VMware Workspace ONE and VMware Horizon Reference Architecture

VMware Workspace ONE UEM
VMware Identity Manager
VMware Workspace ONE Intelligence
VMware Horizon 7
VMware Horizon Cloud Service on Microsoft Azure
VMware App Volumes
VMware User Environment Manager
VMware Unified Access Gateway
Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>7</td>
</tr>
<tr>
<td>Workspace ONE and Horizon Solution Overview</td>
<td>9</td>
</tr>
<tr>
<td>VMware Reference Architectures</td>
<td>9</td>
</tr>
<tr>
<td>Design Tools</td>
<td>9</td>
</tr>
<tr>
<td>Design Decisions</td>
<td>10</td>
</tr>
<tr>
<td>Audience</td>
<td>10</td>
</tr>
<tr>
<td>Workspace ONE Features</td>
<td>10</td>
</tr>
<tr>
<td>VMware Workspace ONE Intelligence</td>
<td>13</td>
</tr>
<tr>
<td>Horizon 7 Platform</td>
<td>13</td>
</tr>
<tr>
<td>Horizon Cloud Service on Microsoft Azure Platform</td>
<td>15</td>
</tr>
<tr>
<td>Reference Architecture Design Methodology</td>
<td>15</td>
</tr>
<tr>
<td>Business Drivers and Use Cases</td>
<td>17</td>
</tr>
<tr>
<td>Addressing Business Requirements</td>
<td>17</td>
</tr>
<tr>
<td>Multi-site Deployment Business Drivers</td>
<td>20</td>
</tr>
<tr>
<td>Use Cases</td>
<td>22</td>
</tr>
<tr>
<td>Service Definitions</td>
<td>28</td>
</tr>
<tr>
<td>Workspace ONE Use Case Services</td>
<td>28</td>
</tr>
<tr>
<td>Horizon 7 Use Case Services</td>
<td>32</td>
</tr>
<tr>
<td>Horizon Cloud Service on Microsoft Azure Use Case Services</td>
<td>40</td>
</tr>
<tr>
<td>Recovery Services</td>
<td>43</td>
</tr>
<tr>
<td>Architectural Overview</td>
<td>53</td>
</tr>
<tr>
<td>Workspace ONE Logical Architecture</td>
<td>53</td>
</tr>
<tr>
<td>Cloud-Based Logical Architecture</td>
<td>53</td>
</tr>
<tr>
<td>On-Premises Logical Architecture</td>
<td>54</td>
</tr>
<tr>
<td>Common Components</td>
<td>55</td>
</tr>
<tr>
<td>Horizon Virtual Desktops and Published Applications</td>
<td>56</td>
</tr>
<tr>
<td>General Multi-site Best Practices</td>
<td>57</td>
</tr>
<tr>
<td>Component Design: Workspace ONE UEM Architecture</td>
<td>59</td>
</tr>
<tr>
<td>Cloud-based Architecture</td>
<td>59</td>
</tr>
<tr>
<td>AirWatch Cloud Connector</td>
<td>63</td>
</tr>
<tr>
<td>On-Premises Architecture</td>
<td>64</td>
</tr>
<tr>
<td>Integration with VMware Identity Manager</td>
<td>76</td>
</tr>
<tr>
<td>Resource Types</td>
<td>76</td>
</tr>
<tr>
<td>Conditional Access</td>
<td>78</td>
</tr>
<tr>
<td>Standalone MAM and Adaptive Management</td>
<td>81</td>
</tr>
<tr>
<td>Mobile Single Sign-On</td>
<td>83</td>
</tr>
<tr>
<td>Email Integration</td>
<td>84</td>
</tr>
<tr>
<td>Content Integration</td>
<td>88</td>
</tr>
<tr>
<td>VMware Tunnel</td>
<td>91</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>93</td>
</tr>
<tr>
<td>Component Design: VMware Identity Manager Architecture</td>
<td>96</td>
</tr>
<tr>
<td>Cloud-Based Architecture</td>
<td>98</td>
</tr>
<tr>
<td>VMware Identity Manager Tenant Installation and Initial Configuration</td>
<td>99</td>
</tr>
<tr>
<td>VMware Identity Manager Connector</td>
<td>99</td>
</tr>
<tr>
<td>On-Premises Architecture</td>
<td>100</td>
</tr>
<tr>
<td>Integration with Workspace ONE Unified Endpoint Management (UEM)</td>
<td>114</td>
</tr>
<tr>
<td>Access to Resources Through VMware Identity Manager</td>
<td>114</td>
</tr>
</tbody>
</table>
Component Design: Workspace ONE Intelligence Architecture ........................................... 118
    Architecture Overview ........................................................................................................ 119
    Scalability and Availability .................................................................................................. 120
    Database Design .................................................................................................................. 120
    Data Sources for Workspace ONE Intelligence ...................................................................... 121
    Insights and Automation ....................................................................................................... 128
    Getting Started with Workspace ONE Intelligence ............................................................. 131

Component Design: Horizon 7 Architecture ........................................................................... 132
    Architectural Overview ....................................................................................................... 132
    Horizon 7 Pod and Block ...................................................................................................... 137
    Scalability and Availability .................................................................................................. 139
    Load Balancing of Connection Servers ................................................................................ 142
    External Access .................................................................................................................... 143
    Authentication ...................................................................................................................... 144
    True SSO .............................................................................................................................. 145
    Scaled Single-Site Architecture .......................................................................................... 148
    Multi-site Architecture ........................................................................................................ 149
    Virtual Machine Build ......................................................................................................... 154
    Physical Hosting ................................................................................................................... 154
    Display Protocol .................................................................................................................. 154
    VMware vRealize Operations for Horizon ........................................................................... 155

Component Design: Horizon Cloud Service on Microsoft Azure ......................................... 161
    Horizon Cloud Service on Microsoft Azure Deployment Overview ....................................... 162
    Scalability and Availability .................................................................................................. 164
    Multi-site Design ................................................................................................................ 166
    Optional Components for a Horizon Cloud Service on Microsoft Azure Deployment ............ 168
    Shared Services Prerequisites .............................................................................................. 168
    Authentication ..................................................................................................................... 169
    True SSO .............................................................................................................................. 169

Component Design: App Volumes Architecture ................................................................... 172
    Architecture Overview ....................................................................................................... 173
    App Volumes in a Horizon 7 Environment ............................................................................ 177
    Scalability and Availability .................................................................................................. 177
    Load Balancing .................................................................................................................... 179
    Database Design .................................................................................................................. 180
    Storage ................................................................................................................................. 181
    AppStacks ............................................................................................................................. 183
    Writable Volumes ................................................................................................................ 190
    Recommended Practices for Master Images ......................................................................... 191
    Recommended Practices for Client Desktops ........................................................................ 191
    Recommended Security Practices for App Volumes .............................................................. 191
    Multi-site Design Using Separate Databases ...................................................................... 192
    Installation and Initial Configuration ................................................................................... 195

Component Design: User Environment Manager Architecture ......................................... 197
    User Profile Strategy .......................................................................................................... 200
    Infrastructure ....................................................................................................................... 201
    Key Design Considerations ................................................................................................. 202
    Multi-site Design ................................................................................................................ 202
    Installation ............................................................................................................................ 205
    Next Steps ........................................................................................................................... 206
Component Design: Unified Access Gateway Architecture .......................................................... 207
  Design Overview .................................................................................................................. 208
  Network Segmentation Options ....................................................................................... 215
  Authentication Options .................................................................................................... 217
  Deployment Methods ....................................................................................................... 218
  Required Deployment Information .................................................................................... 219

Environment Infrastructure Design ................................................................................. 221
  vSphere Design ................................................................................................................. 221
  vSphere Infrastructure Design for Active/Active and Active/Passive Services .......... 225
  NSX Data Center for vSphere ......................................................................................... 228
  Environment Design ....................................................................................................... 234
  Microsoft Azure Environment Infrastructure Design ..................................................... 241

Platform Integration ........................................................................................................ 244
  Workspace ONE UEM and VMware Identity Manager Integration ............................. 244
  Workspace ONE Intelligence and Workspace ONE UEM Integration ..................... 253
  Workspace ONE Intelligence and VMware Identity Manager Integration .............. 255
  Horizon 7 and VMware Identity Manager Integration ................................................. 256
  Horizon Cloud Service and VMware Identity Manager Integration ......................... 265

Service Integration Design .............................................................................................. 271
  Workspace ONE Use Case Service Integration .............................................................. 271
  Horizon 7 Use Case Service Integration ........................................................................ 284
  Horizon Cloud Use Case Service Integration ............................................................... 302
  Recovery Service Integration .......................................................................................... 311

Appendix A: VM Specifications ......................................................................................... 326
  VMware Workspace ONE UEM ...................................................................................... 326
  VMware Identity Manager .............................................................................................. 331
  VMware Workspace ONE Intelligence .......................................................................... 334
  VMware Horizon 7 .......................................................................................................... 334
  VMware App Volumes ..................................................................................................... 339
  VMware vRealize Operations ......................................................................................... 340
  VMware vSphere ............................................................................................................ 341

Appendix B: VMware Horizon Configuration ................................................................... 344
  VMware Horizon 7 Installation and Configuration ........................................................ 344
  Setting Up True SSO for Horizon 7 ................................................................................ 349
  Setting Up True SSO for Horizon Cloud Service on Microsoft Azure ....................... 356
  VMware vRealize Operations for Horizon Deployment and Configuration .............. 357
  Cloud Pod Architecture Global Entitlement Settings .................................................... 360
  Horizon Group Policies ................................................................................................... 363
  User Environment Manager Smart Policies ................................................................. 368
  Additional Configuration for User Environment Manager ............................................ 369

Appendix C: VMware Identity Manager Configuration for Multi-site Deployments .... 371
  Create a Windows Server Failover Cluster .................................................................... 372
  Configure Cluster Quorum Settings .............................................................................. 374
  Install the SQL Server ..................................................................................................... 375
  Create the VMware Identity Manager Database ......................................................... 376
  Sync the Database Account Across the Availability Group Replicas ........................ 376
  Create and Configure the Availability Group ............................................................... 377
  Create a SQL Server Maintenance Job to Back Up the Database .............................. 381
  Deploy and Set Up VMware Identity Manager Appliances ........................................ 383
  Configure Failover and Redundancy for VMware Identity Manager ........................ 386
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy and Set Up the Connectors Inside the Corporate Network</td>
<td>387</td>
</tr>
<tr>
<td>Finalize Failover Preparation</td>
<td>390</td>
</tr>
<tr>
<td>Troubleshoot Elasticsearch</td>
<td>391</td>
</tr>
<tr>
<td><strong>Appendix D: Workspace ONE UEM Configuration for Multi-site Deployments</strong></td>
<td>392</td>
</tr>
<tr>
<td>Create the Workspace ONE UEM Database</td>
<td>393</td>
</tr>
<tr>
<td>Create the Workspace ONE UEM SQL Service Account and Assign Database Owner Roles</td>
<td>394</td>
</tr>
<tr>
<td>Sync the Workspace ONE UEM Database Account Across SQL Server Availability Group Replicas</td>
<td>398</td>
</tr>
<tr>
<td>Create an Always On Availability Group for the Workspace ONE UEM Database</td>
<td>399</td>
</tr>
<tr>
<td>Set Advanced Always On Availability Group Listener Parameters for Multi-site or Multi-sub-net Failover</td>
<td>404</td>
</tr>
<tr>
<td><strong>Appendix E: App Volumes Configuration</strong></td>
<td>407</td>
</tr>
<tr>
<td>Configuration of the Non-Attachable Datastore and Storage Group</td>
<td>407</td>
</tr>
<tr>
<td>Configuration of Separate App Volumes Database Instances per Site</td>
<td>411</td>
</tr>
<tr>
<td>Next Steps: Installing and Setting Up Other App Volumes Components</td>
<td>426</td>
</tr>
<tr>
<td>Next Steps: Additional Configuration Options for Writable Volumes</td>
<td>427</td>
</tr>
<tr>
<td><strong>Appendix F: Horizon 7 Active/Passive Service Using VMware vSAN Stretched Cluster</strong></td>
<td>429</td>
</tr>
<tr>
<td>Recovery Service Definition for a vSAN Stretched Cluster Active/Passive Service</td>
<td>429</td>
</tr>
<tr>
<td>Architectural Approach for the Stretched Cluster Active/Passive Service</td>
<td>431</td>
</tr>
<tr>
<td>vsphere Infrastructure Design Using vSAN</td>
<td>431</td>
</tr>
<tr>
<td>Prerequisites and Settings for the vSAN Stretched Cluster Service</td>
<td>436</td>
</tr>
<tr>
<td>vSAN Stretched Cluster Storage Policies</td>
<td>439</td>
</tr>
<tr>
<td>Steps for Building vSAN Stretched Cluster Recovery Services</td>
<td>439</td>
</tr>
<tr>
<td>Reference Architecture Validation for the Stretched Cluster Service</td>
<td>441</td>
</tr>
<tr>
<td>Test/Recovery Plan for Active/Passive Horizon 7 Service Failover</td>
<td>442</td>
</tr>
<tr>
<td><strong>Appendix G: NSX Data Center for vSphere Configuration</strong></td>
<td>445</td>
</tr>
<tr>
<td>NSX Data Center for vSphere Installation</td>
<td>445</td>
</tr>
<tr>
<td>Post-Installation Configuration</td>
<td>445</td>
</tr>
<tr>
<td>Authors and Contributors</td>
<td>447</td>
</tr>
</tbody>
</table>
Executive Summary

Use this reference architecture as you build services to create an integrated digital workspace—one that addresses your unique business requirements and use cases. You will integrate the components of VMware Workspace ONE®, including VMware Horizon® 7 Enterprise Edition and VMware Horizon® Cloud Service™ on Microsoft Azure.

This reference architecture provides a framework and guidance for architecting an integrated digital workspace using Workspace ONE and Horizon. Design guidance is given for each product—with a corresponding component design chapter devoted to each product—followed by chapters that provide best practices for integrating the components into a complete platform. For validation, an example environment was built. The design decisions made for this environment are listed throughout the document, along with the rationale for each decision and descriptions of the design considerations.

Workspace ONE combines identity and mobility management to provide frictionless and secure access to all the apps and data that employees need to do their work, wherever, whenever, and from whatever device they choose. Mobile device and identity services are delivered through VMware Workspace ONE® Unified Endpoint Management (UEM), powered by AirWatch, and VMware Identity Manager™.

Additionally, Workspace ONE integrates with VMware Horizon® virtual desktops and published applications delivered through Horizon 7 and Horizon Cloud Service on Microsoft Azure. This integration provides fast single-sign-on (SSO) access to a Windows desktop or set of Windows applications for people who use the service.

![Figure 1: User Workspace with VMware Workspace ONE](image)

The example architecture and deployment described in this guide address key business drivers. The approach taken is, as with any technology solution, to start by defining those business drivers and then identify use cases that need to be addressed. Each use case will entail a set of requirements that need to be fulfilled to satisfy the use case and the business drivers.
Once the requirements are understood, the solutions can be defined and blueprints outlined for the services to be delivered. This step allows us to identify and understand the products, components, and parts that need to be designed, built, and integrated.

**Figure 2: Design Approach**

To deliver a Workspace ONE and Horizon solution, you build services efficiently from several reusable components. This modular, repeatable design approach combines components and services to customize the end-user experience without requiring specific configurations for individual users. The resultant environment and services can be easily adapted to address changes in the business and use case requirements.

**Figure 3: Sample Service Blueprint**

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

This VMware Workspace ONE and VMware Horizon Reference Architecture illustrates how to architect and deliver a modern digital workspace that meets key business requirements and common use cases for the increasingly mobile workplace, using Workspace ONE and Horizon.
Workspace ONE and Horizon Solution Overview

VMware Workspace ONE® is a simple and secure enterprise platform that delivers and manages any app on any device. Workspace ONE integrates identity, application, and enterprise mobility management while also delivering feature-rich virtual desktops and applications. It is available either as a cloud service or for on-premises deployment. The platform is composed of several components—VMware Workspace ONE® UEM (powered by VMware AirWatch®), VMware Identity Manager™, VMware Horizon®, and the Workspace ONE productivity apps, which are supported on most common mobile platforms.

VMware Reference Architectures

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

This Workspace ONE and Horizon reference architecture is a framework intended to provide guidance on how to architect and deploy Workspace ONE and Horizon solutions. It presents high-level design and low-level configuration guidance for the key features and integration points of Workspace ONE and Horizon. The result is a description of cohesive services that 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 minimize implementation and operational risks
- Quick implementation and reduced costs

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 and load balancing to ensure that there are no single points of failure and to provide a production-ready design.

Design Tools

The VMware Digital Workspace Designer is a companion and aid for planning and sizing a Workspace ONE and Horizon deployment, maintaining current VMware best practices and assisting you with key design decisions. The tool is aimed at establishing an initial high-level design for any planned deployment and is intended to complement a proper planning and design process.

The VMware Digital Workspace Topology Tool allows you to create a logical architectural diagram by selecting the Workspace ONE and Horizon components. It generates a diagram that shows the selected components and the links between them. The Topology Tool can also be also launched from the Digital Workspace Designer to automatically create an architectural diagram with the components generated as part of a design.

Both tools can be found https://techzone.vmware.com/tools.
Design Decisions

As part of the creation of this reference architecture guide, full environments are designed, built, and tested. Throughout this guide, design decisions are listed that describe the choices we made for our implementation.

Table 1: Design Decision Regarding the Purpose of This Reference Architecture

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full production-ready environments were architected, deployed, and tested.</td>
<td>This allows the content of this guide, including the design, deployment, integration, and delivery, to be verified, validated, and documented.</td>
</tr>
</tbody>
</table>

Each implementation of Workspace ONE and Horizon is unique and will pose distinct requirements. The implementation followed in this reference architecture tries to address the common use cases, decisions, and challenges that need to be addressed in a manner that can be adapted to differing circumstances.

Audience

This reference architecture guide helps IT architects, consultants, and administrators involved in the early phases of planning, designing, and deploying Workspace ONE, VMware Horizon® 7, and VMware Horizon® Cloud Service™ solutions.

You should have:

- A solid understanding of the mobile device landscape
- Deep experience regarding the capabilities and configuration of mobile operating systems
- Familiarity with device-management concepts
- Knowledge of identity solutions and standards, such as SAML authentication
- Understanding of enterprise communication and collaboration solutions, including Microsoft Office 365, Exchange, and SharePoint
- A good understanding of virtualization, in particular any platform used to host services such as VMware vSphere® or Microsoft Azure.
- A solid understanding of desktop and application virtualization
- A solid understanding of firewall policy and load-balancing configurations
- A good working knowledge of networking and infrastructure, covering topics such as Active Directory, DNS, and DHCP

Workspace ONE Features

Workspace ONE features provide enterprise-class security without sacrificing convenience and choice for end users:

- **Real-time app delivery and automation** – Taking advantage of new capabilities in Windows, Workspace ONE allows desktop administrators to automate application distribution and
updates. This automation, combined with virtualization technology, helps ensure application access as well as improve security and compliance. Provision, deliver, update, and retire applications in real time.

- **Self-service access to cloud, mobile, and Windows apps** – After end users are authenticated through either the Workspace ONE app or the VMware Workspace ONE® Intelligent Hub app, they can instantly access mobile, cloud, and Windows applications with one-touch mobile single sign-on (SSO).

- **Choice of any device, employee or corporate owned** – Administrators can facilitate adoption of bring-your-own-device (BYOD) programs by putting choice in the hands of end users. Give the level of convenience, access, security, and management that makes sense for their work style.

- **Device enrollment** – The enrollment process allows a device to be managed in a Workspace ONE UEM environment so that device profiles and applications can be distributed and content can be delivered or removed. Enrollment also allows extensive reporting based on the device’s check-in to the Workspace ONE UEM service.

- **Adaptive management** – For some applications, end users can log in to Workspace ONE and access the applications without first enrolling their device. For other applications, device enrollment is required, and the Workspace ONE app can prompt the user to initiate enrollment.

  Administrators can enable flexible application access policies, allowing some applications to be used prior to enrollment in device management, while requiring full enrollment for apps that need higher levels of security.

- **Conditional access** – Both VMware Identity Manager and Workspace ONE UEM have mechanisms to evaluate compliance. When users register their devices with Workspace ONE, data samples from the device are sent to the Workspace ONE UEM cloud service on a scheduled basis to evaluate compliance. This regular evaluation ensures that the device meets the compliance rules set by the administrator in the Workspace ONE UEM Console. If the device goes out of compliance, corresponding actions configured in the Workspace ONE UEM Console are taken.

  VMware Identity Manager includes an access policy option that administrators can configure to check the Workspace ONE UEM server for device compliance status when users sign in. The compliance check ensures that users are blocked from signing in to an application or using SSO to the VMware Identity Manager self-service catalog if the device is out of compliance. When the device is compliant again, the ability to sign in is restored.

  Actions can be enforced based on the network that users are on, the platform they are using, or the applications being accessed. In addition to checking Workspace ONE UEM for device compliance, VMware Identity Manager can evaluate compliance based on network range of the device, type of device, operating system of the device, and credentials.

- **Unified application catalog** – The VMware Identity Manager and Workspace ONE UEM application catalogs are combined and presented on either the Workspace ONE app’s Catalog tab or the VMware Workspace ONE Intelligent Hub app, depending on which is being used.
• **Secure productivity apps: VMware Workspace ONE® Boxer, Web, Content, Notebook, People, Verify, and PIV-D Manager** – End users can use the included mail, calendar, contacts, browser, content, organization, and authentication capabilities, while policy-based security measures protect the organization from data leakage by restricting the ways in which attachments and files are edited and shared.

• **Mobile SSO** – One-touch SSO technology is available for all supported platforms. The implementation on each OS is based on features provided by the underlying OS. For iOS, one-touch SSO uses technology known as the key distribution center (KDC). For Android, the authentication method is called mobile SSO for Android. And for Windows 10, it is called cloud certificate.

• **Secure browsing** – Using VMware Workspace ONE® Web instead of a native browser or third-party browser ensures that access to sensitive web content is secure and manageable.

• **Data loss prevention (DLP)** – This feature forces documents or URLs to open only in approved applications to prevent accidental or purposeful distribution of sensitive information.

• **Resource types** – Workspace ONE supports a variety of applications exposed through the VMware Identity Manager and Workspace ONE UEM catalogs, including SaaS-based SAML apps, VMware Horizon apps and desktops, Citrix virtual apps and desktops, VMware ThinApp® packaged apps delivered through VMware Identity Manager, and native mobile applications delivered through Workspace ONE UEM.

### Workspace ONE Platform Integration

Workspace ONE UEM delivers the enterprise mobility management portion of the solution. Workspace ONE UEM allows device enrollment and uses profiles to enforce configuration settings and management of users’ devices. It also enables a mobile application catalog to publish public and internally developed applications to end users.

VMware Identity Manager provides the solution’s identity-related components. These components include authentication using username and password, two-factor authentication, certificate, Kerberos, mobile SSO, and inbound SAML from third-party VMware Identity Manager systems. VMware Identity Manager also provides SSO to entitled web apps and Windows apps and desktops delivered through either VMware Horizon or Citrix.

![Figure 4: Workspace ONE Logical Architecture Overview](image-url)

---

VMware Workspace ONE and VMware Horizon Reference Architecture - 12
VMware Workspace ONE Intelligence

VMware Workspace ONE® Intelligence is a service that gives organizations visualization tools and automation to help them make data-driven decisions for operating their Workspace ONE environment.

By aggregating, analyzing, and correlating device, application, and user data, Workspace ONE Intelligence provides extensive ways to filter and reveal key performance indicators (KPIs) at speed and scale across the entire digital workspace environment. After information of interest has been surfaced by Workspace ONE Intelligence, IT administrators can:

- Use the built-in decision engine to create rules that take actions based on an extensive set of parameters.
- Create policies that take automated remediation actions based on context.

With Workspace ONE Intelligence, organizations can easily manage complexity and security without compromising a great user experience.

**Horizon 7 Platform**

With Horizon 7 Enterprise Edition, VMware offers 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 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 a pristine, high-performance personalized desktop every time a user logs in.
  - Improve security by destroying desktops every time a user logs out.

• **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 already logged in to 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.

  **Note**: App Volumes is not currently supported as part of VMware Horizon® Cloud Service™ on Microsoft Azure.

• **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 the existing infrastructure.
  - Speed up the login process by applying configuration and environment settings in an asynchronous process instead of all at login.
  - Provide a dynamic environment configuration, such as drive or printer mappings, when a user launches an application.
- **vSphere Integration** – 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.
  - Leverage native storage optimizations from vSphere, including SE Sparse, VAAI, and storage acceleration, to lower storage costs while delivering a superior user experience.
  - Horizon 7 Enterprise Edition with VMware vSAN™ for Desktop Advanced automates storage provisioning and leverages direct-attached storage resources to reduce storage costs for desktop workloads. Horizon 7 supports all-flash capabilities to better support more end users at lower costs across distributed locations.

**Horizon Cloud Service on Microsoft Azure Platform**

Horizon Cloud Service on Microsoft Azure provides customers with the ability to pair their existing Microsoft Azure infrastructure with the Horizon Cloud Service to deliver feature-rich virtual desktops and applications.

Horizon Cloud uses a purpose-built cloud platform that is scalable across multiple deployment options, including fully managed infrastructure from VMware and public cloud infrastructure from Microsoft Azure. The service supports a cloud-scale architecture that makes it easy to deliver virtualized Windows desktops and applications to any device, anytime.

![Figure 6: Horizon Cloud Service on Microsoft Azure Overview](image)

**Reference Architecture Design Methodology**

To ensure a successful Workspace ONE and Horizon deployment, it is important to follow proper design methodology. To start, you need to understand the business requirements, reasons, and objectives for undertaking the project. From there, you can identify the needs of the users and organize these needs into use cases with understood requirements. You can then align and map those use cases to a set of integrated services provided by Workspace ONE and Horizon.
A Workspace ONE and Horizon design uses a number of components to provide the services that address the identified use cases. Before you can assemble and integrate these components to form a service, you must first design and build the components in a modular and scalable manner to allow for change and growth. You also must consider integration into the existing environment. Then you 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, the steps are cyclical, and any previous decision should be revisited to make sure a subsequent one has not impacted it.
Business Drivers and Use Cases

An end-user-computing (EUC) solution based on VMware Workspace ONE®, VMware Horizon® 7 and VMware Horizon® Cloud Service™ on Microsoft Azure can address a wide-ranging set of business requirements and use cases. In this reference architecture, the solution targets the most common requirements and use cases seen in customer deployments to date.

Addressing Business Requirements

A technology solution should directly address the critical business requirements that justify the time and expense of putting a new set of capabilities in place. 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 following are sample common key business drivers that can be addressed by the Workspace ONE solution.

Mobile Access

Requirement definition: Provide greater business mobility by providing mobile access to modern and legacy applications on laptops, tablets, and smartphones.

Workspace ONE and Horizon solution: Workspace ONE provides a straightforward, enterprise-secure method of accessing all types of applications that end users need from a wide variety of platforms.

- It is the first solution that brings together identity, device and application management, a unified application catalog, and mobile productivity.
- VMware Horizon® Client™ technology supports all mobile and laptop devices as well as common operating systems.
- VMware Unified Access Gateway™ virtual appliances provide secure external access to internal resources without the need for a VPN.

Fast Provisioning and Access

Requirement definition: Allow fast provisioning of and secure access to line-of-business applications for internal users and third-party suppliers, while reducing physical device management overhead.

Workspace ONE and Horizon solution: Workspace ONE can support a wide range of device access scenarios, simplifying the onboarding of end-user devices.

- Adaptive management allows a user to download an app from a public app store and access some published applications. If a user needs to access more privileged apps or corporate data, they are prompted to enroll their device from within the app itself rather than through an agent, such as the VMware Workspace ONE® Intelligent Hub app.
- 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. Applications are delivered on a per-user basis using VMware App Volumes™.
• Horizon Cloud Service on Microsoft Azure delivers feature-rich virtual desktops and applications using a purpose-built cloud platform. This makes it easy to deliver virtualized Windows desktops and applications to any device, anytime. IT can save time getting up and running with an easy deployment process, simplified management, and a flexible subscription model.

• Unified Access Gateway appliances provide a secure and simple mechanism for external users to access virtual desktops or published applications customized using VMware User Environment Manager™.

Reduced Application Management Effort

Requirement definition: Reduce application management overhead and reduce application provisioning time.

Workspace ONE and Horizon solution: Workspace ONE provides end users with a single application catalog for native mobile, SaaS, and virtualized applications and improves application management.

• Workspace ONE provides a consolidated view of all applications hosted across different services with a consistent user experience across all platforms.

• With Horizon 7 and Horizon Cloud Service on Microsoft Azure, Windows-based applications are delivered centrally, either through virtual desktops or as RDSH-published applications. These can be centrally managed, allowing for access control, fast updates, and version control.

• VMware Workspace ONE® Intelligence™ gives IT administrators insights into app deployments and app engagement. Analysis of user behavior combined with automation capabilities allow for quick resolution of issues, reduced escalations, and increased employee productivity.

• 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 Windows applications portable across platforms.

Centralized and Secure Data and Devices

Requirement definition: Centralize management and security of corporate data and devices to meet compliance standards.

Workspace ONE and Horizon solution: All components are designed with security as a top priority.

• VMware Workspace ONE® UEM (powered by AirWatch) provides aggregation of content repositories, including SharePoint, network file shares, and cloud services. Files from these repositories can be synced to the VMware Workspace ONE® Content app for viewing and secure editing.

• Workspace ONE UEM policies can also be established to prevent distribution of corporate files, control where files can be opened and by which apps, and prevent such functions as copying and pasting into other apps, or printing.
- Horizon 7 is a virtual desktop solution where user data, applications, and desktop activity do not leave the data center. Additional Horizon 7 and User Environment Manager policies restrict and control user access to data.

- VMware NSX® provides network-based services such as security, network virtualization and can provide network least-privilege trust and VM isolation using micro-segmentation and identity-based firewalls for the Horizon 7 management, RDSH, and desktop environments.

- Horizon Cloud Service on Microsoft Azure is the platform for delivering virtual desktops or published applications where user data, applications, and desktop activity do not leave the data center. Additional Horizon Cloud and VMware User Environment Manager policies restrict and control user access to data.

- Workspace ONE Intelligence detects and remediates security vulnerabilities at scale. Quickly identify out-of-compliance devices and automate access control policies based on user behavior.

Comprehensive and Flexible Platform for Corporate-Owned or BYOD Strategies

**Requirement definition:** Allow users to access applications, especially the Microsoft Office 365 suite, and corporate data from their own devices.

**Workspace ONE and Horizon solution:** Workspace ONE can meet the device-management challenges introduced by the flexibility demands of BYOD.

- Workspace ONE and features like adaptive management simplify end-user enrollment and empower application access in a secure fashion to drive user adoption.

- With Horizon 7 and Horizon Cloud Service on Microsoft Azure, moving to a virtual desktop and published application solution removes the need to manage client devices, applications, or images. A thin client, zero client, or employee-owned device can be used in conjunction with Horizon Client. IT now has the luxury of managing single images of virtual desktops in the data center.

- Get insights into device and application usage over time with Workspace ONE Intelligence to enable optimizing resource allocation and license renewals. The built-in automation capabilities can tag devices that have been inactive for specific periods of time or notify users when their devices need to be replaced.

Reduced Support Calls and Improved Time to Resolution

**Requirement definition:** Simplify and secure access to applications to speed up root-cause analysis and resolution of user issues.

**Workspace ONE and Horizon solution:** Workspace ONE provides single-sign-on (SSO) capabilities to a wide range of platforms and applications. By leveraging SSO technology, password resets are unnecessary.

- VMware Identity Manager™ provides a self-service single point of access to all applications and, in conjunction with True SSO, provides a platform for SSO. Users no longer need to remember passwords or request applications through support calls.
Both Workspace ONE UEM and VMware Identity Manager include dashboards and analytics to help administrators understand what a profile of application access and device deployment looks like in the enterprise. With greater knowledge of which applications users are accessing, administrators can more quickly identify issues with licensing or potential attempted malicious activities against enterprise applications.

Workspace ONE Intelligence ensures that end users get the best mobile application experience by keeping an eye on app performance, app engagement, and user behavior. With detailed insights around devices, networks, operating systems, geolocation, connectivity state, and current app version, LOB owners can optimize their apps for their unique audience and ensure an optimal user experience.

Horizon 7 Enterprise Edition includes the Horizon Help Desk Tool, which gives insights into users’ sessions and aids in troubleshooting and maintenance operations.

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 display protocol performance to storage and compute utilization, vRealize Operations Manager for Horizon accelerates root-cause analysis of issues that arise.

Multi-site Deployment Business Drivers

There are many ways and reasons to implement a multi-site solution, especially when deploying components on-premises. The most typical setup and requirement is for a two-data-center strategy. The aim is to provide disaster recovery, with the lowest possible recovery time objective (RTO) and recovery point objective (RPO); that is, to keep the business running with the shortest possible time to recovery and with the minimum amount of disruption.

The overall business driver for disaster recovery is straightforward:

- Keep the business operating during an extended or catastrophic technology outage.
- Provide continuity of service.
- Allow staff to carry out their day-to-day responsibilities.

With services, applications, and data delivered by Workspace ONE and Horizon, that means providing continuity of service and mitigating against component failure, all the way up to a complete data center outage.

With respect to business continuity and disaster recovery, this reference architecture addresses the following common key business drivers:

- Cope with differing levels and types of outages and failures.
- Develop predictable steps to recover functionality in the event of failures.
- Provide essential services and access to applications and data delivered by Workspace ONE and Horizon during outages.
- Minimize interruptions during outages.
- Provide the same or similar user experience during outages.
- Provide mobile secure access.

The following table describes the strategy used for responding to each of these business drivers. In this table, the terms active/passive and active/active are used.

- **Active/passive recovery mode** – Requires that the passive instance of the service be promoted to active status in the event of a service outage.
- **Active/active recovery mode** – Means that the service is available from multiple data centers without manual intervention.

### Table 2: Meeting Business Requirements with Multi-site Deployments

<table>
<thead>
<tr>
<th>Business Driver</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide essential services and access to applications and data delivered by Workspace ONE and Horizon 7 during outages. Minimize interruptions during outages.</td>
<td>The highest possible service level is delivered, and downtime is minimized, when all intra-site components are deployed in pairs and all services are made highly available. These services must be capable of being delivered from multiple sites, either in an active/active or active/passive manner.</td>
</tr>
<tr>
<td>Provide a familiar user experience during outages.</td>
<td>To maintain personalized environments for end users, replicate the parts that a user considers persistent (profile, user configuration, applications, and more). Reconstruct the desktop in the second data center using those parts. VMware Identity Manager provides a common entry point to all types of applications, regardless of which data center is actively being used.</td>
</tr>
<tr>
<td>Cope with differing levels and types of outages and failures.</td>
<td>This reference architecture details a design for multi-site deployments to cope with catastrophic failures all the way up to a site outage. The design ensures that there is no single point of failure within a site.</td>
</tr>
<tr>
<td>Develop predictable steps to recover functionality in the event of failures.</td>
<td>The services are constructed from several components and designed in a modular fashion. A proper design methodology, as followed in this reference architecture, allows each component to be designed for availability, redundancy, and predictability. With an effective design in place, you can systematically plan</td>
</tr>
</tbody>
</table>
Table 2: Meeting Business Requirements with Multi-site Deployments (Continued)

<table>
<thead>
<tr>
<th>Business Driver</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>and document the whole end-user service and the recovery steps or processes for each component of the service.</td>
</tr>
<tr>
<td>Provide mobile secure access.</td>
<td>Desktop mobility is a core capability in the Horizon 7 platform. As end users move from device to device and across locations, the solution reconnects end users to the virtual desktop instances that they are already logged in to, even when they access the enterprise from a remote location through the firewall. VMware Unified Access Gateway virtual appliances provide secure external access without the need for a VPN.</td>
</tr>
</tbody>
</table>

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 might be considered a “normal office worker” use case.

Designing an environment includes building out the functional definitions for the use cases and their requirements. We define typical use cases that are also adaptable to cover most scenarios. We also define services to deliver the requirements of those use cases.

Workspace ONE Use Cases

This reference architecture includes the following common Workspace ONE use cases.
### Table 3: Workspace ONE Common Use Cases

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Mobile Task-Based Worker** | Users who typically use a mobile device for a single task through a single application.  
  - Mobile device is highly managed and used for only a small number of tasks, such as inventory control, product delivery, or retail applications.  
  - Communications tools, such as email, might be restricted to only sending and receiving email with internal parties.  
  - Device is typically locked down from accessing unnecessary applications. Access to public app stores is restricted or removed entirely.  
  - Device location tracking, full device wipe, and other features are typically used. |
| **Mobile Knowledge Worker** | Many roles fit this profile, such as a hospital clinician or an employee in finance, marketing, HR, health benefits, approvals, or travel.  
  - These workers use their own personal device (BYOD), a corporate device they personally manage, or a managed corporate device with low restrictions.  
  - Users are typically allowed to access email, including personal email, along with public app stores for personal apps.  
  - Device is likely subject to information controls over corporate data, such as data loss prevention (DLP) controls, managed email, managed content, and secure browsing.  
  - Users need access to SaaS-based applications for HR, finance, health benefits, approvals, and travel, as well as native applications where those applications are available.  
  - Device is a great candidate for SSO because the need to access many diverse applications and passwords becomes an issue for users and the helpdesk.  
  - Privacy is typically a concern that might prevent device enrollment, so adaptive management and clear communication regarding the data gathered and reported to the Workspace ONE UEM service is important to encourage adoption. |
Table 3: Workspace ONE Common Use Cases (Continued)

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
</tr>
</thead>
</table>
| Contractor | Contractors might require access to specific line-of-business applications, typically from a remote or mobile location.  
  - Users likely need access to an organization’s systems for performing specific functions and applications, but access might be for a finite time period or to a subset of resources and applications.  
  - When the contractor is no longer affiliated with the organization, all access to systems must be terminated immediately and completely, and all corporate information must be removed from the device.  
  - Users typically need access to published applications or VDI-based desktops, and might use multiple devices not under company control to do so. Devices include mobile devices as well as browser-based devices. |

**VMware Horizon Use Cases**

This reference architecture includes the following Horizon 7 or Horizon Cloud Service on Microsoft Azure use cases.
### Table 4: VMware Horizon Use Cases

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Task Worker</td>
<td>These workers are typically fixed to a specific location with no remote access requirement. Some examples include call center worker, administration worker, and retail user. A static task worker:</td>
</tr>
<tr>
<td></td>
<td>* Uses a small number of Microsoft Windows applications.</td>
</tr>
<tr>
<td></td>
<td>* Does not install their own applications and does not require SaaS application access.</td>
</tr>
<tr>
<td></td>
<td>* Might require location-aware printing.</td>
</tr>
<tr>
<td>Mobile Knowledge Worker</td>
<td>This worker could be a hospital clinician, a company employee, or have a finance or marketing role. This is a catch-all corporate use case. A mobile knowledge worker:</td>
</tr>
<tr>
<td></td>
<td>* Mainly uses applications from a corporate location but might access applications from mobile locations.</td>
</tr>
<tr>
<td></td>
<td>* Uses a large number of core and departmental applications but does not install their own applications. Requires SaaS application access.</td>
</tr>
<tr>
<td></td>
<td>* Requires access to USB devices.</td>
</tr>
<tr>
<td></td>
<td>* Might require location-aware printing.</td>
</tr>
<tr>
<td></td>
<td>* Might require two-factor authentication when accessing applications remotely.</td>
</tr>
<tr>
<td>Software Developer / IT (Power User)</td>
<td>Power users require administrator privileges to install applications. The operating system could be either Windows or a Linux OS, with many applications, some of which could require extensive CPU and memory resources. A power user:</td>
</tr>
<tr>
<td></td>
<td>* Mainly uses applications from a corporate location but might access applications from mobile locations.</td>
</tr>
<tr>
<td></td>
<td>* Uses a large number of core and departmental applications and installs their own applications. Requires SaaS application access.</td>
</tr>
<tr>
<td></td>
<td>* Requires the ability to view video and Flash content.</td>
</tr>
<tr>
<td></td>
<td>* Requires two-factor authentication when accessing applications remotely.</td>
</tr>
<tr>
<td>Multimedia</td>
<td>These users might require GPU-accelerated applications, which have intensive...</td>
</tr>
</tbody>
</table>

VMware Workspace ONE and VMware Horizon Reference Architecture - 25
Table 4: VMware Horizon Use Cases (Continued)

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designer / Engineer</td>
<td>CPU or memory workloads, or both. Examples are CAD/CAM designers, architects, video editors and reviewers, graphic artists, and game designers.</td>
</tr>
<tr>
<td></td>
<td>A multimedia designer:</td>
</tr>
<tr>
<td></td>
<td>• Has a GPU requirement with API support for DirectX 10+, video playback, and Flash content.</td>
</tr>
<tr>
<td></td>
<td>• Mainly uses applications from a corporate location but might access applications from mobile locations.</td>
</tr>
<tr>
<td></td>
<td>• Might require two-factor authentication when accessing applications remotely.</td>
</tr>
<tr>
<td>Contractor</td>
<td>External contractors usually require access to specific line-of-business applications, typically from a remote or mobile location.</td>
</tr>
<tr>
<td></td>
<td>A contractor:</td>
</tr>
<tr>
<td></td>
<td>• Mainly uses applications from a corporate location but might access applications from mobile locations.</td>
</tr>
<tr>
<td></td>
<td>• Uses a subset of core and departmental applications based on the project they are working on. Might require SaaS application access.</td>
</tr>
<tr>
<td></td>
<td>• Has restricted access to the clipboard, USB devices, and so on.</td>
</tr>
<tr>
<td></td>
<td>• Requires two-factor authentication when accessing applications remotely.</td>
</tr>
</tbody>
</table>

Recovery Use Case Requirements

When disaster recovery is being considered, the main emphasis falls on the availability and recoverability requirements of the differing types of users. For each of the previously defined use cases and their requirements, we can define the recovery requirements.

When using the cloud-based versions of services, such as Workspace ONE UEM, VMware Identity Manager, and Workspace ONE Intelligence, availability is delivered as part of the overall service SLA.

With solutions that have components deployed on-premises, the availability of both the platform delivering the service to the user, and the data they expect to use, has to be considered. For VMware Horizon–based services, the availability portion of the solution might have dependencies on applications, personalization, and user data to deliver a full experience to the user in a recovery site. Consider carefully what type of experience will be offered in a recovery scenario and how that matches the business and user requirements.
This reference architecture discusses two common disaster recovery classifications: active/passive and active/active. When choosing between these recovery classifications, which are described in the following table, be sure to view the scenario from the user’s perspective.

### Table 5: Disaster Recovery Classifications

<table>
<thead>
<tr>
<th>Use Case and Recoverability Objective</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active/Passive</strong></td>
<td></td>
</tr>
<tr>
<td>RTO = Medium</td>
<td>• Users normally work in a single office location.</td>
</tr>
<tr>
<td>RPO = Medium</td>
<td>• Service consumed is pinned to a single data center.</td>
</tr>
<tr>
<td></td>
<td>• Failover of the service to the second data center ensures business continuity.</td>
</tr>
<tr>
<td><strong>Active/Active</strong></td>
<td></td>
</tr>
<tr>
<td>RTO = Low</td>
<td>• Users require the lowest possible recovery time for the service (for example, health worker).</td>
</tr>
<tr>
<td>RPO = Low</td>
<td>• Mobile users might roam from continent to continent.</td>
</tr>
<tr>
<td></td>
<td>• Users need to get served from the nearest geographical data center per continent.</td>
</tr>
<tr>
<td></td>
<td>• Service consumed is available in both primary and secondary data centers without manual intervention.</td>
</tr>
<tr>
<td></td>
<td>• Timely data replication between data centers is extremely important.</td>
</tr>
</tbody>
</table>

With a VMware Horizon–based service, the recovery service should aim to offer an equivalent experience to the user. Usually the service at the secondary site is constructed from the same or similar parts and components as the primary site service. Consideration must be given to data replication and the speed and frequency at which data from the primary site can be replicated to the recovery site. This can influence which type of recovery service is offered, how quickly a recovery service can become available to users, and how complete that recovery service might be.

The RTO (recovery time objective) is defined as the time it takes to recover a given service. RPO (recovery point objective) is the maximum period in which data might be lost. Low targets are defined as 30- to 60-second estimates. Medium targets are estimated at 45–60 minutes. These targets depend on the environment and the components included in the recovery service.
Service Definitions

From our business requirements, we outlined several typical use cases and their requirements. Taking the business requirements and combining them with one or more use cases enables the definition of a service.

The service, for a use case, defines the unique requirements and identifies the technology or feature combinations that satisfy those unique requirements. After the service has been defined, you can define the service quality to be associated with that service. Service quality takes into consideration the performance, availability, security, and management and monitoring requirements to meet SLAs.

The detail required to build out the products and components comes later, after the services are defined and the required components are understood.

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 might mean adding components, while in others it might be possible to remove some that are not required.

You could also combine multiple services together to address more complex use cases. For example, you could combine a VMware Workspace ONE® service with a VMware Horizon® 7 or VMware Horizon® Cloud Service™ and a recovery service.

Figure 8: Example of Combining Multiple Services for a Complex Use Case

Workspace ONE Use Case Services

A use case service identifies the features required for a specific type of user. For example, a mobile task worker might use a mobile device for a single task through a single application. The Workspace ONE use case service for this worker could be called the mobile device management service. This service uses only a few of the core Workspace ONE components, as described in the following table.
**Table 6: Core Components of Workspace ONE**

<table>
<thead>
<tr>
<th>Component</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Workspace ONE® UEM</td>
<td>Enterprise mobility management</td>
</tr>
<tr>
<td>VMware Identity Manager™</td>
<td>Identity platform</td>
</tr>
<tr>
<td>VMware Workspace ONE® Intelligence™</td>
<td>Integrated insights, app analytics, and automation</td>
</tr>
<tr>
<td>Workspace ONE app</td>
<td>End-user access to apps</td>
</tr>
<tr>
<td>VMware Horizon</td>
<td>Virtual desktops and Remote Desktop Services (RDS) published applications delivered either through Horizon Cloud or Horizon 7</td>
</tr>
<tr>
<td>VMware Workspace ONE® Boxer</td>
<td>Secure email client</td>
</tr>
<tr>
<td>VMware Workspace ONE® Web</td>
<td>Secure web browser</td>
</tr>
<tr>
<td>VMware Workspace ONE® Content</td>
<td>Mobile content repository</td>
</tr>
<tr>
<td>VMware Workspace ONE® Tunnel</td>
<td>Secure and effective method for individual applications to access corporate resources</td>
</tr>
<tr>
<td>VMware AirWatch Cloud Connector</td>
<td>Directory sync with enterprise directories</td>
</tr>
<tr>
<td>VMware Identity Manager Connector</td>
<td>Directory sync with enterprise directories</td>
</tr>
<tr>
<td>VMware Unified Access Gateway™</td>
<td>Sync to Horizon resources</td>
</tr>
<tr>
<td>VMware Workspace ONE® Secure Email Gateway</td>
<td>Gateway that provides secure edge services</td>
</tr>
<tr>
<td></td>
<td>Email proxy service</td>
</tr>
</tbody>
</table>

**Enterprise Mobility Management Service**

**Overview:** Many organizations have deployed mobile devices and have lightweight management capabilities, like simple email deployment and device policies, such as a PIN requirement, device
timeouts, and device wiping. But they lack a comprehensive and complete management practice to enable a consumer-simple, enterprise-secure model for devices.

**Use case:** Mobile Task-Based Workers

**Table 7:** Unique Requirements of Mobile Task Workers

<table>
<thead>
<tr>
<th>Unique Requirements</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide device management beyond simple policies</td>
<td>• Workspace ONE native app&lt;br&gt;• VMware Identity Manager authentication&lt;br&gt;• AirWatch Cloud Connector</td>
</tr>
<tr>
<td>Enable adaptive management capabilities</td>
<td>• Workspace ONE native app&lt;br&gt;• Adaptive management&lt;br&gt;• Workspace services device enrollment</td>
</tr>
</tbody>
</table>

**Blueprint**

The following figure shows a high-level blueprint of a Workspace ONE Standard deployment and the available components.

**Enterprise Productivity Service**

**Overview:** Organizations with a more evolved device management strategy are often pushed by end users to enable more advanced mobility capabilities in their environment. Requested capabilities include single sign-on (SSO) and multi-factor authentication, and access to productivity tools. However, from an enterprise perspective, providing this much access to corporate information means instituting a greater degree of control, such as blocking native email clients in favor of managed...
email, requiring syncing content with approved repositories, and managing which apps can be used to open files.

**Use cases:** Mobile Knowledge Workers, Contractors

**Table 8:** Unique Requirements of Mobile Knowledge Workers and Contractors

<table>
<thead>
<tr>
<th>Unique Requirements</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-factor authentication</td>
<td>VMware Workspace ONE® Verify</td>
</tr>
<tr>
<td>SSO</td>
<td>VMware Identity Manager and Workspace ONE UEM</td>
</tr>
<tr>
<td>Managed email</td>
<td>Workspace ONE Boxer</td>
</tr>
<tr>
<td>Enterprise content synchronization</td>
<td>Workspace ONE Content</td>
</tr>
<tr>
<td>Secure browsing</td>
<td>VMware Workspace ONE® Web</td>
</tr>
<tr>
<td>VPN per application</td>
<td>Workspace ONE Tunnel</td>
</tr>
</tbody>
</table>

**Blueprint**

The following figure shows a high-level blueprint of a Workspace ONE Advanced deployment and the available components.

**Enterprise Application Workspace Service**

**Overview:** Recognizing that some applications are not available as a native app on a mobile platform and that some security requirements dictate on-premises application access, virtualized applications
and desktops become a core part of a mobility strategy. Building on the mobile productivity service, and adding access to VMware Horizon–based resources, enables this scenario.

Many current VMware Horizon users benefit from adding the Workspace ONE catalog capabilities as a single, secure point of access for their virtual desktops and applications.

**Use cases:** Contractors, Mobile Knowledge Workers

**Table 9:** Unique Requirements of Contractors and Mobile Knowledge Workers

<table>
<thead>
<tr>
<th>Unique Requirements</th>
<th>Components</th>
</tr>
</thead>
</table>
| Access to virtual apps and desktops | • Horizon Cloud or Horizon 7  
|                              | • VMware Identity Manager Connector              |

**Blueprint**

The following figure shows a high-level blueprint of a Workspace ONE Enterprise Edition deployment and the available components.

**Horizon 7 Use Case Services**

Horizon 7 use case services address a wide range of user needs. For example, a Published Application service can be created for static task workers, who require only a few Windows applications. In contrast, a GPU-Accelerated Desktop service can be created for multimedia designers who require graphics drivers that use hardware acceleration.

The following components are used across the various use cases.
Table 10: Core Components of Horizon 7

<table>
<thead>
<tr>
<th>Component</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon 7</td>
<td>Virtual desktops and RDSH-published applications</td>
</tr>
<tr>
<td>VMware 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>
<tr>
<td>VMware vRealize® Operations for Horizon®</td>
<td>Management and monitoring</td>
</tr>
<tr>
<td>VMware vSphere®</td>
<td>Infrastructure platform</td>
</tr>
<tr>
<td>VMware vSAN™</td>
<td>Storage platform</td>
</tr>
<tr>
<td>VMware NSX®</td>
<td>Networking and security platform</td>
</tr>
</tbody>
</table>

Horizon 7 Published Application Service

**Overview:** Windows applications are delivered as published applications provided by farms of RDSH servers. The RDSH servers are created using instant clones to provide space and operational efficiency. Applications are delivered through App Volumes. Individual or conflicting applications are packaged with VMware ThinApp® and are available through the VMware Identity Manager catalog. User Environment Manager applies profile settings and folder redirection.

**Use case:** Static Task Worker

Table 11: Unique Requirements of Static Task Workers

<table>
<thead>
<tr>
<th>Unique Requirements</th>
<th>Components</th>
</tr>
</thead>
</table>
| Small number of Windows applications | • Horizon 7 RDSH-published applications (a good fit for a small number of applications)  
• App Volumes AppStacks |
| Requires location-aware printing | • ThinPrint  
• User Environment Manager |
### Table 12: Service Qualities of Horizon 7 Published Application Service

<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 12: Horizon 7 Published Application Service Blueprint

#### Horizon 7 GPU-Accelerated Application Service

**Overview:** Similar to the Horizon 7 Published Application service but has more CPU and memory, and uses hardware-accelerated rendering with NVIDIA GRID graphics cards installed in the vSphere servers (vGPU).

**Use case:** Occasional Graphic Application Users
Table 13: Unique Requirements of Occasional Graphic Application Users

<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>Small number of Windows applications</td>
<td>• Horizon 7 RDSH-published applications (a good fit for a small number of applications)</td>
</tr>
<tr>
<td></td>
<td>• App Volumes AppStacks</td>
</tr>
<tr>
<td>Hardware H.264 encoding</td>
<td>Blast Extreme</td>
</tr>
</tbody>
</table>

Table 14: Service Qualities of the Horizon 7 GPU-Accelerated Application Service

<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>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Blueprint

Figure 13: Horizon 7 GPU-Accelerated Application Service Blueprint

**Horizon 7 Desktop Service**

**Overview:** The core Windows 10 desktop is an instant clone, which is kept to a 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 are available through the VMware Identity Manager catalog.

User Environment Manager applies profile settings and folder redirection. Although Windows 10 was used in this design, Windows 7 could be substituted.

**Use cases:** Mobile Knowledge Worker, Contractors

**Table 15:** Unique Requirements of Mobile Knowledge Workers and Contractors

<table>
<thead>
<tr>
<th>Unique Requirements</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large number of core and departmental applications</td>
<td>• Horizon 7 instant-clone virtual desktop (a good fit for larger numbers of applications)</td>
</tr>
<tr>
<td></td>
<td>• App Volumes AppStacks for core applications and departmental applications</td>
</tr>
<tr>
<td>Require access from mobile locations</td>
<td>Unified Access Gateway, Blast Extreme</td>
</tr>
<tr>
<td>Two-factor authentication when remote</td>
<td>Unified Access Gateway, True SSO</td>
</tr>
<tr>
<td>Video content and Flash playback</td>
<td>URL content redirection, Flash redirection</td>
</tr>
<tr>
<td>Access to USB devices</td>
<td>User Environment Manager, Smart Policies, application blocking</td>
</tr>
<tr>
<td>Restricted access to clipboard, USB, and so on (for example, for contractors)</td>
<td></td>
</tr>
</tbody>
</table>

**Table 16:** Service Qualities of the Horizon 7 Desktop Service

<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>
**Horizon 7 Desktop with User-Installed Applications Service**

**Overview:** Similar to the construct of the Horizon 7 Desktop service, with the addition of an App Volumes writable volume. Writable volumes allow users to install their own applications and have them persist across sessions.

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

**Table 17: Unique Requirements of Software Developers and Power Users**

<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>User-installed applications</td>
<td>App Volumes writable volume</td>
</tr>
</tbody>
</table>

**Table 18: Service Qualities of the Horizon 7 Desktop with User-Installed Applications Service**

<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>
Horizon 7 GPU-Accelerated Desktop Service

**Overview:** Similar to the Horizon 7 Desktop Service or the Horizon 7 Desktop with User-Installed Applications service but has more CPU and memory, and can use hardware-accelerated rendering with NVIDIA GRID graphics cards installed in the vSphere servers (vGPU).

**Use case:** Multimedia Designer

<table>
<thead>
<tr>
<th>Table 19: Unique Requirements of Multimedia Designers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unique Requirements</strong></td>
</tr>
<tr>
<td>GPU accelerated</td>
</tr>
<tr>
<td>User-installed applications</td>
</tr>
<tr>
<td>Hardware H.264 encoding</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 20: Service Qualities of the Horizon 7 GPU-Accelerated Desktop Service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance</strong></td>
</tr>
<tr>
<td>High</td>
</tr>
</tbody>
</table>
Service Definitions

Blueprint

Figure 16: Horizon 7 GPU-Accelerated Desktop Service Blueprint

Horizon 7 Linux Desktop Service

Overview: The core desktop is an instant clone of Linux. Applications can be pre-installed into the master VM.

Use case: Linux User

Table 21: Unique Requirements of Linux Users

<table>
<thead>
<tr>
<th>Unique Requirements</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux extensive CPU and memory</td>
<td>Horizon 7 for Linux instant clone</td>
</tr>
</tbody>
</table>

Table 22: Service Qualities of the Linux Desktop Service

<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>
These services address a wide range of user needs. For example, a published application service can be created for static task workers, who require only a few Windows applications. In contrast, a secure desktop service could be created for users who need a larger number of applications that are better suited to a Windows desktop–based offering.

