JMP AND VMWARE HORIZON 7 DEPLOYMENT CONSIDERATIONS
# Table of Contents

**Legacy Content**

**Executive Summary**
- Audience
- Scope

**JMP and Horizon 7 Overview**

**Benefits of JMP**

**JMP Technical Overview**
- Horizon 7 Enterprise Edition
- vSphere 6.x and Instant Clone Technology
- App Volumes
- User Environment Manager
- Workspace ONE

**How JMP Works**

**JMP and Horizon 7 Components**

**Architecture of a JMP and Horizon 7 Deployment**

**Deployment Considerations**
- Horizon 7 and vSphere Deployment Considerations
- App Volumes Deployment Considerations
- User Environment Manager Deployment Considerations
- Workspace ONE Deployment Considerations
Deployment Procedures

- Horizon 7 and vSphere Deployment Overview
- User Environment Manager Deployment Overview
- App Volumes Deployment Overview
- Workspace ONE Integration

Managing Desktops and Applications

- Desktop and RDSH Image Management
- Application Management
- User Profile and Settings Management
- Application Access with Workspace ONE

Appendix A: Deployment Requirements

- Requirements Common to All Components
- Horizon 7 Requirements
- User Environment Manager Requirements
- App Volumes Requirements
- Workspace ONE Requirements

Additional Resources

About the Authors and Contributors
JMP and VMware Horizon 7 Deployment Considerations

Legacy Content

LEGACY CONTENT: This paper contains valuable information, although some details are different for the current release of the product.

Executive Summary

Over a decade ago, when VMware first offered a virtual desktop infrastructure (VDI) solution, the strategy was to take a Windows desktop system, virtualize it, and place it in the data center. In those days, each employee’s virtual machine (VM) was a dedicated, persistent entity that required almost the same maintenance effort as a physical desktop.

Today, with JMP (Just-in-Time Management Platform) technologies from VMware, the components of the desktop are decoupled from each other and are assembled on demand to provide a modern digital workspace.

Figure 1: JMP Technologies Eliminate Cost and Complexity

This guide describes JMP and VMware Horizon® 7 Enterprise Edition version 7.1 (or later) capabilities, architecture, and
JMP AND VMWARE HORIZON 7 DEPLOYMENT CONSIDERATIONS

implementation requirements and addresses frequently asked high-level questions about deploying a JMP solution. The goal of this deployment is a virtual desktop and published application environment delivered by VMware Horizon 7 Enterprise Edition.

We begin with an overview of the various technologies included in JMP, and explain how their interactions create Just-in-Time Desktops and Apps:

- **Instant clones** – Because VMs can now be cloned instantly when needed, they can be destroyed when the user logs out.

- **VMware App Volumes™** – This container-style technology attaches applications to a VM when the user logs in, or, in the case of RDS-provided desktops and apps, when the RDSh server boots up.

- **VMware User Environment Manager™** – User preferences and settings for each application and desktop are applied either at login or when the user launches an application.

- **VMware Workspace™ ONE™** – The Workspace ONE mobile app or browser-based catalog offers a consistent experience across user devices for accessing Just-in-Time Desktops and Apps.

Later sections list the before-, during-, and after-deployment considerations and best practices for operating the JMP technologies in unison. System and software requirements for each technology are collected into an appendix. Just enough detail is provided to give you a good understanding of what it takes to implement a JMP solution.

This paper also serves as your guide to the many white papers and blog posts that delve into various aspects of each JMP technology separately and in combination. For each step or best practice we direct you to perform, we refer to the best white paper, administration guide, or blog post for deepening your understanding and receiving further guidance.

**Audience**

This paper is intended for IT architects and administrators who want to use VMware Horizon 7 to deploy Just-in-Time Desktops and Apps. Familiarity with VMware vSphere® and VMware vCenter Server® is assumed, as is familiarity with other technologies, including desktop and application virtualization, networking and storage in a virtual environment, Active Directory, identity management, and directory services.

**Scope**

Horizon 7 Enterprise Edition includes a vast array of components and features. This guide focuses on the JMP technologies, which provide just-in-time virtualized Microsoft Windows applications and desktops. For this reason, this guide does not include information about components such as VMware Horizon for Linux, or VMware Mirage™ for managing physical desktop images.

**JMP and Horizon 7 Overview**

JMP (pronounced jump), which stands for Just-in-Time Management Platform, represents capabilities in VMware Horizon 7 Enterprise Edition that deliver Just-in-Time Desktops and Apps in a flexible, fast, and personalized manner. JMP is composed of the following VMware technologies:

- **VMware Instant Clone Technology** for fast desktop and RDSH provisioning

- **VMware App Volumes** for real-time application delivery

- **VMware User Environment Manager** for contextual policy management

JMP allows components of a desktop or RDSH server to be decoupled and managed independently in a centralized manner, yet reconstituted on demand to deliver a personalized user workspace when needed. JMP is supported with both on-premises and cloud-based Horizon 7 deployments, providing a unified and consistent management platform regardless of your deployment topology.

The JMP approach provides several key benefits, including simplified desktop and RDSH image management, faster delivery and maintenance of applications, and elimination of the need to manage “full persistent” desktops.

**Benefits of JMP**

In the early years of VDI, the operating system (OS) for each virtual desktop had to be managed and patched regularly, and applications had to be updated, just as if the VM were a physical machine. In recent years, linked-clone technology sped up VM
creation, provisioning, and maintenance, but maintenance windows were still required for refreshing the VM back to its original disk size. The VM also had to go through a lengthy recompose operation to apply OS and application updates. And at regular intervals VMs had to be rebalanced across datastores.

Today with JMP from VMware, because VMs can be cloned in seconds, they no longer need to persist when the user logs out. AppVolumes, a container-style technology, can attach applications to a VM when the user logs in. User preferences and settings for each application are applied when the user launches the application. These are just a few of the benefits of JMP.

Seamless and easy access to any app from any device:

- You can use the JMP technologies with Workspace ONE to create a single unified app catalog for SaaS, web, Horizon 7 published applications, Horizon 7 virtual desktops, Citrix XenApp, and mobile apps.
- After users authenticate once, the single sign-on feature logs them all the way in to their virtual desktop or app.

Persistent end-user experience in nonpersistent environments:

- User Environment Manager delivers a consistent, personalized desktop and app experience across devices.
- Applications installed on multi-user App Volumes AppStacks or user-specific writable volumes are attached to a desktop at user login.

Cost-optimized infrastructure:

- Instant clones allow you to deploy VDI desktops and RDSH servers more rapidly, scale more easily, and perform maintenance up to 85 percent more quickly than was previously possible. No separate server or database instance is required for instant clones.
- Because the OS, applications, and user data are decoupled from each other, you can use the most appropriate type of storage for each component. Applications and the operating system can use fast storage with high-read IOPS, such as VMware vSAN™. Configuration settings and user data can be stored on less expensive NAS-based storage.

Reliability and security:

- Instant clones improve security by regenerating and automatically refreshing VDI desktops when users log out, and regenerating RDSH servers on a scheduled basis.
- VMs can reside on high-availability clusters of VMware vSphere servers.
- Communication among server components, client devices, and, optionally, VDI desktops uses TLS/SSL.

