## Table of Contents

**Executive Summary** ................................................................. 5

**VMware Reference Architectures** ............................................ 7
  Audience ................................................................. 7

**Horizon 7 Enterprise Edition Solution Overview** .......................... 8
  Platform Integration .................................................. 10

**Reference Architecture Design Methodology** .............................. 11

**Business Drivers and Use Cases Definition** ................................. 12
  Business Drivers and Requirements .................................. 12
  Use Cases ................................................................. 12
  Addressing Business Requirements with Horizon 7 Enterprise Edition 13

**Horizon 7 Services Definition** .................................................. 14
  Business Process Application Service ................................ 14
  Mobile Secure Workspace Service .................................. 15
  Dedicated Power Workspace Service ................................. 17
  Developer Workspace Service ....................................... 18
  High-Performance Workspace Service ................................ 19

**Architecture Principles and Concepts** ......................................... 20
  Pod and Block ............................................................ 20
  Horizon 7 Enterprise Edition Logical Architecture ................. 21

**Horizon 7 Enterprise Edition Component Design** .......................... 23
  VMware Identity Manager ........................................... 23
  View in Horizon ...................................................... 29
  Protocol ................................................................. 33
  Access Point ............................................................. 34
  VMware App Volumes .................................................. 40
  VMware User Environment Manager ................................ 44
  True SSO ................................................................. 48
  VMware vRealize Operations Manager for Horizon ................ 51
  VMware ThinApp .......................................................... 54
  Load Balancing and External Access ................................ 55

**vSphere Infrastructure Design** .................................................... 59
  vSphere ................................................................. 59
  Virtual SAN .............................................................. 61
  Networking ............................................................... 62

**Physical Environment Design** .................................................... 63
  Active Directory ........................................................ 63
  Group Policy ............................................................. 63
  DNS ................................................................. 63
  DHCP ................................................................. 64
  Certificate Authority .................................................. 64
  Key Management Service .............................................. 64
Appendix C: Horizon Installation and Configuration

About the Authors and Contributors

User Experience Design

Service Integration Design

Appendix A: Use Case Definitions

Appendix B: Management Virtual Machine Specifications

Appendix C: Horizon Installation and Configuration

Appendix D: Access Point Installation and Configuration
Horizon-Specific Settings ................................................................. 101
Firewall Rules ........................................................................... 103
Deployment .................................................................................. 104
Deployment Steps ......................................................................... 104
Appendix E: Building a Master VM Template. ................................. 105
  Build a New VM and Tune Hardware ......................................... 105
  vGPU Specifications .................................................................. 105
  Tune Windows ........................................................................... 105
  VMware OS Optimization Tool .................................................. 108
  RDSH Specifications ................................................................. 108
  Applications .............................................................................. 108
  Antivirus Best Practices (If not Using Endpoint Antivirus) .......... 108
  Install VMware Tools and Agents. ............................................. 108
  Finalize ..................................................................................... 109
Appendix F: Group Policies ............................................................... 110
  OU GPO Best Practices ............................................................ 110
  Common GPO Settings ............................................................ 110
  Desktop ...................................................................................... 110
  RDS Host OU Level .................................................................. 111
  User Configuration Settings ...................................................... 112
  User Environment Manager – Group Policy Settings .................. 112
Appendix G: Smart Policies ............................................................... 114
Appendix H: Mandatory Profile ....................................................... 116
  Create the Mandatory Profile .................................................. 116
  Configure Active Directory Group Policies for Mandatory Profile . 117
Appendix I: VMware App Volumes Install and Configure ................. 118
  Prerequisites ............................................................................ 118
  Install ...................................................................................... 118
  Next Steps ................................................................................ 118
Appendix J: Printing ....................................................................... 119
  USB Redirection and Printing .................................................... 119
  Location-Based Printing Overview .......................................... 119
  Printing Environment ............................................................... 120
Executive Summary
This paper describes how to address business requirements and use cases with services constructed by integrating the components of VMware Horizon® 7 Enterprise Edition.

It is intended to help customers—IT architects, consultants, and administrators—involved in the early phases of planning, design, and deployment by offering a standard, repeatable, and highly scalable approach to design and integration that can easily be adapted to specific environments and requirements.

The approach taken in this paper is, as with any technology solution, to start by defining business requirements and drivers. These requirements can, in turn, be mapped to use cases that can be adapted to most scenarios.

With Horizon 7 Enterprise Edition we can deliver solutions for these use cases by creating services composed of several components in a very efficient and reusable manner. The resultant environment and the services delivered can easily be adapted to address changes in the business and use cases.

One key step in addressing the use cases is the definition of blueprints for the services to be delivered. This allows us to understand the components and parts that need to be designed, built, and integrated.

Figure 1: Sample Service Blueprint
To provide a common experience, to address more than just the Windows applications, and to future-proof the solution, this reference architecture also includes VMware Identity Manager™ in every use case. VMware Identity Manager is a service that extends the on-premises directory infrastructure to provide a seamless single sign-on (SSO) experience to Web, mobile, SaaS, and legacy applications.

Figure 2: User Workspace Through VMware Identity Manager

A modular, repeatable design approach allows the components and services to be combined in various ways to customize the end-user experience without the need for specific configuration for individual users. This provides operational ease and flexibility by using common nonpersistent building parts and integrating the user configuration and environment to provide a persistent user experience.

This architecture utilizes key features of Horizon 7 Enterprise Edition such as Just-in-Time Delivery, which combines Instant Clone Technology, VMware App Volumes™, and VMware User Environment Manager™ to provide the accelerated delivery of OS, applications, and user configuration. This combination produces user-customized and fully personalized desktops from standardized building blocks.

VMware vSphere® is the foundation platform for any Horizon 7 Enterprise Edition environment. This paper designs and builds out the requirements and best practices using VMware Virtual SAN™ as a storage platform. Virtual SAN comes with Horizon 7 Enterprise Edition and provides an excellent scalable storage layer; however, other storage types can be used instead.

This reference architecture underwent validation of design, environment adaption, component design and build, service build, integration, user workflow, and testing to ensure that all the objectives were met, the use cases were delivered properly, and that real-world application is achievable.
VMware Reference Architectures

VMware reference architectures are designed and validated by VMware and supporting partners to address common use cases, such as enterprise desktop replacement, remote access, and disaster recovery.

This reference architecture is intended to provide detailed configuration information and example architecture for deploying all products in an integrated manner.

This Horizon 7 Enterprise Edition reference architecture presents high-level design and low-level configuration for the key features and integration points of Horizon 7 Enterprise Edition to form cohesive services to address typical business use cases.

VMware reference architectures offer customers:

• Standardized, validated, repeatable components
• Scalable designs that allow room for future growth
• Validated and tested designs that reduce implementation and operational risks
• Quick implementation, reduced costs, and minimized risk

This reference architecture does not provide performance data or stress testing metrics. However, it does provide a structure and guidance on architecting in repeatable blocks for scale. The principles followed include the use of high availability, load balancing, and ensuring that there are no single points of failure to provide a production-ready design.

Audience

This reference architecture helps customers, IT architects, consultants, and administrators involved in the early phases of planning, designing, and deploying Horizon 7 Enterprise Edition solutions.

The reader should have:

• A solid understanding of desktop and application virtualization
• Familiarity with View desktops in VMware Horizon
Horizon 7 Enterprise Edition Solution Overview

With the introduction of Horizon 7 Enterprise Edition, VMware is drawing on the best of mobile and the cloud, offering greater simplicity, security, speed, and scale in delivering on-premises virtual desktops and applications with cloud-like economics and elasticity of scale.

With this latest release, customers can now enjoy key features such as:

- **JMP (Next-Generation Desktop and Application Delivery Platform)** - 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.
• **Just-in-Time Desktops** – Leverages Instant Clone technology coupled with App Volumes to dramatically accelerate the delivery of user-customized and fully personalized desktops. Dramatically reduce infrastructure requirements while enhancing security by delivering a brand new personalized desktop and application services to end users every time they log in.
  - Reap the economic benefits of stateless, nonpersistent virtual desktops served up to date upon each login.
  - Deliver pristine, high-performance personalized desktops to end users every time they log in.
  - Improve security by destroying desktops every time a user logs out.

• **VMware App Volumes** – Provides real-time application delivery and management.
  - Quickly provision applications at scale.
  - Dynamically attach applications to users, groups, or devices, even when users are logged into their desktop.
  - Provision, deliver, update, and retire applications in real time.
  - Provide a user-writable volume allowing users to install applications that follow them across desktops.

• **VMware User Environment Manager** – Offers personalization and dynamic policy configuration across any virtual, physical, and cloud-based environment.
  - Provide end users with quick access to a Windows workspace and applications, with a personalized and consistent experience across devices and locations.
  - Simplify end-user profile management by providing organizations with a single and scalable solution that leverages existing infrastructure.
  - Speed up login process by applying configuration and environment settings in an asynchronous process instead of all at login.
  - Provide dynamic environment configuration, such as drive or printer mappings when a user launches an application.

• **Horizon Smart Policies** – Delivering a real-time, policy-based system that provides contextual, fine-grained control. IT can now intelligently enable or disable client features based on user device, location, and more.
  - Conditions can be reevaluated on specific events, such as user reconnect, allowing the policies to be contextually applied and reassessed.
  - With True SSO, users benefit from single-click, password-free login to their Windows desktops and apps through a single digital workspace.

• **Blast Extreme** – Purpose-built and optimized for the mobile cloud, this new additional display technology is built on industry-standard H.264, delivering a high-performance graphics experience accessible on billions of devices including ultra-low-cost PCs.
  - Multi-codec – Blast Extreme supports the JPG/PNG and H.264 codecs.
  - Multi-protocol – Supports both TCP and UDP transport protocols.
  - Adaptation
    » Automatically selects the appropriate codec based on endpoint and policy.
    » Automatically selects the appropriate transport protocol based on network conditions and policy.
Platform Integration
VMware Horizon 7 Enterprise Edition extends the power of virtualization with virtual compute, virtual storage, and virtual networking and security to drive down costs, enhance the user experience, and deliver greater business agility.

Horizon 7 Enterprise Edition can leverage native storage optimizations from vSphere including SE Sparse, VAAI, and storage acceleration to drive down storage costs while delivering a superior user experience.

Horizon 7 Enterprise Edition with Virtual SAN Advanced for Desktop automates storage provisioning and leverages direct-attached storage resources to drive down storage costs for desktop workloads. Horizon supports all-flash capabilities to better support more end users at lower costs across distributed locations.
Reference Architecture Design Methodology

Before rushing into any build of a Horizon 7 Enterprise Edition environment, it is important to follow proper design methodology. To address business requirements, first identify the needs of the users and organize these into use cases. Then align and map those use cases against a set of integrated services built on Horizon 7 Enterprise Edition.

A Horizon 7 Enterprise Edition design uses a number of complementary components to provide these highly available services to address the identified use cases. Before we can assemble and integrate these together to form a service, we first need to design and build the Horizon and vSphere infrastructure required. We also need to consider integration into the existing environment.

Finally, we can bring the parts together to deliver the integrated services to satisfy the use cases, business requirements, and the user experience.

As with any design process this is cyclical and any previous decision should be revisited to make sure a subsequent one has not impacted it.
Business Drivers and Use Cases Definition

An end-user computing (EUC) solution based on VMware Horizon 7 Enterprise Edition can address a wide-ranging set of business requirements and use cases. In this particular reference architecture, the solution targets the most common requirements and use cases seen in customer deployments to date.

Business Drivers and Requirements

Any technology solution should directly address critical business requirements and drivers. Each and every design choice should center on a specific business requirement. Business requirements could be driven by the “end user” or by the team deploying EUC services. The top eight common key business drivers addressed by this solution are:

1. Provide greater “business mobility” by providing mobile access to modern and legacy applications via laptop, tablet, and smartphone.
2. Reduce user support calls by simplifying and securing access to applications.
3. Allow fast provisioning of and secure access for internal users and third-party suppliers to line-of-business applications.
4. Centralize and secure corporate data to meet compliance standards.
5. Reduce application management overhead and reduce application provisioning time.
6. Simplify root cause analysis and time to resolution of user issues.
7. Reduce physical device management overhead.
8. Allow users to access corporate applications and data from their own devices.

Use Cases

Use cases drive the design for any EUC solution and dictate which technologies are deployed to meet user requirements. Use cases can be thought of as common user scenarios. For example, a finance or marketing user may be considered a “normal office worker” use case. This section describes the common use cases. (For more details, see Appendix A: Use Case Definitions.)

<table>
<thead>
<tr>
<th>USE CASE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Task Worker</td>
<td>Workers typically fixed to a specific location with no remote access requirement. Some examples include call center worker, administration worker, retail user, and so on.</td>
</tr>
<tr>
<td>Mobile Knowledge Worker</td>
<td>Could be a hospital clinician, a company employee, or a finance or marketing role. This is a catch-all use case for many corporate use cases.</td>
</tr>
<tr>
<td>Software Developer / IT (Power User)</td>
<td>Power users that require administration rights to install applications. Could be using Windows or Linux OS, with many applications, some of which require extensive CPU and memory resources.</td>
</tr>
<tr>
<td>Multimedia Designer / Engineer</td>
<td>Intensive users that require GPU accelerated applications and/or intensive CPU and memory workloads. Examples are CAD/CAM designer, architect, video editor/reviewer, graphics artist, or game designer.</td>
</tr>
<tr>
<td>Contractor</td>
<td>External contractor that requires access to specific line-of-business applications, typically from a remote or mobile location.</td>
</tr>
</tbody>
</table>

Table 1: Common Use Cases
Addressing Business Requirements with Horizon 7 Enterprise Edition

<table>
<thead>
<tr>
<th>BUSINESS DRIVER</th>
<th>HORIZON 7 ENTERPRISE EDITION SOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile access</td>
<td>Horizon 7 Client technology supports all mobile and laptop devices as well as common operating systems. Horizon 7 Access Point appliances provide secure external access without the need for VPN.</td>
</tr>
<tr>
<td>Reduced support calls</td>
<td>VMware Identity Manager provides a single self-service portal to all applications and, in conjunction with True SSO, provides a platform for single sign-on. Users no longer need to remember passwords or request applications via support.</td>
</tr>
<tr>
<td>Fast provisioning and access</td>
<td>Horizon 7 Enterprise Edition can provision hundreds of desktops in minutes using Instant Clone technology. Horizon 7 provides the ability to entitle groups or users to pools of desktops quickly and efficiently. Horizon 7 Access Point provides a secure and simple mechanism for external users to access desktops customized using User Environment Manager. Applications are delivered on a per-user basis using App Volumes.</td>
</tr>
<tr>
<td>Centralize and secure</td>
<td>Horizon 7 is an on-premises virtual desktop solution where user data, applications, and desktop activity do not leave the data center. VMware vSphere is a market-leading trusted virtualization platform to run desktop or application workloads. Additional Horizon 7 and User Environment Manager policies restrict and control user access to data.</td>
</tr>
<tr>
<td>Reduce application management</td>
<td>App Volumes provides a simple solution to managing and deploying applications. Applications can be deployed “once” to a single central file and accessed by thousands of desktops. This simplifies application maintenance, deployment, and upgrades. VMware ThinApp® provides additional features to isolate or make applications portable across platforms.</td>
</tr>
<tr>
<td>Improve time to resolution</td>
<td>Reacting to user issues is critical to any enterprise EUC solution. VMware vRealize® Operations Manager™ for Horizon provides a “single pane of glass” for monitoring and predicting the health of any entire Horizon 7 infrastructure. From user protocol performance to storage and compute utilization, vRealize Operations Manager for Horizon provides an extremely fast way to determine root cause.</td>
</tr>
<tr>
<td>Reduce device management overhead / enable BYOD</td>
<td>By moving to a virtual desktop and app solution, there is no need to manage client devices, applications, or images. A thin client, zero client, or employee-owned device (Bring Your Own Device) could be used in conjunction with Horizon 7 Client. IT now has the luxury of just managing single images of virtual desktops in the data center.</td>
</tr>
</tbody>
</table>

Table 2: Business Drivers
Horizon 7 Services Definition
From our business requirements we outlined several typical use cases and their requirements. Taking the business requirements and combining them with a use case(s) enables the definition of a service.

The service defines the unique requirements and identifies the technology or feature combinations that will satisfy those unique requirements. Once the service has been defined, you can define the service quality that will be associated with that service. These qualities will include performance, availability, security, and management / monitoring requirements to meet SLAs.

**Note:** The remainder of this document details the design to satisfy each of the service definitions.

Do not treat the list of services as exclusive or prescriptive; each environment is different. Adapt the services to your particular use cases. In some cases, that may mean adding additional components while in others it may be possible to remove some that are not required. You could also look to combine multiple services together to address more complex use cases.

The following are core components that are used across all use cases.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Identity Manager</td>
<td>Single sign-on, SaaS applications</td>
</tr>
<tr>
<td>vSphere</td>
<td>Infrastructure platform</td>
</tr>
<tr>
<td>Virtual SAN</td>
<td>Storage platform</td>
</tr>
<tr>
<td>vRealize Operations for Horizon</td>
<td>Management and monitoring</td>
</tr>
<tr>
<td>Horizon 7</td>
<td>Virtual desktops and RDS remoted apps</td>
</tr>
<tr>
<td>App Volumes</td>
<td>Application deployment</td>
</tr>
<tr>
<td>User Environment Manager</td>
<td>User profile, IT settings, and configuration for environment and applications</td>
</tr>
</tbody>
</table>

Table 3: Core Components

Business Process Application Service
**Overview:** Windows applications are delivered as RDSH-based remoted apps. The RDS hosts are linked clones to provide space and operational efficiency. Applications are delivered through App Volumes. Individual or conflicting applications are packaged with ThinApp and available through the VMware Identity Manager catalog. User Environment Manager applies profile settings and folder redirection.

**Use Case:** Static Task Worker

<table>
<thead>
<tr>
<th>UNIQUE REQUIREMENTS</th>
<th>COMPONENTS</th>
</tr>
</thead>
</table>
| Small number of Windows applications | • Horizon 7 RDSH remoted applications are a good fit for a small number of applications.  
• App Volumes AppStacks             |
| Require location-aware printing      | • ThinPrint  
• User Environment Manager         |
Service Qualities

<table>
<thead>
<tr>
<th>PERFORMANCE</th>
<th>AVAILABILITY</th>
<th>SECURITY</th>
<th>MANAGEMENT AND MONITORING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Medium</td>
<td>Basic (no external access)</td>
<td>Basic</td>
</tr>
</tbody>
</table>

Blueprint

Figure 5: Business Process Application Service Blueprint

Mobile Secure Workspace Service

**Overview:** The core Windows 10 desktop is an instant clone, which is kept to plain Windows OS, allowing it to address a wide variety of users. The majority of applications are delivered through App Volumes with core and different departmental versions. Individual or conflicting applications are packaged with ThinApp and available through the VMware Identity Manager catalog. User Environment Manager applies profile and folder redirection.