The following core components are used across the various use cases.

Table 23: Core Components of VMware Horizon® Cloud Service™ on Microsoft Azure

<table>
<thead>
<tr>
<th>Component</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Cloud Service on Microsoft Azure</td>
<td>Virtual desktops and RDSH-published applications</td>
</tr>
<tr>
<td>VMware User Environment Manager</td>
<td>User profile, IT settings, and configuration for environment and applications</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>Infrastructure platform</td>
</tr>
</tbody>
</table>

**Horizon Cloud Published Application Service**

**Overview:** Windows applications are delivered as published applications provided by farms of RDSH servers. These applications are optionally available in the catalog and through the Workspace ONE app or web application. User Environment Manager applies profile settings and folder redirection.

**Use case:** Static Task Worker
Table 24: Unique Requirements of Static Task Workers

<table>
<thead>
<tr>
<th>Unique Requirements</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small number of Windows apps</td>
<td>• Horizon Cloud on Microsoft Azure RDSH-published applications (a good fit for a small number of applications)</td>
</tr>
</tbody>
</table>
| (Optional) location-aware printing | • ThinPrint
|                               | • User Environment Manager                                                 |

Blueprint

Horizon Cloud GPU-Accelerated Application Service

Overview: Similar to the Horizon Cloud Published Application service, but this service uses hardware-accelerated rendering with NVIDIA GRID graphics cards available through Microsoft Azure. The Windows applications are delivered as published applications provided by farms of RDSH servers.

Use case: Multimedia Designer/Engineer

Table 25: Unique Requirements of Multimedia Designers

<table>
<thead>
<tr>
<th>Unique Requirements</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPU-accelerated rendering</td>
<td>NVIDIA backed GPU RDSH VM</td>
</tr>
<tr>
<td>Hardware H.264 encoding</td>
<td>Blast Extreme</td>
</tr>
</tbody>
</table>
Horizon Cloud Desktop Service

**Overview**: This service uses a standard Windows 10 desktop that is cloned from a master VM image. User Environment Manager applies the user’s Windows environment settings, application settings, and folder redirection. Desktop and application entitlements are optionally made available through the VMware Identity Manager catalog.

**Use cases**: Mobile Knowledge Worker, Contractors

### Table 26: Unique Requirements of Mobile Knowledge Workers and Contractors

<table>
<thead>
<tr>
<th>Unique Requirements</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large number of core and departmental applications</td>
<td>Horizon virtual desktop running Windows 10 (a good fit for larger numbers of applications)</td>
</tr>
<tr>
<td>Access from mobile locations</td>
<td>Unified Access Gateway, Blast Extreme</td>
</tr>
<tr>
<td>Two-factor authentication when remote</td>
<td>Unified Access Gateway, True SSO</td>
</tr>
<tr>
<td>Video content and Flash playback</td>
<td>URL content redirection, HTML5 redirection, Flash redirection</td>
</tr>
<tr>
<td>- Access to USB devices</td>
<td>User Environment Manager, Horizon Smart Policies, application blocking</td>
</tr>
<tr>
<td>- Restricted access to clipboard, USB, and so on (for example, for contractors)</td>
<td></td>
</tr>
</tbody>
</table>
Recovery Services

To ensure availability, recoverability, and business continuity, the design of the services also needs to consider disaster recovery. We can define recovery services and map them to the previously defined use-case services.

Recovery services can be designed to operate in either an active/active or an active/passive mode and should be viewed from the users’ perspective.

- In active/passive mode, loss of an active data center instance requires that the passive instance of the service be promoted to active status for the user.
- In active/active mode, the loss of a data center instance does not impact service availability for the user because the remaining instance or instances continue to operate independently and can offer the end service to the user.

In the use cases, a user belongs to a home site and can have an alternative site available to them. Where user pinning is required, an active/passive approach results in a named user having a primary site they always connect to or get redirected to during normal operations.

Also, a number of components are optional to a service, depending on what is required. Blueprints for multi-site VMware Identity Manager, App Volumes, and User Environment Manager data are detailed after the main active/passive and active/active recovery services.

VMware Workspace ONE UEM Recovery Service (On-Premises)

Workspace ONE UEM can be consumed as a cloud-based service or deployed on-premises. When deployed on-premises, it is important to provide resilience and failover capability both within and between sites to ensure business continuity. Workspace ONE UEM can be architected in an active/passive manner, with a failover process recovering the service in the standby site.
VMware Identity Manager Recovery Service (On-Premises)

VMware Identity Manager can also be consumed as a cloud-based service or deployed on-premises. When deployed on-premises, it is important to provide resilience and failover capability both within and between sites to ensure business continuity. VMware Identity Manager can be architected in an active/passive manner, with a failover process recovering the service in the standby site.

Horizon 7 Active/Passive Recovery Service

**Requirement:** The use case service is run from a specific data center but can be failed over to a second data center in the event of an outage.
**Overview:** The core Windows desktop is an instant clone or linked clone, which is preferably kept to a vanilla Windows OS, allowing it to address a wide variety of users. The core could also be a desktop or session provided from an RDSH farm of linked clones or instant clones.

Although applications can be installed in the master image OS, the preferred method is to have applications delivered through App Volumes, with core and department-specific applications included in various AppStacks. Individual or conflicting applications are packaged with VMware ThinApp and are available through the VMware Identity Manager catalog.

If the use case requires the ability for users to install applications themselves, App Volumes writable volumes can be assigned.

User Environment Manager applies the profile, IT settings, user configuration, and folder redirection.

The following table details the recovery requirements and the corresponding Horizon 7 component that addresses each requirement.

**Table 27: Active/Passive Recovery Service Requirements**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows desktop or RDSH available in both sites</td>
<td>- Horizon 7 pools or farms are created in both data centers.</td>
</tr>
<tr>
<td></td>
<td>- Master VM can be replicated to ease creation.</td>
</tr>
<tr>
<td></td>
<td>- Cloud Pod Architecture (CPA) is used for user entitlement and control consumption.</td>
</tr>
<tr>
<td>Native applications</td>
<td>Applications are installed natively in the base Windows OS. No replication is required because native applications exist in both data center pools.</td>
</tr>
<tr>
<td>Attached applications (optional)</td>
<td>Applications contained in App Volumes AppStacks are replicated using App Volumes storage groups.</td>
</tr>
<tr>
<td>User-installed applications (optional)</td>
<td>App Volumes writable volumes.</td>
</tr>
<tr>
<td></td>
<td>- RTO = 60–90 minutes</td>
</tr>
<tr>
<td></td>
<td>- RPO = 1–2 hours (array dependent)</td>
</tr>
<tr>
<td>IT settings</td>
<td>User Environment Manager IT configuration is replicated to another data center.</td>
</tr>
<tr>
<td></td>
<td>- RTO = 30–60 seconds</td>
</tr>
<tr>
<td></td>
<td>- RPO = Approximately 5 minutes</td>
</tr>
<tr>
<td>User data and</td>
<td>User Environment Manager user data is replicated to another data center.</td>
</tr>
</tbody>
</table>
Table 27: Active/Passive Recovery Service Requirements (Continued)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration</td>
<td>center.</td>
</tr>
<tr>
<td></td>
<td>- RTO = 30–60 seconds</td>
</tr>
<tr>
<td></td>
<td>- RPO = Approximately 2 hours</td>
</tr>
<tr>
<td>SaaS applications</td>
<td>VMware Identity Manager is used as a single-sign-on workspace and is present in both locations to ensure continuity of access.</td>
</tr>
<tr>
<td>Mobile access</td>
<td>Unified Access Gateway, Blast Extreme</td>
</tr>
</tbody>
</table>

At a high level, this service consists of a Windows environment delivered by either an instant- or linked-clone desktop or RDSH server, with identical pools created at both data centers. With this service, applications can be natively installed in the OS, provided by App Volumes AppStacks, or some combination of the two. User profile and user data files are made available at both locations and are also recovered in the event of a site outage.

**Blueprint**

![Horizon 7 Active/Passive Recovery Service Blueprint](image)

**Figure 23:** Horizon 7 Active/Passive Recovery Service Blueprint

**Horizon 7 Active/Active Recovery Service**

**Requirement:** This use case service is available from multiple data centers without manual intervention.
**Overview:** Windows applications are delivered as natively installed applications in the Windows OS, and there is little to no reliance on the Windows profile in case of a disaster. User Environment Manager provides company-wide settings during a disaster. Optionally, applications can be delivered through App Volumes AppStacks, with core and department-specific applications included in various AppStacks.

This service generally requires the lowest possible RTO, and the focus is to present the user with a desktop closest to his or her geographical location. For example, when traveling in Europe, the user gets a desktop from a European data center; when traveling in the Americas, the same user gets a desktop from a data center in the Americas.

The following table details the recovery requirements and the corresponding Horizon 7 component that addresses each requirement.

**Table 28: Active/Active Recovery Service Requirements**

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Products, Solutions, and Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lowest possible RTO during a disaster</td>
<td>No reliance on services that cannot be immediately failed over.</td>
</tr>
</tbody>
</table>
| Windows desktop or RDSH server available in both sites | - Horizon 7 desktop and application pools are created in both data centers.  
- Master VM can be replicated to ease creation.  
- Cloud Pod Architecture (CPA) is used to ease user entitlement and consumption. |
| Native applications | Applications are installed natively in the base Windows OS. No replication is required because native applications exist in both data center pools. |
| Attached applications (optional) | Applications contained in App Volumes AppStacks are replicated using App Volumes storage groups. |
| IT settings | User Environment Manager IT configuration is replicated to another data center. The following RTO and RPO targets apply during a data center outage when a recovery process is required:  
- RTO = 30–60 seconds  
- RPO = 30–60 seconds |
| User data and | User Environment Manager user data is replicated to another data center |
Table 28: Active/Active Recovery Service Requirements (Continued)

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Products, Solutions, and Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration (optional)</td>
<td>center. The following RTO and RPO targets apply during a data center outage when a recovery process is required:</td>
</tr>
<tr>
<td></td>
<td>* RTO = 30–60 seconds</td>
</tr>
<tr>
<td></td>
<td>* RPO = Approximately 2 hours</td>
</tr>
<tr>
<td>Mobile access</td>
<td>Unified Access Gateway, Blast Extreme</td>
</tr>
</tbody>
</table>

At a high level, this service consists of a Windows environment delivered by a desktop or an RDSH server available at both data centers. With this service, applications can be natively installed in the OS, attached using App Volumes AppStacks, or some combination of the two. If required, the user profile and user data files can be made available at both locations and can also be recovered in the event of a site outage.

Figure 24: Horizon 7 Active/Active Recovery Service Blueprint

**App Volumes Active/Passive Recovery Service**

Although applications can be installed in the base OS, they can alternatively be delivered by App Volumes AppStacks. An AppStack is used to attach applications to either the Horizon 7 desktop or the RDSH server that provides Horizon 7 published applications.

Applications are attached either to the desktop, at user login, or to the RDSH server as it boots. Because AppStacks are read-only to users and are infrequently changed by IT, AppStacks can be replicated to the second, and subsequent, locations and are available for assignment and mounting in those locations as well.
App Volumes writable volumes are, by contrast, used for content such as user-installed applications, and are written to by the end user. Writable volumes must be replicated and made available at the second site. Due to the nature of the content, writable volumes can have their content updated frequently by users. These updates can affect the RPO and RTO achievable for the overall service. Operational decisions can be made as to whether to activate the service in Site 2 with or without the writable volumes to potentially reduce the RTO.

**Figure 25**: App Volumes Active/Passive Recovery Blueprint

### App Volumes Active/Active Recovery Service

As can be seen in the active/passive App Volumes blueprint, App Volumes AppStacks can be replicated from one site to another and made available, actively, in both because AppStacks require read-only permissions for the user. The complication comes with writable volumes because these require both read and write permissions for the user. If a service does not include writable volumes, the App Volumes portion of the service can be made active/active.
Figure 26: App Volumes Active/Active Recovery Blueprint

User Environment Manager Profile Data Recovery Service

User Environment Manager provides profile management by capturing user settings for the operating system, applications, and user personalization. The captured settings are stored on file shares that need to be replicated to ensure site redundancy.

Although profile data can be made available to both data centers, there is a failover process in the event of the loss of Site 1 that can impact the RTO and RPO.

Operational decisions can be made in these scenarios as to whether the service in Site 2 would be made available with reduced functionality (for example, available with the Windows base, the applications, and the IT configuration but without the user-specific settings).
Horizon Cloud on Microsoft Azure Active/Passive Recovery Service

**Requirement**: The use case service is run from a specific Azure region. An equivalent service can be provided from a second Azure region.

**Overview**: The core Windows desktop or RDSH server is a clone of a master VM image. User Environment Manager applies the profile, IT settings, user configuration, and folder redirection.

**Table 29**: Active/Passive Recovery Service Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows desktop or RDSH server available in both sites</td>
<td>Horizon desktop pools or RDSH server farms are created in both data centers.</td>
</tr>
<tr>
<td>Native applications</td>
<td>Applications are installed natively in the base Windows OS.</td>
</tr>
<tr>
<td>IT settings</td>
<td>User Environment Manager IT configuration is replicated to ensure availability in the event that the primary Azure region becomes unavailable.</td>
</tr>
<tr>
<td>User data and configuration</td>
<td>User Environment Manager user data is replicated to ensure availability in the event that the primary Azure region becomes unavailable.</td>
</tr>
</tbody>
</table>
At a high level, this service consists of a Windows environment delivered by either a desktop or an RDSH server, with equivalent resources created at both data centers. User profile and user data files are made available at both locations and are also recovered in the event of a site outage.

Figure 28: Horizon Cloud Active/Passive Recovery Service Blueprint

User Environment Manager provides profile management by capturing user settings for the operating system, applications, and user personalization. The captured settings are stored on file shares that need to be replicated to ensure site redundancy.

Although profile data can be made available to both regions, there is a failover process in the event of the loss of Region 1 that can impact the RTO and RPO.

Operational decisions can be made in these scenarios as to whether the service in Region 2 should be made available with reduced functionality (for example, available with the Windows base, the applications, and the IT configuration but without the user-specific settings).
Architectural Overview

A VMware Workspace ONE® design uses several complementary components and provides 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.

The components in Workspace ONE, such as VMware Identity Manager™, VMware Workspace ONE® UEM (powered by VMware AirWatch®), and VMware Horizon® are available as on-premises and cloud-hosted products.

For this reference architecture, both cloud-hosted and on-premises Workspace ONE UEM and VMware Identity Manager are used separately to prove the functionality of both approaches. These are shown in the cloud-based and on-Premises logical architecture designs described in this chapter.

Note that other components, such as VMware Horizon® 7 or VMware Horizon® Cloud Service™ on Microsoft Azure, can be combined with either a cloud-based or an on-premises Workspace ONE deployment.

Workspace ONE Logical Architecture

The Workspace ONE platform is composed of VMware Identity Manager and Workspace ONE UEM. Although each product can operate independently, integrating them is what enables the Workspace ONE product to function.

VMware Identity Manager and Workspace ONE UEM provide tight integration between identity and device management. This integration has been simplified in recent versions to ensure that configuration of each product is relatively straightforward.

Although VMware Identity Manager and Workspace ONE UEM are the core components in a Workspace ONE deployment, you can deploy a variety of other components, depending on your business use cases. For example, and as shown in the figure in the next section, you can use VMware Unified Access Gateway™ to provide the VMware Workspace ONE® Tunnel or VPN-based access to on-premises resources.

For more information about the full range of components that might apply to a deployment, refer to the VMware Workspace ONE UEM documentation.

Cloud-Based Logical Architecture

With a cloud-based architecture, Workspace ONE is consumed as a service requiring little or no infrastructure on-premises.

- **VMware Workspace ONE UEM SaaS tenant** – Cloud-hosted instance of the Workspace ONE UEM service. Workspace ONE UEM acts as the mobile device management (MDM), mobile content management (MCM), and mobile application management (MAM) platform.

- **VMware Identity Manager SaaS tenant** – Cloud-hosted instance of VMware Identity Manager. VMware Identity Manager acts as an identity provider by syncing with Active Directory to provide single sign-on (SSO) across SAML-based applications, VMware Horizon–based apps and desktops, and VMware ThinApp® packaged apps. It is also responsible for enforcing authentication policy based on networks, applications, or platforms.
With an on-premises deployment of Workspace ONE, both Workspace ONE UEM and VMware Identity Manager are deployed in your data centers.

- **VMware Workspace ONE UEM** – On-premises installation of Workspace ONE UEM. Workspace ONE UEM consists of several core components, which can be installed on a single server. Workspace ONE UEM acts as the MDM, MCM, and MAM platform.

- **VMware Identity Manager** – Acts as an identity provider by syncing with Active Directory to provide SSO across SAML-based applications, VMware Horizon-based applications and desktops, and VMware ThinApp packaged apps. VMware Identity Manager is also responsible for enforcing authentication policy based on networks, applications, or platforms.
Figure 30: Workspace ONE Sample On-Premises Logical Architecture

**Common Components**

A number of optional components in a Workspace ONE deployment are common to both a cloud-based and an on-premises deployment.

- **AirWatch Cloud Connector (ACC)** – Runs in the internal network, acting as a proxy that securely transmits requests from Workspace ONE UEM to the organization’s critical back-end enterprise infrastructure components. Organizations can leverage the benefits of Workspace ONE® UEM MDM, running in any configuration, together with those of their existing LDAP, certificate authority, email, and other internal systems.

- **VMware Identity Manager Connector** – Performs directory sync and authentication between an on-premises Active Directory and the VMware Identity Manager service.

- **Workspace ONE native mobile app** – OS-specific versions of the native app are available for iOS, Android, and Windows 10. The Workspace ONE app presents a unified application catalog across VMware Identity Manager resources and native mobile apps, allows users to easily find and install enterprise apps, and provides an SSO experience across resource types.

- **Secure email gateway** – Workspace ONE UEM supports integration with email services, such as Microsoft Exchange, GroupWise, IBM Notes (formerly Lotus Notes), and G Suite (formerly Google Apps for Work). You have three options for integrating email:
  - **VMware Secure Email Gateway** – Requires a server to be configured in the data center.
  - **PowerShell integration** – Communicates directly with Exchange ActiveSync on Exchange 2010 or later or Microsoft Office 365.
- **G Suite integration** – Integrates directly with the Google Cloud services and does not need additional servers.

- **Content integration** – The Workspace ONE UEM MCM solution helps organizations address the challenge of securely deploying content to a wide variety of devices using a few key actions. An administrator can leverage the Workspace ONE UEM Console to create, sync, or enable a file repository. After configuration, this content deploys to end-user devices with VMware Workspace ONE® Content. Access to content can be either read-only or read-write.

- **VMware Unified Access Gateway** – Virtual appliance that provides secure edge services and allows external access to internal resources. Unified Access Gateway provides:
  - Workspace ONE UEM Per-App Tunnels and the Tunnel Proxy to allow mobile applications secure access to internal services
  - Access from Workspace ONE Content to internal file shares or SharePoint repositories by running the Content Gateway service
  - Reverse proxying of web servers
  - SSO access to on-premises legacy web applications by identity bridging from SAML or certificates to Kerberos
  - Secure external access to Horizon 7 desktops and applications

### Horizon Virtual Desktops and Published Applications

Both Horizon 7 and Horizon Cloud Service can be combined and integrated into a Workspace ONE deployment, regardless of whether you use a cloud-based or on-premises deployment.

- **Horizon 7** – Manages and delivers virtualized or hosted desktops and applications to end users.
  - **Connection Servers** – Broker instances that securely connect users to desktops and published applications running on VMware vSphere® VMs, physical PCs, blade PCs, or RDSH servers. Connection Servers authenticate users through Windows Active Directory and direct the request to the appropriate and entitled resource.
  - **Horizon Administrative Console** – An administrative console that allows configuration, deployment, management, and entitlement of users to resources.

- **Horizon Cloud Service** – A multi-tenant, cloud-scale architecture that enables you to choose where virtual desktops and apps reside: VMware-managed cloud, BYO cloud, or both.
  - **Horizon Cloud Control Plane** – A control plane that VMware hosts in the cloud for central orchestration and management of VDI desktops, RDSH-published desktops, and RDSH-published applications. Because VMware hosts the service, feature updates and enhancements are consistently provided for a software-as-a-service experience.
  - **Horizon Cloud Administration Console** – The cloud control plane also hosts a common management user interface, which runs in industry-standard browsers. This console provides IT administrators with a single location for management tasks involving user assignments to and management of VDI desktops, RDSH-published desktops, and RDSH-published applications.
- **Horizon Cloud pod** – VMware software deployed to a supported capacity environment, such as Microsoft Azure cloud. Along with access to the Horizon Cloud Administration Console, the service includes the software necessary to pair the deployed pod with the cloud control plane and deliver virtual desktops and applications.

### General Multi-site Best Practices

There are numerous ways to implement a disaster recovery architecture, but some items can be considered general best practices.

#### Components That Must Always Run with a Primary Instance

Even with an active/active usage model across two data centers, meaning that the service is available from both data centers without manual intervention, one of the data centers holds certain roles that are not multi-master defined. The following components must run with a primary instance in a given site:

- On-premises Workspace ONE UEM
- On-premises VMware Identity Manager
- User profile and data shares containing VMware User Environment Manager™ user data
- Active Directory flexible single master operations (FSMO) roles, specifically, Primary Domain Controller (PDC) Emulator, because it is required to make changes to domain-based DFS namespaces
- Microsoft SQL Server Always On availability groups (if used)

Be sure to secure those resources that are not multi-master by nature or that cannot be failed over automatically. Procedures must be put in place to define the steps required to recover these resources.

For this reference architecture design, we chose to place the primary availability group member in Site 1 as well as all AD FSMO roles on a domain controller. We made this choice because we had a good understanding of the failover steps required if either Site 1 or Site 2 failed.

#### Component Replication and Traveling Users

Use Workspace ONE and Horizon components to create effective replication strategies and address the needs of users who travel between sites:

- Create a disaster plan up front that defines what a disaster means in your organization. The plan should specify whether you require a 1:1 mapping in terms of resources, or what portion of the workforce is required to keep the organization operational.
- Understand what user data will need to be replicated between sites to allows users to be productive. The quantity, speed, and frequency of replication will affect the time it takes to present a complete service to a user from another site.
- Replicate Horizon desktop and server (RDSH) master image templates between sites to avoid having to build the same templates on both sites. You can use a vSphere content library or perform a manual replication of the resources needed across the whole implementation.

- With Horizon 7, use Cloud Pod Architecture and avoid using a metro-cluster with VMware vSAN™ stretched cluster unless you have a persistent desktop model in the organization that cannot easily be transformed into a nonpersistent-desktop use case.

- With regard to initial user placement, even with a traveling worker use case, a given user must be related to user profile data (User Environment Manager user data), meaning that a relationship must be established between a user account and a data center. This also holds true when planning how users in the same part of the organization (such as sales) should be split between sites to avoid an entire function of the company being unable to work should a disaster strike.

- For a traveling worker use case, where User Environment Manager is used to control the user profile data, VMware recommends that FlexEngine be used whenever possible in combination with folder redirection. This keeps the core profile to a minimum size and optimizes login times in the case where a profile is loaded across the link between the two data centers.

- Use Microsoft SQL Server failover cluster instances and Always On availability groups for on-premises Workspace ONE UEM and VMware Identity Manager where possible. This is not required for VMware vCenter Server®, the Connection Server event database, and VMware vSphere® Update Manager™.
Component Design: Workspace ONE UEM Architecture

VMware Workspace ONE® UEM (powered by AirWatch) is responsible for device enrollment, a mobile application catalog, policy enforcement regarding device compliance, and integration with key enterprise services, such as email, content, and social media.

Workspace ONE Unified Endpoint Management (UEM) features include:

- **Device management platform** – Allows full life-cycle management of a wide variety of devices, including phones, tablets, Windows 10, and rugged and special-purpose devices.

- **Application deployment capabilities** – Provides automatic deployment or self-service application access for employees.

- **User and device profile services** – Ensures that configuration settings for users and devices:
  - Comply with enterprise security requirements
  - Simplify end-user access to applications

- **Productivity tools** – Includes an email client with secure email functionality, a content management tool for securely storing and managing content, and a web browser to ensure secure access to corporate information and tools.

Workspace ONE UEM can be implemented using an on-premises or a cloud-based (SaaS) model. Both models offer the same functionality.

To avoid repetition, an overview of the product, its architecture, and the common components are described in the cloud-based architecture section, which follows. The on-premises architecture section then adds to this information if your preference is to build on-premises.

**Table 30: Strategy of Using Both Deployment Models**

| Decision | Both a cloud-based and an on-premises Workspace ONE UEM deployment were carried out separately. Deployments were sized for 50,000 devices, which allows for additional growth over time without a redesign. |
| Justification | This strategy allows both architectures to be validated and documented independently. |

**Cloud-based Architecture**

With a cloud-based implementation, the Workspace ONE UEM software is delivered as a service (SaaS). To synchronize Workspace ONE with internal resources such as Active Directory or a Certificate Authority, you use a separate cloud connector, which can be implemented using an AirWatch Cloud Connector. The separate connector can run within the internal network in an outbound-only connection mode, meaning the connector receives no incoming connections from the DMZ.
The simple implementation usually consists of:

- A Workspace ONE UEM tenant
- VMware AirWatch Cloud Connector

**Figure 31**: Cloud-Based Workspace ONE UEM Logical Architecture

The main components of Workspace ONE UEM are described in the following table.
### Table 31: Workspace ONE UEM Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace ONE UEM Console</td>
<td>Administration console for configuring policies within Workspace ONE UEM, to monitor and manage devices and the environment. This service is hosted in the cloud and is managed for you as a part of the SaaS offering.</td>
</tr>
<tr>
<td>Workspace ONE UEM Device Services</td>
<td>Services that communicate with managed devices. Workspace ONE UEM relies on this component for:</td>
</tr>
<tr>
<td></td>
<td>• Device enrollment</td>
</tr>
<tr>
<td></td>
<td>• Application provisioning</td>
</tr>
<tr>
<td></td>
<td>• Delivering device commands and receiving device data</td>
</tr>
<tr>
<td></td>
<td>• Hosting the Workspace ONE UEM self-service catalog</td>
</tr>
<tr>
<td></td>
<td>This service is hosted in the cloud and is managed for you as a part of the SaaS offering.</td>
</tr>
<tr>
<td>API endpoint</td>
<td>Collection of RESTful APIs, provided by Workspace ONE UEM, that allows external programs to use the core product functionality by integrating the APIs with existing IT infrastructures and third-party applications.</td>
</tr>
<tr>
<td></td>
<td>Workspace ONE APIs are also used by various Workspace ONE UEM services, such as Secure Email Gateway for interactions and data gathering.</td>
</tr>
<tr>
<td></td>
<td>This service is hosted in the cloud and is managed for you as a part of the SaaS offering.</td>
</tr>
<tr>
<td>AirWatch Cloud Connector</td>
<td>Component that performs directory sync and authentication using an on-premises resource such as Active Directory or a trusted Certificate Authority.</td>
</tr>
<tr>
<td></td>
<td>This service is hosted in your internal network in outbound-only mode and can be configured for automatic updates.</td>
</tr>
</tbody>
</table>
### Table 31: Workspace ONE UEM Components (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch Cloud Messaging service (AWCM)</td>
<td>Service used in conjunction with the AirWatch Cloud Connector to provide secure communication to your backend systems. AirWatch Cloud Connector also uses AWCM to communicate with the Workspace ONE UEM Console. AWCM also streamlines the delivery of messages and commands from the Workspace ONE UEM Console by eliminating the need for end users to access the public Internet or utilize consumer accounts, such as Google IDs. It serves as a comprehensive substitute for Google Cloud Messaging (GCM) for Android devices and is the only option for providing mobile device management (MDM) capabilities for Windows rugged devices. Also, Windows desktop devices that use the VMware Workspace ONE® Intelligent Hub use AWCM for real-time notifications. This service is hosted in the cloud and is managed for you as a part of the SaaS offering.</td>
</tr>
<tr>
<td>VMware Tunnel</td>
<td>The VMware Tunnel™ provides a secure and effective method for individual applications to access corporate resources hosted in the internal network. The VMware Tunnel uses a unique X.509 certificate (delivered to enrolled devices by Workspace ONE) to authenticate and encrypt traffic from applications to the tunnel. VMware Tunnel has two components – Proxy and Per-App VPN. The Proxy component is responsible for securing traffic from endpoint devices to internal resources through the VMware Workspace ONE® Web app and through enterprise apps that leverage the Workspace ONE SDK. The Per-App Tunnel component enables application-level tunneling (as opposed to full device-level tunneling) for managed applications on iOS, macOS, Android, and Windows devices.</td>
</tr>
</tbody>
</table>

### Table 32: Implementation Strategy for Cloud-Based Workspace ONE UEM

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A cloud-based deployment of Workspace ONE UEM and the components required were architected for 50,000 devices, which allows for additional growth over time without a redesign.</td>
<td>This strategy provides validation of design and implementation of a cloud-based instance of Workspace ONE UEM.</td>
</tr>
</tbody>
</table>
AirWatch Cloud Connector

Even when utilizing cloud solutions, such as Workspace ONE UEM, you might want to use some in-house components and resources, for example, email relay, directory services (LDAP/AD), Certificate Authority, and PowerShell Integration with Exchange. These resources are usually secured by strict firewall rules in order to avoid any unintended or malicious access. Even though these components are not exposed to public networks, they offer great benefits when integrated with cloud solutions such as Workspace ONE.

The AirWatch Cloud Connector allows seamless integration of on-premises resources with the Workspace ONE UEM deployment, whether it be cloud-based or on-premises. This allows organizations to leverage the benefits of Workspace ONE UEM, running in any configuration, together with those of their existing LDAP, Certificate Authority, email relay, PowerShell Integration with Exchange, and other internal systems.

The AirWatch Cloud Connector (ACC) runs in the internal network, acting as a proxy that securely transmits requests from Workspace ONE UEM to the organization’s enterprise infrastructure components. The ACC always works in an outbound-only mode, which protects it from targeted inbound attacks and allows it to work with existing firewall rules and configurations.

Workspace ONE UEM and the ACC communicate by means of AirWatch Cloud Messaging (AWCM). This communication is secured through certificate-based authentication, with the certificates generated from a trusted Workspace ONE UEM Certificate Authority.

The ACC integrates with the following internal components:

- Email relay (SMTP)
- Directory services (LDAP/AD)
- Exchange 2010 (PowerShell)
- Syslog (event log data)

The ACC also allows the following PKI integration add-ons:

- Microsoft Certificate Services (PKI)
- Simple Certificate Enrollment Protocol (SCEP PKI)
- Third-party certificate services (on-premises only)
  - OpenTrust CMS Mobile
  - Entrust PKI
  - Symantec MPKI

There is no need to go through AirWatch Cloud Connector for cloud certificate services. You use the ACC only when the PKI is on-premises, not in the cloud (SaaS).

**Table 33**: Deployment Strategy for the AirWatch Cloud Connector

<table>
<thead>
<tr>
<th>Decision</th>
<th>The AirWatch Cloud Connector was deployed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>The ACC provides integration of Workspace ONE UEM with Active Directory.</td>
</tr>
</tbody>
</table>
Scalability

You can configure multiple instances of ACC by installing them on additional dedicated servers using the same installer. The traffic is automatically load-balanced by the AWCM component and does not require a separate load balancer.

Multiple ACC instances can receive traffic (that is, use a live-live configuration) as long as the instances are in the same organization group and connect to the same AWCM server for high availability. Traffic is routed by AWCM using an LRU (least recently used) algorithm, which examines all available connections to decide which ACC node to use for routing the next request.

For recommendations on the number of ACC instances required, and for hardware requirements, see On-Premises Architecture Hardware Assumptions. Note that the documentation shows only the number of connectors required for each sizing scenario to cope with the load demand. It does not include additional servers in those numbers to account for redundancy.

**Table 34**: Strategy for Scaling the ACC Deployment

<table>
<thead>
<tr>
<th>Decision</th>
<th>Three instances of AirWatch Cloud Connector were deployed in the internal network. These instances were installed on Windows Server 2016 VMs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Two ACC instances are required based on load, and a third is added for redundancy.</td>
</tr>
</tbody>
</table>

**AirWatch Cloud Connector Installation**

Refer to the latest VMware Workspace ONE UEM documentation for full details on the VMware AirWatch Cloud Connector Installation Process.

**On-Premises Architecture**

Workspace ONE UEM is composed of separate services that can be installed on a single- or multiple-server architecture to meet security and load requirements. Service endpoints can be spread across different security zones, with those that require external, inbound access located in a DMZ and the administrative console located in a protected, internal network, as shown in the following figure.

Syncing with internal resources such as Active Directory or a Certificate Authority can be achieved directly from the core components (Device Services and Admin Console) or using an AirWatch Cloud Connector. The separate connector can run within the LAN in outbound-only connection mode, meaning the connector receives no incoming connections from the DMZ.

The implementation is separated into the three main components:

- Workspace ONE UEM Admin Console
- Workspace ONE UEM Device Services
- AirWatch Cloud Connector

The AirWatch Cloud Messaging Service can be installed as part of the Workspace ONE UEM Device Services server, and the API Endpoint is installed as part of the Admin Console server. Depending on the scale of the environment, these can also be deployed on separate servers.
In addition to the components already described for this cloud-based architecture, there are additional components required for an on-premises deployment.

**Table 35: Additional On-Premises Workspace ONE UEM Components**

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Database        | Microsoft SQL Server database that stores Workspace ONE UEM device and environment data.  
All relevant application configuration data, such as profiles and compliance policies, persist and reside in this database. Consequently, the majority of the application’s backend workload is processed here. |
| Memcached Server| A distributed data caching application that reduces the workload on the Workspace ONE UEM database. This server is intended for deployments of more than 5,000 devices. |
An on-premises deployment of Workspace ONE UEM and the components required were architected, scaled, and deployed to support 50,000 devices, and additional growth over time without a redesign.

This provides validation of design and implementation of an on-premises instance of Workspace ONE UEM.

**Database**

All critical data and configurations for Workspace ONE UEM are stored in the database. This is the data tier of the solution. Workspace ONE UEM databases are based on the Microsoft SQL Server platform. Application servers receive requests from the console and device users and then process...
the data and results. No persistent data is maintained on the application servers (device and console services), but user and device sessions are maintained for a short time.

In this reference architecture, Microsoft SQL Server 2016 was used and its cluster offering Always On availability groups, which is supported with Workspace ONE UEM. This allows the deployment of multiple instances of each of the Workspace ONE UEM components, pointing to the same database and protected by an availability group. An availability group listener is the connection target for all instances.

Windows Server Failover Clustering (WSFC) can also be used to improve local database availability and redundancy. In a WSFC cluster, two Windows servers are clustered together to run one instance of SQL Server, which is called a SQL Server failover cluster instance (FCI). Failover of the SQL Server services between these two Windows servers is automatic.

Workspace ONE UEM runs on an external SQL database. Prior to running the Workspace ONE UEM database installer, you must have your database administrator prepare an empty external database and schema. Licensed users can use a Microsoft SQL Server 2012, SQL Server 2014, or SQL Server 2016 database server to set up a high-availability database environment.

For guidance on hardware sizing for Microsoft SQL Servers, see On-Premises Recommended Architecture Hardware Sizing.

**Table 37: Implementation Strategy for the On-Premises Workspace ONE UEM Database**

| Decision | An external Microsoft SQL database was implemented for this design. |
| Justification | An external SQL database is recommended for production and allows for scale and redundancy. |

**Memcached**

Memcached is a distributed data-caching application available for use with Workspace ONE UEM environments. It reduces the workload on the database. Memcached replaces the previous caching solution, AW Cache, and is recommended for deployments of more than 5,000 devices.

Once enabled in the Workspace ONE UEM Console, Memcached begins storing system settings and organization group tree information as they are accessed by Workspace ONE UEM components. When a request for data is sent, Workspace ONE UEM automatically checks for the results stored in memory by Memcached before checking the database, thereby reducing the database workload. If this process fails, results data is retrieved from the database and stored in Memcached for future queries. As new values are added and existing values are changed, the values are written to both Memcached and the database.

**Note:** All key/value pairs in Memcached expire after 24 hours.

You can deploy multiple Memcached servers, with each caching a portion of the data, to mitigate against a single server failure degrading the service. With two servers, 50 percent of the data resides on server 1 and 50 percent on server 2, with no replication across servers. A hash table tells the services what data is stored on which server.
If server 1 experiences an outage for any reason, only 50 percent of the cache is impacted. The tables are rebuilt on the second server as services failover to the database and look to cache those gathered items.

For guidance on hardware sizing for Memcached servers, see On-Premises Recommended Architecture Hardware Sizing.

**Table 38: Implementation Strategy for Memcached Servers**

<table>
<thead>
<tr>
<th>Decision</th>
<th>Two Memcached servers were deployed in the internal network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Memcached servers are recommended for environments with more than 5,000 devices. Memcached servers reduce the load on the SQL database.</td>
</tr>
</tbody>
</table>

**Load Balancing**

To remove a single point of failure, you can deploy more than one instance of the different Workspace ONE UEM components behind an external load balancer. This strategy 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 a high-availability (HA) or master/slave configuration.

The AirWatch Cloud Connector traffic is load-balanced by the AirWatch Cloud Messaging component. It does not require a separate load balancer. Multiple AirWatch Cloud Connectors in the same organization group that connect to the same cloud messaging server for high availability can all expect to receive traffic (an active-active configuration). How traffic is routed is determined by the component and depends on the current load.

For more information on load balancing recommendations and HA support for the different Workspace ONE UEM components, see On-Premises Architecture Load Balancer Considerations and High Availability Support for Workspace ONE UEM Components.

**Scalability and Availability**

Workspace ONE UEM core components can be deployed in a single, shared server design, but this is really only recommended for proof-of-concept engagements. For production use, to satisfy load demands and to meet most network architecture designs, the core application components are usually installed on two separate, dedicated servers (Admin Console and Device Services).

For a high-availability environment and to meet load demands of large deployments, multiple instances of each of these components can be deployed on dedicated servers behind a load balancer.
Four instances of the Workspace ONE UEM Device Services servers were deployed in the DMZ.

Three servers are required to handle the load and supporting 50,000 devices. A fourth server is added for redundancy.

These servers will include the following components: Workspace ONE UEM Device Services.

Three instances of the Workspace ONE UEM Console servers were installed in the internal network.

Two servers are required based on load and based on supporting 50,000 devices. A third server is added for redundancy.

These servers include the following component: Workspace ONE UEM Admin Console.

In larger environments, which generally include 50,000 devices or more, the API and AWCM services should also be located on separate, dedicated servers to remove their load from the Device Services and Admin Console servers.

Two instances of the AWCM servers were deployed in the internal network.

To support deployments of 50,000 devices and more, VMware recommends that you separate the AWCM function from the Device Services function.

Two instances of the API servers were deployed in the internal network.

To support deployments of 50,000 devices and more, VMware recommends use separate servers for the API server and Device Services.

Multiple instances of the AirWatch Cloud Connector (ACC) can be deployed in the internal network for a high-availability environment. The load for this service is balanced without the need for an external load balancer.

Three instances of the AirWatch Cloud Connector were deployed.

Two ACC instances are required based on load, and a third is added for redundancy.
Workspace ONE UEM can be scaled horizontally to meet demands regardless of the number of devices. For server numbers, hardware sizing, and recommended architectures for deployments of varying sizes, see On-Premises Recommended Architecture Hardware Sizing. Note that the guide shows only the number of application server components required for each sizing scenario to cope with the load demand. It does not include additional servers in those numbers to account for redundancy.

Due to the amount of data flowing in and out of the Workspace ONE UEM database, proper sizing of the database server is crucial to a successful deployment. For guidance on sizing the database server resources, CPU, RAM, and disk IO requirements, see On-Premises Recommended Architecture Hardware Sizing.

This reference architecture is designed to accommodate up to 50,000 devices, allowing additional growth over time without a redesign. Multiple nodes of each of the components (Device Services, Admin Consoles, API servers, AWCM servers, AirWatch Cloud Connectors) are recommended to meet the demand. To guarantee the resilience of each service within a single site, additional application servers are added. For example, four Device Services nodes are used instead of the three that would be required to meet only the load demand.
This figure shows a scaled environment suitable for up to 50,000 devices. It will also allow additional growth over time without a redesign because it uses dedicated API servers and AWCM servers.

- Workspace ONE UEM Devices Services servers are located in the DMZ, and a load balancer distributes the load.
- Workspace ONE UEM Admin Console Services, Memcached, AWCM servers, and API servers are hosted in the internal network with a load balancer in front of them.
- AirWatch Cloud Connector servers are hosted in the internal network and can use an out-bound-only connection without the need for an external load balancer.
For this reference architecture, split DNS was used; that is, the same fully qualified domain name (FQDN) was used both internally and externally for user access to the Workspace ONE UEM Device Services server. Split DNS is not a strict requirement for a Workspace ONE UEM on-premises deployment but it does improve the user experience.

**Multi-site Design**

Workspace ONE UEM servers are the primary endpoint for management and provisioning of end user devices. These servers should be deployed to be highly available within a site and deployed in a secondary data center for failover and redundancy. A robust back-up policy for application servers and database servers can minimize the steps required for restoring a Workspace ONE UEM environment in another location.

You can configure disaster recovery (DR) for your Workspace ONE UEM solution using whatever procedures and methods meet your DR policies. Workspace ONE UEM has no dependency on your DR configuration, but we strongly recommend that you develop some type of failover procedures for DR scenarios. Workspace ONE UEM components can be deployed to accommodate most of the typical disaster recovery scenarios.

Workspace ONE UEM consists of the following core components, which need to be designed for redundancy:

- Workspace ONE UEM Device Services
- Workspace ONE UEM Admin Console
- Workspace ONE UEM AWCM server
- Workspace ONE UEM API server
- AirWatch Cloud Connector
- Memcached server
- SQL database server

**Table 44**: Site Resilience Strategy for Workspace ONE UEM

<table>
<thead>
<tr>
<th>Decision</th>
<th>A second site was set up with Workspace ONE UEM.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This strategy provides disaster recovery and site resilience for the on-premises implementation of Workspace ONE UEM.</td>
</tr>
</tbody>
</table>

**Workspace ONE UEM Application Servers and AirWatch Cloud Connectors**

To provide site resilience, each site requires its own group of Workspace ONE UEM application and connector servers to allow the site to operate independently, without reliance on another site. One site runs as an active deployment, while the other has a passive deployment.

Within each site, sufficient application servers must be installed to provide local redundancy and withstand the load on its own. The Device Services servers are hosted in the DMZ, while the Admin Console server resides in the internal network. Each site has a local load balancer that distributes the load between the local Device Services servers, and a failure of an individual server is handled with no outage to the service or requirement to fail over to the backup site.
A global load balancer is used in front of each site's load balancer.

At each site, AirWatch Cloud Connector servers are hosted in the internal network and can use an outbound-only connection.

For recommendations on server quantities and hardware sizing of Device Services and Admin Console servers, see On-Premises Recommended Architecture Hardware Sizing.

Table 45: Disaster Recovery Strategy for Workspace ONE UEM Application Servers

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A second set of servers was installed in a second data center. The number and function of the servers was the same as sized for the primary site.</td>
<td>This strategy provides full disaster recovery capacity for all Workspace ONE UEM on-premises services.</td>
</tr>
</tbody>
</table>

Multi-site Console Servers

When deploying multiple Console servers, certain Workspace ONE UEM services must be active on only one primary Console server to ensure maximum performance. These services must be disabled on non-primary servers after Workspace ONE UEM installation is complete.

Workspace ONE UEM services that must be active on only one server are:

- AirWatch Device Scheduler
- AirWatch GEM Inventory Service
- Directory Sync
- Content Delivery Service

When you upgrade the Workspace ONE UEM Console servers, the Content Delivery Service automatically restarts. You must then manually disable the applicable services again on all extra servers to maintain best performance.

Multi-site Database

As previously stated, Workspace ONE UEM supports Microsoft SQL Server 2012 (and later) and its cluster offering Always On availability groups. This allows the deployment of multiple instances of Device Services servers and Workspace ONE UEM Console servers that point to the same database. The database is protected by an availability group, with an availability group listener as the single database connection target for all instances.

For this design, an active/passive database instance was configured using SQL Server Always On. This allows the failover to the secondary site if the primary site becomes unavailable. Depending on the configuration of SQL Server Always On, inter-site failover of the database can be automatic, though not instantaneous.

For this reference architecture, we chose an Always On implementation with the following specifications:

- No shared disks were used.
- The primary database instance ran in Site 1 during normal production.
Within a site, Windows Server Failover Clustering (WSFC) was used to improve local database availability and redundancy. In a WSFC cluster, two Windows servers are clustered together to run one instance of SQL Server, which is called a SQL Server failover cluster instance (FCI). Failover of the SQL Server services between these two Windows servers is automatic. For details of the implementation we used, see "Appendix D: Workspace ONE UEM Configuration for Multi-site Deployments" on page 392.

**Table 46**: Strategy for Multi-site Deployment of the On-Premises Database

<table>
<thead>
<tr>
<th>Decision</th>
<th>A Microsoft SQL Always-On database was used.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This strategy provides replication of the database from the primary site to the recovery site and allows for recovery of the database functionality.</td>
</tr>
</tbody>
</table>

**Failover to a Second Site**

A Workspace ONE UEM multi-site design allows administrators to maintain constant availability of the different Workspace ONE UEM services in case a disaster renders the original active site unavailable. The following diagram shows a sample multi-site architecture.

**Figure 34**: On-Premises Multi-site Workspace ONE UEM Components

To achieve failover to a secondary site, manual intervention might be required for two main layers of the solution:

- **Database** – Depending on the configuration of SQL Server Always On, inter-site failover of the database can be automatic. If necessary, steps should be taken to manually control which site has the active SQL node.
• **Device Services** – The global load balancer controls which site traffic is directed to. During normal operation, the global load balancer directs traffic to the local load balancer in front of the Device Service servers in Site 1. In a failover scenario, the global load balancer should be changed to direct traffic to the equivalent local load balancer in Site 2.

• **Console servers** – When multiple Console servers are deployed, ensure the Workspace ONE UEM services mentioned in “Multi-site Console Servers” on page 73 are active only on the primary servers and are disabled on the non-primary servers for Site 2.

### Prerequisites

This section details the prerequisites for the Workspace ONE UEM configuration:

• **Network Configuration** – Verify that the following requirements are met:
  - Static IP address and DNS Forward (A) are used.
  - Inbound firewall port 443 is open so that external users can connect to the Workspace ONE UEM instance or the load balancer.

• **Active Directory** – Workspace ONE UEM supports Active Directory configurations on Windows 2008 R2, 2012, 2012 R2, and 2016, including:
  - Single AD domain
  - Multidomain, single forest
  - Multi-forest with trust relationships
  - Multi-forest with untrusted relationships (requires external connector configuration)
  - Active Directory Global Catalog optional for Directory Sync

For this reference architecture, Windows 2016 Active Directory was used.

### Installation and Initial Configuration

Workspace ONE UEM is delivered as separate installer for the database and application servers. The database installer must be run before installing any of the application servers. For more information on installing Workspace ONE UEM see the [VMware Workspace ONE UEM Installation Guide](#).

At a high level, the following tasks should be completed:

• **Database:**
  - Create the Workspace ONE UEM database.
  - Run the Workspace ONE UEM database installer.

• **Application Servers (Console, Device Services, API, and AWCM):**
  - Run the application installer on each application server.
  - Select the appropriate services for the component you are installing.
- Run the Secure Channel installer on each AWCM server, and restart the AWCM service after installation is complete.
- Install and configure the Memcached servers.
- Install the AirWatch Cloud Connector.
- Configure Active Directory:
  - Create a connection to Active Directory.
  - Select a bind account with permission to read from AD.
  - Choose groups and users to sync.
  - Initiate a directory sync.
- Configure email (SMTP) (if applicable) at the company organizational group level.
- Upload the SSL certificate for the iOS signing-profile certificate at the global organizational group level.
- Set up Apple Push Notification service (APNs) for iOS devices and a notification service for Android.

**Integration with VMware Identity Manager**

Integrating Workspace ONE UEM and VMware Identity Manager into your Workspace ONE environment provides several benefits. Workspace ONE uses VMware Identity Manager for authentication, SaaS, and VMware Horizon® application access. Workspace ONE uses Workspace ONE UEM for device enrollment and management.

The integration process between the two solutions is detailed in *Integrating Workspace ONE UEM With VMware Identity Manager*.

Also see "Platform Integration" on page 244 for more detail.

**Resource Types**

A Workspace ONE implementation can include the following types of application resources.

**Native Mobile Apps**

Native mobile apps from the Apple App Store, Google Play, and the Microsoft Windows Store have brought about new ways of easily accessing tools and information to make users more productive. A challenge has been making the available apps easy to find, install, and control. Workspace ONE UEM has long provided a platform for distribution, management, and security for these apps. Apps can be published from the app stores themselves, or internally developed apps can be uploaded to the Workspace ONE UEM service for distribution to end users.
Unified App Catalog

When Workspace ONE UEM and VMware Identity Manager are integrated so that apps from both platforms can be enabled for end users, the option to use the unified catalog in VMware Identity Manager is enabled. This catalog pulls entitlements from both platforms and displays them appropriately in the Workspace ONE native app on a mobile device. The Workspace ONE client determines which apps to display on which platform. For example, iOS apps appear only on devices running iOS, and Android apps appear only on Android devices.
With the Workspace ONE conditional access feature, administrators can create access policies that go beyond the evaluation of user identity and valid credentials. Combining Workspace ONE UEM and VMware Identity Manager, administrators can evaluate the target resource being accessed, the source network from which the request originated, and the type and compliance status of the device. With these criteria, access policies can provide a more sophisticated authentication challenge only when needed or deny access when secure conditions are not met.

Using the Workspace ONE UEM Console to Create Access Policies

Configuration of compliance starts in the Workspace ONE UEM Console. Compliance policies are created by determining:

1. A criterion to check, such as a jail-broken or rooted device
2. An action to take, such as an email to an administrator or a device wipe
3. An escalation to further actions if the device is not returned to compliance within a set time
4. An assignment to devices or users

Examples of rules are listed in the following table.
Table 47: Examples of Access Policy Rules

<table>
<thead>
<tr>
<th>Compliance Criterion</th>
<th>Policy Description</th>
</tr>
</thead>
</table>
| Application list     | A device is out of compliance with the policy for one or more of the following reasons:  
  - Blacklisted apps are installed on the device.  
  - Non-whitelisted apps are installed on the device.  
  - Required apps are not installed.  
  - The version of the installed app is different from the one defined in the policy. |
| Last compromised scan| A device complies with this policy if the device was last scanned for compliance within the timeframe defined in the policy. |
| Passcode             | A device complies with this policy if a passcode is set in the device by the user. A corresponding rule provides information on the passcode and encryption status of the device. |
| Device roaming        | A device is out of compliance with this policy if the device is roaming. |

Refer the section Compliance Policy Rules Descriptions for the complete list. Because not all the options apply to all the platforms, also see Compliance Policy Roles by Platform.

Using the Workspace ONE UEM REST API to Extend Device Compliance Parameters

With the Workspace ONE UEM REST API, the definition of a device’s compliance status can be extended beyond what is available within the Workspace ONE UEM Console by leveraging an integration with one or more partners from the extensive list of VMware Mobile Security Alliance (MSA) partners. For more information, see Mitigate Mobile Threats with Best-of-Breed Security Solutions.

To use the device posture from Workspace ONE UEM with VMware Identity Manager, you must enable the Device Compliance option when configuring the Workspace ONE UEM–VMware Identity Manager integration. The Compliance Check function must also be enabled.
After you enable the compliance check through Workspace ONE UEM, you can add a rule that defines what kind of compliance parameters are checked and what kind of authentication methods are used.

Figure 37: Enable Compliance Check

Figure 38: Device Compliance Policy
The device’s unique device identifier (UDID) must also be captured in Workspace ONE UEM and used in the compliance configuration. This feature works with mobile SSO for iOS, mobile SSO for Android, and certificate cloud deployment authentication methods.

**Note:** Before you use the Device Compliance authentication method, you must use a method that obtains the device UDID. Evaluating device compliance before obtaining the UDID does not result in a positive validation of the device's status.

**Multi-factor Authentication**

VMware Identity Manager supports chained, two-factor authentication. The primary authentication methods can be username and password or mobile SSO. You can combine these authentication methods with RADIUS, RSA Adaptive Authentication, and VMware Workspace ONE Verify as secondary authentication methods to achieve additional security for access control.

**Standalone MAM and Adaptive Management**

Workspace ONE supports a variety of device and application management approaches. Standalone mobile application management (MAM) allows a user to download the Workspace ONE app from public app stores and immediately take advantage of entitled apps and corporate-published native mobile apps. The benefits of this approach include:

- IT can distribute corporate-approved public mobile apps to unmanaged devices through the Workspace ONE app catalog.
- With the Workspace ONE app installed, users can use SSO to access other VMware apps, including Workspace ONE Web and VMware Workspace ONE® Content, or any custom app built using the Workspace ONE SDK.
- When an unmanaged device is out of compliance (for example, jail-broken), the system quickly takes action to protect company data. When a violation is detected, all company data is removed from the Workspace ONE app, Workspace ONE productivity apps (for example, Workspace ONE Content), and any custom app built using the Workspace ONE SDK.

**Triggering the Enrollment Process from the Workspace ONE App**

For applications that require a higher level of security assurance, users can enroll their device in Workspace ONE UEM directly from the Workspace ONE app, instead of downloading the Workspace ONE Intelligent Hub. All entitled apps are listed in the catalog. Apps that require enrollment are marked with a star icon. When the user tries to download an app with a star icon, the enrollment process is triggered. For example, users can download a conferencing app, such as WebEx, without enrollment. But they are prompted to enroll when they try to download, for example, Salesforce1, from the catalog.
Enabling Adaptive Management for iOS

Adaptive management is enabled on an application-by-application basis within the Workspace ONE UEM Console. Within an application profile, an administrator can choose to require management of a device prior to allowing use of that app.

This feature is supported only for Apple iOS and is now deprecated for Android. The new standard for app deployment with Android is through Android Enterprise, as described in the Application Management for Android part of the Workspace ONE UEM Integration with Android Platform.
Mobile Single Sign-On

One of the hallmark features of the Workspace ONE experience is mobile SSO technology, which provides the ability to sign in to the app once and gain access to all entitled applications, including SaaS apps. This core capability can help address security concerns and password-cracking attempts and vastly simplifies the end-user experience for a mobile user. A number of methods enable this capability on both VMware Identity Manager and Workspace ONE UEM. SAML becomes a bridge to the apps, but each native mobile platform requires different technologies to enable SSO.

Configuration of mobile SSO for iOS and Android devices can be found in the Guide to Deploying VMware Workspace ONE with VMware Identity Manager.

Mobile SSO for iOS

Kerberos-based SSO is the recommended SSO experience on managed iOS devices. VMware Identity Manager offers a built-in Kerberos adapter, which can handle iOS authentication without the need for device communication to your internal Active Directory servers. In addition, Workspace ONE UEM can distribute identity certificates to devices using a built-in Workspace ONE UEM Certificate Authority, eliminating the requirement to maintain an on-premises CA.

Alternatively, enterprises can use an internal key distribution center (KDC) for SSO authentication, but this typically requires the provisioning of an on-demand VPN. Either option can be configured in the Standard Deployment model, but the built-in KDC must be used in the Simplified Deployment model.
that is referenced in Implementing Mobile Single Sign-in Authentication for Workspace ONE UEM-Managed iOS Devices.

**Mobile SSO for Android**

Workspace ONE offers universal Android mobile SSO, which allows users to sign in to enterprise apps securely without a password. Android mobile SSO technology requires device enrollment and the use of Workspace ONE Tunnel to authenticate users against SaaS applications.

Refer to Implementing Mobile Single Sign-On Authentication for Managed Android Devices.

**Windows 10 and macOS SSO**

Certificate-based SSO is the recommended experience for managed Windows and Mac desktops and laptops. An Active Directory Certificate Services or other CA is required to distribute certificates. Workspace ONE UEM can integrate with an on-premises CA through AirWatch Cloud Connector or an on-demand VPN.

For guidance on Workspace ONE UEM integration with a Certificate Authority, see **Certificate Management**.

**Email Integration**

Workspace ONE offers a great number of choices when it comes to devices and email clients. Although this flexibility offers many choices of email clients, it also potentially exposes the enterprise to data leakage due to a lack of control after email messages reach the device.

Another challenge is that many organizations are moving to cloud-based email services, such as Microsoft Office 365 and G Suite (formerly Google Apps for Work). These services provide fewer email control options than the on-premises models that an enterprise might be accustomed to.