Centralized administration and management:

- With App Volumes, applications become objects (AppStacks) that can be moved easily across data centers and shared with thousands of VMs.
- Desktops and applications are centralized by integrating with VMware vSphere and virtualizing server, storage, and networking resources.
- User Environment Manager allows you to manage Windows settings and application settings, as well as user preferences, from a central console.

Blast Extreme display technology built on industry-standard H.264:

- End users get a high-performance graphics experience accessible on a multitude of devices including ultra-low-cost PCs.
- Both TCP and UDP transport protocols are supported, and Blast Extreme selects the appropriate transport protocol based on network conditions and policy.
- Multiple codecs are supported, and Blast Extreme selects the appropriate codec—JPG/PNG or H.264—based on endpoint and policy.

**JMP Technical Overview**

JMP represents capabilities within Horizon 7 Enterprise Edition version 7.x and Horizon Apps Advanced Edition. These editions include Horizon 7 version 7.x, vSphere 6.x, App Volumes 2.x, User Environment Manager 9.x, and VMware Identity Manager™.

**Horizon 7 Enterprise Edition**

VMware Horizon 7 is a desktop and application virtualization solution that enables organizations to securely deliver desktop services and applications to end users from centralized VMware vSphere servers.
Users can access their personalized virtual desktops or published applications from company laptops, their home PCs, thin client devices, Macs, tablets, or smartphones. As an IT administrator, you can quickly create virtual desktops and published applications on demand, as well as automate the management of desktops and apps.

Horizon 7 Enterprise Edition includes all the same features as the Standard and Advanced Editions, and adds the JMP technologies: Instant Clone Technology, App Volumes, and User Environment Manager.

**vSphere 6.x and Instant Clone Technology**

*Instant Clone Technology* provides single-image management with automation capabilities. A clone is a copy of a master VM with a unique identity of its own, including a MAC address, UUID, and other system information.

Because instant clones are created on demand and are deleted when users log out, or according to schedule for RDSH servers, instant clones require less storage than other types of clones and are less expensive to manage and update.

You can use Instant Clone Technology in combination with VMware User Environment Manager and VMware App Volumes to rapidly create desktops that provide a persistent experience.

**App Volumes**

App Volumes stores applications in shared read-only virtual disks (VMDK files) called AppStacks. A single AppStack can be assigned to many desktops and RDSH servers. The application or applications contained in an AppStack appear and function as if natively installed.

The provisioning of AppStacks requires no special packaging formats. During the creation of an AppStack, App Volumes records the entire application-installation process, along with the system changes made by the native application installers.

In circumstances where you want to allow users to install their own applications, you can provide users with an App Volumes writable volume, which is also a VMDK file.

App Volumes VMDK files can be stored on any supported VMware vSphere datastore, so IT can leverage the most efficient storage—including fast storage with high-read IOPS (such as VMware vSAN) instead of streaming applications across the network from a CIFS share. App Volumes does not move bits across the network.

**User Environment Manager**

User Environment Manager offers simplified profile and policy management with personalized access across devices and locations for end users. Just as App Volumes separates applications from the OS, User Environment Manager decouples personalization from the OS. Users can log in to a different Windows OS and retain their settings.

When a user logs in to a virtual desktop or published application, user environment and personalization settings are imported based on conditions such as the user’s location, type of device, and user group. Network and printer mappings, application blocking rules, shortcuts, and many more settings are configured according to the current policy.

Windows settings (such as the desktop background, desktop screensaver, keyboard settings, and so on) are always injected at login. To minimize login times, application settings are applied at application launch. You can define which application settings can be personalized and which always remain at their initial values to ensure compliance with company policy.

You can also use User Environment Manager to configure folder redirection so that personal user data, documents, pictures, and so on are redirected from specific folders inside the VM. This combination of folder redirection and fine-grained policy control enhances the ability to manage user personas and minimizes the number of files that must be copied to the VM when the user logs in.

**Workspace ONE**

VMware Workspace ONE is a simple and secure enterprise platform that delivers and manages any app on any device by integrating identity, application, and enterprise mobility management. It is available as a cloud service or for on-premises deployment.

Horizon 7 can be integrated with Workspace ONE through VMware Identity Manager (either on-premises or as part of the Workspace ONE service). VMware Identity Manager is provided with Horizon 7 Enterprise Edition or Workspace ONE when purchased.

For Horizon 7 users and administrators, VMware Identity Manager provides application provisioning, a self-service catalog of applications and virtual desktops, conditional access controls, and single sign-on (SSO) for software-as-a-service (SaaS), web, cloud, and native mobile applications.
How JMP Works

JMP offers an alternative to managing per virtual machine. JMP decouples each aspect of a desktop to allow it to be managed on a per-user or per-group basis. Each component of the desktop is virtualized and managed centrally rather than separately, as is done in a traditional distributed per-VM approach.

As illustrated in Figure 2, application-management containers are managed separately from the desktop OS. Similarly, user data files and OS- and application-specific configurations are decoupled from the OS and kept on separate file shares.
JMP and VMware Horizon 7 Deployment Considerations

**JMP Management Strategy**

- **Virtualized Desktop or App Component**
  - App and Environment Configuration
  - User Data Files
  - User-Installed Apps or Local App Cache
  - Applications
  - Operating System

- **Management Strategy**
  - User Environment Manager Share
  - Folder Redirection
  - User Profile Share
  - User Writable Volume
  - AppStack
  - Instant Clone
The following components of JMP work together to compose a just-in-time personalized desktop:

- **User Environment Manager share** – A file share that stores user-specific desktop and application settings, making them available across multiple devices, Windows versions, and application instances. Application settings are imported and applied at application launch. Windows settings (such as the desktop background, desktop screensaver, keyboard settings) are imported at login. When a user quits an application, or logs out of the OS, settings are exported and saved on a file share.

- **User data share** – A file share that stores personal user data, documents, pictures, and so on that are redirected from specific folders inside the VM. This strategy minimizes the number of files that must be copied to the VM when the user logs in.

- **AppStack** – A read-only container for one-to-many delivery of IT-managed applications.
  - For virtual desktops, AppStacks are assigned to an Active Directory user or group, and assigned AppStacks are attached to the desktop when a user logs in.
  - For RDSH servers, which provide published applications and shared session-based desktops, AppStacks are assigned to the group object in Active Directory that contains the computer objects for the servers. Assigned AppStacks are attached to the RDSH server at boot time.

- **Writable volume** – A one-to-one, user-specific, read-and-write container for user-installed applications or for applications that require a local cache, since a writable volume appears as part of the local C: drive.

Users must ordinarily have administrator permissions to install applications in a virtual desktop, just as they would for a physical desktop. User Environment Manager 9.2 has a Permission Elevation feature that administrators can now use so that users can install applications without having to have full administrator permissions.

**Important**: In companies that require tight control over virtual desktops and apps, you need not provide users with a writable volume. In this case, when users log out, they lose any changes they might have made to the OS, as well as any data they might have saved to a folder location that is not redirected.