While Windows 10 was used in this design, Windows 8.1 or 7 could be substituted.
Use Cases: Mobile Knowledge Worker, Contractors

<table>
<thead>
<tr>
<th>UNIQUE REQUIREMENTS</th>
<th>COMPONENTS</th>
</tr>
</thead>
</table>
| Large number of core and departmental applications | • Horizon 7 Instant Clone virtual desktop is a good fit for larger numbers of applications.  
• App Volumes AppStacks easily deliver core applications and departmental applications. |
| May access from mobile locations | • Access Point, Blast Extreme |
| Two-factor authentication when remote | • Access Point, True SSO |
| Video content and Flash playback | • URL content redirection, Flash redirection |
| • Access to USB devices  
• Restricted access to clipboard, USB, and so on (e.g., contractor) | • UEM, Smart Policies, Application Blocking |

Service Qualities

<table>
<thead>
<tr>
<th>PERFORMANCE</th>
<th>AVAILABILITY</th>
<th>SECURITY</th>
<th>MANAGEMENT AND MONITORING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>High</td>
<td>Medium high (contractors)</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Blueprint

Figure 6: Mobile Secure Workspace Service Blueprint
Dedicated Power Workspace Service

Overview: Similar to the construct of the Mobile Secure Workspace Service with the addition of an App Volumes writable volume. This allows users to be able to install their own applications and have them persist across sessions.

Use Case: Software Developer / IT (Power User)

<table>
<thead>
<tr>
<th>UNIQUE REQUIREMENTS</th>
<th>COMPONENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows extensive CPU and memory</td>
<td>• Horizon 7 Instant Clone virtual desktop</td>
</tr>
<tr>
<td>Install their own applications</td>
<td>• App Volumes writable volume</td>
</tr>
</tbody>
</table>

Service Qualities

<table>
<thead>
<tr>
<th>PERFORMANCE</th>
<th>AVAILABILITY</th>
<th>SECURITY</th>
<th>MANAGEMENT AND MONITORING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Blueprint

Figure 7: Dedicated Power Workspace Service Blueprint
Developer Workspace Service

**Overview:** The core desktop is a full clone of Linux. Applications can be pre-installed into the master VM and users can also add their own applications to their individual clones. Desktops are persistent to the user.

**Use Case:** Software Developer / IT (Power User)

<table>
<thead>
<tr>
<th>UNIQUE REQUIREMENTS</th>
<th>COMPONENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux extensive CPU and memory</td>
<td>• Horizon 7 Linux full clone</td>
</tr>
</tbody>
</table>

**Service Qualities**

<table>
<thead>
<tr>
<th>PERFORMANCE</th>
<th>AVAILABILITY</th>
<th>SECURITY</th>
<th>MANAGEMENT AND MONITORING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Basic</td>
</tr>
</tbody>
</table>

**Blueprint**

*Figure 8: Developer Workspace Service Blueprint*
High-Performance Workspace Service

**Overview:** Similar to the Dedicated Power Workspace Service but will have more CPU and memory, and be GPU accelerated with NVIDIA GRID graphics cards installed in the vSphere servers (vGPU).

**Use Case:** Multimedia Designer

<table>
<thead>
<tr>
<th>UNIQUE REQUIREMENTS</th>
<th>COMPONENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPU accelerated</td>
<td>• NVIDIA vGPU-powered</td>
</tr>
<tr>
<td>User-installed applications</td>
<td>• App Volumes writable volume</td>
</tr>
<tr>
<td>Hardware H.264 encoding</td>
<td>• Blast Extreme</td>
</tr>
</tbody>
</table>

**Service Qualities**

<table>
<thead>
<tr>
<th>PERFORMANCE</th>
<th>AVAILABILITY</th>
<th>SECURITY</th>
<th>MANAGEMENT AND MONITORING</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>

**Blueprint**

*Figure 9: High-Performance Workspace Service Blueprint*
Architecture Principles and Concepts
A Horizon 7 Enterprise Edition design uses a number of complementary components to provide a variety of highly available services to address the identified use cases. Before we can assemble and integrate these components to form the desired service, we first need to design and build the infrastructure required.

Pod and Block
One key concept in a VMware Horizon environment design is the use of pods and blocks, which gives us a repeatable and scalable approach.

A pod is made up of a group of interconnected View Connection Servers that broker desktops or published apps. A pod can broker up to 10,000 sessions including desktop and RDSH sessions. Multiple pods can be interconnected using Cloud Pod Architecture (CPA) for a maximum of 50,000 sessions. For numbers above that, separate CPAs can be deployed.

A pod is divided into multiple blocks to provide scalability. Each block typically serves up to 2,000 sessions and is made up of one or more resource vSphere clusters. Each block has its own VMware vCenter Server®, a VMware View® Composer™ Server (where linked clones are to be used), and resource vSphere clusters.

Figure 10: Pod and Block Design
To add more capacity, we simply add more resource blocks. We also add an additional View Connection Server for each additional block. Typically, we have a maximum of five resource blocks each of 2,000 connections and up to seven View Connection Servers in a pod capable of hosting 10,000 sessions. For numbers above that we deploy additional pods.

As you can see, this approach allows us to design a single block capable of up to 2,000 sessions that can then be repeated to create a pod capable of 10,000 sessions. Multiple pods grouped using Cloud Pod Architecture can then be used to scale the environment as large as needed.

This guide will focus on the architecture of a complete Horizon 7 Enterprise Edition environment but will concentrate on the design required to build and scale the first block.

For scalability and operational efficiency, it is a best practice to have a separate vSphere cluster to host all the management components. This structure keeps the VMs that run services like vCenter, View Connection Server, Access Point, and databases separate from the desktop and RDSH VMs.

Other Horizon 7 Enterprise Edition components are generally designed to follow this approach to ensure scalability. We detail the design of each of the components later in this document.

For the purposes of this guide, we focus on a relatively simple environment comprised of a single resource block and a separate management block.

To help you understand the suitable choices for your use cases and what the architecture and scale would look like, use the Horizon Sizing Estimator.

Horizon 7 Enterprise Edition Logical Architecture

From a data center perspective there are several components and servers that must be deployed to create a functioning Horizon 7 Enterprise Edition environment to deliver the desired services.

• VMware Identity Manager – VMware Identity Manager is an Identity-as-a-Service (IDaaS) offering, providing application provisioning, a self-service catalog, conditional access controls, and single sign-on (SSO) for SaaS, Web, cloud, and native mobile applications.

• View Connection Server – Acts as a broker for client connections. Authenticates users through Windows Active Directory and directs the request to the appropriate virtual machine, physical PC, or Microsoft RDS host.

• VMware View Composer – Allows for the creation of a pool of linked clones from a specified parent virtual machine. This can be used for creating large numbers of desktops or RDS hosts.

• Access Point – Functions as a secure gateway for users who want to access remote desktops and applications from outside the corporate firewall.

• App Volumes Manager – Orchestrates application delivery by managing assignments of application volumes (AppStacks and writable volumes) to users, groups, and target computers.

• Microsoft SQL Servers – Microsoft SQL database servers used to host several databases used by the management components of Horizon 7 Enterprise Edition.

• vRealize Operations Manager for Horizon – Provides end-to-end visibility into the health, performance, and efficiency of virtual desktop and application environments from the data center and the network, all the way through to devices.

• File servers – Store user files, profile information, and more.

• VMware vSphere ESXi™ hosts – Physical servers running vSphere.

• Virtual SAN storage – Delivers high-performance, flash-optimized, hyper-converged storage using server-attached flash devices or hard disks to provide a flash-optimized, highly resilient, shared datastore.
**VMware vCenter Server** - Manages the vSphere hosts and virtual machines. Also provides provisioning tasks and is used by View Connection Servers and View Composer to create VMs and clones, and App Volumes to mount AppStacks and user writeable volumes.

---

**Figure 11:** Horizon 7 Enterprise Edition Logical Architecture

The next section of this guide details the design of each of these components.
Horizon 7 Enterprise Edition Component Design

To be able to deliver the Horizon 7 Enterprise Edition services outlined above and to address the use cases we first need to design and build out the infrastructure components required.

This section includes a low-level design of each of the products or areas that need to be considered. This is not an exhaustive design or installation guide, and it is recommended that you also refer to the installation guides.

Installation best practices or recommended configuration for the design outlined in this document can be found in the appendixes.

VMware Identity Manager

VMware Identity Manager provides a number of key capabilities for Horizon implementations. Among them are:

• A portal, referred to as VMware Workspace™ ONE™, which provides access to different types of applications including SaaS-based Web applications (such as Salesforce.com, Dropbox, Concur, and many others), Horizon-based applications and desktops, RDSH-based applications and desktops, ThinApp apps, and Citrix-based applications and desktops. The portal is designed to make application access simple for end users.

• Enterprise identity management to sync and extend Active Directory environments to SaaS applications.

• Enterprise single sign-on to ensure that users have a single identity to log in with for internal, external, and virtual-based applications.

• A self-service app store allows end users to search for and select entitled applications in a simple way, while providing enterprise security and compliance controls to ensure the right users have access to the right applications.

VMware Identity Manager is deployed as a virtual appliance and integrated with the rest of the Horizon suite to enable access to the resources that are being enabled for end users.

Figure 12: User Workspace Delivered by VMware Identity Manager
Design Overview
VMware Identity Manager can be implemented using on-premises or SaaS-based implementation models. In an on-premises implementation, a VMware Identity Manager virtual appliance handles authentication and provides single sign-on services to applications and desktops. In a SaaS-based implementation, a VMware Identity Manager Connector virtual appliance is used to synchronize user accounts from Active Directory to the VMware Identity Manager Service. Applications can then be accessed from a cloud-based portal.

A current limitation in VMware Identity Manager SaaS-only implementations is that access to on-premises Horizon implementations is not available.

**Design Decision:** Due to the use of on-premises Horizon infrastructure, an on-premises VMware Identity Manager design will be utilized.

*Figure 13: VMware Identity Manager Logical Design*
Database

VMware Identity Manager can be set up with an internal or external database to store and organize server data. You can use the PostgreSQL database that is embedded in the VMware Identity Manager virtual appliance, or you can set up an external database. The internal database is the default.

The embedded PostgreSQL database configuration is useful for smaller deployments. It does not require any additional configuration outside VMware Identity Manager, but it is recommended that you configure your internal database for high availability.

To use an external database, have your database administrator prepare an empty external database and schema before you use the VMware Identity Manager Setup wizard to connect to the external database. Licensed users can use an external Microsoft SQL 2014 database server, an Oracle database server, or an external PostgreSQL database server to set up a high-availability external database environment. It is also possible to migrate the internal database to an external database in the event greater scalability is needed as an environment grows. For more information, see Add an External Database to the VMware Identity Manager Appliance in Installing and Configuring VMware Identity Manager. (Note: Use the drop-down menu to select an on-premises version of VMware Identity Manager.)

Database requirements:

- Internal PostgreSQL included with VMware Identity Manager
- External database sizing: 64 GB for first 100,000 users. Add 20 GB for each additional 10,000 users.
- Storage: 32 GB

**Design Decision:** To simplify configuration, the internal database will be implemented as it can easily scale to the 2,000-user design requirement.
Scalability and Availability

VMware Identity Manager has been tested to 100,000 users per single virtual appliance installation. For a high-availability environment, at least two VMware Identity Manager appliances should be configured to ensure availability in the event of a failure of an appliance or ESX host. After initial configuration, the virtual appliance will be cloned and deployed with a new IP address and host name.

With the embedded database in use, the VMware Identity Manager database should be replicated in a master/slave configuration between VMware Identity Manager hosts. This ensures availability of the service in the event of failure of the master appliance.

Figure 14: VMware Identity Manager Availability

For more information on how to set up VMware Identity Manager in a high-availability configuration, see Configuring Redundancy in Installing and Configuring VMware Identity Manager. (Note: Use the drop-down menu to select an on-premises version of VMware Identity Manager.) Additional information can also be found in this blog.

Design Decision: To provide high availability, two VMware Identity Manager appliances will be deployed using the internal database configuration set in a master/slave configuration.
Prerequisites
This section details the prerequisites for the VMware Identity Manager configuration.

vSphere and ESXi
The following versions are supported: 5.0 U2 and later, 5.1 and later, 5.5 and later, and 6.0 and later.

NTP
The Network Time Protocol (NTP) must be correctly configured on all hosts and time-synchronized to an NTP server. You must turn on time sync at the ESXi host level, using an NTP server to prevent a time drift between virtual appliances. If you deploy multiple virtual appliances on different hosts, consider disabling the Sync to Host option for time synchronization. Instead, configure the NTP server in each virtual appliance directly to make sure that there is no time drift between virtual appliances.

Network Configuration
• Static IP address and DNS Forward (A) and Reverse (PTR) records.
• Inbound firewall port 443 is open so that users outside the network can connect to the VMware Identity Manager instance or the load balancer.

Active Directory
VMware Identity Manager supports Active Directory configurations on Windows 2008 R2, 2012, and 2012 R2, including:
• Single AD domain
• Multidomain, single forest
• Multiforest with trust relationships
• Multiforest with untrusted relationships (requires external connector configuration)
• Active Directory Global Catalog optional for Directory Sync

Infrastructure Overview
Each VMware Identity Manager appliance has the following minimum requirements:
• 6 GB RAM
• 2 vCPU
• 36 GB disk space

Install and Initial Configuration
The major steps for on-premises installation and initial configuration of VMware Identity Manager are:

Figure 15: VMware Identity Manager Install and Configure Steps
The VMware Identity Manager appliance is delivered as an OFV template. It is deployed via the vSphere client. For information on deploying the OVF template see Install the VMware Identity Manager OVA File in Installing and Configuring VMware Identity Manager. (Note: Use the drop-down menu to select an on-premises version of VMware Identity Manager.)
Initial connector settings will include Administrator, root, and SSH passwords, and choice of internal or external database.

Initial server settings will include installation of a license, setting, or adding additional required user attributes (objectGUID, for instance, if planning to use Office 365), and setting an SMTP server.

Active Directory configuration involves creating a connection to Active Directory, selecting a bind account with permission to read from AD, choosing groups and users to sync, and then initiating a directory sync.

Final configuration updates will include setting the device FQDN, installing SSL certificates, configuration of load balancers, and enabling logging. Other configurations to complete include joining the appliance or connector to the appropriate Active Directory domain (for ThinApp and Horizon access), configuration of additional authentication methods, and finally, any custom branding to apply corporate logos and color schemes to the portal.

For detailed information on each step, see About Installing and Configuring VMware Identity Manager in Installing and Configuring VMware Identity Manager. (Note: Use the drop-down menu to select an on-premises version of VMware Identity Manager.)

**Next Steps**

This section describes the next steps required in the configuration of VMware Identity Manager.

**Provide Access to Resources**

VMware Identity Manager centralizes access to resources such as Web-based SaaS applications, internal Web applications, ThinApps, and Horizon-based desktops and applications as well as RDSH applications and desktops through the VMware Identity Manager catalog in the Workspace ONE portal.

Based on the types of applications that will be delivered to end users, the VMware Identity Manager catalog will be configured to integrate with the relevant services.
View in Horizon
As detailed in the Architecture Principles and Concepts section, we follow a Pod and Block approach to design and implement View in Horizon 7. This allows us to design, size, and validate in repeatable sized blocks. In this section we detail the design on the first resource block and all components required to implement View.

View allows us to create and broker connections to Windows virtual desktops, Linux virtual desktops, Remote Desktop Server (RDS) hosted applications and desktops, and physical machines.

This core part of View in Horizon includes the following components and features:

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Connection Server</td>
<td>View Connection Server is an enterprise-class desktop management server that securely brokers and connects users to desktops running on vSphere virtual machines, physical PCs, blade PCs, or Microsoft Terminal Services.</td>
</tr>
<tr>
<td>Horizon Administrator</td>
<td>The Horizon Administrator interface is a Web application that is part of the View Connection Server, allowing administrators to configure the Connection Server, deploy and manage desktops, control user authentication, initiate and examine system events, and carry out analytical activities.</td>
</tr>
<tr>
<td>View Composer</td>
<td>View Composer works with the Connection Servers and a vCenter Server. It is one of the methods that enables scalable management of virtual desktops by provisioning from a single master image. It reduces storage costs by using VMware linked-clone technology and streamlines desktop management by enabling automatic updating and patching of hundreds of images from the master image.</td>
</tr>
<tr>
<td>Horizon Agent</td>
<td>The Horizon Agent is a software service that is installed on all guest virtual machines, physical systems, or RDS hosts that allows them to be managed by View Connection Servers.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>The Horizon Client allows a physical device to access a virtual desktop or RDS-based application in a Horizon deployment. (Note: There is also the option to use an HTML client from devices where installation of software is not possible.)</td>
</tr>
<tr>
<td>Access Point</td>
<td>Access Point provides a method to secure connections in access scenarios requiring additional security measures such as over the Internet. (A separate section on Access Point details the design and implementation of this component.)</td>
</tr>
<tr>
<td>Remote Desktop Services (RDS) hosts</td>
<td>Microsoft RDS hosts for providing hosted applications and session-based remote desktops to end users.</td>
</tr>
<tr>
<td>vSphere and VMware vCenter</td>
<td>The vSphere product family includes ESXi and vCenter Server, and is designed for building and managing virtual infrastructures. The vCenter Server system provides key administrative and operational functions such as provisioning, cloning, and virtual machine management features, which are essential for a virtual desktop infrastructure.</td>
</tr>
</tbody>
</table>

Table 4: View in Horizon Components
Logical Architecture
This section will focus on the following core elements of View.

• View Connection Server
• View Composer (only required where linked-clone pools will be deployed)
• Horizon Agent
• Horizon Client

The diagram below shows the high-level logical architecture of these core elements. Other components are shown for illustrative purposes, but the areas of focus are in dark blue.

Figure 16: View Logical Architecture

Design Overview
A successful deployment of Horizon is dependent on good planning and a robust understanding of the platform. This section discusses the design options and details the design decisions that are made to satisfy the design requirements.

Scalability and Availability
vCenter Server
VMware vCenter Servers can scale to handle 10,000 virtual machines, but that would introduce a single point of failure that could affect too large a number of users. It would also have performance implications, as the vCenter would become a bottleneck in provisioning tasks.

Design Decision: 1 x vCenter Server will be deployed per Horizon Block of approximately 2,000 sessions/desktops.
View Connection Server
A View Connection Server supports a maximum of:
• PCoIP sessions = 2,000
• Blast Extreme sessions (TCP) = 2,000
To satisfy the requirements that the proposed solution be robust and able to handle failure, we will deploy (n+1).

Design Decision: 2 x Connection Servers (n+1) will be deployed to satisfy the requirement of one resource block capable of hosting up to 2,000 sessions and also to provide high availability.

View Composer Server
A View Composer Server is paired with a vCenter so in our block architecture where we have one vCenter per 2,000 sessions we typically also have also have a Composer server. This gets high availability provided by vSphere High Availability (HA), which restarts the Composer Virtual Machine (VM) in the case of a vSphere host outage. VM monitoring with VMware HA can also attempt to restart the VM in the case of an operating system crash.

By architecting using the pod and block approach, we deploy a vCenter and a paired Composer per block of 2,000 sessions. This also helps in reducing the impact of any failure while vSphere HA recovers the Composer VM. If the Composer service was unavailable, all existing desktops would continue to work just fine. While HA is restarting the Composer VM, the impact is on any provisioning tasks within that block (refreshes, recomposes, creating new linked clone pools).

Design Decision: 1 x View Composer Server will be deployed per View block of approximately 2,000 sessions.
Load Balancing of Connection Servers

One key design principle is to remove single points of failure in the deployment. For high availability and scalability, it is recommended that multiple connection servers be deployed in a load-balanced replication cluster.

View Connection Servers broker client connections, authenticate users, and direct incoming requests to the correct endpoint. The load balancer serves as a central aggregation point for traffic flow between clients and connection servers, sending clients to the best performing and most available View Connection Server instance.

Using a load balancer with multiple View Connection Servers also facilitates greater flexibility by enabling IT Administrators to perform maintenance, upgrades, and changes in the configuration without impacting users.