This section looks at the email connectivity models and the pros and cons of each.

**Workspace ONE UEM Secure Email Gateway Proxy Model**

The Workspace ONE UEM Secure Email Gateway proxy server is a separate server installed in-line with your existing email server to proxy all email traffic going to mobile devices. Based on the settings you define in the Workspace ONE UEM Console, the Workspace ONE UEM Secure Email Gateway proxy server allows or blocks email for every mobile device it manages, and it relays traffic only from approved devices. With some additional configuration, no devices are allowed to communicate directly with the corporate email server.
Direct PowerShell Model

In this model, Workspace ONE UEM adopts a PowerShell administrator role and issues commands to the Exchange ActiveSync infrastructure to permit or deny email access based on the policies defined in the Workspace ONE UEM Console. PowerShell deployments do not require a separate email proxy server, and the installation process is simpler. In the case of an on-premises Exchange server, AirWatch Cloud Connector (ACC) can be leveraged to prevent inbound traffic flow.
Supported Email Infrastructure and Models

Use the following table to compare these models and the mail infrastructures they support.

**Table 48: Supported Email Deployment Models**

<table>
<thead>
<tr>
<th>Deployment Model</th>
<th>Configuration Mode</th>
<th>Mail Infrastructure</th>
</tr>
</thead>
</table>
| Proxy model      | Workspace ONE UEM Secure Email Gateway (proxy) | • Microsoft Exchange 2010, 2013, and 2016  
                  |                                                              | • IBM Domino with Lotus Notes  
                  |                                                              | • Novel GroupWise (with EAS)  
                  |                                                              | • G Suite  
                  |                                                              | • Office 365 (For attachment encryption) |
| Direct model     | PowerShell model            | • Microsoft Exchange 2010, 2013, and 2016  
                  |                                                              | • Microsoft Office 365 |
| Direct model     | Google model                | G Suite |

Microsoft Office 365 requires additional configuration for the Workspace ONE UEM Secure Email Gateway proxy model. VMware recommends the direct model of integration with cloud-based email servers unless encryption of attachments is required.

The following table summarizes the pros and cons of the deployment features of Workspace ONE UEM Secure Email Gateway and PowerShell to help you choose which deployment is most appropriate.
**Table 49: Workspace ONE UEM Secure Email Gateway and PowerShell Feature Comparison**

<table>
<thead>
<tr>
<th>Model</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
</table>
| Workspace ONE UEM Secure Email Gateway | - Real-time compliance  
- Attachment encryption  
- Hyperlink transformation | - Additional servers needed  
- Office 365 must be federated with Workspace ONE to prevent users from directly connecting to Office 365 |
| PowerShell | No additional on-premises servers required for email management | - No real-time compliance sync  
- Not recommended for deployments larger than 100,000 devices  
- VMware Workspace ONE® Boxer is required to containerize attachments and hyperlinks in Workspace ONE Content and Workspace ONE Web |

**Key Design Considerations**

VMware recommends using Workspace ONE UEM Secure Email Gateway for all on-premises email infrastructures with deployments of more than 100,000 devices. For smaller deployments or cloud-based email, PowerShell is another option.

For more information on design considerations for mobile email management, see the most recent *Workspace ONE UEM Mobile Email Management Guide*.

**Table 50: Email Deployment Model for This Reference Architecture**

| Decision | The PowerShell model was used with Workspace ONE Boxer. |
| Justification | This design includes Microsoft Office 365 email. Although this decision limits employee choice of mail client and removes native email access in the Mobile Productivity service, it provides the best protection available against data leakage. |

**Next Steps**

- Configure Microsoft Office 365 email through PowerShell.
- Configure Workspace ONE Boxer as an email client for deployment as part of device enrollment.

**Conditional Access Configured for Microsoft Office 365 Basic Authentication**

By default, Microsoft Office 365 basic authentication is vulnerable because credentials are entered in the app itself rather than being submitted to an identity provider (IdP) in a browser, as with modern
You can now control access to Office 365 active flows based on the following access policies in VMware Identity Manager:

- Network range
- Device OS type
- Group membership
- Email protocol
- Client name

![Edit SaaS Application](image)

**Figure 43:** Microsoft Office 365 Active Flow Conditional Access Policies

### Content Integration

Mobile content management (MCM) can be critical to device deployment, ensuring that content is safely stored in enterprise repositories and available to end users when and where they need it with the appropriate security controls. The MCM features in Workspace ONE UEM provide users with the content they need while also providing the enterprise with the security control it requires.

### Content Management Overview

1. **Workspace ONE UEM managed content repository** – Workspace ONE UEM administrators with the appropriate permissions can upload content to the repository and have complete control over the files that are stored in it.
   The synchronization process involves two components:
- **VMware Content Gateway** – This on-premises node provides secure access to content repositories or internal file shares. You can deploy it as a service on a VMware Unified Access Gateway™ virtual appliance. This gateway supports both cascade mode (formally known as relay-endpoint) and basic (formally known as endpoint-only) deployment models.

- **Corporate file server** – This preexisting repository can reside within an organization’s internal network or on a cloud service. Depending on an organization’s structure, the Workspace ONE UEM administrator might not have administrative permissions for the corporate file server.

2. **VMware Workspace ONE Content** – After this app is deployed to end-user devices, users can access content that conforms to the configured set of parameters.

![Figure 44: Mobile Content Management with Workspace ONE UEM](image)

You can integrate Workspace ONE Content with a large number of corporate file services, including Box, Google Drive, network shares, various Microsoft services, and most websites that support Web Distributed Authoring and Versioning (WebDAV). It is beyond the scope of this document to list all of them.

For full design considerations for mobile content management, see the most recent Workspace ONE UEM Mobile Content Management.

**Content Gateway**

VMware Content Gateway provides a secure and effective method for end users to access internal repositories. Users are granted access only to their approved files and folders based on the access control lists defined in the internal repository through Workspace ONE Content. To prevent security vulnerabilities, Content Gateway servers support only Server Message Block (SMB) v2.0 and SMBv3.0. SMBv2.0 is the default. Content Gateway offers basic and cascade mode (formally known as relay-endpoint) architecture models for deployment.
Content Gateway can be deployed as a service within VMware Unified Access Gateway 3.3.2 and later. For guidance on deployment and configuration of Content Gateway service, see Content Gateway on Unified Access Gateway.

For step-by-step instructions, see Configuring Content Gateway Edge Services on Unified Access Gateway.

**Scalability**

Unified Access Gateway can be used to provide edge and gateway services for VMware Content Gateway and VMware Tunnel functionality. For architecture and sizing guidance, see "Component Design: Unified Access Gateway Architecture" on page 207.

**Data Protection in Workspace ONE Content**

Workspace ONE Content provides considerable control over the types of activities that a user can perform with documents that have been synced to a mobile device. Applications must be developed using Workspace ONE SDK features or must be wrapped to use these restrictions. The following table lists the data loss prevention features that can be controlled.

**Table 51: Data Loss Prevention Features**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Copy and Paste</td>
<td>Allows an application to copy and paste on devices</td>
</tr>
<tr>
<td>Enable Printing</td>
<td>Allows an application to print from devices</td>
</tr>
<tr>
<td>Enable Camera</td>
<td>Allows applications to access the device camera</td>
</tr>
<tr>
<td>Enable Composing Email</td>
<td>Allows an application to use the native email client to send email</td>
</tr>
<tr>
<td>Enable Data Backup</td>
<td>Allows wrapped applications to sync data with a storage service such as iCloud</td>
</tr>
<tr>
<td>Enable Location Services</td>
<td>Allows wrapped applications to receive the latitude and longitude of the device</td>
</tr>
<tr>
<td>Enable Bluetooth</td>
<td>Allows applications to access Bluetooth functionality on devices</td>
</tr>
<tr>
<td>Enable Screenshot</td>
<td>Allows applications to access screenshot functionality on devices</td>
</tr>
</tbody>
</table>
Table 51: Data Loss Prevention Features (Continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Watermark</td>
<td>Displays text in a watermark in documents in the Workspace ONE Content</td>
</tr>
<tr>
<td>Limit Documents to Open Only in</td>
<td>Controls the applications used to open resources on devices</td>
</tr>
<tr>
<td>Approved Apps</td>
<td></td>
</tr>
<tr>
<td>Allowed Applications List</td>
<td>Lists the applications that are allowed to open documents</td>
</tr>
</tbody>
</table>

Key Design Considerations

Because this environment is configured with Microsoft Office 365, SharePoint-based document repositories are configured as part of the Workspace ONE Content implementation. Data loss prevention (DLP) controls are used in the Mobile Productivity service and Mobile Application Workspace profiles to protect corporate information.

Table 52: Implementation Strategy for Providing Content Gateway Services

<table>
<thead>
<tr>
<th>Decision</th>
<th>Unified Access Gateway was used to provide Content Gateway services.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Unified Access Gateway was chosen as the standard edge gateway appliance for</td>
</tr>
<tr>
<td></td>
<td>Workspace ONE services, including VMware Horizon and content resources.</td>
</tr>
</tbody>
</table>

VMware Tunnel

VMware Tunnel leverages unique certificates deployed from Workspace ONE UEM to authenticate and encrypt traffic from the mobile device to resources on the internal network. It consists of following two components:

1. **Proxy** – This component secures the traffic between the mobile device and the backend resources through the Workspace ONE Web application. To leverage the proxy component with an internally developed app, you must embed the Workspace ONE SDK in the app. The proxy component, when deployed, supports SSL offloading.

2. **Per-App Tunnel** – This component allows certain applications on your device to communicate with your backend resources. This restricts access to unwanted applications, unlike the device-level VPN. The Per-App Tunnel supports TCP, UDP and HTTP(S) traffic and works for both public and internally developed apps. It requires the Workspace ONE Tunnel application to be installed and managed by Workspace ONE UEM.

   **Note:** The Per-App Tunnel does not support SSL offloading.

VMware Tunnel Service Deployment

The VMware Tunnel service can be deployed as a service within VMware Unified Access Gateway 3.3.2 and later as the preferred method, or as a standalone Linux server, both deployments support
the Proxy and the Per-App Tunnel modules.

For guidance on deployment and configuration of the VMware Tunnel service, see Deploying VMware Tunnel on Unified Access Gateway. For step-by-step instructions, see Configuring VMware Tunnel Edge Services on Unified Access Gateway.

**Architecture**

The Per-App Tunnel component is recommended because it provides most of the functionality with easier installation and maintenance. It leverages native APIs offered by Apple, Google, and Windows to provide a seamless end-user experience and does not require additional configuration as the Proxy model does.

The VMware Tunnel service can reside in:

- DMZ (single-tier, basic mode)
- DMZ and internal network (multi-tier, cascade mode)

Both configurations support load balancing and high availability.

![Figure 45: VMware Tunnel and Content Deployment Modes](image)

For guidance on Deployment modes, see Deploying VMware Tunnel on Unified Access Gateway.

**Scalability**

Unified Access Gateway can be used to provide edge and gateway services for VMware Content Gateway and VMWare Tunnel functionality. For architecture and sizing guidance, see "Component Design: Unified Access Gateway Architecture" on page 207.
Installation

For installation prerequisites, see System Requirements for Deploying VMware Tunnel with Unified Access Gateway.

After the installation is complete, configure the VMware Tunnel by following the instructions in VMware Tunnel Core Configuration.

Table 53: Strategy for Providing Tunnel Services

<table>
<thead>
<tr>
<th>Decision</th>
<th>Unified Access Gateway was used to provide tunnel services.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Unified Access Gateway was chosen as the standard edge gateway appliance for Workspace ONE services, including VMware Horizon and content resources.</td>
</tr>
</tbody>
</table>

Data Loss Prevention

Applications built using the Workspace ONE SDK or wrapped by the Workspace ONE UEM App Wrapping engine can integrate with the SDK settings in the Workspace ONE UEM Console to apply policies, control security and user behavior, and retrieve data for specific mobile applications without changing the application itself. The application can also take advantage of controls designed to make accidental, or even purposeful, distribution of sensitive information more difficult. DLP settings include the ability to disable copy and paste, prevent printing, disable the camera or screenshot features, or require adding a watermark to content when viewed on a device. You can configure these features at a platform level with iOS- or Android-specific profiles applied to all devices, or you can associate a specific application for which additional control is required.

Workspace ONE UEM applications, including Workspace ONE Boxer and Workspace ONE Content, are built to the Workspace ONE SDK, conform to the Workspace ONE platform, and can natively take advantage of these capabilities. Other applications can be wrapped to include such functionality, but typically are not enabled for it out of the box.
Another set of policies can restrict actions a user can take with email. For managed email clients such as Workspace ONE Boxer, restrictions can be set to govern copy and paste, prevent attachments from being accessed, or force all hyperlinks in email to use a secure browser, such as Workspace ONE Web.
VMware Boxer - Add Assignment

<table>
<thead>
<tr>
<th>Data Loss Prevention</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Paste</td>
<td>restricted</td>
</tr>
<tr>
<td>Hyperlinks</td>
<td>restricted</td>
</tr>
<tr>
<td>Sharing</td>
<td>preview only</td>
</tr>
<tr>
<td>Caller ID</td>
<td>restricted</td>
</tr>
</tbody>
</table>

When Restricted, all hyperlinks will open only in VMware Browser.

Figure 47: Workspace ONE Boxer Content Restriction Settings
Component Design: VMware Identity Manager Architecture

VMware Identity Manager™ is a key component of VMware Workspace ONE®. Among the capabilities of VMware Identity Manager are:

- **Simple application access for end users** – Provides access to different types of applications, including internal web applications, SaaS-based web applications (such as Salesforce, Dropbox, Concur, and more), native mobile apps, native Windows and macOS apps, VMware ThinApp® packaged applications, VMware Horizon®-based applications and desktops, and Citrix-based applications and desktops, all through a unified application catalog.

- **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 that the right users have access to the right applications. Users can customize the Bookmarks tab for fast, easy access to frequently used applications, and place the apps in a preferred order. IT can optionally push entries onto the Bookmarks tab using automated application entitlements.

- **Enterprise single sign-on (SSO)** – Simplifies business mobility with an included Identity Provider (IdP) or integration with existing on-premises identity providers so that you can aggregate SaaS, native mobile, and Windows 10 apps into a single catalog. Users have a single sign-on experience regardless of whether they log in to an internal, external, or virtual-based application.

- **Conditional access** – Includes a comprehensive policy engine that allows the administrator to set different access policies based on the risk profile of the application. An administrator can use criteria such as network range, user group, application type, method of authentication, or device operating system to determine if the user should have access or not.

In addition, VMware Identity Manager has the ability to validate the compliance status of the device in VMware Workspace ONE® UEM (powered by AirWatch). Failure to meet the compliance standards blocks a user from signing in to an application or accessing applications in the catalog until the device becomes compliant.

- **Enterprise identity management with adaptive access** – Establishes trust between users, devices, and applications for a seamless user experience and powerful conditional access controls that leverage Workspace ONE UEM device enrollment and SSO adapters.

- **Workspace ONE native mobile apps** – Includes native apps for iOS, Android, macOS, and Windows 10 to simplify finding, installing enterprise apps, and providing an SSO experience across resource types.

- **VMware Horizon / Citrix** – VMware Identity Manager can also be integrated with VMware Horizon, VMware Horizon® Cloud Service™, and Citrix published applications and desktops. The VMware Identity Manager handles authentication and provides SSO services to applications and desktops.
To leverage the breadth of the Workspace ONE experience, you must integrate Workspace ONE UEM and VMware Identity Manager into Workspace ONE. After integration, Workspace ONE UEM can use VMware Identity Manager for authentication and access to SaaS and VMware Horizon applications. Workspace ONE can use Workspace ONE UEM for device enrollment and management.

See the Guide to Deploying VMware Workspace ONE with VMware Identity Manager for more details.

VMware Identity Manager can be implemented using either an on-premises or a cloud-based (SaaS) implementation model.

To avoid repetition, an overview of the product, its architecture, and the common components are described in the cloud-based architecture section, which follows. The on-premises architecture section then adds to this information if your preference is to build on-premises.

Although VMware Identity Manager offers flexibility in terms of implementation options, our design decisions were based on the most current best practices, which include using the Windows version of the VMware Identity Manager Connector and the Linux virtual appliance for VMware Identity Manager service.

Table 54: Strategy of Using Both Deployment Models

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both a cloud-based and an on-premises VMware Identity Manager deployment were carried out separately.</td>
<td>This strategy allows both architectures to be validated and documented independently.</td>
</tr>
<tr>
<td>Both deployments were sized for 50,000 users.</td>
<td></td>
</tr>
</tbody>
</table>
Cloud-Based Architecture

In a cloud-based implementation, the VMware Identity Manager Connector service synchronizes user accounts from Active Directory to the VMware Identity Manager tenant service. Applications can then be accessed from a cloud-based entry point.

![Cloud-based VMware Identity Manager Logical Architecture](image)

**Figure 49**: Cloud-based VMware Identity Manager Logical Architecture

The main components of a cloud-based VMware Identity Manager implementation are described in the following table.

**Table 55**: VMware Identity Manager Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Identity Manager tenant</td>
<td>Hosted in the cloud and runs the main VMware Identity Manager service.</td>
</tr>
<tr>
<td>VMware Identity Manager Connector</td>
<td>Responsible for directory synchronization and authentication between on-premises resources such as Active Directory, VMware Horizon, Citrix, and the VMware Identity Manager service. You can deploy the connector by running the Windows-based installer.</td>
</tr>
</tbody>
</table>

**Table 56**: Implementation Strategy for Cloud-Based VMware Identity Manager

<table>
<thead>
<tr>
<th>Decision</th>
<th>A cloud-based deployment of VMware Identity Manager and the components required were architected for 50,000 users.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This strategy provides validation of design and implementation of a cloud-based instance of VMware Identity Manager.</td>
</tr>
</tbody>
</table>
VMware Identity Manager Tenant Installation and Initial Configuration

Because the VMware Identity Manager tenant is cloud-based, you do not have to make design decisions with regards to database, network access, or storage considerations. The VMware Identity Manager service scales to accommodate virtually any size of organization.

Connectivity to the VMware Identity Manager service is through outbound port 443. This connection is used for directory synchronization, authentication, and syncing entitlements for resources, such as Horizon desktops and apps. Organizations can take advantage of this configuration with no additional inbound firewall ports opened to the Internet.

Initial configuration involves logging in to the VMware Identity Manager service with the provided credentials at a URL similar to https://<company>.vmwareidentity.com.

For more details, see VMware Identity Manager Cloud Deployment.

VMware Identity Manager Connector

The VMware Identity Manager Connector can synchronize resources such as Active Directory, Horizon Cloud, VMware Horizon and Citrix virtual apps and desktops. The connector enables other typical on-premises resources such as RSA SecurID, RSA Adaptive Authentication, RADIUS, and Active Directory Kerberos authentication. The connector typically runs inside the LAN and connects to the hosted VMware Identity Manager service using an outbound-only connection. This means there is no need to expose the connector to the Internet.

Deploying a VMware Identity Manager Connector provides the following capabilities:

- Synchronization with an enterprise directory (Active Directory/LDAP) to import directory users to Workspace ONE components
- VMware Identity Manager Connector–based authentication methods such as username and password, certificate, RSA Adaptive Authentication, RSA SecurID, RADIUS, and Active Directory Kerberos authentication for internal users
- Integration with the following resources:
  - On-premises Horizon desktop and application pools
  - Horizon Cloud Service desktops and applications
  - Citrix-published desktops and applications

Table 57: Implementation Strategy for the VMware Identity Manager Connector

<table>
<thead>
<tr>
<th>Decision</th>
<th>The VMware Identity Manager Connector was deployed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This strategy supports the requirements of VMware Identity Manager directory integration and allows a wide range of authentication methods. This connector also enables synchronization of resources from VMware® Horizon 7 and Horizon Cloud Service into the Workspace ONE catalog.</td>
</tr>
</tbody>
</table>
Connector Sizing and Availability

VMware Identity Manager Connector can be set up for high availability and failover by adding multiple connector instances in a cluster. If one of the connector instances becomes unavailable for any reason, other instances will still be available.

To create a cluster, you install new connector instances and configure the authentication methods in exactly the same way as you set up the first connector. You then associate all the connector instances with the built-in identity provider. The VMware Identity Manager service automatically distributes traffic among all the connectors associated with the built-in identity providers so that you do not need an external load balancer. If one of the connectors becomes unavailable, the service does not direct traffic to it until connectivity is restored.

See Configuring High Availability for the VMware Identity Manager Connector for more detail.

Note: Active Directory Kerberos authentication has different requirements than other authentication methods with regards to clustering the VMware Identity Manager Connector. See Adding Kerberos Authentication Support to Your VMware Identity Manager Connector Deployment for more detail.

After you set up the connector cluster, the authentication methods that you have enabled on the connectors are highly available. If one of the connector instances becomes unavailable, authentication is still available. However, directory sync can be enabled on only one connector at a time, and you must modify the directory settings in the VMware Identity Manager service to use another connector instance instead of the original connector instance. For instructions, see Enabling Directory Sync on Another Connector in the Event of a Failure.

Sizing guidance and the recommended number of VMware Identity Manager Connectors are given in the System Requirements for VMware Identity Manager Connector (Windows) section of the online documentation.

Table 58: Strategy for Scaling the VMware Identity Manager Connector Service

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two instances of VMware Identity Manager Connectors were deployed in the internal network.</td>
<td>Two connectors are recommended to support an environment with 50,000 users.</td>
</tr>
</tbody>
</table>

VMware Identity Manager Connector Installation and Configuration

For prerequisites, including system and network configuration requirements, see Preparing to Install the VMware Identity Manager Connector on Windows.

For installation instructions, see Installing the VMware Identity Manager Connector on Windows.

Be sure to configure the VMware Identity Manager Connector authentication methods in outbound-only mode. This removes any requirement for organizations to change their inbound firewall rules and configurations. See Enable Outbound Mode for the VMware Identity Manager Connector.

On-Premises Architecture

For the on-premises deployment, we use the Linux-based virtual appliance version of the VMware Identity Manager service. This appliance is often deployed to the DMZ. There are use cases for LAN deployment, but they are rare, and we focus on the most common deployment method in this guide.
Syncing resources such as Active Directory, Citrix apps and desktops, and Horizon desktops and published apps is done by using a separate VMware Identity Manager Connector. The VMware Identity Manager Connector runs inside the LAN using an outbound-only connection to the VMware Identity Manager service, meaning the connector receives no incoming connections from the DMZ or from the Internet.

**Figure 50**: On-Premises VMware Identity Manager Logical Architecture

**Table 59**: Strategy for an On-Premises Deployment of VMware Identity Manager

<table>
<thead>
<tr>
<th>Decision</th>
<th>An on-premises deployment of VMware Identity Manager and the components required were architected, scaled, and deployed for 50,000 users.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This strategy provides validation of design and implementation of an on-premises instance of VMware Identity Manager.</td>
</tr>
</tbody>
</table>

The implementation is separated into the three main components.
Table 60: VMware Identity Manager Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Identity Manager appliance</td>
<td>Runs the main VMware Identity Manager service.</td>
</tr>
<tr>
<td>VMware Identity Manager Connector</td>
<td>Performs directory synchronization and authentication between on-premises resources such as Active Directory, VMware Horizon, and the VMware Identity Manager service. You deploy the connector by running a Windows-based installer.</td>
</tr>
<tr>
<td>Database</td>
<td>Stores and organizes server-state data and user account data.</td>
</tr>
</tbody>
</table>

**Database**

VMware Identity Manager can be set up with an internal or external database to store and organize server data and user accounts. A PostgreSQL database is embedded in the VMware Identity Manager virtual appliance, but this internal database is not recommended for use with production deployments.

To use an external database, have your database administrator prepare an empty external database and schema before you use the VMware Identity Manager web-based setup wizard to connect to the external database. Licensed users can use an external Microsoft SQL Server 2012, 2014, or 2016 database server to set up a high-availability external database environment. For more information, see Create the VMware Identity Manager Service Database.

The database requires 100 GB of disk space for the first 100,000 users. Add another 10 MB disk space for each 1,000 users brought into the system, plus an additional 1 MB for each 1,000 entitlements. For example, if you had 5,000 users and each user was entitled to 5 apps, you would have 25,000 entitlements in total. Therefore, the additional space required would be 50 MB + 25 MB = 75 MB.

For more guidance on hardware sizing for Microsoft SQL Servers, see System and Network Configuration Requirements.

Table 61: Implementation Strategy for the On-Premises VMware Identity Manager Database

<table>
<thead>
<tr>
<th>Decision</th>
<th>An external Microsoft SQL database was implemented for this design.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>An external SQL database is recommended for production because it provides scalability and redundancy.</td>
</tr>
</tbody>
</table>

**Scalability and Availability**

VMware Identity Manager has been tested to 100,000 users per single virtual appliance installation. To achieve failover and redundancy, deploy multiple VMware Identity Manager virtual appliances in a
cluster. If one of the appliances has an outage, VMware Identity Manager will still be available.

A cluster is recommended to contain three VMware Identity Manager service appliance nodes to avoid split-brain scenarios. See Recommendations for VMware Identity Manager Cluster for more information. After initial configuration, the first virtual appliance is cloned twice and deployed with new IP addresses and host names.

In this reference architecture, Microsoft SQL Server 2016 was used along with its cluster offering Always On availability groups, which is supported with VMware Identity Manager. This allows the deployment of multiple instances of VMware Identity Manager service appliances, pointing to the same database and protected by an availability group. An availability group listener is the single Java Database Connectivity (JDBC) target for all instances.

Windows Server Failover Clustering (WSFC) can also be used to improve local database availability and redundancy. In a WSFC cluster, two Windows servers are clustered together to run one instance of SQL Server, which is called a SQL Server failover cluster instance (FCI). Failover of the SQL Server services between these two Windows servers is automatic.

Figure 51: On-Premises Scaled VMware Identity Manager Architecture

For more information on how to set up VMware Identity Manager in a high-availability configuration, see Using a Load Balancer or Reverse Proxy to Enable External Access to VMware Identity Manager
and Configuring Failover and Redundancy in a Single Datacenter in "Appendix C: VMware Identity Manager Configuration for Multi-site Deployments" on page 371.

For guidance on server quantities and hardware sizing of VMware Identity Manager servers and VMware Identity Manager Connectors, see System and Network Configuration Requirements.

For more information about port requirements, see Deploying VMware Identity Manager in the DMZ.

**Network Latency**

There are multiple connectivity points between VMware Identity Manager service nodes, connectors, and the backend identity store (that is, AD domain controllers). The maximum latency between nodes and components, within a site cluster, must not exceed 4 ms (milliseconds).

**Table 62: Latency Requirements for Various VMware Identity Manager Connections**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Latency Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Identity Manager service nodes</td>
<td>Microsoft SQL Server</td>
<td>&lt;= 4 ms</td>
</tr>
<tr>
<td>VMware Identity Manager service nodes</td>
<td>VMware Identity Manager Connector</td>
<td>&lt;= 4 ms</td>
</tr>
<tr>
<td>VMware Identity Manager Connector</td>
<td>Domain controller (AD)</td>
<td>&lt;= 4 ms</td>
</tr>
</tbody>
</table>

**Table 63: Implementation Strategy for On-Premises VMware Identity Manager Appliances**

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Three instances of the VMware Identity Manager appliance were deployed in the DMZ.</td>
<td>Three servers are required to support high availability for 50,000 users.</td>
</tr>
</tbody>
</table>

**Table 64: Implementation Strategy for VMware Identity Manager Connectors**

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two instances of VMware Identity Manager Connectors were deployed in the internal network.</td>
<td>Two connectors are recommended to support an environment with 50,000 users.</td>
</tr>
</tbody>
</table>

**Table 65: Cluster Strategy for SQL Servers**

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server 2016 database server was installed on a two-node Windows Server Failover Cluster (WSFC), which uses a SQL Server Always On availability group.</td>
<td>The WSFC provides local redundancy for the SQL database service. The use of SQL Server Always On allows for the design of a disaster-recovery scenario in a second site.</td>
</tr>
</tbody>
</table>
Load Balancing

To remove a single point of failure, we can deploy the VMware Identity Manager service in a cluster configuration and use a third-party load balancer. Most load balancers can be used with VMware Identity Manager. The load balancer must, however, support long-lived connections and web sockets, which are required for the VMware Identity Manager Connector communication channel.

Deploying VMware Identity Manager in a cluster not only provides redundancy but also allows the load and processing to be spread across multiple instances of the service. To ensure that the load balancer itself does not become a point of failure, most load balancers allow for the setup of multiple nodes in an HA or master/slave configuration.

The following figure illustrates how load balancers distribute the load to a cluster of VMware Identity Manager appliances in the DMZ. VMware Identity Manager Connector virtual appliances are hosted in the internal network. These appliances connect to the VMware Identity Manager service nodes and the service URL using an outbound-only connection.

Figure 52: On-Premises VMware Identity Manager Load Balancing and External Access
In this example, the VMware Identity Manager service URL is my.vmweuc.com, and this hostname is resolved in the following ways:

- External clients resolve this name to 80.80.80.80.
- All internal components and clients resolve this name to 192.168.2.50.

**Note:** VMware Identity Manager Connectors must be able to connect to both the VMware Identity Manager service URL and each individual VMware Identity Manager virtual appliance.

Split DNS is not a requirement for VMware Identity Manager but is recommended. VMware Identity Manager supports only one namespace; that is, the same fully qualified domain name (FQDN) for VMware Identity Manager must be used both internally and externally for user access. This FQDN is referred to as the VMware Identity Manager service URL.

You might decide to use two load balancer instances; one for external access and one that handles internal traffic. This is optional but provides an easy way to block access from the Internet to the management console of the VMware Identity Manager web interface.

Although VMware Identity Manager does support configuring load balancers for TLS pass-through, it is often easier to deploy using TLS termination (re-encrypt) on the load balancer. This way the certificates on each VMware Identity Manager service node can be left using the default self-signed certificate.

**Certificate Restrictions**

VMware Identity Manager has the following requirements for certificates to be used on the load balancer and, if using pass-through, also on each node.

- Only SHA-256 (and above) based certificates are supported. SHA-1-based certificates are not supported due to security concerns.
- The required key size is 2048 bits.

**Note:** VMware Identity Manager Connectors must be able to use TCP 443 (HTTPS) to communicate with both the VMware Identity Manager service URL and each VMware Identity Manager service appliance.

It could be beneficial to add a redirect from HTTP to HTTPS for the load balancer and for the VMware Identity Manager service URL. This way end users do not have to specify https:// when accessing VMware Identity Manager.

For this reference architecture, we used F5 load balancers, but any load balancer that supports the requirements should work. The following features must be supported by the load balancer:

- TLS 1.2
- Sticky sessions
- WebSockets
- X-Forwarded-For (XFF) headers
- Cipher support with forward secrecy
- SSL pass-through/termination
- Configurable request time-out value
- Layer 4 support if using iOS Mobile SSO

**Table 66: Implementation Strategy for Global and Local Load Balancing**

<table>
<thead>
<tr>
<th>Decision</th>
<th>In this reference architecture, we used F5 load balancers for both the local data center and the global load balancer. We used split DNS for the VMware Identity Manager service URL.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>F5 supports the global load-balancing functionality required for the design. Split DNS allows for the most efficient traffic flow.</td>
</tr>
</tbody>
</table>

**Multi-site Design**

VMware Identity Manager is the primary entry point for end users to consume all types of applications, including SaaS, web, VMware Horizon virtual desktops and published applications, Citrix XenApp and XenDesktop, and mobile apps. Therefore, when deployed on-premises, it should be highly available within a site, and also deployed in a secondary data center for failover and redundancy.

The failover process that makes the secondary site’s VMware Identity Manager appliances active requires a change at the global load balancer to direct the traffic of the service URL to the desired instance. For more information see [Deploying VMware Identity Manager in a Secondary Data Center for Failover and Redundancy](#).

VMware Identity Manager consists of the following layers, which need to be designed for redundancy:

- VMware Identity Manager appliances and connectors
- Database
- Unified app catalog that can contains SaaS, web, VMware Horizon published applications and desktops, Citrix XenApp and XenDesktop, and mobile apps

**Table 67: Site Resilience Strategy for On-Premises VMware Identity Manager**

<table>
<thead>
<tr>
<th>Decision</th>
<th>A second site was set up with VMware Identity Manager.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This strategy provides disaster recovery and site resilience for the on-premises implementation of VMware Identity Manager.</td>
</tr>
</tbody>
</table>

**VMware Identity Manager Appliances and Connectors**

To provide site resilience, each site requires its own group of VMware Identity Manager virtual appliances to allow the site to operate independently, without reliance on another site. One site runs as the active VMware Identity Manager, while the second site has a passive group. The determination of which site has the active VMware Identity Manager is usually controlled by the global load balancer.
balancer’s namespace entry or a DNS entry, which sets a given instance as the target for the namespace in use by users.

Within each site, VMware Identity Manager must be installed with a minimum of three appliances. This provides local redundancy and ensures that services such as Elasticsearch function properly.

A local load balancer distributes the load between the local VMware Identity Manager instances, and a failure of an individual appliance is handled with no outage to the service or failover to second site. Each local site load balancer is also load-balanced with a global load balancer.

At each site, two VMware Identity Manager Connector virtual appliances are hosted in the internal network and use an outbound-only connection to the VMware Identity Manager service appliances. These connectors connect over TCP 443 (HTTPS) to both the global load balancer and each individual VMware Identity Manager service appliance. It is therefore critical the VMware Identity Manager Connectors be able to resolve the VMware Identity Manager service URL as well as each individual appliance’s FQDN.

| Table 68: Disaster Recovery Strategy for On-Premises VMware Identity Manager |
|--------------------------------|--------------------------------------------------------------------------------|
| **Decision**                   | A second set of servers was installed in a second data center. The number and     |
|                                | function of the servers was the same as sized for the primary site.              |
| **Justification**              | This strategy provides full disaster recovery capacity for all VMware Identity   |
|                                | Manager on-premises services.                                                   |

**Multi-site Database**

VMware Identity Manager 2.9 (and later) supports Microsoft SQL Server 2012 (and later) and its cluster offering Always On availability groups. This allows us to deploy multiple instances of VMware Identity Manager that point to the same database. The database is protected by an availability group, with an availability group listener as the single Java Database Connectivity (JDBC) target for all instances.

VMware Identity Manager is supported with an active/passive database instance with failover to the secondary site if the primary site becomes unavailable. Depending on the configuration of SQL Server Always On, inter-site failover of the database can be automatic, though not instantaneous.

For this reference architecture, we chose an Always On implementation with the following specifications:

- No shared disks were used.
- The primary database instance ran in Site 1 during normal production.

Within a site, Windows Server Failover Clustering (WSFC) was used to improve local database availability and redundancy. In a WSFC cluster, two Windows servers are clustered together to run one instance of SQL Server, which is called a SQL Server failover cluster instance (FCI). Failover of the SQL Server services between these two Windows servers is automatic.

This architecture is depicted in the following figure.
For this design, VMware Identity Manager was configured as follows:

- It uses an active-hot standby deployment.
- VMware Identity Manager nodes in Site 1 form an Elasticsearch cluster and an Ehcache cluster. Nodes in Site 2 form a separate Elasticsearch cluster and Ehcache cluster. Elasticsearch and Ehcache are embedded in the VMware Identity Manager virtual appliance. Note: Elasticsearch is a search and analytics engine used for auditing, reports, and directory sync logs. Ehcache provides caching capabilities.
- Only the active site can service user requests.
- An active VMware Identity Manager group exists in the same site as the primary replica for the Always On availability group.

Note: To implement this strategy, you must perform all the tasks described in Deploying VMware Identity Manager in a Secondary Data Center for Failover and Redundancy. One step that is easily overlooked is the editing of the runtime-config.properties file in the secondary data center. For more information, see Edit runtime-config.properties File in Secondary Data Center.

All JDBC connection strings for VMware Identity Manager appliances should point to the SQL Server availability group listener (AGL) and not directly to an individual SQL Server node. For detailed instructions about deploying and configuring the VMware Identity Manager, creating SQL Server failover cluster instances, creating an Always On availability group, and configuring VMware Identity Manager appliances to point to the AGL, see "Appendix C: VMware Identity Manager Configuration for Multi-site Deployments" on page 371.

If your organization has already deployed Always On availability groups, consult with your database administrator (DBA) about the requirements for the database used with VMware Identity Manager.
The SQL Server Always On setup can be configured to automatically fail over and promote the remaining site’s database to become the primary.

Table 69: Strategy for Multi-site Deployment of the On-Premises Database

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server was deployed in both sites. A SQL Always On availability group was used.</td>
<td>This strategy provides replication of the SQL database to the second site and a mechanism for recovering the SQL database service in the event of a site outage.</td>
</tr>
</tbody>
</table>

Prerequisites

This section details the prerequisites for the VMware Identity Manager configuration.

vSphere and ESXi

Although several versions are supported, we used VMware vSphere® 6.5. See the VMware Product Interoperability Matrices for more details about supported versions.

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 VMware ESXi™ host level, using an NTP server to prevent a time drift between virtual appliances. If you deploy multiple virtual appliances on different hosts, make sure all ESXi hosts are time-synced.

Network Configuration

- Static IP addresses and DNS Forward (A) and Reverse (PTR) records are required for all servers and the VMware Identity Manager service URL.
- Inbound firewall port 443 must be open so that users outside the network can connect to the VMware Identity Manager service URL load balancer.

Active Directory

VMware Identity Manager 3.0 (and later) supports Active Directory configurations on Windows 2008 R2, 2012, 2012 R2, and 2016, including:

- Single AD domain
- Multidomain, single forest
- Multiforest with trust relationships
- Multiforest with untrusted relationships
- Active Directory Global Catalog (optional for Directory Sync)

For this reference architecture, Windows Server 2016 Active Directory was used.
Virtual Machine Build

Specifications are detailed in "Appendix A: VM Specifications" on page 326. Each server is deployed with a single network card, and static IP address information is required for each server.

**Table 70: Operating System Choices for Server Components**

<table>
<thead>
<tr>
<th>Decision</th>
<th>Windows Server 2016 was used for the VMware Identity Manager Connector servers. VMware Identity Manager Appliances included the required SUSE Linux Enterprise Server (SLES) operating system. IP address information was allocated for each server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Best practice is to use the latest supported OS.</td>
</tr>
</tbody>
</table>

Installation and Initial Configuration

The major steps for on-premises installation and initial configuration of VMware Identity Manager are depicted in the following diagram.

**Figure 54: VMware Identity Manager Installation and Configuration Steps**

**VMware Identity Manager OVA**

The VMware Identity Manager service appliance is delivered as an Open Virtualization Format (OVF) template and deployed using the VMware vSphere® Web Client. For information on deploying the
VMware Identity Manager service appliance, see About Installing and Configuring VMware Identity Manager for Linux. Before you deploy the appliance, it is important to have DNS records (A and PTR) and network configuration specified. As you complete the OVF Deployment Wizard, you will be prompted for this information.

**Note:** In the OVF Deployment Wizard, you must specify the appliance’s FQDN in the Host Name field, as shown in the following figure.

![Fully Qualified Domain Name](image)

**Figure 55:** VMware Identity Manager OVF Wizard

After deployment and on the first boot, you must enter passwords for the SSHUSER, ROOT, and ADMIN user. By default, SSH is disabled for the ROOT user. If you want to SSH into the appliance, you must do so using the SSHUSER account, and you can then switch user to ROOT. The ADMIN user is your local administrator in the VMware Identity Manager web console.

After you configure directory sync, VMware recommends that you promote at least one synced user to administrator and use this account for your everyday operations. The local ADMIN password is also used to access the appliance settings page. You can later change both so that they are not the same. For more information, see Manage Your Appliance Passwords.

You will also be prompted to complete database setup. Here, you enter the JDBC connection string, username, and password. For more information, see “Appendix C: VMware Identity Manager Configuration for Multi-site Deployments” on page 371.

**VMware Identity Manager Configuration**

After the initial setup is done, you can access the VMware Identity Manager web console. Because VMware Identity Manager depends heavily on the VMware Identity Manager service URL, VMware recommend that you configure this service URL first. For more information, see Modifying the VMware Identity Manager Service URL. If you ever need to change the service URL for troubleshooting purposes, see Workspace Portal / vIDM – Trouble Changing the FQDN.
After you have changed the service URL, do not forget to enable the New User Portal UI. Enter the license key, and generate activation codes for your VMware Identity Manager Connectors. VMware Identity Manager supports the use of an external Syslog server.

**VMware Identity Manager Connector Configuration**

The VMware Identity Manager Connector is delivered as a Windows installer and are deployed by installing it on an existing Windows machine. For more information about deploying the VMware Identity Manager Connector, see [Installing and Configuring VMware Identity Manager Connector 2018.8.1.0 (Windows)](#).

On first boot, you are prompted for the local admin user’s password. This password is used to access the appliance configuration of the VMware Identity Manager Connector. As the final step of the VMware Identity Manager Connector Setup Wizard, you are prompted for the connector activation code generated in the previous step.

**Cluster Configuration**

The procedure to create a VMware Identity Manager cluster is described in [Configuring Failover and Redundancy in a Single Datacenter](#). Make sure to start the original appliance first and allow it to fully start up all services before powering on the other nodes. Verify that the Elasticsearch cluster health is green. After the cluster is operational VMware recommend always powering down the Elasticsearch master last. When you power the cluster back on, try to always start the Elasticsearch master first. You can find more information in [Verify Cluster in Primary Data Center](#).

**Directory Configuration**

Although using local users (rather than syncing users from an existing directory) is supported, most implementations of VMware Identity Manager do synchronize users from a Microsoft Active Directory.

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 initiating a directory sync. You can specify what attributes users in VMware Identity Manager should have. See [Set User Attributes at the Global Level](#) for more information.

**Note:** The required flag for attributes only means, for example, that if a user in Active Directory does not have the attribute populated, the user will not be synced to VMware Identity Manager. If the user has the attribute populated and if VMware Identity Manager has the attribute mapped to its internal attributes, the value will be synced (with or without the required flag set). Therefore, most of the time, you do not need to change attributes so that they are required.

**Connectors Updates**

Configure all connectors with the same authentication methods and add them to the WorkspaceIDP. For more information see: [Deploying VMware Identity Manager Connector in the Enterprise Network](#). The VMware Identity Manager Connector supports adding an external Syslog server.

**Service Updates**

Make sure all the VMware Identity Manager Connectors are added to the built-in idP and verify that authentication methods are configured in outbound-only mode. Configuring network ranges, authentication methods, and access policies are important tasks to complete before allowing users access to VMware Identity Manager.
Application Catalog

Finally, you configure application integration and publish applications in the VMware Identity Manager user catalog. You can specify application-specific access policies.

Integration with Workspace ONE Unified Endpoint Management (UEM)

To leverage the breadth of the Workspace ONE experience, you must integrate Workspace ONE UEM and VMware Identity Manager into Workspace ONE. After integration:

- Workspace ONE UEM can use VMware Identity Manager for authentication and access to SaaS and VMware Horizon applications.

- Workspace ONE can use Workspace ONE UEM for device enrollment and management.

See the Guide to Deploying VMware Workspace ONE with VMware Identity Manager for more details.

When using cloud-based VMware Identity Manager, you can use Hub Services. More information about Hub Services can be found in Integrating Hub Services with VMware Identity Manager.

Access to Resources Through VMware Identity Manager

VMware Identity Manager powers the Workspace ONE catalog, providing self-service access to company applications for business users. VMware Identity Manager is responsible for the integration with web-based SaaS applications, internal web applications, Citrix, and VMware Horizon for the delivery of virtual desktops and published applications. All these desktops and apps are displayed to the user in the catalog based on directory entitlements.

Based on the types of applications to be delivered to end users, the catalog is configured to integrate with the relevant services.

Workspace ONE Native Mobile Apps

For many users, their first experience with Workspace ONE is through the Workspace ONE native mobile application, which displays a branded self-service catalog. The catalog provides the necessary applications for the user to do their job, and also offers access to other company resources, such as a company directory lookup. Native operating features, such as Apple Touch ID on an iOS device or Windows Hello on Windows 10, can be used to enhance the user experience.

The Workspace ONE app:

- Delivers a unified application catalog of web, mobile, Windows, macOS, and virtual applications to the user.
  Through integration, VMware Identity Manager applications are aggregated with Workspace ONE UEM–delivered applications.

- Provides a launcher to access the web, SaaS apps, and Horizon and Citrix virtual desktops and apps to give a consolidated and consistent way of discovering and launching all types of applications.
- Gives the user the ability to search across an enterprise’s entire deployment of application resources.
- Offers SSO technology for simple user access to resources without requiring users to remember each site’s password.
- Can search the company’s user directory, retrieving employees’ phone numbers, email addresses, and position on the org chart.

Figure 56: Workspace ONE App for Windows 10

The Workspace ONE native app is available from the various app stores and can be deployed through Workspace ONE UEM as part of the device enrollment process. Platforms supported are iOS, Android, macOS, and Windows 10.

**SaaS Apps**

SaaS applications, such as Concur and Salesforce, are often authenticated through federation standards, such as Security Assertion Markup Language (SAML), to offload authentication to an identity provider. These applications are published through VMware Identity Manager and allow users seamless SSO access while being protected by the rich access policies within VMware Identity Manager.

The cloud application catalog in VMware Identity Manager includes templates with many preconfigured parameters to make federating with the SaaS provider easier. For SaaS providers, where there is no template, a wizard guides you through configuring the application and entitling users. VMware Identity Manager supports SAML and OpenID Connect protocols for federation. VMware Identity Manager also supports WS-Fed for integration with Microsoft Office 365.
**Figure 57**: Administrator Adding a New SaaS Application to the Catalog
The capability to deliver virtual apps and desktops continues to be a significant value for Workspace ONE users. VMware Identity Manager can be integrated with a VMware Horizon implementation to expose the entitled apps and desktops to end users. Through VMware Horizon® Client™ for native mobile platforms, access to these resources can be easily extended to mobile devices.

You must deploy the VMware Identity Manager Connector to provide access to Horizon resources from the VMware Identity Manager cloud-based or on-premises service. The connector enables you to synchronize entitlements to the service.

**Note:** VMware Identity Manager does not proxy or tunnel the traffic to the resource. The end user’s device must be able to connect to the resource, web, or Horizon or Citrix desktops and apps. Establishing access to the resource can be done in many ways, for example, VPN, Per-App VPN, publicized on the Internet, and more.

Refer to **Setting Up Resources in VMware Identity Manager (SaaS)** or **Setting Up Resources in VMware Identity Manager (On Premises)** for more details on how to add applications and other resources to the Workspace ONE catalog.
Component Design: Workspace ONE Intelligence Architecture

The shift from traditional mobile device management (MDM) and PC management to a digital workspace presents its own challenges.

- **Data overload** – When incorporating identity into device management, IT departments are deluged by an overwhelming volume of data from numerous sources.
- **Visibility silos** – From a visibility and management standpoint, working with multiple un-integrated modules and solutions often results in security silos.
- **Manual processes** – Traditional approaches such as using spreadsheets and scripting create bottlenecks and require constant monitoring and corrections.
- **Reactive approach** – The process of first examining data for security vulnerabilities and then finding solutions can introduce delays. These delays significantly reduce the effectiveness of the solution. A reactive approach is not the best long-term strategy.

VMware Workspace ONE® Intelligence™ is designed to simplify user experience without compromising security. The intelligence service aggregates and correlates data from multiple sources to give complete visibility into the entire environment. It produces the insights and data that will allow you to make the right decisions for your VMware Workspace ONE® deployment. Workspace ONE Intelligence has a built-in automation engine that can create rules to take automatic action on security issues.

![Figure 59: Workspace ONE Intelligence Logical Architecture.](image-url)
Table 71: Implementation Strategy for Workspace ONE Intelligence

<table>
<thead>
<tr>
<th>Decision</th>
<th>Workspace ONE Intelligence was implemented.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>The intelligence service aggregates and correlates data from multiple sources to optimize resources and strengthen security and compliance across the entire digital workspace.</td>
</tr>
</tbody>
</table>

**Architecture Overview**

Workspace ONE Intelligence is a cloud-only service, hosted on Amazon Web Services (AWS), that offers the following advantages:

- Reduces the overhead of infrastructure and network management, which allows users to focus on utilizing the product.
- Complements the continuous integration and continuous delivery approach to software development, allowing new features and functionality to be released with greater speed and frequency.
- Helps with solution delivery by maintaining only one version of the software without any patching.
- AWS are industry leaders in cloud infrastructure, with a global footprint that enables the service to be hosted in different regions around the world.
- AWS offers a variety of managed services out-of-the-box for high availability and easy monitoring.
- Leveraging these services allows VMware to focus on product feature development and security rather than infrastructure management.

Workspace ONE Intelligence includes the following components.
### Table 72: Components of Workspace ONE Intelligence

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace ONE Intelligence Connector</td>
<td>An ETL (Extract, Transform, Load) service responsible for collecting data from the Workspace ONE database and feeding it to the Workspace ONE Intelligence cloud service.</td>
</tr>
<tr>
<td>Intelligence Cloud Service</td>
<td>Aggregates all the data received from an Intelligence Connector and generates reports. Populates the Workspace ONE Intelligence dashboard with different data points, in the format of your choice.</td>
</tr>
<tr>
<td>Consoles</td>
<td>Workspace ONE Intelligence currently leverages the following consoles:</td>
</tr>
<tr>
<td></td>
<td>• Workspace ONE UEM Console</td>
</tr>
<tr>
<td></td>
<td>• Workspace ONE Intelligence Console</td>
</tr>
<tr>
<td></td>
<td>• Apteligent (for app analytics) Console</td>
</tr>
<tr>
<td>Data sources</td>
<td>VMware Workspace ONE® UEM, VMware Identity Manager™, Workspace ONE Intelligence SDK, and Common Vulnerability and Exposures (CVE).</td>
</tr>
</tbody>
</table>

### Scalability and Availability

The Workspace ONE Intelligence service is currently hosted in six production regions, including Oregon (two locations), Ireland, Frankfurt, Tokyo, and Sydney. It leverages the same auto-scaling and availability principles as those described in [AWS Auto Scaling](https://aws.amazon.com/email) and [High Availability (Multi-AZ) for Amazon RDS](https://aws.amazon.com/rds/).

### Database Design

Workspace ONE Intelligence uses a variety of databases, depending on the data type and purpose. These databases are preconfigured, offered out-of-the-box as per the cloud service offering, and no additional configuration is necessary.
### Table 73: Workspace ONE Intelligence Databases

<table>
<thead>
<tr>
<th>Database Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Amazon S3     | - Ultimate source of truth  
|               | - Cold storage for all data required for database recovery if needed  
|               | - Also used actively for scenarios such as app analytics loads and usage |
| Dynamo DB     | - Managed service of AWS  
|               | - Stores arbitrary key-value pairs for different data types  
|               | - Data resource for reports for dashboard and subscriptions |
| Elasticsearch – History | - Historical charts  
|               | - Historical graphs |
| Elasticsearch – Snapshot | - Report previews  
|               | - Current counts |

**Data Sources for Workspace ONE Intelligence**

The following figure shows how the various data sources contribute to Workspace ONE Intelligence.

![Figure 60: Workspace ONE Intelligence Data Sources](image)

*VMware Workspace ONE and VMware Horizon Reference Architecture - 121*
Workspace ONE Unified Endpoint Management

After a device is enrolled with Workspace ONE UEM, it starts reporting a variety of data points to the Workspace ONE UEM database, such as device attributes, security posture, and application installation status. Along with this, Workspace ONE UEM also gathers information about device users and user attributes from local databases and from Active Directory.

After the administrator opts in to Workspace ONE Intelligence, ETL starts sending data. The data is aggregated and correlated by the platform for display purposes and to perform automated actions that enhance security and simplify user experience.

Figure 61: Workspace ONE Intelligence Components for UEM

The Workspace ONE Intelligence Connector service (also known as the ETL service) is responsible for aggregating the data from Workspace ONE UEM and feeding it to Workspace ONE Intelligence. After the data is extracted, the Workspace ONE Intelligence service processes it to populate dashboards and to generate reports based on the attributes selected by the intelligence administrator.

Your Workspace ONE Intelligence region is assigned based on your Workspace ONE UEM SaaS deployment location. No additional configuration is required to leverage Workspace ONE Intelligence. Find your shared and dedicated SaaS Workspace ONE UEM location and see its corresponding Workspace ONE Intelligence region at [Workspace ONE UEM SaaS Environment Location Mapped to a Workspace ONE Intelligence Region](#).

When deploying Workspace ONE UEM on-premises, you will be asked to select a region to send data to during the installation of the ETL service. Available regions are the United States, Ireland, Frankfurt, Sydney, and Tokyo.

The Workspace ONE Intelligence Connector service is currently not supported for high availability in an active/active mode. However, additional instances are added for redundancy and disaster recovery, and server resources are increased according to the load to handle scaling.

For more information on how to deploy Workspace ONE Intelligence Connector service for on-premises Workspace ONE UEM, see [Workspace ONE Intelligence and Workspace ONE UEM Integration](#) in "Platform Integration" on page 244.
Table 74: Implementation Strategy for On-Premises Workspace ONE UEM

<table>
<thead>
<tr>
<th>Decision</th>
<th>A Workspace ONE Intelligence Connector (ETL) was deployed and configured to aggregate data from the Workspace ONE UEM instance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>The Workspace ONE Intelligence Connector is required to send on-premises Workspace ONE UEM data to Workspace ONE Intelligence.</td>
</tr>
</tbody>
</table>

Common Vulnerabilities and Exposures (CVE)

CVE is a list of entries for publicly known cyber security vulnerabilities. With regards to Windows 10 managed devices, the CVE integration in Workspace ONE Intelligence performs a daily import of CVE details, as well as risk scores derived from the Common Vulnerability Scoring System (CVSS).

Because Workspace ONE UEM provides an update service for Windows 10 managed devices based on KBs released by Microsoft, Workspace ONE Intelligence is able to correlate its imported CVE details and risk scores with the Microsoft KBs.

The CVE information allows IT administrators and security teams to prioritize which vulnerabilities to fix first and helps them gauge the impact of vulnerabilities on their systems. This can be achieved through daily or even hourly reporting to security teams of all devices that are deemed vulnerable based on CVSS score.

Custom dashboards can then provide insights and real-time visibility into the security risks affecting all managed devices. The Workspace ONE Intelligence rules engine can take automated remediation actions, such as applying patches to the impacted devices.

![Figure 62: CVE Metrics Based on Workspace ONE Intelligence](image)

So long as Workspace ONE UEM is integrated with Workspace ONE Intelligence through the ETL service, no additional configuration is required to obtain and correlate the CVE data.

Table 75: Strategy for Monitoring Security Risks to Windows 10 Devices
<table>
<thead>
<tr>
<th>Decision</th>
<th>The Workspace ONE Intelligence dashboard was configured to provide real-time visibility into the impact of CVE entries on Windows 10 managed devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Workspace ONE Intelligence increases security and compliance across the environment by providing integrated insights and automating remediation actions.</td>
</tr>
</tbody>
</table>

**VMware Identity Manager**

Integrating VMware Identity Manager with Workspace ONE Intelligence allows administrators to track login and logout events for applications in the Workspace ONE catalog. This integration also captures application launches in the Workspace ONE catalog for both Service Provider (SP)–initiated and Identity Provider (IdP)–initiated workflows. This information is available for web, native, and virtual applications and is presented in preconfigured and as well as custom dashboards.

IT administrators can gather insight into:

- **Application adoption** – By determining how many unique users have launched a particular application
- **Application engagement** – By collecting user-experience statistics about the most-used applications
- **Security issues** – By examining data about failed login attempts

User login events are represented by the following types:

- **Login** – A user attempts to access an app listed in the Workspace ONE catalog.  
  **Note**: Just logging in to the Workspace ONE catalog alone does not count as a user login.
- **Logout** – A user manually logs out of the Workspace ONE catalog.  
  A logout event is not generated when:
  - A user logs out of a particular app, because the user is still authenticated to the catalog.
  - The session times out or the user closes the browser.
- **Login failures** – A user enters an incorrect password, the second factor of two-factor authentication is incorrect, the certificate is missing, and so on.
App launch events are captured under two scenarios:

- A user launches an app from the Workspace ONE catalog (IdP-initiated).
- A user navigates directly to a web app, so that SSO occurs through Workspace ONE (SP-initiated).

App launch events are captured for web, SaaS, and virtual apps, and for any other type of app configured as part of the Workspace ONE catalog. To provide insights about these apps, Workspace ONE Intelligence displays information about app events through widgets in the Apps dashboard.
To add VMware Identity Manager as a data source to Workspace ONE Intelligence, navigate to Intelligence Settings in the Intelligence dashboard and select VMware Identity Manager. Enter the tenant URL for the VMware Identity Manager cloud-based tenant and select Authorize. For more information, see *Workspace ONE Intelligence and VMware Identity Manager Integration* in "Platform Integration" on page 244.

