	DWORD	15	Recommended
ReAttachIntervalSeconds	DWORD	15	Recommended
ReAttachRetryCount	DWORD	3	Recommended
SizeInMBs	DWORD	30000	Default
VHDLocations	**MULTI_SZ or REG_SZ**	\\<storage-account-name>.file.core.windows.net\<share-name>	**Example**
VolumeType	REG_SZ	VHDX	Recommended

Demo

Install and Configure FSLogix

Conclusions

Microsoft FSLogix Office Container

What is FSLogix

FSLogix Eligibility

FSLogix and Antivirus

Configure FSLogix Profile Containers

Configure FSLogix Configure ODFC containers

Clones

Full Clone

Instant-clone

Instant-clone advantages

Provisioning technology for instant-clone desktop pools

Instant-clone automated pool setup

Pushing updated images to instant-clone desktop pools

Full Clone

A complete and independent copy of the original template VM

An automated desktop pool that contains full-clone virtual machines

Create a virtual machine template

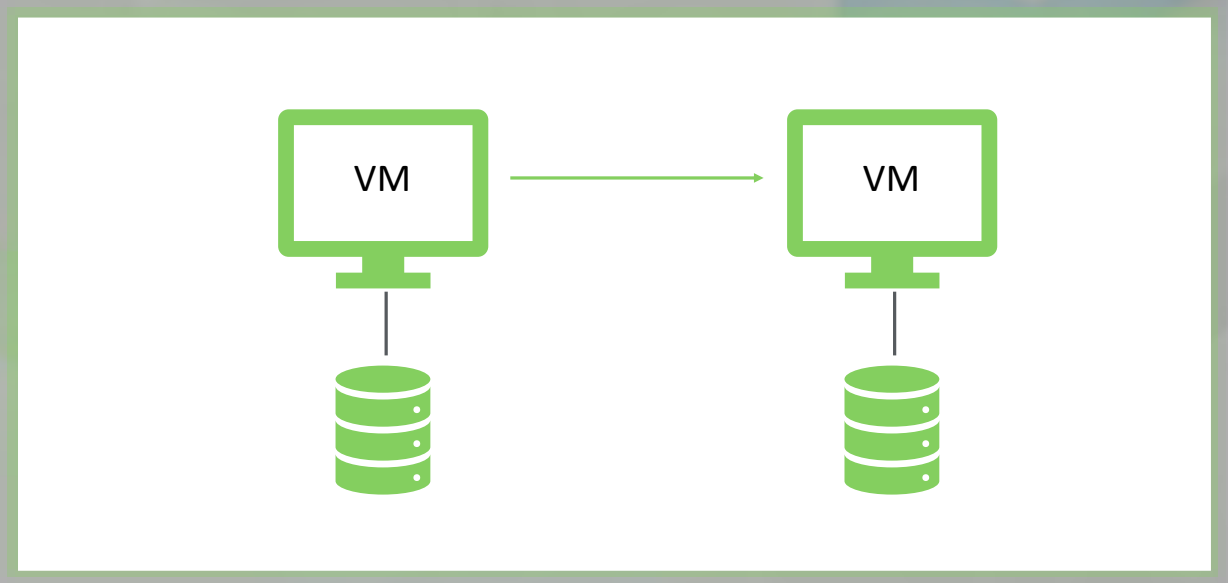
Horizon uses that template to create full clone, disk independent virtual machines

Once the clone is created it is a fully independent virtual machine.

Can be customized with additional applications and VM configuration

Uses the MOST resources such as disk and memory

Full Clones



Instant-clone

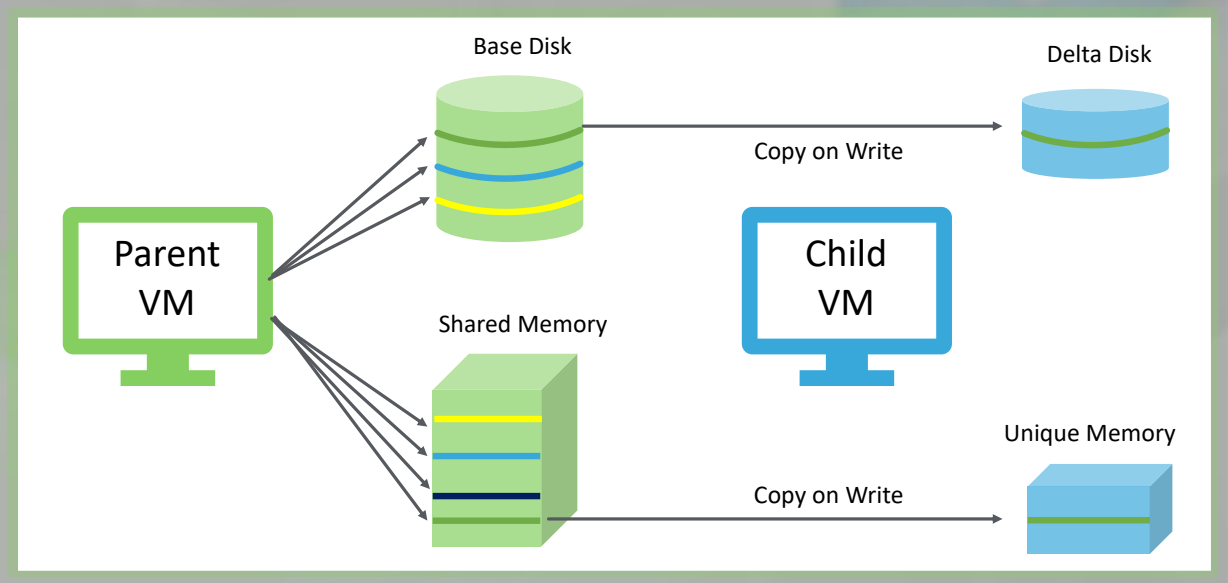
An instant copy of a running virtual machine

The Instant clone shares the same virtual hard disk as the parent with a delta file, or difference file, for copy on write operations.

Instant clones also use the same shared memory that the parent VM does with the same Copy-on-write technology, but for memory

More like containerized virtualization then linked clones that only share the base hard disk

Instant Clones



Instant-clone Advantages

- Use fewer resources
  - Memory
  - Hard disk
- Faster desktop deployment
- Simplified management
  - OS Patching
  - Application updates/upgrades
- Do not need to be refreshed, recomposed, or rebalanced
  - When users logs out of Instant-clones, the clone gets deleted and recreated from the latest patch

Provisioning technology for instant-clone desktop pools

Created from a golden image using the vmFork technology (instant clone API) in vCenter Server.

Creates several types of internal VMs to manage the instant clones in a more scalable way

- Internal Template
- Replica VM
- Parent VM

Use of a parent VM improves the provisioning speed, it also **increases** the memory requirement across the cluster

When the benefit of having more memory outweighs the increase in provisioning speed, Horizon 8 automatically chooses to provision instant clones directly from a replica VM without creating a parent VM

This is called Smart Provisioning

Smart Provisioning creates Instant Clones by either

- Instant clones with parent VM
- Instant clones without parent VM

Instant clones are created in a powered-on state

Instant-clone Advantages

Instant-clone Automated Pool Setup

Select Inventory > Desktops

Click Add

Select Automated Desktop Pool and click Next

Select Instant Clones, select the vCenter Server instance, and click Next

Follow the rest of the prompts to create the pool

Demo

Create an Instant-clone automated pool

Pushing Updated Images to Instant-clone Desktop Pools

Prepare a new golden image and snapshot with the operating system image and/or applications updates installed.

Schedule a push-image operation with the updated golden image and snapshot

When the push-image operation starts

- Horizon 8 deletes unused old instant-clone desktops and creates new instant clones using on the new image

Old instant-clone desktops that are in-use are undisturbed

- When the user logs out, Horizon 8 deletes the old instant clone and recreates a new instant clone using the updated image

Pushing Updated Images to Instant-clone Desktop Pools

In Horizon Console, select Inventory > Desktops

Click the pool ID

On the Summary tab, click Maintain > Schedule

The Schedule Push Image window opens

On the Image step, select the snapshot to use.

- The default image for the pool is already selected

On the Schedule step, select the Schedule image push option.

- You can schedule the task to start immediately or sometime in the future
- For clones with user sessions, you can specify whether to force the users to log out or to wait
- When the users log out, Horizon 8 recreates the clones.

On the Ready to Complete step, click Finish.