- **Instant clone** – A new type of cloned VM that is created using vSphere vmFork technology to rapidly clone both the memory and the disk of a running parent VM. Instant Clone Technology requires half the required steps compared to View Composer linked-clone technology when deploying or scaling. In VMware lab tests, an instant-clone farm of 200 RDSH servers was created in less time than View Composer took to create a single RDSH server.

**JMP and Horizon 7 Components**

Figure 3 and corresponding descriptions show the relationships between the major Horizon 7 version 7.1 (or later) components of a JMP deployment.
1. **Horizon Client** – Client software is available from app stores or from VMware for iOS, Android, Chrome, Windows, Linux, and macOS so that users can access published applications and VDI desktops from any device. An HTML Access web client is also available, and it does not require installing any software on client devices.

2. **Connection Server** – Horizon Client is configured to access the Connection Server. This server, which integrates with Windows Active Directory, provides access to virtual desktops and published applications. This server also includes the instant-clone engine, which provides single-image management with automation capabilities.

3. **VMware Instant Clone Technology** – Use this key Horizon 7 feature to create instant-clone desktop pools and automated farms of instant-clone Microsoft RDSH servers.

4. **RDSH VMs and Desktop VMs** – To provide published applications, you attach App Volumes AppStacks to one or more Microsoft RDSH servers. You can also use RDSH servers to provide shared session-based virtual desktops. In contrast, with single-user virtual desktops, each user gets an individual desktop VM.

5. **Agents** – You install the Horizon Agent, the App Volumes Agent, and the User Environment Manager FlexEngine service on the master images for Microsoft RDSH servers and single-user virtual desktops.
   - Horizon Agent communicates with Horizon Client to provide features such as connection monitoring, virtual printing, folder sharing (client-drive redirection), and access to locally connected USB devices.
   - App Volumes Agent runs as a service and uses a filter driver to handle application calls and filesystem redirects to AppStack and writable volume VM disks (VMDKs).
   - FlexEngine, the User Environment Manager agent, starts at login and imports policy settings, including application and user environment settings, from a configuration share. This agent also loads personalization settings from a user profile archives share.

You use the provided Group Policy Object (GPO) administrative templates (.admx files) to enable and configure FlexEngine.

6. **RDSH farms** – One or more RDSH servers make up a farm, and from that farm you create application and shared session-based desktop pools. Each individual farm can contain up to 200 RDSH servers.

7. **Application pools** – Each application that you select to publish becomes an application pool. For example, using the Add Application Pool wizard, if you select the Paint and Calculator apps to publish, when you complete the wizard, you will have a Paint application pool and a Calculator application pool.

8. **Desktop pools** – You can create an instant-clone pool from a Windows 7 or Windows 10 master image, or you can create a desktop pool based on an automated instant-clone farm of RDSH servers. Like View Composer linked-clone pools, instant-clone pools have been tested to support up to 2,000 single-user desktops in a pool.

9. **App Volumes Manager** – You use this administrative console for configuring VMware App Volumes to attach applications (AppStacks) to virtual desktops and to RDSH servers, simplifying application distribution and update. Also use this console to attach writable volumes to virtual desktops if users need to install their own applications.

10. **User Environment Manager** – Use the VMware User Environment Manager Management Console to configure user-specific Windows desktop and application settings that are applied in the context of client device, location, or other conditions. Policies are enforced when users log in, launch an app, reconnect, or when some other triggering event occurs.

You can also configure folder redirection for storing personal user data, including documents, pictures, and so on.

11. **VMware Unified Access Gateway™** – A Unified Access Gateway virtual appliance (formerly known as Access Point) functions as a secure gateway for users to access resources such as remote desktops and applications from outside the corporate firewall. Unified Access Gateway appliances typically reside within a network demilitarized zone (DMZ).

12. **Workspace ONE** – Workspace ONE leverages VMware Identity Manager, which provides application provisioning, a self-service catalog, conditional access controls, and single sign-on for SaaS, web, cloud, and native mobile applications. When Workspace ONE is integrated with Horizon 7, users access the app catalog through either the Workspace ONE app or the Workspace ONE browser-based catalog. With one click in the Workspace ONE catalog, the selected published app or virtual desktop is launched in Horizon Client.

13. **Display Protocol** – Blast Extreme is the newest VMware user-interface remoting technology, which can use natively supported
encoding formats H.264 (for longer device battery life) or JPG/PNG, and can use either UDP or TCP transport. Blast Extreme is supported on all Horizon Client OS types and on more than 70 thin and zero clients. Alternatively, the PCoIP display protocol is also supported.

Architecture of a JMP and Horizon 7 Deployment

Figure 4 shows the architectural layout of a JMP deployment, which includes App Volumes, instantclone VDI desktops and RDSH server farms, and User Environment Manager.
Figure 4: On-Premises Deployment of JMP Components for a Single Site

This diagram depicts a one-site deployment, which includes one Horizon 7 pod containing three resource blocks and a single management block.

- **Pod** – A pod is made up of a group of interconnected Connection Servers that broker desktops or published applications. A pod can broker up to 10,000 sessions, including desktop and RDSH sessions. A pod is divided into multiple resource blocks.

- **Resource blocks** – Each resource block consists of a VM cluster of desktop pools, RDSH pools, or both types of pools, as well as VMware ESXi™ hosts, shared storage for VMs, a switched Ethernet network, and a vCenter Server. Shared storage has separate datastores for desktop and RDSH server master images and for App Volumes AppStacks.

- **Management block** – The management block includes vCenter Server, Unified Access Gateway appliances, Connection Servers, GPOs for User Environment Manager, and App Volumes Managers. A highly available SQL database cluster can support databases for all the App Volumes Managers, Horizon 7 Event databases, and vCenter Servers in the environment, as described in the VMware Horizon 7 Enterprise Edition Reference Architecture.

- **SMB file shares** – Server Message Block file shares store user data through folder redirection, and file shares store User Environment Manager profiles and configuration files. User Environment Manager combined with folder redirection is the recommended solution for managing user personas. For more information, see the VMware blog post VMware User Environment Manager with VMware App Volumes.

This diagram shows a single-site design. For more information about App Volumes multi-site design and how to replicate writable volumes, see the VMware Horizon 7 Enterprise Edition Multi-Site Reference Architecture. For information about replicating AppStacks between the two data centers using a nonattachable datastore and App Volumes storage groups, see the VMware App Volumes Deployment Considerations guide.

Deployment Considerations

For each technology involved in a JMP deployment, you must consider business requirements, user experience, and system and software requirements.

**Note:** The system and software requirements of each JMP component are listed in Appendix A: Deployment Requirements.

Horizon 7 and vSphere Deployment Considerations

The following items give you an idea of the sorts of considerations to take into account with regard to Horizon 7. All of these items are discussed in the VMware Horizon 7 Enterprise Edition Reference Architecture. For some items, be sure to also see the additional guides listed.

- **Business drivers** – Align the solution to directly address critical business requirements and drivers. Each and every design choice should center on a specific business requirement; for example, providing mobile access, centralizing and securing data, reducing support calls, and reducing desktop and application provisioning time.

- **Use cases** – Group usage patterns and common user scenarios into use cases. Take into account the applications that each group requires, the amount of processing power they need, and the locations they work from.