Only cloud-based instances of VMware Identity Manager can be integrated with Workspace ONE Intelligence. On-premises deployments of VMware Identity Manager cannot be integrated into Workspace ONE Intelligence.

**Table 76: Implementation Strategy for Integrating VMware Identity Manager**

<table>
<thead>
<tr>
<th>Decision</th>
<th>Workspace ONE Intelligence was configured to collect data from VMware Identity Manager.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This strategy collects user data around events and users from VMware Identity Manager and integrates this data with Workspace ONE Intelligence. Web application data displays on the Apps dashboard, allowing the visualization of both Workspace ONE logins and application load events.</td>
</tr>
</tbody>
</table>
App Analytics with Workspace ONE Intelligence SDK

Integrating the Workspace ONE Intelligence SDK (formerly known as the Apteligent SDK) with Workspace ONE Intelligence provides insight into app and user behavior analytics. After an app that has the Intelligence SDK embedded is registered with Workspace ONE Intelligence, the Apps dashboard starts populating the relevant data.

The prerequisites are that enterprise applications have the Workspace ONE Intelligence SDK embedded in them, and that applications are managed by Workspace ONE UEM.

The platforms supported with the Intelligence SDK are Apple (iOS, tvOS), Android, and hybrid platforms (that is, a native platform with an HTML5 component).

The following data is captured and correlated from Apteligent and Workspace ONE UEM.

Table 77: App Dashboard Widgets Summary

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total installs</td>
<td>Total number of installations of the application</td>
</tr>
<tr>
<td>Devices missing app</td>
<td>Number of devices that do not have a specific app</td>
</tr>
<tr>
<td>App install status</td>
<td>Installation status of the app; for example, installing, failed, pending removal, and managed</td>
</tr>
<tr>
<td>App version over time</td>
<td>Version of the app for the selected amount of time</td>
</tr>
<tr>
<td>Installs over time</td>
<td>Number of times the application was installed</td>
</tr>
</tbody>
</table>

Mobile apps that integrate with the Intelligence SDK must be registered in Workspace ONE Intelligence by following the instructions in Register Apteligent in Settings, or through the step-by-step video VMware Workspace ONE Intelligence Integration with Apteligent Feature Walk-through. The registration process enables the visualization of app analytics through the App dashboard and available widgets.

The app analytics feature in the Workspace ONE Intelligence Console is currently limited to correlating app loads with app deployment information. These analytics include:

- Daily active users (last 24 hours)
- Rolling monthly active users (last 30 days)
- DAU/MAU (stickiness of the application)
- App deployment over time per version and latest version deployed
To leverage the full capabilities of app analytics, you can leverage the Apteligent Console. For more information, see the Apteligent documentation.

**Insights and Automation**

All data collected from the data sources is aggregated and correlated by the Workspace ONE Intelligence service. The data is then made available for visualization from a business, process, and security standpoint. Also, the Workspace ONE Intelligence service can perform automatic actions based on the rules defined in the Intelligence Console.

**Dashboards**

Dashboards present the historical or latest snapshot of information about the selected attributes, such as devices, users, operating systems, and applications. These dashboards are populated using widgets that are fully customizable, including, for example, layout tools, editing filters, and other options. Information can be displayed in the form of horizontal or vertical bar charts, donuts, and tables. You can also choose a specific date range to visualize historical data. All the widgets can be added as part of My Dashboard.

Following is a summary of the predefined widgets.
Table 78: Examples of Out-of-the-Box Dashboard Widgets

<table>
<thead>
<tr>
<th>Widget Category</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td>Number of enrolled devices, operating system breakdowns, compromised status</td>
</tr>
<tr>
<td>Apps</td>
<td>Most popular apps, agent installed (by version)</td>
</tr>
<tr>
<td>OS Updates</td>
<td>Top-ten KBs installed, devices with a CVSS risk score higher than 7</td>
</tr>
<tr>
<td>User Logins</td>
<td>Trend of user logins, login failures (by authentication method)</td>
</tr>
<tr>
<td>App Launches</td>
<td>Top-five apps launched, according to both unique user count and total number of launches</td>
</tr>
</tbody>
</table>

You can extend the filters and data points for the out-of-the-box widgets or create new widgets from scratch.

In addition to My Dashboard, Workspace ONE Intelligence includes three additional predefined dashboards (Security Risk, OS Updates, and Apps) allowing IT administrators to quickly gather insights into their environment and make data-driven decisions.

Figure 66: Device Passcode Risk Over Time, Displayed in the Security Risk Dashboard
Dashboards are available as a part of Workspace ONE Intelligence cloud offerings. No additional configuration is needed for this feature.

**Reports**

Reports are generated based on data fetched from Workspace ONE UEM, giving administrators real-time information about the deployment. The data is extracted from devices, applications, OS updates, and user data points.

Workspace ONE Intelligence offers a set of predefined templates. Additionally, you can customize these templates or create a new template from scratch to generate reports on the specific data points. Using the reports dashboard of Workspace ONE Intelligence, you can run, subscribe to, edit, copy, delete, and download (CSV format) reports.

Reports are available as a part of Workspace ONE Intelligence cloud offerings. No additional configuration is needed for this feature when you use cloud-based Workspace ONE UEM. For an on-premises deployment of Workspace ONE UEM, you must deploy the Workspace ONE Intelligence Connector. Reports are available only to groups whose organization group type is Customer.

**Automation Capabilities**

Automation in Workspace ONE Intelligence acts across categories that include devices, apps, and OS updates. Administrators can specify the conditions under which automatic actions will be performed. Automation removes the need for constant monitoring and manual processing to react to a security vulnerability. Configuring automation involves setting up the trigger, condition, and automated action, such as sending out a notification or installing or removing a certain profile or app.

Automation is facilitated by automation connectors. These connectors leverage Workspace ONE UEM REST APIs to communicate with Workspace ONE UEM and third-party services. The current list of automation connectors includes Workspace ONE UEM, Service Now, and Slack, but the list is growing quickly.

![Figure 67: Workspace ONE Intelligence Connectors](image)

To learn more about how to integrate Workspace ONE Intelligence Connector with Workspace ONE UEM and third-part services, see Automation Connections, API Communications, and Third-Party Connections.
Getting Started with Workspace ONE Intelligence

Workspace ONE Intelligence is offered as a 30-day free trial or can be purchased as an add-on and included with the Workspace ONE Enterprise bundle. The first time you log in to the Workspace ONE Intelligence dashboard, you must opt-in to Workspace ONE Intelligence by selecting a check box.

For more information, see the VMware Workspace ONE Intelligence guide.
Component Design: Horizon 7 Architecture

VMware Horizon® 7 is a platform for managing and delivering virtualized or hosted desktops and applications to end users. Horizon 7 allows you to create and broker connections to Windows virtual desktops, Linux virtual desktops, Remote Desktop Server (RDS)-hosted applications and desktops, and physical machines.

A successful deployment of Horizon 7 depends on good planning and a robust understanding of the platform. This section discusses the design options and details the design decisions that were made to satisfy the design requirements.

Table 79: Horizon 7 Environment Setup Strategy

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Horizon 7 deployment was designed, deployed, and integrated with the VMware Workspace ONE® platform. The environment was designed to be capable of scaling to 8,000 concurrent connections for users.</td>
<td>This strategy allowed the design, deployment, and integration to be validated and documented.</td>
</tr>
</tbody>
</table>

Architectural Overview

The core components of Horizon 7 include a VMware Horizon® Client™ authenticating to a Connection Server, which brokers connections to virtual desktops and apps. The Horizon Client then forms a protocol session connection to a Horizon Agent running in a virtual desktop or RDSH server.

Figure 68: Horizon 7 Core Components

External access includes the use of VMware Unified Access Gateway™ to provide secure edge services. The Horizon Client authenticates to a Connection Server through the Unified Access Gateway. The Horizon Client then forms a protocol session connection, through the gateway service on the Unified Access Gateway, to a Horizon Agent running in a virtual desktop or RDSH server. This process is covered in more detail in “External Access” on page 143.
Figure 69: Horizon 7 Core Components for External Access

The following figure shows the high-level logical architecture of the Horizon 7 components with other Horizon 7 Enterprise Edition components shown for illustrative purposes.

Figure 70: Horizon 7 Enterprise Edition Logical Components

**Components**

The components and features of Horizon 7 are described in the following table.
### Table 80: Components of Horizon 7

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Server</td>
<td>An enterprise-class desktop management server that securely brokers and connects users to desktops and published applications running on VMware vSphere® VMs, physical PCs, blade PCs, or RDSH servers. Authenticates users through Windows Active Directory and directs the request to the appropriate and entitled resource.</td>
</tr>
<tr>
<td>Horizon Agent</td>
<td>A software service installed on the guest OS of all target VMs, physical systems, or RDSH servers. This allows them to be managed by Connection Servers and allows a Horizon Client to form a protocol session to the target VM.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>Client-device software that allows a physical device to access a virtual desktop or RDSH-published application in a Horizon 7 deployment. You can optionally use an HTML client for devices for which installing software is not possible.</td>
</tr>
<tr>
<td>Unified Access Gateway</td>
<td>Virtual appliance that provides a method to secure connections in access scenarios requiring additional security measures, such as over the Internet. (See “Component Design: Unified Access Gateway Architecture” on page 207 for design and implementation details.)</td>
</tr>
<tr>
<td>Horizon Console</td>
<td>A web application that is part of the Connection Server, allowing administrators to configure the server, deploy and manage desktops, control user authentication, initiate and examine system and user events, carry out end-user support, and perform analytical activities.</td>
</tr>
<tr>
<td>VMware Instant Clone Technology</td>
<td>VMware technology that provides single-image management with automation capabilities. You can rapidly create automated pools or farms of instant-clone desktops or RDSH servers from a master image. The technology reduces storage costs and streamlines desktop management by enabling automatic updating and patching of hundreds of images from the master image. Instant Clone Technology accelerates the process of creating cloned VMs over the previous Composer linked-clone technology. In addition, instant clones require less storage and are less expensive to manage and update.</td>
</tr>
<tr>
<td>RDSH servers</td>
<td>Microsoft Windows Servers that provide published applications and session-based remote desktops to end users.</td>
</tr>
<tr>
<td>Enrollment Server</td>
<td>Server that delivers True SSO functionality by ensuring a user can single-sign-on to a Horizon resource when launched from VMware Identity Manager™, regardless of the authentication method.</td>
</tr>
</tbody>
</table>
### Table 80: Components of Horizon 7 (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment Server</td>
<td>The Enrollment Server is responsible for receiving certificate signing requests from the Connection Server and then passing them to the Certificate Authority to sign. True SSO requires Microsoft Certificate Authority services, which it uses to generate unique, short-lived certificates to manage the login process. See the &quot;True SSO&quot; on page 145 section for more information.</td>
</tr>
</tbody>
</table>
| JMP Server                         | 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. The JMP server enables the use of JMP workflows by providing a single console to define and manage desktop workspaces for users or groups of users. A JMP assignment can be defined that includes information about:  
  - Operating system, by assigning a desktop pool  
  - Applications, delivered by VMware App Volumes™ AppStacks  
  - Application and environment configuration, with VMware User Environment Manager™ settings  

  The JMP automation engine communicates with the Connection Server, App Volumes Managers, and User Environment Manager systems to entitle the user to a desktop. For more information, see the Quick-Start Tutorial for VMware Horizon JMP Integrated Workflow. |
| Cloud Connector (not pictured)     | The Horizon 7 Cloud Connector is required to use with Horizon 7 subscription licenses and management features hosted in the VMware Horizon® Cloud Service™. The Horizon 7 Cloud Connector is a virtual appliance that connects a Connection Server in a pod with the Horizon Cloud Service. You must have an active My VMware account to purchase a Horizon 7 license from https://my.vmware.com. |
Table 80: Components of Horizon 7 (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Composer</td>
<td>The Composer server is only required when using linked-clones. This is the legacy method that enables scalable management of virtual desktops by provisioning clones from a single master image. The Composer service works with the Connection Servers and a VMware vCenter Server®.</td>
</tr>
<tr>
<td>vSphere and vCenter Server</td>
<td>The vSphere product family includes VMware ESXi™ and vCenter Server, and it is designed for building and managing virtual infrastructures. The vCenter Server system provides key administrative and operational functions, such as provisioning, cloning, and VM management features, which are essential for VDI.</td>
</tr>
</tbody>
</table>

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

![Figure 71: Horizon 7 Enterprise Edition Logical Architecture](image)

In addition to the core components and features, other products can be used in a Horizon 7 Enterprise Edition deployment to enhance and optimize the overall solution:
- **VMware Identity Manager** – Provides enterprise single sign-on (SSO), securing and simplifying access to apps with the included identity provider or by integrating with existing identity providers. It provides application provisioning, a self-service catalog, conditional access controls, and SSO for SaaS, web, cloud, and native mobile applications. (See "Component Design: VMware Identity Manager Architecture" on page 96 for design and implementation details.)

- **App Volumes Manager** – Orchestrates application delivery by managing assignments of application volumes (AppStacks and writable volumes) to users, groups, and target computers. (See "Component Design: App Volumes Architecture" on page 172 for design and implementation details.)

- **User Environment Manager** – Provides profile management by capturing user settings for the operating system and applications. (See "Component Design: User Environment Manager Architecture" on page 197 for design and implementation details.)

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

- **VMware 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.

- **VMware vSAN™ 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 NSX® Data Center for vSphere®** – Provides network-based services such as security, virtualization networking, routing, and switching in a single platform. With micro-segmentation, you can set application-level security policies based on groupings of individual workloads, and you can isolate each virtual desktop from all other desktops as well as protecting the Horizon 7 management servers.

  **Note:** NSX Data Center for vSphere is licensed separately from Horizon 7 Enterprise Edition.

---

### Horizon 7 Pod and Block

One key concept in a Horizon 7 environment design is the use of pods and blocks, which gives us a repeatable and scalable approach.

The numbers, limits, and recommendations given in this section were correct at time of writing. For the most current numbers, see the VMware Knowledge Base article [VMware Horizon 7 Sizing Limits and Recommendations](https://kb.vmware.com/kb/2150348).

A *pod* is made up of a group of interconnected Connection Servers that broker connections to desktops or published applications. A pod can broker up to 20,000 sessions (10,000 recommended), including desktop and RDSH sessions. Multiple pods can be interconnected using Cloud Pod Architecture (CPA) for a maximum of 200,000 sessions. For numbers above that, separate CPAs can be deployed.

A pod is divided into multiple *blocks* to provide scalability. Each block is made up of one or more resource vSphere clusters, and each block has its own vCenter Server, Composer server (where linked clones are to be used), and VMware NSX® Manager™ (where NSX is being used). The number of
virtual machines (VMs) a block can typically host depends on the type of Horizon 7 VMs used. See "vCenter Server" on the next page for details.

Figure 72: Horizon 7 Pod and Block Design

To add more resource capacity, we simply add more resource blocks. We also add an additional Connection Server for each additional block to add the capability for more session connections.

Depending on the types of VMs (instant clones, linked clones, full clones, using App Volumes) a resource block could host a different number of VMs (see "Scalability and Availability" on the next page). Typically, we have multiple resource blocks and up to seven 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 thousands of sessions that can then be repeated to create a pod capable of handling 10,000 sessions. Multiple pods grouped using Cloud Pod Architecture can then be used to scale the environment as large as needed.

Important: A single pod and the Connection Servers in it must be located within a single data center and cannot span locations. Multiple Horizon 7 pods and locations must be interconnected using Cloud Pod Architecture. See "Multi-site Architecture" on page 149 and "Cloud Pod Architecture" on page 150 for more detail.

Options regarding the location of management components, such as Connection Servers, include:

- Co-located on the same vSphere hosts as the desktops and RDSH servers that will serve end-users
- On a separate vSphere cluster

In large environments, for scalability and operational efficiency, it is normally best practice to have a separate vSphere cluster to host the management components. This keeps the VMs that run services such as vCenter Server, NSX Manager, Connection Server, Unified Access Gateway, and databases separate from the desktop and RDSH server VMs.
Management components can be co-hosted on the same vSphere cluster as the end-user resources, if desired. This architecture is more typical in smaller environments or where the use of converged hardware is used and the cost of providing dedicated hosts for management is too high. If you place everything on the same vSphere cluster, you must configure the setup to ensure resource prioritization for the management components. Sizing of resources (for example, virtual desktops) must also take into account the overhead of the management servers. See vSphere Resource Management for more information.

Table 81: Pod and Block Design for This Reference Architecture

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A pod was formed in each site.</td>
<td>This allowed the design, deployment of the block, pod, and Cloud Pod Architecture (CPA) to be validated and documented.</td>
</tr>
<tr>
<td>Each pod contained one or more resource blocks.</td>
<td></td>
</tr>
</tbody>
</table>

Scalability and Availability

One key design principle is to remove single points of failure in the deployment. The numbers, limits and recommendations given in this section were correct at time of writing. For the most current numbers, see the VMware Knowledge Base article VMware Horizon 7 Sizing Limits and Recommendations (2150348).

Connection Server

A single Connection Server supports a maximum of 4,000 sessions (using the Blast Extreme or PCoIP display protocol), although 2,000 is recommended as a best practice. Up to seven Connection Servers are supported per pod with a recommendation of 10,000 sessions in total per pod.

To satisfy the requirements that the proposed solution be robust and able to handle failure, deploy one more server than is required for the number of connections (n+1).

Table 82: Strategy for Deploying Connection Servers

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Five Horizon Connection Servers were deployed.</td>
<td>One Connection Server is recommended per 2,000 concurrent connections.</td>
</tr>
<tr>
<td>These ran on dedicated Windows 2016 VMs located in the internal network.</td>
<td>Four Connection Servers are required to handle the load of the target 8,000 users.</td>
</tr>
<tr>
<td></td>
<td>A fifth server provides redundancy and availability (n+1).</td>
</tr>
</tbody>
</table>

For more information, see "Appendix B: VMware Horizon Configuration" on page 344.

vCenter Server

vCenter Server is the delimiter of a resource block.

The recommended number of VMs that a vCenter Server can typically host depends on the type of Horizon 7 VMs used. The following limits have been tested.
- 8,000 instant-clone VMs
- 4,000 linked-clone or full-clone VMs

Just because VMware publishes these configuration maximums does not mean you should necessarily design to them. Using a single vCenter Server does introduce a single point of failure that could affect too large a percentage of the VMs in your environment. Therefore, carefully consider the size of the failure domain and the impact should a vCenter Server become unavailable.

A single vCenter Server might be capable of supporting your whole environment, but to reduce risk and minimize the impact of an outage, you will probably want to include more than one vCenter Server in your design. You can increase the availability of vCenter Server by using VMware vSphere® High Availability (HA), which restarts the vCenter Server VM in the case of a vSphere host outage. **vCenter High Availability** can also be used to provide an active-passive deployment of vCenter Server appliances, although caution should be used to weigh the benefits against the added complexity of management.

Sizing can also have performance implications because a single vCenter Server could become a bottleneck if too many provisioning tasks run at the same time. Do not just size for normal operations but also understand the impact of provisioning tasks and their frequency.

For example, consider instant-clone desktops, which are deleted after a user logs off and are provisioned when replacements are required. Although a floating desktop pool can be pre-populated with spare desktops, it is important to understand how often replacement VMs are being generated and when that happens. Are user logoff and the demand for new desktops spread throughout the day? Or are desktop deletion and replacement operations clustered at certain times of day? If these events are clustered, can the number of spare desktops satisfy the demand, or do replacements need to be provisioned? How long does provisioning desktops take, and is there a potential delay for users?

Table 83: Implementation Strategy for vCenter Server

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
</table>
| Two resource blocks were deployed per site, each with their own vCenter Server virtual appliance, located in the internal network. | A single resource block and a single vCenter Server are supported for the intended target of 8,000 instant-clone VMs; however, having a single vCenter Server for the entire user environment presents too large a failure domain.  
Splitting the environment across two resource blocks, and therefore over two vCenter Servers reduces the impact of any potential outage.  
This approach also allows each resource block to scale to a higher number of VMs and allow for growth, up to the pod recommendation, without requiring us to rearchitect the resource blocks. |

**JMP Server**

The JMP Server enables the use of JMP workflows by providing a single console to define assignments that can include information about the desktop pool, the App Volumes AppStacks, and User Environment Manager settings. The JMP automation engine communicates with the Connection
Server, App Volumes Managers, and User Environment Manager systems to entitle the user to a desktop.

A single JMP Server is supported per pod. High availability is provided by vSphere High Availability (HA), which restarts the JMP Server VM in the case of a vSphere host outage. VM monitoring with vSphere HA can also attempt to restart the VM in the case of an operating system crash.

If the JMP Server is unavailable, the only functionality affected is the administrator’s ability to create new JMP workflow assignments.

Table 84: Implementation Strategy for the JMP Server

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>One JMP Server was deployed per pod.</td>
<td>This allows for the use of the Horizon Console and workflows to create JMP assignments that include Horizon desktops, App Volumes AppStacks, and User Environment Manager configuration settings.</td>
</tr>
<tr>
<td>The JMP Servers ran on dedicated Windows Server 2016 VMs located in the internal network zones.</td>
<td>Only one JMP Server per pod is supported.</td>
</tr>
</tbody>
</table>

Cloud Connector

The Horizon 7 Cloud Connector is deployed as a virtual appliance from VMware vSphere® Web Client and paired to one of the Connection Servers in the pod. As part of the pairing process, the Horizon 7 Cloud Connector virtual appliance connects the Connection Server to the Horizon Cloud Service to manage the subscription license. With a subscription license for Horizon 7, you do not need to retrieve or manually enter a license key for Horizon 7 product activation. However, license keys are still required for supporting the components, which include vSphere, vSAN, and vCenter Server. These keys are emailed to the https://my.vmware.com contact.

You must have an active My VMware® account to purchase a Horizon 7 license from https://my.vmware.com. You then receive a subscription email with the link to download the Horizon 7 Cloud Connector as an OVA (Open Virtual Appliance) file.

A single Cloud Connector VM is supported per pod. High availability is provided by vSphere HA, which restarts the Cloud Connector VM in the case of a vSphere host outage.

Table 85: Implementation Strategy for the Horizon Cloud Connector

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Cloud Connector per pod was deployed in the internal network.</td>
<td>The environment uses subscription licensing.</td>
</tr>
</tbody>
</table>

Composer Server

The Composer server is required only when using linked clones. Instant clones do not require a Composer server.
Each Composer server is paired with a vCenter Server. For example, in a block architecture where we have one vCenter Server per 4,000 linked-clone VMs, we would also have one Composer server.

High availability is provided by vSphere HA, which restarts the Composer VM in the case of a vSphere host outage. VM monitoring with vSphere HA can also attempt to restart the VM in the case of an operating system crash.

If the VMware View Composer service becomes unavailable, all existing desktops can continue to work just fine. While vSphere HA is restarting the Composer VM, the only impact is on any provisioning tasks within that block, such as image refreshes or recomposes, or creating new linked-clone pools.

**Table 86: Decision Regarding Composer**

<table>
<thead>
<tr>
<th>Decision</th>
<th>A Composer server was not deployed in this environment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Instant clones satisfy all use cases, which means that linked clones and the Composer service are not required.</td>
</tr>
<tr>
<td></td>
<td>If the requirements change, a separate server running the Composer service can easily be added to the design.</td>
</tr>
</tbody>
</table>

### Load Balancing of Connection Servers

For high availability and scalability, VMware recommends that multiple Connection Servers be deployed in a load-balanced replication cluster.

Connection Servers broker client connections, authenticate users, and direct incoming requests to the correct endpoint. Although the Connection Server helps form the connection for authentication, it typically does not act as part of the data path after a protocol session has been established.

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 Connection Server instance. Using a load balancer with multiple Connection Servers also facilitates greater flexibility by enabling IT administrators to perform maintenance, upgrades, and changes in the configuration without impacting users. 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.
Connection Servers require 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 Connection Server. For more information, see the VMware Knowledge Base article [Load Balancing for VMware HorizonView (2146312)](https://kb.vmware.com/s/article/2146312).

**Table 87: Strategy for Using Load Balancers with Connection Servers**

<table>
<thead>
<tr>
<th>Decision</th>
<th>A third-party load balancer was used in front of the Connection Servers. Source IP is configured for the persistence or affinity type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This provides a common namespace for the Connection Servers, which allows for ease of scale and redundancy.</td>
</tr>
</tbody>
</table>

**External Access**

Secure external access for users accessing resources is provided through the integration of Unified Access Gateway (UAG) appliances. We also use load balancers to provide scalability and allow for redundancy. A Unified Access Gateway appliance can be used in front of Connection Servers to provide access to on-premises Horizon 7 desktops and published applications.

For design detail, see "Component Design: Unified Access Gateway Architecture" on page 207.
Figure 74: External Access Through Unified Access Gateway

Table 88: Implementation Strategy for External Access

| Decision | Five standard-size Unified Access Gateway appliances were deployed as part of the Horizon 7 solution. These were located in the DMZ network. |
| Justification | UAG provides secure external access to internally hosted Horizon 7 desktops and applications. One standard UAG appliance is recommended per 2,000 concurrent Horizon connections. Four UAG appliances are required to handle the load of the target 8,000 users. A fifth UAG provides redundancy and availability (n+1). |

For the full detail and diagrams of all the possible ports for different display protocols and between all Horizon 7 components, see the Network Ports in VMware Horizon 7.

**Authentication**

One of the methods of accessing Horizon 7 desktops and applications is through VMware Identity Manager. This requires integration between Connection Servers 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. If you set up the True SSO feature, users can log in using authentication mechanisms other than AD credentials.

See Using SAML Authentication and see Setting Up True SSO for details.

Table 89: Strategy for Authenticating Users Through VMware Identity Manager

<table>
<thead>
<tr>
<th>Decision</th>
<th>SAML authentication was configured to be allowed on the Connection Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>With this configuration, Connection Servers allow VMware Identity Manager to be a dynamic SAML authenticator. This strategy facilitates the launch of Horizon resources from VMware Identity Manager.</td>
</tr>
</tbody>
</table>

True SSO

Many user authentication options are available for logging in to VMware Identity Manager or Workspace ONE. Active Directory credentials are only one of these many authentication options. Ordinarily, using anything other than AD credentials would prevent a user from being able to single-sign-on to a Horizon 7 virtual desktop or published application. After selecting the desktop or published application from the catalog, the user would be prompted to authenticate again, this time with AD credentials.

True SSO provides users with SSO to Horizon 7 desktops and applications regardless of the authentication mechanism used. True SSO uses SAML, where Workspace ONE is the Identity Provider (IdP) and the Horizon 7 server is the Service Provider (SP). True SSO generates unique, short-lived certificates to manage the login process.

Figure 75: True SSO Logical Architecture
Table 90: Implementation Strategy for SSO

<table>
<thead>
<tr>
<th>Decision</th>
<th>True SSO was configured and enabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This feature allows SSO to Horizon resources when launched from VMware Identity Manager, even when the user does not authenticate with Active Directory credentials.</td>
</tr>
</tbody>
</table>

True SSO requires the Enrollment Server service to be installed using the Horizon 7 installation media.

**Design Overview**

For True SSO to function, several components must be installed and configured within the environment. This section discusses the design options and details the design decisions that satisfy the requirements.

**Note:** For more information on how to install and configure True SSO, see Setting Up True SSO in the Horizon 7 Administration documentation and the Setting Up True SSO for Horizon 7 section in "Appendix B: VMware Horizon Configuration" on page 344.

The Enrollment Server is responsible for receiving certificate signing requests (CSRs) from the Connection Server. The enrolment server then passes the CSRs to the Microsoft Certificate Authority to sign using the relevant certificate template. The Enrollment Server is a lightweight service that can be installed on a dedicated Windows Server 2016 instance, or it can co-exist with the MS Certificate Authority service. It cannot be co-located on a Connection Server.

**Scalability**

A single Enrollment Server can easily handle all the requests from a single pod of 10,000 sessions. The constraining factor is usually the Certificate Authority (CA). A single CA can generate approximately 70 certificates per second (based on a single vCPU). This usually increases to over 100 when multiple vCPUs are assigned to the CA VM.

To ensure availability, a second Enrollment Server should be deployed per pod \((n+1)\). Additionally, ensure that the certificate authority service is deployed in a highly available manner, to ensure complete solution redundancy.
With two Enrollment Servers, and to achieve high availability, it is recommended to:

- Co-host the Enrollment Server service with a Certificate Authority service on the same machine.
- Configure the Enrollment Server to prefer to use the local Certificate Authority service.
- Configure the Connection Servers to load-balance requests between the two Enrollment Servers.

Table 91: Implementation Strategy for Enrollment Servers

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two Enrollment Servers</td>
<td>One Enrollment Server is capable of supporting a pod of 10,000 sessions.</td>
</tr>
<tr>
<td>were deployed per Pod.</td>
<td>A second server provides availability (n+1).</td>
</tr>
<tr>
<td>These ran on dedicated</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2016</td>
<td></td>
</tr>
<tr>
<td>VMs located in the</td>
<td></td>
</tr>
<tr>
<td>internal network.</td>
<td></td>
</tr>
<tr>
<td>These servers also had</td>
<td></td>
</tr>
<tr>
<td>the Microsoft Certificate Authority service installed.</td>
<td></td>
</tr>
</tbody>
</table>
Load Balancing of Enrollment Servers

Two Enrollment Servers were deployed in the environment, and the Connection Servers were configured to communicate with both deployed Enrollment Servers. The Enrollment Servers can be configured to communicate with two Certificate Authorities.

By default, the Enrollment Servers use an Active / Failover method of load balancing. It is recommended to change this to round robin when configuring two Enrollment Servers per pod to achieve high availability.

Table 92: Strategy for Load Balancing Between the Enrollment Servers

<table>
<thead>
<tr>
<th>Decision</th>
<th>The Connection Server were configured to load balance requests using round robin between the two Enrollment Servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>With two Enrollment Servers per pod, this is the recommendation when designing for availability.</td>
</tr>
</tbody>
</table>

vSphere HA and VMware vSphere® Storage DRS™ can be used to ensure the maximum availability of the Enrollment Servers. DRS rules are configured to ensure that the devices do not reside on the same vSphere host.

Scaled Single-Site Architecture

The following diagram shows the server components and the logical architecture for a single-site deployment of Horizon 7. For clarity, the focus in this diagram is to illustrate the core Horizon 7 server
components, so it does not include additional and optional components such as App Volumes, User Environment Manager, and VMware Identity Manager.

**Note**: In addition to Horizon 7 server components, the following diagram shows database components, including Microsoft availability group (AG) listeners.

**Figure 78**: On-Premises Single-Site Horizon 7 Architecture

### Multi-site Architecture

This reference architecture documents and validates the deployment of all features of Horizon 7 Enterprise Edition across two data centers.
The architecture has the following primary tenets:

- **Site redundancy** – Eliminate any single point of failure that can cause an outage in the service.
- **Data replication** – Ensure that every layer of the stack is configured with built-in redundancy or high availability so that the failure of one component does not affect the overall availability of the desktop service.

To achieve site redundancy,

- Services built using Horizon 7 are available in two data centers that are capable of operating independently.
- Users are entitled to equivalent resources from both the primary and the secondary data centers.
- Some services are available from both data centers (active/active).
- Some services require failover steps to make the secondary data center the live service (active/passive).

To achieve data replication,

- Any component, application, or data required to deliver the service in the second data center is replicated to a secondary site.
- The service can be reconstructed using the replicated components.
- The type of replication depends on the type of components and data, and the service being delivered.
- The mode of the secondary copy (active or passive) depends on the data replication and service type.

**Cloud Pod Architecture**

A key component in this reference architecture, and what makes Horizon 7 Enterprise Edition truly scalable and able to be deployed across multiple locations, is Cloud Pod Architecture (CPA).

CPA introduces the concept of a global entitlement (GE) through joining multiple pods together into a federation. This feature allows us to provide users and groups with a global entitlement that can contain desktop pools or RDSH-published applications from multiple different pods that are members of this federation construct.

This feature provides a solution for many different use cases, even though they might have different requirements in terms of accessing the desktop resource.

The following figure shows a logical overview of a basic two-site CPA implementation, as deployed in this reference architecture design.
For the full documentation on how to set up and configure CPA, refer to *Administering Cloud Pod Architecture in Horizon 7.*

**Important:** This type of deployment is not a stretched deployment. Each pod is distinct, and all Connection Servers belong to a specific pod and are required to reside in a single location and run on the same broadcast domain from a network perspective.

As well as being able to have desktop pool members from different pods in a global entitlement, this architecture allows for a property called scope. Scope allows us to define where new sessions should or could be placed and also allows users to connect to existing sessions (that are in a disconnected state) when connecting to any of the pod members in the federation.

CPA can also be used within a site:

- To use global entitlements that span multiple resource blocks and pools
- To federate multiple pods on the same site, when scaling above the capabilities of a single pod

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Separate pods were deployed in separate sites. Cloud Pod Architecture was used to federate the pods.</td>
<td>This provides site redundancy and allows an equivalent service to be delivered to the user from an alternate location.</td>
</tr>
</tbody>
</table>

### Active/Passive Architecture

Active/passive architecture uses two or more pods of Connection Servers, with at least one pod located in each data center. Pods are joined together using Cloud Pod Architecture configured with global entitlements.

Active/passive service consumption should be viewed from the perspective of the user. A user is assigned to a given data center with global entitlements, and user home sites are configured. The user actively consumes Horizon 7 resources from that pod and site and will only consume from the other site in the event that their primary site becomes unavailable.
Active/Active Architecture

Active/active architecture also uses two or more pods of Connection Servers, with at least one pod located in each data center. The pods are joined using Cloud Pod Architecture, which is configured with global entitlements.

As with an active/passive architecture, active/active service consumption should also be viewed from the perspective of the user. A user is assigned global entitlements that allow the user to consume Horizon 7 resources from either pod and site. No preference is given to which pod or site they consume from. The challenges with this approach are usually related to replication of user data between sites.

Stretched Active/Active Architecture (Unsupported)

This architecture is unsupported and is only shown here to stress why it is not supported. Connection Servers within a given site must always run on a well-connected LAN segment and therefore cannot be running actively in multiple geographical locations at the same time.
Multi-site Global Server Load Balancing

A common approach is to provide a single namespace for users to access Horizon pods deployed in separate locations.

A Global Server Load Balancer (GSLB) or DNS load balancer solution can provide this functionality and can use placement logic to direct traffic to the local load balancer in an individual site. Some GSLBs can use information such as the user's location to determine connection placement.

The use of a single namespace makes access simpler for users and allows for administrative changes or implementation of disaster recovery and failover without requiring users to change the way they access the environment.

Note the following features of a GSLB:

- GSLB is similar to a Domain Name System (DNS) service in that it resolves a name to an IP address and directs traffic.
- Compared to a DNS service, GSLB can usually apply additional criteria when resolving a name query.
- Traffic does not actually flow through the GSLB to the end server.
- Similar to a DNS server, the GSLB does not provide any port information in its resolution.
- GSLB should be deployed in multiple nodes in an HA or master/slave configuration to ensure that the GSLB itself does not become a point of failure.

Table 94: Strategy for Global Load Balancing

<table>
<thead>
<tr>
<th>Decision</th>
<th>A global server load balancer was deployed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This provides a common namespace so that users can access both sites.</td>
</tr>
</tbody>
</table>
Multi-site Architecture Diagram

The following diagram shows the server components and the logical architecture for a multi-site deployment of Horizon 7. For clarity, the focus in this diagram is to illustrate the core Horizon 7 server components, so it does not include additional and optional components such as App Volumes, User Environment Manager, and VMware Identity Manager.

Virtual Machine Build

Connection Servers and Composer servers run as Windows services. Specifications are detailed in "Appendix A: VM Specifications" on page 326. Each server is deployed with a single network card, and static IP address information is required for each server.

<table>
<thead>
<tr>
<th>Table 95: Operating System Used for Server Components</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Decision</strong></td>
</tr>
<tr>
<td>Windows Server 2016 was used for the OS build.</td>
</tr>
<tr>
<td>IP address information was allocated for each server.</td>
</tr>
<tr>
<td><strong>Justification</strong></td>
</tr>
<tr>
<td>As a best practice, server VMs use the latest supported OS.</td>
</tr>
</tbody>
</table>

Physical Hosting

The Connection Server and Enrollment Server VMs are hosted on vSphere servers. vSphere HA and DRS can be used to ensure maximum availability.

Display Protocol

Horizon 7 is a multi-protocol solution. Three remoting protocols are available when creating desktop pools or RDSH-published applications: Blast Extreme, PCoIP, and RDP.
Table 96: Display Protocol for Virtual Desktops and RDSH-Published Apps

<table>
<thead>
<tr>
<th>Decision</th>
<th>For this design, we leveraged Blast Extreme.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>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 encoding with NVIDIA GRID vGPU. This protocol has full feature and performance parity with PCoIP and is optimized for mobile devices, which can decode video using the H.264 protocol in the device hardware.</td>
</tr>
</tbody>
</table>

Blast Extreme is configured through Horizon 7 when creating a pool. The display protocol can also be selected directly on the Horizon Client side when a user selects a desktop pool.

See the Blast Extreme Display Protocol in VMware Horizon 7 document for more information, including optimization tips.

**VMware vRealize Operations 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 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.

vRealize Operations for Horizon provides end-to-end visibility into Horizon 7 and its supporting infrastructure, enabling administrators to:

- Meet service-level agreements (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

**Architectural Components**

vRealize Operations for Horizon consists of multiple components. These components are described here, and design options are discussed and determined.
vRealize Operations for Horizon consists of the following components:

- vRealize Operations Manager
- Horizon adapter
- Broker agent
- Desktop agent

Other adapters can be added to gather information from other sources; for example, the VMware vSAN management pack can be used to display vSAN storage metrics within the vRealize Operations Manager dashboards.

See [VMware vRealize Operations for Horizon Installation](#) for more detail.

<table>
<thead>
<tr>
<th>Decision</th>
<th>The latest versions of the vRealize Operations Manager and vRealize Operations for Horizon were deployed.</th>
</tr>
</thead>
</table>
| Justification | This meets the requirements for monitoring Horizon 7. |}

**vRealize Operations Manager**

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 consists of multiple nodes (appliances). This provides flexibility and the ability to scale to suit most enterprise deployments while providing high availability.

- **Cluster + remote collector node** – Remote collector nodes are deployed in the data center or on a remote site to capture information before compressing and passing it back to the cluster.

vRealize Operations Manager appliances can perform various node roles, as described in the following table.

**Table 98: vRealize Operations Manager Node Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Management</td>
<td>A cluster consists of a master node and an optional replica node to provide high availability for cluster management. It can also have additional data nodes and optional remote collector nodes. Deploy nodes to separate vSphere hosts to reduce the chance of data loss in the event that a physical host fails. You can use DRS anti-affinity rules to ensure that VMs remain on separate hosts.</td>
</tr>
<tr>
<td>Master Node</td>
<td>The initial, required node in vRealize Operations Manager. All other nodes are managed by the master node. In a single-node installation, the master node manages itself, has adapters installed on it, and performs all data collection and analysis.</td>
</tr>
<tr>
<td>Replica Node</td>
<td>When high availability is enabled on a cluster, one of the data nodes is designated as a replica of the master node and protects the analytics cluster against the loss of a node. Enabling HA within vRealize Operations Manager is not a disaster recovery solution. When you enable HA, you protect vRealize Operations Manager from data loss in the event that a single node is lost by duplicating data. If two or more nodes are lost, there might be permanent data loss.</td>
</tr>
<tr>
<td>Data Analytics Node</td>
<td>Additional nodes in a cluster that can perform data collection and analysis. Larger deployments usually have adapters on the data nodes so that master and replica node resources can be dedicated to cluster management.</td>
</tr>
</tbody>
</table>
Table 98: vRealize Operations Manager Node Roles (Continued)

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Collector Node</td>
<td>If vRealize Operations Manager is monitoring resources in additional data centers, you must use remote collectors and deploy the remote collectors in the remote data centers. Because of latency issues, you might need to modify the intervals at which the configured adapters on the remote collector collect information. VMware recommends that latency between sites not exceed 200ms. Remote collectors can also be used within the same data center as the cluster. Adapters can be installed on these remote collectors instead of the cluster nodes, freeing the cluster nodes to handle the analytical processing.</td>
</tr>
<tr>
<td>Collector Group</td>
<td>A collector group is a collection of nodes (analytic nodes and remote collectors). You can assign adapters to a collector group rather than to a single node. If the node running the adapter fails, the adapter is automatically moved to another node in the collector group.</td>
</tr>
</tbody>
</table>

**Sizing**

vRealize Operations for Horizon can scale to support very high numbers of Horizon sessions. For enterprise deployments of vRealize Operations Manager, deploy all nodes as large or extra-large deployments, depending on sizing requirements and your available resources.

To assess the requirements for your environment, see the VMware Knowledge Base article vRealize Operations Manager 7.0 Sizing Guidelines (57903). Use the spreadsheet attached to this KB to assist with sizing.

Additionally, review the Reference Architecture Overview and Scalability Considerations in the vRealize Operations Manager documentation.

Table 99: Implementation Strategy for vRealize Operations Manager

<table>
<thead>
<tr>
<th>Decision</th>
<th>Two large-sized nodes of vRealize Operations Manager were deployed, forming a cluster. The VM appliances were deployed in the internal network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Two large cluster nodes support the number of Horizon VMs (8,000), and meet requirements for high availability. Although medium-sized nodes would suffice for the current number of VMs, deploying large-sized nodes follows best practice for enterprise deployments and allows for growth in the environment without needing to rearchitect.</td>
</tr>
</tbody>
</table>
Horizon Adapter

The Horizon adapter obtains inventory information from the broker agent and collects metrics and performance data from desktop agents. The adapter passes this data to vRealize Operations Manager for analysis and visualization.

The Horizon adapter runs on the master node or a remote collector node in vRealize Operations Manager. Adapter instances are paired with one or more broker agents to receive communications from them.

Creating a Horizon adapter instance on a remote collector node is recommended in the following scenarios:

- With large-scale environments of over 5,000 desktops, to give better scalability and to offload processing from cluster data nodes.
- With remote data centers to minimize network traffic across WAN or other slow connections.
  - Deploy a remote collector node in each remote data center.
  - Create an adapter instance on each remote collector node and pair each instance with the broker agent that is located in the same data center.
- Creating the Horizon adapter instance on a collector group is not supported.
  - If a failover occurs and the Horizon adapter instance is moved to a different collector in the group, it cannot continue to collect data.
  - To prevent communication interruptions, create the adapter instance on a remote collector node.

Creating more than one Horizon adapter instance per collector is not supported. You can pair the broker agents installed in multiple pods with a single Horizon adapter instance, as long as the total number of desktops in those pods does not exceed 10,000. If you need to create multiple adapter instances, you must create each instance on a different node.

Table 100: Implementation Strategy for Horizon Adapters

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A large remote collector node was deployed for each site. A Horizon adapter instance was created on each of these nodes to collect data from their local Horizon pods.</td>
<td>Separating the Horizon adapter onto a remote collector is recommended in environments of more than 5,000 desktops. The environment is designed for 8,000 users. Horizon adapter instances are not supported on a collector group. Using remote collectors for remote sites allows for efficient data collection.</td>
</tr>
</tbody>
</table>

Broker Agent

The broker agent is a Windows service that runs on a Horizon Connection Server host that collects Horizon 7 inventory information, and then sends that information to the vRealize Operations for
The broker agent is installed on one Connection Server host in each Horizon 7 pod.

Only one broker agent exists in each Horizon 7 pod.

Table 101: Implementation Strategy for the Broker Agent

| Decision | The broker agent was configured to collect information from the event database. The agent was deployed to a single Connection Server within each pod. |
| Justification | The broker agent is a required component to allow vRealize Operations for Horizon to collect data from the Horizon environment. Only a single broker per pod is supported. |

Desktop Agent

The vRealize Operations for Horizon desktop agent runs on each remote desktop or RDSH server VM in the Horizon 7 environment.

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

The vRealize Operations for Horizon desktop agent can be installed as a part of the Horizon Agent installation. See the table in Desktop Agent to find the version included with the version of Horizon Agent being used and determine whether you need to install a newer version separately.

Table 102: Implementation Strategy for the vRealize Operations for Horizon Desktop Agent

| Decision | The desktop agent was installed as part of the standard Horizon Agent and was enabled during installation. |
| Justification | With Horizon Agent 7.7, the included version of the vRealize Operations for Horizon desktop agent supports the selected version of vRealize Operations for Horizon. |
Component Design: Horizon Cloud Service on Microsoft Azure

VMware Horizon® Cloud Service™ is available using a software-as-a-service (SaaS) model. This service comprises multiple software components.

Horizon Cloud Service provides a single cloud control plane, run by VMware, that enables the central orchestration and management of remote desktops and applications in your Microsoft Azure capacity, in the form of one or multiple subscriptions in Microsoft Azure.

VMware is responsible for hosting the Horizon Cloud Service control plane and providing feature updates and enhancements for a software-as-a-service experience. The Horizon Cloud Service is an application service that runs in multiple Amazon Web Services (AWS) regions.

The cloud control plane also hosts a common management user interface called the Horizon Cloud Administration Console, or Administration Console for short. The Administration Console runs in industry-standard browsers. It provides you with a single location for management tasks involving user assignments, virtual desktops, RDSH-published desktop sessions, and applications. This service is currently hosted in three AWS regions: United States, Germany, and Australia. The Administration Console is accessible from anywhere at any time, providing maximum flexibility.
Component Design: Horizon Cloud Service on Microsoft Azure

Horizon Cloud Service on Microsoft Azure Deployment Overview

A successful deployment of VMware Horizon® Cloud Service™ on Microsoft Azure depends on good planning and a robust understanding of the platform. This section discusses the design options and details the design decisions that were made to satisfy the design requirements of this reference architecture.

The core elements of Horizon Cloud Service include:

- Horizon Cloud control plane
- Horizon Cloud Manager VM, which hosts the Administration Console UI
- VMware Unified Access Gateway™
- Horizon Agent
- VMware Horizon® Client™

The following figure shows the high-level logical architecture of these core elements. Other components are shown for illustrative purposes.

Figure 86: Horizon Cloud Service on Microsoft Azure Logical Architecture

This figure demonstrates the basic logical architecture of a Horizon Cloud Service pod on your Microsoft Azure capacity.

- Your Microsoft Azure infrastructure as a service (IaaS) provides capacity.
- Your Horizon Cloud Service control plane is granted permission to create and manage resources with the use of a service principal in Microsoft Azure.
- You provide additional required components, such as Active Directory, as well as optional components, such as a Workspace ONE Connector or RDS license servers.
The Horizon Cloud Service control plane initiates the deployment of the Horizon Cloud Manager VM, Unified Access Gateway appliances for secure remote access, and other infrastructure components that assist with the configuration and management of the Horizon Cloud Service infrastructure.

After the Horizon Cloud Service pod is deployed, you can connect the pod to your own corporate AD infrastructure or create a new AD configuration in your Microsoft Azure subscription. You deploy VMs from the Microsoft Azure marketplace, which are sealed into images, and can be used in RDSH server farms.

With the VDI functionality, you can also create Windows 10 assignments of both dedicated and floating desktops.

Horizon Cloud Service on Microsoft Azure includes the following components and features.

Table 103: Components of Horizon Cloud on Microsoft Azure

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jumpbox</td>
<td>The jumpbox is a temporary Linux-based VM used during environment buildout and for subsequent environment updates and upgrades. One jumpbox is required per Azure pod only during platform buildout and upgrades.</td>
</tr>
<tr>
<td>Management VM</td>
<td>The management VM appliance provides access for administrators and users to operate and consume the platform. One management VM appliance is constantly powered on; a second is required during upgrades.</td>
</tr>
<tr>
<td>Horizon Cloud control plane</td>
<td>This cloud-based control plane is the central location for conducting all administrative functions and policy management. From the control plane, you can manage your virtual desktops and RDSH server farms and assign applications and desktops to users and groups from any browser on any machine with an Internet connection. The cloud control plane provides access to manage all Horizon Cloud pods deployed to your Microsoft Azure infrastructure in a single, centralized user interface, no matter which regional data center you use.</td>
</tr>
</tbody>
</table>
| Horizon Cloud Administration Console | This component of the control plane is the web-based UI that administrators use to provision and manage Horizon Cloud desktops and applications, resource entitlements, and VM images. The Administration Console provides full life-cycle management of desktops and Remote Desktop Session Host (RDSH) servers through a single, easy-to-use web-based console. Organizations can securely provision and manage…
### Table 103: Components of Horizon Cloud on Microsoft Azure (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Agent</td>
<td>This software service, installed on the guest OS of all virtual desktops and RDSH servers, allows them to be managed by Horizon Cloud pods.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>This software, installed on the client device, allows a physical device to access a virtual desktop or RDSH-published application in a Horizon deployment. You can optionally use an HTML client on devices for which installing software is not possible.</td>
</tr>
</tbody>
</table>
| Unified Access Gateway | This gateway is a hardened Linux virtual appliance that allows for secure remote access to the Horizon Cloud environment. This appliance is part of the Security Zone (for external Horizon Cloud access) and the Services Zone (for internal Horizon Cloud access).

The Unified Access Gateway appliances deployed as a Horizon Cloud pod are load balanced by an automatically deployed and configured Microsoft Azure load balancer. The design decisions for load balancing within a pod are already made for you. |
| RDSH servers    | These Windows Server VMs provide published applications and session-based remote desktops to end users.                                                                                                    |

### Table 104: Implementation Strategy for Horizon Cloud Service on Microsoft Azure

<table>
<thead>
<tr>
<th>Decision</th>
<th>A Horizon Cloud Service on Microsoft Azure deployment was designed and integrated with the Workspace ONE platform. This design accommodates an environment capable of scaling to 6,000 concurrent connections or users.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This strategy allowed the design, deployment, and integration to be validated and documented.</td>
</tr>
</tbody>
</table>

### Scalability and Availability

When creating your design, keep in mind that you want an environment that can scale up when necessary, and also remain highly available. Design decisions need to be made with respect to some Microsoft Azure limitations, and with respect to some Horizon Cloud limitations.
**Configuration Maximums for Horizon Cloud Service**

Horizon Cloud on Microsoft Azure has certain configuration maximums you must take into account when making design decisions:

- Up to 2,000 concurrent active connections are supported per Horizon Cloud pod.
- Up to 2,000 desktop and RDSH server VMs are supported per Horizon Cloud pod.
- Up to 2,000 desktop and RDSH server VMs are supported per Microsoft Azure region or subscription.

To handle larger user environments, you can deploy multiple Horizon Cloud pods, but take care to follow the accepted guidelines for segregating the pods from each other. For example, under some circumstances, you might deploy a single pod in two different Microsoft Azure regions, or you might be able to deploy two pods in the same subscription in the same region as long as the IP address space is large enough to handle multiple deployments.

For more information, see [VMware Horizon Cloud Service on Microsoft Azure Service Limits](#).

For information about creating subnets and address spaces, see [Configure the Required Virtual Network in Microsoft Azure](#).

**Table 105: Implementation Strategy for Horizon Cloud Pods**

<table>
<thead>
<tr>
<th>Decision</th>
<th>Three Horizon Cloud pods were deployed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This design meets the requirements for scaling to 6,000 concurrent connections or users.</td>
</tr>
</tbody>
</table>

**Configuration Maximums for Microsoft Azure Subscriptions**

Horizon Cloud on Microsoft Azure leverages Microsoft Azure infrastructure to deliver desktops and applications to end users. Each Microsoft Azure region can have different infrastructure capabilities. You can leverage multiple Microsoft Azure regions for your infrastructure needs.

A Microsoft Azure region is a set of data centers deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network.

These deployments are a part of your Microsoft Azure subscription or subscriptions. A subscription is a logical segregation of Microsoft Azure capacity that you are responsible for. You can have multiple Microsoft Azure subscriptions as a part of the organization defined for you in Microsoft Azure.

A Microsoft Azure subscription is an agreement with Microsoft to use one or more Microsoft cloud platforms or services, for which charges accrue based either on a per-user license fee or on cloud-based resource consumption. For more information on Microsoft Azure subscriptions, see [Subscriptions, licenses, accounts, and tenants for Microsoft’s cloud offerings](#).

Some of the limitations for individual Microsoft Azure subscriptions might impact designs for larger Horizon Cloud on Microsoft Azure deployments. For details about Microsoft Azure subscription limitations, see [Azure subscription and service limits, quotas, and constraints](#). Microsoft Azure has a maximum of 10,000 vCPUs that can be allotted for any given Microsoft Azure subscription per region.
If you plan to deploy 2,000 concurrent VDI user sessions in a single deployment of Horizon Cloud on Microsoft Azure, consider the VM configurations you require. If necessary, you can leverage multiple Microsoft Azure subscriptions for a Horizon Cloud on Microsoft Azure deployment.

**Note:** You might need to request increases in quota allotment for your subscription in any given Microsoft Azure region to accommodate your design.

### Table 106: Implementation Strategy Regarding Microsoft Azure Subscriptions

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple Microsoft Azure subscriptions were used.</td>
<td>This strategy provides an environment capable of scaling to 6,000 concurrent connections or users, where each session involves a VDI desktop with 2 vCPUs (or cores), making a total requirement of 12,000 vCPUs. Because the requirement for 12,000 vCPUs exceeds the maximum number of vCPUs allowed per individual subscription, multiple subscriptions must be used.</td>
</tr>
</tbody>
</table>

### Other Design Considerations

Several cloud- and SaaS-based components are included in a Horizon Cloud on Microsoft Azure deployment. The operation and design of these services are considered beyond the scope of this reference architecture because it is assumed that no design decisions you make will impact the nature of the services themselves. Microsoft publishes a [Service Level Agreement](#) for individual components and services provided by Microsoft Azure.

Horizon Cloud on Microsoft Azure uses [Azure availability sets](#) for some components included in the Horizon Cloud pod—specifically for the two Unified Access Gateways that are deployed as a part of any Internet-enabled deployment.

You can manually build and configure Horizon Cloud pods to provide applications and desktops in the event that you have an issue accessing a Microsoft Azure regional data center. Microsoft has suggestions for candidate regions for disaster recovery. For more information, see [Business continuity and disaster recovery (BCDR): Azure Paired Regions](#).

As was mentioned previously, Horizon Cloud on Microsoft Azure has no built-in functionality to handle business continuity or regional availability issues. In addition, the Microsoft Azure services and features regarding availability are not supported by Horizon Cloud on Microsoft Azure.

### Multi-site Design

You can deploy Horizon Cloud pods to multiple Microsoft Azure regions and manage them all through the Horizon Cloud Administration Console. Each Horizon Cloud pod is a separate entity and is managed individually. VM master images, assignments, and users must all be managed within each pod. No cross-pod entitlement or resource sharing is available.
Component Design: Horizon Cloud Service on Microsoft Azure

Figure 87: Logical Diagram Showing Horizon Cloud on Microsoft Azure Pod Deployments

Table 107: Implementation Strategy for Multi-site Deployments

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A total of three Horizon Cloud pods were deployed to Microsoft Azure regions:</td>
<td>The use of separate Microsoft Azure regions illustrates how to scale and deploy Horizon Cloud for multi-site deployments.</td>
</tr>
<tr>
<td>• Two pods were deployed to the US East Region of Microsoft Azure.</td>
<td></td>
</tr>
<tr>
<td>• One pod was deployed to the US East 2 Region of Microsoft Azure.</td>
<td></td>
</tr>
<tr>
<td>Each region uses a different subscription.</td>
<td></td>
</tr>
</tbody>
</table>

Note that a Split-horizon DNS configuration might be required for a multi-site deployment, depending on how you want your users to access the Horizon Cloud on Microsoft Azure environment.

Entitlement to Multiple Pods

You can manually spread users across multiple Horizon Cloud pods. However, each Horizon Cloud pod is managed individually, and there is no way to cross-entitle users to multiple pods. Although the same user interface is used to manage multiple Horizon Cloud pods, you must deploy separate VM images, RDSH server farms, and assignments on each pod individually.

You can mask this complexity from a user’s point of view by implementing VMware Identity Manager™ so that end users must use VMware Workspace ONE® to access resources. For example, you could entitle different user groups to have exclusive access to different Horizon Cloud on Microsoft Azure deployments, and then join each pod to the same Active Directory.

Note: Although this method works, there is currently no product support for automatically balancing user workloads across Horizon Cloud pods.
External Access

You can configure each pod to provide access to desktops and applications for end users located outside of your corporate network. By default, Horizon Cloud pods allow users to access the Horizon Cloud environment from the Internet. When the pod is deployed with this ability configured, the pod includes a load balancer and Unified Access Gateway instances to enable this access.