Demo

Pushing updated images to instant-clone desktop pools

Conclusions

Clones

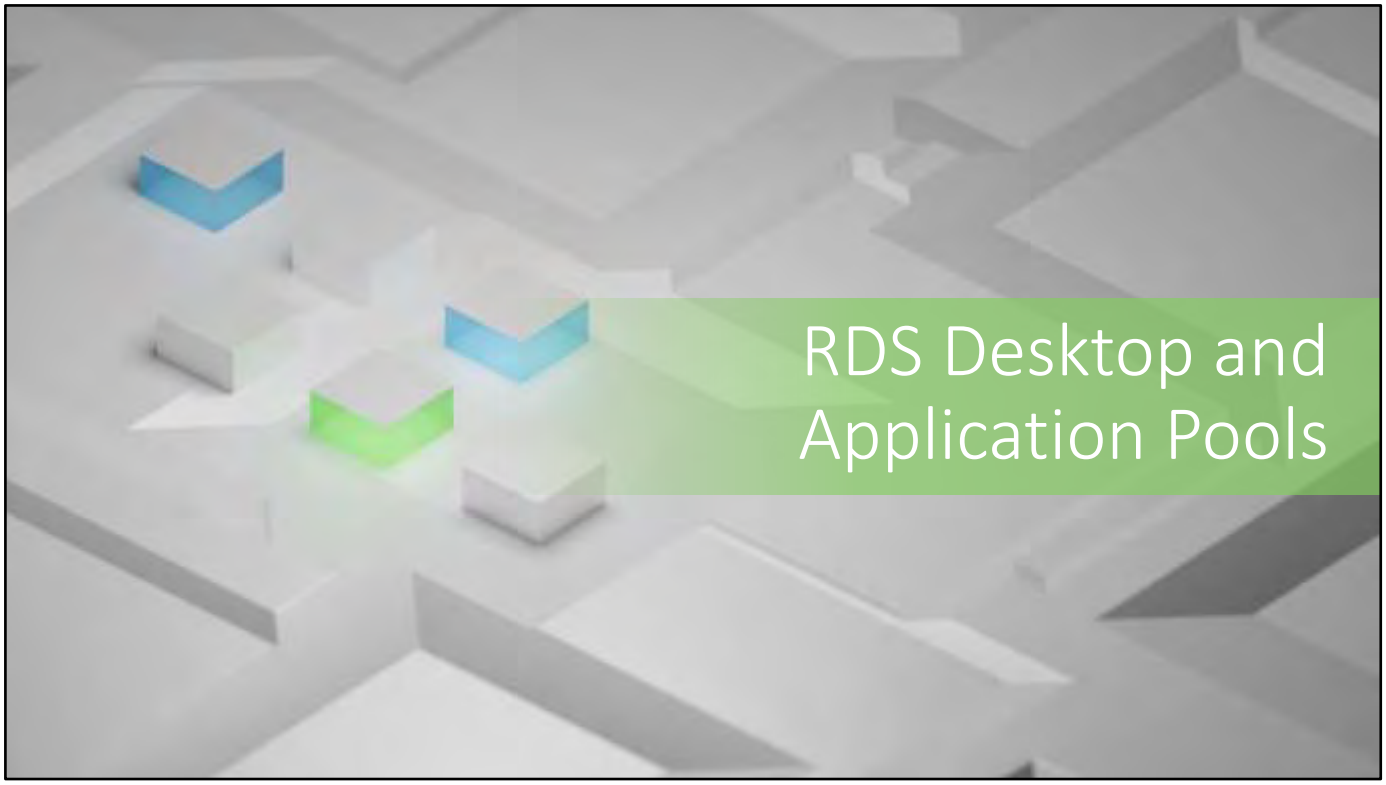
What are clones

Full Clones

Instant Clones

Provisioning technology for instant-clone desktop pools

Pushing updated images to instant-clone desktop pools



RDS Desktop and Application Pools

RDS Desktop and Application Pools

- RDS desktop pool vs automated pool
- RDS session host pool vs. farm vs. application pool
- Create RDS desktop and application pools - Demo
- Accessing RDS desktops and applications from Horizon Client - Demo
- Using instant-clone to automate RDSH farm building
- Setup load-balancing for RDSHs on a farm - Demo

RDS desktop pool

An RDS desktop pool is a group of RDS hosts or a RDS farm

An RDS host is a Windows server running the RDS role that can host multiple RDS desktop sessions

An RDS desktop is based on an RDP session on an RDS host.

RDS desktop pool vs automated pool

An RDS desktop is based on an RDP session on an RDS host

Multiple other users sessions could be sharing the same operating system, installed applications and server resources

A desktop in an automated desktop pool is based on a virtual machine

Each desktop in an automated desktop pool has a unique operating system, applications, and resources for that user session

A desktop in a manual desktop pool is based on a fully unique and independtent virtual or physical machine

RDS session host pool vs. RDS Farm

RDS hosts are Windows servers that have Windows Remote Desktop Services role and Horizon Agent installed

RDS hosts provide users access to applications that users can access remotely

RDS Farms are collections of RDS hosts

RDS Farms facilitate the management of RDS hosts

RDS Farms provide a common set RDS published desktops and applications to users

Application pool

Application pools are published applications that run on a farm of RDS hosts

Let you deliver seamless applications to many users that run on servers in a data center instead of on their personal desktops

When you create an RDS application pool you specify a RDS farm

Demo

Create RDS Desktop

Demo

Create Application Pools

Demo

Accessing RDS desktops and applications from Horizon Client

Using instant-clone to automate RDSH farm Creation

Create golden image for RDSH

Horizon creates a farm of RDS hosts using the golden image

Can update all hosts in farm from a single central image

Do not store any data locally on the farm VMs

- Data will be lost on image update
- Data should be stored on remote file shares using DEM or FSLogix

Demo

Setup load-balancing for an RDSHs farm

Conclusions

RDS Desktop and Application Pools

RDS desktop pool vs automated pool
RDS session host pool vs. farm vs. application pool
Accessing RDS desktops and application pools
Using instant-clone to automate RDSH farm Creation
Setup load-balancing for RDSHs on a farm

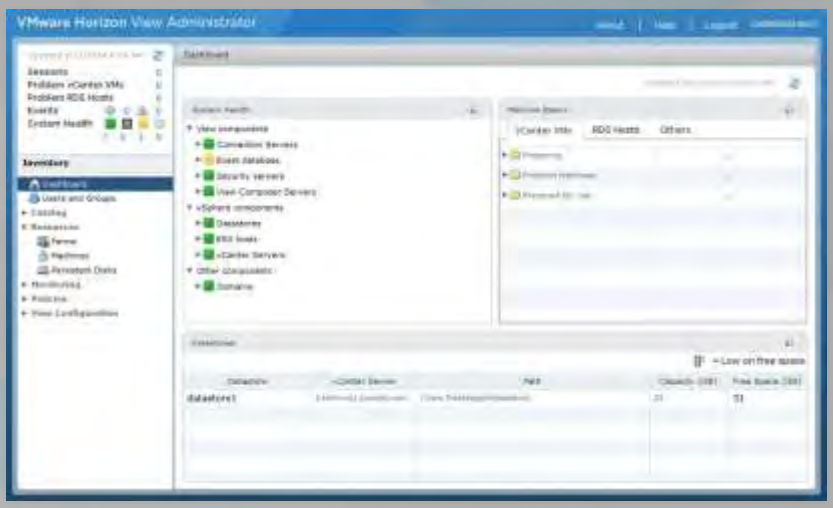
Horizon Monitoring

- Using Horizon Administrator console dashboard
- Monitoring desktop sessions with the HelpDesk tool
- Using Horizon Performance Tracker to monitor remote desktop performance

Using Horizon Administrator console dashboard

- Using Horizon Administrator console dashboard

Horizon Administrator console dashboard



Demo

- Using Horizon Administrator console dashboard

Monitoring desktop sessions with the HelpDesk tool

- Monitoring desktop sessions with the HelpDesk tool

Demo

- Monitoring desktop sessions with the HelpDesk tool

Using Horizon Performance Tracker to monitor remote desktop performance

- Using Horizon Performance Tracker to monitor remote desktop performance

Demo

Horizon Performance Tracker

Conclusions

Horizon Monitoring

Using Horizon Administrator console dashboard

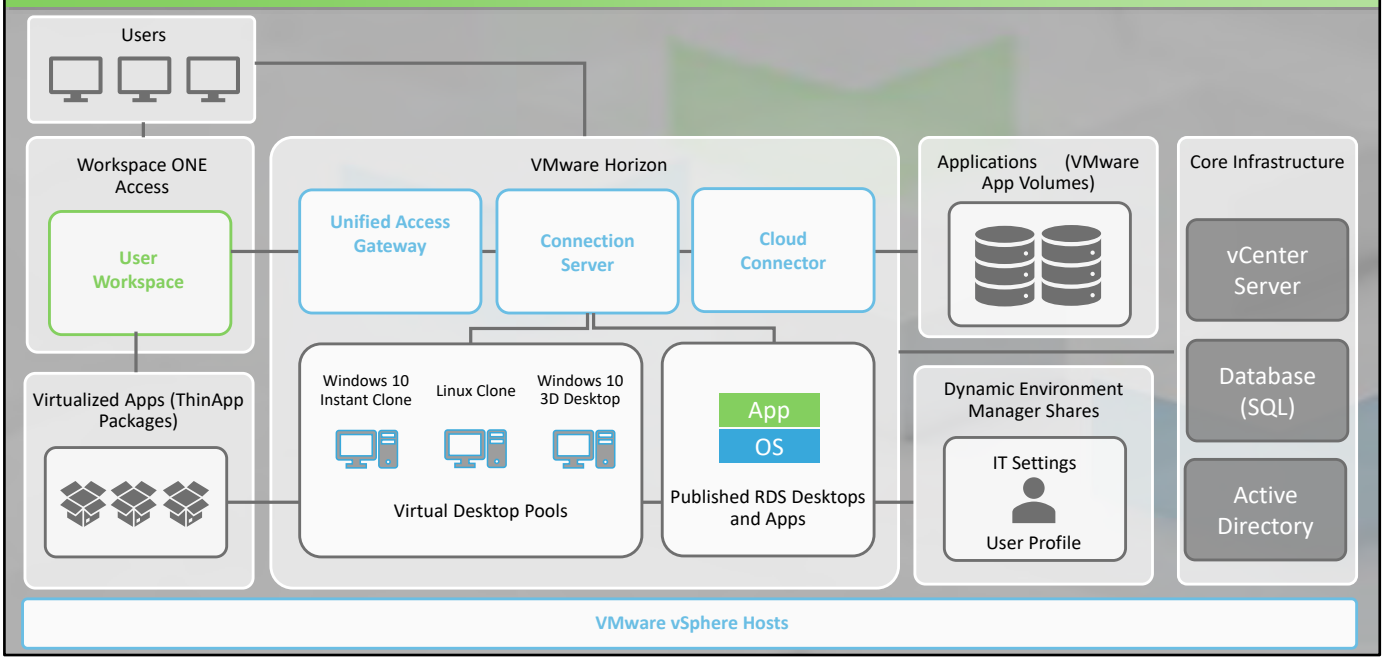
Monitoring desktop sessions with the HelpDesk tool

Using Horizon Performance Tracker

Horizon Connection Server

- Horizon reference architecture
- Horizon Connection Server features
- Horizon Connection Server system requirements
- Setup Horizon event database
- Initial Horizon Connection Server configuration
- AD LDS database with Horizon Connection Server
- True SSO

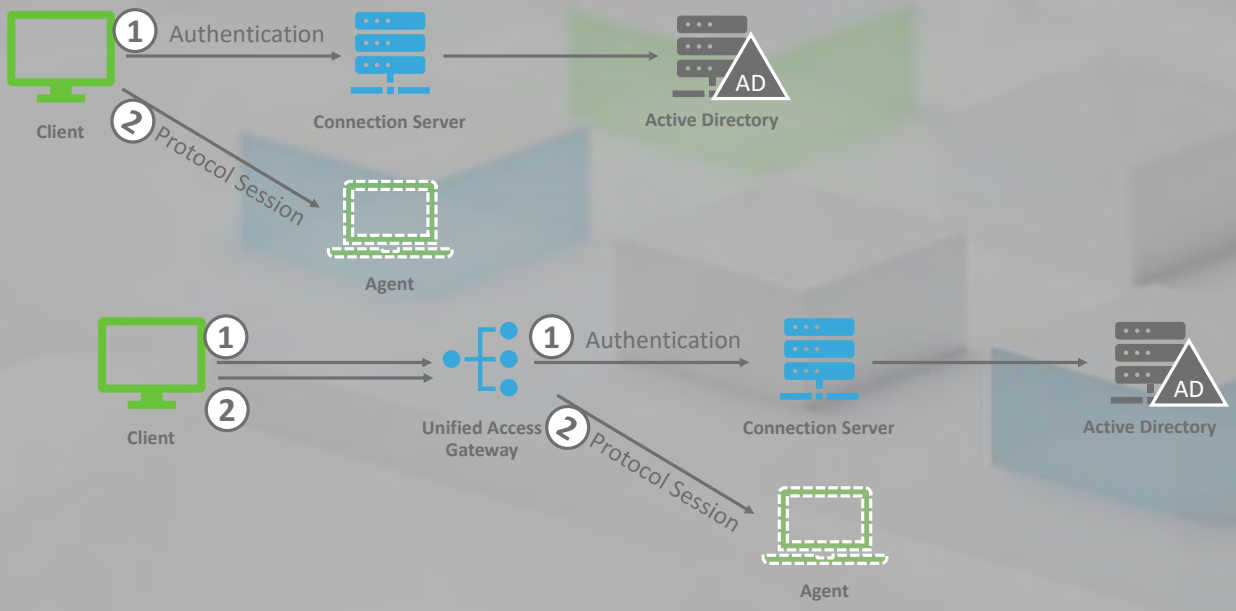
Horizon Reference Architecture



Horizon Connection Server Features

- **Acts as a broker for client connections**
- **Authenticates users through Windows Active Directory**
- **Directs the request to the**
  - Virtual machine
  - Physical PC
  - Microsoft RDS host
- **Assigning applications packaged with VMware ThinApp to specific desktops and pools**
- **Establishing secure connections between users and remote desktops and applications**
- **Enabling single sign-on**
- **Setting and applying policies**