View requires the load balancer to have a session persistence setting. This is sometimes referred to as persistent connections or sticky connections, and ensures data stays directed to the relevant View server.

- Type = Server Cookie
- Cookie Name = JSESSIONID

**Design Decision:** A load balancer will be placed in front of the View Connection Servers for both internal connections and those coming externally via the Access Points.
Authentication
One of the methods of accessing Horizon desktops and applications will be through VMware Identity Manager. This requires integration between View and VMware Identity Manager using the SAML 2.0 standard to establish mutual trust, which is essential for single sign-on (SSO) functionality. When SSO is enabled, users who log in to VMware Identity Manager with Active Directory credentials can launch remote desktops and applications without having to go through a second login procedure. See Using SAML Authentication in the View Administration guide for details.

**Design Decision:** SAML Authentication will be set to allowed on the Connection Servers. The Connection Servers will be configured to allow the VMware Identity Manager to be a dynamic SAML authenticator.

Virtual Machine Build
View Connection Server and View Composer Servers run as Windows services. Specifications are detailed in the Appendix. Each server is deployed with a single network card and static IP address information is required for each server.

**Design Decision:** Windows 2012 R2 will be used for the OS build as the latest supported version. IP address info will be allocated for each server.

Physical Hosting
The Connection Server and View Composer VMs should reside with the management block and be placed on the Management vSphere hosts. HA and DRS can be used to ensure the maximum availability.

Protocol
Horizon 7 is a multi-protocol solution. There are three remoting protocols available when creating desktop pools or hosted applications—RDP, PCoIP, and the new Blast Extreme protocol.

**Design Decision:** For this design we will leverage the new Horizon 7 Blast Extreme display protocol. This display protocol supports multiple codecs (JPG/PNG and H.264), both TCP and UDP from a transport protocol perspective, and the ability to do hardware encode with NVIDIA GRID. This protocol has full feature and performance parity with PCoIP and is optimized for mobile devices since they are able to decode the H.264 protocol in hardware.

Configuration
Blast Extreme is configured through Horizon 7 when creating a pool. The Blast Extreme display protocol is integrated directly into the Horizon 7 broker so there is no installation needed. The protocol can also be selected directly on the Horizon Client side when a user selects a desktop pool. Blast Extreme can also use TCP port sharing with Access Point 2.5 so firewall configuration and port requirements can be simplified.

Prerequisites
In order to use the Blast Extreme display protocol, the following must be in place:

- Horizon 7 infrastructure.
- Horizon 4.x Client must be used to connect.
Key Design Considerations

- Use TCP and H.264 when possible.
- TCP 443 port sharing with Access Point 2.5 simplifies port requirements.
- Most modern devices have the ability to hardware decode H.264.
- Even if a pool is forced to Blast Extreme, devices such as PCoIP zero clients will connect via PCoIP.
- Horizon 4.x Client must be used to connect.

**Access Point**

Access Point is an integral component in any Horizon deployment. It enables remote access from outside the corporate network to internally hosted Horizon desktops and applications. Access Point is typically deployed within the corporate DMZ and acts as a proxy host for connections to your company’s resources. Access Point directs authenticated requests to the appropriate resource and discards any unauthenticated requests. Access Point can also perform authentication if desired.

To meet with the design requirements, Access Point 2.5 and Access Point 2.6 are deployed.

- Access Point 2.5 handles all Horizon connections.
- Access Point 2.6 acts as a reverse proxy for connections to the VMware Identity Manager appliances.

VMware Identity Manager performs two-factor authentication and True SSO is configured in the environment. (For more information, see the True SSO section).

The diagram below describes the high-level logical architecture when both VMware Identity Manager and Horizon connections are protected by Access Point.

![Access Point Logical Architecture](image-url)
Design Overview
A successful deployment of Access Point is dependent on good planning and a robust understanding of the platform. This section discusses the design options and details the design decisions that are made to satisfy the design requirements.

Access Point 2.5 and 2.6
There are two different releases of Access Point. A brief overview of the differences is discussed here:

- Access Point 2.5 only supports connections to Horizon desktops and applications.
- Access Point 2.6 only supports connections to VMware Identity Manager appliances.

**Design Decision:** Both Access Point 2.5 and 2.6 will be used to satisfy the requirements of the design to support connections to VMware Identity Manager and Horizon.

Scalability
Access Point supports a maximum of:

- PColP Sessions = 2,000
- Blast Extreme Sessions – UDP = 1,000
- Blast Extreme Sessions – TCP = 2,000

To satisfy the requirements for the proposed solution to be robust and to be able to handle failure we will deploy (n+1).

**Design Decision:** 2 x Access Points 2.5 (n+1) will be deployed to satisfy the requirement of 2,000 sessions and high availability.
Load Balancing

It is highly recommended that users connect to Access Point using a load-balanced VIP. This ensures that user load is evenly distributed across all available Access Points. Using a load balancer also facilitates greater flexibility by enabling IT administrators to perform maintenance, upgrades, and changes in the configuration without impacting users.

Additionally, it is also recommended that connections from the Access Points to the View Connection Servers are also load balanced, although this is not required.

Figure 19: Access Point Load Balancing

Only the initial XML API connection is load balanced; PCoIP, Blast Extreme, or RDP connections will connect directly to the Access Point that brokered the initial XML API connection. For load balancing to function correctly a connection must maintain persistence/affinity of the session. To facilitate this, there are two methods that can be implemented in the environment to support session persistence/affinity:

• SSL ID
• Source IP address

The capabilities of the load balancer will determine which method will be used. If both are supported then a preference of SSL ID should be considered as this gives the most even spread of connections.

Design Decision: A load balancer will be placed both in front of the Access Points and between the Access Points and the View Connection Servers. SSL ID will be used as the method to support session persistence / affinity.
**Authentication Options**

Access Point 2.6 for VMware Identity Manager connections will forward a connection request to VMware Identity Manager via the Access Point reverse proxy engine.

Access Point 2.5 for Horizon supports multiple authentication options, for example, pass-through, RSA SecurID, RADIUS, and smart card. Pass-through authentication forwards the XML API request from the HTTPS Web server and passes it to the View Connection Server via the XML API Tunnel within the Access Point. Other authentication types enable authentication at the Access Point, before passing an authenticated session to a connection server.

This is depicted in the diagrams below:

![Figure 20: Access Point Pass-Through Authentication](image)

![Figure 21: Access Point Two-Factor Authentication](image)

**Design Decision:** For access to VMware Identity Manager, Access Point 2.6 will be leveraged and configured as a reverse proxy. User connections will then be authenticated at VMware Identity Manager and True SSO will be configured. As connections to Horizon will be authenticated at VMware Identity Manager and True SSO is used, the Access Point 2.5 must be configured with pass-through authentication, otherwise True SSO would fail.
Network Deployment Options
Access Point can be deployed with either one, two, or three network interface controllers (NIC). The decision will be determined by your network requirements and discussions with the security teams to ensure compliance with company policy.

**Single NIC**
In a single NIC deployment, all traffic (Internet, backend, and management) use the same network interface. Consider this deployment for non-production environments.

Figure 22: Access Point Single NIC Deployment
Dual NIC
A dual NIC deployment separates the Internet traffic onto its own NIC, while the management and backend network data still share a NIC. This type of deployment is suitable for production environments.

![Figure 23: Access Point Dual NIC Deployment](image)

Three NIC
A three NIC deployment separates the Internet traffic onto its own NIC, and separates management and backend network data onto dedicated networks. This type of deployment is suitable for production environments.

![Figure 24: Access Point Three NIC Deployment](image)
Design Decision: To meet with the requirements of separating Internet traffic from management and backend data, the Access Point will be deployed in a dual NIC mode.

Management Block
The Access Point appliances reside within the Management Block and are placed in the management cluster. HA and DRS can be used to ensure the maximum availability of the Access Points. DRS rules will be configured to ensure that the devices do not reside on the same host; this will enhance High Availability.

VMware App Volumes
Design Overview
The VMware App Volumes just-in-time application model separates IT-managed applications and application suites into administrator-defined application containers, and introduces an entirely different container used for persisting user changes between sessions.

![Figure 25: App Volumes Just-in-Time Application Model](image)
Design Overview

VMware App Volumes is used to serve two functions. The first is delivery of applications that are not in the parent image for VDI and RDSH. App Volumes groups applications into AppStacks based on the requirements of each use case. An AppStack is a group of applications that are captured together. The AppStacks can then be assigned to a user, group, OU, or machine (RDSH) and mounted each time the user logs in to a desktop. For VDI use cases, AppStacks can be mounted either on-demand or at login. With RDSH use cases, we are assigning the AppStack to the machine account so AppStacks can only be mounted when the App Volumes service starts.

App Volumes will also provide user-writable volumes for a limited number of users. This provides a mechanism to capture user-installed applications that are not, or cannot be, delivered by AppStacks. This reduces the likelihood that persistent desktops would be required for a use case. The user-installed applications follow the user as they connect into different virtual desktops.

App Volumes is comprised of several components, listed below.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Volumes Manager</td>
<td>• Console for management of App Volumes including configuration, creation of AppStacks, and assignment of AppStacks and writable volumes</td>
</tr>
<tr>
<td></td>
<td>• Broker for App Volumes Agent for the assignment of applications and writable volumes</td>
</tr>
<tr>
<td>App Volumes Agent</td>
<td>• File system and registry abstraction layer running on the target system</td>
</tr>
<tr>
<td></td>
<td>• Virtualizes file system writes as appropriate (when used with optional writable volume)</td>
</tr>
<tr>
<td>AppStack Volume(s)</td>
<td>• Read-only volume containing applications</td>
</tr>
<tr>
<td></td>
<td>• Can map more than one AppStack per user or machine</td>
</tr>
<tr>
<td></td>
<td>• Deploy apps to VDI or RDSH</td>
</tr>
<tr>
<td>Writable volume</td>
<td>• Per-user read-write volume used to persist changes written in the session</td>
</tr>
<tr>
<td></td>
<td>• One writable volume per user</td>
</tr>
<tr>
<td></td>
<td>• User-installed applications and user profile</td>
</tr>
<tr>
<td></td>
<td>• Only available with user or group assignments</td>
</tr>
<tr>
<td>Provisioning VMs</td>
<td>• Clean Windows virtual machine with App Volumes Agent</td>
</tr>
<tr>
<td></td>
<td>• Provision and update applications into an AppStack</td>
</tr>
</tbody>
</table>

Table 5: App Volumes Components
Infrastructure Overview

The VMware App Volumes infrastructure is comprised of the following components:

- Virtual desktops or RDSH hosts running the App Volumes Agent
- Load balancer to manage connections to the App Volumes Manager servers
- Pair of App Volumes Manager servers to handle brokering and management
- vCenter managing vSphere hosts for attaching and detaching AppStacks and writable volumes
- Highly available SQL server for hosting App Volumes Manager data
- Active Directory environment for assigning AppStacks and writable volumes

Figure 26: App Volumes Logical Architecture

Key Design Considerations

- Always use at least two App Volumes Managers.
  - Requires a shared SQL Server.
- Any kernel mode applications should reside in base image and not in an AppStack.
- Use Storage Group (if not Virtual SAN) to aggregate load and IOPS.
  - AppStacks are very read intensive.
- Place AppStacks on storage optimized for read (100 percent read).
- Place writable volumes on storage optimized for random IOPS (50/50 read/write).
- Do not assign more than 8–10 AppStacks per user or device.
- Always use “Mount on Host.” This option issues the API calls directly to the host that the desktop receiving the AppStack resides on. This speeds up the mount and login process and reduces overall load on vCenter.
Scalability and Availability

**App Volumes Managers**
The App Volumes Managers are the primary point of management and configuration, and are used for brokering volumes to agents. For a production environment at least two App Volumes Manager servers should be deployed. The App Volumes Manager is stateless—all of the data required by App Volumes is located in a SQL database. By deploying at least two App Volumes Manager servers we can ensure availability of App Volumes services and distribute user load.

**Design Decision:** Two VMware App Volumes Manager servers will be deployed with a load balancer.

**Database**
VMware App Volumes 2.11 uses a Microsoft SQL Server database to store all of the configuration, assignment, and metadata. This database is a critical aspect of the design and it must be accessible by all of the App Volumes Managers.

**Design Decision:** The SQL database will be placed on a highly available SQL cluster and both of the VMware App Volumes Managers point to this cluster.

**AppStack Storage**
VMware App Volumes uses a construct of Storage Groups. A Storage Group is a collection of datastores that will be used to serve AppStacks or distribute writeable volumes. In App Volumes 2.11 the AppStacks within a Storage Group can be replicated among its peers to ensure all AppStacks are available. Having a common datastore presented to all hosts in all vCenters allows AppStacks to be replicated across vCenters and datastores.

**Note:** This design utilizes Virtual SAN, which provides a single highly available datastore per vSphere cluster.

**Design Decision:** Storage Groups will be used in this design, as there are separate Virtual SAN datastores for the linked-clone and instant-clone pools. AppStacks will be automatically replicated between the two datastores by the Storage Group.

**Load Balancing**
App Volumes Manager servers require an external load balancer to balance connections between App Volumes Managers. This is done for performance and availability purposes. The main concern with App Volumes Managers is handling login storms, as this is when they are the most heavily loaded. In 2.11, each App Volumes Manager can handle up to 2,000 users but the exact number can vary depending on the load and the specifics of each environment. It is recommended that you test the load and size the number of App Volumes Manager servers appropriately. To size this design, we assumed each App Volumes Manager was able to handle 1,000 users.

**Design Decision:** A load balancer will be placed in front of the App Volumes Manager servers. This will properly distribute load and keep the services available in the event of an issue with one of the managers.
VMware User Environment Manager
VMware User Environment Manager provides profile management by capturing user settings for the operating system and applications. Unlike traditional application profile management solutions, User Environment Manager does not manage the entire profile. Instead it captures settings that the administrator has specified. This reduces login and logout time as less data needs to be loaded. The settings can be dynamically applied when a user launches an application, making the login process more asynchronous. User data is managed through folder redirection.

Figure 27: User Environment Manager
VMware User Environment Manager is a Windows-based application that consists of the following components.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Active Directory Group Policy | • Configuration of the VMware User Environment Manager.  
                               • ADMX template files are provided with the product.                                                                                   |
| Configuration share        | • A central share (SMB) on a file server.  
                               • This can be a replicated share (DFS-R) for multisite scenarios as long as the path to the share is the same for all client devices.  
                               • If using DFS-R, it must be configured as hub and spoke. Multimaster replication is not supported.                                    |
| Profile Archives share      | • File shares (SMB) to store the users’ profile archives and profile archive backups.  
                               • Archives should be placed on a share close to the computer where the User Environment Manager FlexEngine runs for best performance. |
| UEM FlexEngine             | • The User Environment Manager Agent that resides on the client being managed.                                                               |
### COMPONENT | DESCRIPTION
--- | ---
Application Profiler | - The Application Profiler is used to create a User Environment Manager profile from an application by determining where the application stores configuration data in the registry and file system. User Environment Manager will manage settings for applications that have a valid User Environment Manager Profile in the configuration share.

Helpdesk | - Allows helpdesk to reset or restore user settings.
- Support for profile archives.
- Analysis of Profile Archive sizes.
- Log file viewer.

Self Support | - Optional self-service tool to allow users to manage and restore their configuration settings on an environment setting or application.

SyncTool | - Synchronizes profile archives and configuration files.
- Targeted for laptop users and those with limited bandwidth or connectivity.

| Table 6: User Environment Manager Components |

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Profiler</td>
<td>- The Application Profiler is used to create a User Environment Manager profile from an application by determining where the application stores configuration data in the registry and file system. User Environment Manager will manage settings for applications that have a valid User Environment Manager Profile in the configuration share.</td>
</tr>
</tbody>
</table>
| Helpdesk | - Allows helpdesk to reset or restore user settings. 
- Support for profile archives. 
- Analysis of Profile Archive sizes. 
- Log file viewer. |
| Self Support | - Optional self-service tool to allow users to manage and restore their configuration settings on an environment setting or application. |
| SyncTool | - Synchronizes profile archives and configuration files. 
- Targeted for laptop users and those with limited bandwidth or connectivity. |

**Figure 28: User Environment Manager Logical Architecture**
User Profile Strategy

A Windows User Profile is made of multiple components including local data, user data, and the user registry.

![User Environment Manager User Profile Strategy](image)

**Figure 29: User Environment Manager User Profile Strategy**

In conjunction with User Environment Manager, mandatory, roaming, local, or folder redirection can be used to redirect user data.

**Design Decision:** Mandatory profiles and folder redirection will be used. A mandatory user profile is a preconfigured roaming user profile that is used to specify settings for users. With mandatory user profiles, a user can modify their desktop, but the changes are not saved when the user logs out. Since all settings will be managed by User Environment Manager, there is no need to persist these settings on log out.

See **Appendix H: Mandatory Profile** for condensed instructions for creating mandatory profiles. Further instruction can be found on the Microsoft Web site.
Infrastructure

User Environment Manager requires little infrastructure. AD GPOs are used to specify User Environment Manager settings and SMB shares are used to host the configuration data and profile data. User Environment Manager is used by administrators to configure settings.

Prerequisites

- Create SMB file shares for configuration data and user data.
- Import ADMX Templates for User Environment Manager.
- Create Group Policy settings for User Environment Manager.
- Install FlexEngine agent on clients to be managed.
- Install the User Environment Manager Management Console and point to the configuration share.
- Use Easy Start to do initial configuration of settings (installs many common configuration and application settings as well as Microsoft Office profiles).

Key Design Considerations

- Use DFS-R or file server clustering to provide HA to configuration and user shares.
  - DFS-R can only be hub and spoke. Multimaster replication is not supported.
  - See the Microsoft KB article Microsoft’s Support Statement Around Replicated User Profile Data for supported scenarios.
- Use loopback processing when applying the GPO settings to computer objects.
Install
Refer to the User Environment Manager Administrator’s Guide for detailed installation procedures.

Next Steps
After the install of User Environment Manager, the following is required to verify functionality:

• Install User Environment Manager Agent on one or more clients.
• 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.
• 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.

True SSO
True SSO is used in conjunction with VMware Identity Manager or WorkSpace ONE to enable users to single sign-on to Horizon desktops and applications regardless of the authentication mechanism used.

True SSO uses SAML, where Workspace ONE is the Identity Provider (IdP) and Horizon is the Service Provider (SP). True SSO generates unique, short-lived certificates to manage the login process. This enhances security as no passwords are transferred within the data center.

True SSO requires a new service—the enrollment server—to be installed using the Horizon 7 installation media. The enrollment server can be installed on either a dedicated Windows 2012 R2 server or it can co-exist on the server running the MS Certificate Authority service.
Design Overview
For True SSO to function the following components must be installed and configured within the environment. This section discusses the design options and details the design decisions that are made to satisfy the design requirements.

**Note:** For more information on how to install and configure True SSO, see *Setting Up True SSO* in the View Administration guide.

Enrollment Server
The enrollment server is required to support the implementation of True SSO. The enrollment server is responsible for receiving certificate signing requests from the connection server and then passing them to the Certificate Authority to sign using the relevant certificate template.

Scalability
The enrollment server is a lightweight service that can either be installed on a dedicated Windows 2012 R2 server or it can co-exist with the MS Certificate Authority.

A single enrollment server can easily handle all the requests from a single View pod.

To satisfy the requirements for the proposed solution to be robust and to be able to handle failure, we deploy (n+1).