If you do not select Internet Enabled Desktops for your deployment, clients must connect directly to the pod and not through Unified Access Gateway. In this case, you must perform some post-deployment steps to create the proper internal network routing rules so that users on your corporate network have access to your Horizon Cloud environment.

If you decide to implement Horizon Cloud on Microsoft Azure so that only internal connections are allowed, you will need to configure your DNS correctly with a Split-horizon DNS configuration.

Optional Components for a Horizon Cloud Service on Microsoft Azure Deployment

You can implement optional components to provide additional functionality and integration with other VMware products:

- **VMware Identity Manager** – Implement and integrate the deployment with VMware Identity Manager so that end users can access all their apps and virtual desktops from a single unified catalog.

- **VMware User Environment Manager™** – Leverage User Environment Manager to provide a wide range of capabilities such as personalization of Windows and applications, contextual policies for enhanced user experience, and privilege elevation so that users can install applications without having administrator privileges.

- **True SSO Enrollment server** – Deploy a True SSO Enrollment Server to integrate with VMware Identity Manager and enable single-sign-on features in your deployment. Users will be automatically logged in to their Windows desktop when they open a desktop from the Workspace ONE user interface.

Shared Services Prerequisites

The following shared services are required for a successful implementation of Horizon Cloud on Microsoft Azure deployment:

- **DNS** – DNS is used to provide name resolution for both internal and external computer names. For more information, see Configure the Virtual Network’s DNS Server.

- **Active Directory** – There are multiple configurations you can use for an Active Directory deployment. You can choose to host Active Directory completely on-premises, completely in Microsoft Azure, or in a hybrid (on-premises and in Microsoft Azure) deployment of Active Directory for Horizon Cloud on Microsoft Azure. For supported configurations, see Active Directory Domain Configurations.

- **RDS licensing** – For connections to RDSH servers, each user and device requires a Client Access License assigned to it. RDS licensing infrastructure can be deployed either on-
premises or in a Microsoft Azure region based on your organization’s needs. For details, see License your RDS deployment with client access licenses (CALs).

- **DHCP** – In a Horizon environment, desktops and RDSH servers rely on DHCP to get IP addressing information. Microsoft Azure provides DHCP services as a part of the platform. You do not need to set up a separate DHCP service for Horizon Cloud Service on Microsoft Azure. For information on how DHCP works in Microsoft Azure, see Address Types in Add, change, or remove IP addresses for an Azure network interface.

- **Certificate services** – The Unified Access Gateway capability in your pod requires SSL/TLS for client connections. To serve Internet-enabled desktops and published applications, the pod deployment wizard requires a PEM-format file. This file provides the SSL/TLS server certificate chain to the pod’s Unified Access Gateway configuration. The single PEM file must contain the entire certificate chain, including the SSL/TLS server certificate, any necessary intermediate CA certificates, the root CA certificate, and the private key.

  For additional details about certificate types used in Unified Access Gateway, see Selecting the Correct Certificate Type. Also see "Environment Infrastructure Design" on page 221 for details on how certificates impact your Horizon Cloud on Microsoft Azure deployment.

### Authentication

One method of accessing Horizon desktops and applications is through VMware Identity Manager. This requires integration between the Horizon Cloud Service 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 when they access a Horizon desktop or application.

- When users are authenticating to VMware Identity Manager and using authentication mechanisms other than AD credentials, True SSO can be used to provide SSO to Horizon resources for the users.

For details, see Integrate a Horizon Cloud Node with a VMware Identity Manager Environment and Configure True SSO for Use with Your Horizon Cloud Environment.

See the section on "Platform Integration" on page 244 for more detail on integrating Horizon Cloud with VMware Identity Manager.

### True SSO

Many user authentication options are available for logging in to VMware Identity Manager or Workspace ONE. Active Directory credentials are only one of these many authentication options. Ordinarily, using anything other than AD credentials would prevent a user from being able to SSO to a Horizon virtual desktop or published application through Horizon Cloud on Microsoft Azure. After selecting the desktop or published application from the catalog, the user would be prompted to authenticate again, this time with AD credentials.

True SSO provides users with SSO to Horizon Cloud on Microsoft Azure desktops and applications regardless of the authentication mechanism used. True SSO uses SAML, where Workspace ONE is the Identity Provider (IdP) and the Horizon Cloud pod is the Service Provider (SP). True SSO
generates unique, short-lived certificates to manage the login process. This enhances security because no passwords are transferred within the data center.

Figure 88: True SSO Logical Architecture

True SSO requires a new service—the Enrollment Server—to be installed.

Table 108: Implementation Strategy for SSO Using Authentication Mechanisms Other Than AD Credentials

| Decision | True SSO was implemented. |
| Justification | This strategy allows for SSO to Horizon Cloud Service on Microsoft Azure desktops and applications through VMware Identity Manager, even when the user does not authenticate with Active Directory credentials. |

Design Overview

For True SSO to function, several components must be installed and configured within the environment. This section discusses the design options and details the design decisions that satisfy the requirements.

The Enrollment Server is responsible for receiving certificate-signing requests from the Connection Server and passing them to the Certificate Authority to sign using the relevant certificate template. The Enrollment Server is a lightweight service that can be installed on a dedicated Windows Server 2016 VM, or it can run on the same server as the MS Certificate Authority service.
Scalability

A single Enrollment Server can easily handle all the requests from a single pod. The constraining factor is usually the Certificate Authority (CA). A single CA can generate approximately 70 certificates per second (based on a single vCPU). This usually increases to over 100 when multiple vCPUs are assigned to the CA VM.

To ensure availability, a second Enrollment Server should be deployed per pod \((n+1)\). Additionally, ensure that the Certificate Authority service is deployed in a highly available manner, to ensure complete solution redundancy.

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

**Figure 89**: True SSO Availability and Redundancy

With two Enrollment Servers, and to achieve high availability, it is recommended to co-host the Enrollment Server service with a Certificate Authority service on the same machine.

**Table 109**: Implementation Strategy for Enrollment Servers

<table>
<thead>
<tr>
<th>Decision</th>
<th>Two Enrollment Servers were deployed in the same Microsoft Azure region as the Horizon Cloud pod. These ran on dedicated Windows Server 2016 VMs. These servers also had the Microsoft Certificate Authority service installed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Having two servers satisfies the requirements of handling 2,000 sessions and provides high availability.</td>
</tr>
</tbody>
</table>

For information on how to install and configure True SSO, see [Configure True SSO for Use with Your Horizon Cloud Environment](#). Also see [Setting Up True SSO for Horizon Cloud Service on Microsoft Azure](#) in "Appendix B: VMware Horizon Configuration" on page 344.
Component Design: App Volumes Architecture

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.

![App Volumes Architecture Diagram](image)

**Figure 90**: App Volumes Just-in-Time Application Model

App Volumes serves two functions. The first is delivery of applications that are not in the master VM 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, organizational unit (OU), or machine, and can be mounted each time the user logs in to a desktop, or at machine startup. For VDI use cases, AppStacks can be mounted either on-demand or at login. With RDSH use cases, because AppStacks are assigned to the machine account, the AppStacks are mounted when the App Volumes service starts.

App Volumes also provides user-writable volumes, which can be used in specific use cases. Writable volumes provide a mechanism to capture user profile data, user-installed applications that are not, or cannot be delivered by AppStacks, or both. This reduces the likelihood that persistent desktops would be required for a use case. User profile data and user-installed applications follow the user as they connect to different virtual desktops.

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Volumes was deployed and integrated into the VMware Horizon® 7 on-premises environment.</td>
<td>This strategy allows the design, deployment, and integration to be validated and documented.</td>
</tr>
<tr>
<td>This design was created for an environment capable of scaling to 8,000 concurrent user connections.</td>
<td></td>
</tr>
</tbody>
</table>

**Table 110**: Implementation Strategy for App Volumes
**Note**: If you are new to App Volumes, VMware recommends the following resources to help you familiarize yourself with the product:

- VMware App Volumes Product Page
- VMware App Volumes Technical Overview (video)
- Horizon 7 Enterprise – JMP, App Volumes and User Environment Manager (hands-on lab)

For additional hands-on learning, consider this three-day course on implementing App Volumes and User Environment Manager on Horizon 7.

**Architecture Overview**

The App Volumes Agent is installed on nonpersistent guest VMs. The agents communicate with the App Volumes Manager instances to determine AppStack and writable volumes entitlements. AppStacks and writable volumes virtual disks are attached to the guest VM, making applications and personalized settings available to end users.

![Diagram of App Volumes Logical Components](image)

*Figure 91: App Volumes Logical Components*

The components and features of App Volumes are described in the following table.
## Table 111: App Volumes Components and Concepts

<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  &lt;br&gt; • Broker for App Volumes Agent for the assignment of applications and writable volumes</td>
</tr>
<tr>
<td>App Volumes Agent</td>
<td>• Virtual desktops or RDSH servers running the App Volumes Agent  &lt;br&gt; • File system and registry abstraction layer running on the target system  &lt;br&gt; • Virtualizes file system writes as appropriate (when used with an optional writable volume)</td>
</tr>
<tr>
<td>AppStack volumes</td>
<td>• Read-only volume containing applications  &lt;br&gt; • One or more AppStacks per user or machine  &lt;br&gt; • Deploys apps to VDI or RDSH</td>
</tr>
<tr>
<td>Writable volume</td>
<td>• Read-write volume that persists changes written in the session, including user-installed applications and user profile  &lt;br&gt; • One writable volume per user  &lt;br&gt; • Only available with user or group assignments  &lt;br&gt; • User writable volumes are not applicable to RDSH</td>
</tr>
<tr>
<td>Database</td>
<td>• A Microsoft SQL database that contains configuration information for AppStacks, writable volumes, and user entitlements  &lt;br&gt; • Should be highly available</td>
</tr>
<tr>
<td>Active Directory</td>
<td>• Environment used to assign and entitle users to AppStacks and writable volumes</td>
</tr>
<tr>
<td>VMware vCenter Server®</td>
<td>• App Volumes uses vCenter Server to connect to resources within the VMware vSphere® environment  &lt;br&gt; • Manages vSphere hosts for attaching and detaching AppStacks and writable volumes to target VMs</td>
</tr>
</tbody>
</table>
Table 111: App Volumes Components and Concepts (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning VMs</td>
<td>• Clean Windows VM with App Volumes Agent</td>
</tr>
<tr>
<td></td>
<td>• Provisions and updates applications into an AppStack</td>
</tr>
<tr>
<td>Storage group (not shown)</td>
<td>• Group of datastores used to replicate AppStacks and distribute writable volumes</td>
</tr>
</tbody>
</table>

The following figure shows the high-level logical architecture of the App Volumes components, scaled out with multiple App Volumes Manager servers using a third-party load balancer.

**Figure 92: App Volumes Logical Architecture**

**Key Design Considerations**

- Always use at least two App Volumes Manager servers, preferably configured behind a load balancer.
  
  **Note:** This setup requires a shared SQL Server.

- An App Volumes instance is bounded by the SQL database.

- Any kernel mode applications should reside in the base image and not in an AppStack.

- Use storage groups (if you are not using VMware vSAN™) to aggregate load and IOPS.
  
  **Note:** AppStacks are very read intensive.

- Storage groups may still be applicable to vSAN customers for replicating AppStacks. See "Multi-site Design Using Separate Databases" on page 192 for more information.

- Place AppStacks on storage that is optimized for read (100 percent read).
- Place writable volumes on storage optimized for random IOPS (50/50 read/write).
- Assign as few AppStacks as possible per user or device. See the VMware Knowledge Base article [VMware App Volumes Sizing Limits and Recommendations (67354)] for the recommended number of AppStacks per VM.
- App Volumes version 2.14 and later defaults to an optimized Machine Managers configuration. Use the default configuration and make changes only when necessary.

![Machine Managers Configuration](image)

**Figure 93**: Default Machine Managers Configuration

**Note**: With previous versions of App Volumes, configuring the Mount ESXi option or, mount on host was recommended to reduce the load on vCenter Server and improve App Volumes performance. App Volumes 2.14 and later provides new optimizations in the communication with vCenter Server. Most implementations will no longer benefit from enabling the Mount ESXi option.

You can enable the Mount Local storage option in App Volumes to check local storage first and then check central storage. AppStacks are mounted faster if stored locally to the ESXi (vSphere) host. Place VMDKs on local storage and, as a safeguard, place duplicates of these VMDKs on central storage in case the vSphere host fails. Then the VMs can reboot on other hosts that have access to the centrally stored VMDKs.
If you choose to enable Mount ESXi or Mount Local, all vSphere hosts must have the same user credentials. Root-level access is not required. See Create a Custom vCenter Role for more information.

**Network Ports for App Volumes**

A detailed discussion of network requirements for App Volumes is outside of the scope of this guide. See Network connectivity requirements for VMware App Volumes. See Network Ports in VMware Horizon 7 for a comprehensive list of ports requirements for VMware Horizon®, App Volumes, and much more.

**App Volumes in a Horizon 7 Environment**

One key concept in a VMware Horizon® 7 environment design is the use of pods and blocks, which gives us a repeatable and scalable approach.

See the Horizon Pod and Block section of "Component Design: Horizon 7 Architecture" on page 132 for more information on pod and block design.

Consider the Horizon 7 block design and scale when architecting App Volumes.

**Table 112: Strategy for Deploying App Volumes in Horizon 7 Pods**

<table>
<thead>
<tr>
<th>Decision</th>
<th>An App Volumes Manager instance was deployed in each pod in each site. The App Volumes machine manager was configured for communication with the vCenter Server in each resource block.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Standardizing on the pod and block approach simplifies the architecture and streamlines administration.</td>
</tr>
</tbody>
</table>

In a production Horizon 7 environment, it is important to adhere to the following best practices:

- Sizing and scaling best practices, as documented in the Horizon 7 Architecture Planning guide
- vSphere scalability best practices, as documented in Performance Best Practices for VMware vSphere 6.7
- vSphere architectural best practices, as documented in the vSphere Resource Management guide

**Scalability and Availability**

As with all server workloads, it is strongly recommended that enterprises host App Volumes Manager servers as vSphere virtual machines. vSphere availability features such as cluster HA, VMware vSphere® Replication™, and VMware Site Recovery Manager™ can all complement App Volumes deployments and should be considered for a production deployment.

In production environments, avoid deploying only a single App Volumes Manager server. It is far better to deploy an enterprise-grade load balancer to manage multiple App Volumes Manager servers connected to a central, resilient SQL Server database instance.
As with all production workloads that run on vSphere, underlying host, cluster, network, and storage configurations should adhere to VMware best practices with regard to availability. See the vSphere Availability Guide for more information.

App Volumes Managers

App Volumes Managers are the primary point of management and configuration, and they broker volumes to agents. For a production environment, deploy at least two App Volumes Manager servers. App Volumes Manager is stateless—all of the data required by App Volumes is located in a SQL database. Deploying at least two App Volumes Manager servers ensures the availability of App Volumes services and distributes the user load.

For more information, see the VMware Knowledge Base article VMware App Volumes Sizing Limits and Recommendations (67354)

Although two App Volumes Managers might support the 8,000 concurrent users design, additional managers are necessary to accommodate periods of heavy concurrent usage, such as for logon storms.

Table 113: Strategy for Scaling App Volumes

| Decision | Four App Volumes Manager servers were deployed with a load balancer. |
| Justification | This strategy satisfies the requirements for load and provides redundancy. |

Multiple-vCenter-Server Considerations

Configuring multiple vCenter Servers is a way to achieve scale for a large Horizon 7 pod, for multiple data centers, or for multiple sites.

With machine managers, you can use different credentials for each vCenter Server, but vSphere host names and datastore names must be unique across all vCenter Server environments. After you have enabled multi-vCenter-Server support in your environment, it is not recommended to revert back to a single vCenter Server configuration.

Note: In a multiple-vCenter-Server environment, an AppStack is tied to storage that is available to each vCenter Server. It is possible that an AppStack visible in App Volumes Manager could be assigned to a VM that does not have access to the storage. To avoid this issue, use storage groups to replicate AppStacks across vCenter Servers.

Multiple-AD-Domain Considerations

App Volumes supports environments with multiple Active Directory domains, both with and without the need for trust types configured between them. See Configuring and Using Active Directory for more information.

An administrator can add multiple Active Directory domains through the Configuration > Active Directories tab in App Volumes Manager. An account with a minimum of read-only permissions for each domain is required. You must add each domain that will be accessed for App Volumes by any computer, group, or user object. In addition, non-domain-joined entities are now allowed by default.
vSphere Considerations

Host configurations have significant impact on performance at scale. Consider all ESXi best practices during each phase of scale-out. To support optimal performance of AppStacks and writable volumes, give special consideration to the following host storage elements:

- Host storage policies
- Storage network configuration
- HBA or network adapter (NFS) configuration
- Multipath configuration
- Queue-depth configuration

For best results, follow the recommendations of the relevant storage partner when configuring hosts and clusters.

For more information, see the vSphere Hardening Guide.

Load Balancing

Use at least two App Volumes Managers in production and configure each App Volumes Agent to point to a load balancer, or use a DNS server that resolves to each App Volumes Manager in a round-robin fashion.

For high performance and availability, an external load balancer is required to balance connections between App Volumes Managers.

The main concern with App Volumes Managers is handling login storms. During the login process, user-based AppStacks and writable volumes must be attached to the guest OS in the VMs. The greater the number of concurrent attachment operations, the more time it might take to get all users logged in.

For App Volumes 2.15, the exact number of users each App Volumes Manager can handle will vary, depending on the load and the specifics of each environment. See the VMware Knowledge Base article VMware App Volumes Sizing Limits and Recommendations (67354) for tested limits of users per App Volumes Manager server and login rates.

VMware recommends that you test the load and then size the number of App Volumes Manager servers appropriately. To size this design, we assumed each App Volumes Manager was able to handle 2,000 users.

Table 114: Strategy for App Volumes Scalability and Availability

| Decision | A third-party load balancer was placed in front of the App Volumes Manager servers. |
| Justification | The load balancer properly distributes load and keeps the services available in the event of an issue with one of the managers. |

The following figure shows how virtual desktops and RDSH-published applications can point to an internal load balancer that distributes the load to two App Volumes Managers.
In the following list, the numbers correspond to numbers in the diagram.

1. No additional configuration is required on the App Volumes Manager servers.

2. Load balancing of App Volumes Managers should use the following:
   - Ports = 80, 443
   - Persistent or session stickiness = Hash all Cookies
   - Timeout = 6 minutes
   - Scheduling method = round robin
   - HTTP headers = X-Forward-For
   - Real server check = HTTP

**Database Design**

App Volumes 2.15 uses a Microsoft SQL Server database to store configuration settings, assignments, and metadata. This database is a critical aspect of the design, and it must be accessible to all App Volumes Manager servers.

An App Volumes instance is defined by the SQL database. Multiple App Volumes Manager servers may be connected to a single SQL database.

For nonproduction App Volumes environments, you can use the Microsoft SQL Server Express database option, which is included in the App Volumes Manager installer. Do not use SQL Server Express for large-scale deployments or for production implementations.
App Volumes works well with both SQL Server failover cluster instances (FCI) and SQL Server Always On availability groups. Consult with your SQL DBA or architect to decide which option better fits your environment.

**Table 115: Implementation Strategy for the SQL Server Database**

<table>
<thead>
<tr>
<th>Decision</th>
<th>A SQL database was placed on a highly available Microsoft SQL Server. This database server was installed on a Windows Server Failover Cluster, and an Always On availability group was used to provide high availability.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>An Always On availability group achieves automatic failover. Both App Volumes Manager servers point to the availability group listener for the SQL Server.</td>
</tr>
</tbody>
</table>

**Storage**

A successful implementation of App Volumes requires several carefully considered design decisions with regards to disk volume size, storage IOPS, and storage replication.

**AppStack and Writable Volume Template Placement**

When new AppStacks and writable volumes are deployed, predefined templates are used as the copy source. Administrators should place these templates on a centralized shared storage platform. As with all production shared storage objects, the template storage should be highly available, resilient, and recoverable. See Configuring Storage for AppStacks and Writable Volumes to get started.

**Free-Space Considerations**

AppStack sizing and writable volume sizing are critical for success in a production environment. AppStack volumes should be large enough to allow applications to be installed and should also allow for application updates. AppStacks should always have at least 20 percent free space available so administrators can easily update applications without having to resize the AppStack volumes.

Writable volumes should also be sufficiently sized to accommodate all users’ data. Storage platforms that allow for volume resizing are helpful if the total number of writable volume users is not known at the time of initial App Volumes deployment.

Because AppStacks and writable volumes use VMware vSphere® VMFS, the thin-provisioned, clustered Virtual Machine File System from VMware, storage space is not immediately consumed. Follow VMware best practices when managing thin-provisioned storage environments. Free-space monitoring is essential in large production environments.

**Writable Volumes Delay Creation Option**

Two policy options can complicate free-space management for writable volumes:

- The option to create writable volumes on the user’s next login means that storage processes and capacity allocation are impacted by user login behavior.
The option to restrict writable volume access (and thus initial creation) to a certain desktop or group of desktops can also mean that user login behavior dictates when a writable volume template is copied.

In a large App Volumes environment, it is not usually a good practice to allow user behavior to dictate storage operations and capacity allocation. For this reason, VMware recommends that you create writable volumes at the time of entitlement, rather than deferring creation.

Storage Groups

App Volumes uses a construct called storage groups. A storage group is a collection of datastores that are used to serve AppStacks or distribute writable volumes.

The two types of storage groups are:

- **AppStack storage groups** – Used for replication.

- **Writable volume storage groups** – Used for distribution.

In App Volumes 2.15, 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 vCenter Servers allows AppStacks to be replicated across vCenter Servers and datastores.

Two automation options for AppStack storage groups are available:

- **Automatic replication** – Any AppStack placed on any datastore in the storage group is replicated across all datastores in the group every four hours.

- **Automatic import** – After replication, the AppStack is imported into App Volumes Manager and is available for assignment from all datastores in the storage group.

When using AppStack storage groups, the App Volumes Manager manages the connection to the relevant AppStack, based on location and number of attachments across all the datastores in the group.

Storage Groups for Scaling App Volumes

Once created, AppStacks are read-only. As more and more users are entitled to and begin using a given AppStack, the number of concurrent read operations increases. With enough users reading from a single AppStack, performance can be negatively impacted. Performance can be improved by creating one or more copies of the AppStack on additional datastores, and spreading user access across them.

AppStacks can be automatically replicated to multiple datastores in a storage group. This replication creates multiple copies of AppStacks. Access is spread across the datastores, ensuring good performance as App Volumes scales to serve more end users. See the VMware Knowledge Base article [VMware App Volumes Sizing Limits and Recommendations (67354)](https://kb.vmware.com/kb/67354) for the recommended number of concurrent attachments per AppStack.
Storage Groups for Multi-site App Volumes Implementations

Storage groups can also be used to replicate AppStacks from one site to another in multi-site App Volumes configurations. By using a non-attachable datastore available to hosts in each site, AppStacks created at one site can be replicated to remote sites to serve local users.

A datastore configured as non-attachable is ignored by the App Volumes Manager while mounting volumes, and the storage can be used solely for replication of AppStacks. This means you can use a datastore on slow or inexpensive storage for replication, and use high-speed, low-latency storage for storing mountable volumes.

This non-attachable datastore can also be used as a staging area for AppStack creation before deploying to production storage groups. This topic is covered in more detail in the "Multi-site Design Using Separate Databases" on page 192 section and in "Appendix E: App Volumes Configuration" on page 407.

Storage Groups for Writable Volumes

Writable volume storage groups are used to distribute volumes across datastores to ensure good performance as writable volumes are added. See the VMware Knowledge Base article VMware App Volumes Sizing Limits and Recommendations (67354) for the recommended number of writable volumes per datastore.

Table 116: Implementation Strategy for Storage Groups

<table>
<thead>
<tr>
<th>Decision</th>
<th>Storage groups were set up to replicate AppStacks between datastores. An NFS datastore was used as a common datastore between the different vSphere clusters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This strategy allows the AppStacks to be automatically replicated between VMFS datastores, between vSAN datastores and between vSphere clusters.</td>
</tr>
</tbody>
</table>

AppStacks

This section provides guidance about creating, sizing, scaling, provisioning, configuring, and updating AppStacks.

AppStack Templates

By default, a single 20-GB AppStack template is deployed in an App Volumes environment. This template is thin-provisioned and is provided in both a VMDK and VHD format. This template can be copied and customized, depending on how large the AppStack needs to be for a given deployment scenario. For more information, see the VMware Knowledge Base article Creating a new App Volumes AppStack template VMDK smaller than 20 GB (2116022).

If you have AppStacks from a previous 2.x release of App Volumes, they will continue to work with App Volumes 2.15. However, additional features or fixes included in later versions are not applied to AppStacks created with earlier versions.
AppStacks at Scale

The number of AppStacks that can be attached to a given VM is technically limited by Windows and vSphere. In practice, the number of AppStacks attached to a VM should be considerably fewer. See the VMware Knowledge Base article VMware App Volumes Sizing Limits and Recommendations (67354) for guidance. Attaching AppStacks involves the following processes:

- The disk mount (mounting the AppStack VMDK to the VM)
- The virtualization process applied to the content in the AppStack (merging files and registry entries with the guest OS)

The time required to complete the virtualization process varies greatly, depending on the applications contained in a given AppStack. The more AppStacks that need to be attached, the longer this operation might take to complete.

AppStacks may be assigned to a number of Active Directory objects, which has implications for the timing and specifics of which volumes are attached. See Assigning and Attaching AppStacks.

Recommended Practices for AppStacks in Production Environments

The size of the default AppStack is 20 GB. The default writable volume template is 10 GB. In some environments, it might make sense to add larger or smaller templates. For information on creating multiple, custom-sized templates, see the VMware Knowledge Base article Creating a New App Volumes AppStack template VMDK smaller than 20 GB (2116022).

Keep the total number of AppStacks assigned to a given user or computer relatively small. This can be accomplished by adding multiple applications to each AppStack. Group applications in such a way as to simplify distribution.

The following is a simple example for grouping applications into AppStacks:

- Create an AppStack containing core applications (apps that most or all users should receive). This AppStack can be assigned to a large group or OU.
- Create an AppStack for departmental applications (apps limited to a department). This AppStack can be assigned at a group or departmental level.

For traditional storage (VMFS, NFS, and so on):

- Do not place AppStacks and VMs on the same datastore.
- Use storage groups for AppStacks when AppStacks are assigned to a large population of users or desktops. This helps to distribute the aggregated I/O load across multiple datastores, while keeping the assignments consistent and easy to manage.

For vSAN:

- AppStacks and VMs can be placed on a single datastore.
- Storage groups for AppStacks are not applicable in a vSAN implementation.
See the VMware Knowledge Base article VMware App Volumes Sizing Limits and Recommendations (67354) for recommendations on number of user mounts per AppStack.

**Recommended Practices for Creating and Provisioning AppStacks**

Consider the following best practices when creating and provisioning AppStacks:

- The following characters cannot be used when naming AppStacks: & " ' < >

- Provision AppStacks on a clean master image that resembles as closely as possible the target environment where the AppStack is to be deployed. For example, the provisioning VM and target should be at the same OS patch and service pack level and, if applications are included in the master image, they should also be in the provisioning VM.

- Consider using the App Volumes Packaging Machine template in the VMware OS Optimization Tool to configure your provisioning VM.

- Do not use a provisioning machine where you have previously installed and then uninstalled any of the applications that you will capture. Uninstalling an application might not clean up all remnants of the application, and the subsequent App Volumes application capture might not be complete.

- Always take a snapshot of your provisioning VM before provisioning or attaching any AppStacks to it. If any AppStacks have been assigned to the VM, or if the VM has been used previously for provisioning, revert that VM to the clean snapshot before provisioning a new AppStack.

**Recommended Practices for Configuring AppStacks**

When there is an application conflict, the last AppStack virtualized “wins.” The Override Precedence option allows you to define AppStack ordering. It might be necessary to reorder AppStacks in order to remove application conflicts. This option can also be used to ensure that an AppStack with a supporting application loads before an AppStack with an application that requires that supporting application. See AppStacks Precedence for additional information.

In the App Volumes Manager, use the Override Precedence option. On the Directory tab, click the Users, Computers, or Groups sub-tab and select one of the objects.

**Recommended Practices for Updating and Assigning Updated AppStacks**

You update applications on the original AppStack from the App Volumes Manager console. This process clones the original AppStack, so the existing applications are available to users. The new AppStack with the updated applications is provisioned at next login.

Consider the following best practices when updating and assigning updated AppStacks:

- After updating an AppStack, unassign the original AppStack before assigning the updated AppStack. Failure to unassign the old AppStack before assigning the new one can result in application conflicts because most Windows applications cannot run side by side with older versions of themselves in a Windows OS.
- Unassign AppStacks to take effect on next login rather than immediately. Removing applications while in use could result in user data loss and OS instability.


**Horizon Integration**

Although not required, App Volumes is often implemented in a Horizon environment. Consider the following when integrating App Volumes and Horizon.

- Do not attempt to include the Horizon Agent in an AppStack. The Horizon Agent should be installed in the master image.

- Do not use a Horizon VM (guest OS with Horizon Agent installed) as a clean provisioning VM. You must uninstall the Horizon Agent if it is present. Dependencies previously installed by the Horizon Agent, such as Microsoft side-by-side (SxS) shared libraries, are not reinstalled, and therefore are not captured by the App Volumes provisioning process.

- See Installation order of End User Computing Agents for User Environment Manager (UEM) and App Volumes (2118048) for information on agent installation order.

**Performance Testing for AppStacks**

Test AppStacks immediately after provisioning to determine their overall performance. Using a performance analytics tool, such as VMware vRealize® Operations Manager™, gather virtual machine, host, network, and storage performance information for use when AppStacks are operated on a larger scale. Do not neglect user feedback, which can be extremely useful for assessing the overall performance of an application.

Because App Volumes provides an application container and brokerage service, storage performance is very important in a production environment. AppStacks are read-only. Depending on utilization patterns, the underlying shared storage platform might have significant read I/O activity. Consider using flash and hybrid-flash storage technologies for AppStacks.

This evaluation can be time-consuming for the administrator, but it is necessary for any desktop-transformation technology or initiative.

**ThinApp Integration with AppStacks**

Network latency is often the limiting factor for scalability and performance when deploying ThinApp packages in streaming mode. Yet ThinApp provides exceptional application-isolation capabilities. With App Volumes, administrators can present ThinApp packages as dynamically attached applications that are located on storage rather than as bits that must traverse the data center over the network.

Using App Volumes to deliver ThinApp packages removes network latency due to Windows OS and environmental conditions. It also allows for the best of both worlds—real-time delivery of isolated and troublesome applications alongside other applications delivered on AppStacks.

With App Volumes in a virtual desktop infrastructure, enterprises can take advantage of local deployment mode for ThinApp packages. ThinApp virtual applications can be provisioned inside an
AppStack using all the storage options available for use with AppStacks. This architecture permits thousands of virtual desktops to share a common ThinApp package through AppStacks without the need to stream or copy the package locally.

**Microsoft Office Applications on AppStacks**

For deploying Microsoft Office applications through App Volumes, see the VMware knowledge base article [VMware App Volumes 2.x with Microsoft Office Products (2146035)](https://kb.vmware.com/kb/2146035).

**Office Plug-Ins and Add-Ons**

The most straightforward method is to provision Microsoft Office plug-ins or add-ons in the same AppStack as the Microsoft Office installation.

However, if necessary, you can provision plug-ins or add-ons in AppStacks that are separate from the AppStacks that contain the Microsoft applications to which they apply. Before provisioning the plug-in or add-on, install the primary application natively in the OS of the provisioning VM.

AppStack precedence is important. Attach the Office AppStack first, and then attach the AppStack containing plug-ins or add-ons. You can define AppStack precedence from the App Volumes Manager console.

**Note:** Ensure the plug-in or add-on is at the same version as the Microsoft Office AppStack. This includes any patches or updates.

**Recommended Practices for Installing Office**

VMware recommends that you install core Microsoft Office applications in the base virtual desktop image, and create one AppStack for non-core Microsoft Office applications, such as Visio, Project, or Visio and Project together.

To provision the AppStack with Visio and Project, use a provisioning machine with the same core Microsoft Office applications as on the base image. After the AppStack is created, you can assign the AppStack to only the users who require these non-core Microsoft Office applications.

**RDSH Integration with AppStacks**

App Volumes supports AppStack integration with Microsoft RDSH-published desktops and published applications. AppStacks are assigned to RDSH servers rather than directly to users. AppStacks are attached to the RDSH server when the machine is powered on and the App Volumes service starts, or when an administrator chooses the Attach AppStack Immediately option. Users are then entitled to the RDSH-published desktops or applications through the Horizon 7 entitlement process.

**Note:** Writable volumes are not supported with RDSH assignments.

Consider associating AppStacks at the OU level in Active Directory, rather than to individual computer objects. This practice reduces the number of AppStack entitlements and ensures AppStacks are always available as new hosts are created and existing hosts are refreshed.

Entitling AppStacks to an OU where Horizon 7 instant-clone RDSH server farms are provisioned ensures that all hosts are configured exactly alike, and supports dynamic growth of farms with minimal administrative effort.
Create dedicated AppStacks for RDSH servers. Do not reuse an AppStack that was originally created for a desktop OS.

When creating the AppStack, install applications on a provisioning machine that has the same operating system as that used on the deployed RDSH servers. Before installing applications, switch the RDSH server to RD-Install mode. For more information, see Learn How To Install Applications on an RD Session Host Server.

See Infrastructure and Networking Requirements to verify that the Windows Server version you want to use for RDSH is supported for the App Volumes Agent.


**Application Suitability for AppStacks**

Most Windows applications work well with App Volumes, including those with services and drivers, and require little to no additional interaction. If you need an application to continue to run after the user logs out, it is best to natively install this application on the desktop or desktop image.

The following is a brief description of situations and application types where App Volumes might need special attention to work properly or where the application would work best within the master image, rather than in an AppStack. This section addresses these special cases in detail.

**Applications That Work Best in the Master Image**

Applications that should be available to the OS in the event that an AppStack or writable volume is not present should remain in the master image and not in an App Volumes container. These types of applications include antivirus, Windows updates, and OS and product activations, among others. Applications that should be available to the OS when no user is logged in should also be placed in the master image.

Similarly, applications that integrate tightly with the OS should not be virtualized in an AppStack. If these apps are removed from the OS in real time, they can cause issues with the OS. Again, if the application needs to be present when the user is logged out, it must be in the master image and not in an AppStack. Applications that start at boot time or need to perform an action before a user is completely logged in, such as firewalls, antivirus, and Microsoft Internet Explorer, fall into this category.

Applications that use the user profile as part of the application installation should not be virtualized in an App Stack. App Volumes does not capture the user profile space C: \users\<username>. If, as part of its installation process. If an application places components into this space, those components will not be recorded as part of the provisioning process. If this happens, undesired consequences or failure of the application might result when the application is captured in an AppStack.

**Applications Whose Components Are Not Well Understood**

In the rare event that an issue with an application does present itself, it is important to have a thorough understanding of how the application functions. Understanding the processes that are spawned, file and registry interactions, and where files are created and stored is useful troubleshooting information.
App Volumes is a delivery mechanism for applications. It is important to understand that App Volumes does an intelligent recording of an installation during the provisioning process and then delivers that installation. If the installation is not accurate or is configured incorrectly, the delivery of that application will also be incorrect (“garbage in, garbage out”). It is important to verify and test the installation process to ensure a consistent and reliable App Volumes delivery.

**App Volumes Agent Altitude and Interaction with Other Mini-Filter Drivers**

The App Volumes Agent is a mini-filter driver. Microsoft applies *altitudes* to filter drivers. The concept is that the larger the number, the “higher” the altitude. Mini-filter drivers can see only the other filter drivers that are at a higher altitude. The actions at a lower altitude are not seen by filter drivers operating at a higher altitude.

The lower-altitude mini-filter drivers are the first to interact with a request from the OS or other applications. Generally speaking, the requests are then given to the next mini-filter driver in the stack (next highest number) after the first driver finishes processing the request. However, this is not always the case because some mini-filter drivers might not release the request and instead “close” it out to the OS or application.

In the case where a request is closed, the subsequent mini-filter drivers will never see the request at all. If this happens with an application running at a lower altitude than App Volumes, the App Volumes mini-filter driver will never get a chance to process the request, and so will not be able to virtualize the I/O as expected.

This is the primary reason that certain applications that use a mini-filter driver should be disabled or removed from the OS while you install applications with App Volumes. There might be additional scenarios where App Volumes Agent should be disabled, allowing other applications to install correctly in the base OS.

**Other Special Considerations**

The following guidelines will also help you determine whether an application requires special handling during the virtualization process or whether virtualization in an AppStack is even possible:

- **Additional application virtualization technologies** – Other application virtualization technologies (Microsoft App-V, ThinApp, and others) should be disabled during provisioning because the filter drivers could potentially conflict and cause inconsistent results in the provisioning process.

- **Mixing of 32- and 64-bit OS types** – The OS type (32- or 64-bit) of the machine that the AppStack is attached to should match the OS type that applications were provisioned on. Mixing of application types in App Volumes environments follows the same rules as Windows application types—that is, if a 32-bit application is certified to run in a 64-bit environment, then App Volumes supports that configuration also.

- **Exceptional applications** – Some applications just do not work when installed on an App Volumes AppStack. There is no list of such applications, but an administrator might discover an issue where an application simply does not work with App Volumes.

In summary, most applications work well with App Volumes, with little to no additional interaction needed. However, you can save time and effort by identifying potential problems early, by looking at the application type and use case before deciding to create an AppStack.
Writable Volumes

Writable volumes can be used to persist a variety of data as users roam between nonpersistent desktop sessions. As is described in **App Volumes 2.14 Technical What's New Overview**, Outlook OST and Windows Search Index files are automatically redirected to writable volumes, improving search times for customers using these technologies. See **Working with Writable Volumes** for information on creating and managing writable volumes.

Writable volumes are often complemented by VMware User Environment Manager™ to provide a comprehensive profile management solution. For technical details on using App Volumes with User Environment Manager, see the VMware blog post **VMware User Environment Manager with VMware App Volumes**.

Note the key differences between AppStacks and writable volumes:

- AppStack VMDKs are mounted as read-only and can be shared among all desktop VMs within the data center.
- Writable volumes are dedicated to individual users and are mounted as the user authenticates to the desktop. Writable volumes are user-centric and roam with the user for nonpersistent desktops.

Writable Volume Templates

Several writable volume templates are available to suit different use cases. See **Configuring Storage for AppStacks and Writable Volumes** for options.

The UIA (user-installed applications)-only template provides persistence for user-installed applications. After a writable volume with the UIA-only template is created and assigned to a user, that user can install and configure applications as they normally would. The installation is automatically redirected to the writable volume, and persisted between desktop sessions.

**Note:** For this functionality to work properly, users require account permissions in Windows that allow application installation. You may also use **User Environment Manager Privilege Elevation** to complement UIA-only writable volumes.

### Table 117: Implementation Strategy for App Volumes Writable Volumes

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Writable volumes were created for and assigned to end users who required the ability to install their own applications.</td>
<td>Writable volumes provide added flexibility for end users who are permitted to install software outside of the IT-delivered set of applications.</td>
</tr>
<tr>
<td>The UIA-only writable volume template was used.</td>
<td>The UIA-only template ensures application installation and configuration data is stored, while profile data is managed using other technologies.</td>
</tr>
<tr>
<td></td>
<td>If a writable volume becomes corrupt, applications can be reinstalled without the risk of data loss.</td>
</tr>
</tbody>
</table>
Performance Testing for Writable Volumes

Writable volumes are read-write. Storage utilization patterns are largely influenced by user behavior with regard to desktop logins and logouts, user-installed applications, and changes to local user profiles. Group each set of similar users into use cases, and evaluate performance based on peak average use.

Additional Writable Volumes Operations

See the section Next Steps: Additional Configuration Options for Writable Volumes of "Appendix E: App Volumes Configuration" on page 407.

Recommended Practices for Master Images

Master images should be optimized for VDI or RDSH to ensure the best performance possible in a virtualized environment. Consider using the instructions in Creating an Optimized Windows Image for a VMware Horizon Virtual Desktop when building your master images. The VMware OS Optimization Tool is referenced, and helps optimize Windows desktop and server operating systems for use with Horizon 7.

The OS Optimization Tool includes customizable templates to enable or disable Windows system services and features, per VMware recommendations and best practices, across multiple systems. A template specifically created for an App Volumes packaging (provisioning) machine is also available. Because most Windows system services are enabled by default, the OS Optimization Tool can be used to easily disable unnecessary services and features to improve performance.

Recommended Practices for Client Desktops

When setting up client endpoint devices, consider the following best practices:

- When reverting a desktop VM that is running the App Volumes Agent to a previous snapshot, make sure that the VM is gracefully shut down, to avoid synchronization issues. This is primarily relevant to the provisioning desktop and master VMs for Horizon 7 linked- and instant-clone pools.
- If you are using a Horizon 7 pool, the App Volumes Agent should be installed on the master VM for linked- and instant-clone pools, or on the VM template for full-clone pools, for ease of distribution.
- If using a Horizon 7 linked-clone pool, make sure the Delete or Refresh machine on logoff policy in Desktop Pool Settings is set to Refresh Immediately. This policy ensures that the VMs stay consistent across logins.

Recommended Security Practices for App Volumes

To support a large production environment, there are some important security configurations that administrators should put in place:

- Open only essential, required firewall ports on App Volumes Manager and SQL. Consider using an advanced firewall solution, such as VMware NSX®, to dynamically assign virtual machine firewall policies based on server role.
Replace the default self-signed TLS/SSL certificate with a certificate for App Volumes Manager signed by a reliable certificate authority. See Replacing the Self-Signed Certificate in VMware App Volumes 2.12.

Verify that App Volumes Manager can accept the vCenter Server certificate. App Volumes Manager communicates with vCenter Server over SSL. The App Volumes Manager server must trust the vCenter Server certificate.

**Note:** It is possible to configure App Volumes Manager to accept an unverifiable (self-signed) certificate. Navigate to Configuration > Machine Managers in the management console. Each machine manager (vCenter Server) has a Certificate option that shows the current status of the certificate and allows an administrator to explicitly accept an unverifiable certificate.

Consider using ThinApp to package applications, to take advantage of the security benefits of isolation modes, when required. Each ThinApp package can be isolated from the host system, and any changes, deletions, or additions made by the application to the file system or registry are recorded in the ThinApp sandbox instead of in the desktop operating system.

For writable volumes, determine which end users require ongoing administrator privileges. Writable volumes with user-installed applications require that each desktop user be assigned local computer administrator privileges to allow the installation and configuration of applications.

Some use cases could benefit from temporary, request-based elevated privileges to allow incidental application installation for a specific user or user group. Carefully consider the security risks associated with granting users these elevated privileges.

Create and use an AD user service account specifically for App Volumes. This is good security hygiene and a forensics best practice. It is never a good idea to use a blanket or general-purpose AD user account for multiple purposes within AD.

Consider creating an administrative role in vCenter Server to apply to the App Volumes service account.

**Multi-site Design Using Separate Databases**

VMware recommends designing multi-site implementations using a separate-databases, or multi-instance model. This option uses a separate SQL Server database at each site, is simple to implement and allows for easy scaling if you have more than two sites. Additionally, latency or bandwidth restrictions between sites have little impact on the design.

In this model, each site works independently, with its own set of App Volumes Managers and its own database instance. During an outage, the remaining site can provide access to AppStacks with no intervention required. For detailed information on the failover steps required and the order in which they need to be executed, refer to “Failover with Separate Databases” on page 195.
This strategy makes use of the following components:

- **App Volumes Managers** – At least two App Volumes Manager servers are used in each site for local redundancy and scalability.

- **Load balancers** – Each site has its own namespace for the local App Volumes Manager servers. This is generally a local load balancer virtual IP that targets the individual managers. **Note:** The App Volumes Agent, which is installed in virtual desktops and RDSH servers, must be configured to use the appropriate local namespace.

- **Separate databases** – A separate database is used for each site; that is, you have a separate Windows Server Failover Clustering (WSFC) cluster and an SQL Server Always On availability group listener for each site, to achieve automatic failover within a site.

- **vCenter Server machine managers** – The App Volumes Manager servers at each site point to the local database instance and have machine managers registered only for the vCenter Servers from their own site.

- **Storage groups** – Storage groups containing a common, non-attachable datastore can be used to automatically replicate AppStacks from one site to the other. This common datastore must be visible to at least one vSphere host from each site. **Note:** In some environments, network design might prevent the use of storage group replication between sites. See **Copying an AppStack to another App Volumes Manager instance** for more information about manually copying AppStacks.

- **Entitlement replication** – To make user-based entitlements for AppStacks available between sites, you can reproduce entitlements at each site. You can either manually reproduce the entitlements at each site or use a PowerShell script, which VMware provides. See the "Appendix E: App Volumes Configuration" on page 407. Manually reproducing entitlements can be somewhat streamlined by entitling AppStacks to groups and OUs, rather than individuals.
Table 118: Strategy for Deploying App Volumes in Multiple Sites

| Decision | App Volumes was set up in the second site used for Horizon 7 (on-premises). A separate database and App Volumes instance deployment option was used. An NFS datastore was used as a common datastore among the storage groups to facilitate cross-site AppStack replication. |
| Justification | This strategy provides App Volumes capabilities in the second site. The separate-databases option is the most resilient, provides true redundancy, and can also scale to more than two sites. With AppStacks replicated between sites, the AppStacks are available for use at both locations. |

Configuration with Separate Databases

When installing and configuring the App Volumes Managers in a setup like this, each site uses a standard SQL Server installation.

1. Install the first App Volumes Manager in Site 1. If using Always On availability groups to provide a local highly available database, use the local availability group listener for Site 1 when configuring the ODBC connection. **Important**: For step-by-step instructions on this process, see “Appendix E: App Volumes Configuration” on page 407.

2. Complete the App Volumes Manager wizard and add the vCenter Servers for Site 1 as machine managers, including mapping their corresponding datastores.

3. Continue with installing the subsequent App Volumes Managers for Site 1. Add them as targets to the local load balancer virtual IP.

4. Repeat steps 1–3 for Site 2 so that the App Volumes Managers in Site 2 point to the local availability group listener for Site 2, and register the local vCenter Servers for Site 2 as machine managers.

5. For details on setting up storage groups for replicating AppStacks from site to site, see the Recovery Service Integration section of “Service Integration Design” on page 271.

6. Replicate AppStack entitlements between sites, as described in “Appendix E: App Volumes Configuration” on page 407.

With this design, the following is achieved:

- AppStacks are made available in both sites.
- AppStacks are replicated from site to site through storage groups defined in App Volumes Manager and through the use of a common datastore that is configured as non-attachable.
- User-based entitlements for AppStacks are replicated between sites.
- A writable volume is normally active in one site for a given user.
Writable volumes can be replicated from site to site using processes such as array-based replication. An import operation might be required on the opposite site. The order and details for these steps are outlined in "Failover with Separate Databases" below.

Entitlements for writable volumes are available between sites.

Failover with Separate Databases

In this model, each site works independently, with its own set of App Volumes Managers and its own database instance. During an outage, the remaining site can provide access to AppStacks with no intervention required.

- The AppStacks have previously been copied between sites using non-attachable datastores that are members of both sites’ storage groups.
- The entitlements to the AppStacks have previously been reproduced, either manually or through an automated process.

In use cases where writable volumes are being used, there are a few additional steps:

1. Mount the replicated datastore that contains the writable volumes.
2. Perform a rescan of that datastore. If the datastore was the default writable volume location, App Volumes Manager automatically picks up the user entitlements after the old assignment information has been cleaned up.
3. (Optional) If the datastore is not the default writable volume location, perform an Import Writable Volumes operation from the App Volumes Manager at Site 2.

All assignments to writable volumes are successfully added, but to the new valid location.

Installation and Initial Configuration

Installation prerequisites are covered in more detail in the System Requirements section of the VMware App Volumes Installation Guide. The following table lists the versions used in this reference architecture.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
<td>VMware vSphere 6.7</td>
</tr>
<tr>
<td>Virtual Center</td>
<td>VMware vCenter 6.7</td>
</tr>
<tr>
<td>App Volumes Manager</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Active Directory</td>
<td>2016 Functional Level</td>
</tr>
</tbody>
</table>
Table 119: App Volumes Components and Version (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server</td>
<td>SQL Server 2016</td>
</tr>
<tr>
<td>OS for App Volumes Agent</td>
<td>Windows 10 and Windows Server 2016</td>
</tr>
</tbody>
</table>

Refer to the VMware App Volumes Installation Guide for installation procedures. This document outlines the initial setup and configuration process.

After installation is complete, you must perform the following tasks to start using App Volumes:

- Complete the App Volumes Initial Configuration Wizard (https://avmanager).
- Install the App Volumes Agent on one or more clients and point the agent to the App Volumes Manager address (load-balanced address).
- Select a clean provisioning system and provision an AppStack. See Working with AppStacks in the VMware App Volumes Administration 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.
Component Design: User Environment Manager Architecture

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 specifies. This reduces login and logout time because 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.

![Diagram of User Environment Manager Architecture]

**Figure 96**: User Environment Manager

**Note**: VMware App Volumes™ AppStack applications are not currently supported on VMware Horizon® Cloud Service™ on Microsoft Azure.

User Environment Manager is a Windows-based application that consists of the following components.
### Table 120: User Environment Manager Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Active Directory Group Policy      | - Mechanism for configuring User Environment Manager.  
- ADMX template files are provided with the product.                                                                                                   |
| NoAD mode XML file                 | An alternative to using Active Directory Group Policy for configuring User Environment Manager. With NoAD mode, you do not need to create a GPO, write logon and logoff scripts, or configure Windows Group Policy settings. |
| IT configuration share             | - A central share (SMB) on a file server, which can be a replicated share (DFS-R) for multi-site scenarios, as long as the path to the share is the same for all client devices.  
- Is read-only to users.  
- If using DFS-R, it must be configured as hub and spoke. Multi-master replication is not supported.                                                  |
| Profile Archives share             | - File shares (SMB) to store the users’ profile archives and profile archive backups.  
- Is used for read and write by end users.  
- For best performance, place archives on a share near the computer where the User Environment Manager FlexEngine (desktop agent) runs. |
| UEM FlexEngine                     | The User Environment Manager Agent that resides on the virtual desktop or RDSH server VM being managed.                                                                                                   |
| Application Profiler               | Utility that creates a User Environment Manager Flex configuration file from an application by determining where the application stores configuration data in the registry and file system. User Environment Manager can manage settings for applications that have a valid Flex configuration file in the configuration share. |
| Helpdesk Support Tool              | - Allows support personnel to reset or restore user settings.  
- Enables administrators to open or edit profile archives.  
- Allows analysis of profile archive sizes.  
- Includes a log file viewer.                                                                                                                      |
| Self-Support                       | Optional self-service tool to allow users to manage and restore their...                                                                                                                                 |

**VMware Workspace ONE and VMware Horizon Reference Architecture - 198**
### Table 120: User Environment Manager Components (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configuration settings on an environment setting or application.</td>
</tr>
<tr>
<td>SyncTool</td>
<td>Optional component designed to support physical PCs working offline or in limited bandwidth scenarios.</td>
</tr>
</tbody>
</table>

The following figure shows how these components interact.

![User Environment Manager Logical Architecture](image.png)

**Figure 97: User Environment Manager Logical Architecture**

### Table 121: Implementation Strategy for User Environment Manager

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Environment Manager was implemented to support both VMware Horizon® 7 and VMware Horizon® Cloud Service™ environments.</td>
<td>User Environment Manager enables configuration of IT settings such as Horizon Smart Policies, predefined application settings, and privilege elevation rules, while providing user personalization for Windows and applications. Applied across Horizon 7 and Horizon Cloud Service environments, this strategy provides consistency and a persistent experience for the users.</td>
</tr>
</tbody>
</table>
User Profile Strategy

A Windows user profile is made of multiple components, including profile folders, user data, and the user registry. See About User Profiles for more information about Windows user profiles.

There are a number of user profile types, such as local, roaming, and mandatory. User Environment Manager complements each user profile type, providing a consistent user experience as end users roam from device to device. User Environment Manager is best-suited to run long-term with local and mandatory profile types. See User Environment Manager Scenario Considerations for more information and considerations when using roaming profiles.

Folder redirection can be used to abstract user data from the guest OS, and can be configured through GPO or using the User Environment Manager user environment settings.

Figure 98: User Environment Manager User Profile Strategy

Table 122: User Profile Strategy with User Environment Manager

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory profiles and folder redirection were used in this reference architecture. A mandatory user profile is a preconfigured roaming user profile that specifies settings for users.</td>
<td>With mandatory user profiles, a user can modify their desktop during a session, but the changes are not saved when the user logs out. Because all settings are managed by User Environment Manager, there is no need to persist these settings on log-out.</td>
</tr>
</tbody>
</table>

To learn more, see the blog post VMware User Environment Manager, Part 2: Complementing Mandatory Profiles with VMware User Environment Manager.

We followed the process outlined in Creating an Optimized Windows Image for a VMware Horizon Virtual Desktop to create the mandatory profile. This produced a single mandatory profile that can be used for Horizon 7 on-premises and for Horizon Cloud Service on Microsoft Azure.

Restrictions in the Microsoft Azure interface interfere with the creation of a mandatory profile on an Azure VM. Instead, we completed the process on a vSphere VM in the on-premises data center, and copied the mandatory profile to Azure.

Important: If you take this approach, use the same Windows build and profile version when building the mandatory profile as you will deploy in Horizon Cloud on Microsoft Azure. See the VMware Horizon Cloud Service on Microsoft Azure Release Notes in the VMware Horizon Cloud Service on
Microsoft Azure documentation for a list of supported guest OS versions. For a list of associated profile versions, see Create Mandatory User Profiles.

**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. Administrators use the User Environment Manager Management Console to configure settings.

**Figure 99**: User Environment Manager Infrastructure

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Group Policy is chosen over NoAD mode.</td>
<td>This provides the flexibility to apply different user environment configuration settings for different users. An ADMX template is provided to streamline configuration.</td>
</tr>
</tbody>
</table>

If you choose to use NoAD mode:

- The FlexEngine agent must be installed in NoAD mode.
- Be sure to configure your User Environment Manager configuration share *before* installing the FlexEngine agent. You must specify the path to the configuration share as part of the NoAD-mode installation process.
If you use the Import Image wizard from the Azure Marketplace with Horizon Cloud Service on Microsoft Azure, the FlexEngine agent will be automatically installed for use with GPOs. You will need to reinstall the agent in NoAD mode.

**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. Multi-master 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.

**Multi-site Design**

User Environment Manager data consists of the following types. This data is typically stored on separate shares and can be treated differently to achieve high-availability:

- **IT configuration data** – IT-defined settings that give predefined configuration for the user environment or applications
  
  *Note*: A User Environment Manager instance is defined by the IT configuration data share.

- **Profile archive (user settings and configuration data)** – The individual end user’s customization or configuration settings

It is possible to have multiple sets of shares to divide the user population into groups. This can provide separation, distribute load, and give more options for recovery. By creating multiple User Environment Manager configuration shares, you create multiple environments. You can use a central installation of the Management Console to switch between these environments and to export and import settings between environments. You can also use User Environment Manager group policies to target policy settings to specific groups of users, such as users within a particular Active Directory OU.

To meet the requirements of having User Environment Manager IT configuration data and user settings data available across two sites, this design uses Distributed File System Namespace (DFS-N) for mapping the file shares.

Although we used DFS-N, you are not required to use DFS-N. Many different types of storage replication and common namespaces can be used. The same design rules apply.

**IT Configuration Share**

For IT configuration file shares, having multiple file server copies active at the same time with DFS-N is fully supported. This is possible because end users are assigned read-only permissions to the file shares so as to avoid write conflicts.

There are two typical models for the layout of the IT configuration share.

- **Centralized IT configuration share** – Designing a multi-site User Environment Manager instance using a centralized IT configuration share streamlines administration for centralized IT. Changes to the IT configuration share are made to a master copy, which is then replicated
to one or more remote sites.

- **Separate IT configuration share at each site** – Another option is to implement multiple User Environment Manager sites by creating an IT configuration share at each site. This model supports decentralized IT, as IT admins at each site can deploy and manage their own User Environment Manager instances.

**Note**: Only administrators should have permissions to make changes to the content of the IT configuration share. To avoid conflicts, have all administrators use the same file server for all the writes, connecting using the server URL rather than with DFS-N.