- **User functional requirements** – Consider how the users are going to interact and use the solution. How will they connect and authenticate (smart card, touch, two-factor authentication, AD credentials, and so on)? What devices match their requirements, and will the experience match their expectations?

**Note:** Client devices (thin clients, mobile devices, PCs, Linux clients, and so on) offer varying support for Horizon Client features. You need a clear understanding of the features required before choosing or recommending a client device.

- **User experience** – Responsiveness and a high-fidelity display for applications and desktops will be critical to users. In order to ensure the best user experience, understand the networks users will use to access their applications and desktops. Additionally, understand the graphical demands of user applications, including whether they require 3D hardware acceleration or high-definition displays. Each of these considerations impacts the required bandwidth for the display protocol. Blast Extreme is the recommended display protocol and can adapt to changing network conditions.

- **Horizon 7 infrastructure design** – Determine how many Horizon 7 pods, blocks, and server components are needed to support
JMP AND VMWARE HORIZON 7 DEPLOYMENT CONSIDERATIONS

your desktop and application deployment. You need at least one pod per site.

- **Horizon 7 management block** – It is a best practice to use separate ESXi hosts for the management server VMs and the desktop and RDSH server VMs. The management block can include two to seven Connection Servers, one vCenter Server per resource block, databases, at least two App Volumes Manager servers, and at least two Unified Access Gateways. Size the hosts required depending on the type and number of servers required. The *VMware Horizon 7 Enterprise Edition Reference Architecture* details which vSphere DRS rules should be enabled on the management cluster to prevent the servers that perform identical operations from running on the same ESXi host.

- **Horizon 7 resource block** – This type of block is used to host VMs for desktops and RDSH servers. It is recommended to separate blocks into 2D desktop clusters, 3D desktop clusters, and RDSH clusters. In theory, a block could accommodate 10,000 sessions; however, the best practice recommendation is to have about 2,000 sessions per block.

- **ESXi nodes for desktops** – As a general rule, plan for 8 to 10 virtual desktops per CPU core. Think of memory capacity in terms of virtual desktop RAM, host RAM, and overcommit ratio. For more information, see *View Architecture Planning*.

- **ESXi nodes for RDSH servers** – When sizing RDSH servers, avoid overcommitting CPU resources (keep one vCPU to one physical core) and reserve the memory. Typical sizing of an RDSH VM is four vCPUs with approximately 30 GB of RAM, although memory is dependent on application usage. When sizing the ESXi hosts, plan to reserve an extra CPU core or two for virtual networking, storage, and other host tasks. For example, if the vSphere host has 22 cores, use only 20 for RDSH VMs. For more information, see *Just-in-Time Apps with VMware Horizon 7*.

- **OS optimization** – Master images should be optimized for VDI or RDSH to ensure the best performance possible in a virtualized environment and to reduce the resources consumed. The *VMware OS Optimization Tool* includes customizable templates to enable or disable Windows system services and features, per VMware recommendations and best practices, across multiple systems.

- **vSphere infrastructure design** – For vSphere architectural best practices, see the *vSphere Resource Management Guide* and the *vSphere Availability Guide*. For guidance about scalability, see the *Performance Best Practices for VMware vSphere 6.0*.

- **vSphere storage** – Consider whether to use traditional storage (SAN/NAS) or VMware vSAN, which is included in VMware Horizon 7 Advanced Edition and Horizon 7 Enterprise Edition. See also the *VMware Virtual SAN Design and Sizing Guide*.

- **vSphere network** – Configure redundant network components and separate various traffic types to distribute traffic between physical adapters and reroute traffic in the event of adapter failure. See also the *vSphere Networking Guide* and VMware knowledge base article *Configuring Flow Control on VMware ESXi and VMware ESX* (1013413).

### App Volumes Deployment Considerations

The following items give you an idea of the sorts of considerations to take into account with regard to App Volumes. For more information, be sure to read *VMware App Volumes Deployment Considerations*.

- **AppStack design** – Consider which applications to group together in a particular AppStack, and which AppStacks to assign to particular users or farms of RDSH servers. VMware recommends not assigning more than 8–10 AppStacks to one virtual desktop or RDSH server.

- **Application suitability** – Consider which applications to place in an AppStack as opposed to installing in the base OS image of the VM. For single-user desktops, if you need an application to continue to run after the user logs out, it is best to natively install this application on the master image. Do not install antivirus software or OS patches on AppStacks.

- **Writable volumes** – Consider whether and how to use writable volumes so that end users can install their own applications, or to satisfy the requirement some applications have for a local cache.

- **Storage** – Consider which storage group options to use for replicating AppStacks and writable volumes among data centers, using read-optimized storage for AppStacks, and using storage optimized for random IOPS for writable volumes.

- **Hypervisor options** – Consider whether to use the mount-on-host option to issue AppStack or writable volume mount commands directly to vSphere hosts instead of vCenter Server, and decide which settings to use for storage policies and network configuration.

### User Environment Manager Deployment Considerations

The following items give you an idea of the sorts of considerations to take into account with regard to User Environment Manager. For more information, be sure to read *VMware User Environment Manager Deployment Considerations*.
JMP AND VMWARE HORIZON 7 DEPLOYMENT CONSIDERATIONS

• Policies and settings – For each group of users, consider which applications to block from access altogether, and which condition sets to create for disabling features such as USB redirection, printing, and client-drive redirection.

• App Volumes integration – If desired, you can assign AppStacks to a VM and then capture application settings in a configuration file with the User Environment Manager Application Profiler. For more information, see VMware User Environment Manager with VMware App Volumes.

• RDSH servers – You will need to create special configurations for applying policies to computer objects rather than users (loopback processing) and for dealing with a user having multiple desktop and application sessions on one RDSH server.

• Folder redirection – Determine which folders to redirect using User Environment Manager, which folders to redirect using standard group policy, and which folders to manage using User Environment Manager import and export functionality.

• Mandatory user profiles – Consider which desktop settings to control so that changes users make are not retained when they log in again. See also VMware User Environment Manager, Part 2: Complementing Mandatory Profiles with VMware User Environment Manager.

• Application profiles – Choose the templates or tools to use to determine where an application stores its file and registry configuration settings during installation, launch, update, and so on. User Environment Manager provides templates for many commonly used applications but also includes the standalone Application Profiler application. For more information, see the VMware blog posts Profiling Applications with VMware User Environment Manager, Part 1: Introduction to Application Profiler and Part 2: Applying and Troubleshooting Predefined Settings.

• Multiple environments – If you have a multitenant infrastructure or wish to separate departments, consider using multiple User Environment Manager configuration shares and managing them from a central installation of the Management Console.

Workspace ONE Deployment Considerations

VMware Identity Manager provides the identity-related components of Workspace ONE, including identity management through synchronizing with Active Directory and enabling enterprise single sign-on (SSO) to all the applications in the Workspace ONE app catalog.

This self-service catalog is a portal for requesting and accessing SaaS-based web applications (such as Salesforce.com, Dropbox, Concur, and many others), Horizon 7–based applications and desktops, RDSH-based applications and desktops, and Citrix-based applications and desktops.