Horizon Authorization



Horizon Connection Server Hardware Requirements

Hardware Component	Required	Recommended
Processor	Pentium IV 2.0GHz processor or higher	4 CPUs
Memory	4GB RAM or higher	At least 10GB RAM for deployments of 50 or more remote desktops
Network Adapter	100Mbps NIC	1Gbps NICs

Horizon Connection Server Software Requirements

Operating System	Supported Editions	Supported Horizon versions
Windows Server 2012 R2	Standard Datacenter	Horizon 8 2006 and later
Windows Server 2016	Standard Datacenter	Horizon 8 2006 and later
Windows Server 2019	Standard Datacenter	Horizon 8 2006 and later
Windows Server 2022	Standard Datacenter	Horizon 8 2111 and later

Setup Horizon Event Database

In Horizon Console,

- Settings > Event Configuration.

In the Event Database section,

- click Edit
- enter the information in the fields provided
- click OK

To clear the event database information

- click Clear

In the Event Settings window (Optionally)

- Click Edit
- Change the length of time to show events and the number of days to classify events as new
- click OK

Verify that the connection to the event database is successful

- Monitoring > Events

Initial Horizon Connection Server Configuration

- Start the Connection Server installation program
- Accept the VMware license terms
- Accept or change the destination folder
- Select the Horizon Standard Server installation option
- Make sure that Install HTML Access is selected if you intend to allow users to connect to their desktops by using a Web browser
- IPv4 is selected by default
  - If IPv6 is not displayed, it is because HTML Access is not supported in an IPv6 environment
  - Horizon 8 components with the same IP version must be selected
- Select whether to enable or disable FIPS mode
  - This option is available only if FIPS is enabled in Windows
- Type a data recovery password and optional password reminder.
  - A data recovery password is required when you recover a backup of Connection Server
- Choose how to configure the Windows Firewall service
  - Configure Windows Firewall automatically
  - Do not configure Windows Firewall

Initial Horizon Connection Server Configuration

- Authorize a Horizon Administrators account
  - Authorize the local Administrators group
  - Authorize a specific domain user or domain group
- Choose whether to participate in the customer experience improvement program
- Select where you want to deploy Connection Server
  - General
  - AWS
  - DELL/EMC
  - Azure
  - Google
  - Oracle Cloud
- Click Install to complete the wizard and install Connection Server
- Run Windows Update as needed

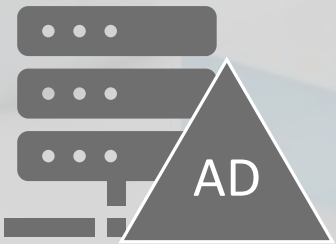
AD LDS Database

Active Directory Lightweight Directory Services (AD LDS)

ADAM LDAP in previous versions

An independent mode of Active Directory, minus infrastructure features

That provides directory services for applications



AD LDS Database With Horizon Connection Server

From View Connection Server computer

Start the ADSI Edit utility

- Via PowerShell
- Start Menu Folder (Windows Administrative Tools)
- Added as a snapin to an mmc console

In the console tree launched for ADSI Edit

- select Connect to

Enter connection settings into the dialog box to connect into the Local Horizon View Database

- In the Select or type a Distinguished Name or Naming Context text box
- dc=vdi, dc=vmware, dc=int
- If you are unable to connect try using dc=vdi;dc=vmware;dc=int

In the Select or type a domain or server text box

- localhost:389
- Or the fully qualified domain name (FQDN) of the View Connection Server computer followed by port 389
- example localhost:389 or mycomputer.mydomain.com:389

Click OK

True SSO

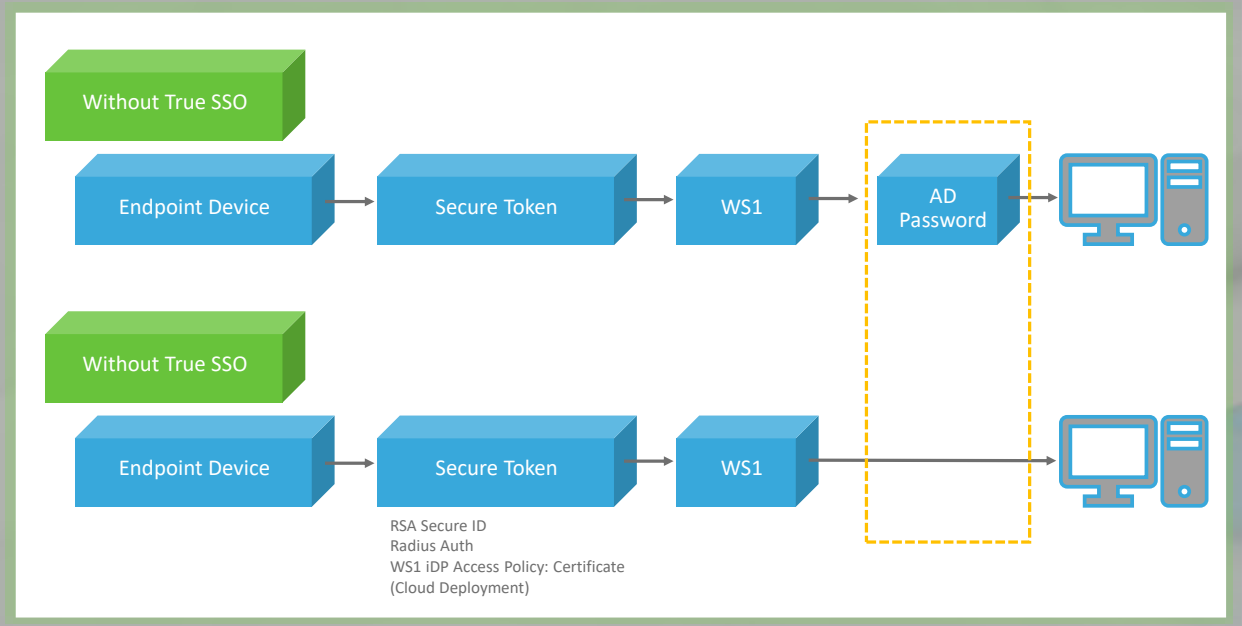
After users log in to VMware Workspace ONE Access using

- A smart card
- RSA SecurID
- RADIUS authentication
- Third-party identity provider using a Unified Access Gateway appliance
- Users are not required to also enter Active Directory credentials

If a user authenticates by using Active Directory credentials the True SSO feature is not necessary

- Can configure True SSO to be used even in this case
- The AD credentials that the user provides are ignored and True SSO is used

True SSO



Conclusions

Horizon Connection Server

Horizon reference architecture

Horizon Connection Server features

Horizon Connection Server system requirements

Setup Horizon event database

Initial Horizon Connection Server configuration

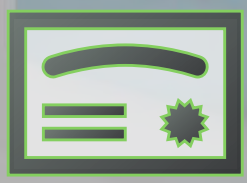
AD LDS database with Horizon Connection Server

True SSO

Authentication and Certificates

Authentication and Certificates

- Supported authentication options
- Importance of certificates in Horizon Connection Server
- Supported Smartcard authentication options
- Installing and configuring Horizon Connection Server certificates
- Creating Horizon administrator and custom roles
- Configure Horizon Connection Server for True SSO
- Roles available in Horizon



Supported authentication options

Uses existing Active Directory infrastructure for user authentication and management

Can also integrate with two-factor authentication solutions

RSA SecurID
RADIUS
Smart card authentication solutions

Supported Smartcard authentication options

A smart card

A small plastic card embedded with a computer chip

Example Common Access Card (CAC) used by many government agencies and large enterprises

Client connections that use smart card authentication, are TLS/SSL enabled

Client machines must have smart card middleware and a smart card reader installed

Creating Horizon administrator

In Horizon Console

- Settings > Administrators

On the Administrators and Groups tab

- Click Add User or Group.
- Click Add
- Select one or more search criteria
- Click Find to filter Active Directory users or groups based on your search criteria

Select the Active Directory user or group that you want to be an administrator user or group

- Click OK
- click Next

Press the Ctrl and Shift keys to select multiple users and groups

Select a role to assign to the administrator user or group

Demo

Creating Horizon administrator

Creating Horizon Custom Roles

In Horizon Console

Settings > Administrators.

On the Role Privileges tab

click Add Role.