---

**Figure 100**: IT Configuration Share – Supported DFS Topology

**Table 124**: Strategy for Managing Configuration Shares

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IT configuration shares were replicated to at least one server in each site using DFS-R. Each server was enabled with DFS-N to allow each server to be used as a read target.</td>
<td>This strategy provides replication of the IT configuration data and availability in the event of a server or site outage. Aligned with Active Directory sites, this can also direct usage to the local copy to minimize cross-site traffic. This strategy provides centralized administration for multiple sites, while configuration data is read from a local copy of the IT configuration share.</td>
</tr>
</tbody>
</table>

**Profile Archive Shares**

For user settings file shares, DFS-N is supported and can be used to create a unified namespace across sites. Because the content of these shares will be read from and written to by end users, it is
important that the namespace links have only one active target. Configuring the namespace links with multiple active targets can result in data corruption. See the Microsoft KB article Microsoft's Support Statement Around Replicated User Profile Data for more information.

Configuring the namespace links with one active and one or more inactive (passive) targets provides you the ability to quickly, albeit manually, fail over to a remote site in case of an outage.

Figure 101: Profile Archive Shares – Supported DFS Topology

Switching to another file server in the event of an outage requires a few simple manual steps:

1. If possible, verify that data replication from the active DFS-N folder target to the passive DFS-N folder target has completed.
2. Manually disable the active DFS-N folder target.
3. Enable the passive DFS-N folder target.
4. Remove the read-only option on the target.
The profile archive shares were replicated to at least one server in each site using DFS-R. DFS-N was configured, but only one server was set as an active referral target. The rest were set as disabled targets.

This strategy provides replication of the profile archive data and availability in the event of a server or site outage. A disabled target can be enabled in the event of a server or site outage to provide access to the data. User configuration data is accessed or modified on a local copy of the profile archive share, ensuring good performance for end users.

The User Environment Manager Management Console can be installed on as many computers as desired. If the Management Console is not available after a disaster, you can install it on a new management server or on an administrator’s workstation and point that installation to the User Environment Manager configuration share.

**Installation**

You can install and configure User Environment Manager in a few easy steps:

1. Create SMB file shares for configuration data and user data.
2. Import ADMX templates for User Environment Manager.
3. Create Group Policy settings for User Environment Manager.
4. Install the FlexEngine agent on the virtual desktop or RDSH server VMs to be managed.
- If you manually create a master VM, install the FlexEngine agent according to the VMware UserEnvironment Manager documentation.

- The FlexEngine agent is automatically installed when the image is created using the Import Image wizard to import from the Azure Marketplace. The installation directory defaults to `C:\Program Files\VMware\Horizon Agent\s\User Environment Manager`.

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

Refer to Installing and Configuring User Environment Manager for detailed installation procedures. Also see the Quick-Start Tutorial for User Environment Manager. We used User Environment Manager 9.6.

**Next Steps**

After installing User Environment Manager, perform the following tasks to verify functionality:

- Install the User Environment Manager Agent (FlexEngine agent) on one or more virtual desktop or RDSH server VMs to be managed.

- Set a few customizations (for example, desktop shortcuts for VLC, Notepad++).

- Use the Management Console to download and use configuration templates for one or more applications. Configuration templates are preconfigured Flex configuration files that are designed to facilitate the initial implementation of popular applications. The configuration templates are starter templates that you must test in your environment and possibly modify to suit the needs of your organization. See Download Configuration Templates.

- (Optional) Use the Easy Start feature when performing a proof of concept. Easy Start is not recommended for production implementations.

  **Important:** If the FlexEngine agent was automatically installed in your Windows desktop image as part of the Horizon Cloud on Microsoft Azure Import Image wizard, any desktop shortcut that references FlexEngine.exe will need to be modified to reflect the correct executable path.

- Log in to the virtual desktop or RDSH-published application and verify that User Environment Manager has made the requested changes.

- Check the user log to verify that User Environment Manager is working, or troubleshoot if it is not working as expected. The logs folder is in the SMB share specified for user data.

- Familiarize yourself with Horizon Smart Policies and Horizon Client Property conditions. See Using Smart Policies for requirements, settings, and configuration details.

  **Important:** Take note of the following nuances when using Smart Policies with Horizon Cloud Service on Microsoft Azure as opposed to Horizon 7.

  - The Horizon Client Property **Pool Name** applies to pools in Horizon 7, but in Horizon Cloud, this property applies to a similar construct called an Assignment.

  - The Horizon Client Property **Launch Tags** is applicable only to Horizon 7. Horizon Cloud Service on Microsoft Azure does not support the Launch Tags property.
Component Design: Unified Access Gateway Architecture

VMware Unified Access Gateway™ is an extremely useful component within a VMware Workspace ONE® and VMware Horizon® deployment because it enables secure remote access from an external network to a variety of internal resources. Unified Access Gateway supports multiple use cases:

- Per-app Tunneling of native and web apps on mobile and desktop platforms to secure access to internal resources through the VMware Tunnel service
- Access from VMware Workspace ONE® Content to internal file shares or SharePoint repositories by running the Content Gateway service
- Reverse proxying of web applications
- Identity bridging for authentication to on-premises legacy applications that use Kerberos or header-based authentication
- Secure external access to desktops and applications on VMware Horizon® Cloud Service™ on Microsoft Azure, and VMware Horizon® 7 on-premises

When providing access to internal resources, Unified Access Gateway can be deployed within the corporate DMZ or internal network, and acts as a proxy host for connections to your company’s resources. Unified Access Gateway directs authenticated requests to the appropriate resource and discards any unauthenticated requests, it also can perform the authentication itself, leveraging additional authentication when enabled.

Figure 103: Unified Access Gateway Logical Architecture
Unified Access Gateway, and all its edge services, support being deployed across VMware vSphere®, Microsoft Azure, and Amazon Web Services. For Microsoft Hyper-V, only VMware Tunnel® and Content Gateway edge services are supported.

Table 126: Implementation Strategy for External Access for the Entire Workspace ONE Environment

<table>
<thead>
<tr>
<th>Decision</th>
<th>Multiple Unified Access Gateway appliances were deployed on vSphere to support the whole Workspace ONE environment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This strategy provides external access for Workspace ONE users to internal resources, such as web applications, file repositories, and virtual desktops and applications.</td>
</tr>
</tbody>
</table>

On Horizon Cloud Service on Microsoft Azure, Unified Access Gateway appliances can be deployed as part of the Horizon Cloud pod’s gateway configuration. See Specify the Pod’s Gateway Configuration in the Horizon Cloud Deployment Guide.

Table 127: Implementation Strategy for External Access to the Horizon Cloud Service Component

<table>
<thead>
<tr>
<th>Decision</th>
<th>Unified Access Gateway was deployed as part of Horizon Cloud Service on Microsoft Azure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This strategy provides external access for Workspace ONE users of the Horizon Cloud desktops and applications. Deployment is automated when selected as part of the Horizon Cloud pod’s gateway configuration</td>
</tr>
</tbody>
</table>

**Design Overview**

A successful deployment of Unified Access Gateway is dependent on good planning and a robust understanding of the platform. The following sections discuss the design options and detail the design decisions that were made to satisfy the design requirements.

**Scalability**

Unified Access Gateway gives two sizing options during deployment.
Table 128: Unified Access Gateway Sizing Options

<table>
<thead>
<tr>
<th>Item</th>
<th>Standard</th>
<th>Large</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU (Cores)</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Memory (GB)</td>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>Recommended use</td>
<td>For VMware Workspace ONE® UEM deployments with fewer than 10,000 connections</td>
<td>For Workspace ONE UEM deployments with more than 10,000 connections</td>
</tr>
<tr>
<td>Sizing</td>
<td>1 appliance per 2,000 Horizon connections</td>
<td>1 appliance per 2,000 Horizon connections</td>
</tr>
<tr>
<td></td>
<td>1 appliance per 10,000 Workspace ONE UEM service concurrent sessions</td>
<td>1 appliance per 50,000 Workspace ONE UEM service concurrent sessions</td>
</tr>
</tbody>
</table>

To satisfy high availability requirements, the proposed solution was deployed based on the best practice of using $n+1$ appliances.

Table 129: Implementation Strategy for Accommodating Horizon Desktop and App Connections

<table>
<thead>
<tr>
<th>Decision</th>
<th>Five standard-sized Unified Access Gateway appliances were deployed to satisfy the requirement for 2,000 concurrent external connections to Horizon 7 desktops and applications.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Four appliances can satisfy the load demand, and a fifth provides high availability ($n+1$).</td>
</tr>
</tbody>
</table>

Table 130: Implementation Strategy for Accommodating Workspace ONE UEM Service Sessions

<table>
<thead>
<tr>
<th>Decision</th>
<th>Three large-sized Unified Access Gateway appliances were deployed to satisfy the requirement for 50,000 devices that will leverage Workspace ONE Tunnel, Workspace ONE Content and identity bridging.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Each service is designed to support 50,000 sessions, which gives a total of 100,000 sessions. Two appliances satisfy the load demand and a third provides high availability ($n+1$).</td>
</tr>
</tbody>
</table>

**Deployment Model**

Unified Access Gateway offers basic and cascade-mode architecture models for deployment. Both configurations support load-balancing for high availability and SSL offloading.
In the basic deployment model, Unified Access Gateway is typically deployed in the DMZ network, behind a load balancer.

The cascade-mode deployment model includes front-end and backend instances of the Unified Access Gateway, which have separate roles. The Unified Access Gateway front-end appliance resides in the DMZ and can be accessed from public DNS over the configured ports.

Cascade mode is supported only for the following edge services: Horizon, VMware Tunnel and Content Gateway.

Reasons to adopt cascade mode for VMware Tunnel and Content Gateway edge services, are:

- An organization might have limited or no DNS access in the DMZ, which makes it difficult to resolve the internal FQDN or host name that the edge service requires.
- The organization’s security policies might restrict access from the DMZ directly to internal resources.

In a Horizon deployment, cascade mode does not require a double DMZ, but for environments where a double DMZ is mandated, the front-end Unified Access Gateway appliance can act as the Web Reverse Proxy in the DMZ, and the backend appliance can have the Horizon edge service enabled.
**Decision**

Basic deployment mode was used to deploy all Unified Access Gateway appliances, which were located behind load balancers.

**Justification**

DNS was available in the DMZ and was able to resolve internal host names. Access to the internal network was restricted to the Unified Access Gateway backend NIC by means of firewall rules. Incoming traffic was restricted to the Internet NIC by means of load-balancers.

### Load Balancing

It is strongly recommended that users connect to Unified Access Gateway using a load-balanced virtual IP (VIP). This ensures that user load is evenly distributed across all available Unified Access Gateway appliances. Using a load balancer also facilitates greater flexibility by enabling IT administrators to perform maintenance, upgrades, and configuration changes without impacting users.

### High Availability

Unified Access Gateway provides, out-of-the-box, a high-availability solution for the Unified Access Gateway edge services deployed in vSphere environments. The solution supports up to 10,000 concurrent connections in a high-availability (HA) cluster and simplifies HA deployment and configuration of the services.

The HA component of Unified Access Gateway requires an administrator to specify an IPv4 virtual IP address (VIP) and a group ID. Unified Access Gateway assigns this VIP address to only one of the nodes in the cluster. If that node fails, the VIP address gets reassigned automatically to one of the other available nodes in the cluster. HA and load distribution occur among all the nodes in the cluster that share the same group ID.

---

**Figure 105**: Virtual IP Address and Group ID Configuration for HA in Two Separate Clusters

Unified Access Gateway leverages different algorithms to balance traffic and session affinity:
For Horizon 7 and web reverse proxy, source IP affinity is used with a round-robin algorithm for distribution.

For VMware Tunnel (Per-App VPN) and Content Gateway, there is no session affinity, and a least-connection algorithm is used for distribution.

Regarding IP address requirements, n+1 public IP addresses are required for Horizon 7 components:

- One IP address for the load-balanced floating VIP used for the XML-API
- An additional one per Unified Access Gateway appliance for the secondary protocols (tunnel, Blast, PCoIP), which is the IP assigned to NIC 1 (eth0) and will not use HA

The XML-API traffic is routed to the current master (VIP), and represents less than 1 percent of the Horizon Client traffic. The rest of the traffic goes directly from the client to the assigned Unified Access Gateway during XML-API authentication.

![Figure 106: Unified Access Gateway HA Flow for Horizon Edge Services](image)

For the Web Reverse Proxy, Per-App Tunnel, and Content Gateway, only a single public IP address for the VIP is required because traffic will always flow to the VIP address first and then be forwarded to the correct Unified Access Gateway appliance.
Figure 107: Unified Access Gateway HA Flow for VMware Tunnel and Content Gateway Edge Services

For more information on the Unified Access Gateway High Availability component and configuration of edge services in HA, see the following resources:

- Configure High Availability Settings
- Unified Access Gateway Configured with Horizon
- VMware Tunnel (Per-App VPN) Connection with Basic Configuration
- VMware Tunnel (Per-App VPN) Connections in Cascade Mode
- Content Gateway with Basic Configuration
- Content Gateway in Cascade (formerly known as Relay and Endpoint) Configuration

Unified Access Gateway continues to support third-party load balancers, for organizations who prefer this mode of deployment. For more information, see:

- Unified Access Gateway Load Balancing Topologies
- Load Balancing across VMware Unified Access Gateway Appliances

When deploying Unified Access Gateway on Amazon Web Services or Microsoft Azure, VMware strongly recommends leveraging the native HA/load balancing solution offered by the cloud provider.

Table 132: Load-Balancing Strategy for Unified Access Gateway Appliances

| Decision | An external third-party load balancer was deployed in front of the Unified Access Gateway appliances. |
| Justification | To meet the goals of scalability and availability, multiple Unified Access Gateway appliances are required. |
**Service Design**

A Unified Access Gateway appliance is capable of running multiple edge services on the same appliance. In larger environments, be sure to separate Horizon traffic from Workspace ONE UEM services, and have discrete sets of Unified Access Gateway appliances for each. The Web Reverse Proxy edge service is the only exception. It can be enabled in conjunction with Horizon and Workspace ONE UEM services.

**Table 133: Strategy for Separating Horizon Traffic from Workspace ONE UEM Services**

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Separate sets of Unified Access Gateway appliances were deployed for on-premises services. One set provided Horizon 7 services, and a second supported Workspace ONE UEM services (Content and Tunnel).</td>
<td>A best practice for large deployments is to separate the network traffic and load required for Horizon 7 from other uses.</td>
</tr>
</tbody>
</table>

Because multiple edge services can be enabled on the same appliance, by default each one of them runs on a separate port, which can require opening multiple ports and creating additional firewall rules. In order to avoid that situation, Unified Access Gateway introduced TLS port sharing, which allows VMware Tunnel (Per-App VPN), Content Gateway, and Web Reverse Proxy edge services to all use TCP port 443.

When sharing TCP port 443, ensure that each configured edge service has a unique external DNS entry pointing to the Unified Access Gateway external NIC IP address.

For services that do not share TCP port 443, a single DNS entry can be shared across those services.

**Table 134: Strategy for Port Sharing by Edge Services**

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity bridging, VMware Tunnel, and Content edge services were enabled on the same appliance. The services shared TCP port 443, but a unique DNS entry was created for each service. The DNS entry pointed to the load balancer, which forwarded traffic to the pool of external Unified Access Gateway IP addresses.</td>
<td>This strategy leverages TLS port sharing for identity bridging, Tunnel, and Content services to minimize the number of nonstandard ports and firewall rules required.</td>
</tr>
</tbody>
</table>

**Table 135: Port Strategy for the Horizon Edge Service**

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Horizon edge service was configured to use TCP port 443 to perform authentication and TCP port 8443 and UDP port 8443 to access internal desktops and RDSH-published applications using the Blast Extreme display protocol.</td>
<td>Best practice is to use Blast Extreme with TCP 8443 and UDP 8443, which are the defaults. When a client environment has UDP blocked, Blast Extreme still works; however, when UDP 8443 is allowed, communication is more efficient.</td>
</tr>
</tbody>
</table>
Network Segmentation Options

Unified Access Gateway can be deployed with one, two, or three network interface controllers (NICs). The choice is determined by your network requirements and discussions with your security teams to ensure compliance with company policy.

Single-NIC Deployment

In a single-NIC deployment, all traffic (Internet, backend, and management) uses the same network interface. Authorized traffic is then forwarded by Unified Access Gateway through the inner firewall to resources on the internal network using the same NIC. Unauthorized traffic is discarded by Unified Access Gateway.

![Figure 108: Unified Access Gateway Single-NIC Deployment](image)

Two-NIC Deployment

A two-NIC deployment separates the Internet traffic onto its own NIC, while the management and backend network data still share a NIC.

The first NIC still used for Internet facing unauthenticated access, but the backend authenticated traffic and management traffic are separated onto a different network. This type of deployment is suitable for production environments.
In this two-NIC deployment, traffic going to the internal network through the inner firewall must be authorized by Unified Access Gateway. Any unauthorized traffic is not allowed on this backend network. Management traffic such as the REST API for Unified Access Gateway uses only this second network.

If a device on the unauthenticated front-end network is compromised—for example, if a load balancer were compromised—then reconfiguring that device to bypass Unified Access Gateway would still not be possible in this two NIC deployment. It combines layer 4 firewall rules with layer 7 Unified Access Gateway security.

Similarly, if the Internet-facing firewall is misconfigured to allow TCP port 9443 through, the Unified Access Gateway Management REST API would still not be exposed to Internet users. A defense-in-depth principle uses multiple levels of protection, such as knowing that a single configuration mistake or system attack will not necessarily create an overall vulnerability.

In a two-NIC deployment, it is common to put additional infrastructure systems such as DNS servers, RSA SecurID Authentication Manager servers, and so on in the backend network within the DMZ so that they are not visible from the Internet-facing network. This guards against layer-2 attacks from a compromised front-end system on the Internet-facing LAN and thereby effectively reduces the overall attack surface.

When the Horizon service is enabled on Unified Access Gateway, most network traffic is the display protocol traffic for Blast Extreme and PCoIP. With a single NIC, display protocol traffic to or from the Internet is combined with traffic to or from the backend systems. When two or more NICs are used, the traffic is spread across front-end and backend NICs and networks. This can result in performance benefits by reducing the potential bottleneck of a single NIC.

**Three-NIC Deployment**

A three-NIC deployment separates the Internet traffic onto its own NIC, and separates management and backend network data onto dedicated networks. HTTPS management traffic to port 9443 is then only possible from the management LAN. This type of deployment is suitable for production environments.
Decision | Unified Access Gateway appliances were deployed in a dual-NIC mode.
---|---
Justification | This strategy meets the requirements of separating Internet traffic from management and backend data.

**Table 136**: Strategy for Separating Front-End, Backend, and Management Traffic

**Authentication Options**

Unified Access Gateway supports multiple authentication options, for example, pass-through, RSA SecurID, RADIUS, and certificates including smart cards. Pass-through authentication forwards the request to the internal server or resource. Other authentication types enable authentication at the Unified Access Gateway, before passing authenticated traffic through to the internal resource.

In addition to the current authentication methods available, you can use services such as VMware Tunnel, and VMware Identity Manager to provide an additional layer of authentication. These authentication mechanisms come into play based on device certificate, device compliance, or both. Certificate and compliance checks are performed when the device traffic arrives at the Unified Access Gateway. At that point, the edge services communicate with Workspace ONE UEM through APIs.

These options are depicted in the following diagrams.
For guidance on how to setup authentication on DMZ, see Configuring Authentication in DMZ.

Table 137: Type of Authentication Chosen for This Reference Architecture

<table>
<thead>
<tr>
<th>Decision</th>
<th>Pass-through authentication was configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>Users can authenticate through Workspace ONE and VMware Identity Manager. Having authentication performed by Unified Access Gateway would force users to authenticate to resources a second time.</td>
</tr>
</tbody>
</table>

**Deployment Methods**

In this section, we briefly discuss the two supported methods of deploying Unified Access Gateway and then detail the optimal solution to satisfy the design requirements.

- **VMware vSphere OVF® template and administration console** – With this option, you run the Import OVF (Open Virtualization Format) wizard and respond to various deployment questions. This method requires responses from an IT administrator during deployment. If you use this method, the Unified Access Gateway is not production ready on first boot and requires post-deployment configuration using the administration console. The required configuration
tasks can be performed either manually or by importing a configuration file from another Unified Access Gateway appliance.

- **PowerShell script** – The PowerShell method ensures that the Unified Access Gateway virtual appliance is production ready on first boot. This method uses the VMware OVF Tool command-line utility in the background. The IT administrator updates an INI file with the required configuration settings and then deploys the Unified Access Gateway by entering a simple deployment command in PowerShell (\uagdeploy.ps1 .\<name>.ini).

### Table 138: Strategy for Deploying and Configuring Unified Access Gateway Appliances

<table>
<thead>
<tr>
<th>Decision</th>
<th>The PowerShell method for deployment was used.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>This option does not require the IT administrator to manually enter settings during deployment and so is less prone to input error. This option also makes upgrading and deploying additional appliances easier.</td>
</tr>
</tbody>
</table>

More information on using the PowerShell method is available on the Using PowerShell to Deploy VMware Unified Access Gateway community page. The PowerShell script and sample INI files can be downloaded from the Unified Access Gateway product download page. For step-by-step instructions on how to deploy Unified Access Gateway, see the following articles on Tech Zone:

- Deploying Unified Access Gateway with One NIC Through vSphere
- Deploying Unified Access Gateway with Two NICs Through PowerShell

### Required Deployment Information

Before deploying a Unified Access Gateway appliance, you must verify that certain prerequisites are met and provide the following information.

### Certificates

TLS/SSL certificates are used to secure communications for the user between the endpoint and the Unified Access Gateway and between the Unified Access Gateway and internal resources. Although Unified Access Gateway generates default self-signed certificates during deployment, for production use, you should replace the default certificates with certificates that have been signed by a trusted certificate authority (CA-signed certificates). You can replace certificates either during deployment or as part of the initial configuration. The same certificate or separate certificates can be used for the user and the administrative interfaces, as desired.

The following types of certificates are supported:

- Single-server-name certificates, which means using a unique server certificate for each Unified Access Gateway appliance
- Subject alternate name (SAN) certificates
- Wildcard certificates

Certificate files can be provided in either PFX or PEM format.
For guidance on how to configure and update Unified Access Gateway to use TLS/SSL, see Configuring Unified Access Gateway Using TLS/SSL Certificates and Update SSL Server Signed Certificates.

Passwords
Unified Access Gateway requires the IT administrator to define two passwords during installation: The first secures access to the REST API, and the second secures access to the Unified Access Gateway appliance console. The passwords must meet the minimum requirements documented Modify User Account Setting.

IP Address and Fully Qualified Domain Name (FQDN)
As previously discussed, the Unified Access Gateway in this scenario is configured with two NICs:

- Internet-facing IP address and external FQDN
- Backend and management IP address and FQDN
Environment Infrastructure Design

Several environment resources are required to support a VMware Workspace ONE® and VMware Horizon® deployment. In most cases these will already exist. It is important to ensure that minimum version requirements are met and that any specific configuration for Workspace ONE and Horizon is followed. For any supporting infrastructure component that Workspace ONE depends on, that component must be designed to be scalable and highly available. Some key items are especially important when the environment is used for a multi-site deployment.

vSphere Design

VMware vSphere® is the foundation that hosts on-premises infrastructure and components.

All editions of VMware Horizon® 7 come bundled with vSphere for Desktops. Additionally, VMware vSAN™ Advanced is included in VMware Horizon 7 Advanced Edition and Horizon 7 Enterprise Edition.

This chapter describes how components of vSphere were used in this reference architecture, including the design for vSAN and VMware NSX®.

- vSAN pools its server-attached HDDs and SSDs to create a distributed shared datastore that abstracts the storage hardware and provides hyper-converged storage optimized for VMs without the need for external SAN or NAS.
- NSX provides network-based services such as security, network virtualization, routing, and switching in a single platform.

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 113: vSphere and vSAN High-Level Architecture](image-url)
Horizon 7 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 vSphere host.

Although this reference architecture utilizes the benefits of an all-flash vSAN, traditional storage (such as SAN or NAS) is of course also still supported.

**vSphere**

This document does not try to cover vSphere design and installation. That is well documented in other resources, including the [VMware vSphere documentation](https://docs.vmware.com). Best practices around vSphere configuration and vSAN networking should be followed.

For the vSphere clusters hosting management servers such as Horizon Connection Server, or VMware Identity Manager™ appliances, VMware vSphere® Storage DRS™ rules should be enabled to prevent the servers that perform identical operations from running on the same vSphere host. This prevents multiple VM failures if a host fails and these VMs exist on the failed physical vSphere host.

For this reference architecture, we recommend the following settings.

<table>
<thead>
<tr>
<th>vSphere DRS</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere DRS</td>
<td>Turn on vSphere DRS</td>
</tr>
<tr>
<td>DRS Automation</td>
<td>Fully Automated</td>
</tr>
<tr>
<td>Power Management</td>
<td>Off</td>
</tr>
</tbody>
</table>

Table 139: vSphere Distributed Resource Scheduler Settings

Leave all other DRS settings set to the default.

**vSAN**

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

vSAN uses VM-centric storage policies to automate the storage service levels on a per-VM basis. Horizon 7 integrates into this consumption model and automatically generates the required storage policies as pools are deployed onto a vSAN datastore.

For best-practice recommendations, see the [VMware Horizon 7 on VMware vSAN Best Practices](https://www.vmware.com) technical white paper.

For full design and architectural guidance for deploying vSAN see the various resources on [https://storagehub.vmware.com/t/vmware-vsan/](https://storagehub.vmware.com/t/vmware-vsan/)
Networking

At a high level, all network components are configured redundantly to operate in either active/passive mode or active/active mode where allowed, and the various traffic types are separated from each other. Quality of service is controlled with network IO control (NIOC) on the configured distributed virtual switch.

Figure 114: vSphere Networking

The configuration uses 10-GbE adapters to simplify the 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.

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 similarly to those for CPU and memory. The vSphere administrator is given control to ensure predictable network performance when multiple traffic types contend for the same physical network resources.
Table 140: NIOC Configuration

<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>vSAN 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>

Flow control is disabled for VMkernel interfaces tagged for vSAN (vmk2). vSAN networks 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 vSAN. 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 because network convergence on these switch ports can happen quickly after the failure due to the port entering the spanning-tree forwarding state immediately, bypassing the listening and learning states.

The following table shows the distributed switch and port group policies.

Table 141: Distributed Switch Settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting</th>
<th>Default</th>
<th>Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Port Binding</td>
<td>Static</td>
<td>–</td>
</tr>
<tr>
<td>Policies: Security</td>
<td>Promiscuous mode</td>
<td>Reject</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>MAC address changes</td>
<td>Accept</td>
<td>Reject</td>
</tr>
<tr>
<td></td>
<td>Forged transmits</td>
<td>Accept</td>
<td>Reject</td>
</tr>
<tr>
<td>Policies: Traffic Shaping</td>
<td>Status</td>
<td>Disabled</td>
<td>–</td>
</tr>
<tr>
<td>Policies: Teaming and Failover</td>
<td>Load balancing</td>
<td>Route based on the originating virtual port ID</td>
<td>Route based on physical NIC load</td>
</tr>
</tbody>
</table>
Table 141: Distributed Switch Settings (Continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting</th>
<th>Default</th>
<th>Revised</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failover detection</td>
<td>Caution Link Status only</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Notify switches</td>
<td>Yes</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Policies: Resource Allocation</td>
<td>Network I/O Control</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Advanced</td>
<td>Maximum MTU</td>
<td>1500</td>
<td>9000</td>
</tr>
</tbody>
</table>

A single vSphere distributed switch was created with two 10-Gb interfaces in a team. Five port groups isolate network traffic:

- Virtual machines
- VMware ESXi™ management network
- VMware vSphere® vMotion®
- iSCSI 1 and iSCSI 2

**Note:** Two iSCSI port groups are required in order to configure vmknic-based iSCSI multi-pathing.

Quality of service is enforced with network I/O control (NIOC) on the distributed virtual switch, guaranteeing a share of bandwidth to each type of traffic. A vmkernel interface (vmknic) is created on the ESXi management port group, vSphere vMotion port group, and on each iSCSI port group.

Both 10-Gb adapters are configured as active/active for the VM port group, ESXi management network port group, and the vSphere vMotion port group.

- The iSCSI 1 port group is bound to a single 10-Gb adapter, with only storage traffic permitted on that adapter.
- The iSCSI 2 port group is bound to the second 10-Gb network adapter, with only storage traffic permitted over that adapter.

For more information, see the **vSphere Networking**.

**vSphere Infrastructure Design for Active/Active and Active/Passive Services**

Standard vSphere design and installation should be followed to create a compute and storage platform to run Horizon 7 resources. This section describes the design used for a Horizon 7 multi-site deployment. For a vSAN stretched cluster, within a metro or campus network environment with low
network latency between sites, see “Appendix F: Horizon 7 Active/Passive Service Using VMware vSAN Stretched Cluster” on page 429.

The active/active and the active/passive services for a multi-site setup are based on separate sets of vSphere clusters in each site. The storage used was all-flash arrays. Horizon 7 Cloud Pod Architecture was used to give global entitlements across both sites. Details in this section are specific to the environments put in place to validate the designs in this guide. Different choices in some of the configurations, hardware, and components are to be expected.

The vSphere infrastructure is deployed identically in both data centers, following VMware best practices for pod and block design concepts. For further details, see “Component Design: Horizon 7 Architecture” on page 132.

**Storage**

When designing storage for a Horizon 7 environment, consideration should be given to the mixed workloads. There are management servers running in the management block and desktops and RDSH VMs running in the resource blocks. The storage selected should be able to

- Handle the overall I/O load and provide sufficient space.
- Ensure performance for key components so that a noisy neighbor such as a desktop does not affect the performance of the environment.

Depending on the capability of the storage being used, it is generally recommended to separate these mixed workloads.

In the environment built to validate this reference architecture, the underlying physical storage, all-flash, was shared between the management block and the resource blocks running desktop and RDSH workloads. This was possible because all-flash storage can handle mixed workloads while still delivering great performance.

This approach can be seen in the following logical diagram.
Storage Replication

For some components of the active/passive service, which uses two geographically dispersed sites, storage array data replication is necessary to provide complete business continuity.

If possible, use an asynchronous replication engine that can support bi-directional replication, which facilitates use of DR (disaster recovery) infrastructure for DR and production. VMware recommends using a replication engine that compares the last replicated snapshot to the new one and sends only incremental data between the two snapshots, thus reducing network traffic. Snapshots that can be deduplicated provide space efficiency.
VMware recommends replicating User Environment Manager data between sites. In the case of a site failure, a protected volume that is replicated to the DR site can be recovered promptly and presented. In the case of an active/active deployment, VMware User Environment Manager™ volumes are replicated in each direction.

For optimal performance, VMware recommends implementing the advanced vSphere configuration changes outlined in the following table. Leave all other HA settings set to the default.

**Table 142: vSphere High Availability (HA) Settings**

<table>
<thead>
<tr>
<th>vSphere HA</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere HA</td>
<td>Turn on vSphere HA</td>
</tr>
<tr>
<td>Host Monitoring</td>
<td>Enabled</td>
</tr>
<tr>
<td>Host Hardware Monitoring – VM Component Protection: “Protect against Storage Connectivity Loss”</td>
<td>Disabled (default)</td>
</tr>
<tr>
<td>Virtual Machine Monitoring</td>
<td>Disabled (default)</td>
</tr>
</tbody>
</table>

**NSX Data Center for vSphere**

VMware NSX® Data Center for vSphere® (NSX-V) provides network-based services such as security, virtualization networking, routing, and switching in a single platform. These capabilities are delivered for the applications within a data center, regardless of the underlying physical network and without
the need to modify the application. NSX-V provides key benefits to the Horizon 7 infrastructure components and the desktop environments.

As the following figure shows, NSX-V performs several security functions within a Horizon 7 solution:

- **Protects VDI infrastructure** – NSX Data Center for vSphere secures inter-component communication among the management components of a Horizon 7 infrastructure.

- **Protects desktop pool VM communication with enterprise applications** – Virtual desktops contain applications that allow users to connect to various enterprise applications inside the data center. NSX Data Center for vSphere secures and limits access to applications inside the data center from each desktop.

- **Provides user-based access control** – NSX Data Center for vSphere allows user-level identity-based micro-segmentation for the Horizon 7 desktops. This enables fine-grained access control and visibility for each desktop based on the individual user.

![Figure 117: How NSX-V Protects a Horizon 7 Environment](image)

**Design Overview**

The following diagram shows how NSX Data Center for vSphere and Horizon 7 components fit together.
The NSX Data Center for vSphere platform consists of several components that make up the overall architecture. A highly scalable NSX Data Center for vSphere infrastructure design is typically split into two clusters to create fault domains: the compute cluster and the management cluster. In a Horizon 7 design, however, we also have a desktop cluster.

- The management cluster provides resources for the Horizon 7 and NSX Data Center for vSphere management servers.
- The compute cluster provides compute hosts for the server data center environment.
- The desktop cluster provides resources for building out VDI and RDSH servers for the Horizon 7 environment.

As is shown in the diagram, the server domain is separated from the desktop domain. The server domain houses the Horizon 7, NSX Data Center for vSphere, and VMware vCenter Server® management components. The desktop domain houses the desktop and RDSH-published application pools and server farms, along with the NSX Manager and vCenter Server for the desktop cluster.

### Table 143: Implementation Strategy for NSX Manager

<table>
<thead>
<tr>
<th>Decision</th>
<th>Two NSX Managers were deployed in the Horizon 7 on-premises environment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification</td>
<td>The Horizon 7 design has two vCenter Servers. An NSX Manager must be deployed for each one to allow segmentation and firewall rules to be applied.</td>
</tr>
</tbody>
</table>

The following table lists the components of NSX Data Center for vSphere that were used in this reference architecture.
### Table 144: NSX-V Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager</td>
<td>The management plane for the NSX Data Center for vSphere platform. The software deployments and Distributed Firewall rules are configured and managed from here. NSX-V Manager is configured to communicate with a vCenter Server.</td>
</tr>
<tr>
<td></td>
<td>- NSX Manager secures the Horizon 7 management servers.</td>
</tr>
<tr>
<td></td>
<td>- The desktop domain NSX Manager connects to an Active Directory domain controller to provide access for the NSX Identity Firewall. AD groups are used to provide the objects in which Distributed Firewall rule sets are built.</td>
</tr>
<tr>
<td>Database</td>
<td>NSX Manager uses an embedded database. There is no option to use an external database. To protect this database, use the NSX Manager administration console to schedule regular backups.</td>
</tr>
<tr>
<td>Distributed Firewall</td>
<td>A hypervisor kernel-embedded firewall that provides visibility and control for virtualized workloads and networks.</td>
</tr>
<tr>
<td>Identity Firewall</td>
<td>Allows an NSX administrator to create Active Directory user-based distributed firewall (DFW) rules.</td>
</tr>
</tbody>
</table>

### Scalability

See the NSX Data Center for vSphere Recommended Configuration Maximums guide. With regard to a Horizon 7 environment, the two most relevant sections are the Distributed Firewall and the Identity Firewall sections.

### Micro-segmentation

The concept of micro-segmentation takes network segmentation, typically done with physical devices such as routers, switches, and firewalls at the data center level, and applies the same services at the individual workload (or desktop) level, independent of network topology.

NSX Data Center for vSphere and its Distributed Firewall feature are used to provide a network-least-privilege security model using micro-segmentation for traffic between workloads within the data center. NSX Data Center for vSphere provides firewalls services, within the vSphere ESXi hypervisor kernel, where every virtual workload gets a stateful firewall at the virtual network card of the workload. This firewall provides the ability to apply extremely granular security policies to isolate and segment workloads regardless of and without changes to the underlying physical network infrastructure.

Two foundational security needs must be met to provide a network-least-privilege security posture with NSX micro-segmentation. NSX Data Center for vSphere uses a Distributed Firewall (DFW) and can use network virtualization to deliver the following requirements.
Isolation

Isolation can be applied for compliance, software life-cycle management, or general containment of workloads. In a virtualized environment, NSX Data Center for vSphere can provide isolation by using the DFW to limit which workloads can communicate with each other. In the case of Horizon 7, NSX Data Center for vSphere can block desktop-to-desktop communications, which are not typically recommended, with one simple firewall rule, regardless of the underlying physical network topology.

![Diagram of Isolation Between Desktops](image)

Figure 119: Isolation Between Desktops

Another isolation scenario, not configured in this reference architecture, entails isolating the Horizon 7 desktop and application pools. Collections of VDI and RDSH machines that are members of specific Horizon 7 pools and NSX security groups can be isolated at the pool level rather than per machine. Also, identity-based firewalling can be incorporated into the configuration, which builds on the isolation setup by applying firewall rules that depend on users’ Active Directory group membership, for example.

Segmentation

Segmentation can be applied at the VM, application, infrastructure, or network level with NSX. Segmentation is accomplished either by segmenting the environment into logical tiers, each on its own separate subnet using virtual networking, or by keeping the infrastructure components on the same subnet and using the NSX DFW to provide segmentation between them. When NSX micro-segmentation is coupled with Horizon 7, NSX can provide logical trust boundaries around the Horizon 7 infrastructure as well as provide segmentation for the infrastructure components and for the desktop pools. As an example, the following figure illustrates how segmentation could be used between logical tiers of an application. The same principles apply to Horizon 7 components.
**Advanced Services Insertion (Optional)**

Although we did not use this option for this reference architecture, it warrants some discussion. As one of its key functionalities, NSX provides stateful DFW services at layers 2–4 for micro-segmentation. Customers who require higher-level inspection for their applications can leverage one or more NSX extensible network frameworks, in this case NetX, in conjunction with third-party next-generation firewall (NGFW) vendors for integration and traffic redirection. Specific traffic types can be sent to the NGFW vendor for deeper inspection or other services.

The other network extensibility framework for NSX Data Center for vSphere is Endpoint Security, EPSec. NSX Data Center for vSphere uses EPSec for capabilities leveraged to provide enhanced agentless antivirus/malware or endpoint-monitoring functions from third-party security vendors as well. This integration is optional and in Horizon 7 deployments is beneficial for removing the need for antivirus or anti-malware (AV/AM) agents on the guest operating system. This functionality is provided by NSX through guest introspection, which is also leveraged to provide information for the identity firewall.

To implement guest introspection, a guest introspection VM must be deployed on each ESXi host in the desktop cluster. Also, the VMware Tools driver for guest introspection must be installed on each desktop or RDSH VM.
Installation and Configuration

For an outline of the steps for installing and configuring NSX, see "Appendix G: NSX Data Center for vSphere Configuration" on page 445.

Environment Design

As might be expected, several environment resources might be required to support a Workspace ONE and Horizon deployment, including Active Directory, DNS, DHCP, security certificates, databases, and load balancers. For any external component that Workspace ONE or Horizon depends on, the component must be designed to be scalable and highly available, as described in this section.

The following components should not be treated as an exhaustive list.

Active Directory

Workspace ONE and VMware Horizon require an Active Directory domain structure for user authentication and management. Standard best practices for an Active Directory deployment must be followed to ensure that it is highly available.

Because cross-site traffic should be avoided wherever possible, configure AD sites and services so that each subnet used for desktops and services is associated with the correct site. This guarantees that lookup requests, DNS name resolution, and general use of AD are kept within a site where possible. This is especially important in terms of Microsoft Distributed File System Namespace (DFS-N) to control which specific file server users get referred to.
Table 145: Implementation Strategy for Active Directory Domain Controllers

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory domain controllers will run in each location. Core data center locations may have multiple domain controllers.</td>
<td>This provides domain services close to the consumption. Multiple domain controllers ensure resilience and redundancy.</td>
</tr>
</tbody>
</table>

For Horizon 7 specifics, see the Preparing Active Directory for details on supported versions and preparation steps. For Horizon Cloud Service on Microsoft Azure specifics, see Active Directory Domain Configurations, in the Getting Started with VMware Horizon Cloud Service on Microsoft Azure guide for details on supported Active Directory configurations and preparation steps.

Additionally, for Horizon usage, whether Horizon 7 or Horizon Cloud, set up dedicated organizational units (OUs) for the machine accounts for virtual desktops and RDSH servers. Consider blocking inheritance on these OUs to stop any existing GPOs from having an undesired effect.

Group Policy

Group Policy objects (GPOs) can be used in a variety of ways to control and configure both VMware Horizon® Cloud Service™ on Microsoft Azure components and also standard Windows settings.

These policies are normally applied to the user or the computer Active Directory account, depending on where the objects are located in Active Directory. In a Horizon Cloud Service on Microsoft Azure environment, it is typical to set specific user policy settings for the specific Horizon Cloud Service 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 applies only user settings, so if the User Environment Manager GPOs are applied to computer objects, loopback processing must be enabled.

Group policies can also be associated at a site level. Refer to the Microsoft Web site for details.

DNS

The Domain Name System (DNS) is widely used in a Workspace ONE and a Horizon 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 virtual desktops.
Table 146: Implementation Strategy for DNS

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS were provided by using Active Directory-integrated DNS zones. The DNS service ran on select Windows Servers running the domain controller roles.</td>
<td>The environment already had DNS servers with Active Directory-integrated DNS zones</td>
</tr>
</tbody>
</table>

**DHCP**

In a Horizon environment, desktops and RDSH servers rely on DHCP to get IP addressing information. DHCP must be allowed on the VM networks designated for these virtual desktops and RDSH servers.

In Horizon 7 multi-site deployments, the number of desktops a given site is serving usually changes when a failover occurs. Typically, the recommendation is to over-allocate a DHCP range to allow for seamlessly rebuilding pools and avoiding scenarios where IPs are not being released from the DHCP scope for whatever reason.

For example, take a scenario where 500 desktops are deployed in a single subnet in each site. This would normally require, at a minimum, a /23 subnet range for normal production. To ensure additional capacity in a failover scenario, a larger subnet, such as /21, might be used. The /21 subnet range would provide approximately 2,000 IP addresses, meeting the requirements for running all 1,000 desktops in either site during a failover while still leaving enough capacity if reservations are not released in a timely manner.

It is not a requirement that the total number of desktops be run in the same site during a failover, but this scenario was chosen to show the most extreme case of supporting the total number of desktops in each site during a failover.

There are other strategies for addressing this issue. For example, you can use multiple /24 networks across multiple desktop pools or dedicate a subnet size you are comfortable using for a particular desktop pool. The most important consideration is that there be enough IP address leases available.

The environment can be quite fluid, with instant-clone desktops being deleted at logout and recreated when a pool dips below the minimum number. For this reason, make sure the DHCP lease period is set to a relatively short period. The amount of time depends on the frequency of logouts and the lifetime of a clone.

Table 147: Implementation Strategy for DHCP

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP was available on the VM network for desktops and RDSH servers.</td>
<td>Virtual desktops can be short lived so a shorter lease period ensures that leases are released quicker.</td>
</tr>
<tr>
<td>DHCP failover was implemented to ensure availability.</td>
<td>A lease period of 4 hours is based on an average logout after 8 hours.</td>
</tr>
<tr>
<td>The lease duration of the scopes used was set to 4 hours.</td>
<td></td>
</tr>
</tbody>
</table>
Microsoft Azure has a built-in DHCP configuration that is a part of every VNet configured in Microsoft Azure. For more information, see IP Configurations in the Microsoft Azure documentation.

**Distributed File System**

File shares are critical in delivering a consistent user experience. They store various types of data used to configure or apply settings that contribute to a persistent-desktop experience.

The data can include the following types:

- IT configuration data, as specified in User Environment Manager
- User settings and configuration data, which are collected by User Environment Manager
- Windows mandatory profile
- User data (documents, and more)
- VMware ThinApp® packages

The design requirement is to have no single point of failure within a site while replicating the above data types between the two data centers to ensure their availability in a site-failure scenario. This reference architecture uses Microsoft Distributed File System Namespace (DFS-N) with array-level replication.

**Table 148: Implementation Strategy for Replicating Data to Multiple Sites**

<table>
<thead>
<tr>
<th>Decision</th>
<th>DFS-Replication (DFS-R) was used to replicate user data from server to server and optionally between sites.</th>
</tr>
</thead>
</table>
| Justification | Replication between servers provides local redundancy.  
Replication between sites provides site redundancy. |

**DFS Namespace**

The namespace is the referred entry point to the distributed file system.

- A single-entry point is enabled and active for profile-related shares to comply with the Microsoft support statements (for example, User Environment Manager user settings).
- Other entry points can be defined but disabled to stop user referrals to them. They can then be made active in a recovery scenario.
- Multiple active entry points are possible for shares that contain data that is read-only for end users (for example, User Environment Manager IT configuration data, Windows mandatory profile, ThinApp packages).
DFS-Namespace (DFS-N) was used. Depending on the data type and user access required, either one or multiple referral entry points may be enabled.

DFS-N provides a common namespace to the multiple referral points of the user data that is replicated by DFS-R.

More detail on how DFS design applies to profile data can be found in "Component Design: User Environment Manager Architecture" on page 197.

**Certificate Authority**

A Microsoft Enterprise Certificate Authority (CA) is often used for certificate-based authentication, SSO, and email protection. A certificate template is created within the Microsoft CA and is used by VMware Workspace ONE® UEM to sign certificate-signing requests (CSRs) that are issued to mobile devices through the Certificate Authority integration capabilities in Workspace ONE UEM and Active Directory Certificate Services.

The Microsoft CA can be used to create CSRs for VMware Unified Access Gateway™, VMware Identity Manager, and any other externally facing components. The CSR is then signed by a well-known external CA to ensure that any device connecting to the environment has access to a valid root certificate.

Having a Microsoft Enterprise CA is a prerequisite for Horizon True SSO. A certificate template is created within the Microsoft CA and is used by True SSO to sign CSRs that are generated by the VM. These certificates are short-lived (approximately 1 hour) and are used solely for the purpose of single-signing a user into a desktop through VMware Identity Manager without prompting for AD credentials.

Details on setting up a Microsoft CA can be found in the Setting Up True SSO section in "Appendix B: VMware Horizon Configuration" on page 344.

**Microsoft RDS Licensing**

Applications published with Horizon use Microsoft RDSH servers as a shared server platform to host Windows applications. Microsoft RDSH servers require licensing through a Remote Desktop Licensing service. It is critical to ensure that the Remote Desktop Licensing service is highly available within each site and also redundant across sites.

| Decision | DFS-Namespace (DFS-N) was used. Depending on the data type and user access required, either one or multiple referral entry points may be enabled. |
| Justification | DFS-N provides a common namespace to the multiple referral points of the user data that is replicated by DFS-R. |

| Decision | A Microsoft Enterprise CA was set up. |
| Justification | This can be used to support certificate authentication for Windows 10 devices and to support the Horizon True SSO capability. |
Table 151: Implementation Strategy for Microsoft RDS Licensing

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple RDS Licensing servers were configured.</td>
<td>This provides licensing for Microsoft RDSH servers where used for delivering Horizon published applications.</td>
</tr>
<tr>
<td>At least one was configured per site.</td>
<td></td>
</tr>
</tbody>
</table>

**Microsoft Key Management Service**

To activate Windows (and Microsoft Office) licenses in a VDI environment, VMware recommends using Microsoft Key Management Service (KMS) with volume license keys. Because desktops are typically deleted at logout and are recreated frequently, it is important that this service be highly available. See the Microsoft documentation on how best to deploy volume activation. It is critical to ensure that the KMS service is highly available within each site and also redundant across sites.

Table 152: Implementation Strategy for the KMS Service

<table>
<thead>
<tr>
<th>Decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft KMS was deployed in a highly available manner</td>
<td>This allows Horizon virtual desktops and RDSH servers to activate their Microsoft licenses.</td>
</tr>
</tbody>
</table>

**Load Balancer**

To remove a single point of failure from some components, we can deploy more than one instance of the component 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.

Throughout this paper, in each of the sections specific to a component, the back-end design and the front-end access mechanism are discussed to show how to design the components to be highly available both within a site and between sites, for example, by using Global Traffic Manager (GTM) from F5.

This section describes load balancing between the two sites in general and explains how the active/active service differs from the active/passive service in terms of persistence and end-user access.

All DNS services ran as Active Directory integrated zones on Windows Server 2016–based domain controllers with no changes beyond Microsoft best practices.

This reference architecture uses the following global namespace resources:

- my.vmweuc.com
- horizon.vmweuc.com
Those namespaces are delegated to the F5 BIG-IP DNS (GTM) function because it is effectively in charge of deciding where a user is directed based on the topology setup defined on F5 BIG-IP DNS for each of those services.

For guidance on how to configure F5 BIG-IP DNS (GTM) for the services listed above, refer to the following resources:

- For setting up the global load balancer: Managing Horizon Traffic Across Multiple Data Centers with BIG-IP (used with Horizon 7 and VMware Identity Manager)
- For setting up the local, site-specific load balancers: Load Balancing VMware Identity Manager
- F5 with App Volumes Configuration Guide

**Load Balancing for a Horizon 7 Active/Active Service**

The active/active service in this design uses the end user’s current physical location. Geo-location attributes align a user in Europe with a data center in Europe and a user in the U.S. with a U.S. data center.

When a user travels from, for example, Europe to the U.S., existing sessions are honored and reconnected, but new connections are always established with the data center closest to the user.

This kind of intelligent placement relies on the load balancer or geographic DNS capabilities, or both, to be functional. This is critical for the active/active service to ensure that a user is always getting a desktop in a data center closest to their current physical location.

The following figure presents a logical overview. The load balancer monitors both pods for availability and health-check status and then decides, based on availability and the end user’s physical location, where a session should be placed.

![Multi-Geo Active/Active Load Balancing](image-url)
Load Balancing for a Horizon 7 Active/Passive Service

User affinity for the active/passive service is based on the source IP address and is configured only on the Local Traffic Manager (LTM) layer because the F5 GTM flow checks only whether the LTM module of a given site is available. No affinity or session management occurs at the GTM layer. F5 GTM performs the initial placement based on the following:

- For external access, the geo-location of the user is considered.
- For internal access, the user is directed to one of the sites based on their client subnet value as defined by the VLAN (port group) the desktop pool is associated with.

This allows for the control of the traffic flow for on-premises users because we know the internal IP subnets used and can direct users accordingly. For example, if F5 GTM sees a connection associated with a subnet in Site 1, it directs the requests to Site 1 unless that site's LTM instance is not responding to requests.

Microsoft Azure Environment Infrastructure Design

In this reference architecture, multiple Azure regional data centers were used to demonstrate multi-site deployments of Horizon Cloud Service on Microsoft Azure. We configured infrastructures in two Microsoft Azure regions (US East, US East 2) to facilitate this example.

Each region was configured with the following components.

Table 153: Microsoft Azure Infrastructure Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management VNet</td>
<td>Microsoft Azure Virtual Network (VNet) configured to host shared services for use by the Horizon Cloud deployments.</td>
</tr>
<tr>
<td>VNet peer (management to pod)</td>
<td>Unidirectional network connection between two VNets in Microsoft Azure. Both the Allow forwarded traffic and Allow Gateway Transit options were selected in the VNet configuration to ensure proper connectivity between the two VNets.</td>
</tr>
<tr>
<td>VNet peer (pod to management)</td>
<td>Unidirectional network connection between two VNets in Microsoft Azure. Both the Allow Forwarded Traffic and the Allow Gateway Transit options were selected in the VNet configuration to ensure proper connectivity between the two VNets.</td>
</tr>
<tr>
<td>Microsoft Azure VPN Gateway</td>
<td>VPN gateway resource provided by Microsoft Azure to provide point-to-point private network connectivity to another network.</td>
</tr>
</tbody>
</table>
Table 153: Microsoft Azure Infrastructure Components (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two Microsoft Windows Server VMs</td>
<td>Two Windows servers provide redundancy in each Microsoft Azure region for common network services.</td>
</tr>
<tr>
<td>Active Directory domain controller</td>
<td>Active Directory was implemented as a service on each Windows server. Active Directory was configured according to Option 3 in Networking and Active Directory Considerations on Microsoft Azure for use with VMware Horizon Cloud Service.</td>
</tr>
<tr>
<td>DNS server</td>
<td>DNS was implemented as a service on each Windows server.</td>
</tr>
<tr>
<td>Windows DFS file share</td>
<td>A Windows share with DFS was enabled on each Windows server to contain the User Environment Manager profile and configuration shares.</td>
</tr>
<tr>
<td>Horizon Cloud control pod VNet</td>
<td>Microsoft Azure VNet created for use of the Horizon Cloud pod. This VNet contains all infrastructure and user services components (RDSH servers, VDI desktops) provided by the Horizon Cloud pod.</td>
</tr>
</tbody>
</table>

We also leveraged two separate Microsoft Azure subscriptions to demonstrate that multiple pods could be deployed to different subscriptions and managed from the same Horizon Cloud Service with Microsoft Azure control plane. For more detail on the design decisions that were made for Horizon Cloud pod deployments, see "Component Design: Horizon Cloud Service on Microsoft Azure" on page 161.

**Network Connectivity to Microsoft Azure**

You do not need to provide private access to Microsoft Azure as a part of your Horizon Cloud on Microsoft Azure deployments. The Microsoft Azure infrastructure can be provided from the Internet.

There are several methods for providing private access to infrastructure deployed to any given Microsoft Azure subscription in any given Microsoft Azure region, including by using a **VPN** or **ExpressRoute** configurations.
Table 154: Implementation Strategy for Providing Private Access to Horizon Cloud Service

<table>
<thead>
<tr>
<th>Decision</th>
<th>VPN connections were leveraged. Connections were made from the on-premises data center to each of the two Microsoft Azure regions used for this design.</th>
</tr>
</thead>
</table>
| Justification | This is the most typical configuration that we have seen in customer environments to date.  
See [Connecting your on-premises network to Azure](#) for more details on the options available to provide a private network connection to Microsoft Azure. |

**Microsoft Azure Virtual Network (VNet)**

In a Horizon Cloud Service on Microsoft Azure deployment, you are required to configure virtual networks (VNets) for use by the Horizon Cloud pod. You must have already created the VNet you want to use in that region in your Microsoft Azure subscription before deploying Horizon Cloud Service.

Note that DHCP is a service that is a part of a VNet configuration. For more information on how to properly configure a VNet for Horizon Cloud Service, see [Configure the Required Virtual Network in Microsoft Azure](#).

Another useful resource is the [VMware Horizon Cloud Service on Microsoft Azure Requirements Checklist](#).
Platform Integration

After the various VMware Workspace ONE® and VMware Horizon® products and components have been designed and deployed, some one-time integration tasks must be completed to realize the full power of the Workspace ONE platform.

- Integrate VMware Workspace ONE® UEM with VMware Identity Manager™.
- Integrate VMware Horizon® Cloud Service™ with VMware Identity Manager.

Workspace ONE UEM and VMware Identity Manager Integration

VMware Identity Manager and Workspace ONE UEM (powered by AirWatch) are built to provide tight integration between identity and device management. This integration has been simplified in recent versions to ensure that configuration is relatively straightforward. For information about the latest release, see Integrating Workspace ONE UEM With VMware Identity Manager.

Although VMware Identity Manager and Workspace ONE UEM are the core components in a Workspace ONE deployment, you can also deploy a variety of other components, depending on your business use cases. As the following figure shows, you can use VMware Workspace ONE® UEM Secure Email Gateway (SEG) for access to an on-premises Exchange server or use VMware Unified Access Gateway to provide VMware Workspace ONE® Tunnel or VPN-based access to internal resources. Refer to the various sections in the VMware Workspace ONE UEM Online Help for documentation of the full range of components that apply to a deployment.

Figure 123: Sample Workspace ONE Architecture

Many other enterprise components can be integrated into a Workspace ONE deployment. These components include technologies such as a Certificate Authority, Active Directory, file services, email.
system, SharePoint servers, external access servers, or reverse proxies. We assume that these enterprise systems are in place and are functional if necessary.

To successfully integrate Workspace ONE UEM with VMware Identity Manager, you can use the Workspace ONE Getting Started wizards. The Identity and Access Management wizard walks you through setting up the AirWatch Cloud Connector to allow the components of Workspace ONE, Workspace ONE UEM, and VMware Identity Manager to communicate with your Active Directory. Documentation for this process is available in the Guide to Deploying VMware Workspace ONE.

**AirWatch Cloud Connector and Directory Integration Configuration Wizard**

You can use the Workspace ONE wizards to set up the AirWatch Cloud Connector, Active Directory integration, and VMware Identity Manager integration.

![Figure 124: Identity and Access Management Wizard](image)

The first step in the wizard is to connect the Workspace ONE UEM instance to the VMware Identity Manager tenant.
After you enter the fully qualified domain name (FQDN) and supply authentication credentials for the VMware Identity Manager tenant, the connection can be made.