Key deployment considerations for Workspace ONE include the following:

• Choose to integrate with Workspace ONE – Because its catalog capabilities provide a single, secure point of access for Windows-based virtual desktops and applications, use the Workspace ONE app or browser-based catalog as the primary way users access resources. This strategy will keep support calls to a minimum with respect to password issues and access to applications.

• Cloud-hosted versus on-premises implementation – Although Workspace ONE can be deployed either on-premises or in the cloud, the simplest deployment and maintenance scenario is to use the Workspace ONE cloud service.

• VMware Identity Manager Connector – Determine how many of these virtual appliances you will need. Multiple appliances can be used on premises for redundancy and scale. The connector synchronizes user accounts from Active Directory to the VMware Identity Manager cloud service. Applications are then accessed from a browser-based portal or the Workspace ONE mobile app. For complete information, see Deploying the VMware Identity Manager Connector in VMware Identity Manager Cloud Deployment.

• User authentication method – Choose from one or more of the following authentication methods: AD credentials, Kerberos, RSA SecurID, certificate user authentication, and more, as described in Configuring User Authentication in VMware Identity Manager in the VMware Identity Manager Administration Guide.

• True SSO – With the True SSO feature, after users log in to Workspace ONE using any non-AD method (for example, RSA SecurID or RADIUS authentication), users are not prompted to also enter Active Directory credentials in order to use a remote desktop or application. True SSO works by generating a unique, short-lived certificate for the Windows login process. For more information, see Setting Up True SSO in View Administration.

• Unified Access Gateway – Use at least two of these virtual appliances to provide access to the catalog of virtual desktops and apps from outside the corporate network. For more information, see the VMware Unified Access Gateway Documentation.

Because this guide is focused on JMP technologies and their integration with Workspace ONE, this guide does not detail deployment
considerations for the VMware AirWatch® component of Workspace ONE. For information about the VMware AirWatch component, see the VMware Workspace ONE Enterprise Edition Reference Architecture.

**Deployment Procedures**

To aid with troubleshooting your JMP deployment, implement each technology separately before continuing on to the next. That is, install, configure, and test the Horizon 7 and vSphere infrastructure before setting up the User Environment Manager component. After you verify that these two components are working correctly, install App Volumes and create AppStacks and writable volumes.

**Horizon 7 and vSphere Deployment Overview**

The following steps provide an overview of the installation and configuration. For detailed information, see the VMware Horizon 7 Documentation, or, for certain steps, see the specific referenced document.

To deploy a Horizon 7 environment on a vSphere infrastructure:

1. Set up the required groups in Active Directory:
   - Set up the required administrator users and groups for administering Horizon 7.
   - Set up the required user groups for controlling access to desktops and RDSH-provided applications.
   - Set up the required organizational units (OUs) for computer objects that contain instant-clone desktops and RDSH servers.
   For detailed steps with screen shots, see the Reviewer’s Guide for View in VMware Horizon 7: Instant Clones.

2. Install and set up ESXi hosts and vCenter Server. See the VMware vSphere 6 Documentation. VMware vSphere Replication™ and VMware Site Recovery Manager™ can complement App Volumes deployments and should be considered for a production deployment. vSphere 6.5 is recommended.

3. Install and set up the Connection Server 7.1 or later, including configuring the event database.

4. Create one or more VMs that can be used as a master VM for instant-clone desktop pools. See the Reviewer’s Guide for View in VMware Horizon 7: Preparing Virtual Machines for Desktop Pools.

5. Set up an RDSH server VM and install applications to be remoted to end users. See Publishing Applications with VMware Horizon 7.

6. Create desktop pools, application pools, or both.

7. Entitle user access to desktops and applications. See the Reviewer’s Guide for View in VMware Horizon 7: Provisioning Users.

8. Install Horizon Client on an end user’s machine and test the access to the remote desktops and applications. See the Reviewer’s Guide for View in VMware Horizon 7: Provisioning Users.

After you successfully implement a Horizon 7 deployment, you can continue on and implement User Environment Manager in the deployment.

**User Environment Manager Deployment Overview**

The following steps provide an overview of the installation and configuration. For detailed information, see Installing and Configuring User Environment Manager. User Environment Manager 9.2 or later is recommended.

To deploy User Environment Manager:

1. Create SMB file shares for configuration data and user data.

2. Import GPO administrative templates (ADMX files) for User Environment Manager.

3. Create Group Policy settings for User Environment Manager.

4. Install the FlexEngine agent on the master VM for desktops and RDSH servers.
**Note**: Be sure to install the FlexEngine agent after you install Horizon Agent, which is part of the Horizon 7 deployment procedure.

5. Install the User Environment Manager Management Console and point to the configuration share.

6. Set a few customizations (for example, desktop shortcuts, VLC, Notepad++). Log in to the client and verify that User Environment Manager has made the requested changes.

8. Check the user log to verify User Environment Manager is working, or troubleshoot. The logs folder is in the SMB share specified for user data.

After you successfully implement User Environment Manager, you can continue on and implement App Volumes in the deployment.

### App Volumes Deployment Overview

The following steps provide an overview of the installation and configuration. For detailed information, see the [VMware App Volumes User Guide](#) and the [VMware App Volumes Reviewer’s Guide](#), which contains screen shots.

To deploy App Volumes:

1. Set up the required administrator users and groups in Active Directory.
2. Create a database instance for App Volumes Manager.
3. Install and configure the App Volumes Manager 2.11 or later.

**Important**: If you plan to use App Volumes with RDSH instant-clone server farms, you must assign App Volumes AppStacks to Active Directory OUs rather than groups. Contact Global Support Services for the App Volumes 2.12.3 hot patch. This fix will also be included in general releases of App Volumes later than 2.12.

4. Install the App Volumes Agent on the master VM for desktops and RDSH servers.

**Note**: Be sure to install the App Volumes Agent after you install the FlexEngine agent and Horizon Agent. The correct order of installation is Horizon Agent, FlexEngine agent, and App Volumes Agent. 5. Build a provisioning VM.

6. Create AppStacks and writable volumes.
8. Log in to the client and verify that the correct AppStacks are available.

After you successfully implement App Volumes, you can configure additional application settings with User Environment Manager and verify that all components are working together as expected.

### Workspace ONE Integration

To plan a Workspace ONE deployment that integrates with Horizon 7, see the [VMware Workspace ONE Enterprise Edition Reference Architecture](#). The following steps provide an overview of the installation and configuration.

To implement a Workspace ONE solution that includes Horizon 7:

1. Set up the VMware Identity Manager component of Workspace ONE:
   a. Acquire a VMware Identity Manager tenant as part of the VMware Identity Manager cloud service.
   b. Use vSphere Web Client to deploy an on-premises VMware Identity Manager Connector virtual appliance in outbound-only connection mode. This is the on-premises component for user authentication and AD integration. For a summary of the connector requirements, see [Workspace ONE Requirements](#).
   c. In the VMware Identity Manager administration console, create a directory that includes selected AD users and groups, and synchronize the directory to the VMware Identity Manager service.
   d. In the VMware Identity Manager administration console, enable the authentication adapters for the types of user authentication you plan to use.

   For detailed information about all these steps, see [VMware Identity Manager Cloud Deployment](#).