Enter a name and description for the new role

Select one or more privileges
Click OK

Demo

Creating Horizon Custom Roles

Roles available in Horizon

- Administrators
- Global Configuration and Policy Administrators
- Help Desk Administrators
- Inventory Administrators
- Local Administrators
- Agent Registration Administrators

- Administrators (Read only)
- Global Configuration and Policy Administrators (Read only)
- Help Desk Administrators (Read Only)
- Inventory Administrators (Read only)
- Local Administrators (Read Only)

Demo

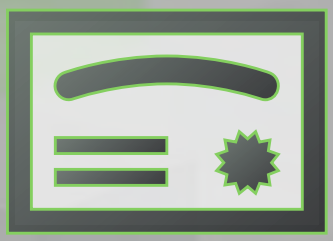
View Roles available in Horizon

Importance of certificates in Horizon Connection Server

TLS server certificates are required for client connections to

Client-facing Connection Server instances

Intermediate servers that terminate TLS connections

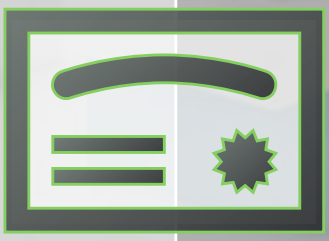


Certificates in Horizon Connection Server Installation

Connection server installation generates a self-signed certificate

The installation uses an existing certificate if

- A valid certificate with a Friendly name of vdm already exists in the Windows Certificate Store
- Upgrading to VMware Horizon 8 from an earlier release and a valid keystore file is configured on the Windows Server computer
- The installation extracts the keys and certificates
- Imports them into the Windows Certificate Store



Installing Horizon Connection Server certificates

The Horizon Connection Server is installed on a Windows Server

Installing a certificate for a Horizon Connection Server is installing a certificate on a Windows Server

- Open an MMC console
- Add the Certificate Snap-In to MMC the MMC console
- Import a Signed Server Certificate into a Windows Certificate Store
- Modify the Certificate Friendly Name (vdm)
- Import the Root Certificate and Intermediate Certificates into the Windows Certificate Store

Demo

Installing Horizon Connection Server certificates

Prerequisites to Configure Horizon Connection Server for True SSO

- Login with a user account with administrator privileges
- Insure you have the fully qualified domain name (FQDN) for the following servers
  - Connection Server
  - Enrollment server
  - Enterprise certificate authority
- Insure you have the Netbios name or the **FQDN** of the domain
- Insure you have created a certificate template
- Insure you have created a SAML authenticator to delegate authentication to VMware Workspace ONE Access

Configure Horizon Connection Server for True SSO

Installing and configuring True SSO

Add an enrollment server to the global list

On a Connection Server in the cluster, open a command prompt and enter the command to add an enrollment server

```
vdmUtil --authAs admin-role-user --authDomain domain-
name --authPassword admin-user-password --truesso --
environment --add --enrollmentServer enroll-server-fqdn
```

Enter the command to list the information for that enrollment server

```
vdmUtil --authAs admin-role-user --authDomain domain-
name --authPassword admin-user-password --truesso --
environment --list --enrollmentServer enroll-server-fqdn
--domain domain-fqdn
```

Configure Horizon Connection Server for True SSO

Enter the command to create a True SSO connector, which will hold the configuration information, and enable the connector

```
vdmUtil --authAs admin-role-user --authDomain domain-name --
authPassword admin-user-password --truesso --create --
connector --domain domain-fqdn --template TrueSSO-template-
name --primaryEnrollmentServer enroll-server-fqdn --
certificateServer ca-common-name --mode enabled
```

Enter the command to discover which SAML authenticators are available

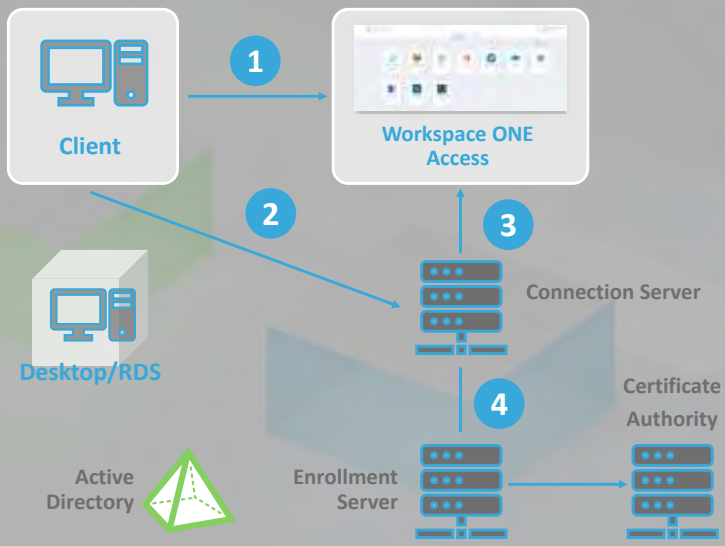
```
vdmUtil --authAs admin-role-user --authDomain domain-name --
authPassword admin-user-password --truesso --list --
authenticator
```