- The Workspace ONE UEM Administration Console servers must be able to reach the VMware Identity Manager tenant through port 443.
- The VMware Identity Manager tenant must be able reach the Workspace ONE UEM API service through port 443.

After the connection is made, the first step in the Identity and Access Management wizard is marked as complete.

The next step in the Identity and Access Management wizard is to install the AirWatch Cloud Connector and connect Workspace ONE UEM to Active Directory.
The AirWatch Cloud Connector provides the ability to integrate Workspace ONE UEM with an organization’s backend enterprise systems. It is enabled in the Workspace ONE UEM Console and is downloaded to a Windows Server in the enterprise to enable communication between Active Directory and the Workspace ONE service.

Figure 127: AirWatch Cloud Connector and VMware Identity Manager Connector

The wizard prompts you to set up a password before downloading the AirWatch Cloud Connector installer. Use this password while running the installer.

Previous versions of Workspace ONE UEM provided access to the AirWatch Cloud Connector by using the Enterprise Systems Connector installer, a bundled installer of the AirWatch Cloud Connector and VMware Identity Manager. With current versions of Workspace ONE UEM, the VMware Identity Manager connector is downloaded as a separate installer.
Active Directory Integration

The next step, after setting up the AirWatch Cloud Connector, is to enter your Active Directory and bind authentication information to integrate AD with Workspace ONE UEM. Because you are making connections from the AirWatch Cloud Connector, ensure that networking and server IPs and host names can be resolved.

**Note:** Ensure that the Active Directory domain name you enter in the wizard matches the name used in VMware Identity Manager. Otherwise, administrators will not be able to access some features and configurations of VMware Identity Manager from the Workspace ONE UEM Console.

![Image of VMware Identity Manager Connector Configuration](image)

**Figure 129:** Connect to Active Directory

**VMware Identity Manager Connector Configuration**

The VMware Identity Manager Connector provides connectivity to synchronize VMware Identity Manager with your user directory, such as Active Directory. The VMware Identity Manager Connector also provides user authentication and integration with Horizon Cloud, along with following capabilities:

- Many authentication methods for external users, including password, RSA Adaptive Authentication, RSA SecurID, and RADIUS
- Kerberos authentication for internal users
- Access to VMware Horizon Cloud Service resources
- Access to VMware Horizon resources
- Access to Citrix-published resources
To set up the VMware Identity Manager Connector along with directory integration, see Installing and Configuring VMware Identity Manager Connector 2018.8.1.0 (Windows) and Directory Integration with VMware Identity Manager.

Catalog Population

The unified Workspace ONE app catalog contains many types of applications. SaaS-based SAML apps and Horizon apps and desktops are delivered through the VMware Identity Manager catalog, and native mobile apps are delivered through the Workspace ONE UEM catalog.

Table 155: Configuration Considerations for Populating the VMware Identity Manager Catalog

<table>
<thead>
<tr>
<th>Resource</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS apps</td>
<td>• To add a new SaaS application, go to the Catalog tab, select Web Apps from the drop-down list, and select New.</td>
</tr>
<tr>
<td></td>
<td>• Applications can be defined manually, or a predefined application template can be customized. See Setting Up Resources in VMware Identity Manager (SaaS) or Setting Up Resources in VMware Identity Manager (On Premises).</td>
</tr>
<tr>
<td></td>
<td>• You can manually create SaaS apps that do not have a template in the cloud catalog by using the appropriate parameters.</td>
</tr>
<tr>
<td></td>
<td>• Assign the appropriate users or groups to the applications being published and choose whether the entitlement is user-activated or automatic.</td>
</tr>
<tr>
<td>VMware Horizon® 7 or Horizon Cloud</td>
<td>• To include Horizon 7 or Horizon Cloud resources in the catalog, entitlements are synced from the Horizon environment to VMware Identity Manager.</td>
</tr>
<tr>
<td></td>
<td>• Horizon 7 and Horizon Cloud pods are added into the VMware Identity Manager catalog.</td>
</tr>
<tr>
<td></td>
<td>• For more information, see &quot;Horizon 7 and VMware Identity Manager Integration&quot; on page 256 and &quot;Horizon Cloud Service and VMware Identity Manager Integration&quot; on page 265.</td>
</tr>
<tr>
<td></td>
<td>• The launch of a Horizon desktop or application from VMware Identity Manager does not alter the traffic path of the Horizon session. External access to Horizon environments still requires Unified Access Gateway appliances.</td>
</tr>
</tbody>
</table>
Table 156: Configuration Considerations for Populating the Workspace ONE UEM Catalog

<table>
<thead>
<tr>
<th>Resource</th>
<th>Configuration Considerations</th>
</tr>
</thead>
</table>
| Native mobile apps                | • In the Workspace ONE UEM Console, you use the Apps and Books node to assign apps from the public app stores to their respective device platforms. Apps are defined by platform (iOS, Android, Windows, and more) and located in the app store for that platform.  
• The apps are then assigned to Smart Groups as appropriate.  
• Application configuration key values are provided to point the Workspace ONE app to the appropriate VMware Identity Manager tenant.  
• Recommended apps to deploy include the Workspace ONE mobile app and popular Workspace ONE apps such as VMware Workspace ONE® Boxer, VMware Workspace ONE® Content, and VMware Workspace ONE® Browser. |

**Device Profile Configuration and Single Sign-On**

Device profiles provide key settings that are applied to devices as part of enrollment in Workspace ONE UEM. The settings include payloads, such as credentials, passcode requirements, and other parameters used to configure and secure devices. Different payloads are configured in different services for this document, but SSO is a common requirement across all devices and use cases.
The iOS platform uses the mobile SSO authentication adapter. The authentication adapter is enabled in VMware Identity Manager and added to an access policy. A profile is deployed that provides the appropriate certificate payloads to support trust between the user, the iOS device, Workspace ONE UEM, and VMware Identity Manager. For more information, see Implementing Mobile Single Sign-in Authentication for Workspace ONE UEM-Managed iOS Devices.

- Use the Mobile SSO Getting Started wizard to enable mobile SSO in your environment.
- The Mobile SSO wizard creates an SSO profile that uses a certificate issued by the AirWatch Certificate Authority.

Android SSO

- Android uses the mobile SSO authentication adapter. It is enabled in VMware Identity Manager and added to an access policy. A profile is deployed to support SSO. For more information, see Implementing Mobile Single Sign-On Authentication for Workspace ONE UEM Managed Android Devices.
- Use the Mobile SSO Getting Started wizard to enable mobile SSO in your environment.
- The Mobile SSO wizard creates the necessary Workspace ONE Tunnel device profile, publishes the Workspace ONE Tunnel application, and creates the required network rules.

Windows 10 SSO

- Windows 10 SSO uses certificate authentication. A certificate is generated from the AirWatch CA through a SCEP (Simple Certificate Enrollment Protocol) profile. When a device profile is deployed, the appropriate certificates are generated for the user and are installed on the user’s device. The certificate (cloud deployment) authentication adapter is enabled to use Windows 10 SSO. For more information, see Configuring a Certificate or Smart Card Adapter for Use with VMware Identity Manager.
- The user is prompted to select a certificate at Workspace ONE app launch.
- For device-compliance checking to function, part of the certificate request template for Workspace ONE UEM must include a SAN type of DNS name with a value of $UDID=${DeviceUId}.

### Table 157: Configuration Considerations for Device Profiles in Workspace ONE UEM

<table>
<thead>
<tr>
<th>Device Profiles</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS SSO</td>
<td>- The iOS platform uses the mobile SSO authentication adapter. The authentication adapter is enabled in VMware Identity Manager and added to an access policy. A profile is deployed that provides the appropriate certificate payloads to support trust between the user, the iOS device, Workspace ONE UEM, and VMware Identity Manager. For more information, see Implementing Mobile Single Sign-in Authentication for Workspace ONE UEM-Managed iOS Devices. - Use the Mobile SSO Getting Started wizard to enable mobile SSO in your environment. - The Mobile SSO wizard creates an SSO profile that uses a certificate issued by the AirWatch Certificate Authority.</td>
</tr>
<tr>
<td>Android SSO</td>
<td>- Android uses the mobile SSO authentication adapter. It is enabled in VMware Identity Manager and added to an access policy. A profile is deployed to support SSO. For more information, see Implementing Mobile Single Sign-On Authentication for Workspace ONE UEM Managed Android Devices. - Use the Mobile SSO Getting Started wizard to enable mobile SSO in your environment. - The Mobile SSO wizard creates the necessary Workspace ONE Tunnel device profile, publishes the Workspace ONE Tunnel application, and creates the required network rules.</td>
</tr>
<tr>
<td>Windows 10 SSO</td>
<td>- Windows 10 SSO uses certificate authentication. A certificate is generated from the AirWatch CA through a SCEP (Simple Certificate Enrollment Protocol) profile. When a device profile is deployed, the appropriate certificates are generated for the user and are installed on the user’s device. The certificate (cloud deployment) authentication adapter is enabled to use Windows 10 SSO. For more information, see Configuring a Certificate or Smart Card Adapter for Use with VMware Identity Manager. - The user is prompted to select a certificate at Workspace ONE app launch. - For device-compliance checking to function, part of the certificate request template for Workspace ONE UEM must include a SAN type of DNS name with a value of $UDID=${DeviceUId}.</td>
</tr>
</tbody>
</table>
The VMware Identity Manager directory synchronizes user account information from Active Directory and uses it for entitling applications to users through the Workspace ONE app or browser page. For SSO and True SSO to work when integrating with VMware Identity Manager and VMware Horizon, a number of configuration considerations must be considered.

**Table 158: Configuration Considerations for Features in VMware Identity Manager**

<table>
<thead>
<tr>
<th>Component</th>
<th>Configuration Considerations</th>
</tr>
</thead>
</table>
| VMware Identity Manager catalog | This catalog is the launch point for applications through the Workspace ONE portal. Applications in the following categories are expected to be configured:  
  - SaaS apps  
  - VMware ThinApp® packages  
  - Horizon 7 and Horizon Cloud desktop assignments  
  - Horizon 7 and Horizon Cloud RDSH-published apps |
| True SSO | True SSO support is configured in VMware Identity Manager to ensure simple end-user access to desktops and apps without multiple login prompts and without requiring AD credentials. |
| Identity Manager Connectors | VMware Identity Manager Connectors are placed in the internal network to ensure that users external to the organization can access the resources that have been configured in the Workspace ONE catalog. |
| ThinApp packages | A ThinApp repository with ThinApp packages can 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 application in order to use ThinApp packages in your environment. For more information see: Providing Access to VMware ThinApp Packages.  
**Note:** In this reference architecture we used the Windows-based VMware Identity Manager Connector. Today this version does not support ThinApp. If you require ThinApp support, you must use the Linux (virtual appliance) version of the VMware Identity Manager Connector. |
| SaaS-based web apps | SaaS-based applications that use SAML as an authentication method can be accessed through VMware Identity Manager. Configuration of applications is done through the templates in the cloud application catalog. See Setting Up Resources in VMware Identity Manager (SaaS) or Setting Up Resources in VMware Identity Manager (On Premises). |
| Horizon desktop | - In the VMware Identity Manager administration console, create one or more virtual apps collections for the Horizon 7 pods or Horizon Cloud ten- |
### Table 158: Configuration Considerations for Features in VMware Identity Manager (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>assignments</td>
<td>- Configure SAML authentication between VMware Identity Manager and the Horizon 7 pods or Horizon Cloud tenants.</td>
</tr>
<tr>
<td>Horizon published applications</td>
<td>- RDSH-published applications and their entitlements populate the VMware Identity Manager catalog when Horizon 7 pods or Horizon Cloud tenants are configured as described for virtual desktop assignments.</td>
</tr>
</tbody>
</table>
| Active Directory Kerberos authentication | - To provide SSO to the VMware Identity Manager catalog, the appropriate authentication methods must be enabled.  
  - The default authentication method is password, which prompts for the user’s Active Directory user ID and password.  
  - If Kerberos is enabled as the default authentication method, the user’s Windows credentials are passed to VMware Identity Manager when the user opens the catalog.  
  - Kerberos authentication must be enabled under the Connectors section in the administration console. For more information, see Implementing Kerberos for Desktops with Integrated Windows Authentication. |
| Access policies | - Access policies are configured to establish how users will authenticate to an operating system, network, or application.  
  - Use the **Identity and Access Management** tab to manage policies and edit the default access policy, as described in Managing Access Policies.  
  - You can use different policies for different network ranges so that, for example, AD Kerberos is used for internal connections but other authentication methods are used for external connections. |

### Workspace ONE Intelligence and Workspace ONE UEM Integration

VMware Workspace ONE Intelligence offers insights into your digital workspace. It offers enterprise mobility management (EMM) planning and automation. All these components help to optimize resources, strengthen security and compliance, and increase user experience across your environment.

Workspace ONE UEM is the minimum and main required integration point for Workspace ONE Intelligence. When Workspace ONE UEM is hosted on-premises, it requires the installation of the...
Workspace ONE Intelligence Connector service (also known as the ETL installer) on the internal network.
For those using cloud-based Workspace ONE UEM, there is no need to install the Workspace ONE Intelligence Connector service because it is already enabled by default.

The Workspace ONE Intelligence Connector service collects data related to devices, apps, and OS updates from your Workspace ONE UEM database and pushes this data to the cloud-based report service.

![Diagram of Workspace ONE UEM and Workspace ONE Intelligence Integration](image)

**Figure 130**: Integration of Workspace ONE UEM with Workspace ONE Intelligence Cloud Service.

The integration consists of five high-level steps:

1. Define the region where the ETL service will sync the data. This information will be required during the installation process.

2. Ensure you have whitelisted the applicable URLs so that the connector installation process can communicate with the correct cloud-based reports service.
   For the list of URLs, see [URLs to Whitelist for On-Premises by Region](#).
   If you use a proxy server and want to use it with the Workspace ONE Intelligence Connector, make sure you have whitelisted specific destinations. If you do not whitelist these destinations, the installation can fail. See [URLs to Whitelist for the Use of a Proxy Server in On-Premises Deployments](#).

3. Ensure you have met the hardware, software, and network requirements outlined in [Workspace ONE Intelligence Requirements](#).

4. Run the ETL installer, which will ask for the Workspace ONE UEM Installation Token that can be generated through [https://my.workspaceone.com](https://my.workspaceone.com).
   For more information, see [Install the Workspace ONE Intelligence Connector Service for On-Premises](#).

After you successfully install the ETL service and opt in to Workspace ONE Intelligence through Workspace ONE UEM console, the ETL service will perform the first import of all devices, apps, and...
OS updates data. Subsequent synchronizations will be based on samples taken from the devices, apps, and OS updates.

**Workspace ONE Intelligence and VMware Identity Manager Integration**

VMware Identity Manager can be integrated with Workspace ONE Intelligence to provide insights on user logins and application launches. The integration requires a cloud-based VMware Identity Manager tenant and a licensed tenant of Workspace ONE Intelligence.

![Integration of Workspace ONE Intelligence Cloud Service with VMware Identity Manager](image)

**Figure 131**: Integration of Workspace ONE Intelligence Cloud Service with VMware Identity Manager.

Because the integration is performed between two cloud services, there are no need to perform on-premises configurations.

The integration consists of two high-level steps:

1. Log in to VMware Identity Manager as an administrator.

2. Register the VMware Identity Manager tenant in the Workspace ONE Intelligence Console, as outlined in **Register VMware Identity Manager in Settings**.

![Settings](image)

**Figure 132**: Workspace ONE Intelligence Successfully Integrated with VMware Identity Manager.

After integration is complete, Workspace ONE Intelligence collects user and event data about Workspace ONE logins and app loads for all the apps contained in the Workspace ONE catalog. Events are synced every second or when 50,000 events have accumulated, whichever comes first.

For a complete list of data collected by the integration, see:
- Data Collected from VMware Identity Manager for the App Launches Templates
- Data Collected from VMware Identity Manager for the User Logins Templates

For step-by-step instructions on how to integrate VMware Identity Manager with Workspace ONE Intelligence, and an overview of how to create dashboards, watch VMware Workspace ONE Intelligence: VMware Identity Manager Integration - Feature Walk-through.

**Horizon 7 and VMware Identity Manager Integration**

Horizon 7 can be integrated into Workspace ONE through VMware Identity Manager. You can set up SSO for Horizon 7 apps and desktops, ensure security with multi-factor authentication, and control conditional access.

The Horizon 7 Enterprise Edition license includes the on-premises version of VMware Identity Manager, which supports access to Horizon 7 apps and desktops only.

![Horizon 7 and On-Premises VMware Identity Manager Integration Diagram](image)

**Figure 133:** Integration of Horizon 7 and On-Premises VMware Identity Manager

Horizon 7 can be used with other license types and deployment models of VMware Identity Manager (such as cloud-based) if access to other apps such as Horizon 7 apps and desktops, SaaS apps, or mobile apps, is also required.
Integrating Horizon 7 with an instance of VMware Identity Manager consists of three high-level steps:

1. Complete the prerequisite steps outlined in the next section. These steps include deploying VMware Identity Manager Connectors and configuring Active Directory synchronization.

2. Create one or more virtual apps collections, as described in "Virtual Apps Collection Creation for Horizon 7 Integration" below.

3. Configure SAML authentication in your Horizon 7 environment, as described in "SAML Authentication Configuration for Horizon 7 Integration" on page 261.

**Prerequisites for Horizon 7 Integration**

- Prepare the VMware Identity Manager environment by following the instructions in Using Virtual Apps Collections for Desktop Integrations and Providing Access to View, Horizon 6, or Horizon 7 Desktop and Application Pools.

- Ensure time synchronization is set so that VMware Identity Manager, VMware Identity Manager Connectors, and Horizon Connection Servers have the same time.

**Virtual Apps Collection Creation for Horizon 7 Integration**

You can integrate Horizon 7 desktops and applications into VMware Identity Manager by using virtual apps collections. See Configure Horizon Pods and Pod Federations in VMware Identity Manager.

1. Log in to the VMware Identity Manager administrative console.

2. From the Catalog drop-down menu, select Virtual Apps.

3. Click the Virtual App Configuration button.
If this is the first time the configuration has been run, a screen appears that provides information about virtual apps collections, as shown in the next step.

4. If the following screen appears, click the **Get Started** button.

5. Create a Horizon 7 virtual apps collection for each Horizon 7 pod that will host desktop or application capacity.

A virtual apps collection contains configuration information about your Horizon 7 environment, VMware Identity Manager Connectors, and settings to sync resources and entitlements to VMware Identity Manager. For clarity, the wizard is displayed in four parts in the steps that follow.

6. Name the virtual app collection and select the connectors.
   a. Give the virtual app collection a unique name.
   b. Select the VMware Identity Manager Connectors that will perform synchronization.
7. Add the Horizon 7 pods.
   a. Enter details for the first Horizon pod, specifying one of the Horizon Connection Servers, credentials, and whether smart card authentication or True SSO is set up in the pod.
   b. Click **Add Pod** and repeat the process for each Horizon pod in your environment.

   a. Select the check box to indicate if Cloud Pod Architecture is enabled.
   b. Specify a unique federation name.
   c. Select and add the pods that are part of this federation.
d. Complete the **Launch FQDN** field. This is usually the load balancer namespace for the Horizon environment.

9. Select **Do not sync duplicate applications**.
10. Choose which default client should be used for a Horizon session.
11. Setup a sync frequency schedule.

12. In addition to specifying a sync frequency, if you want to force synchronization of any entitlements, select the **Sync** button on the Virtual Apps page.

**Note:** You can also configure different client access FQDNs for specific network ranges. For example, perhaps different FQDNs should be used for internal and external connections.
The default configuration for network settings in VMware Identity Manager specifies a single All Ranges scope. Any Horizon 7 pods added will, by default, use the FQDN of the Horizon Connection Server used for adding the pod. Be sure to change the FQDN to the load balancer common namespace for the Connection Servers. Also consider adding additional network ranges and tailoring the client access FQDN as necessary.

See Configure Horizon Pods and Pod Federations in VMware Identity Manager for more information.

**SAML Authentication Configuration for Horizon 7 Integration**

After you create a virtual apps collection for Horizon 7 in the VMware Identity Manager console, add VMware Identity Manager as a SAML 2.0 authenticator to the Horizon Connection Servers. Repeat this process for each additional pod.

1. Open the Horizon 7 Administrator console.
2. Navigate to View Configuration > Servers > Connection Servers.
3. Select one of the Connection Servers and click Edit.
4. On the Authentication tab, change Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator) to either Allowed or Required.
5. Select Manage SAML Authenticators and click Add.
6. Enter a label to identify the authenticator.
7. In the Metadata URL field, change <YOUR SAML AUTHENTICATOR NAME> to the FQDN of VMware Identity Manager. Leave the other text as it is.
8. Leave Enabled for Connection Server selected and click OK.
Although the SAML 2.0 authenticator is defined once per pod, you must enable the authenticator individually on each Connection Server that is to use SAML authentication.

1. Use the Horizon 7 Administrator console to edit the configuration of each Connection Server.
2. Select the Authentication tab and change Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator) to either Allowed or Required, matching what was selected on the first Connection Server.
3. Select Manage SAML Authenticators, select the SAML authenticator just defined, and click Edit.
4. Select Enabled for Connection Server and click OK.

For more information see, Configure SAML Authentication.

**Communication Flow When Launching a Horizon 7 Resource from VMware Identity Manager**

After Horizon 7 has been integrated with VMware Identity Manager, a user can select a Horizon resource, such as desktop or a published application, from the Workspace ONE browser page or mobile app.

**Internal Client**

The following figure depicts the flow of communication that takes place when an internal user selects and launches an entitled Horizon desktop or application. Although this illustrates the use of an on-
premises deployment of VMware Identity Manager, the traffic flow is the similar if a cloud-based tenant of VMware Identity Manager is used.

**Figure 136**: Internal Launch of a Horizon 7 Resource from Workspace ONE

1. After the user is authenticated to VMware Identity Manager, either in a browser or using the Workspace ONE app, the user selects and launches a Horizon 7 resource.

2. VMware Identity Manager generates a SAML assertion and an artifact that contains the \texttt{vmware-view} URL. It returns this SAML artifact to the browser on the client device (\texttt{vmware-view://URL SAMLArt=<saml-artifact>}).

3. The default URL handler for \texttt{vmware-view} types (normally the VMware Horizon® Client™) is launched using the URL that was returned in the artifact (XML-API request do-submit-authentication \texttt{<saml-artifact>}).

4. The Horizon Connection Server performs a SAML Artifact Resolve operation against VMware Identity Manager (\texttt{<saml-artifact>}).

5. VMware Identity Manager validates the artifact and returns a SAML Assertion to the Horizon Connection Server (\texttt{<saml-assertion>}).


7. The remote protocol client launches the session with the parameters returned.

**External Client**

The following figure depicts the flow of communication that takes place when an external user selects and launches an entitled Horizon desktop or application. Although this illustrates the use of an on-
premises deployment of VMware Identity Manager, the traffic flow is similar if a cloud-based tenant of VMware Identity Manager is used.

Figure 137: External Launch of a Horizon 7 Resource from Workspace ONE

1. After the user is authenticated to VMware Identity Manager, either in a browser or using the Workspace ONE app, the user selects and launches a Horizon 7 resource.

2. VMware Identity Manager generates a SAML assertion and a SAML artifact that contains the vmware-view URL. It returns this URL to the browser on the client device (vmware-view://URL SAMLArt=<saml-artifact>).

3. The default URL handler for vmware-view types (normally the VMware Horizon® Client™) is launched using the URL that was returned in the artifact (XML-API request do-submit-authentication <saml-artifact>).

4. Unified Access Gateway proxies the authentication to the Horizon Connection Server

5. The Horizon Connection Server performs a SAML resolve against VMware Identity Manager (<saml-artifact>).

6. VMware Identity Manager validates the artifact and returns an assertion to the Horizon Connection Server (<saml-assertion>).


8. Unified Access Gateway returns the successful authentication to the Client

9. The remote protocol client launches the session with the parameters returned.

10. Unified Access Gateway proxies the protocol session to the Horizon Agent.
Horizon Cloud Service and VMware Identity Manager Integration

Horizon Cloud can be integrated into Workspace ONE through VMware Identity Manager. You can set up SSO for Horizon Cloud apps and desktops, ensure security with multi-factor authentication, and control conditional access.

The Horizon Cloud license includes the cloud-hosted version of VMware Identity Manager, which supports access to Horizon Cloud apps and desktops only. Horizon Cloud can be used with other license types and deployment models of VMware Identity Manager (such as on-premises) if access to other apps such as Horizon 7 apps and desktops, SaaS apps, or mobile apps, is also required.

![Figure 138: Integration of Horizon Cloud and VMware Identity Manager](image)

With VMware Horizon® Cloud Service™ on Microsoft Azure, you can specify creation of a cloud-based VMware Identity Manager tenant during the pod deployment process. The VMware Identity Manager tenant is associated with your Horizon Cloud customer record. Pods that already exist for the same Horizon Cloud customer record can then be integrated with that tenant.

Integrating Horizon Cloud Service with a cloud-hosted VMware Identity Manager tenant consists of three high-level steps:

1. Complete the prerequisite steps outlined in the next section. These steps include deploying VMware Identity Manager Connectors and configuring Active Directory synchronization.

2. Create one or more virtual apps collections, as described in "Virtual Apps Collection Creation for Horizon Cloud Integration" on the next page.

3. Configure SAML authentication in your Horizon Cloud tenant, as described in "SAML Authentication Configuration for Horizon Cloud Integration" on page 268.

Prerequisites for Horizon Cloud Integration

- Prepare the VMware Identity Manager environment by following the instructions in Providing Access to VMware Horizon Cloud Service Desktops and Applications.

- Verify that VMware Identity Manager is joined to same Active Directory domain structure as the Horizon Cloud pod.
Ensure that time synchronization is set so that VMware Identity Manager and Horizon Cloud pod have the same time.

**Virtual Apps Collection Creation for Horizon Cloud Integration**

You can integrate Horizon Cloud desktops and applications into VMware Identity Manager by using virtual apps collections. See [Configure Horizon Cloud Tenant in VMware Identity Manager](#).

1. Log in to the VMware Identity Manager administrative console.
2. From the **Catalog** drop-down menu, select **Virtual Apps**.
3. Click the **Virtual App Configuration** button.

If this is the first time the configuration has been run, a screen appears that provides information about virtual apps collections, as shown in the next step.

4. If the following screen appears, click the **Get Started** button.

5. Create a Horizon Cloud virtual apps collection for each Horizon Cloud pod that will host desktop or application capacity.
The virtual apps collection contains configuration information about your Horizon Cloud tenant, VMware Identity Manager Connectors, and settings to sync resources and entitlements to VMware Identity Manager. For clarity, the wizard is displayed in three parts in the steps that follow.

6. Name the virtual app collection and select the connectors.
   
a. Give the virtual app collection a unique name.
   
b. Select the VMware Identity Manager Connectors that will perform synchronization.

7. Add the Horizon Cloud tenants.
   
a. Enter the details of the first tenant host, supply credentials, specify the Active Directory domains to sync, and specify whether True SSO is configured.
   
b. Click Add Tenant and repeat the process for each Horizon tenant.

8. Choose which default client should be used for a Horizon session.
9. Select a schedule from the **Sync Frequency** drop-down list.

   ![Image showing default launch client and sync frequency settings]

10. In addition to specifying a sync frequency, if you want to force synchronization of any entitlements, click the **Sync** button on the Virtual Apps page.

   ![Image showing VMware Identity Manager with SAML configurations]

For more information on configuring virtual apps collections, see Using Virtual Apps Collections for Desktop Integrations.

**SAML Authentication Configuration for Horizon Cloud Integration**

After you create a virtual apps collection for the Horizon Cloud tenant in the VMware Identity Manager console, configure SAML authentication in the Horizon Cloud tenant.

You can create a new Identity Management entry for each pod in your Horizon Cloud tenant.

1. Log in to the Horizon Cloud Administrative Console.
2. From **Settings**, select **Identity Management** and click **New**.

   ![Image showing new identity manager configuration]

For more information see, Configure SAML Authentication in the Horizon Cloud Tenant.
Communication Flow When Launching a Horizon Cloud Resource from VMware Identity Manager

After Horizon Cloud has been integrated with VMware Identity Manager, a user can select a Horizon resource, such as desktop or a published application, from the Workspace ONE browser page or mobile app.

The following figure depicts the flow of communication that takes place when a user selects and launches an entitled Horizon desktop or application.

![Diagram](image)

Figure 139: Traffic Flow on Launch of a Horizon Cloud Resource from Workspace ONE

1. After the user is authenticated to VMware Identity Manager, either in a browser or using the Workspace ONE app, the user selects and launches a Horizon resource.

2. VMware Identity Manager generates a SAML assertion and an artifact that contains the `vmware-view` URL. It returns this URL to the browser on the client device (`vmware-view://URL SAMLArt=<saml-artifact>`).

3. The default URL handler for `vmware-view` types (normally the VMware Horizon Client) is launched using the URL that was returned in the artifact (`XML-API request do-submit-authentication <saml-artifact>`).

4. If in-line, VMware Unified Access Gateway (UAG) proxies the authentication to the Horizon Cloud pod.

5. The Horizon Cloud pod performs a SAML resolve against VMware Identity Manager (`<saml-artifact>`).
6. VMware Identity Manager validates the artifact and returns an assertion to the Horizon Cloud pod (<saml-assertion>).


8. If in-line, Unified Access Gateway returns the successful authentication to the Horizon Client.

9. The remote protocol client launches the session with the parameters returned.

10. If in-line, Unified Access Gateway proxies the protocol session to the Horizon Agent in the virtual desktop or RDSH server (if the resource is a published application or desktop).
Service Integration Design

At this stage, the VMware Workspace ONE® and VMware Horizon® components have been designed and deployed, and the environment has all the functionality and qualities that are required. We can now proceed to creating the parts from each component and assembling and integrating them into the various services that are to be delivered to end users. Some components are common to multiple services.

Workspace ONE Use Case Service Integration

The following table lists the parts required for each Workspace ONE service. The rest of this section details the design and configuration of each service.

Table 159: Service Requirements

<table>
<thead>
<tr>
<th>Service</th>
<th>Enterprise Mobility Management Service</th>
<th>Enterprise Productivity Service</th>
<th>Enterprise Application Workspace Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Workspace ONE® UEM</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VMware Identity Manager™</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>AirWatch Cloud Connector</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VMware Identity Manager Connector</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VMware Workspace ONE® Verify</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Adaptive management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device enrollment</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Native mobile apps</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SaaS apps</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unified app catalog</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mobile email management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile content management</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 159: Service Requirements (Continued)

<table>
<thead>
<tr>
<th></th>
<th>Enterprise Mobility Management Service</th>
<th>Enterprise Productivity Service</th>
<th>Enterprise Application Workspace Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP restrictions</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Secure browsing</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Mobile SSO</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Conditional access</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VMware Horizon® 7 or VMware Horizon® Cloud Service™</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>VMware Unified Access Gateway™</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

The two broad categories of application types are handled as follows:

- **SaaS applications** – Are added from the Workspace ONE SaaS cloud catalog and are entitled to appropriate users.
- **Native mobile apps** – Are added from the Workspace ONE UEM Console. Privileged apps have the Require Management option selected; other apps do not.

**Enterprise Mobility Management Service**

The Enterprise Mobility Management service brings an organization that has minimal device management capabilities—such as Exchange ActiveSync policies applied for passcode, wipe, and other basic settings—under an EMM strategy.

The devices are initially configured to support adaptive management. Some less critical applications are enabled for SSO, while other applications are configured to require enrollment. Employees are encouraged, but not required, to enroll their devices. Users can use their native email clients, email apps available from the public app stores, or VMware Workspace ONE® Boxer.
Devices in this service have the following characteristics.

**Table 160: Configuration Considerations for the Enterprise Mobility Management Service**

<table>
<thead>
<tr>
<th>Service Feature</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive management</td>
<td>- Adaptive management enables applications such as WebEx and Concur to be used with mobile SSO across all platforms without device enrollment. Other applications, such as HR sites, ADP, or Salesforce, require device enrollment to have a high degree of control over the device.</td>
</tr>
<tr>
<td></td>
<td>- Users are encouraged to download the Workspace ONE app from a public app store.</td>
</tr>
<tr>
<td></td>
<td>- Applications that are deemed to have a higher risk to user or company data are set to require management in the VMware Workspace ONE® UEM device profile.</td>
</tr>
<tr>
<td>Active Directory – cloud password authentication</td>
<td>VMware Identity Manager is configured with a policy to use the cloud password from the built-in identity provider and authenticate through the VMware Identity Manager Connector to the Active Directory account.</td>
</tr>
<tr>
<td>Email access</td>
<td>- Users are provided appropriate documentation on how to configure their device for native or third-party email client access.</td>
</tr>
<tr>
<td></td>
<td>- If users choose to install Workspace ONE Boxer, their email configuration is automatically pushed to the device. Typically, users are provided with the Exchange ActiveSync Server address (outlook.office365.com) and their email address and password.</td>
</tr>
<tr>
<td>Enrollment</td>
<td>- Enrollment is completed through the Workspace ONE application. If a user attempts to access an application that has been deployed as one that requires management in Workspace ONE UEM, the enrollment process is initiated.</td>
</tr>
<tr>
<td></td>
<td>- After enrollment in Workspace ONE, end users have all applications available to them. They can also use mobile SSO after they have enrolled because they have a device profile. This profile deploys the appropriate payloads to authenticate using the appropriate SSO technology.</td>
</tr>
<tr>
<td></td>
<td>- Additional compliance information is passed to VMware Identity Manager. If the device is no longer in compliance, the user loses access to the applications provided by VMware Identity Manager.</td>
</tr>
</tbody>
</table>
Enterprise Productivity Service

The Enterprise Productivity service builds on the previous service in that it begins with devices that have been enrolled with the VMware Workspace ONE® Intelligent Hub (formerly called the VMware AirWatch Agent) and that are fully managed at deployment. When new devices are brought into the organization, they are essentially quarantined until enrolled.

Devices in this service have the following characteristics.

Table 161: Configuration Considerations for the Enterprise Productivity Service

<table>
<thead>
<tr>
<th>Service Feature</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device enrollment</td>
<td>All devices in the Enterprise Productivity service are required to enroll using the Workspace ONE Intelligent Hub. These devices are likely to have valuable enterprise data on them and so require a higher level of control and security.</td>
</tr>
<tr>
<td>Email restrictions</td>
<td>Native and third-party email apps are blocked, and all users use Workspace ONE Boxer for increased security.</td>
</tr>
<tr>
<td>Content access</td>
<td>VMware Workspace ONE® Content is pushed to the device and configured for secure access to corporate repositories.</td>
</tr>
<tr>
<td>Secure browsing</td>
<td>VMware Workspace ONE® Web is pushed to the device to ensure that links to intranet sites are always opened in a secure browser.</td>
</tr>
<tr>
<td>Email access</td>
<td>Email and content are delivered from Microsoft Office 365, so federation with the Microsoft Office 365 service is enabled to allow SSO to the Office service and native mobile Microsoft Office 365 apps.</td>
</tr>
<tr>
<td>Data loss prevention</td>
<td>DLP components are enabled within Workspace ONE Content and Workspace ONE Boxer to prevent the use of unapproved applications, ensuring that data cannot be inadvertently or purposely copied and pasted into other apps.</td>
</tr>
<tr>
<td>Multi-factor authentication</td>
<td>Multi-factor authentication through Workspace ONE Verify is used when users need to access the Workspace ONE application and they are in a network range that is not within the corporate network. On corporate Wi-Fi, users need only mobile SSO-based authentication. Workspace ONE Verify is also required on personally owned, non-managed PCs that use only the browser to access SaaS apps.</td>
</tr>
</tbody>
</table>
Figure 141: Enterprise Productivity Service Blueprint
**Table 162: Configuration Considerations for Microsoft Office 365 Federation**

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Tasks and Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federation to Microsoft Office 365</td>
<td>• VMware Identity Manager uses the Microsoft Federated Identity approach to authenticate login requests to the Microsoft Office 365 service.</td>
</tr>
<tr>
<td></td>
<td>• For information about this configuration, see the following resources:</td>
</tr>
<tr>
<td></td>
<td>◦ The <a href="#">VMware Identity Manager and Microsoft Azure with Office 365 Integration video</a></td>
</tr>
<tr>
<td></td>
<td>◦ <a href="#">Converting Office 365 to a Federated Domain for Single Sign-On and Changing Office 365 Parameters to Workspace in VMware Identity Manager Integration with Office 365</a></td>
</tr>
<tr>
<td>Enable federation in the Microsoft Office 365 or Microsoft Azure AD portals</td>
<td>• Sync Active Directory user accounts through the Microsoft Azure AD or Microsoft Office 365 portal.</td>
</tr>
<tr>
<td></td>
<td>• Use PowerShell scripting to configure the Microsoft Office 365 service to authenticate through Workspace ONE as a federated identity provider. A set of PowerShell scripts with appropriate parameters and signing certificates establish trust between Microsoft Office 365 and VMware Identity Manager.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> An important criterion to make Microsoft Office 365 integration work is ensuring that the attribute ObjectGUID is synced from AD to the VMware Identity Manager service.</td>
</tr>
<tr>
<td>Configure Microsoft Office 365 apps in VMware Identity Manager</td>
<td>Using the templates in the Cloud Application Catalog, configure the Microsoft Office 365, WS-fed based template to allow authentication against VMware Identity Manager for Microsoft Office 365-based apps and resources, such as email, SharePoint Online, Skype for Business, and other Microsoft Services.</td>
</tr>
</tbody>
</table>
Table 163: Configuration Considerations for Email

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Tasks and Considerations</th>
</tr>
</thead>
</table>
| Email integration with Microsoft Office 365 through PowerShell | Workspace ONE UEM issues commands through PowerShell to Exchange in Microsoft Office 365. Devices communicate directly with Exchange ActiveSync in the Microsoft Office 365 service.  
For full configuration information, see PowerShell Integration with VMware Workspace ONE UEM. |
| PowerShell Roles in Office 365 | PowerShell requires specific roles to be established in the Microsoft Office 365 administration portal for Exchange. These roles enable the execution of PowerShell cmdlets from Workspace ONE UEM to the Microsoft Office 365 service. |
| Blocking and quarantine rules | To prevent unauthorized devices from connecting to the Exchange server, you can block or quarantine devices until they have enrolled. PowerShell commands are used to set the appropriate policy. These rules are not needed for environments where enrollment is not required. |
| Email compliance policies | Compliance policies for email include a range of options for controlling managed and unmanaged devices:  
- Must the device be enrolled to perform email sync?  
- Which email clients are allowed to sync email?  
- Is device encryption required for email sync?  
- Are jail-broken or otherwise compromised devices allowed? |
| ActiveSync profiles for email clients | • To enable email sync, you must configure the Exchange ActiveSync payload for the device profiles. The hostname for Microsoft Office 365 is typically outlook.office365.com.  
• The domain, username, and email address are configured with lookup values. Make sure that these values are available in the directory and are properly mapped from AD through the AirWatch Cloud Connector (ACC). |
### Table 164: Configuration Considerations for Content

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Tasks and Considerations</th>
</tr>
</thead>
</table>
| Content integration with Microsoft Office 365 | - Integration is established through the Workspace ONE UEM Console under the Content node.  
- From here, you configure templates for the SharePoint libraries in Microsoft Office 365, to sync to the mobile devices.  
For more information see [Corporate File Servers](#). |
| Office 365 SharePoint document libraries | Use [https://portal.office.com](https://portal.office.com) to log in to Microsoft Office 365 and create SharePoint sites with document libraries containing content. |
| Content templates in Workspace ONE UEM for automatic deployment | To create these templates:  
In the Workspace ONE UEM Console, access the Content node, select **Templates**, and then select **Automatic**.  
- Configure SharePoint Office 365 as the repository type.  
- Configure the **Link** field with the path to the SharePoint document library. For example, [https://<domain>.sharepoint.com/Sales_Material/Shared%20Documents](https://<domain>.sharepoint.com/Sales_Material/Shared%20Documents)  
- Enable **Allow Write** if read/write access is needed.  
- If content is synced, choose **Allow Offline Viewing**.  
- If content is used with other apps, select **Allow Open in Third Party Apps**.  
- Review other security settings per your enterprise policy.  
- Assign appropriate groups to the repository.  
For more information, see [Enable End-User Access to Corporate File Server Content](#). |
| Workspace ONE Content | To ensure access to content, require that Workspace ONE Content be automatically deployed to groups who use SharePoint. |
### Table 165: Configuration Considerations for Data Loss Prevention

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Tasks and Considerations</th>
</tr>
</thead>
</table>
| DLP configuration on a global basis | - You can set DLP configuration on a global basis, platform basis, or per application deployment.  
  - For DLP settings to take effect, the application must be built with the VMware Workspace ONE® Software Development Kit (SDK), or, for an internal application, DLP settings must be supported through app wrapping.  
  - Workspace ONE Boxer, Workspace ONE Content, and Workspace ONE Web are built using the Workspace ONE SDK and honor the settings chosen. |
| SDK profile defaults for iOS or Android | SDK profiles allow global configuration of DLP settings that are applied to applications on the platform for which the profile is defined. Policy settings include enabling or disabling:  
  - Printing  
  - Composing email  
  - Location services  
  - Data backup  
  - Camera  
  - Watermarking  
  - Ability to open documents in certain apps  
  - Copy and paste in and out  
  - Third-party keyboards |
| Custom policies for Workspace ONE Content and Workspace ONE Boxer | Workspace ONE Content can use the default policies defined in the SDK profile, or defaults can be overridden by enabling custom policies. Requiring MDM (mobile device management) enrollment ensures that content is accessed only by enrolled devices. |
| Email compliance policies | When configuring Workspace ONE Content policies, verify that the email compliance policies match corporate standards, including whether devices must be enrolled in device management to receive email. |
### Table 166: Configuration Considerations for Workspace ONE Verify

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Tasks and Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication adapter in VMware Identity Manager</td>
<td>Workspace ONE Verify is an authentication method within VMware Identity Manager. You must enable the built-in authentication adapter by selecting a check box.</td>
</tr>
<tr>
<td>Access policies</td>
<td>To use an authentication method, you add it to a policy. You can configure Workspace ONE Verify as a standalone authentication method in a policy, but it is typically chained with other methods to implement multi-factor authentication. To use Workspace ONE Verify in conjunction with mobile SSO for iOS, click the + icon and add VMware Verify. After authenticating through mobile SSO, users are prompted for Workspace ONE Verify credentials.</td>
</tr>
<tr>
<td>Installation</td>
<td>The Workspace ONE Verify app is available from the Apple App Store, Google Play, and as an add-in for Chrome on Windows and macOS.</td>
</tr>
<tr>
<td>Device enrollment</td>
<td>When users access Workspace ONE Verify for the first time, they are asked for a phone number. The phone number is then associated with the VMware Identity Manager service, and a notification is sent to the user’s device to enroll it. After enrollment, the user’s phone is issued an authentication token. If the phone can receive push notifications, it lets the user choose to allow or reject the authentication.</td>
</tr>
<tr>
<td>Registration of additional devices</td>
<td>You can register additional devices for the end user by leveraging a previously registered device. During registration of an additional device, an authentication request is sent to a previously registered device for verification.</td>
</tr>
</tbody>
</table>
Policy | Tasks and Considerations
---|---
Workspace ONE UEM compliance | - Create a compliance policy for the appropriate platforms through the Workspace ONE UEM Console. Criteria for evaluation can include jailbroken or rooted devices, devices that have not checked in to the Workspace ONE UEM environment in a certain period of time, or the installation of blacklisted applications.
- The policy can include an escalation of notifications as actions, starting with an email notification to the user, followed by an email notification to an administrator, and ultimately blocked access to email if the device is not remediated in time.

VMware Identity Manager compliance | - VMware Identity Manager compliance checking is enabled through policy configuration. Policies include device compliance with the Workspace ONE UEM authentication adapter and other authentication methods, such as a password.
- You can use the policies in conjunction with network ranges, OS platforms, or specific applications, allowing varying requirements to evaluate whether an application can launch based on the location of the user, which device they are using, and how they are authenticating.

**Enterprise Application Workspace Service**

The Enterprise Application Workspace service has a similar configuration to the Enterprise Productivity service, but also includes access to Horizon applications running on Horizon 7 or Horizon Cloud. Horizon resources can be synced with Workspace ONE through an outbound-only connection from the VMware Identity Manager Connector. This method allows entitlements to sync to the service.

Inbound access to the Horizon 7 environment or the Horizon Cloud pod, virtual desktops, and applications is still required. Therefore, Unified Access Gateway is also part of this solution.

Components in the Enterprise Application Workspace service have the following unique characteristics.
### Table 168: Enterprise Application Workspace Service Details

<table>
<thead>
<tr>
<th>Component</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Identity Manager Connector</td>
<td>The connector component of VMware Identity Manager is installed and run as a service on a Windows server (or delivered as a virtual appliance running Linux). The connector integrates with your enterprise directory to sync users and groups to the VMware Identity Manager service and to provide authentication.</td>
</tr>
<tr>
<td>Horizon entitlements</td>
<td>Entitlements are enabled through the VMware Identity Manager catalog by connecting to Horizon 7 pods or Horizon Cloud tenants that expose user-entitled apps and desktops. The Horizon-based services that facilitate these entitlements are described separately, in the following sections of this guide: &quot;Horizon 7 Use Case Service Integration&quot; on page 284 and &quot;Horizon Cloud Use Case Service Integration&quot; on page 302.</td>
</tr>
<tr>
<td>VMware Unified Access Gateway</td>
<td>This component enables external VMware Horizon® Client™ devices to securely access Horizon resources for virtual apps and desktops.</td>
</tr>
</tbody>
</table>

![Figure 142: Enterprise Application Workspace Service Blueprint](image-url)
### Table 169: Configuration Considerations for VMware Identity Manager

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Tasks and Considerations</th>
</tr>
</thead>
</table>
| VMware Identity Manager Connector deployment | - The connector can be deployed either on-premises or in any data center that has a line of sight to Active Directory domain controllers. Instructions for deploying the connector are given in Installing and Configuring VMware Identity Manager Connector.

- The connector can support Horizon entitlement sync when configured as an outbound-only connector, which does not require inbound ports opened at the network perimeter beyond the ports required to access virtual desktop and application resources. Instructions for enabling the outbound-only authentication adapters are in Using Built-In Identity Providers.

- This authentication method, when enabled, is referred to as Password (cloud deployment). See Using Outbound Connector for Authentication in Built-in Identity Providers. |
| Directory sync | After the connector is deployed, directory synchronization is performed to sync Active Directory users and groups with the VMware Identity Manager service. For more information, see Integrating Your Enterprise Directory with VMware Identity Manager. |
| Access to Horizon 7 desktops and applications in the Workspace ONE app catalog | To make Horizon 7 resources available in the Workspace ONE app, you create one or more virtual apps collections in the VMware Identity Manager administration console. The collections contain the configuration information for the Horizon 7 pods, as well as sync settings.

See Providing Access to View, Horizon 6, or Horizon 7 Desktop and Application Pools and Using SAML Authentication for VMware Identity Manager Integration.

User entitlements for apps and desktops are made available through the Horizon 7 configuration and automatically appear in the Workspace ONE app and in a web browser. |
| Access to Horizon 7 from external devices | - To access the resources made available through Horizon 7, you must establish a means of access from Internet-based devices.

- You can configure Unified Access Gateway and optionally True SSO to allow egress and provide connectivity to the Horizon 7 pods. |

See Deployment with Horizon and Horizon Cloud with On-Premises Infrastructure in the Unified Access Gateway documentation. |
To make Horizon Cloud resources available in the Workspace ONE app, you create one or more virtual apps collections in the VMware Identity Manager administration console. The collections contain the configuration information for the Horizon Cloud tenants, as well as sync settings.

See Integrate a Horizon Cloud Node with a VMware Identity Manager Environment and Providing Access to VMware Horizon Cloud Service Desktops and Applications.

User entitlements for apps and desktops are made available through the Horizon Cloud configuration and automatically appear in the Workspace ONE app and in a web browser.

To access the resources made available through Horizon Cloud, you must establish a means of access from Internet-based devices.

- You can configure Unified Access Gateway along with True SSO to allow egress and provide connectivity to the Horizon Cloud pods.
- Unified Access Gateway appliances can be automatically deployed in external or internal configurations.

See Add a Unified Access Gateway Configuration to a Node, With or Without Two-Factor Authentication.

When Horizon resources are used in Workspace ONE, the resources appear on the Launcher page of the app, but the resources launch using the Horizon Client native mobile app.

The following table details the parts required for each Horizon 7–based service. The rest of this section details the design and build of each of these services.
<table>
<thead>
<tr>
<th>Component</th>
<th>Published App Service</th>
<th>GPU-Accelerated App Service</th>
<th>Desktop Service</th>
<th>Desktop with User-Installed App Service</th>
<th>GPU-Accelerated Desktop Service</th>
<th>Linux Desktop Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10 instant clone</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RDSH instant clone</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux instant clone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VMware App Volumes™ AppStack</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>App Volumes writable volume</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VMware User Environment Manager™</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Smart Policies</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Application blocking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Folder redirection</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mandatory profile</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>GPO</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Virtual printing</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>ThinApp Packages</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SaaS apps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Unified Access Gateway</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>True SSO</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vGPU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VMware NSX® Firewall</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Optional</td>
</tr>
</tbody>
</table>

Table 171: Components Required by Horizon 7 Services
Multiple Horizon 7 services can use the same underlying desktop pool type (core service). When there is no variation in the hardware specifications of the desktop, you can reuse the same pool to address multiple use cases. App Volumes and User Environment Manager can provide the customization to the use case.

**Horizon 7 Published Application Service**

This service is created for static task workers, who require a small number of Windows applications.

**Core Service**

The core service consists of RDSH-published applications that can optionally be made available to end users through the Workspace ONE app catalog.

---

**Table 172: Configuration Considerations for RDSH-Published Applications**

<table>
<thead>
<tr>
<th>RDSH Instant Clone</th>
<th>Configuration Considerations</th>
</tr>
</thead>
</table>
| Automated RDSH farm | - Create a Horizon RDSH automated farm using the prepared master VM. See Creating Farms.  
- For details on the specific settings to use, see the VMware Horizon 7 Installation and Configuration section in "Appendix B: VMware Horizon Configuration" on page 344 |

**Applications**

The applications available from the RDSH server farm can be either of the following:
- Applications that are installed in the master VM image.
- Applications that are part of App Volumes AppStacks, which are attached to the RDSH server at system startup.

We assign the AppStack containing the core applications, and each RDSH instant-clone server has the same application set for publishing.

Placing the applications in AppStacks allows for the separation of the application from the Windows operating system. This strategy can offer operational efficiencies, such as updating applications without having to update the master VM image and the RDSH server farm. It also allows the master VM image to be reused for different farms that might use different applications.

![Diagram](Figure 144: Horizon 7 Published Application Service – Applications)
**Overview**

Create AppStacks as required to address the use cases.

With RDSH instant clones, App Volumes saves us from needing to install the same applications on each node. We assign the AppStack containing the core applications so that each RDSH instant-clone server has the same application set for publishing.

**Provisioning machine**

Because the AppStacks are created for an RDSH server, each AppStack must be captured on the same operating system (we used Windows Server 2016) to ensure that applications are compatible with the OS that they are being attached to.

**Core applications**

- Create an AppStack to contain all core applications to be delivered as RDSH-published applications. Follow the instructions in [Working with AppStacks](#) for details.

- These AppStack-delivered applications are published through RDSH.

- Assign and entitle the AppStacks to an Active Directory OU containing the RDSH server machine accounts—these are machine-based assignments.

  **Note:** OU-based assignments are not required, but ensure that AppStacks are available as soon as new hosts in an RDSH farm are provisioned.

**Application pool**

- Use the Horizon Administrator console to add an application pool and publish the desired applications. See [Creating Application Pools](#).

- Entitle the relevant user groups to the matching published applications.

---

**Profile and User Data**

With User Environment Manager, a combination of the mandatory profile, Windows and application environment settings, user preference settings, and folder redirection work together to create and
maintain the user profile.

![Diagram of user profile components]

**Figure 145**: Horizon 7 Published Application Service – Profile and User Data

For detailed instructions for all of the tasks mentioned in the following table, see the [VMware User Environment Manager Administration Guide](#).

**Table 174**: Configuration Considerations for User Profiles in the Business Process Application Service

<table>
<thead>
<tr>
<th>Profiles</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory profile</td>
<td>Set up a mandatory profile, and use a group policy to assign it to the OU that contains the desktop objects. See the <em>Horizon Group Policies</em> section in “Appendix B: VMware Horizon Configuration” on page 344.</td>
</tr>
<tr>
<td>Environment settings</td>
<td>- Map the H: drive to the users’ home drive with User Environment Manager.</td>
</tr>
<tr>
<td></td>
<td>- Map location-based printers with User Environment Manager, according to the IP address range.</td>
</tr>
<tr>
<td>Personalization – applications</td>
<td>- Verify that User Environment Manager Flex configuration files are created and configured properly for each application that allows users to save preference settings.</td>
</tr>
<tr>
<td></td>
<td>- Verify that each application that persists user settings across sessions has a User Environment Manager Flex configuration file.</td>
</tr>
<tr>
<td></td>
<td>- If a User Environment Manager Flex configuration file does not exist, use the Application Profiler to create one and place it in the configuration share. See <em>Introduction to User Environment Manager Application Profiler</em> to get started, and <em>Profiling Applications: VMware User Environment Manager Operational Tutorial</em> for advanced profiling guidance.</td>
</tr>
</tbody>
</table>

VMware Workspace ONE and VMware Horizon Reference Architecture - 289
Table 174: Configuration Considerations for User Profiles in the Business Process Application Service (Continued)

<table>
<thead>
<tr>
<th>Profiles</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder redirection</td>
<td>Folder redirection is configured from User Environment Manager, which redirects user profile folders to a file share so that user data persists across sessions. See the Horizon Group Policies section in &quot;Appendix B: VMware Horizon Configuration&quot; on page 344.</td>
</tr>
<tr>
<td>Smart Policies</td>
<td>Leverage Horizon Smart Policies to apply the Internal Horizon Smart Policy profile, which allows USB, copy and paste, client-drive redirection, and printing. See the Horizon Group Policies section in &quot;Appendix B: VMware Horizon Configuration&quot; on page 344.</td>
</tr>
</tbody>
</table>

**Horizon 7 GPU-Accelerated Application Service**

This service is similar to the Horizon 7 Published Application service but has more CPU and memory and can use hardware-accelerated rendering with NVIDIA GRID graphics cards installed in the VMware vSphere® servers (vGPU).

**Core Service**

The core service consists of RDSH-published applications and is constructed similarly to the core. When creating the master VM, you must prepare the VM for NVIDIA GRID vGPU capabilities.

See Deploying Hardware-Accelerated Graphics with VMware Horizon 7 for installation, configuration and setup instruction. The high-level steps are given in Configuring 3D Graphics for RDS Hosts.

![Core Service Diagram](image)

**Figure 146:** Horizon 7 GPU-Accelerated Application Service – Core

To understand the GPU profile choices, see the NVIDIA vGPU Deployment Guide for VMware Horizon 7.x on VMware vSphere 6.7 and the VMware Compatibility Guide.

You should also configure DRS and affinity rules to ensure that these RDSH VMs always remain on hosts that have NVIDIA cards, if the whole vSphere cluster is not vGPU enabled.
Table 175: Configuration Considerations for GPU-Accelerated Applications

<table>
<thead>
<tr>
<th>RDSH Instant Clone</th>
<th>Configuration Considerations</th>
</tr>
</thead>
</table>
| Windows Server 2016 master VM |  - Build a Windows 2016 VM using the guidelines in *Creating an Optimized Windows Image for a VMware Horizon Virtual Desktop*.  
- Prepare the master VM to use NVIDIA GRID vGPU.  
See *Configuring 3D Graphics for RDS Hosts* and the *NVIDIA vGPU Deployment Guide for VMware Horizon 7.x on VMWARE 7.x vSphere 6.7*. |
| Automated RDSH farm |  - Create a Horizon RDSH automated farm using the prepared master VM. See *Creating Farms*.  
- At farm creation, chose NVIDIA GRID vGPU as the 3D Renderer option. The clones will use the same graphics profile that was selected during master VM creation.  
- For details on the specific settings to use, see the *RDS Farm Settings* section in "Appendix B: VMware Horizon Configuration" on page 344. |

Applications

This service uses the same application types as the "Horizon 7 Published Application Service" on page 286. The actual applications available from the RDSH farm can either be applications installed in the master VM image or as part of App Volumes AppStacks. After the applications are installed or attached, create the application pools and entitle users or groups.