2. In Horizon Administrator, create desktop and application pools that meet certain requirements for Workspace ONE integration.
   a. Verify that you have a DNS entry and an IP address that can be resolved during reverse lookup for each Connection Server in your Horizon 7 setup.

   **Important**: VMware Identity Manager requires reverse lookup for Connection Servers, security servers, Unified
Access Gateway appliances, and load balancers. If reverse lookup is not properly configured, integration fails.

- When configuring pools on the Desktop Pool Settings tab in Horizon Administrator, ensure that in Remote Settings, you set the **Automatically log off after disconnect** option to 1 or 2 minutes instead of **Immediately**. Similarly, when configuring RDSH farm settings, on the Farm Settings tab, set **Log off disconnected sessions to 1 or 2 minutes**.
- Ensure that you create desktop pools and RDSH server farms in the root access group folder in Horizon Administrator. If you create pools in a folder other than the root access group, VMware Identity Manager cannot query those pools and entitlements.

3. In Horizon Administrator, add a SAML authenticator for VMware Identity Manager, and then extend the expiration period for service provider metadata to 90 days. See Configure a SAML Authenticator in View Administrator and Change the Expiration Period for Service Provider Metadata on View Connection Server in View Administration. Integration between Horizon 7 and VMware Identity Manager uses the SAML 2.0 standard to establish mutual trust, which is essential for single sign-on (SSO) functionality. With SSO, users can log in to VMware Identity Manager and launch Horizon 7 desktops and apps without having to go through a second login procedure.

4. In the VMware Identity Manager administration console, add Connection Server details and sync with the Connection Server instance. See Integrating Independent View Pods in Setting Up Resources in VMware Identity Manager.

**Note:** To integrate a Horizon 7 Cloud Pod Architecture rather than an independent pod, you must integrate all pods in the federation, add the pod federation details, and sync resources and entitlements from the pod federation. See Integrating View Cloud Pod Architecture (CPA) Deployments in Setting Up Resources in VMware Identity Manager.

5. Deploy one or more Unified Access Gateway virtual appliances so that users can access their virtual desktop and application resources over the Internet. See Deploying and Configuring Unified Access Gateway.

6. Install, or have your end users install, the Workspace ONE app on end users’ devices for access to Workspace ONE. Both the Workspace ONE app and the Horizon Client app are designed to provide a consistent user experience for every operating system while at the same time being integrated into the OS to take advantage of OS-specific features. For example, on iOS you can use Touch ID to authenticate, and on Windows 10, you can use Windows Hello to authenticate.

### Managing Desktops and Applications

This section lists many of the best practices and considerations for maintaining and operating a production JMP environment.

#### Desktop and RDSH Image Management

After your desktops and RDSH servers are deployed, as described in Horizon 7 and vSphere Deployment Overview, ongoing maintenance is a straightforward and largely automated process.

- To maintain desktop VMs in an optimal state, the system deletes the VM when users log out. Users automatically get a fresh VM when they log in again.
- To maintain RDSH server VMs in an optimal state, set a maintenance schedule. VMs in the farm are deleted according to this schedule and new VMs are created. The OS disk is restored to its original state and size. See Publishing Applications with VMware Horizon 7.

**Note:** To achieve zero downtime, you can edit the farm and specify the minimum number of RDSH servers that must remain available for users during these maintenance operations.

- To update the master image, install the updates, run the VMware OS Optimization Tool, and use the recommended utilities to reclaim disk space, as described in Just-in-Time Apps with VMware Horizon 7, before taking a new VM snapshot.
- To update single-user desktops, use the Push Image operation on the Horizon Administrator desktop pool Summary tab to schedule the update and force users to log out if necessary. See the Reviewer’s Guide for View in VMware Horizon 7: Instant Clones.
- To update RDSH servers, select Immediate for the maintenance schedule, and select the new updated master image. The Immediate maintenance schedule works similarly to the Push Image operation for desktops. See Just-in-Time Apps with VMware Horizon 7.
Application Management

Most of the following general App Volumes recommendations are excerpted from the Best Practices for an App Volumes Deployment in Production section of VMware App Volumes Deployment Considerations:

- Always use at least two App Volumes Managers for redundancy, fronted with a load balancer.
- Use the Storage Groups feature to balance AppStack load across multiple datastores.
- Use the Mount on Host feature to issue AppStack or writable volume mount commands directly to vSphere hosts instead of vCenter Server.

This feature speeds up the mount and login process and reduces overall load on vCenter Server. To use this feature, verify that the ESXi hosts use the same root-level user credentials.

- On the VM that you use for provisioning an AppStack, make sure that no AppStacks have ever been attached to the VM, that the VM has never before been used for provisioning, and that the VM does not have Horizon Agent, App Volumes Agent, or the User Environment Manager FlexEngine service installed.

These agents are instead installed on the master VM used for creating the instant-clone desktop pool or RDSH server farm.

- For single-user desktops, if you need an application to continue to run after the user logs out, it is best to natively install this application on the master image.
- Do not install kernel mode applications, such as antivirus software or OS patches, on AppStacks.
- Group multiple applications together into an AppStack so as to avoid assigning more than 8–10 AppStacks to a particular user, group, or RDSH server.
- If multiple AppStacks are assigned to a user, group, or RDSH server, the last AppStack to be attached takes precedence.

To avoid application conflict, in App Volumes Manager, use the Override Precedence option to control the order in which AppStacks are attached.

- When assigning AppStacks to RDSH servers, be sure to assign the AppStacks to the Active Directory OU that contains the RDSH server computer objects.

During maintenance operations, RDSH server VMs are deleted and recreated, possibly with new computer names. Assigning the AppStack to the OU ensures that the AppStack is attached to all computer objects in the OU, regardless of computer name.

With regards to using AppStacks for Microsoft Office applications, you have a choice of several strategies:

- You can install core Microsoft Office 2013 or 2016 applications in the base virtual desktop image and create an AppStack for non-core Office applications, such as Visio, Project, or Visio and Project together.

For more information, see the VMware App Volumes Technical FAQ.

- You can install all Office 2013 or 2016 applications in an AppStack. See the VMware knowledge base article Installing and Using Microsoft Office Products with VMware App Volumes 2.x (2146035).
- If you plan to use Microsoft Office 365, which does not support two separate Click-to-Run packages on the same computer, you can deploy all Office applications as a single Click-to-Run package to a single AppStack, or create separate AppStacks with all required combinations and assign them to appropriate domain groups.

For example, create one AppStack with Office 365 for one group and another AppStack with Office 365 plus Visio for another group. See the VMware App Volumes Provisioning Recipe for Microsoft Office 365.

- You can install Microsoft Office 365 in the master RDSH image and not use AppStacks at all.

For instructions, see Best Practices for Delivering Microsoft Office 365 in VMware Horizon 7 with Published Applications.

User Profile and Settings Management

User Environment Manager provides easy-to-use templates for specifying the Windows environment settings and application settings.
that you want to control on a per-user or per-group basis. The settings can be applied based on various conditions and triggering events, and you can control whether the user is allowed to change the default settings you specify.