Configure Horizon Connection Server for True SSO

Enter the command to enable the authenticator to use True SSO mode.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --
authPassword admin-user-password --truesso --authenticator --
edit --name authenticator-fqdn --truessoMode {ENABLED|ALWAYS}
```

True SSO for Horizon Connection Server



Conclusions

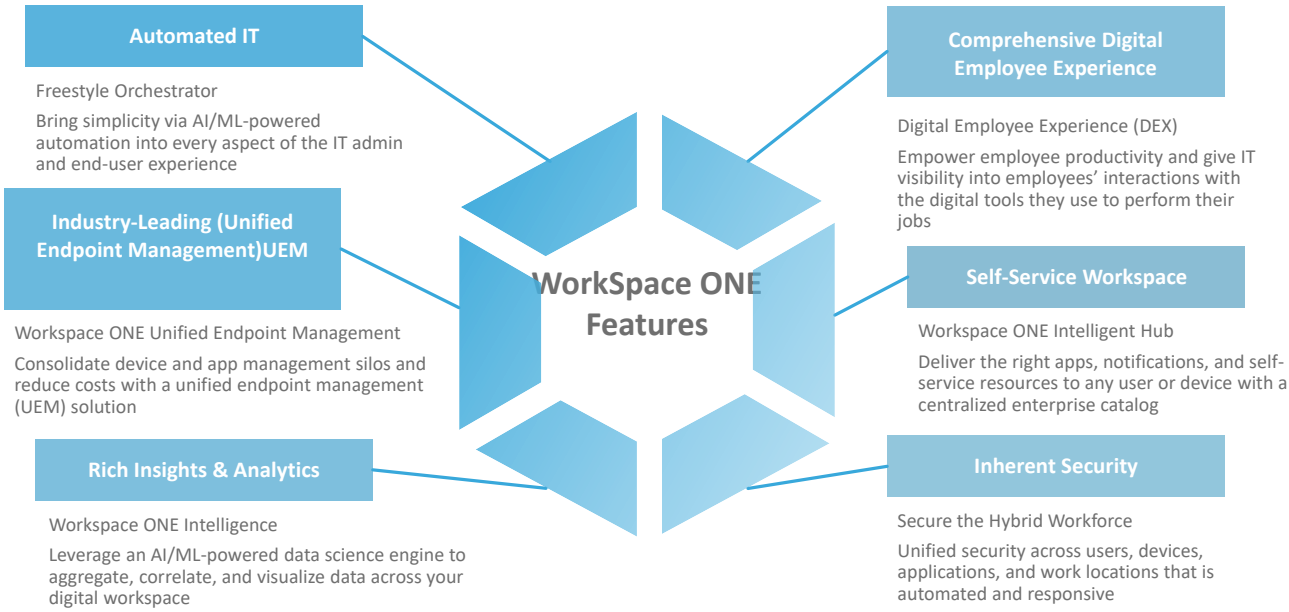
Authentication and Certificates

- Supported authentication options
- Supported Smartcard authentication options
- Creating Horizon administrator and custom roles
- Roles available in Horizon
- Importance of certificates in Horizon Connection Server
- Installing and configuring Horizon Connection Server certificates
- Configure Horizon Connection Server for True SSO

WorkSpace ONE

- Features and benefits
- Console features
- Identity management
- Access management
- Directory integration
- Deploying virtual applications using Workspace services

WorkSpace ONE



Workspace ONE Console Features

Dashboards

Device tab

- Summary of information regarding the device
- Is the device in compliance
- Device serial number

Profiles tab

- All the policies and configurations pushed down to a device
- Click a profile name for additional information on a specific profile

Apps tab

- A listing of all the applications installed on the device
- Different options available for the different applications

Workspace ONE Console Features

Multi-tenant Architecture

Uses organization groups to be able to customize your environment to match your organization's structure

Production / Test Dev

Execs / HR / Sales

Roles Based Access

Help Desk Users can have only certain privileges to certain organizational groups

Admins can have full access to the full organization

Demo

WorkSpace ONE Console

Workspace ONE Access Management

Brokering Between Identity Stores and Providers

Bridge between AD, ADFS, AAD, Okta, Ping and others to deliver a seamless user experience without rearchitecting your identity environment

Integrated Password-less Authentication and Single Sign-On

Reduce the risk of security breaches with password-less MFA integrated directly into Workspace ONE Intelligent Hub

Single-Sign-on to mobile, SaaS, web and virtual apps improves security, reduces helpdesk calls and improves user experience

Risk Based Conditional Access

Establish trust between users, devices and apps for a seamless user experience

Easily enable dozens of access policy combinations that leverage Workspace ONE device enrollment, network and SSO policies, automated device remediation and 3rd party information.

Cloud Hosted

Available as a hosted solution to dramatically reduce implementation time and maintenance overhead with a VMware managed Workspace ONE Access tenant

Demo

WorkSpace ONE Access management

Workspace ONE Directory Integration

Can integrate enterprise directories

- Sync users and groups

Integrates with

- Active Directory
- LDAP directories such as OpenLDAP

Syncs a limited number of user and group attributes

- Specified by the administrator
- User passwords and other attributes not specified by the administrator are not synced

Directory Sync service is required for directory integration

Workspace One Virtual Apps Collections

Provide end users access to resources from the Workspace ONE Intelligent Hub app or portal

Web applications

VMware Horizon applications and desktops

Applications and desktops running on

- Horizon Cloud Service on Microsoft Azure with Single-Pod Broker
- Horizon Cloud Service on IBM Cloud
- Citrix-published applications and desktops
- ThinApp packaged applications with Workspace ONE Access

Requires installing the Virtual App service

- Component of the Workspace ONE Access connector

Prerequisites to Deploying Virtual Applications Using Workspace Services

Install the Virtual App service, a component of the Workspace ONE Access connector

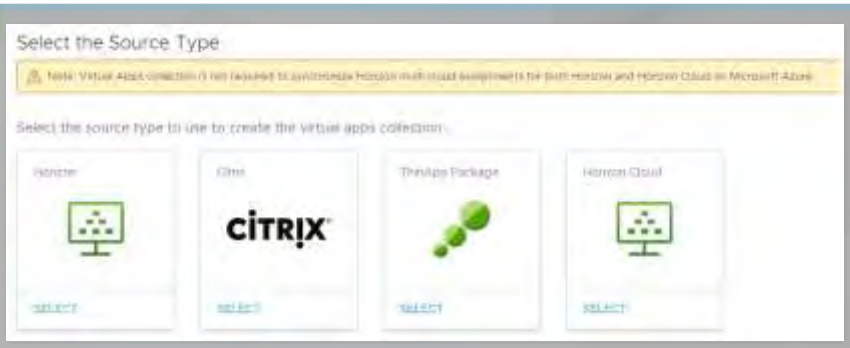
Login with a user account with the correct administrative privilege

Create Virtual Applications Using Workspace Services

Select Resources > Virtual Apps Collections

If an information page appears, review the information and click Get Started, otherwise click New

Select the type of resource to integrate



Create Virtual Applications Using Workspace Services

Follow the New Collection wizard to create the collection

The steps for each type of integration is different and requires different configuration information

- Horizon on premises integration
- Horizon Cloud integration
- ThinApp integration
- Citrix integration

Conclusions

WorkSpace ONE

Features and benefits

Console features

Identity management

Access management

Directory integration

Deploying virtual applications using Workspace services

Display Protocols

- Blast vs PCoIP
- BLAST Display Protocol Codec
- BLAST Codec option summary
- BLAST Codec ideal applications
- BLAST and PCoIP ADMX GPO configuration

Horizon 8 Remote display protocols Blast Extreme

- Used with the HTML Access client, when using the HTML Access feature
- Used with a remote Linux desktop
- Optimized for mobile cloud
- Lowest CPU consumption for longer battery life
- Compensates for an increase in latency or a reduction in bandwidth
- Can use either TCP and UDP network transports
- Additional performance counters displayed using PerfMon on Windows
- Connections to headless machines are supported with NVIDIA graphics cards

Horizon 8 Remote display protocols Blast Extreme and PCoIP

- VPN or Unified Access Gateway supported
- Advanced Encryption Standard (AES) 128-bit encryption by default
  - Can change the encryption key cipher to AES-256
- 32-bit color for virtual displays
- ClearType fonts support
- Audio redirection and Real-Time Audio-Video on some clients
- Copy and paste of text and, on some clients' images
- Multiple monitors are supported for some clients
- USB redirection is supported for some clients
- MMR redirection
  - On some Windows client operating systems and some remote desktop operating systems with Horizon Agent installed

BLAST Display Protocol Codecs

JPG/PNG

- Ideall for typical Windows and Linux applications
- Good at reproducing intricate fonts and screen content with fine details
- Such as still images and low-motion 3D modeling

Blast Codec

- Similar to JPG/PNG
- Used less CPU and network bandwidth
- Designed to support not just typical Windows and Linux apps, but also SaaS applications, line-of-business apps like Point of Sale, and any that require low-motion, high-quality graphics support such as CATIA, Photoshop, and AutoCAD

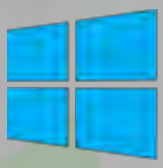
BLAST Display Protocol Codecs

- H.264
  - Most common codec in the world
  - Designed specifically to support entertainment content
  - Use in encoding Blu-ray movies
  - Requires more processing power to perform its encoding and decoding operations
  - Processing can be offloaded from the CPU to graphics cards (GPU)
- HEVC (High Efficiency Video Coding or H.265)
  - Provides up to 50% better compression, the same quality as H.264
  - Reduction in the network bandwidth required, similar to CPU
  - Uses substantially more CPU to encode and decode
  - Requires that the ESXi hosts have NVIDIA Tesla or newer GPUs to offload its encoding

BLAST Display Protocol Codec

- Improves on Adaptive and on H.264 encoders
- Delivers sharper images and fonts
- Operates like a video codec
  - Motion detection
  - Motion vectors
  - Inter-predicted macroblocks
- Supported on Windows and Linux
- Disabled by default

Enable BLAST Display Protocol Codec



Windows

Set the registry key

HKLM\SOFTWARE\VMware, Inc.\Vmware Blast\Config\EncoderBlastCodecEnabled = 1

Linux

\etc\vmware\config

set RemoteDisplay.allowBlastCodec=TRUE

BLAST Codec option summary

H.264 with High Color Accuracy

Encoder Switch

Offloading H.264 and H.264 with High Color Accuracy to an NVIDIA GPU

HEVC with High Dynamic Range (HDR) Encoding

BLAST Codec ideal applications

Codec	Ideal Applications
JPG/PNG	Typical productivity applications such as Microsoft Office, plus those requiring support for fine details and higher still image quality
Blast Codec	Typical productivity applications such as Microsoft Office, plus those requiring support for fine details and higher still image quality
PNG (Build-to-Lossless)	Applications requiring lossless reproduction of original screen content such as non-diagnostic medical imaging
H.264	Multimedia applications such as streaming video, video games, and productivity applications with rapidly changing content
H.264 with High Color Accuracy (HCA)	Applications that require higher color quality or that exhibit lack of clarity with H.264 alone
Encoder Switch: JPG/PNG and H.264	Same applications as for the JPG/PNG codec and the H.264 codec