**Design Decision:** 2 x enrollment servers will be deployed within a View pod to satisfy the requirement of 2,000 sessions and high availability. Each enrollment server will be hosted on a dedicated Windows 2012 R2 VM.
Load Balancing

Two enrollment servers are deployed in the environment and the View Connection Servers are configured to communicate to both deployed enrollment servers. The enrollment servers can be configured to communicate with two Certificate Authorities. By default, the enrollment servers use the Active / Failover method of load balancing. This can be changed to round robin if required.

![Diagram of SSO Availability and Redundancy](image)

**Design Decision:** The default mode of Active / Failover is sufficient to meet the requirements and will be left in its default state.

Management Block

The enrollment servers reside within the management block and are placed in the management cluster. HA and DRS can be used to ensure the maximum availability of the enrollment server. DRS rules are configured to ensure that the devices do not reside on the same host. This enhances High Availability.
VMware vRealize Operations Manager for Horizon
Traditionally management and monitoring of enterprise environments involved monitoring a bewildering array of systems, requiring administrators to switch between multiple consoles to support the environment.

VMware vRealize Operations Manager for Horizon provides end-to-end visibility of Horizon and its supporting infrastructure, enabling administrators to:

• Meet SLAs
• Reduce the first time to resolution (FTR)
• Improve user satisfaction
• Proactively monitor the environment and resolve issues before they affect users
• Optimize resources and lower management costs
• Monitor reporting
• Create custom dashboards

Design Overview
VMware vRealize Operations Manager for Horizon facilitates proactive monitoring and management of a Horizon environment and can also proactively monitor vSphere and display all information, alerts, and warnings for compute, storage, and networking.

VMware vRealize for Horizon consists of two components: the vRealize Operations Manager appliance and the Horizon Adapter (vRealize Operations Manager for Horizon Adapter). Other adapters can be added to the core vRealize for Operations Manager appliance to gather information from other sources; for example, the VMware vRealize Operations for Published Applications™ adapter retrieves information from Citrix environments and displays it within the vRealize Operations Manager dashboards.

The latest release of vRealize Operations Manager (6.2) and the Horizon Adapter (6.2) are used.

Design Decision: To meet with the customer requirements, the vRealize Operations Manager for Horizon appliance and vRealize Adapter for Horizon will be deployed.

Deployment Options
VMware vRealize Operations Manager can be deployed on either Windows or Linux. It can also be deployed as a self-contained appliance.

VMware vRealize Operations Manager can be deployed as a single node, as part of a cluster, or as a cluster with remote nodes.

• Single Node – A single-node deployment does not provide high availability and is limited in the number of objects it can support.
• Cluster – A cluster can consist of up to eight nodes (appliances). This provides flexibility and the ability to scale to suit most customer deployments while providing high availability.
• Cluster + Remote Node – A remote node is deployed on a remote site or data center to capture information before compressing and passing it back to the cluster for processing. Remote nodes can also be used within the same data center as the cluster and have adapters installed on them instead of the cluster nodes, freeing the cluster nodes to handle the analytical processing.

Design Decision: The vRealize Operations Manager appliances will be deployed as part of a cluster to meet the requirements.
Scalability

VMware vRealize for Operations Manager can scale to support very high numbers of Horizon sessions. To assess the requirements for your environment, use the vRealize Operations Manager sizing calculator. A summary of recommended options is provided for different node configurations:

<table>
<thead>
<tr>
<th>NODE FORM FACTOR</th>
<th>NUMBER OF NODES</th>
<th>DATA DISK SIZE PER NODE (GB)</th>
<th>IOPS PER NODE</th>
<th>TOTAL VCPUS</th>
<th>TOTAL MEMORY (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extra small</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Small</td>
<td>Recommend using larger nodes</td>
<td>Recommend using larger nodes</td>
<td>Recommend using larger nodes</td>
<td>Recommend using larger nodes</td>
<td>Recommend using larger nodes</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>385</td>
<td>520</td>
<td>24</td>
<td>96</td>
</tr>
<tr>
<td>Large</td>
<td>2</td>
<td>580</td>
<td>780</td>
<td>32</td>
<td>96</td>
</tr>
</tbody>
</table>

Table 7: Recommended Node Configurations

**Design Decision**: To support the number of RDSH sessions per hosts and VDI desktops per session, and to meet with the requirements for high availability, a three-medium-node cluster will be deployed.
Architectural Components

VMware vRealize Operations Manager for Horizon consists of multiple components. These components are described here and design options are discussed and determined.

**Figure 33:** vRealize Operations Manager for Horizon Logical Architecture

**Broker Agent**

The broker agent is a Windows service that runs on a View Connection Server host that collects Horizon inventory information, then sends that information to the vRealize Operations for Horizon Adapter.

- The broker agent can collect information from the Horizon Events database and send it to the Horizon adapter.
- The broker agent is installed on one View Connection Server host in each View pod.
- Only one broker agent in each View pod.
- View Connection Server 6.0.1 or later.
- .NET Framework 4.5.

**Design Decision:** The broker agent will be configured to collect information from the Horizon Events database. It will be deployed to a single connection server within the pod.
**Horizon Adapter**

The adapter passes data from the agents to vRealize Operations Manager for analysis and visualization. It also obtains inventory information from the broker agent and collects metrics and performance data from desktop agents. Horizon Adapters do not support HA. In the event of a failure, data will not be collected until the issue is resolved and the adapter brought back online.

**Design Decision:** Install the Horizon Adapter on one of the cluster nodes.

**Desktop Agent**

The vRealize Operations Manager for Horizon desktop agent runs on each remote desktop virtual machine or RDS host in the Horizon environment. In Horizon 6.1 and later, the desktop agent is part of the Horizon Agent install. It collects metrics and performance data and sends that data to the Horizon Adapter. Metrics collected by the desktop agent include:

- Desktop and application objects
- Users’ login time and duration
- Session duration
- Resource and protocol information

**Design Decision:** The desktop agent is installed as part of the standard Horizon Agent and will be enabled during installation.

**Firewall Ports**

To support a successful installation, the following firewall ports must be open between the broker agent and desktop agent to the node hosting the adapter: 3099, 3100, and 3101.

See *Create an Instance of the Horizon Adapter* in the vRealize Operations for Horizon Installation guide for more detail.

**VMware ThinApp**

While our primary mechanism for delivering applications is using VMware App Volumes there may be niche situations that require the application virtualization and isolation that VMware ThinApp can provide. These include application conflicts and per-user assignment of applications.

With ThinApp we can package an entire 32-bit or 64-bit application and its settings into a single .MSI or .EXE executable that can be deployed to many Windows operating environments. These virtual applications are isolated from each other and execute independently without making changes to the underlying operating system, eliminating application-to-application conflict as well as application-to-OS conflicts.

**Design Decision:** ThinApp packages will be used sparingly where application isolation or granular assignment is required and App Volumes cannot fulfill the requirement.
Infrastructure Overview
The infrastructure required for ThinApp is quite light.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture machine</td>
<td>A virtual machine running the same OS as the destination machines. This is used to capture the applications.</td>
</tr>
<tr>
<td>SMB project file share</td>
<td>File share to store working projects of captured applications.</td>
</tr>
<tr>
<td>SMB app file share</td>
<td>Redundant file share to store the virtualized applications.</td>
</tr>
</tbody>
</table>

Table 8: ThinApp Infrastructure

Install
To use ThinApp, set up a clean capture machine where we can run the ThinApp capture and install applications. This should match the OS and build level that the ThinApps will ultimately be consumed on.

Ideally the capture machine should be just Windows OS with no applications installed. Disable Windows Updates to ensure that they do not trigger during a capture process.

To enable clean captures, the capture machine should also be a virtual machine with a snapshot taken before the capture. This allows you to reset it back to a clean state after a capture.

See the ThinApp User's Guide for more detail.

Next Steps
The agentless functionality of ThinApps makes them easy to distribute in a variety of manners and they are generally streamed to the endpoint for execution. For more information, see Deploying Captured ThinApp Applications in the ThinApp User’s Guide.

Design Decision: Captured ThinApps will be deployed through the VMware Identity Manager application catalog. This makes control and consumption easy for users.

Load Balancing and External Access
Secure external access for users accessing resources is provided through integration of Access Point appliances using load balancers to provide scalability and allow for redundancy. There are several integration points between the load balancers and the Access Points and the internal View Connection Servers or VMware Identity Managers.

For an overview of ports see the Firewall and External Access Networking overview section. For the full detail and diagrams of all the possible ports for different protocols and between all components, see this blog or the KB article VMware View ports and network connectivity requirements.
**View Connection Servers**

![Diagram of View Connection Server Load Balancing and External Access](image)

**Figure 34:** View Connection Server Load Balancing and External Access

While the diagram illustrates the use of Split DNS, this is not a requirement for Connection Server traffic. Split DNS does, however, provide certain advantages as users can use the same name internally and externally.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>No additional configuration is required on the View Connection Servers.</td>
</tr>
</tbody>
</table>
| **2** | Load balancing of View Connection Servers should use the following:  
  • Ports = 443, 389  
  • Persistent or session stickiness = Server Cookie  
  • Cookie name = JSESSIONID  
  • Timeout = 30 minutes  
  • Real Server Check = HTTPS |
| **3** | Deploy the Access Points version 2.5 using Horizon script (see Appendix D: Access Point Installation and Configuration). |
| **4** | Load balancing of Access Points for traffic destined for View Connection Servers:  
  • Ports = 443  
  • Persistent or session stickiness = Source IP Hash  
  • Add an HTTP redirect  
  • Real Server Check = HTTPS, URL =/favicon.ico, Method = GET |
VMware Identity Manager

Figure 35: VMware Identity Manager Load Balancing and External Access

Split DNS is a requirement for VMware Identity Manager, that is, the fully qualified domain name (FQDN) used internally and externally for user access to VMware Identity Manager must be the same.

1
   a. Import the certificates.
   b. Change the FQDN to match the load-balanced name.
   c. Enable the New Portal UI.
   d. Clone the first appliance (IDM1) to create second (IDM2).

2
   Load balancing of VMware Identity Managers should use the following:
   • Persistent or session stickiness = Super HTTP
   • Timeout = 60 minutes
   • Scheduling Method = least connection
   • HTTP Headers = X-Forward-For
   • Add a HTTP redirector
   • Real Server Check = HTTPS, URL = /, Method = GET

3
   Deploy Access Points version 2.6 using VMware Identity Manager script (see Appendix D: Access Point Installation and Configuration). Make sure to use version apdeploy-260-v6 or later and check that System Setting is set to “cookiesToBeCached”: “none”.

4
   Load balancing of Access Points for traffic destined for VMware Identity Manager:
   • Persistent or session stickiness = Super HTTP
   • Timeout = 60 minutes
   • Scheduling Method = least connection
   • HTTP Headers = X-Forward-For
   • Add an HTTP redirector
   • Real Server Check = HTTPS, URL = /favicon.ico, Method = GET
No additional configuration is required on the App Volumes Manager servers.

Load balancing of App Volumes Managers should use the following:
- Ports = 80, 3443
- Persistent or session stickiness = Hash all Cookies
- Timeout = 6 minutes
- Scheduling method = round robin
- HTTP Headers = X-Forward-For
- Real Server Check = HTTP
vSphere Infrastructure Design

VMware vSphere is the foundation that will run all the infrastructure and components. It will also run all the end services or resources that the users will consume. All editions of Horizon come bundled with vSphere for Desktops. Additionally, Virtual SAN Advanced is included in VMware Horizon Advanced Edition and Horizon Enterprise Edition.

This lets us build in a hyper-converged hardware model based on a physical server as the building block. The server provides not only the compute and memory but also the storage in a modular fashion.

Figure 37: vSphere and Virtual SAN High-Level Architecture

VMware Horizon deployments benefit from granular, elastic storage capacity that scales without forklift upgrades. Instead of having to add an entire storage array when more desktops are needed, we can simply add more disks, flash storage, or another host.

While this reference architecture utilized the benefits of an all-flash Virtual SAN, it should be noted that traditional storage (SAN/ NAS) is of course still supported.

vSphere

This document does not try to cover vSphere design and installation. That is well documented in resources including the VMware vSphere documentation. Best practices around vSphere ESXi configuration and Virtual SAN networking should be followed.

As outlined in the Reference Architecture Design Methodology, a Horizon environment uses pod and block design. A separate vSphere cluster is used to host the management server components. These server components could equally be placed on an existing vSphere cluster with sufficient capacity.

Each block then has one or more vSphere clusters to host and run the resources such as virtual desktops or RDS hosts.
For the ESXi clusters hosting the View Connection Server, View Security servers, and vCenter virtual machines, vSphere DRS rules should be enabled to prevent the servers performing identical operations from running on the same ESXi host. This prevents multiple VM failures if a host fails and these VMs exist on the failed physical ESXi host.

<table>
<thead>
<tr>
<th>VM/HOST RULES</th>
<th>RULE SETTING</th>
<th>TYPE</th>
<th>VIRTUAL MACHINES</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Connection Server Rule</td>
<td>Enabled</td>
<td>Separate Virtual</td>
<td>horizon1, horizon2</td>
</tr>
<tr>
<td>Horizon Access Point Rule</td>
<td>Enabled</td>
<td>Separate Virtual</td>
<td>horizonap1, horizonap2</td>
</tr>
<tr>
<td>V4H Rule</td>
<td>Enabled</td>
<td>Separate Virtual</td>
<td>v4h1, v4h2, v4h3</td>
</tr>
<tr>
<td>Identity Manager Access Point Rule</td>
<td>Enabled</td>
<td>Separate Virtual</td>
<td>idmap1, idmap2</td>
</tr>
<tr>
<td>Identity Manager Rule</td>
<td>Enabled</td>
<td>Separate Virtual</td>
<td>idm1, idm2</td>
</tr>
<tr>
<td>App Volumes Manager Rule</td>
<td>Enabled</td>
<td>Separate Virtual</td>
<td>appvolumes1, appvolumes2</td>
</tr>
</tbody>
</table>

Table 9: vSphere DRS Rules

Virtual SAN

Virtual SAN pools server-attached HDDs and SSDs to create a distributed shared datastore that abstracts the storage hardware and provides hyper-converged storage optimized for virtual machines without the need for external SAN or NAS.

Virtual SAN uses virtual machine-centric storage policies to automate the storage services levels on a per-VM basis. Horizon integrates into this consumption model and automatically generates the required storage policies as pools are deployed onto a Virtual SAN datastore. For more information, see the VMware Virtual SAN 6.0 Design and Sizing Guide.
Networking
At a high level all network components are configured redundantly either as active/passive or active/active where allowed, and the various traffic types are separated from each other and Quality of Service is controlled with Network IO Control (NIOC) on the configured Distributed Virtual Switch.

![vSphere Networking Diagram](image)

The configuration uses 10 GbE adapters to simplify networking infrastructure and remedy other 1 GB drawbacks such as inadequate bandwidth and lower utilization. Even with these 10 GbE advantages, it is still necessary to ensure that traffic flows can access sufficient bandwidth.

Network I/O Control (NIOC) addresses this requirement by enabling diverse workloads to coexist on a single networking pipe, thus taking full advantage of 10 GbE. NIOC revolves around resource pools similar to those for CPU and memory. The VMware vSphere administrator is given control to ensure predictable network performance when multiple traffic types contend for the same physical network resources.

<table>
<thead>
<tr>
<th>TRAFFIC TYPE</th>
<th>SHARES</th>
<th>SHARES VALUE</th>
<th>RESERVATION</th>
<th>LIMIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Traffic</td>
<td>Normal</td>
<td>50</td>
<td>0 Mbit/s</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Virtual Machine Traffic</td>
<td>High</td>
<td>100</td>
<td>0 Mbit/s</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Virtual SAN Traffic</td>
<td>Normal</td>
<td>50</td>
<td>0 Mbit/s</td>
<td>Unlimited</td>
</tr>
<tr>
<td>vMotion Traffic</td>
<td>Normal</td>
<td>50</td>
<td>0 Mbit/s</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

Table 10: NIOC Configuration
Flow control is disabled for VMkernel interfaces tagged for Virtual SAN (vmk2). Virtual SAN network can use teaming and failover policy to determine how traffic is distributed between physical adapters and how to reroute traffic in the event of adapter failure. NIC teaming is used mainly for high availability for Virtual SAN. However, additional vSphere traffic types sharing the same team still leverage the aggregated bandwidth by distributing different types of traffic to different adapters within the team. Load-based teaming is used, as network convergence on these switch ports will happen fast after the failure because the port will enter the spanning-tree forwarding state immediately, bypassing the listening and learning states.

For more information, see the vSphere Networking guide and Configuring Flow Control on VMware ESXi and VMware ESX.

Physical Environment Design
Several environment resources are required to support a Horizon deployment. In most cases these will already exist. It is important to ensure that minimum versions are met and that any specific configuration for Horizon is followed.

Active Directory
Horizon requires an Active Directory domain structure for user authentication and management. See the View Installation guide for details on supported versions and preparation steps. Standard best practice for an Active Directory deployment should be followed to ensure that it is highly available.

Additionally, for Horizon, set up dedicated organizational units (OUs) for the machine accounts for virtual desktops and RDSH hosts. Consider blocking inheritance on these OUs to stop any existing GPOs from having an undesired effect.

Group Policy
Group Policy (GPO) can be used in a variety of ways to control and configure both Horizon components and also standard Windows settings.

These policies are normally applied to the user or the computer Active Directory account depending on where they are located in Active Directory. In a Horizon environment it is typical to set specific user policy settings for the specific Horizon session only when a user connects to it. We also want to have user accounts processed separately from computer accounts with GPOs. This is where the loopback policy is widely used in any GPO that also needs to configure user settings. This is particularly important with User Environment Manager. User Environment Manager only applies user settings, so if the User Environment Manager GPOs are applied to computer objects, loopback processing must be enabled.

Refer to the Microsoft Web site for details.

DNS
The Domain Name System (DNS) is widely used in a Horizon Enterprise Edition environment, from server components communication to clients and virtual desktops. Follow standard design principles for DNS, making it highly available. Additionally, ensure that:

- Forward and reverse zones are working well.
- Dynamic updates are enabled so that desktops register with DNS correctly.
- Scavenging is enabled and tuned to cope with the rapid cloning and replacement of desktops.
DHCP
In a Horizon environment desktops and RDS hosts rely on DHCP to get IP addressing information. DHCP must be allowed on the VM networks designated for these.

The environment can be quite fluid, with floating pools created with instant clones deleting desktops at logout and recreating replacements. Because of this we need to make sure the lease period is set to a relatively short period (this will depend on the frequency of logouts and the lifetime of a clone).

**Design Decision:** DHCP will be available on the desktops and RDS hosts VM network. It will be deployed using DHCP failover to ensure availability. The lease duration of the scopes used will be set to 4 hours (based on average logout after 8 hours).

Certificate Authority
A Microsoft Enterprise Certificate Authority (CA) is a prerequisite for True SSO. A certificate template is created within the Microsoft CA and is used by True SSO to sign certificate signing requests (CSR) that are generated by the virtual machine. These certificates are short-lived (approximately 1 hour) and are used solely for the purpose of single-signing a user into a desktop without the user having to provide AD credentials when accessing through VMware Identity Manager.

The Microsoft CA will be used to create certificate signing requests for Access Point, VMware Identity Manager, and any other externally facing components. The CSR will then be signed by a well-known external CA to ensure that any device connecting to the environment will have access to a valid root certificate.

Details on setting up a Microsoft CA can be found in the View Administration guide.