- Use User Environment Manager in combination with applications you bundle into App Volumes AppStacks. There is no difference in User Environment Manager between an App Volumes application or a natively installed application. See VMware User Environment Manager with App Volumes.
- Use the DirectFlex feature so that application settings are imported and applied at application launch rather than when the user logs in. See VMware User Environment Manager Deployment Considerations and the User Environment Manager Administration Guide.
- Do not use roaming profiles. The Windows roaming profiles feature copies information about all Windows settings and user data, which increases login times to an unacceptable level. Instead configure folder redirection with User Environment Manager, and configure mandatory user profiles.

User Environment Manager is a whitelist technology, which means that user profiles contain data about only those settings you wish to control. For more information, see VMware User Environment Manager, Part 2: Complementing Mandatory Profiles with VMware User Environment Manager.

- To create the User Environment Manager Flex configuration file that contains settings for an application you want to manage, you can use predefined application templates or the Application Profiler, as described in Profiling Applications with VMware User Environment Manager, Part 1: Introduction to Application Profiler.
- When managing an application update, you can use the Application Migration tab in User Environment Manager to apply a user’s application settings to the new version of the application. See the User Environment Manager Administration Guide.

Application Access with Workspace ONE

Workspace ONE provides the central platform for users to access their digital workspace. All Microsoft Windows, SaaS, web, Citrix, and mobile apps can be accessed securely through Workspace ONE from any device.

![Workspace ONE App Catalog](image)

**Figure 5**: The Workspace ONE App Catalog

Be sure to follow these best practices with regard to Workspace ONE:

- Ensure all users are using Workspace ONE as the single way to access their virtualized Windows apps and desktops, as well as SaaS apps and public mobile apps. This approach simplifies client support for users accessing corporate resources.
To entitle users to Horizon 7 desktops and apps, administrators simply add the entitlements in Horizon 7, and those entitlements are automatically synchronized to the Workspace ONE app catalog. For more information, see Entitling Users and Groups in Setting Up Published Desktops and Applications in Horizon 7 or Setting Up Virtual Desktops in Horizon 7.

For applications outside of Horizon 7, administrators can use Workspace ONE to entitle users. For more information, see Add Resources to Groups in the VMware Identity Manager Administration Guide.

Optionally, by integrating VMware AirWatch, administrators can provide a catalog that includes mobile applications. See Integrating AirWatch with VMware Identity Manager in the VMware Identity Manager Administration Guide.

If you need enhanced security, consider creating an authentication chain that connects authentication options and ties them to selected network locations. With an authentication chain, if one option fails, the authentication falls back to the next option in the chain. See Configuring Access Policy Settings in the VMware Identity Manager Administration Guide.

If you plan to add many apps and virtual desktops to the Workspace ONE catalog, group resources (apps and desktops) into logical categories to make it easier for users to locate the resource they need. You can assign more than one category to a resource. See Grouping Resource into Categories in the VMware Identity Manager Administration Guide.

### Appendix A: Deployment Requirements

The tables listed in the following sections summarize the requirements for various technologies. For more information about the requirements, see the VMware Horizon 7 Enterprise Edition Reference Architecture.

### Requirements Common to All Components

The following requirements are shared by the JMP technologies.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
<td>VMware vSphere 6.0 Update 2 or later (Instant Clone Technology support); vSphere 6.5 or later recommended</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>VMware vSphere 6.0 Update 2 or later (Instant Clone Technology support); vSphere 6.5 or later recommended</td>
</tr>
<tr>
<td></td>
<td>If you use a Windows Server VM instead of a vCenter Server virtual appliance, note the following requirements:</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 or Windows Server</td>
</tr>
<tr>
<td></td>
<td>• 2 vCPU and 4 GB RAM, with 1 NIC</td>
</tr>
<tr>
<td></td>
<td>• Static IP address</td>
</tr>
<tr>
<td>Active Directory server</td>
<td>• Microsoft AD domain, 2008 functional or later</td>
</tr>
<tr>
<td></td>
<td>• Static IP address</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>Can be used to create database instances for App Volumes Manager, vCenter Server, and the Horizon 7 Events database:</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>• 8 vCPU and 24 GB RAM, with 1 NIC</td>
</tr>
<tr>
<td>Security certificates</td>
<td>By default, and for testing purposes, a self-signed server security certificate is installed in the various server components. For a production environment, VMware recommends that you replace self-signed certificates with approved certificates signed by a certificate authority, a trusted entity that issues digital certificates verifying another digital entity’s identity on the Internet.</td>
</tr>
</tbody>
</table>

| Table 1: Common Requirements |
### Horizon 7 Requirements

The following table lists requirements specific to Horizon 7 and Instant Clone Technology.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server user accounts</td>
<td>For Horizon Administrator, an account that is assigned a role with the required privileges. For a list of the privileges to include in the role, see Privileges Required for the vCenter Server User in the View Installation guide.</td>
</tr>
</tbody>
</table>
| AD accounts                | • For Horizon Administrator, a designated AD user group that allows administrator access to the Connection Server used for accessing the Horizon Administrator console.   
• For instant clones, a domain user account that has permission to create computer objects, delete computer objects, and write properties in the domain. (See the Reviewer’s Guide for View in VMware Horizon 7: Instant Clones.)
• For instant clones, OUs of computer accounts for instant-clone VMs for single-user virtual desktops and RDSH session-based desktops and apps. (See the Reviewer’s Guide for View in VMware Horizon 7: Instant Clones.)
• OUs for user groups, to provide application and desktop entitlement as well as finegrained policy control |
| Connection Server          | • Horizon 7 version 7.1 or later  
• Windows Server 2012 R2 or Windows Server 2016
• 4 vCPU and 12 GB RAM, with 1 NIC  
• DNS entry (must be resolvable using reverse lookup for Workspace ONE integration)  
• Static IP address (must be resolvable using reverse lookup for Workspace ONE integration) |
| Master image storage       | Can use traditional, spinning media-backed datastores. These disks provide lower performance, typically supporting 200 IOPS. They are inexpensive and provide high storage capacity, which makes them suited for storing a large number of clones. Note: VMware vSAN automatically places VMs on the correct type of storage. |
| Replica storage            | For a tiered-storage model, use a solid-state, disk-backed datastore. Solid-state disks have low storage capacity and high-read performance, typically supporting 20,000 IOPS. |
| Instant-clone storage      | • Can use traditional, spinning media-backed datastores  
• Do not place AppStacks and VMs on the same datastore (unless using VMware vSAN). |
| Virtual desktop            | • Windows 7 or Windows 10  
• 2 vCPU and 4 GB RAM is typical for Windows 10. |
| RDSH server                | • Windows Server 2008 R2 or Windows Server 2012 R2  
• 4 vCPU and 30 GB RAM |
| Basic networking access    | The following default settings can be customized:  
• Horizon Administrator web console: 443 (HTTPS)  
• For a complete list of ports, see the Ports and Services chapter of the View Security guide.  
• See also the Network Ports Diagram Updated for Horizon 7. |