Encoder Switch: Blast Codec and H.264	Same applications as for the Blast Codec and the H.264 codec

BLAST Codec ideal applications

Codec	Ideal Applications
Encoder Switch: JPG/PNG and H.264 with HCA	Same applications as for the JPG/PNG codec and the H.264 with HCA codec
Encoder Switch: Blast Codec and H.264 with HCA	Same applications as for the Blast Codec and the H.264 with HCA codec.
High Efficiency Video Coding (HEVC)	Applications that require the same quality as H.264 with less bandwidth utilization or that require higher quality with similar bandwidth utilization as H.264
HEVC with High Dynamic Range (HDR) Encoding	Applications that require higher graphical quality with improved color range and contrast, such as digital photography
NVIDIA Encoded H.264 (H.264 Offloaded to GPU)	Same applications that are ideal for H.264 while offloading the encoding from the ESXi host CPUs to an NVIDIA GPU
NVIDIA H.264 with HCA	Same applications that are ideal for H.264 with HCA while offloading the encoding from the ESXi host CPUs to an NVIDIA GPU

BLAST and PCoIP ADMX GPO configuration

Many codec options and Blast Extreme settings are controlled by administrators in the Windows Registry

Codec Options can be configured

- In the Windows Registry with Registry Editor
- GPO

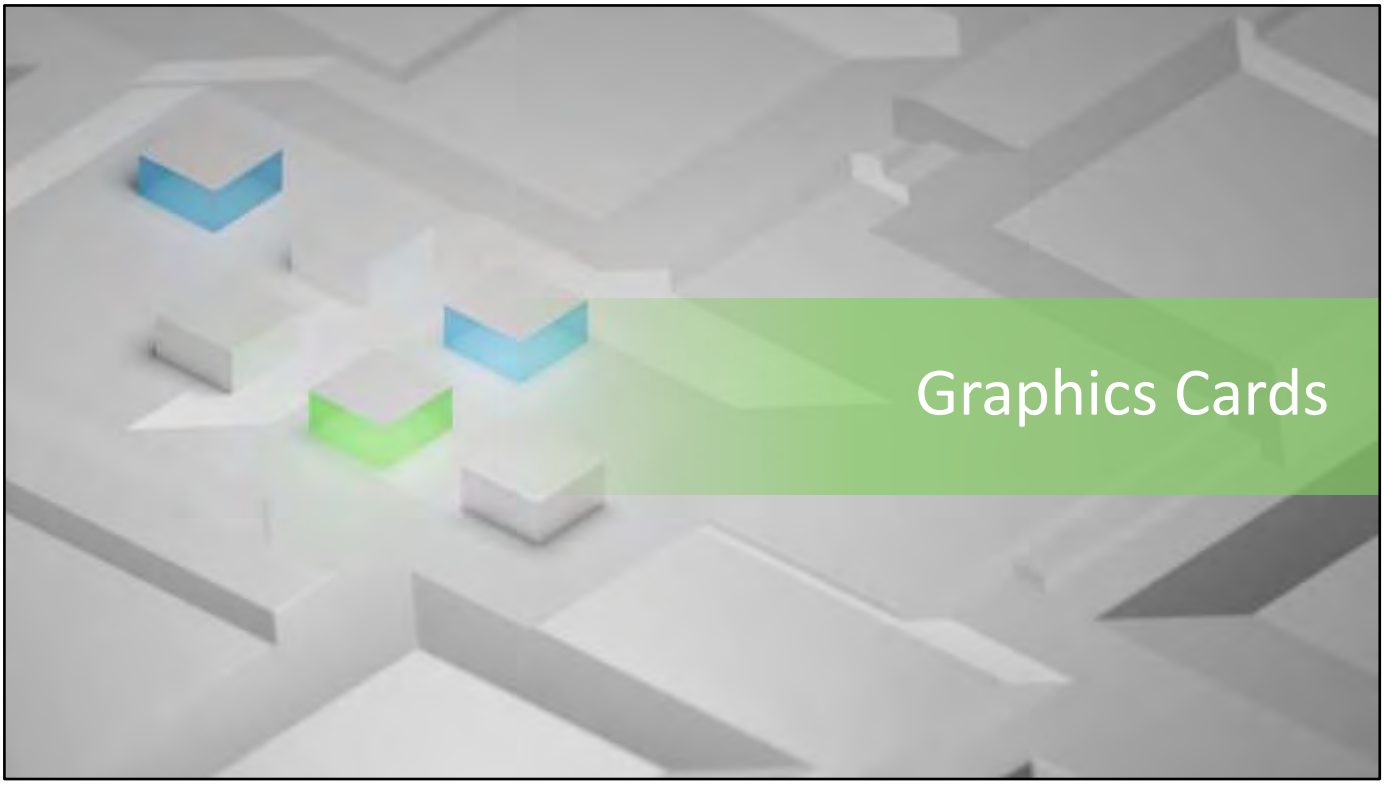
Windows Group Policy template provided with VMware Horizon

- The Blast Extreme template is named: vdm_blast.admx
- In the VMware-Horizon-Extras-Bundle-xxx.zip file (xxx indicating Horizon version)

Conclusions

Protocols

- Display
- Remote display
- BLAST
  - Codecs
- PCOIP ADMX GPO



Graphics Cards

- 3D Rendering Options Full-Clone Desktop Pool
- 3D Rendering Options Instant-Clone Desktop Pool
- vSGA vs vDGA

3D Rendering Options Full-Clone Desktop Pool

Before you attempt to create desktop pools in Horizon Console you must configure in the vSphere Client

- Virtual Shared Graphics Acceleration (vSGA)
- Virtual Dedicated Graphics Acceleration (vDGA)
- AMD MxGPU
- NVIDIA GRID vGPU

3D Rendering Options Full-Clone Desktop Pool

Six 3D Renderer Options in Horizon Console

Manage using vSphere Client

- 3D Renderer option is set in vSphere Web Client for a virtual machine
- Horizon 8 does not control 3D rendering
- Configure VRAM for 3D Guests, Max number of monitors, and Max resolution of any one monitor settings are inactive in Horizon Console

Automatic - 3D rendering is enabled

- ESXi host reserves GPU hardware resources on a first-come, first-served basis at VM powered on
- If no GPU hardware resources are available when a VM is powered on software renderer is used

3D Rendering Options Full-Clone Desktop Pool

Software - 3D Rendering is Enabled

Uses software 3D graphics rendering

Any GPU graphics cards installed on the ESXi host will not be used

Use this setting to configure Soft 3D

Hardware - 3D Rendering is Enabled

Reserves GPU hardware resources on a first-come, first-served basis as VM are powered on

If a user tries to connect to a Desktop when all GPU hardware is reserved the VM will not power on

If a VM is vMotion to an ESXi host that does not have GPU hardware configured, the VM will not power on.

This setting is an option when configuring vSGA

3D Rendering Options, NVIDIA GRID vGPU Full-Clone Desktop Pool

NVIDIA GRID vGPU - 3D rendering is enabled for NVIDIA GRID vGPU

Reserves GPU hardware resources on a first-come, first-served basis as VM are powered on

If a connection is attempted to a VM when all GPU hardware resources are being used by other VMs on the host,

Connection Server will attempt to move the VM to another ESXi host

Use this setting when configuring NVIDIA GRID vGPU.

The virtual machine cannot be suspended or resumed

VMs can not be powered on powered hosts with out GPU hardware in a cluster with hosts with NVIDIA GRID vGPU enabled

All ESXi hosts in the cluster must be version 6.0 or later

All VMs must be hardware version 11 or later

If an ESXi cluster contains a host that is NVIDIA GRID vGPU enabled and a host that is not, the hosts display a yellow (warning) status in the Horizon Console Dashboard

Demo

Configuring 3D Rendering Options in a Full-Clone Desktop Pool

3D Rendering Options Instant-Clone Desktop Pool

- Horizon 8 does not directly control settings for 3D rendering of an instant-clone pool as it does with full-clone pools
- 3D settings are configure using the vSphere Client in the ESXi hosts, and then in your golden image
- Instant-clone VMs will inherit those settings from the golden image
- Horizon Console will display some of the settings configured, but cannot edit or interact with those settings

Demo

Configuring 3D Rendering Options in an Instant-Clone Desktop Pool

vSGA vs vDGA

Virtual Shared Graphics Acceleration (vSGA)

Allows multiple virtual machines to share the physical GPUs

Suitable for mid-range 3D design, modeling, and multimedia applications.

Virtual Direct Graphics Acceleration (vDGA)

Assigns a dedicated Nvidia GPU to the VDI desktop reserving the entire GPU

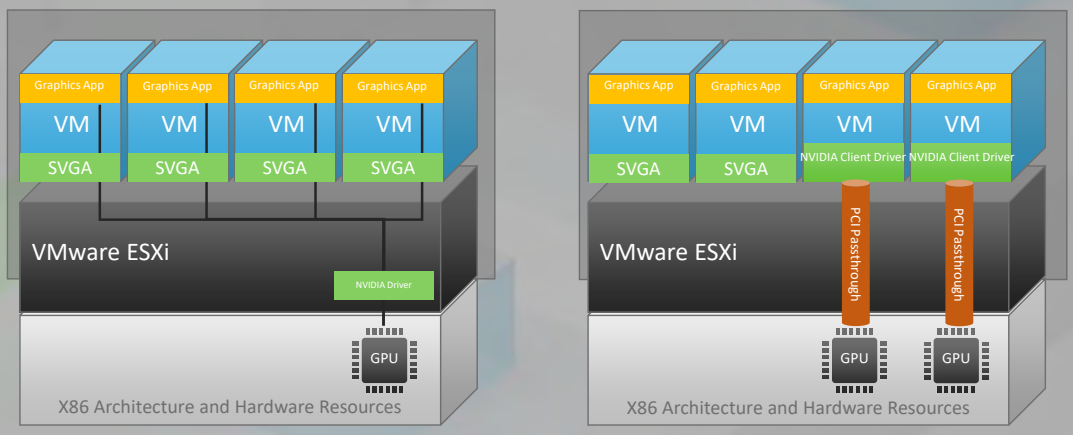
Number of desktops per ESXi host is limited to the number of Nvidia graphics adapters in the host

Uses VMware DirectPath I/O, so vMotion, DRS, and HA are not supported

Uses the Nvidia graphics drivers instead of the VMware SVGA 3D driver

Cannot live switch between software or hardware acceleration

vSGA vs vDGA



Conclusions

Graphics Cards

3D Rendering Options Full-Clone Desktop Pool

3D Rendering Options Instant-Clone Desktop Pool

vSGA vs vDGA

Scalability

- Multiple Horizon Connection Server Instances
- Horizon 8 Pod
- Unified Access Gateway
- Horizon Cloud Pod Architecture

Multiple Horizon Connection Server Instances

- One or more additional instances of Connection Server replicate an existing Connection Server instance
  - The existing and newly installed instances of Connection Server are identical
- VMware Horizon 8 copies the Horizon LDAP configuration data from the existing Connection Server instance to the new replica and identical Horizon LDAP configuration data is maintained on all Connection Server instances
- When a change is made, the updated information is copied to the other instances
- In case of an instance failure
  - The other instances in the group continue to operate
  - When the failed instance resumes activity, its configuration is updated with the changes that took place during the outage.

Multiple Horizon Connection Server Instances

The replica server software cannot coexist with any other VMware Horizon 8 software component including

- Horizon Agent
- Horizon Client

When the current Connection Server instance is in a different domain than the replicated instance, the domain user installing the replica needs to also have Administrator privileges on the computer where the existing instance redides

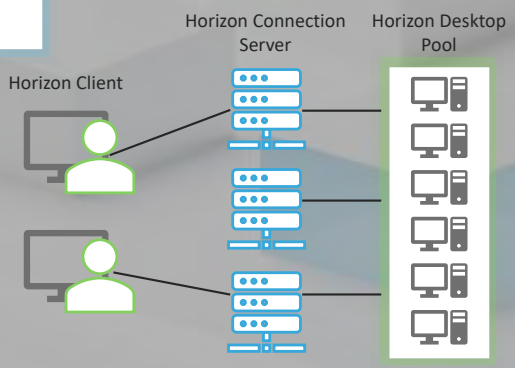
When installing replicated Horizon Connection Server instances, configure the instances in the same high speed L2 network and broadcast domain

- ie IP subnet
- To use a group of replicated Connection Servers across a routed network you must use the Cloud Pod Architecture feature

Replica connection server purpose

Provide high availability

Provide load balancing



Horizon 8 Pod

A Horizon 8 pod is

- Set of Connection Server instances
- Shared storage
- Database server
- vSphere
- Network infrastructures

In a traditional Horizon 8 implementation you manage each pod independently

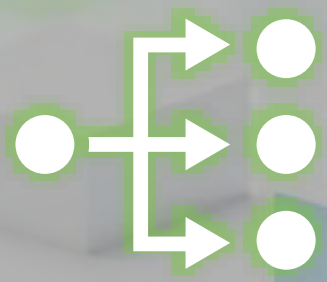
A Cloud Pod Architecture, you can join together multiple pods to form a single Horizon 8 implementation called a pod federation

Unified Access Gateway

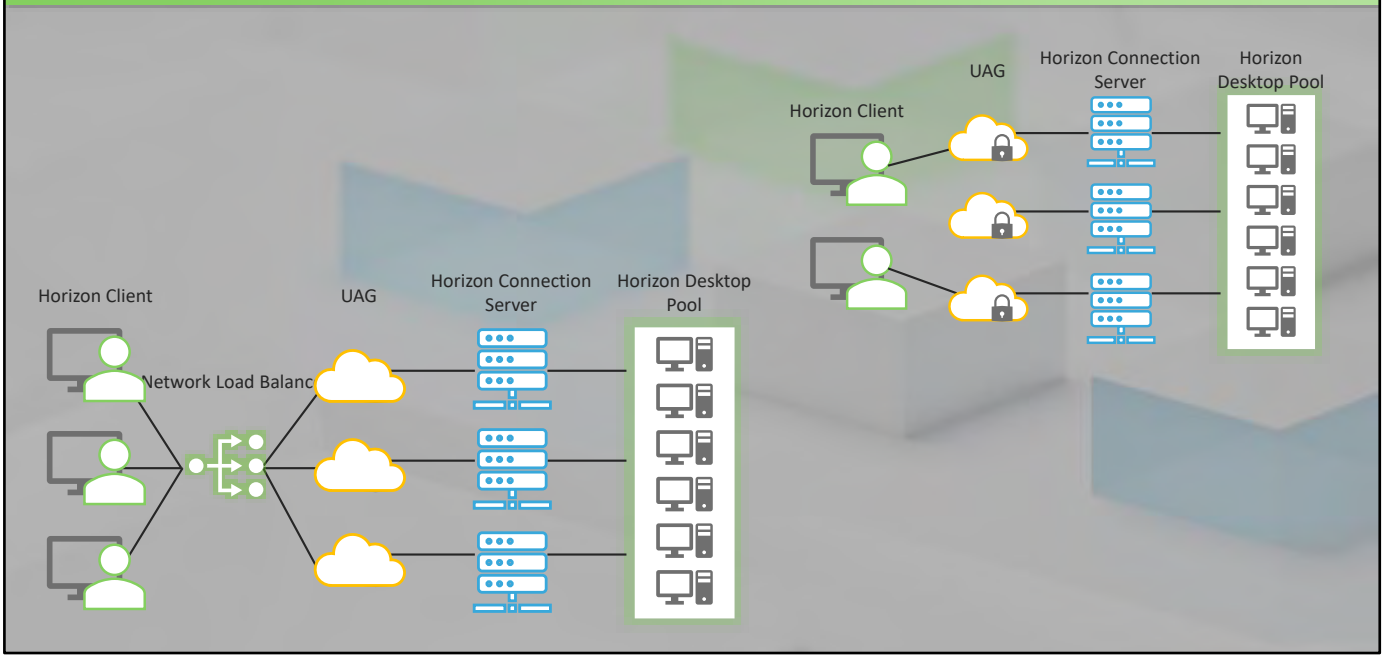
Load-balancer

Deployed in a demilitarized zone (DMZ).

Directs authentication requests to the appropriate server and discards any unauthenticated request to ensure restricted resource access



Unified Access Gateway



Horizon 8 Cloud Pod Architecture

Link together multiple pods to create a single desktop and application brokering and management environment

Multiple Pods linked together is called a Pod Federation

Can span multiple sites and data centers

Simplifies the administration of large-scale deployments

Unified Access Gateway appliances is associated with a single pod

Horizon 8 Cloud Pod Architecture

The Global Data Layer is setup on each Connection Server instance in a pod federation when you initialize the Cloud Pod Architecture feature

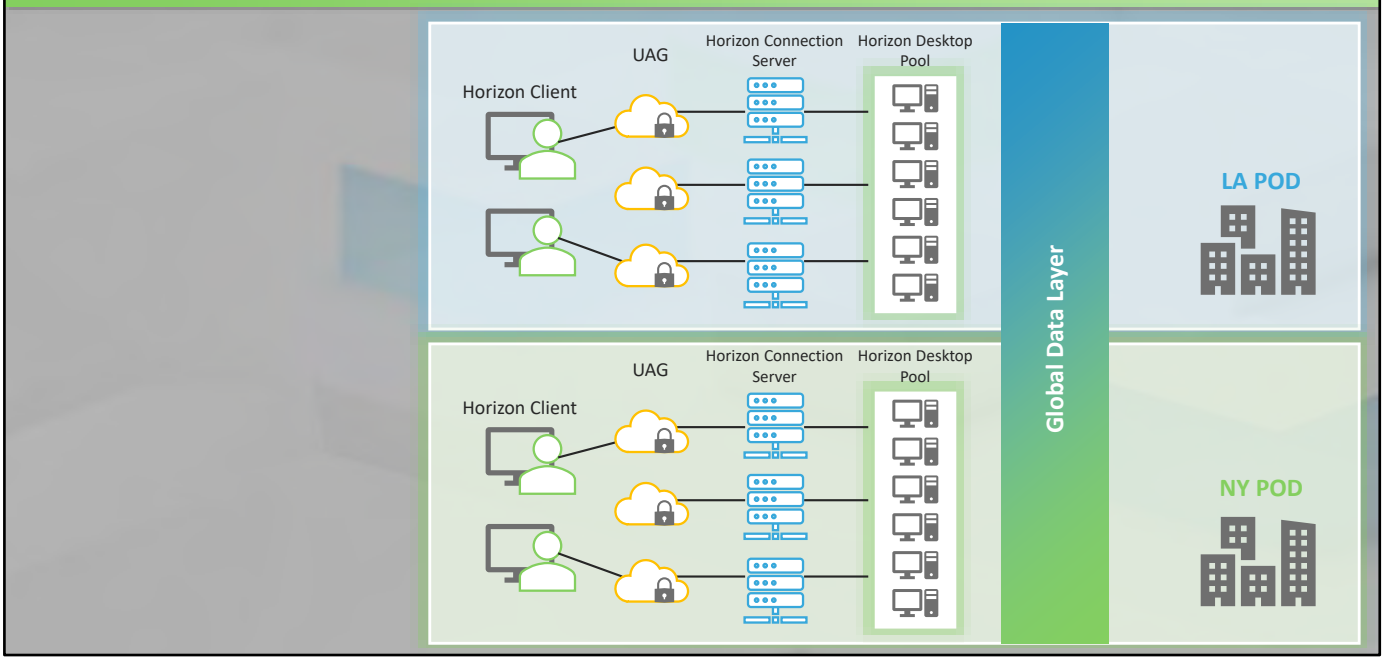
Shared Key Data in the Global Data Layer

- Information about the pod federation topology
- User and group entitlements
- Policies
- Other Cloud Pod Architecture configuration information

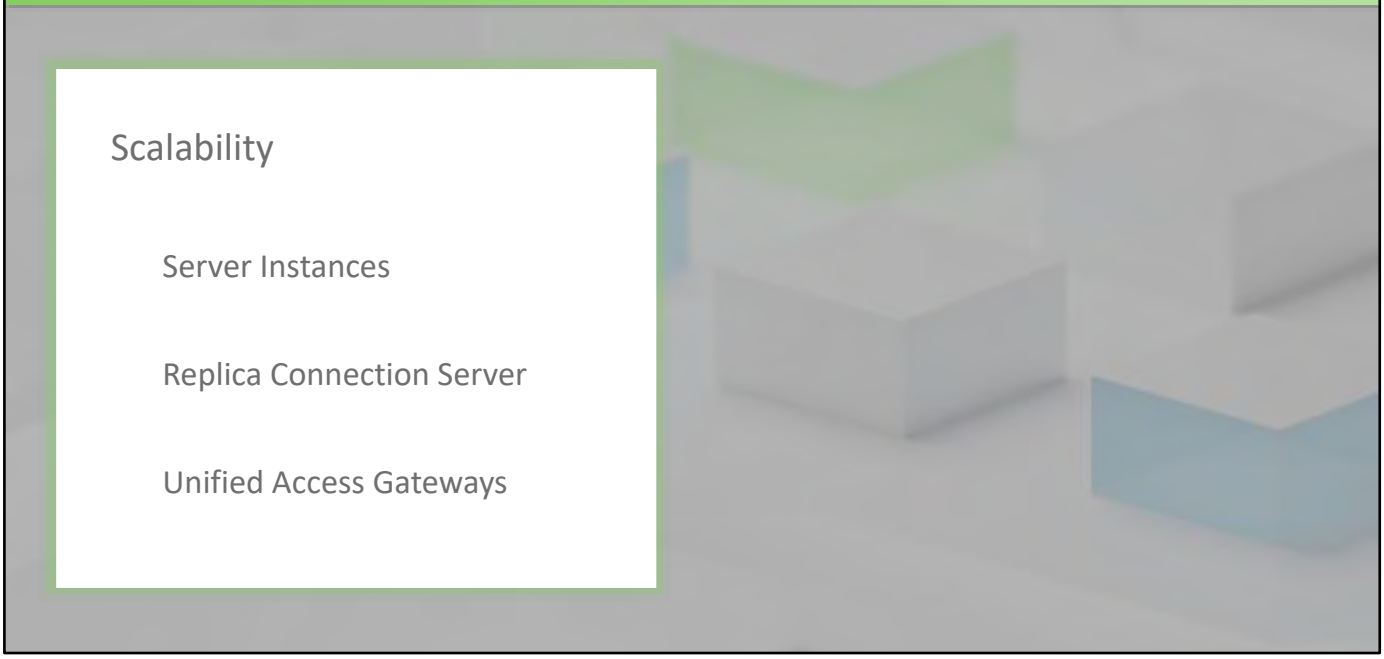
Sending Messages Between Pods