**Design Decision:** A Microsoft Enterprise Certificate Authority will be set up to support the True SSO capability.

Key Management Service
To license activate Windows (and Microsoft Office) instances in a VDI environment the recommended method is to use Microsoft Key Management Service (KMS) with volume license keys. As we are typically deleting a desktop at logout and recreating desktops frequently, it is important that this service is highly available. See the Microsoft documentation on how best to deploy volume activation.

**Design Decision:** Microsoft Key Management Service (KMS) will be deployed in a highly available manner to allow desktops and RDS hosts to activate their Microsoft licenses.

Database
As detailed in the component design section, several products require a database to store data and configuration. The database server needs to be highly available and scale to match the demand. One option when using Microsoft SQL Server is to use clustering for HA.

**Design Decision:** Microsoft SQL Server will be set up utilizing Microsoft Failover Clustering to ensure availability.

More information is available in the Microsoft guides on configuring failover clustering for SQL.
Load Balancer
To remove a single point of failure from some components, we can deploy more than one instance and use a third-party load balancer. This not only provides redundancy but also allows the load and processing to be spread across multiple instances of the component. To ensure that the load balancer itself does not become a point of failure, most load balancers allow for setup of multiple nodes in an HA or master/slave configuration.

Firewall and External Access Networking
As we are designing the services to utilize Blast Extreme and external access will be via Access Point appliances with port sharing, the networking and port requirements are fairly straightforward.

- Internal users will connect directly to the load-balanced VMware Identity Managers over port 443, and to the load-balanced View Connection Server also over port 443.
- External users connect through the Access Points for VMware Identity Manager over port 443, which then communicates with the internal VMware Identity Managers over 443. They also connect through the Access Points for Connection Servers over 443.

![Figure 42: User Connectivity Ports](image)
For the full details on all the possible ports, especially when using different protocols, see this blog or this KB article.

File Servers
User Home Drives, User Environment Manager repositories, and ThinApp shares are stored externally from the View environment on SMB shares provided by Windows file servers. We will be using two file servers with Distributed File Services enabled. This will allow both servers to provide the SMB shares under a common shared namespace (DFS-N).

We will use DRS-R in a hub-spoke model to make sure that the primary file server replicates changes to the secondary file server. (Multimaster replication of profile data is not supported by Microsoft.) In the event of an issue with one of the file servers, the share and data will remain available. For more information, refer to the DFS-R Overview from Microsoft.
Service Integration Design

At this stage we have our Horizon 7 Enterprise Edition components designed and deployed and have ensured the environment has all the functionality and qualities that are required. We can now proceed to creating the parts from each of the components, then assembling and integrating them into the end service that will be delivered to the users.

The table below details the parts required for each service. The rest of this section will detail the design and build of each of the services.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Identity Manager</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Windows 10 instant clone</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 10 linked clone</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RDSH linked clone</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux clone</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>App Volumes AppStack</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>App Volumes writable volume</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>User Environment Manager</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Smart Policies</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Application blocking</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Folder redirection</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Mandatory profile</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>GPO</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Printing (ThinPrint)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>ThinApps</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>SaaS Apps</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Access Point</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>True SSO</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>vGPU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 11: Components Required by Service
Common Components
There are common components that will be used in multiple services. To avoid repeating information common to each individual service, we will outline the design of common components first.

Applications
All services are designed to have the option of delivery of applications through VMware Identity Manager.

**Figure 43: Common Application Service Components**

<table>
<thead>
<tr>
<th><strong>VMWARE IDENTITY MANAGER</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Identity Manager directory</td>
<td>VMware Identity Manager will synchronize user account information from Active Directory and use it for entitling applications to users through the Workspace ONE portal.</td>
</tr>
</tbody>
</table>
| VMware Identity Manager catalog | The VMware Identity Manager catalog will be the launch point for applications through the Workspace ONE portal. Applications in the following categories are expected to be configured:  
  • SaaS apps  
  • ThinApps  
  • Horizon desktops  
  • Horizon apps  
  • RDSH apps |
| True SSO | Horizon True SSO support will be configured in VMware Identity Manager to ensure simple end-user access to desktops and apps without multiple login prompts. |
| Access Point | VMware Identity Manager and Access Point will be configured in order to ensure users external to the organization will be able to access the resources that have been configured in the Workspace ONE catalog. See *Deploying Access Point for Reverse Proxy* in *Installing and Configuring VMware Identity Manager* for more information. *(Note: Use the drop-down menu to select an on-premises version of VMware Identity Manager.)* |

<table>
<thead>
<tr>
<th><strong>THINAPPPS</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Identity Manager directory</td>
<td>A ThinApp repository with ThinApp packages will allow use of ThinApp packages through the VMware Identity Manager catalog. ThinApp 4.7.2 and later packages are supported. You must install the VMware Identity Manager desktop in order to use ThinApp apps in your environment. See <em>Integrating VMware ThinApp Packages</em> in <em>Installing and Configuring VMware Identity Manager</em> for more information. <em>(Note: Use the drop-down menu to select an on-premises version of VMware Identity Manager.)</em></td>
</tr>
</tbody>
</table>
### SAAS
Saas-based applications that use SAML as an authentication method will be accessed through VMware Identity Manager. Configuration of applications is done through the templates in the Cloud Application Catalog. See the VMware Identity Manager Integrations documentation for more information.

### VIEW DESKTOPS AND APPLICATION POOLS

| View desktops | From the Catalog tab, under Manage Desktop Applications, select View Application and enable View Pools.  
|               | • Provide View pod information for the pods you are adding.  
|               | • Configure SAML authentication between VMware Identity Manager and View Connection Servers. |

| View application pools | RDSH apps and their entitlements will populate the VMware Identity Manager catalog when View pools and a View pod are configured as above. |

### AUTHENTICATION METHODS

#### Kerberos
- In order to provide single sign-on to the VMware Identity Manager portal, the appropriate authentication methods must be enabled.
  - The default authentication method is password, which will prompt for the user’s Active Directory user ID and password.
  - If Kerberos is enabled as the default authentication method, the user’s Windows credentials will be passed to VMware Identity Manager when they open the portal.
  - Kerberos authentication must be enabled under the Connectors section of the Identity and Access Management tab in the portal.
  - Select the name of the VMware Identity Manager Server in the Worker column, and choose Auth Adapters.
  - Enable the Kerberos adapter.
  - Finally, configure the user’s Web browser to automatically log in to Web sites in the Intranet zone.
  - See Implementing Kerberos for Desktops with Integrated Windows Authentication in the VMware Identity Manager Administration Guide for more information. *(Note: Use the drop-down menu to select an on-premises version of VMware Identity Manager.)*

#### Configure Access Policies
- Access policies are configured to establish how an operating system, network, or application should be set up to authenticate.
  - Under the Identity and Access Management tab, select Policies. Select Default_Access_Policy and for the Web browser choose Kerberos as the first authentication method, and Password for the second.
  - Note that you may want to use different policies for different network ranges so that Kerberos is used for internal connections but other authentication methods are used for external connections.
  - See Managing Access Policies in the VMware Identity Manager Administration Guide for more information. *(Note: Use the drop-down menu to select an on-premises version of VMware Identity Manager.)*
## High Availability

**Cloning VMware Identity Manager**

- To create a high-availability VMware Identity Manager environment, the VMware Identity Manager appliance will be cloned and redeployed under a new name and IP address.
- With the use of an internal database, the database must be replicated between VMware Identity Manager clones. See the KB article Using embedded vPostgres in production for VMware Workspace Portal VA 2.1 and VMware Identity Manager 2.4 for more information.

  **Important:** The script provided in the article might not open the appropriate ports for communication. Verify that port 5432 has been opened by checking the file:

  - `/usr/local/horizon/conf/iptables.cfg`
  - for the line:

    ```
    TOMCAT_tcp_all="443 80 8443 8080 6443 5443 5432"
    ```

- See Configuring Failover and Redundancy in Installing and Configuring VMware Identity Manager for details. *(Note: Use the drop-down menu to select an on-premises version of VMware Identity Manager.)*

## Cloud Pod Architecture

- To configure VMware Identity Manager to be able to work with Horizon Cloud Pod Architecture entitlements, each of the VMware Identity Manager connectors must be able to access all of the View pods within the global cluster.
- Configure pod, then under the Federation tab, enable CPA Federations.
- Configure network ranges within the Identity & Access Management tab to reflect the site and external topology of your network.
Desktop Pools
Multiple services will use the same underlying desktop pool type (core service). Where there is no variation in the hardware specifications of the desktop, the same pool can be re-used to address multiple use cases. AppVolumes and User Environment Manager will provide the customization to the use case.

Business Process Application Service
Core Service

![Diagram of Business Process Application Service – Core](image)

**Figure 45: Business Process Application Service – Core**

<table>
<thead>
<tr>
<th>RDS HOST LINKED CLONE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows 2012 R2 master virtual machine</strong></td>
</tr>
<tr>
<td><strong>Automated RDSH farm</strong></td>
</tr>
</tbody>
</table>
Applications

![Diagram](image)

**Figure 46: Business Process Application Service - Applications**

<table>
<thead>
<tr>
<th>APP VOLUMES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create AppStacks as required to address the use cases. Follow the instructions in <em>Working with AppStacks</em> in the VMware App Volumes User Guide for details. Since the AppStacks will be targeting an RDSH server, the AppStack will need to be captured on the same operating system (Windows Server 2008 R2 or Windows Server 2012 R2). This is done to ensure that applications are compatible with the OS they are being attached to. Since we are using RDSH linked clones, App Volumes saves us from needing to install the same applications on each node. We assign the AppStack containing the core applications and each RDSH linked-clone server will have the same application set for publishing.</td>
</tr>
<tr>
<td>Core applications</td>
</tr>
</tbody>
</table>
| • Create an AppStack to contain all core applications to be delivered as RDSH published applications.  
• These AppStack-delivered applications will be published via RDSH.  
• Assign and entitle to an Active Directory group containing the RDSH Server machine accounts—these will be machine-based assignments. |
| Application pool |
| • Add an application pool in the Horizon Administrator console to publish the desired applications. See *Creating Application Pools* in Setting Up Desktop and Application Pools in View for details.  
• Entitle the relevant user groups to the matching published apps. |
### Profile and User Data

![Profile and User Data Diagram](image)

**Figure 47: Business Process Application Service – Profile and User Data**

#### PROFILE CONFIGURATION

| Mandatory profile | • Set up a mandatory profile and use a group policy to assign it to the OU that will contain the desktop objects.  
|                   | • See Appendix H: Mandatory Profile for details. |
| User Environment Manager | Make sure there are User Environment Manager profiles created and configured properly for each application you wish to save user settings for. |
| Environment settings | • Map H: drive to the users' home drive with User Environment Manager.  
|                       | • Map location-based printers with User Environment Manager (IP Address Range). |
| Personalization – applications | • Verify there is a profile for each application that should persist user settings across sessions.  
|                       | • If a profile does not exist, use the Application Profile to create one and place it in the configuration share. |
| Folder redirection | • Folder redirection will be configured from User Environment Manager 9.0. This will automatically redirect the user profile folders to a file share, so user data will persist across sessions.  
|                       | • See Appendix G: Smart Policies for details. |

#### Policy

| PROFILE CONFIGURATION | Leverage Horizon 7 Smart Policies to do the following:  
|                       | • Apply the Internal Horizon Smart Policy profile, which allows USB, copy/paste, client drive redirection, and printing.  
|                       | • See Appendix G: Smart Policies for details. |
Mobile Secure Workspace Service

**Core Service**

![Diagram](image)

**Figure 48: Mobile Secure Workspace Service – Core**

<table>
<thead>
<tr>
<th>WINDOWS 10 INSTANT CLONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10 master virtual machine</td>
</tr>
</tbody>
</table>
| Automated desktop pool | • Create a Horizon automated instant clone desktop pool using the prepared master VM. See Create an Instant-Clone Desktop Pool in Setting Up Desktop and Application Pools in View for details.  
  • Use the specific pool settings from Appendix C: Horizon Installation and Configuration.  
  • Entitle users = Add AD group |
Applications

### APP VOLUMES

Create AppStacks as required to address the use cases. Follow the instructions in *Working with AppStacks* in the VMware App Volumes User Guide for details.

| Core applications | • Create an AppStack to contain all core applications.  
|                   | • Assign and entitle the AppStack to an Active Directory group.  
| Departmental applications | • Create an AppStack for each department containing unique applications to them.  
|                          | • Assign and entitle relevant user groups to their matching departmental AppStack.  

Profile and User Data

This service will use the same structure and design for profile and user data as outlined above in the Mobile Secure Workspace Service.
Policy

<table>
<thead>
<tr>
<th>PROFILE CONFIGURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Smart Policies</strong></td>
</tr>
<tr>
<td>• Internal location: Apply internal Horizon Smart Policy.</td>
</tr>
<tr>
<td>• External location: Apply external Horizon Smart Policy.</td>
</tr>
<tr>
<td>zContractors</td>
</tr>
<tr>
<td>(Note: Smart Policies are evaluated in alphabetical order. Adding the z character before Contractor places the policy name at the bottom of the sort group.)</td>
</tr>
<tr>
<td>See Appendix G: Smart Policies for samples.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Application Blocking</strong></th>
<th>Leverage Application blocking in User Environment Manager to block the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Regedit.exe</td>
<td></td>
</tr>
<tr>
<td>• Cmd.exe</td>
<td></td>
</tr>
</tbody>
</table>

| **Group Policies**      | No specific group policies. |

Dedicated Power Workspace Service

The Dedicated Power Workspace Service uses similar integration as the Mobile Secure Workspace Service described above, with the addition of an App Volumes writable volume.

Applications

Figure 50: Dedicated Power Workspace Service – Applications
APP VOLUMES

Create AppStacks as required to address the use cases. Follow the instructions in Working with AppStacks in the VMware App Volumes User Guide for details.

| Core applications | • Create an AppStack to contain all core applications. |
|                   | • Assign and entitle the AppStack to an Active Directory group. |
| Departmental applications | • Create an AppStack for each department containing unique applications to them. |
|                          | • Assign and entitle relevant user groups to their matching departmental AppStack. |

Create writeable volumes for each user (or for the user group) that will be entitled to this desktop pool. This writeable volume will capture any user-installed application and persist the applications across user sessions.

Follow the instructions in Working with Writable Volumes in the VMware App Volumes User Guide for details.

Profile and User Data

This service will use the same structure and design for profile and user data as outlined above in the Mobile Secure Workspace Service.

Policy

<table>
<thead>
<tr>
<th>PROFILE CONFIGURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Policies</td>
</tr>
<tr>
<td>- Internal location: Apply internal Horizon Smart Policy.</td>
</tr>
<tr>
<td>- External location: Apply external Horizon Smart Policy.</td>
</tr>
<tr>
<td>IT (Power User)</td>
</tr>
<tr>
<td>- External location: Apply external Horizon Smart Policy.</td>
</tr>
<tr>
<td>Application Blocking</td>
</tr>
<tr>
<td>Group Policies</td>
</tr>
</tbody>
</table>

Developer Workspace Service

Horizon for Linux centralizes desktop management and secures data in the data center while supporting end users with seamless access to Linux services across devices, locations, mediums, and connections. Furthermore, this solution allows organizations to move away from costly Windows licensing and to embrace low-cost endpoints to deliver the best possible total cost of ownership.
Core Service and Apps

The core Linux desktop in the service is constructed using full clones of a Linux Master VM that has applications pre-installed. The process of creating the clones can be automated for bulk deployment.

<table>
<thead>
<tr>
<th>LINUX CLONE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux master virtual machine</td>
<td>Follow the instructions in Create a Virtual Machine Template for Cloning Linux Desktop Machines in Setting Up Horizon 7 for Linux Desktops.</td>
</tr>
<tr>
<td>Customization specification</td>
<td>Follow the instructions in Create a Customization Specification for Linux in the vSphere Virtual Machine Administration Guide.</td>
</tr>
<tr>
<td>Install applications</td>
<td>Install all needed applications on the master virtual machine.</td>
</tr>
<tr>
<td>Clone virtual machine</td>
<td>Follow the instructions in Sample Script to Clone Linux Virtual Machines in Setting Up Horizon 7 for Linux Desktops.</td>
</tr>
<tr>
<td>Join Active Directory</td>
<td>Follow the instructions in Sample Script to Join Cloned Virtual Machines to AD Domain in Setting Up Horizon 7 for Linux Desktops.</td>
</tr>
<tr>
<td>Configure 3D on virtual machine (optional)</td>
<td>Follow the instructions in Configure RHEL 6.6 and RHEL 7.1 for vGPU in Setting Up Horizon 7 for Linux Desktops.</td>
</tr>
<tr>
<td>Install Horizon Agent</td>
<td>Follow the instructions in Sample Script to Install Horizon Agent on Linux Virtual Machines in Setting Up Horizon 7 for Linux Desktops.</td>
</tr>
<tr>
<td>Update configuration options</td>
<td>Follow the instructions in Sample Script to Upload Configuration Files to Linux Virtual Machines in Setting Up Horizon 7 for Linux Desktops.</td>
</tr>
<tr>
<td>Create a desktop pool</td>
<td>Follow the instructions in Create a Desktop Pool That Contains Linux Virtual Machines in Setting Up Horizon 7 for Linux Desktops.</td>
</tr>
</tbody>
</table>
User Data

Users can reach their Windows user data from their file shares. For automount on Red Hat Enterprise Linux, see AUTOFS.

High-Performance Workspace Service

Core Service

Figure 52: Developer Workspace Service – User Data

Figure 53: High Performance Workspace Service – Core
The core is constructed using Horizon linked clones. A master virtual machine will be configured, then a snapshot is taken. That snapshot is cloned into the replica, which is shared by all of the linked clones. The linked clones access the replica read-only and save any changes to the linked-clone delta files. Since we are using folder redirection there should be little data stored to the linked clones. During the pool creation we will choose a graphics profile and deploy these to vSphere hosts that have NVIDIA vGPU cards installed.

Depending on the NVIDIA graphics cards chosen, there are different profiles with different capabilities available. To understand the choices, see NVIDIA Virtual GPU Types in Setting Up Horizon 7 for Linux Desktops and the NVIDIA Web site.

We also need to be sure that we properly configure DRS and affinity rules to keep these desktops only on hosts that have NVIDIA cards.

<table>
<thead>
<tr>
<th>WINDOWS 10 LINKED CLONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10 master</td>
</tr>
<tr>
<td>Automated desktop pool</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Applications

This service uses the same application types as the Dedicated Power Workspace service above. Departmental AppStacks will be created for specific applications required by that department.
Profile and User Data

This service will use the same structure and design for profile and user data as is outlined above in the Mobile Secure Workspace Service.

Policy

<table>
<thead>
<tr>
<th>POLICY CONFIGURATION</th>
<th>Description</th>
</tr>
</thead>
</table>
| Smart Policies        | Multimedia Designer  
  • Internal location: Apply internal Horizon Smart Policy.  
  • External location: Apply external Horizon Smart Policy.  
  See Appendix G: Smart Policies for samples. |
| Application blocking  | No application blocking settings. |
| Group policies        | No specific group policies. |
User Experience Design
The success of any end-user computing solution hinges on the quality of the end user’s experience. This can sometimes be difficult to measure because it can be affected by the users’ perception. It is important to understand how users will interact with the environment and whether it delivers what they need. Feedback from users should be incorporated into the design—and on an ongoing basis—to ensure that any required changes are made to keep the solution relevant.