**Table 2: Horizon 7 Requirements**

For more information about these system requirements see VMware Horizon 7 Documentation. For information about obtaining and configuring security certificates, see Configuring SSL Certificates for View Servers in the View Installation guide.
User Environment Manager Requirements
The following table lists requirements specific to User Environment Manager.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>REQUIREMENT</th>
</tr>
</thead>
</table>
| User Environment Manager Management Console | • User Environment Manager 9.2 or later  
• Install the User Environment Manager Management Console component on any desktop from which you want to manage the environment—no server infrastructure required! |
| User Environment Configuration Share   | This can be the same server as is used for the profile (user data) share.  
• Windows Server 2012 R2 SMB (Server Message Block) file share  
• 1 GB disk space per 5,000 users  
• Resides in the same data center or network as virtual desktops  
• NTFS security permissions: For administrators, full control over users’ folders, subfolders, and files; for users, permission to read and execute files in that user’s folder  
Note: Microsoft Distributed File System (DFS) is supported. |
| User Environment Manager Profile Share | This can be the same server as is used for the configuration share.  
• Windows Server 2012 R2 SMB file share  
• 100 MB disk space per user  
• NTFS security permissions: For administrators, full control over users’ folders, subfolders, and files; for users, permission to create that user’s folder and append data  
• File server: 4 vCPU and 16 GB RAM for servicing 10,000 users  
Note: Microsoft Distributed File System (DFS) is supported. |

Table 3: User Environment Manager Requirements
For more information about these system requirements, see Installing and Configuring User Environment Manager.

App Volumes Requirements
The following table lists requirements specific to App Volumes.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server user accounts</td>
<td>A service account within a vCenter Server with administrator privileges</td>
</tr>
</tbody>
</table>
| AD accounts                            | • A designated AD user group that allows administrator access to the App Volumes Manager server  
• A read-only AD account for each domain that App Volumes Agents will reside in |
| App Volumes Manager                    | • App Volumes 2.11 or later  
Important: If you plan to use App Volumes with RDSH instant-clone server farms, you must assign App Volumes AppStacks to Active Directory OUs rather than groups. Contact Global Support Services for the App Volumes 2.12.3 hot patch. This fix will also be included in general releases of App Volumes later than 2.12.  
• Windows Server 2012 R2  
• 2 vCPU and 2 GB RAM, with 1 NIC  
• .NET 3.5 Framework  
• Static IP address  
• Application Server role installed |
| AppStacks storage                      | • Flash or hybrid-flash storage recommended  
• Shared storage for all ESXi hosts that host desktops connecting to AppStacks and writable volume  
• Approximately 20 GB disk space per AppStack (can be configured) |
| Provisioning VM                        | • Must match the OS of the master virtual desktop VM or RDSH server VM  
• For RDSH servers, RAM can be 12 GB rather than 30 GB |
| Basic networking access                | The following default settings can be customized:  
• App Volumes Manager web console: 80 (HTTP), 443 (HTTPS)  
• App Volumes Agent-to-server communications: 80 (HTTP), 443 (HTTPS)  
• App Volumes server to vCenter Server and ESXi hosts: 443 (SOAP/hosted)  
• App Volumes server to remote SQL Server: 1433 |
Table 4: App Volumes Requirements

For more information about these system requirements see the VMware App Volumes User Guide.

Workspace ONE Requirements

The following table lists requirements specific to the VMware Identity Manager connector component of Workspace ONE.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise directory</td>
<td>One of the following directory types:</td>
</tr>
<tr>
<td></td>
<td>• Active Directory over LDAP, for a single AD domain</td>
</tr>
<tr>
<td></td>
<td>• Active Directory using Integrated Windows Authentication, for multi-domain</td>
</tr>
<tr>
<td></td>
<td>or multiforest AD environments with or without trust relationships</td>
</tr>
<tr>
<td>VMware Identity Manager connector virtual appliance</td>
<td>• VMware Identity Manager 2.9.1 or later (on-premises) or the latest version of VMware Identity Manager Cloud Hosted</td>
</tr>
<tr>
<td></td>
<td>• DNS entry</td>
</tr>
<tr>
<td></td>
<td>• Static IP address</td>
</tr>
<tr>
<td></td>
<td>• 2 vCPU and 6 GB RAM, 24 GB disk space</td>
</tr>
<tr>
<td></td>
<td>• Ability to access the enterprise directory to sync users and groups</td>
</tr>
<tr>
<td></td>
<td>See the topics Integrating with Your Enterprise Directory and Integrating with Active Directory in VMware Identity Manager Cloud Deployment.</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Several user authentication methods are available and can be used individually or in combination: AD credentials, Kerberos, RSA SecurID, certificate user authentication, and more. For more information, see Configuring User Authentication in VMware Identity Manager in the VMware Identity Manager Administration Guide.</td>
</tr>
<tr>
<td>Basic networking access</td>
<td>• VMware Identity Manager: 443 (HTTPS)</td>
</tr>
<tr>
<td></td>
<td>• VMware Identity Manager connector administration console: 8443 (HTTPS)</td>
</tr>
<tr>
<td></td>
<td>• For a complete list of port requirements, see the System and Network Configuration Requirements in VMware Identity Manager Cloud Deployment.</td>
</tr>
</tbody>
</table>

Table 5: Workspace ONE Requirements

For more information about system requirements, see the VMware Workspace ONE Enterprise Edition Reference Architecture and VMware Identity Manager Cloud Deployment.

Additional Resources

Installing and using Microsoft Office Products with VMware App Volumes 2.x (2146035) (VMware knowledge base article)

Just-in-Time Apps with VMware Horizon 7 (VMware blog post)

Performance Best Practices for VMware vSphere 6.0

Profiling Applications with VMware User Environment Manager, Part 1: Introduction to Application Profiler and Part 2: Applying and Troubleshooting Predefined Settings (VMware blog posts)

Publishing Applications with VMware Horizon 7

Reviewer’s Guide for View in VMware Horizon 7

Reviewer’s Guide for Cloud-Based VMware Workspace ONE

VMware App Volumes Deployment Considerations
VMware App Volumes Reviewer’s Guide
VMware App Volumes Technical FAQ
VMware App Volumes User Guide
VMware Horizon 7 Documentation
VMware Horizon 7 Enterprise Edition Multi-Site Reference Architecture
VMware Horizon 7 Enterprise Edition Reference Architecture
VMware OS Optimization Tool
VMware User Environment Manager Deployment Considerations
VMware User Environment Manager Documentation
VMware User Environment Manager with VMware App Volumes (VMware blog post)
VMware User Environment Manager, Part 2: Complementing Mandatory Profiles with VMware User Environment Manager (VMware blog post)
VMware Virtual SAN Design and Sizing Guide
VMware vSphere 6 Documentation
VMware Workspace ONE Enterprise Edition Reference Architecture
Workspace ONE Documentation

About the Authors and Contributors

The following team wrote this document:

• Caroline Arakelian, Senior Technical Marketing Manager, End-User-Computing Technical Marketing, VMware
• Matt Coppinger, Director in VMware End-User-Computing Technical Marketing, VMware
• Josh Spencer, EUC Architect, EUC Technical Marketing, VMware
• Graeme Gordon, Senior EUC Architect, EUC Technical Marketing, VMware
• Jim Yanik, Senior Manager, End-User-Computing Technical Marketing, VMware
• Todd Dayton, Principal Systems Engineer, End-User Computing, VMware

To comment on this paper, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.