- Communicate between Pods uses an interpod communication protocol called the View InterPod API (VIPA)

Unified Access Gateway



Conclusions



Scalability

- Server Instances
- Replica Connection Server
- Unified Access Gateways

Security

- VMware Horizon Accounts
- Horizon Database Accounts
- Horizon files needing protection
- VMware Horizon Log Files
- Security-Related Global Settings in Horizon Console
- Security-Related Server Settings in Horizon Console
- Security-Related Server Settings for User Authentication

Security

- Ports and Services (Firewalls)
- Default Global Policies for Security Protocols and Cipher Suites
- Older Protocols and Ciphers Disabled in VMware Horizon
- Configuring Security Protocols and Cipher Suites for Blast Secure Gateway
- Configuring Security Protocols and Cipher Suites for PCoIP Secure Gateway
- Deploying USB Devices in a Secure VMware Horizon Environment
- HTTP Protection Measures on Connection Servers
- Other Protection Measures

VMware Horizon Accounts

Horizon Client

Configure user accounts in Active Directory for the users who have access to remote desktops and applications

User accounts must be members of the Remote Desktop Users group

Accounts do not require Horizon administrator privileges

vCenter Server

Configure a user account in Active Directory with permission to perform the operations in vCenter Server that are necessary to support VMware Horizon

For the required privileges, see the Horizon Installation document

Horizon Database Accounts

- Configure VMware Horizon databases on servers that are separate from other database servers that your organization uses
- Do not allow a single user account to access multiple databases
- Configure a separate account for access to the event database

Horizon Files Needing Protection

- LDAP settings
- LDAP backup files
- locked.properties
  - Secure gateway configuration file
- * absg.properties
  - Blast Secure Gateway configuration file
- Log files
- web.xml
  - Tomcat configuration file

VMware Horizon Log Files

- All components (installation logs)
  - %TEMP%\vminst.log_date_timestamp
  - %TEMP%\vmmsi.log_date_timestamp
- Horizon Agent
  - <Drive Letter>:\ProgramData\VMware\VDM\logs
  - logs for PCoIP are named
  - pcoip_agent*.log
  - pcoip_server*.log
- Published Applications
  - The Horizon Event Database configured on an SQL Server
  - Windows Application Event logs, disabled by default
- Connection Server
  - Drive Letter>:\ProgramData\VMware\VDM\logs
- Horizon Services
  - Horizon Event Database configured on an SQL Server, Windows System Event logs

Demo

- VMware Horizon Log File locations

Security-Related Global Settings in Horizon Console

- Client sessions and connections are accessible in Horizon Console
  - Settings > Global Settings > Security Settings
  - Settings > Global Settings > General Settings
- Change data recovery password
- Message security mode
  - Default setting is Enhanced
- Enhanced Security Status (Read-only)
  - Appears when Message security mode is changed from Enabled to Enhanced.
  - Change is made in phases, this field shows the progress through the phases
  - Message security mode default setting is Enhanced already.

Security-Related Global Settings in Horizon Console

- Reauthenticate secure tunnel connections after network interruption
  - Determines if user credentials must be reauthenticated after a network interruption when Horizon Clients use secure tunnel connections
  - This setting is disabled by default.
- Forcibly disconnect users
  - The default is 600 minutes
- For clients that support applications. If the user stops using the keyboard and mouse, disconnect their applications and discard SSO credentials
  - The default is Never.
  - Other clients. Discard SSO credentials
  - This setting is for clients that do not support application remoting
  - The default is After 15 minutes
- View Administrator session timeout
  - Determines how long an idle Horizon Console session continues before the session times out.
  - By default, the Horizon Console session timeout is 30 minutes

Security-Related Settings in Horizon LDAP

- In Horizon Connection Server Console
  - Settings > Servers
- Use PCoIP Secure Gateway for PCoIP connections to machine * PCoIP
  - This setting is disabled by default.
- Use Secure Tunnel connection to machine * HTTPS
  - This setting is enabled by default.
- Use Blast Secure Gateway for Blast connections to machine
  - This setting is disabled by default

Demo

Security-Related Global Settings in Horizon Console

Ports and Services (Firewalls)

- Horizon Security Guide
  - Over 4 pages of Protocols and Ports
- The UDP port number that clients use for PCoIP might change
  - You must configure firewalls with ANY where an asterisk (*) is listed in the table.
- Microsoft Windows Server requires a dynamic range of ports to be open between all Connection Servers in the VMware Horizon environment
  - These ports are required by Microsoft Windows for the normal operation of Remote Procedure Call (RPC) and Active Directory replication.
- Connection attempts over HTTP are silently redirected to HTTPS
  - To prevent redirection for all HTTP connection attempts instructions are in the Horizon Installation Guide

TrueSSO Ports Used by VMware H
Ports and Services (Firewalls)

Source	Target	Port	Protocol
Horizon Client	VMware Identity Manager appliance	TCP 443	HTTPS
Horizon Client	Horizon Connection Server	TCP 443	HTTPS
Horizon Connection Server	VMware Identity Manager appliance	TCP 443	HTTPS
Horizon Connection Server	Horizon Enrollment Server	TCP 32111	
Horizon Agent	Horizon Connection Server	TCP 400	JMS over TLS
Virtual desktop or published application	AD DC		
Horizon Client	Horizon Agent (protocol session)	TCP/UDP 22443	Blast
Horizon Client	Horizon Agent (protocol session)	UDP 4172	PCoIP

Default Global Policies for Security Protocols and Cipher Suites

- To change the global acceptance and proposal policies for security protocols and cipher suites
  - Use the ADSI edit utility to edit horizon LDAP attributes
  - Horizon Security Guide Page 30
- Default Global Acceptance and Proposal Policy TLS 1.1 amd 1.2 Enabled by default
  - Defined in horizon LDAP attributes
  - We may want to disable TLS 1.1
  - Each policy is a single-valued attribute in the following horizon LDAP location:
    - cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int
      - The following attribute lists security protocols. You must order the list by placing the latest protocol first:
        - pae-ServerSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
- Normally, the server's ordering of cipher suites is unimportant, and the client's ordering is used. To use the server's ordering of cipher suites instead, set the following attribute:
  - pae-ServerSSLHonorClientOrder = 0
- You can configure acceptance policies on individual servers
  - Not suggested as can cause intermittent results

Older Protocols and Ciphers Disabled in VMware Horizon

Older protocols and ciphers that are no longer considered secure are disabled in VMware Horizon by default

- SSLv3
- TLSv1 and TLSv1.1
- RC4
- DHE cipher suites
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

If required, you can enable them manually

- Should not be needed in most environments

Configuring Security Protocols and Cipher Suites for Blast Secure Gateway

The security settings for Connection Server do not apply to Blast Secure Gateway (BSG).

You must configure security for BSG separately.

You can configure the security protocols and cipher suites that BSG's client-side listener accepts

- Editing the file absg.properties

Examine the BSG's absg.log file to discover the values that are in force for a specific BSG instance

Configuring Security Protocols and Cipher Suites for PCoIP Secure Gateway

Security settings for Connection Server do not apply to PCoIP Secure Gateway (PSG)

You must configure security for PSG separately

You can configure the security protocols and cipher suites that PSG's client-side listener accepts by editing the registry.

This task can also be performed on a RDS host

Deploying USB Devices in a Secure VMware Horizon Environment

- By default, all USB devices are allowed to be redirected unless otherwise blocked.
- Prevent USB devices from being redirected to remote desktops and applications
- When you install Horizon Agent on a desktop image or RDS host, deselect the USB redirection setup option.
  - Deselected by default
  - Prevents access to USB devices
- In Horizon Console, edit the USB access policy for a specific pool to either deny or allow access.
  - Can control access to USB devices in specific desktop and application pools
  - Do not have to change the desktop image
- After you set the policy at the desktop or application pool level