- How do users connect?
- How do users interact with the interfaces, applications, and other aspects of the solution?
- Does the workflow match how they need to work?
- What will it look like for them?
- Do the client device capabilities fulfill the use case needs?
- Does the environment deliver a usable and reliable experience? Consider response time, availability, ease of use, and the ability to customize to individual needs.

Client Devices (Endpoints)
One of the aims of Horizon 7 Enterprise Edition is to allow access to applications and desktops from any device. The use in this reference architecture of VMware Identity Manager as the common access mechanism for all resources provides a familiar interface and experience across all devices.

When accessing Horizon desktops and remoted applications it should be noted that not all clients are equal, nor do all clients have the same capabilities. While a tablet device such as an iPad may be great for mobility and certain use cases, it would not be suitable if features such as multimonitor or USB redirection were required.

A user’s main working client device should match the requirements for that use case. This does not mean that a user is limited to just that device, just that other devices may not have all the functionality needed to deliver the full experience and capabilities.

- Understand the use cases thoroughly.
- There is no one perfect endpoint—different uses may require different choices.
- Users will use multiple devices—try to set expectations about differences.
- Understand Microsoft Virtual Desktop Access (VDA) licensing implications.

One area that needs careful consideration is the use of Real-Time Audio-Video (RTAV) solutions such as Microsoft Skype for Business (Lync), especially where this includes VoIP or video calling.

For example, the Lync client plug-in that gets installed onto the endpoint is only available from Microsoft for Windows devices. This drives the choice of client device to be a thick or thin Windows device that is able to have this plug-in installed.

More detail is available in Configuring Real-Time Audio-Video in Setting Up Desktop and Application Pools in View and in Microsoft Lync 2013 on View in VMware Horizon 6.
Sample User Workflows

User Application Access

The solution provides simple authentication and single sign-on to a single catalog of applications. Users have access to a variety of entitled applications.

Figure 55: Internal Login to VMware Identity Manager
External access requires two-factor authentication. Depending on entitlements, some users will have a mix of SaaS and published (RDSH) apps, and some will have virtual desktops.

Figure 56: External Login to VMware Identity Manager

Figure 57: Applications in VMware Identity Manager
Figure 58: Desktops and Applications in VMware Identity Manager

Users can self-serve and add applications through the catalog. They can also use filters and searches to help find things in both the catalog and on their own workspace.

Figure 59: VMware Identity Manager Self-Service
User Application Launch

Users can launch differing types of applications from within their workspace. Web page links open in new tabs. When launching links to SaaS applications (for example, Salesforce), single sign-on is used and the user is automatically authenticated.

Figure 60: SaaS Application Launch and Single Sign-On

If entitled, users can launch a virtual desktop and single sign-on to the desktop.

Figure 62: User Launch of a Horizon Desktop
When in the desktop, users will also be single-signed into VMware Identity Manager inside the desktop to provide access to all applications delivered through VMware Identity Manager.

Figure 63: Single Sign-On to VMware Identity Manager Inside a Horizon Desktop

Inside a virtual desktop, Windows applications can be run in the usual manner within Windows. As per the services design, these Windows applications could be:

- Pre-installed into the Master VM (and so present in all clones)
- Core applications attached through a common App Volumes AppStack
- Departmental applications given to specific users through an AppStack

If a user is a power user and has been entitled (given an App Volumes writeable volume), they will also be able to install their own applications and have them persist across sessions.
About the Authors and Contributors

Lead Author
Graeme Gordon is a Senior End-User Computing (EUC) Architect in VMware End-User Computing Technical Marketing. He is currently focusing on best-practice technical architecture throughout the Horizon portfolio, white paper and collateral creation, enablement of technical communities, and tool development. He has over 25 years of industry experience in Infrastructure and end-user computing in the design and implementation of complex computing environments of all scopes and sizes and in leading teams to deliver them.

Contributing Authors
Alex Birch is an EUC Architect in VMware End-User Computing Technical Marketing. His role involves creating deep-dive content and he produces technical content for specialist staff and partners. Alex has more than 20 years of IT experience, which includes working within the EUC space for more than 15 years and specializing in virtual desktop design and implementation since 2007.

Chris Halstead is an EUC Architect in VMware End-User Computing Technical Marketing. He has over 20 years’ experience in the end-user computing space. Chris’s experience ranges from managing a global desktop environment for a Fortune 500 company, to managing and proving EUC professional services at a VMware partner and most recently as an End-User Computing SE for VMware. Chris has written five VMware Flings, many detailed blog articles, and has been a VMware vExpert since 2012.

Kevin Sheehan is an EUC Architect with VMware End-User Computing Technical Marketing. He has over 20 years’ experience in the IT industry related to productivity, operating system, device, and management technologies. Kevin’s present focus is on VMware Identity Manager and Workspace ONE products.

Hilko Lantinga is an EUC Architect in VMware End-User Computing Technical Marketing, with a focus on 3D, Horizon, Horizon Air, Linux, AirWatch, and Applications. Previously he was a Senior Consultant in VMware Professional Services, leading large-scale EUC deployments in EMEA and has 18 years of experience in end-user computing.

Donal Geary is a Reference Architect Engineer in VMware End-User Computing Technical Marketing. Previously he worked as Lead System Administrator for VMware Internal IT, and as Senior Technical Support Engineer for the VMware Global Support Services Organization.

Stephane Asselin is a Senior Architect in VMware End-User Computing Technical Marketing.

Matt Coppinger is a Director in VMware End-User Computing Technical Marketing.
Appendix A: Use Case Definitions

Static Task Worker
Static task workers are typically fixed to a specific location with no remote access requirement. Examples include call center worker, administration worker, and retail user. A static task worker:

• Uses a small number of Microsoft Windows applications. They do not install their own applications and do not require SaaS application access.
• Requires location aware printing.

Mobile Knowledge Worker
A mobile knowledge worker could be a hospital clinician, a company employee, or work in finance or marketing. This is a catch-all use case for many corporate use cases. A mobile knowledge worker:

• Mainly uses applications from a corporate location, but may access applications from mobile locations.
• Uses a large number of core and departmental applications but does not install their own applications. Requires SaaS application access.
• Has a video playback and Flash content requirement. Their GPU requirement is minimal, but GPU would improve user experience.
• Requires access to USB devices.
• Requires location-aware printing.
• Requires two-factor authentication when accessing applications remotely.

Software Developer / IT (Power User)
Power users require administration rights to install applications. They could be using Windows or Linux OS, with many applications, some of which require extensive CPU and memory resources. A power user:

• Mainly uses applications from a corporate location, but may access applications from mobile locations.
• Uses a large number of core and departmental applications and installs their own applications. Requires SaaS application access.
• Has a video playback and Flash content requirement.
• Requires two-factor authentication when accessing applications remotely.

Multimedia Designer
Multimedia designers are intensive users that require GPU-accelerated applications and/or intensive CPU and memory workloads. Examples are CAD/CAM designers, architects, video editor/reviewers, graphics artists, or game designers. A multimedia designer:

• Mainly uses applications from a corporate location, but may access applications from mobile locations.
• Uses a large number of core and departmental applications and installs their own applications. Requires SaaS application access.
• Has a GPU requirement with API support for DirectX 10+, video playback, and Flash content.
• Requires two-factor authentication when accessing applications remotely.
Contractor
An external contractor requires access to specific line-of-business applications, typically from a remote or mobile location.

• Mainly uses applications from a corporate location, but may access applications from mobile locations.
• Uses a subset of core and departmental applications based on the project they are working on. May require SaaS application access.
• Has restricted access to clipboard, USB devices, and so on. Requires two-factor authentication when accessing applications remotely.
Appendix B: Management Virtual Machine Specifications

For each of the management virtual machines there are recommended builds and specifications.

**vCenter Server**

A vCenter Server can be deployed as a prepackaged appliance, as was done for this paper, or alternatively, it can be installed in a Windows server.

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>vCenter 6U2</td>
</tr>
<tr>
<td>Virtual machine hardware</td>
<td>VMware Virtual Hardware version 8</td>
</tr>
<tr>
<td>OS</td>
<td>SUSE Linux Enterprise 11 (64-bit)</td>
</tr>
<tr>
<td>vCPU</td>
<td>8</td>
</tr>
<tr>
<td>vMemory</td>
<td>24 GB</td>
</tr>
<tr>
<td>vNICs</td>
<td>1</td>
</tr>
<tr>
<td>Virtual network adapter 1</td>
<td>VMXNET3 Adapter</td>
</tr>
<tr>
<td>Virtual SCSI controller 0</td>
<td>LSI Logic Parallel</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:0 Disk 12 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:1 Disk 14 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:2 Disk 50 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:3 Disk 50 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:4 Disk 25 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:5 Disk 25 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:6 Disk 10 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:8 Disk 50 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:10 Disk 10 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:12 Disk 25 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:14 Disk 25 GB</td>
</tr>
</tbody>
</table>

*Table 12: vCenter Server Virtual Machine Specifications*
SQL Server

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>SQL Server 2012 Standard SP2</td>
</tr>
<tr>
<td>Virtual machine hardware</td>
<td>VMware Virtual Hardware version 11</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td>vCPU</td>
<td>2</td>
</tr>
<tr>
<td>vMemory</td>
<td>8 GB</td>
</tr>
<tr>
<td>vNICs</td>
<td>1</td>
</tr>
<tr>
<td>Virtual network adapter 1</td>
<td>VMXNET3 Adapter</td>
</tr>
<tr>
<td>Virtual SCSI controller 0</td>
<td>LSI Logic SAS</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:0 Windows OS 40 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:1 Data Disk 50 GB</td>
</tr>
</tbody>
</table>

Table 13: SQL Server Virtual Machine Specifications

View Connection Server

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Horizon View 7.0</td>
</tr>
<tr>
<td>Virtual machine hardware</td>
<td>VMware Virtual Hardware version 11</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td>vCPU</td>
<td>4</td>
</tr>
<tr>
<td>vMemory</td>
<td>12 GB</td>
</tr>
<tr>
<td>vNICs</td>
<td>1</td>
</tr>
<tr>
<td>Virtual network adapter 1</td>
<td>VMXNET3 Adapter</td>
</tr>
<tr>
<td>Virtual SCSI controller 0</td>
<td>LSI Logic SAS</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:0 Windows OS 40 GB</td>
</tr>
</tbody>
</table>

Table 14: View Connection Server Virtual Machine Specifications
### VMware View Composer

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>VMware View Composer 7.0</td>
</tr>
<tr>
<td>Virtual machine hardware</td>
<td>VMware Virtual Hardware version 11</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td>vCPU</td>
<td>4</td>
</tr>
<tr>
<td>vMemory</td>
<td>12 GB</td>
</tr>
<tr>
<td>vNICs</td>
<td>1</td>
</tr>
<tr>
<td>Virtual network adapter 1</td>
<td>VMXNET3 Adapter</td>
</tr>
<tr>
<td>Virtual SCSI controller 0</td>
<td>LSI Logic SAS</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:1 Windows OS 40 GB</td>
</tr>
</tbody>
</table>

Table 15: View Composer Virtual Machine Specifications

### VMware App Volumes Manager

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>VMware App Volumes 2.11</td>
</tr>
<tr>
<td>Virtual machine hardware</td>
<td>VMware Virtual Hardware version 11</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td>vCPU</td>
<td>2</td>
</tr>
<tr>
<td>vMemory</td>
<td>8 GB</td>
</tr>
<tr>
<td>vNICs</td>
<td>1</td>
</tr>
<tr>
<td>Virtual network adapter 1</td>
<td>VMXNET3 Adapter</td>
</tr>
<tr>
<td>Virtual SCSI controller 0</td>
<td>LSI Logic SAS</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:1 Windows OS 40GB</td>
</tr>
</tbody>
</table>

Table 16: App Volumes Manager Virtual Machine Specifications
**VMware vRealize Operations Manager**

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>VMware vRealize Operations Manager 6.2</td>
</tr>
<tr>
<td>Virtual machine hardware</td>
<td>VMware Virtual Hardware version 8</td>
</tr>
<tr>
<td>OS</td>
<td>SUSE Linux Enterprise 11 (64-bit)</td>
</tr>
<tr>
<td>vCPU</td>
<td>4</td>
</tr>
<tr>
<td>vMemory</td>
<td>16 GB</td>
</tr>
<tr>
<td>vNICs</td>
<td>1</td>
</tr>
<tr>
<td>Virtual network adapter 1</td>
<td>VMXNET3 Adapter</td>
</tr>
<tr>
<td>Virtual SCSI controller 0</td>
<td>LSI Logic Parallel</td>
</tr>
</tbody>
</table>
| Virtual disk – VMDK (scsi0:x) | Scsi0:0 Disk 20GB  
Scsi0:1 Disk 250GB  
Scsi0:2 Disk 4GB          |

*Table 17: vRealize Operations Manager Virtual Machine Specifications*
Appendix C: Horizon Installation and Configuration

Installation Prerequisites
Before starting, certain other infrastructure components must be in place and configured:

• Management vSphere cluster
• VDI vSphere cluster
• Windows 2012 R2 VM template
• Active Directory
• DNS
• DHCP
• Certificate Authority
• Load balancer

Installation Steps
This section outlines the Horizon installation steps.

<table>
<thead>
<tr>
<th>STEP</th>
<th>TASK</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Set up the required administrator users and groups in Active Directory.</td>
</tr>
<tr>
<td>2</td>
<td>If you have not yet done so, install and set up ESXi hosts and vCenter Server.</td>
</tr>
<tr>
<td>3</td>
<td>(Optional) If you are going to deploy linked-clone desktops, install View Composer, either on the vCenter Server system or on a separate server. Also install the View Composer database.</td>
</tr>
<tr>
<td>4</td>
<td>Install and set up View Connection Server. Also install the event database.</td>
</tr>
<tr>
<td>5</td>
<td>Create one or more virtual machines that can be used as a template for full-clone desktop pools or as a parent for linked-clone desktop pools or instant-clone desktop pools.</td>
</tr>
<tr>
<td>6</td>
<td>Set up an RDS host VM and install applications to be remoted to end users.</td>
</tr>
<tr>
<td>7</td>
<td>Create desktop pools, application pools, or both.</td>
</tr>
<tr>
<td>8</td>
<td>Control user access to desktops.</td>
</tr>
<tr>
<td>9</td>
<td>Install Horizon Client on end users’ machines and have end users access their remote desktops and applications.</td>
</tr>
<tr>
<td>10</td>
<td>(Optional) Create and configure additional administrators to allow different levels of access to specific inventory objects and settings.</td>
</tr>
<tr>
<td>11</td>
<td>(Optional) Configure policies to control the behavior of Horizon components, desktop and application pools, and end users.</td>
</tr>
<tr>
<td>12</td>
<td>(Optional) For added security, integrate smart card authentication or a RADIUS two-factor authentication solution, especially where external access is allowed. This is covered in Appendix D: Access Point Installation and Configuration.</td>
</tr>
</tbody>
</table>
Preparation
Build three virtual machines (VMs), two for Connection Servers and one for the View Composer Server. These will be hosted and physically located in the management cluster.

Follow the hardware specifications in Appendix A and assign all three VMs static IP addresses.

Deployment
This guide is not intended to replace the Horizon documentation. Please follow the relevant section of the View Installation guide to install the following components.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>INSTALL GUIDE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install the first Standard Connection Server</td>
<td>See Install View Connection Server with a New Configuration in the View Installation guide.</td>
</tr>
<tr>
<td>2. Install a Replica Connection Server</td>
<td>See Install a Replicated Instance of View Connection Server in the View Installation guide.</td>
</tr>
</tbody>
</table>

Post-Installation Configuration
Connect to the first Connection Server.

<table>
<thead>
<tr>
<th>TASK</th>
<th>DOCUMENTATION INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Apply license. • Add vCenter. • Add View Composer and domains. • Configure View Storage Accelerator.</td>
<td>See Configuring View Connection Server for the First Time in the View Installation guide.</td>
</tr>
<tr>
<td>Add instant clone domain admins.</td>
<td>See Add an Instant-Clone Domain Administrator in the Setting Up Desktop and Application Pools in View guide.</td>
</tr>
<tr>
<td>Configure event reporting.</td>
<td>See Configuring Event Reporting in the View Installation guide.</td>
</tr>
<tr>
<td>Assign administrators and roles.</td>
<td>See Configuring Role-Based Delegated Administration in the View Administration guide.</td>
</tr>
</tbody>
</table>
For each of the Connection Servers, configure the following.

<table>
<thead>
<tr>
<th>TASK</th>
<th>DETAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>General settings</td>
<td>As we are using Access Point for external connectivity the following fields will be left unselected: HTTPS Secure Tunnel, PCoIP Secure Gateway, Blast Secure Gateway.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Follow the steps in Configure a SAML Authenticator in View Administrator in the View Administration guide to set up the VMware Identity Manager as a SAML authenticator.</td>
</tr>
<tr>
<td>Backup</td>
<td>Define a backup schedule and location for the Connection Server config as per View Configuration Backup Settings in the View Administration guide.</td>
</tr>
</tbody>
</table>
| Origin checking   | With multiple Connection Servers fronted by a load balancer, it is necessary to change origin checking on each server. This requires the creation of a locked.properties file in the C:\Program Files\VMware\VMware View\Server\sslgateway\conf directory and the addition of the following entries as detailed in Origin Checking in the View Security guide.  
  • checkOrigin=false  
  • balancedHost=horizon.example.com  
  • portalHost.1=access-point-name-1.example.com  
  • portalHost.2=access-point-name-2.example.com |

Certificates
When you first install Horizon, it uses self-signed certificates. It is not recommended that you use these in production. At a high level, the steps for replacing the certificates on the Connection Servers and the View Composer Server are:

1. Create a certificate signing request (CSR) config file. This file is used to generate the CSR to request a certificate.
2. Once you receive the signed certificate, import it.
3. Configure Horizon to use the signed certificate.

For the full process, see Obtaining SSL Certificates from a Certificate Authority in Scenarios for Setting Up SSL Certificates for View.
## Pool Settings

<table>
<thead>
<tr>
<th>Desktop Pool Definition</th>
<th>INSTANT-CLONE POOL</th>
<th>LINKED-CLONE POOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Type</td>
<td>Automated</td>
<td>Automated</td>
</tr>
<tr>
<td>• User Assignment</td>
<td>Floating</td>
<td>Floating</td>
</tr>
<tr>
<td>• vCenter Server</td>
<td>Instant clones</td>
<td>View Composer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Linked clones</td>
</tr>
<tr>
<td>Desktop Pool Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Remote Machine Power Policy</td>
<td>N/A</td>
<td>Always powered on</td>
</tr>
<tr>
<td>• Delete or refresh machine on logout</td>
<td>N/A</td>
<td>Refresh immediately</td>
</tr>
<tr>
<td>• Default display protocol</td>
<td>VMware Blast</td>
<td>VMware Blast</td>
</tr>
<tr>
<td>• 3D renderer</td>
<td>N/A</td>
<td>NVIDIA GRID vGPU</td>
</tr>
<tr>
<td>• HTML access</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

| Provisioning Settings   |                    |                   |
| • Provision all machines up-front | Selected | Selected |

| Storage Optimization    |                    |                   |
| • Use VMware Virtual SAN | Selected           | Selected          |

| Guest Customization     |                    |                   |
| • AD container          | Dedicated OU for this type of desktop | Dedicated OU for this type of desktop |

Table 18: Pool Settings

## RDS Farm Settings

<table>
<thead>
<tr>
<th>RDS Farm Settings</th>
<th>RDS FARM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Pool Definition</td>
<td>Automated</td>
</tr>
<tr>
<td>Identification and settings</td>
<td>VMware Blast Enabled 30</td>
</tr>
<tr>
<td>Storage Optimization</td>
<td>Selected</td>
</tr>
<tr>
<td>Guest Customization</td>
<td>Dedicated OU for this type of desktop Predefined spec</td>
</tr>
</tbody>
</table>

Table 19: RDS Farm Settings
Appendix D: Access Point Installation and Configuration

To facilitate a successful installation of Access Point, various prerequisites must be in place prior to performing an installation. The following section details the prerequisites and deployment options available that satisfy the design requirements.

**Note:** Only the options that satisfy the design requirements are described here. Other options are available and documented within the Access Point documentation.

Not all sections apply to a VMware Identity Manager or Horizon deployment.

Appliance Requirements

Each Access Point appliance has the following requirements:

- 4 GB RAM
- 2 x vCPU
- 1 - 3 NICs
- 20 GB disk space

Deployment Options

There are three supported methods of deploying Access Point. In this section we briefly discuss each option and then detail the optimal solution to satisfy the design requirements.

**OVF Wizard (Manual Deployment)**

Access Point can be deployed by using the OVF wizard and responding to various deployment questions during the deployment phase. The manual method requires responses from an IT administrator during deployment—the Access Point is not production-ready on first boot and requires significant post-deployment configuration using the RESTAPI and multiple reboots to make the appliance production-ready.

**OVF Tool (Automated Method)**

The OVF Tool method ensures that the Access Point is production-ready on first boot. It is a fully scripted and automated method of deployment. The OVF Tool method is the most flexible as it allows you to define all the configuration options during deployment. However, the command line to perform the installation is complex and prone to syntax errors when typing the command-line parameters. It also requires the IT administrator to be comfortable with converting standard PEM certificates into single-line PEM certificates.

**APDeploy (Automated Method)**

The APDeploy method also ensures that the Access Point is production-ready on first boot. This method still uses the OVF Tool in the background; however, the IT administrator simply updates an INI file with the configuration settings they require and deploys the Access Point by typing a simple deployment command in PowerShell (`\apdeploy.ps1 -infile <name>.ini`).

**Design Decision:** The APDeploy method will be used as it will satisfy most deployment scenarios and does not require the IT administrator to enter complex OVF Tool commands to complete the deployment.

Download the APDeploy tool from: [https://communities.vmware.com/docs/DOC-30835](https://communities.vmware.com/docs/DOC-30835).
Installation Prerequisites
Certificates
Certificates are used to secure communications between the endpoint and the Access Point and between the Access Point and View Connections Servers and VMware Identity Manager.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate format</td>
<td>At a minimum two certificates are required: a server certificate and the associated private key. If your Certificate Authority uses intermediate certificates, then you will need to create a certificate chain that includes the server certificate and the intermediate certificates.</td>
</tr>
<tr>
<td>Supported certificate types</td>
<td>Access Point requires certificates to be formatted as a PEM certificate. If your CA uses .PFX- or .P12-formatted certificates, you will need to convert these to PEM certificates. See Convert Certificate Files to One-Line PEM Format in the Deploying and Configuring Access Point for instructions.</td>
</tr>
</tbody>
</table>

Table 20: Certificate Details
Password Requirement
Access Point requires the IT administrator to define two passwords during installation: The first is to secure access to the REST API, the second is to secure access to the Access Point appliance console. The passwords must meet with the minimum requirements as stated in the Access Point documentation.

vCenter Network Profiles
Regardless of the type of deployment chosen, vCenter network profiles are required for each network that the Access Point is attached to. The network profile will provide:

- Default Gateway
- Subnet mask
- Subnet
- DNS Servers
- DNS Domain

IP Address and Fully Qualified Domain Name (FQDN)
As previously discussed, the Access Point in this scenario will be configured with two NICs. An IP address for each of following will be required:

- Internet facing IP address + External FQDN
- Backend and management IP address + FQDN

Horizon-Specific Settings
This section details settings that are specific to an Access Point and Horizon installation.

View Connection Server Details
Access Point needs to know how to contact the View Connection Servers. In this deployment scenario we are using a load balancer (LB) to provide control over how load is distributed across the Connection Servers. The fully qualified domain name (FQDN) of the virtual IP (VIP) associated with the load balancer is specified during installation of the Access Point.

Horizon Thumbprint Info – Self-Signed Certificates
If the View Connection Servers are using certificates from a trusted CA, then you can ignore this section. If your Connection Servers are using self-signed certificates or have a certificate from an untrusted CA, locate the Thumbprint information stored within the certificate. Each Thumbprint will need to be defined during installation so that the Access Point can trust connections to the View Connection Server.
The Thumbprint can be found by opening the certificate on the Connection Server and looking at the Details tab for the Thumbprint information.

Figure 65: Certificate Thumbprint
Firewall Rules

The tables below list the firewall rules that should be considered when deploying Access Point within a DMZ. Not all ports are required, but functionality will be reduced if all the ports are not opened.

### Table 21: External Firewall Rules

<table>
<thead>
<tr>
<th>SOURCE</th>
<th>PROTOCOL</th>
<th>PORT</th>
<th>DESTINATION</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>TCP</td>
<td>443</td>
<td>Access Point</td>
<td>443 (HTTPS)</td>
</tr>
<tr>
<td>Any</td>
<td>TCP/UDP</td>
<td>8443</td>
<td>Access Point</td>
<td>Blast – UDP for Blast Port Sharing</td>
</tr>
<tr>
<td>Any</td>
<td>TCP</td>
<td>443</td>
<td>Access Point 2.5 only</td>
<td>Blast Port Sharing – TCP only</td>
</tr>
<tr>
<td>Any</td>
<td>TCP</td>
<td>80</td>
<td>Access Point</td>
<td>External client redirected to 443</td>
</tr>
<tr>
<td>Access Point</td>
<td>TCP/UDP</td>
<td>4172</td>
<td>Access Point</td>
<td>PCoIP</td>
</tr>
<tr>
<td>Access Point</td>
<td>UDP</td>
<td>4172</td>
<td>Horizon Client</td>
<td>PCoIP</td>
</tr>
</tbody>
</table>

### Table 22: Internal Firewall Rules

<table>
<thead>
<tr>
<th>SOURCE</th>
<th>PROTOCOL</th>
<th>PORT</th>
<th>DESTINATION</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Point</td>
<td>HTTPS</td>
<td>443</td>
<td>View Connection server or Load Balancers</td>
<td></td>
</tr>
<tr>
<td>Access Point</td>
<td>RDP</td>
<td>3389</td>
<td>Remote Desktop</td>
<td>Used to exchange RDP data</td>
</tr>
<tr>
<td>Access Point</td>
<td>MMR/CDR</td>
<td>9427</td>
<td>Remote Desktop</td>
<td>Multimedia and Client Drive Mapping</td>
</tr>
<tr>
<td>Access Point</td>
<td>PCoIP</td>
<td>4172</td>
<td>Remote Desktop or Application</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td>Remote Desktop/Application</td>
<td>PCoIP</td>
<td>4172</td>
<td>Access Point</td>
<td>^</td>
</tr>
<tr>
<td>Access Point</td>
<td>TCP</td>
<td>32111</td>
<td>Remote Desktop</td>
<td>USB Redirection</td>
</tr>
<tr>
<td>Access Point</td>
<td>Blast</td>
<td>22443</td>
<td>Remote Desktop</td>
<td>Blast uses 22443 TCP/UDP to exchange Blast Extreme data</td>
</tr>
<tr>
<td>Access Point</td>
<td>HTTPS</td>
<td>22443</td>
<td>Remote Desktop</td>
<td>If you use HTML access, AP connects to remote desktop on HTTPS 22443 communicating with BLAST Agent</td>
</tr>
<tr>
<td>Access Point</td>
<td>RSA SecurID</td>
<td>5500</td>
<td>RSA Server</td>
<td>Used by AP to communicate with SecurID</td>
</tr>
<tr>
<td>Access Point</td>
<td>UDP</td>
<td>514</td>
<td>Syslog Server</td>
<td></td>
</tr>
<tr>
<td>Any</td>
<td>HTTPS</td>
<td>9443</td>
<td>Access Point</td>
<td>REST API Traffic</td>
</tr>
</tbody>
</table>
Deployment
To meet with the design requirements, Access Point will be deployed based on the key decisions made. For clarity the key decision points are summarized here:

<table>
<thead>
<tr>
<th>DESIGN</th>
<th>DESIGN DECISION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Versions</td>
<td>Both Access Point 2.5 and 2.6 will be used to satisfy the requirements of the design to support connections to VMware Identity Manager and Horizon.</td>
</tr>
<tr>
<td>Scalability</td>
<td>2 x Access Points 2.5 (n+1) will be deployed to satisfy the requirement of 2,000 sessions and high availability.</td>
</tr>
<tr>
<td>Deployment method</td>
<td>The APDeploy method will be used as it will satisfy most deployment scenarios and does not require the IT administrator to enter complex OVF Tool commands to complete the deployment.</td>
</tr>
<tr>
<td>Load balancing</td>
<td>A load balancer will be placed both in front of the Access Point and between the Access Point and the Connection Servers. SSL ID will be used as the method to support session persistence / affinity. For specific details on load balancing settings see the Load Balancing and External Access section.</td>
</tr>
<tr>
<td>Authentication</td>
<td>For access to VMware Identity Manager, Access Point 2.6 will be used and configured as a reverse proxy. User connections will then be authenticated at VMware Identity Manager and True SSO will be configured. As connections to View Connection Servers will be authenticated at VMware Identity Manager and True SSO is used, the Access Point 2.5 must be configured with pass-through authentication, otherwise True SSO would fail.</td>
</tr>
<tr>
<td>Network architecture</td>
<td>To meet with the requirements of separating Internet traffic from management and backend data, the Access Point will be deployed in a dual NIC mode.</td>
</tr>
</tbody>
</table>

Table 23: Access Point Deployment Decisions

Deployment Steps
Listed below is a high-level list of steps that should be followed in order to ensure a successful deployment.
1. Download the Access Point OVF file from VMware.com.
2. Download and install the OVF Tool onto a Windows desktop (virtual or physical).
4. Copy the APDeploy and associated files into a directory on the Windows desktop.
5. Edit the sample INI file, replacing the settings as required.
6. Run the script.
7. Validate the installation has completed.
Appendix E: Building a Master VM Template

Build a clean VM. Do not convert (P2V) or reuse an image that was designed for physical PCs. Optimize, optimize...optimize!

Build a New VM and Tune Hardware

Start by building a new virtual machine and tuning the virtual hardware.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>SPECIFICATIONS</th>
</tr>
</thead>
</table>
| CPU and memory        | • Size appropriately  
                          • 2 vCPU and 4 GB RAM typical for Windows 10                             |
| SCSI disk controller  | LSI Logic SAS                                                               |
| Network card          | VMXNET3                                                                    |
| Video card            | • Set video memory to auto-detect and let Horizon handle.  
                          • Enable 3D support if required.                                         |
| CD-ROM                | • Set to Client Device and Not to Connect at power on (delete if not needed).|
| Floppy drive          | Delete                                                                     |
| COM and LPT           | Disable unused ports, such as COM1, COM2, and LPT (delete if not needed).   |
| Hotplug               | • Follow instructions in Disabling the HotAdd/HotPlug capability in ESXi 5.x and ESXi/ESX 4.x virtual machines. This removes certain critical devices from the Remove Hardware system tray icon such as virtual disk and network card.  
                          • devices.hotplug=false                                                   |
| Time sync             | In VMware Tools™ settings, enable Synchronize guest time with host.         |

Table 24: VM Tuning Specifications

Note: When removing hardware such as the floppy drive this should be deleted from the VM configuration and also disabled in the BIOS of the VM.

vGPU Specifications

Follow additional steps in chapter 10 of the NVIDIA deployment guide to add the required virtual hardware and driver for GPU-enabled desktops.

Tune Windows

After installing Windows there are lots of optimizations that can be made to reduce the resources needed and to improve the user experience. Follow the Windows Optimization Guide for full details on tuning and optimizing Windows for use in a virtual environment. The paper also provides details on how to use the VMware OS Optimization Tool.

As we are using VMware Identity Manager in conjunction with Horizon desktops, we should join the virtual machine to the Active Directory domain that will be used for the resultant instant- or linked-clone desktops.
## Task 1: Adjust display Properties

Choose a basic theme.
- Set the background to a solid color.
- Set the screen saver to **None**.
- Set visual effects to **Adjust for best performance**.
- Disable Aero if not required.
- Verify that full hardware acceleration is enabled.

## Task 2: Power policy

- Select a high-performance power option.
- Change plan so that display never turns off.
  - Windows 8 and above
- Do not specify a sleep timer, standby, hibernation, or any other power option that could make the desktop unreachable.
- Disable hibernation = `powercfg.exe /h`

## Task 3: Restore points

- Remove or minimize system restore points.
- Turn off system protection on C: \.

## Task 4: Sound scheme

- Set the sound scheme to **No Sounds**.

## Task 5: Windows Media Player

- Open Windows Media Player and use the default settings.

## Task 6: Networking

- Disable IPv6 if not needed.
- De-select **Link-layer Topology Discovery Mapper I/O Driver**
- Refer to [Configure the Windows Firewall Service to Restart After Failures](Setting Up Desktop and Application Pools in View) for more information.
  - Windows 2012 R2, 8.1, and 10 only

## Task 7: Active setup

Improve login time for floating desktops by disabling Windows Active Setup components. Refer to the KB article [Improving log in time for floating desktops on DaaS and Horizon View](Improving log in time for floating desktops on DaaS and Horizon View).

## Task 8: Updates

- Turn off automatic updates.

## Task 9: Disk defragmenter

- Windows schedules some services to run by default, e.g. disk defragmenter.
- These services and tasks can cause OS disks to expand every few hours, even when idle.
- Services that affect disk expansion also generate additional IOPS.
- Disable unnecessary services such as disk defragmenter

## Task 10: Indexing service

- Unless there are user requirements for it, disable the Indexing Service component.

### Table 25: Windows Tuning Specifications

Evaluate the effects before implementing a change. For example, Indexing Service may be required if users expect (and you want to allow) them to be able to search Outlook.
Some items to consider tuning include:

<table>
<thead>
<tr>
<th>COMMON SERVICES TO DISABLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Hibernation</td>
</tr>
<tr>
<td>Windows Scheduled Disk Defragmentation</td>
</tr>
<tr>
<td>Windows Update service</td>
</tr>
<tr>
<td>Windows Diagnostic Policy service</td>
</tr>
<tr>
<td>Prefetch and Superfetch</td>
</tr>
<tr>
<td>Windows Registry Backup</td>
</tr>
<tr>
<td>System Restore</td>
</tr>
<tr>
<td>Windows Defender</td>
</tr>
<tr>
<td>Microsoft Feeds Synchronization Task</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WINDOWS 10 APPS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>News / Sports / Weather</strong></td>
</tr>
<tr>
<td>• BingFinance</td>
</tr>
<tr>
<td>• BingNews</td>
</tr>
<tr>
<td>• BingSports</td>
</tr>
<tr>
<td>• BingWeather</td>
</tr>
<tr>
<td><strong>Help / Get</strong></td>
</tr>
<tr>
<td>• Getstarted</td>
</tr>
<tr>
<td>• SkypeApp</td>
</tr>
<tr>
<td>• MicrosoftOfficeHub</td>
</tr>
<tr>
<td><strong>Games / Xbox</strong></td>
</tr>
<tr>
<td>• XboxApp</td>
</tr>
<tr>
<td>• ZuneMusic</td>
</tr>
<tr>
<td>• ZuneVideo</td>
</tr>
<tr>
<td>• MicrosoftSolitaireCollection</td>
</tr>
<tr>
<td><strong>Others</strong></td>
</tr>
<tr>
<td>• 3DBuilder</td>
</tr>
<tr>
<td>• People</td>
</tr>
<tr>
<td>• Windows.Photos</td>
</tr>
<tr>
<td>• WindowsAlarms</td>
</tr>
<tr>
<td>• WindowsCalculator</td>
</tr>
<tr>
<td>• WindowsCamera</td>
</tr>
<tr>
<td>• WindowsMaps</td>
</tr>
<tr>
<td>• WindowsPhone</td>
</tr>
<tr>
<td>• WindowsSoundRecorder</td>
</tr>
<tr>
<td>• Office.OneNote</td>
</tr>
<tr>
<td>• WindowsStore</td>
</tr>
<tr>
<td>• Appconnector</td>
</tr>
</tbody>
</table>

Table 26: Common Windows Optimizations

As with any tuning, consider the balance between resource consumption and user experience before removing applications, for example, WindowsCalculator.
VMware OS Optimization Tool
To help in optimizing Windows 7, 8, 2008, and 2012, VMware has released the OS Optimization Tool. This tool allows you to analyze and then optimize an installation of Windows. It includes customizable templates to enable or disable Windows system services and features per VMware recommendations and recommended best practices.

The OS Optimization Tool provides the following functionality:
• Local analyze / optimize
• Remote analyze
• Optimization history and rollback
• Managing templates

RDSH Specifications
For Windows 2012 R2 servers that will become RDS hosts, you must install the required roles. In Server Manager add the following roles and features:
• Role = Remote Desktop Services > Remote Desktop Session Host
• Feature = User Interfaces and Infrastructure > Desktop Experience
We will define the licensing for RDSH via a group policy in Appendix F.

Applications
While our primary application-delivery mechanism is App Volumes, it may be desirable to install select applications into the master VM so that all clones get those applications in their base disk.

Many applications have integrated auto-update functionality. These applications should be installed and updated, and then the auto-update functionality should be turned off or disabled to prevent the clones updating individually.

Antivirus Best Practices (If not Using Endpoint Antivirus)
Follow best practices for antivirus for virtual desktops and RDS hosts as detailed in Antivirus Considerations in a VMware Horizon 7 Environment.

Install VMware Tools and Agents
When preparing a virtual machine for use as a virtual desktop or as an RDS host, the relevant product agents must be installed. The installation order is important and if one is updated all subsequent agents should be removed and updated to maintain the installation order.

Agent Install Order
1. vSphere VMTools
2. Horizon Agent
3. User Environment Manager FlexEngine
4. VMware Identity Manager Client
5. App Volumes Agent
VMware Identity Manager Client
This will enable virtual desktops to launch application types such as ThinApps that are delivered through VMware Identity Manager. Install from the command line and specify the following parameters:

```
/v WORKSPACE_SERVER="https://workspace.vmweuc.com"
INSTALL_MODE=RUN_FROM_SHARE
```

**Note:** Replace the WORKSPACE_SERVER URL with your own for VMware Identity Manager.

Horizon Agent
1. Select IPv4 or IPv6.
   - Agent, Client, and Connection Servers must all use the same IP version.
2. Remember to select additional features, if required:
   - USB Redirection
   - Scanner Redirection
   - Smartcard Redirection
   - Serial Port Redirection
   - Flash Redirection
3. Select a cloning technology. Choose either **Instant Clone** or **View Composer Linked Clone**.
4. Enable Remote Desktop, if not already done.
   - Give suitable security group access (e.g., Domain Users).
   - Add Firewall exceptions if enabling manually.

Finalize
The last step before we can use this VM is to clean up and take a vSphere snapshot.