  - Override the policy for a specific user in the pool
  - Selecting the User Overrides setting and selecting a user
- Set the Exclude All Devices policy to true, on the Horizon Agent side or on the client side
  - If you set the Exclude All Devices policy to true, Horizon Client prevents all USB devices from being redirected

Demo

Securing USB Devices in a VMware Horizon Environment

HTTP Protection Measures on Connection Servers

- Transport Layer Security (TLS) – Renegotiation Indication Extension, also known as secure renegotiation default Enabled
- Client-initiated renegotiation on Connection Servers default Disabled
- HTTP Strict Transport Security (HSTS), also known as transport security default Enabled
  - Cannot be disabled
- HTTP Header Field X-Frame-Options, also known as counter clickjacking default enabled
- Origin Checking, which protects against cross-site request forging default enabled
  - In earlier releases, this protection was disabled by default
- Cross-Origin Resource Sharing (CORS) constrains client-side cross-origin requests
- Content Security Policy (CSP), which mitigates a broad class of content injection vulnerabilities default Enabled

Additional Protection Measures

Reducing MIME Type Security Risks

Enabled by default

Mitigating Cross-Site Scripting Attacks

Enabled by default

Content Type Checking

Accepts requests with the following declared content types only
application/x-www-form-urlencoded
application/xml
text/xml
In earlier releases, this protection was disabled by default.

Conclusions

Lesson name goes here

VMware Horizon Accounts
Horizon files needing protection
VMware Horizon Log Files
Security-Related Global Settings
Ports and Services (Firewalls)
Default Global Policies for Security Protocols and Cipher Suites
Older Protocols and Ciphers Disabled in VMware Horizon
Configuring Security Protocols and Cipher Suites for PCoIP and Blast Secure Gateway
Deploying USB Devices in a Secure VMware Horizon Environment
HTTP Protection Measures on Connection Servers
Other Protection Measures

Troubleshooting

- Collect valid and accurate information regarding problems
- Understand where to get to logs and how to generate a log bundle
- Systematic troubleshooting methods
- Troubleshoot Horizon
- Configuring Horizon Event Database
- Permission in Horizon Console
- Troubleshoot Horizon replication
- Troubleshoot Horizon Desktop trust relationships
- Troubleshoot Horizon client black screen

Horizon 8 Logs

Horizon 8 Component	File Path and Other Information
All components (installation logs)	%TEMP%\vminst.log_date_timestamp %TEMP%\vmmsi.log_date_timestamp
Horizon Agent	<Drive Letter>:\ProgramData\VMware\VDM\logs Must open the logs from an application with elevated administrator privileges The logs for PCoIP are named pcoip_agent*.log and pcoip_server*.log
Remote Desktop Features	**Windows Client**: C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT\support.bat **Mac Client**: /Applications/VMware Horizon Client.app/Contents/Library/dct/HorizonCollector.sh **Linux Client**: /usr/bin/vmware-view-log-collector
Published Applications	The Horizon Event Database configured on a Microsoft SQL Server, Oracle database server, or PostgreSQL database server Windows Application Event logs. Disabled by default

Horizon 8 Logs

Horizon 8 Component	File Path and Other Information
Connection Server	<Drive Letter>:\ProgramData\VMware\log\ConnectionServer. Note: This file path is a symbolic link that redirects to the actual location of the log files, which is <Drive Letter>:\ProgramData\VMware\VDM\logs. The log directory is configurable in the log configuration settings of the Common Configuration ADMX template file (vdm_common.admx) . PCoIP Secure Gateway logs are written to files named SecurityGateway_*.log in the PCoIP Secure Gateway subdirectory. Blast Secure Gateway logs are written to files named absg*.log in the Blast Secure Gateway subdirectory.
Horizon Services	Horizon Event Database configured on a Microsoft SQL Server, Oracle database server, or PostgreSQL database server. Windows System Event logs

How to generate a log bundle

- Horizon Connection Server
  - Start > Programs > VMware.
  - Click Generate Horizon Connection Server Log Bundle
  - On the desktop, the folder vdm-sdct contains zipped log files with the date of generation in the filename
- To enable advanced debug logging:
  - Start > Programs > VMware
  - Select Set Horizon Connection Server Log Levels
  - When prompted, press 3 to enable advanced logging

Systematic troubleshooting method

- Identify the problem
- Plan a response
- Test the solution
- Resolve the problem

Troubleshooting Horizon Client

- Many problems with Horizon Client can be resolved by
  - Restarting or resetting remote desktops or published applications
  - Reinstalling Horizon Client
  - Repair Horizon Client for Windows
- Problems with Keyboard Input
  - Disable the keystroke logging detection feature of your antivirus or security software
- Horizon Client Quits Unexpectedly
  - Can occur when the connection to the server is lost
- When you try to connect to a connection server using the Horizon Client, you're redirected you to the Workspace ONE portal
  - A Horizon administrator enabled Workspace ONE mode on a Connection Server instance
  - Going forward use Workspace ONE to connect to a Workspace ONE enabled server and access your remote desktops or published applications

Configuring Horizon Event Database

- In Horizon Console
  - Settings > Event Configuration
- In the Event Database section, click Edit
  - Enter the database information in the fields provided
  - Click OK.
- To clear the event database information, click Clear.
- Optionally in the Event Settings window
  - Click Edit
  - Set the length of time to show events and the number of days to classify events as new
  - Click OK.
- To verify that the connection to the event database is successful
  - Monitoring > Events

Demo

Configuring Horizon Event Database

Permission in Horizon Console

In Horizon Console

- Settings > Administrators.

Create the permission.

- Create a permission that includes a specific administrator user or group
- Create a permission that includes a specific role
- Create a permission that includes a specific access group

Demo

- Create Permission in Horizon Console

Troubleshoot Horizon replication

Issue

- Connection server replication fails
- Cannot replicate successfully from a Connection server to any other Connection servers in the replicated group
- When you run this command, it results in an LDAP error:
  - repadmin.exe /showrepl localhost:389DC=vdi,DC=vmware,DC=int
- You see an LDAP error similar to:
  - DsReplicaSync() failed with the status 8606 (0x219e)
  - Insufficient attributes where given to create an object. This object may not exist because it may have been deleted and already garbage collected

Resolution

- Uninstall and reinstall the connection server on which replication is failing.

Troubleshoot Horizon Desktop trust relationships

Issue

- Connecting to desktops in VMware Horizon View fails
- When logging in to a linked clone, you see the error

Cause

- Active Directory computer accounts are configured to change their machine password every 30 days
- The pool is not recomposed within 30 days and the security policy is set to default, the computers change their password

Resolution

- Recompose the computers more frequently, sooner then every 30 days
- Group policies can change these settings to be longer if needed
- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Option

Troubleshoot Horizon client black screen

Issue

When trying to connect using the PCoIP, a black screen is displayed temporarily, and the client disconnects. RDP is successful.

From the internal network, PCoIP connections is successful, connecting externally through UAG results in a black screen.

Connections from a PCoIP Zero Client fail, connecting using the Horizon client is successful.

Horizon dual monitor displays a black screen.

The error message below is displayed

"the connection to the remote computer timed out"

Causes

Misconfiguration of connection server settings

vRAM shortage on the Horizon Virtual Desktop

Incorrect video driver version installed on the Horizon Virtual Desktop

Required ports are not open between UAG/Connection server to VDI machine.

Conclusions

Troubleshooting

- Collect valid and accurate information regarding problems
- Understand where to get to logs and how to generate a log bundle
- Systematic troubleshooting methods
- Troubleshoot Horizon
- Configuring Horizon Event Database
- Permission in Horizon Console
- Troubleshoot Horizon replication
- Troubleshoot Horizon Desktop trust relationships
- Troubleshoot Horizon client black screen