1. Cleanup
   - Delete all event logs.
   - Delete all hidden update folders in C:\Windows
     - Example: $NtUninstallKB893756$ (except $hf_mig$).
   - Turn off disk performance counters (diskperf -n).
   - Delete contents of C:\Windows\Temp\.
   - Run Disk Cleanup to remove temporary files, empty the Recycle Bin, and remove other unneeded files.
   - Run Disk Defragmenter (you may have to temporarily re-enable the Optimize drives service).
   - Flush DNS and release the DHCP IP Address lease.
2. Shutdown
   - Disconnect the CD-ROM and make sure no ISO is configured in the virtual machine.
3. Snapshot
Appendix F: Group Policies

OU GPO Best Practices
- Re-use GPOs.
- Separate OUs for users and computers.
- Ensure that each GPO is enabled or disabled for Computer and User settings.
- Group similar settings into one GPO.
- Monolithic and functional GPO.
  - Monolithic GPOs contain settings for many different areas and are quite large.
    - All settings in one place; should be used for generic settings that apply to all users or computers.
  - Functional GPOs contain a limited set of settings for a specific area.
    - Smaller GPOs that facilitate settings being defined for particular users or VMs.
- Link the GPOs to the OU structure (or site), and then use Security Groups to selectively apply these GPOs to particular users or computers.
- Use loopback replace to ensure that only settings for the VM's OU are applied to the session.

Below is a list of group policy settings that would typically be applied (this is not an exhaustive list). Most other settings will be applied through User Environment policies. As part of the download of Horizon there is a View GPO Bundle ZIP file that contains a set of group policy templates to assist in defining these and other GPO settings.

Common GPO Settings

<table>
<thead>
<tr>
<th>SETTING</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Configuration/Policies/Administrative Templates/System/Group Policy/</td>
<td></td>
</tr>
<tr>
<td>Configure user Group Policy loopback processing mode</td>
<td>Enabled</td>
</tr>
<tr>
<td>Configure Logon Script Delay</td>
<td>Disabled</td>
</tr>
<tr>
<td>Computer Configuration/Policies/Administrative Templates/System/Logon/</td>
<td></td>
</tr>
<tr>
<td>Show first sign-in animation</td>
<td>Disabled</td>
</tr>
<tr>
<td>Always wait for the network at computer startup and logon</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Table 27: Common GPO Settings

Desktop

<table>
<thead>
<tr>
<th>SETTING</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Configuration/Policies/Administrative Templates/System/User Profiles/</td>
<td></td>
</tr>
<tr>
<td>Set roaming profile path for all users logging onto this computer</td>
<td>Enabled</td>
</tr>
<tr>
<td>(Specify the mandatory network share path).</td>
<td></td>
</tr>
</tbody>
</table>

Table 28: Desktop Settings
RDS Host OU Level

When we are using RDS hosts, there are group policy settings that must be applied as per *Using Remote Desktop Services Group Policies* in *Setting Up Desktop and Application Pools in View*. To define these, we first need to copy the `vmware_rdsh.admx` and `vmware_rdsh_server.admx` files and the `en-US` folder (from the View GPO Bundle ZIP) to the `C:\Windows\PolicyDefinitions` folder on the Active Directory Domain Controller you are creating GPOs on.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computer Configuration/Policies/Administrative Templates/Windows Components/Horizon View RDSH Services/Remote Desktop Session Host/Licensing/</strong></td>
<td></td>
</tr>
<tr>
<td>Use the specified Remote Desktop license servers</td>
<td>Enabled (List license servers)</td>
</tr>
<tr>
<td>Hide notifications about RD Licensing problems that affect the RD Session Host server</td>
<td>Enabled</td>
</tr>
<tr>
<td>Set the Remote Desktop licensing mode</td>
<td>Enabled (Match mode of licenses)</td>
</tr>
<tr>
<td><strong>Computer Configuration/Policies/Administrative Templates/Windows Components/Horizon View RDSH Services/Remote Desktop Session Host/Profiles/</strong></td>
<td></td>
</tr>
<tr>
<td>Use mandatory profiles on the RD Session Host server</td>
<td>Enabled</td>
</tr>
<tr>
<td>Set path for Remote Desktop Services Roaming User Profile</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Computer Configuration/Policies/Administrative Templates/Windows Components/Horizon View RDSH Services/Remote Desktop Session Host/Device and Resource Redirection/</strong></td>
<td></td>
</tr>
<tr>
<td>Allow time zone redirection</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Table 29: RDS Host Settings
User Configuration Settings
There are various settings that can be used to optimize the user experience while protecting the system. Below are a few basic, initial settings that would normally be applied. Note that as these are user settings, this will require the use of the loopback processing setting.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Configuration/ Policies/Administrative Templates/Start Menu and Taskbar/</td>
<td></td>
</tr>
<tr>
<td>Remove and prevent access to the Shut Down, Restart, Sleep and Hibernate commands</td>
<td>Enabled</td>
</tr>
<tr>
<td>Add Logoff to the Start Menu</td>
<td>Enabled</td>
</tr>
<tr>
<td>User Configuration/ Policies/Administrative Templates/Windows Components/Internet Explorer/</td>
<td></td>
</tr>
<tr>
<td>Automatically activate newly installed add-ons</td>
<td>Enabled</td>
</tr>
<tr>
<td>User Configuration/ Policies/Administrative Templates/Windows Components/Internet Explorer/Internet Control Panel/ Security Page/</td>
<td></td>
</tr>
<tr>
<td>Site to Zone Assignment List</td>
<td>Enabled</td>
</tr>
<tr>
<td>• Zone assignments</td>
<td></td>
</tr>
<tr>
<td>&lt;URL of Identity Manager&gt; 1</td>
<td>Example: <a href="https://workspace.vmweuc.com">https://workspace.vmweuc.com</a> 1</td>
</tr>
<tr>
<td>&lt;URL of ThinApp Share&gt; 1</td>
<td>Example: \vmweuc.com\files\ 1</td>
</tr>
</tbody>
</table>

Table 30: User Configuration Settings

User Environment Manager – Group Policy Settings
The following instructions are excerpted from the User Environment Manager Administrator’s Guide. Refer to this guide for more details on Group Policy settings.

1. Copy the VMware UEM.admx and VMware UEM FlexEngine.admx ADMX templates (and their corresponding ADML files) from the download package to the ADMX location as described in the Managing Group Policy ADMX Files Step-by-Step Guide on the Microsoft Web site.
2. Open the Group Policy Management Console.
   a. Create a new Group Policy Object (GPO) or select an existing GPO that is applied to the users for which you want to configure FlexEngine.
   b. To open the Group Policy Management Editor, right-click the selected GPO and then click Edit.
3. The FlexEngine ADMX template is available under User Configuration\ Administrative Templates\VMware UEM\FlexEngine.
Configure the appropriate User Environment Manager Group Policy settings. At a minimum, the following must be set:

- **Flex config Files** – Location of the User Environment Manager configuration share
- **Profile archives** – Location of the User Environment Manager user profile share
- **Run FlexEngine as a Group Policy Extension** – This is what enables the FlexEngine agent. Alternatively, it can be called from a logon script.
- **A logoff script** must be defined for User Environment Manager to save settings on logoff. The syntax of the logoff script should be:

  "C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe" -s

<table>
<thead>
<tr>
<th>SETTING</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Configuration\Policies\Administrative Templates\VMware UEM\FlexEngine</strong></td>
<td></td>
</tr>
<tr>
<td>Flex config files</td>
<td>Enabled (Enter User Environment Manager configuration share)</td>
</tr>
<tr>
<td>Profile archives</td>
<td>Enabled (Location of the User Environment Manager user profile share)</td>
</tr>
<tr>
<td>Run FlexEngine as Group Policy Extension</td>
<td>Enabled</td>
</tr>
<tr>
<td>*<em>User Configuration\Policies\Windows Settings\Scripts*</em></td>
<td></td>
</tr>
<tr>
<td>Logoff</td>
<td>Script Name = C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe</td>
</tr>
<tr>
<td></td>
<td>Script Parameters = -s</td>
</tr>
</tbody>
</table>

*Table 31: User Environment Manager Group Policy Settings*
Appendix G: Smart Policies

Below are some simple sample Horizon policies. Adapt and embellish to suit the use case and environment.

The following policies are defined in the User Environment Manager console.

<table>
<thead>
<tr>
<th>HORIZON POLICY – EXTERNAL</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB redirection</td>
<td>Disable</td>
</tr>
<tr>
<td>Printing</td>
<td>Disable</td>
</tr>
<tr>
<td>Clipboard</td>
<td>Disable</td>
</tr>
<tr>
<td>Client drive redirection</td>
<td>Disable</td>
</tr>
<tr>
<td>PCoIP profile</td>
<td>Not set</td>
</tr>
<tr>
<td>Conditions</td>
<td>Horizon Client property ‘Client location’ is equal to <strong>External</strong></td>
</tr>
</tbody>
</table>

Table 32: External Horizon Smart Policies

<table>
<thead>
<tr>
<th>HORIZON POLICY – INTERNAL</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB redirection</td>
<td>Enable</td>
</tr>
<tr>
<td>Printing</td>
<td>Enable</td>
</tr>
<tr>
<td>Clipboard</td>
<td>Enable</td>
</tr>
<tr>
<td>Client drive redirection</td>
<td>Enable</td>
</tr>
<tr>
<td>PCoIP profile</td>
<td>Not set</td>
</tr>
<tr>
<td>Conditions</td>
<td>Horizon Client property ‘Client location’ is equal to <strong>Internal</strong></td>
</tr>
</tbody>
</table>

Table 33: Internal Horizon Smart Policies
### HORIZON POLICY – CONTRACTOR

<table>
<thead>
<tr>
<th>HORIZON POLICY SETTING</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB redirection</td>
<td>Disable</td>
</tr>
<tr>
<td>Printing</td>
<td>Enable</td>
</tr>
<tr>
<td>Clipboard</td>
<td>Disable</td>
</tr>
<tr>
<td>Client drive redirection</td>
<td>Disable</td>
</tr>
<tr>
<td>PCoIP profile</td>
<td>Not set</td>
</tr>
<tr>
<td>Conditions</td>
<td>Horizon Client property ‘Client location’ is equal to <strong>Internal</strong> and User is a member of group ‘Contractor’</td>
</tr>
</tbody>
</table>

**Table 34: zContractor Horizon Smart Policies**

You should also configure a triggered task to ensure that Smart Policies are reevaluated every time a user reconnects to a session so the user gets the appropriate policy applied.

### TRIGGERED TASK – HORIZON POLICIES

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Reconnect Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Use Environment refresh</td>
</tr>
<tr>
<td>Refresh</td>
<td>Horizon Policies</td>
</tr>
</tbody>
</table>

**Table 35: Triggered Task Horizon Smart Policies**

### FOLDER REDIRECTION

<table>
<thead>
<tr>
<th>Folder Redirection Settings</th>
<th>Users Home drive share using <code>username</code> variable Example: <code>\vmweuc.com\share\Users\%username%</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote path</td>
<td>Documents</td>
</tr>
<tr>
<td>Folders to redirect</td>
<td>Note: Depending on your needs, you may also want to select Downloads, Music, Pictures, and Videos. Be aware that this will place a larger load on your file servers requiring more space and performance.</td>
</tr>
<tr>
<td>Conditions</td>
<td>None</td>
</tr>
</tbody>
</table>

**Table 36: Folder Redirection Horizon Smart Policies**
Appendix H: Mandatory Profile

Create the Mandatory Profile

<table>
<thead>
<tr>
<th>STEP</th>
<th>TASK</th>
</tr>
</thead>
</table>
| 1    | • From source Windows 10 or Windows 2012 R2 machine, browse to C:\Users\.
   • If the Default profile folder is not visible, change your default folder view options. (Show hidden files, folders, and drives, and uncheck **Hide protected operating system files**). |
| 2    | • Copy the C:\Users\Default folder to your Mandatory profile network share.
   • Make sure the share is set for Everyone to have a minimum of Read access. |
| 3    | • In the network copy of the Default folder you made, rename NTUSER.DAT to NTUSER.MAN.
   • Delete NTUSER.DAT.LOG1 and NTUSER.DAT.LOG2. |
| 4    | • Run regedit: Click **hkey_users** and load Hive. Browse to ntuser.man.
   • Give your hive a name to help you identify it while you are editing it.
   • Set the correct permissions on the hive.
   • Remove Profile User and administrators.
   • Add in Full Control for authenticated users. |
| 5    | • Rename the Default folder to Default:V5 (see below).
   • Change the properties so it is not hidden. |

**Note:** The extension you use on the profile folder (for example, the .V5) depends on the Windows version.

<table>
<thead>
<tr>
<th>PROFILE EXTENSION</th>
<th>WINDOWS VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Windows XP</td>
</tr>
<tr>
<td>.V2</td>
<td>Windows 7</td>
</tr>
<tr>
<td></td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>.V3</td>
<td>Windows 8</td>
</tr>
<tr>
<td>.V4</td>
<td>Windows 8.1</td>
</tr>
<tr>
<td>.V5</td>
<td>Windows 10</td>
</tr>
</tbody>
</table>

*Table 37: Profile Folder Extensions*
Configure Active Directory Group Policies for Mandatory Profile

<table>
<thead>
<tr>
<th>STEP</th>
<th>TASK</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>• Edit or create a Group Policy on the OU that will contain our virtual desktop objects.</td>
</tr>
</tbody>
</table>
| 2    | • Enable *Always wait for the network at computer startup and logon*.  
     | • Navigate to **Computer Configuration > Policies > Administrative Templates > System > Logon**.  
     | • Always wait for the network at computer startup and logon = Enabled. |
| 3    | • Enable the Mandatory profile.  
     | **For virtual desktops**  
     | • Navigate to **Computer Configuration > Policies > Administrative Templates > System > User Profiles**.  
     | • Set roaming profile path for all users logging into this computer = Enabled.  
     | • Specify the mandatory network share path.  
     | • Example: `\server\share\Default` (Do not include the `.V5` in the folder path.)  
     | **For RDS hosts**  
     | • Navigate to **Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Profiles**.  
     | • Use mandatory profiles on the RD Session Host server = Enabled.  
     | • Set path for Remote Desktop Services Roaming User Profile = Enabled.  
     | • Specify the mandatory network share path as above. |

When using mandatory profiles, we also use folder redirection. This will be configured in the User Environment policy.
Appendix I: VMware App Volumes Install and Configure

Prerequisites

The prerequisites are covered in more detail in the System Requirements section of the VMware App Volumes Users Guide. Below is the list of prerequisites:

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
<td>VMware vSphere 6.0u1a or later (Instant Clone Technology support)</td>
</tr>
<tr>
<td>Virtual Center</td>
<td>VMware vCenter 6.0u1a or later (Instant Clone Technology support)</td>
</tr>
<tr>
<td>App Volumes Manager</td>
<td>Windows Server 2008 R2 or Windows Server 2012 R2</td>
</tr>
<tr>
<td>Active Directory</td>
<td>2003 Functional Level or Above</td>
</tr>
<tr>
<td>SQL Server</td>
<td>SQL Server 2008 R2 or SQL Server 2012</td>
</tr>
<tr>
<td>App Volumes Agent</td>
<td>Windows 7, Windows 8.1, or Windows 10</td>
</tr>
</tbody>
</table>

Table 38: App Volumes Installation Prerequisites

Install

Again, refer to the VMware App Volumes Users Guide for installation procedures. This document will outline the initial setup and configuration process.

Next Steps

After installation you will need to do the following to start using App Volumes:

• Complete the App Volumes Initial Configuration Wizard (https://avmanager).
• To optimize the speed of AppStack attachments, it is recommended that mount on host is set. This requires user accounts with same username and password on all resource vSphere hosts.
• Install the App Volumes Agent on one or more clients.
  – Point the agent to the App Volumes Manager address (load-balanced address).
• Select a clean provisioning system, install the App Volumes Agent, and provision an AppStack. See Working with AppStacks in the VMware App Volumes User Guide for instructions.
• Assign the AppStack to a test user and verify it is connecting properly.
• Assign a writable volume to a test user and verify it is connecting properly.
Appendix J: Printing

The virtual printing feature allows end users to use local or network printers from a Horizon 7 desktop or RDS session without requiring that additional print drivers be installed in the Horizon 7 desktop or RDS host. For each printer available through this feature, you can set preferences for data compression, print quality, double-sided printing, color, and so on.

The virtual printing feature allows Horizon Client users to transparently use local or network printers from within their remote client systems, yet removes the requirement for installing proprietary printer drivers on each Horizon-managed virtual desktop.

USB Redirection and Printing

To send print jobs to a USB printer, users can use USB redirection. In a Horizon 7 environment, virtual printers and redirected USB printers can work together without conflict. A USB printer is a printer that is attached to a USB port on the local client system.

You can use USB redirection to attach a USB printer to a virtual USB port in the Horizon 7 desktop or RDS session as long as the required driver is also installed on the Horizon 7 desktop.

If you use USB redirection, the printer is no longer attached to the physical USB port on the client. This is why the USB printer does not appear in the list of local printers that the virtual printing feature displays. This also means that you can print to the USB printer from the Horizon 7 desktop or RDS session, but not from the local client machine.

On Windows clients, you can alternatively use virtual printing to send print jobs to a USB printer. If you use virtual printing you can print to the USB printer from both the Horizon 7 desktop and the local client, and you do not need to install print drivers on the Horizon 7 desktop or RDS host.

Location-Based Printing Overview

Location-based printing capabilities with Horizon 7 allow IT organizations to map Horizon 7 desktops to the printer that is closest to the endpoint client device.

For example, as a doctor moves from room to room in a hospital, each time the doctor prints a document, the print job is sent to the nearest printer. For sites that do not want to use virtual printing, a GPO setting can be applied through the Horizon Client group policy template, or through virtual channel or Windows Service management through GPO.

Location-based printing allows virtual desktops to be automatically mapped to network printers based on rules specified in the ThinPrint component TPVMGPoACmap.dll that appears as a Group Policy local computer setting when registered. The ThinPrint GPO rules apply one printer per rule. If multiple printers are to be mapped to the same set of virtual desktops, then multiple rules are required.

The ThinPrint AutoConnect component included with VMware Tools will rebuild the virtual desktop’s printer list based on these rules at login or reconnect from a disconnected Horizon 7 session.

The printer-mapping component can map printers to virtual desktops based on the following rules:

- Client-access device IP address range.
- Client access device name.
- Client-access device MAC address.
- Active Directory user name of logged in user.
- Active Directory group membership of the logged in user.

VMware recommends using the IP address range of the client-access device to map local network printers to the virtual desktops being used, if this feature will be used.
Printing Environment
The following provides a high-level overview of how printing is typically used in an environment:

• **Network printing** – At the main campus and remote offices, users connect to a dedicated print server configured with printer shares. Users can select their printer from a portal-based map or configure them through Active Directory (printers are filtered based on Active Directory sites or services).

• **Direct IP printing** – There are use cases where printer connections are made directly to the IP address of the printer, bypassing the network printing shares on file servers or centrally managed print servers.

• **Local printers** – Users may also have a locally attached printer to their current endpoint or PC. These connections are typically USB connections to the endpoint. Other types of printer connections are unknown.

**Design Decision:** To provide a unified approach for installing and managing printers in the virtual desktops, User Environment Manager will be used to map printers to users.

For remote or untrusted devices using Horizon 7 Windows-based clients, printers will be automatically brought into the virtual desktop using ThinPrint virtual printing technologies. No drivers will need to be installed on the local Windows endpoint. Other thin clients, zero clients, or mobile devices will use the printer map to select their on-premises printer.

Non-Windows devices that do not use ThinPrint and have local printers attached to them can use USB redirection for printing, if necessary.