![Horizon 7 GPU-Accelerated Desktop Service – Applications](image)

*Figure 147: Horizon 7 GPU-Accelerated Desktop Service – Applications*
Applications | Configuration Considerations
--- | ---
Application pool | - Use the Horizon Administrator console to add an application pool and publish the desired applications. See Creating Application Pools.
- Entitle the relevant user groups to the matching published applications.

**Profile and User Data**

This service uses the same structure and design for profile and user data as was outlined previously in "Horizon 7 Published Application Service" on page 286.

**Horizon 7 Desktop Service**

This service is created for mobile knowledge workers and contractors, who require a large number of core and departmental applications, require access from many external locations, and might need access to USB devices.

**Core Service**

The core service consists of a Windows 10 virtual desktop made available to end users through the Workspace ONE app catalog.

![Core Service Diagram]

**Figure 148**: Horizon 7 Desktop Service – Core

When creating an automated, instant-clone desktop pool, you can choose between floating and dedicated user assignment.

- Floating instant-clone desktop pools.
  - Users are assigned random desktops from the pool. When a user logs out, the desktop VM is deleted.
  - New clones are created according to the provisioning policy, which can be on-demand or up-front.
• Dedicated instant-clone desktop pools.
  ▪ Users are assigned a particular remote desktop, and they return to the same desktop at each login.
  ▪ When a user logs out, a resync operation on the master image retains the name and MAC address of the VM.
  ▪ Dedicated desktops are useful when you must retain the identity of the desktop. For example, some software uses the MAC address to track license activation.
  ▪ Because each user is assigned a dedicated desktop, which no other user is allowed to use, the pool size reflects the total number of users. This can lead to more desktops being required for a dedicated pool than for a floating pool, which means an increase in the resources consumed.

Table 177: Configuration Considerations for Windows 10 Instant-Clone Desktops

<table>
<thead>
<tr>
<th>Windows 10 Instant Clone</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10 master VM</td>
<td>Build a Windows 10 VM using the guidelines in Creating an Optimized Windows Image for a VMware Horizon Virtual Desktop.</td>
</tr>
</tbody>
</table>
| Automated desktop pool  | • Create a Horizon 7 automated instant-clone desktop pool using the prepared master VM. See Create an Instant-Clone Desktop Pool.  
  • Use the specific pool settings from "Appendix B: VMware Horizon Configuration" on page 344.  
  • Entitle users by adding the appropriate AD group or groups. |

Applications

The actual applications available on the desktops can either be applications installed in the master VM image or as part of App Volumes AppStacks. The use of App Volumes allows the master image to be reused in more use cases and gives operational advantages. With App Volumes the majority of applications are delivered with core and different departmental AppStacks. Individual or conflicting
applications are packaged with ThinApp and available through the Workspace ONE app catalog.

![Figure 149: Horizon 7 Desktop Service – Applications](image)

**Table 178: Configuration Considerations for AppStacks in the Horizon 7 Desktop Service**

<table>
<thead>
<tr>
<th>App Volumes</th>
<th>Configuration Considerations</th>
</tr>
</thead>
</table>
| Core applications            | • Create an AppStack to contain all core applications. See the instructions in *Working with AppStacks* for details.  
                                | • Assign and entitle the AppStack to an AD 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 uses the same structure and design for profile and user data as outlined in *"Horizon 7 Published Application Service"* on page 286.
Policy | Configuration Considerations
--- | ---
Smart Policies | - Mobile knowledge worker:
  - Internal location: Apply an internal Horizon Smart Policy.
  - External location: Apply an external Horizon Smart Policy.
- Contractors: Apply the restrictive zContractor Horizon Smart Policy at all times.
  **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.
- For examples, see the section *User Environment Manager Smart Policies* in "Appendix B: VMware Horizon Configuration" on page 344.

Application blocking | Leverage application blocking in User Environment Manager to block the following executables:
  - Cmd.exe

Group policies | No specific group policies.

---

**Table 179: Configuration Considerations for User Profiles in the Horizon 7 Desktop Service**

---

**Horizon 7 Desktop with User-Installed Applications Service**

The Horizon 7 Desktop with User-Installed Applications service uses a similar integration as the "Horizon 7 Desktop Service" on page 292, with the addition of an App Volumes writable volume.

**Core Service**

The core service consists of a Windows 10 virtual desktop and is constructed similarly to the "Horizon 7 Desktop Service" on page 292.

**Applications**

This service uses similar application types as the "Horizon 7 Desktop Service" on page 292. The actual applications available on the desktops can either be applications installed in the master VM image or as part of App Volumes AppStacks.

For user-installed applications, the user gets an App Volumes writable volume, which helps provide a persistent experience for the user. Individual or conflicting applications are packaged with ThinApp.
Figure 150: Horizon 7 Desktop with User-Installed Applications Service – Applications

Table 180: Configuration Considerations for AppStacks and Writable Volumes in the Horizon 7 Desktop with User-Installed Applications Service

<table>
<thead>
<tr>
<th>App Volumes</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core applications</td>
<td>• Create an AppStack to contain all core applications. See the instructions in Working with AppStacks for details.</td>
</tr>
<tr>
<td></td>
<td>• Assign and entitle the AppStack to an AD group.</td>
</tr>
<tr>
<td>Departmental applications</td>
<td>• Create an AppStack for each department containing unique applications for that department.</td>
</tr>
<tr>
<td></td>
<td>• Assign and entitle relevant user groups to their matching departmental AppStack.</td>
</tr>
<tr>
<td>Writable volumes</td>
<td>• Create writable volumes for each user (or for the user group) entitled to this desktop pool.</td>
</tr>
<tr>
<td></td>
<td>• See Working with Writable Volumes.</td>
</tr>
<tr>
<td></td>
<td>• We used the User-Installed Applications (UIA) template to create the writable volumes. This writable volume type can capture any user-installed application and persist the application across user sessions.</td>
</tr>
<tr>
<td></td>
<td>• See Configuring Storage for AppStacks and Writable Volumes for more information about writable volume template options.</td>
</tr>
</tbody>
</table>
Profile and User Data

This service uses the same structure and design for profile and user data as outlined in "Horizon 7 Desktop Service" on page 292.

Table 181: Configuration Considerations for User Profiles in the Horizon 7 Desktop with User-Installed Applications Service

<table>
<thead>
<tr>
<th>Policy</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Policies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software developer:</td>
</tr>
<tr>
<td></td>
<td>- Internal location: Apply an internal Horizon Smart Policy.</td>
</tr>
<tr>
<td></td>
<td>- External location: Apply an external Horizon Smart Policy.</td>
</tr>
<tr>
<td></td>
<td>IT (power user):</td>
</tr>
<tr>
<td></td>
<td>- Internal location: Apply an internal Horizon Smart Policy.</td>
</tr>
<tr>
<td></td>
<td>- External location: Apply an external Horizon Smart Policy.</td>
</tr>
<tr>
<td></td>
<td>See the section User Environment Manager Smart Policies in &quot;Appendix B: VMware Horizon Configuration&quot; on page 344.</td>
</tr>
<tr>
<td>Application</td>
<td>No application blocking settings</td>
</tr>
<tr>
<td>blocking</td>
<td></td>
</tr>
<tr>
<td>Group policies</td>
<td>No specific group policies.</td>
</tr>
</tbody>
</table>

Horizon 7 GPU-Accelerated Desktop Service

This service is similar to that described in "Horizon 7 Desktop Service" on page 292 but has more CPU and memory and can use hardware-accelerated rendering with NVIDIA GRID graphics cards installed in the vSphere servers (vGPU).

Core Service

The core is constructed using Horizon 7 instant clones similar to that described in "Horizon 7 Desktop Service" on page 292. When creating the master VM, you must prepare the VM for NVIDIA GRID vGPU capabilities.

See Deploying Hardware-Accelerated Graphics with VMware Horizon 7 for installation, configuration and setup instruction. The high-level steps are given in Preparing for NVIDIA GRID vGPU Capabilities.
To understand the graphic profile choices, see the NVIDIA vGPU Deployment Guide for VMware Horizon 7.x on VMware vSphere 6.7 and the VMware Compatibility Guide.

You should also configure DRS and affinity rules to ensure that these desktops always remain on hosts that have NVIDIA cards if the whole vSphere cluster is not vGPU-enabled.

### Table 182: Configuration Considerations for the Windows 10 VM in the Horizon 7 GPU-Accelerated Desktop Service

<table>
<thead>
<tr>
<th>Windows 10 Instant Clone</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10 master VM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Build a Windows 10 VM using the guidelines in Creating an Optimized Windows Image for a VMware Horizon Virtual Desktop.</td>
</tr>
<tr>
<td></td>
<td>● Prepare the master VM to use NVIDIA GRID vGPU. See Preparing for NVIDIA GRID vGPU Capabilities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Automated desktop pool</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● Create a Horizon 7 automated instant-clone desktop pool using the prepared master VM. See Create an Instant-Clone Desktop Pool.</td>
</tr>
<tr>
<td></td>
<td>● At pool creation, chose NVIDIA GRID vGPU as the 3D Renderer option. The clones will use the same graphics profile that was selected during master VM creation.</td>
</tr>
<tr>
<td></td>
<td>● Use the specific pool settings from the Desktop Pool Settings section in &quot;Appendix B: VMware Horizon Configuration&quot; on page 344.</td>
</tr>
<tr>
<td></td>
<td>● Entitle users by adding the appropriate AD group or groups.</td>
</tr>
</tbody>
</table>
Applications

This service uses similar application types as those described in “Horizon 7 Desktop with User-Installed Applications Service” on page 295. The actual applications available on the desktops can either be applications installed in the master VM image or as part of App Volumes AppStacks.

For user-installed applications, the user gets an App Volumes writable volume, which helps provide a persistent experience for the user. Individual or conflicting applications are packaged with ThinApp.

Profile and User Data

This service uses the same structure and design for profile and user data as was outlined previously in "Horizon 7 Desktop Service" on page 292.
Table 183: Configuration Considerations for User Profiles in the High-Performance Workspace Service

<table>
<thead>
<tr>
<th>Policy</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Policies</td>
<td>Multimedia Designer:</td>
</tr>
<tr>
<td></td>
<td>- Internal location: Apply an internal Horizon Smart Policy.</td>
</tr>
<tr>
<td></td>
<td>- External location: Apply external Horizon Smart Policy.</td>
</tr>
<tr>
<td></td>
<td>For examples, see the section User Environment Manager Smart Policies in &quot;Appendix B: VMware Horizon Configuration&quot; on page 344.</td>
</tr>
<tr>
<td>Application blocking</td>
<td>No application blocking settings.</td>
</tr>
<tr>
<td>Group policies</td>
<td>No specific group policies.</td>
</tr>
</tbody>
</table>

**Horizon 7 Linux Service**

VMware 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 desktop is a full clone of a Linux VM that already has applications installed. Applications can be preinstalled in the master VM, and users can add their own applications to their individual clones. Desktops are persistent to the user.

Figure 153: Horizon 7 Linux Desktop Service – Core and Apps
**Table 184**: Configuration Considerations for the VM in the Horizon 7 Linux Desktop Service

<table>
<thead>
<tr>
<th>Linux Clone</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux master VM</td>
<td>Follow the instructions in <em>Preparing a Linux Virtual Machine for Desktop Deployment</em>.</td>
</tr>
<tr>
<td>Install applications</td>
<td>Install all required applications on the master VM.</td>
</tr>
<tr>
<td>Domain join</td>
<td>Follow the instructions in <em>Setting Up Active Directory Integration for Linux Desktops</em>.</td>
</tr>
<tr>
<td>3D rendering (optional)</td>
<td>Follow the instructions in <em>Setting Up Graphics for Linux Desktops</em>.</td>
</tr>
<tr>
<td>Horizon Agent</td>
<td>Follow the instructions in <em>Installing Horizon Agent</em>.</td>
</tr>
<tr>
<td>Configuration options (optional)</td>
<td>Follow the instructions in <em>Setting Options in Configuration Files on a Linux Desktop</em>.</td>
</tr>
<tr>
<td>Manual pool configuration (optional)</td>
<td>If you are setting up manual pools of Linux desktops review the tasks and options in <em>Bulk Deployment of Horizon 7 for Manual Desktop Pools</em>.</td>
</tr>
<tr>
<td>Desktop pool</td>
<td>Follow the instructions in <em>Create and Manage Linux Desktop Pools</em> to create the desired type of desktop pool.</td>
</tr>
<tr>
<td>Linux master VM</td>
<td>Follow the instructions in <em>Preparing a Linux Virtual Machine for Desktop Deployment</em>.</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*.

![Figure 154: Horizon 7 Linux Desktop Service – User Data](image)
Horizon Cloud Use Case Service Integration

The following table details the parts required for each Horizon Cloud–based service. The rest of this section details the design and build of each of these services.

Table 185: Components Required by Horizon Cloud Services

<table>
<thead>
<tr>
<th>Published Application Service</th>
<th>GPU-Accelerated Application Service</th>
<th>Secure Desktop Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10 clone</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>RDSH clone</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VMware User Environment Manager</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Smart Policies</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Application blocking</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Folder redirection</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mandatory profile</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>GPO</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Virtual printing (ThinPrint)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>ThinApp Packages</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Unified Access Gateway</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>True SSO</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>GPU</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Horizon Cloud Published Application Service

This service is created for the static task worker use case identified earlier. Static task workers require a small number of Windows applications.

**Core Service**

The core service consists of RDSH-published applications that are made available to end users through the Workspace ONE app catalog.
Table 186: Configuration Considerations for the Core of the Horizon Cloud Published Application Service

<table>
<thead>
<tr>
<th>RDSH Server Clone</th>
<th>Configuration Considerations</th>
</tr>
</thead>
</table>
| Windows Server master VM | • Build a Windows Server VM. See the latest VMware Horizon Cloud Service on Microsoft Azure Release Notes for a list of supported operating systems.  
• You can build the master VM automatically, by using an import process from the Azure Marketplace, or you can build the VM manually.  
• For details on creating and customizing a master VM, as well as publishing an image, see Creating Desktop Images for a Horizon Cloud Node in Microsoft Azure. |
| Automated RDSH farm | • Create a Horizon Cloud automated RDSH server farm using the published image.  
• For details, see Farms in Horizon Cloud. |

Applications

The actual applications available from the RDSH server farm should be installed in the master VM image, along with any other customization or optimization settings. Optionally, applications can be streamed using ThinApp. Install applications on the master VM, and then publish an image from the master VM. Each RDSH server clone in the farm inherits the same set of applications from the published image, which can then be published to end users.
After the farm of RDSH servers is created, you add applications from the farm to the Horizon Cloud inventory. After the applications are in the inventory, remote application assignments can be created to entitle end users to the applications.

Adding and assigning applications

From the Horizon Cloud Inventory tab, add new applications. You can import applications automatically, by performing an auto-scan from farm operation, or you can add them manually.

After applications are added to the Horizon Cloud inventory, create application assignments to entitle users and groups to the applications.

See Applications in Your Horizon Cloud Inventory.

**Profile and User Data**

With User Environment Manager, a combination of the mandatory profile, Windows and application environment settings, user preference settings, and folder redirection all work together to create and maintain the user profile.
### Table 188: Configuration Considerations for User Profiles in the Horizon Cloud Published Application Service

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Tasks and Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory profile</td>
<td>• Set up a mandatory profile, and use a group policy to assign it to the OU that contains the computer objects.</td>
</tr>
<tr>
<td></td>
<td>• Follow the process outlined in Creating an Optimized Windows Image for a VMware Horizon Virtual Desktop to create a mandatory profile.</td>
</tr>
<tr>
<td></td>
<td>• Restrictions in the Microsoft Azure interface interfere with the creation of a mandatory profile on an Azure VM. One option is to complete the process on an on-premises Windows server, and copy the mandatory profile to Azure.</td>
</tr>
<tr>
<td></td>
<td>• It is important to use the same Windows build and profile version when building the mandatory profile as will be deployed in Horizon Cloud on Microsoft Azure.</td>
</tr>
<tr>
<td></td>
<td>See the latest <a href="#">VMware Horizon Cloud Service on Microsoft Azure Release Notes</a> for a list of supported guest operating system versions.</td>
</tr>
<tr>
<td></td>
<td>For a list of associated profile versions, see <a href="#">Create Mandatory User Profiles</a> in the Microsoft documentation.</td>
</tr>
<tr>
<td>Environment settings</td>
<td>• Map the H: drive to the user’s home drive with User Environment Manager.</td>
</tr>
<tr>
<td></td>
<td>• Map location-based printers with User Environment Manager, according to the IP address range.</td>
</tr>
<tr>
<td>Personalization – applications</td>
<td>• Verify that User Environment Manager Flex configuration files are created and configured properly for each application that allows users to save preference settings.</td>
</tr>
<tr>
<td></td>
<td>• Verify that each application that persists user settings across sessions has a User Environment Manager Flex configuration file.</td>
</tr>
<tr>
<td></td>
<td>• If a User Environment Manager Flex configuration file does not exist, download a configuration file template from the VMware Marketplace, or use the Application Profiler to create one and place it in the configuration share.</td>
</tr>
<tr>
<td>Folder redirection</td>
<td>Folder redirection is configured from User Environment Manager, which redirects user profile folders to a file share so that user data persists across sessions.</td>
</tr>
</tbody>
</table>
Table 188: Configuration Considerations for User Profiles in the Horizon Cloud Published Application Service (Continued)

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Tasks and Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>See Configure Folder Redirection.</td>
</tr>
<tr>
<td>Smart Policies</td>
<td>Leverage Horizon Smart Policies to apply the Internal Horizon Smart Policy profile, which allows USB, copy and paste, client-drive redirection, and printing.</td>
</tr>
<tr>
<td></td>
<td>See Using Smart Policies.</td>
</tr>
<tr>
<td></td>
<td>For policy examples, see the section User Environment Manager Smart Policies in &quot;Appendix B: VMware Horizon Configuration&quot; on page 344.</td>
</tr>
</tbody>
</table>

**Horizon Cloud GPU-Accelerated Application Service**

This service is similar to the Horizon Cloud Published Application service but uses hardware-accelerated rendering with NVIDIA GRID graphics cards available through Microsoft Azure.

**Core Service**

The core is constructed using Horizon Cloud RDSH server farms. A master VM is created, configured, and published as an image. The published image is used to create a farm of RDSH servers. Because we are using folder redirection, there should be little data stored on the hosts in the farm.

![Horizon RDS Farm](image)

When creating the master VM, you must prepare the VM for NVIDIA GRID GPU capabilities. Follow the steps in Install NVIDIA Graphics Drivers in a GPU-Enabled Master Image.

When importing a VM into Horizon Cloud, select an OS that supports an NVIDIA GPU, and enable the Include GPU option. This ensures that a GPU-backed VM type will be imported from the Azure Marketplace.
Table 189: Configuration Considerations for the Horizon Cloud GPU-Accelerated Application Service

<table>
<thead>
<tr>
<th>RDSH Server Clone</th>
<th>Tasks and Considerations</th>
</tr>
</thead>
</table>
| Windows Server 2016 master VM | • Build a Windows Server 2016 VM. See the latest VMware Horizon Cloud Service on Microsoft Azure Release Notes for a list of supported operating systems.  
  **Note**: Windows Server 2012 R2 limits the maximum number of sessions and is not recommended.  
  • You can build the master VM automatically, by using an import process from the Azure Marketplace, or you can build the VM manually.  
  • For details on creating and customizing a master VM, as well as publishing an image, see Creating Desktop Images for a Horizon Cloud Node in Microsoft Azure. |
| GPU enable master VM       | • If you create a master image VM with a GPU, you must log in to the VM’s Windows operating system and install the supported NVIDIA graphics drivers to get the GPU capabilities of that VM. You install the drivers after the VM is created and after the Imported VMs page shows the agent-related status as active.  
  • See Install NVIDIA Graphics Drivers in a GPU-Enabled Master Image for details on creating and customizing a master VM with NVIDIA GPU. |
| Automated desktop pool     | • Create a Horizon Cloud automated RDSH server farm using the published image.  
  • For details, see Farms in Horizon Cloud. |

**Applications**

This service uses the same structure and design for applications as was outlined previously in "Horizon Cloud Published Application Service" on page 302.

**Profile and User Data**

This service uses the same structure and design for profile and user data as was outlined previously in "Horizon Cloud Published Application Service" on page 302.
Table 190: Configuration Considerations for User Profiles in the Horizon Cloud GPU-Accelerated Application Service

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Tasks and Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Policies</td>
<td>For the multimedia designer use case:</td>
</tr>
<tr>
<td></td>
<td>• Internal location: Apply an internal Horizon Smart Policy.</td>
</tr>
<tr>
<td></td>
<td>• External location: Apply an external Horizon Smart Policy.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Using Smart Policies.</td>
</tr>
<tr>
<td>Application blocking</td>
<td>Do not use application-blocking settings.</td>
</tr>
</tbody>
</table>

**Horizon Cloud Desktop Service**

This service is created for the mobile knowledge workers and contractors use cases, who require a large number of core and departmental applications, require access from many external locations, and might need access to USB devices.

**Core Service**

The core service consists of a Windows 10 virtual desktop, which can optionally be made available to end users through the Workspace ONE app catalog.
**Table 191: Configuration Considerations for Windows 10 Desktops**

<table>
<thead>
<tr>
<th>Windows 10 Clone</th>
<th>Tasks and Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10 master VM</td>
<td></td>
</tr>
</tbody>
</table>
- Build a Windows desktop VM. See the latest VMware Horizon Cloud Service on Microsoft Azure Release Notes for a list of supported operating systems.
- You can build the master VM automatically, by using an import process from the Azure Marketplace, or you can build the VM manually.
- For details on creating and customizing a master VM, as well as publishing an image, see Creating Desktop Images for a Horizon Cloud Node in Microsoft Azure.
- Whether you create the VM automatically or manually, consider optimizing Windows to provide the best user experience. See Creating an Optimized Windows Image for a VMware Horizon Virtual Desktop. |
| Desktop assignment | Create a Horizon Cloud desktop assignment from the published image. See Creating Desktop Assignments in Horizon Cloud. |

**Applications**

The majority of applications should be installed in the master VM image, along with any other customization or optimization settings. Optionally, conflicting applications are packaged with ThinApp and made available through the Workspace ONE app catalog. We install applications on the master VM, and then publish an image from the master VM. A new dedicated or floating desktop assignment is created and entitled to groups or individual users. Each Windows 10 VM created as part of the desktop assignment inherits the applications, customizations, and optimization settings from the referenced published image.
Profile and User Data

This service uses the same structure and design for profile and user data as outlined in "Horizon Cloud Published Application Service" on page 302.

Table 192: Configuration Considerations for User Profiles in the Horizon Cloud Desktop Service

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Tasks and Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Policies</td>
<td>For the mobile knowledge worker use case:</td>
</tr>
<tr>
<td></td>
<td>1. Internal location: Apply an internal Horizon Smart Policy.</td>
</tr>
<tr>
<td></td>
<td>2. External location: Apply an external Horizon Smart Policy.</td>
</tr>
<tr>
<td></td>
<td>For the contractor use case: Apply the restrictive zContractor Horizon Smart Policy at all times.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Smart Policies are evaluated in alphabetical order. Adding the z character before Contractor places the policy name at the bottom of the sort group. For examples, see the section User Environment Manager Smart Policies in &quot;Appendix B: VMware Horizon Configuration&quot; on page 344.</td>
</tr>
<tr>
<td>Application blocking</td>
<td>Leverage application blocking in User Environment Manager to block executables such as Cmd.exe.</td>
</tr>
</tbody>
</table>

Figure 160: Horizon Cloud Desktop Service – Applications
Recovery Service Integration

With a focus on disaster recovery, consideration must be given to the questions of if and how the user is to consume an equivalent service in the event of a site outage.

At this stage, we have all of the disaster recovery components designed and deployed, and the environment should have all the functionality and qualities that are required to deliver the services defined earlier. The components required can now be created, assembled, and integrated into the recovery services to be mapped against the use case services that are consumed by end users.

Some of these steps might have already been completed while creating the use case services described earlier.

Where services are being consumed as cloud-based services, such as Workspace ONE UEM and VMware Identity Manager, availability is delivered as part of the platform.

Any services that have been deployed on-premises, including Horizon 7, App Volumes, User Environment Manager, VMware Identity Manager, and Workspace ONE UEM, should have been deployed across multiple sites to provide resilience and disaster recovery capabilities.

Some cloud-based services, including Horizon Cloud, might contain user configuration settings and user data, and might be running in a single Azure region. To provide full disaster recovery, a second, equivalent service can be built in a different Azure region.

Horizon 7 Recovery Services

The following table details the components required for each recovery service. Some are optional, as indicated in the Recovery Services section of "Service Definitions" on page 28. The rest of this section details the steps for implementing each of the recovery service types.

Note: This section details the components of a multi-site active/active and active/passive deployment. For component details of a vSAN stretched active/passive service, within a metro or campus network environment with low network latency between sites, see "Appendix F: Horizon 7 Active/Passive Service Using VMware vSAN Stretched Cluster" on page 429.

Table 193: Horizon 7 Recovery Service Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Active/Passive Recovery Service</th>
<th>Active/Active Recovery Service</th>
<th>vSAN Stretched Active/Passive Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace ONE UEM</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VMware Identity Manager</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Windows instant clone</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows linked clone</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RDSH linked clone</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Windows full clone</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>App Volumes AppStack</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>App Volumes writable volume</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 193: Horizon 7 Recovery Service Components (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Active/Passive Recovery Service</th>
<th>Active/Active Recovery Service</th>
<th>vSAN Stretched Active/Passive Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Environment Manager</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Folder redirection</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mandatory profile</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Storage replication (active/active)</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vSAN stretched cluster</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Some parts are prerequisites for any of the services. Ensure that these services are configured and functional before looking at the specifics for a given service:

- User Environment Manager GPO (ADMX) configuration
- DFS namespace (for User Environment Manager profile global access)
- Storage array replication
- Mandatory profile
- SQL Server Always On (for App Volumes and VMware Identity Manager databases)
- Load balancing between sites
- Load balancing within sites

**Horizon 7 Active/Passive Recovery Service**

This section covers the high-level steps required to build out the active/passive service, which can be seen from a blueprint perspective.
Desktops and RDSH-Published Applications

The first step is to create the Windows component of the service. This consists of either desktops or RDSH servers in pools or farms at both sites. Cloud Pod Architecture is then configured to provide a global entitlement to pools of desktops and published applications from both sites.

Table 194: Steps for Creating the Windows Component of a Horizon 7 Active/Passive Service

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load balancing</td>
<td>Verify both global and local load balancing are functional.</td>
</tr>
<tr>
<td>Master VM</td>
<td>Build out a master VM image in Site 1 to meet requirements. Reconfigure the master VM image to Site 2.</td>
</tr>
<tr>
<td>Create pools or farms</td>
<td>For desktops, create identical desktop pools in both sites based on the master VM.</td>
</tr>
<tr>
<td></td>
<td>For RDSH-published applications:</td>
</tr>
<tr>
<td></td>
<td>• Create RDSH server farms in both sites using the master VM image.</td>
</tr>
<tr>
<td></td>
<td>• Add application pools in both sites containing the required applications.</td>
</tr>
<tr>
<td>Cloud Pod Architecture</td>
<td>Set up and initialize Cloud Pod Architecture between the two sites.</td>
</tr>
<tr>
<td></td>
<td>• Create sites and assign the pods to their respective sites.</td>
</tr>
<tr>
<td></td>
<td>• Create global entitlements.</td>
</tr>
<tr>
<td></td>
<td>• Associate pools from both sites.</td>
</tr>
<tr>
<td></td>
<td>See the Cloud Pod Architecture section in &quot;Appendix B: VMware Horizon Configuration&quot; on page 344 for detail.</td>
</tr>
</tbody>
</table>

Profile (User Environment Manager) and User Creation

To manage user settings, user data, and users’ access to applications, set up file shares in Site 1, set up DFS-N so that the file shares are replicated to Site 2, and determine which site is primary for each user so that the profile service can function as shown in the following figure.
**Table 195: Steps for Creating the User Profile Component of an Active/Passive Service**

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>File shares</td>
<td>Create four file shares on the file server in Site 1 and set the relevant permissions.</td>
</tr>
<tr>
<td></td>
<td>- User Environment Manager IT configuration</td>
</tr>
<tr>
<td></td>
<td>- User Environment Manager user settings</td>
</tr>
<tr>
<td></td>
<td>- Mandatory profile (optional)</td>
</tr>
<tr>
<td></td>
<td>- Home file shares for redirected folders (optional)</td>
</tr>
<tr>
<td></td>
<td>Set up DFS-N following the guidance given in &quot;Component Design: User Environment Manager Architecture&quot; on page 197.</td>
</tr>
<tr>
<td>User placement</td>
<td>- Decide where a given named user is initially placed (Site 1 or Site 2).</td>
</tr>
<tr>
<td></td>
<td>- Map a user to a GPO that matches that placement from a User Environment Manager perspective.</td>
</tr>
<tr>
<td></td>
<td>- Verify profile creation and functionality by performing a login with a user.</td>
</tr>
</tbody>
</table>

**App Volumes Active/Passive Design**

To set up this container-style technology that attaches applications to a VM when the user logs in, you must install redundant instances of App Volumes Manager, create AppStacks, which store
applications in shared read-only virtual disks (VMDK files), and, optionally, create writable volumes if users need to install their own applications.

Figure 163: App Volumes Active/Passive Recovery Service Component
### Table 196: Steps for Creating the Streamlined Application Component of an Active/Passive Service

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
</table>
| **App Volumes installation** | 1. Set up two App Volumes Managers in Site 1.  
                             2. Set up two App Volumes Managers in Site 2.  
| **Load balancing**        | 3. Configure local load balancing within each site with a virtual IP (VIP) for the local App Volumes Managers.  
                             4. Point the desktop master images to their respective VIP based on their site. |
| **Storage groups**        | Set up one App Volumes storage group in Site 1 and one storage group in Site 2. For each storage group:  
                             - Configure automatic replication for AppStacks.  
                             - Select all datastores to be used for AppStacks.  
                             - Additionally, select one common datastore to be used to replicate AppStacks between sites. NFS is a good choice for this datastore.  
                             - Mark this common datastore as non-attachable. |
| **AppStacks**             | - Create AppStacks as required to address the use cases. Follow the instructions in Working with AppStacks.  
                             - Place the AppStacks in the local storage group to allow them to replicate to every datastore in the local storage group and also to the other site. |
| **Entitlement replication** | If you are using separate databases for each site, do one of the following:  
                           - Manually reproduce entitlements made at one site to the other sites. Use active directory groups to minimize the administrative overhead.  
                           - Configure PowerShell for replicating application entitlements between the sites, as described in PowerShell Script for Replicating App Volumes Application Entitlements in "Appendix E: App Volumes Configuration" on page 407. |
| **Writable volumes (optional)** | - Create a writable volume for each user who requires one. Follow the instructions in Working with Writable Volumes.  
                             - Place writable volumes on dedicated LUNs, which can later be configured to be protected using storage replication. |
Horizon 7 Active/Active Recovery Service

This section covers the high-level steps required to build out the active/active service, which can be seen from a blueprint perspective in the following figure.

Figure 164: Horizon 7 Active/Active Recovery Service Components

Desktops and RDSH-Published Applications

The first step is to create the Windows component of the service. This consists of either desktops or RDSH servers in pools or farms at both sites. Cloud Pod Architecture is then configured to provide a global entitlement to pools of desktops and published applications from both sites.
Table 197: Steps for Creating the Windows Component of a Horizon 7 Active/Active Recovery Service

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load balancing</td>
<td>Verify both global and local load balancing are functional.</td>
</tr>
<tr>
<td>Master VM</td>
<td>Build out a master VM image in Site 1 to meet requirements.</td>
</tr>
<tr>
<td></td>
<td>Replicate the master VM image to Site 2.</td>
</tr>
<tr>
<td>Create pool or farm</td>
<td>For desktops, create identical desktop pools in both sites based on the</td>
</tr>
<tr>
<td></td>
<td>master VM image.</td>
</tr>
<tr>
<td></td>
<td>For RDSH-published applications:</td>
</tr>
<tr>
<td></td>
<td>- Create RDSH server farms in both sites using the master VM image.</td>
</tr>
<tr>
<td></td>
<td>- Add application pools in both sites containing the required</td>
</tr>
<tr>
<td></td>
<td>applications.</td>
</tr>
<tr>
<td>Cloud Pod Architecture</td>
<td>Set up and initialize Cloud Pod Architecture between the two sites.</td>
</tr>
<tr>
<td></td>
<td>- Create sites and assign the pods to their respective sites.</td>
</tr>
<tr>
<td></td>
<td>- Create global entitlements.</td>
</tr>
<tr>
<td></td>
<td>- Associate pools from both sites.</td>
</tr>
</tbody>
</table>

**Profile (User Environment Manager) and User Creation**

The next step is to set up file shares in Site 1, set up DFS-N so that the file shares are replicated to Site 2, and determine which site is primary for each user so that the profile service can function as shown in the following figure.
Figure 165: Profile Recovery Service Component

### Table 198: Steps for Creating the User Profile Component of an Active/Active Recovery Service

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>File shares</td>
<td>Create four file shares on the file server in Site 1 and set the relevant permissions.</td>
</tr>
<tr>
<td></td>
<td>- User Environment Manager IT configuration</td>
</tr>
<tr>
<td></td>
<td>- User Environment Manager user settings</td>
</tr>
<tr>
<td></td>
<td>- Mandatory profile</td>
</tr>
<tr>
<td></td>
<td>- Home file shares for redirected folders (optional)</td>
</tr>
<tr>
<td></td>
<td>Set up DFS-N following the guidance given in the &quot;Component Design: User Environment Manager Architecture&quot; on page 197 and the Distributed File System section of &quot;Environment Infrastructure Design&quot; on page 221.</td>
</tr>
<tr>
<td>User placement</td>
<td>- Decide where a given named user is initially placed (Site 1 or Site 2).</td>
</tr>
<tr>
<td></td>
<td>- Map a user to a GPO that matches that placement from a User Environment Manager perspective.</td>
</tr>
<tr>
<td></td>
<td>- Verify profile creation and functionality by performing a login with a user.</td>
</tr>
</tbody>
</table>

**App Volumes Active/Active Design**

To set up this container-style technology that attaches applications to a VM when the user logs in, you must install redundant instances of App Volumes Manager, and create AppStacks, which store
applications in shared read-only virtual disks (VMDK files).

Figure 166: App Volumes Active/Active Recovery Service Component
**Table 199**: Steps for Creating the Streamlined Application Component of an Active/Active Recovery Service

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Volumes installation</td>
<td>1. Set up two or more App Volumes Managers in Site 1.  &lt;br&gt;2. Set up two or more App Volumes Managers in Site 2.  &lt;br&gt;See “Component Design: App Volumes Architecture” on page 172 for details.</td>
</tr>
<tr>
<td>Load balancing</td>
<td>1. Configure local load balancing within each site with a virtual IP (VIP) namespace for the local App Volumes Managers.  &lt;br&gt;2. Point the desktop master images to their respective namespace based on their site.</td>
</tr>
<tr>
<td>Storage groups</td>
<td>Set up one App Volumes storage group in Site 1 and one storage group in Site 2.  For each storage group:  &lt;br&gt;• Configure automatic replication for AppStacks.  &lt;br&gt;• Select all datastores to be used for AppStacks.  &lt;br&gt;• Additionally, select one common datastore to be used to replicate AppStacks between sites. NFS is a good choice for this datastore.  &lt;br&gt;• Mark this common datastore as non-attachable.</td>
</tr>
<tr>
<td>AppStacks</td>
<td>1. Create AppStacks as required to address the use cases. Follow the instructions in Working with AppStacks.  &lt;br&gt;2. Place the AppStacks in the local storage group to allow them to replicate to every datastore in the local storage group and also to the other site.</td>
</tr>
<tr>
<td>Entitlement replication</td>
<td>If you are using the separate databases at each site, do one of the following:  &lt;br&gt;• Manually reproduce entitlements made at one site to the other sites.  &lt;br&gt;• Or, configure PowerShell for replicating application entitlements between the sites, as described in the section PowerShell Script for Replicating App Volumes Application Entitlements in &quot;Appendix E: App Volumes Configuration&quot; on page 407.</td>
</tr>
</tbody>
</table>

The following sections detail the components required for a Horizon Cloud Service on Microsoft Azure recovery service and the steps for implementing an active/passive recovery service type. To provide an equivalent service in different Microsoft Azure regions, certain configuration settings and user data might need to be replicated or reproduced between the regions.
- User Environment Manager GPO (ADMX) configuration
  - User Environment Manager configuration data
  - User Environment Manager profile archive data
- Mandatory profile
- Redirected user data (folder redirection, and so on)

To build equivalent entitlements in a second region, a comparable master VM must also be created in that region, using the same process that was used in the first region.

Any design that includes separate locations or regions should also consider the supporting infrastructure, such as AD, DNS, VNET configuration and other components, as detailed in "Environment Infrastructure Design" on page 221.

**Horizon Cloud Active/Passive Recovery Service**

The following figure outlines the components you must implement for an effective recovery service.

![Horizon Cloud Active/Passive Recovery Service Components](image)

**Figure 167**: Horizon Cloud Active/Passive Recovery Service Components

**Desktops and RDSH-Published Applications**

The first step is to create the Windows component of the service. This consists of either desktops or RDSH servers in desktop assignments or server farms, respectively, at both sites. Users are then entitled to resources at the primary site. In the case of a site failure, entitlements can be duplicated at the secondary site.
Table 200: Steps for Creating the Windows Component of an Active/Passive Service

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
</table>
| Create a master VM | - Build a master VM in Site 1 to meet your requirements. Follow the instructions in "Horizon Cloud Use Case Service Integration" on page 302.  
- Build an equivalent master VM image in Site 2. |
| Create desktops assignments or farms | - For desktops, create identical desktop assignments in both sites based on the master VM.  
- For RDSH-published applications:  
  - Create RDSH server farms in both sites using the master VM.  
  - Add application pools in both sites containing the required applications. |

Profile (User Environment Manager) and User Creation

To manage user settings, user data, and users’ access to applications, file replication needs to be set up to ensure that a copy exists outside of the first region. The example here uses Distributed File Shares (DFS), although other file replication technology could also be used.

Table 201: Steps for Creating the User Profile Component of an Active/Passive Service

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
</table>
| File shares | 1. Create the following four file shares on the file server in region 1 and set the relevant permissions:  
  a. User Environment Manager IT configuration  
  b. User Environment Manager profile archive  
  c. Mandatory profile  
  d. Home file shares for redirected folders (optional)  
  2. Set up four equivalent file shares in a separate location, such as region 2.  
  3. Configure DFS replication and namespaces.  
  Refer to the multi-site design section of “Component Design: User Environment Manager Architecture” on page 197 for considerations on setting up DFS-Replication and DFS-Namespace. |
At this stage, we have all of the disaster recovery components designed and deployed, and the environment should have all the functionality and qualities that are required to deliver the services defined earlier. The components required can now be created, assembled, and integrated into the recovery services to be mapped against the use case services that are consumed by end users.

Some of these steps might have already been completed while creating the use case services described earlier.

**On-Premises VMware Workspace ONE UEM Recovery Service**

The Workspace ONE UEM service is responsible for device enrollment, a mobile application catalog, and policy enforcement regarding device compliance. To build this service and to provide site redundancy, you deploy the required components, including device services, console services, and AirWatch Cloud Connectors, in both sites. Global load balancing then directs traffic to the active site.

![VMware Workspace ONE UEM Recovery Service Component](image)

**Figure 168**: VMware Workspace ONE UEM Recovery Service Component

For instructions, see "Appendix D: Workspace ONE UEM Configuration for Multi-site Deployments" on page 392.

**On-Premises VMware Identity Manager Recovery Service**

The VMware Identity Manager service provides a common entry point to all types of applications, regardless of which data center is actively being used. To build this service, you deploy three instances in Site 1, three instances in Site 2, and set up global load balancing.
Figure 169: VMware Identity Manager Recovery Service Component

For instructions, see "Appendix C: VMware Identity Manager Configuration for Multi-site Deployments" on page 371.
Appendix A: VM Specifications

The sections in this appendix list the specifications for the various management servers and connector virtual machines used to validate this reference architecture.

**VMware Workspace ONE UEM**

Several servers are required to take advantage of all features in a VMware Workspace ONE® UEM deployment.

**VMware AirWatch Cloud Connector Server**

Depending on the scale of the environment and the number of devices to be supported, the recommended resources allocated to each VMware AirWatch® Cloud Connector VM can differ.

The AirWatch Cloud Connector synchronizes Workspace ONE with internal resources such as Active Directory or a Certificate Authority and can be used in both cloud-based and on-premises deployments of Workspace ONE UEM.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>VMware Workspace ONE UEM 1811</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>vCPU</td>
<td>2</td>
</tr>
<tr>
<td>vMemory</td>
<td>4 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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:1 Windows OS 50 GB</td>
</tr>
</tbody>
</table>

**Workspace ONE UEM Device Services Server**

This server hosts VMware Workspace ONE® Device Services, which communicate with end-user devices for device enrollment, application provisioning, delivering device commands, receiving device data, and providing the self-service portal.
Device Service servers are required only in an on-premises deployment of Workspace ONE UEM.

### Table 203: VMware Workspace ONE UEM Device Services VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>VMware Workspace ONE UEM 1811</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>vCPU</td>
<td>4</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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:1 Windows OS 50 GB</td>
</tr>
</tbody>
</table>

### Workspace ONE UEM Console Services Server

This server hosts the browser-based Workspace ONE UEM Console that administrators use to secure, configure, monitor, and manage their environment.

Console Service servers are required only in an on-premises deployment of Workspace ONE UEM.

### Table 204: Workspace ONE UEM Console Services VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>VMware Workspace ONE UEM 1811</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>vCPU</td>
<td>4</td>
</tr>
</tbody>
</table>
### Appendix A: VM Specifications

#### VMware Workspace ONE and VMware Horizon Reference Architecture - 328

**Table 204**: Workspace ONE UEM Console Services VM Specifications (Continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:1 Windows OS 50 GB</td>
</tr>
</tbody>
</table>

#### Workspace ONE UEM Memcached Server

Recommended for deployments that include more than 5,000 devices, this cache server stores information from the database to reduce the volume of calls made directly to the database server.

Memcached servers are an optional component in an on-premises deployment of Workspace ONE UEM.

**Table 205**: Workspace ONE UEM Memcached Server VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>VMware Workspace ONE UEM 1811</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>CentOS 7.4-1708</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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:1 Windows OS 50 GB</td>
</tr>
</tbody>
</table>
Workspace ONE UEM AWCM Server

The AirWatch Cloud Messaging (AWCM) server is used by the AirWatch Cloud Connector to communicate with the Workspace ONE UEM console.

AWCM servers are an optional component in an on-premises deployment of Workspace ONE UEM.

Table 206: Workspace ONE UEM AWCM VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>VMware Workspace ONE UEM 1811</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>vCPU</td>
<td>4</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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:1 Windows OS 50 GB</td>
</tr>
</tbody>
</table>

Workspace ONE UEM API Server

This server hosts the REST (Representational State Transfer) and SOAP (Simple Object Access Protocol) APIs that developers can use to integrate their own applications with Workspace ONE UEM.

API servers are an optional component in an on-premises deployment of Workspace ONE UEM.
Table 207: Workspace ONE UEM API Server VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>VMware Workspace ONE UEM 1811</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>vCPU</td>
<td>4</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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:1 50 GB</td>
</tr>
</tbody>
</table>

**SQL Server for Workspace ONE UEM**

This database server stores all device and environment data for Workspace ONE UEM and is required only for an on-premises deployment of Workspace ONE UEM.

Table 208: SQL Server for Workspace ONE UEM VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>SQL Server 2016</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>vCPU</td>
<td>8</td>
</tr>
<tr>
<td>vMemory</td>
<td>64 GB</td>
</tr>
</tbody>
</table>
### VMware Identity Manager

Depending on the scale of the environment and the number of devices to be supported, the recommend resources allocated to each VMware Identity Manager™ and VMware Identity Manager Connector VMs can differ. For this reference architecture, a 50,000-device deployment was considered. See "Component Design: VMware Identity Manager Architecture" on page 96 for guidance on sizing for different numbers of devices.

### VMware Identity Manager Connector Server

The VMware Identity Manager Connector is responsible for directory synchronization and authentication between on-premises resources such as Active Directory, VMware Horizon, and the VMware Identity Manager service.

The VMware Identity Manager Connector can be used in both cloud-based and on-premises deployments of VMware Identity Manager.

---

#### Table 208: SQL Server for Workspace ONE UEM VM Specifications (Continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:0 Windows OS 50 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:1 Database Disk 500 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:2 Log Disk 200 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:3 Temp Disk 200 GB</td>
</tr>
</tbody>
</table>

---

#### Table 209: VMware Identity Manager Connector VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>VMware Identity Manager 3.3.0</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</td>
</tr>
</tbody>
</table>
Table 209: VMware Identity Manager Connector VM Specifications (Continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:0 Windows OS 50 GB</td>
</tr>
</tbody>
</table>

**VMware Identity Manager Appliance**

This server hosts the VMware Identity Manager service, which provides the app catalog, conditional access, and single sign-on.

VMware Identity Manager Appliances are required only in an on-premises deployment of VMware Identity Manager.

Table 210: VMware Identity Manager Appliance VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>VMware Identity Manager 3.3.0</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</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>16 GB</td>
</tr>
<tr>
<td>vNICs</td>
<td>1</td>
</tr>
<tr>
<td>Virtual network adapter 1</td>
<td>E1000 Adapter</td>
</tr>
</tbody>
</table>
Table 210: VMware Identity Manager Appliance VM Specifications (Continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual SCSI controller 0</td>
<td>LSI Logic Parallel</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:0 100 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:1 100 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:2 10 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:3 10GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:4 100GB</td>
</tr>
</tbody>
</table>

SQL Server for VMware Identity Manager

This database server stores VMware Identity Manager data and is required only for an on-premises deployment of VMware Identity Manager.

Table 211: SQL Server for VMware Identity Manager VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>SQL Server 2016</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>vCPU</td>
<td>8</td>
</tr>
<tr>
<td>vMemory</td>
<td>64 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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:0 Windows OS 50 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:1 Data Disk 100 GB</td>
</tr>
</tbody>
</table>
VMware Workspace ONE Intelligence

VMware Workspace ONE® Intelligence™ is designed to simplify user experience without compromising security. The intelligence service aggregates and correlates data from multiple sources to give complete visibility into the entire environment. Workspace ONE Intelligence requires its own connector server.

Intelligence Collection Service (ETL) Connector Server

This server hosts the ETL (Extract, Transform, Load) service responsible for collecting data from the Workspace ONE database and feeding it to the Workspace ONE Intelligence cloud service.

**Table 212: Intelligence Collection Service (ETL) Connector VM Specifications**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>18.9.26</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>vCPU</td>
<td>4</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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:1 Windows OS 50 GB</td>
</tr>
</tbody>
</table>

VMware Horizon 7

Several servers are required to take advantage of all features in a VMware Horizon® 7 deployment.

**Enrollment Server**

The enrollment server is required for the VMware True SSO feature.
Table 213: Horizon Enrollment Server VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Horizon 7, version 7.7.0</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:1 Windows OS 50 GB</td>
</tr>
</tbody>
</table>

Horizon 7 – Connection Server

This server acts as a broker for client connections. It authenticates users through Windows Active Directory and directs the request to the appropriate virtual machine, physical PC, or Microsoft RDSH server.

Table 214: Horizon 7 Connection Server VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Horizon 7, version 7.7.0</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>vCPU</td>
<td>4</td>
</tr>
<tr>
<td>vMemory</td>
<td>12 GB</td>
</tr>
</tbody>
</table>
Table 214: Horizon 7 Connection Server VM Specifications (Continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:1 Windows OS 50 GB</td>
</tr>
</tbody>
</table>

Horizon 7 – Composer Server

Composer can be installed as a standalone server, or it can be co-installed on a Windows server with vCenter Server. This server works with the Connection Servers and a vCenter Server. Composer is the legacy method that enables scalable management of virtual desktops by provisioning from a single master image using linked-clone technology.

Table 215: Horizon 7 Composer VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Horizon 7, version 7.7.0</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:1 Windows OS 50 GB</td>
</tr>
</tbody>
</table>
Horizon 7 – JMP Server

The JMP (Just-in-Time Management Platform) server provides an interface that simplifies using the three VMware technologies that deliver Just-in-Time Desktops and Apps in a flexible, fast, and personalized manner. You create a desktop workspace by defining a JMP assignment that includes information about the desktop pool, App Volumes AppStacks, and User Environment Manager settings.

**Table 216: Horizon 7 Cloud Connector VM Specifications**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Horizon 7, version 7.7.0</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>vCPU</td>
<td>4</td>
</tr>
<tr>
<td>vMemory</td>
<td>8</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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:1 Windows OS 50 GB</td>
</tr>
</tbody>
</table>

Horizon – Cloud Connector

You deploy the Horizon Cloud Connector virtual appliance to allow pairing with a Connection Server in an on-premises pod. As a result, the pod is connected to the Horizon Cloud control plane. This pairing also enables the use of subscription licensing.
### Table 217: Horizon Cloud Connector VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Horizon 7, version 7.7.0</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>VMware Photon OS</td>
</tr>
<tr>
<td>vCPU</td>
<td>2</td>
</tr>
<tr>
<td>vMemory</td>
<td>4</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>Scsi0:1 40 GB</td>
</tr>
</tbody>
</table>

### SQL Server for Horizon 7

SQL Server is used for the Connection Server event database, the Composer database, and the App Volumes database.

### Table 218: SQL Server for Horizon 7 VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>SQL Server 2016</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>vCPU</td>
<td>2</td>
</tr>
<tr>
<td>vMemory</td>
<td>8 GB</td>
</tr>
</tbody>
</table>
Table 218: SQL Server for Horizon 7 VM Specifications (Continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:0 Windows OS 50 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:1 Data Disk 50 GB</td>
</tr>
</tbody>
</table>

**VMware App Volumes**

For VMware App Volumes™ you deploy a VM that hosts the App Volumes Manager server.

**App Volumes Manager Server**

Table 219: App Volumes Manager VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>VMware App Volumes 2.15.0</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2016</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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:1 Windows OS 50 GB</td>
</tr>
</tbody>
</table>
VMware vRealize Operations

VMware vRealize® Operations 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.

vRealize Operations Manager

This server hosts the vRealize Operations Manager, which monitors Horizon components and vSphere, and displays all information, alerts, and warnings for compute, storage, and networking.

Table 220: vRealize Operations Manager VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>VMware vRealize Operations Manager 7.0.0</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 11</td>
</tr>
<tr>
<td>OS</td>
<td>SUSE Linux Enterprise 11 (64-bit)</td>
</tr>
<tr>
<td>vCPU</td>
<td>16</td>
</tr>
<tr>
<td>vMemory</td>
<td>48 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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:0 Disk 20 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:1 Disk 250 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:2 Disk 4 GB</td>
</tr>
</tbody>
</table>

vRealize Operations Manager – Remote Collector

This type of server overcomes data collection issues across the enterprise network, such as limited network performance. Remote collector virtual appliances gather statistics about inventory objects and forward collected data to the data nodes. Remote collector nodes do not store data or perform analysis.
Table 221: vRealize Operations Manager VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>VMware vRealize Operations Manager 7.0.0</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 11</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>VMware Paravirtual</td>
</tr>
<tr>
<td>Virtual disk – VMDK (scsi0:x)</td>
<td>Scsi0:0 Disk 20 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:1 Disk 250 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:2 Disk 4 GB</td>
</tr>
</tbody>
</table>

**VMware vSphere**

The VMware vSphere® server components include VMware vCenter Server® and VMware NSX® Data Center for vSphere®.

**vCenter Server**

A vCenter Server can be deployed as a prepackaged virtual appliance, as was done for this reference architecture, or alternatively, it can be installed in a Windows server.
### Table 222: vSphere vCenter Server VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>vCenter Server 6.7.0.20000</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Other 3.x Linux (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 1.6 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 25 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:8 Disk 1.4 TB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:9 Disk 10 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:10 Disk 25 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:11 Disk 25 GB</td>
</tr>
<tr>
<td></td>
<td>Scsi0:12 Disk 100 GB</td>
</tr>
</tbody>
</table>

**NSX Manager**

NSX provides network-based services such as security, virtualization networking, routing, and switching in a single platform. NSX Manager is the management plane for the NSX platform. The software deployments and Distributed Firewall rules are configured and managed from here. NSX Manager is configured to communicate with a vCenter Server.
### Table 223: NSX Manager VM Specifications

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>NSX Manager 6.4.4</td>
</tr>
<tr>
<td>VM hardware</td>
<td>VMware Virtual Hardware version 14</td>
</tr>
<tr>
<td>OS</td>
<td>Other 3.x Linux (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 60 GB</td>
</tr>
</tbody>
</table>
Appendix B: VMware Horizon Configuration

This appendix provides details about VMware Horizon® installation, deployment, configuration. It is not intended to replace the product documentation but to reference and supplement it with additional guidance.

VMware Horizon 7 Installation and Configuration

This section provides an overview of the VMware Horizon® 7 deployment process, points to specific documents for detailed instructions, and lists certain settings that were used in this reference architecture.

Installation Prerequisites

Before starting, certain other infrastructure components must be in place and configured. Refer to "Environment Infrastructure Design" on page 221, and see the following sections in that chapter:

- Management VMware vSphere® cluster, as described in the vSphere section
- VDI vSphere cluster, as described in the vSphere section
- Active Directory, as described in the Active Directory section
- DNS, as described in the DNS section
- DHCP, as described in the DHCP section
- Certificate Authority, as described in the Certificate Authority section
- A third-party load balancer, as described in the Load Balancing sections in "Component Design: Horizon 7 Architecture" on page 132.

You must also create a Windows 2016 RDSH VM template, using the guidelines in Creating an Optimized Windows Image for a VMware Horizon Virtual Desktop.

Installation Steps

This section outlines the Horizon 7 installation steps.

1. Set up the required administrator users and groups in Active Directory.
2. If you have not yet done so, install and set up VMware ESXi™ hosts and VMware vCenter Server®.
3. (Optional) If you are going to deploy linked-clone desktops, install Composer, either on the vCenter Server system or on a separate server. Also install the Composer database.
4. Install and set up Connection Servers. Also install the event database.
5. Create one or more VMs that can be used as a template for full-clone desktop pools or as a master for linked-clone desktop pools or instant-clone desktop pools.
6. Set up an RDSH server VM and install applications to be remoted to end users.
7. Create desktop pools, application pools, or both.
8. Entitle users to desktops and published applications.
9. Install VMware Horizon® Client™ on end users’ machines and have end users access their remote desktops and applications.

10. (Optional) Set up and configure enrollment servers to enable True SSO. See "Setting Up True SSO for Horizon 7" on page 349.

11. (Optional) Install a JMP Server to allow the use of JMP workflows and assignments. See VMware Horizon JMP Server Installation and Setup Guide for instructions.

12. (Optional) Create and configure additional administrators to allow different levels of access to specific inventory objects and settings.

13. (Optional) Configure policies to control the behavior of Horizon 7 components, desktop and application pools, and end users. See Configuring Policies in Horizon Administrator and Active Directory.

14. (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 "Component Design: Unified Access Gateway Architecture" on page 207.

Preparation

Build four Windows 2016 VMs: two for Connection Servers and two for the enrollment servers (required for True SSO).

Follow the hardware specifications in "Appendix A: VM Specifications" on page 326 and assign the VMs static IP addresses.

Deployment

This guide is not intended to replace the Horizon 7 documentation. Follow the relevant section of the Horizon 7 Installation documentation to install the following components in the following order:

1. Install the first standard Connection Server – See Install Horizon Connection Server with a New Configuration.

2. Install a replica Connection Server – See Install a Replicated Instance of Horizon Connection Server.

3. Install and configure the Horizon Cloud Connector – See Enabling Horizon 7 for Subscription Licenses.

   Note: This is only required when using subscription-based licensing.


Post-Installation Configuration

Connect to the first Connection Server and perform the following tasks in the following order:

1. Apply the perpetual license key – See Install the Product License Key.

   Note: This step is not necessary if subscription licensing is being used and you have deployed the Horizon Cloud Connector.
2. **Add vCenter Server and configure the View Storage Accelerator** – See Configuring Horizon 7 for the First Time.

3. **Add instant clone domain administrators** – See Add an Instant-Clone Domain Administrator.

4. **Configure event reporting** – See Configuring Event Reporting.

5. **Assign administrators and roles** – See Configuring Role-Based Delegated Administration.


For each of the Connection Servers, configure the following.

### Table 224: Connection Server Configuration Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Detail</th>
</tr>
</thead>
</table>
| General settings            | Because we are using Unified Access Gateway for external connectivity, ensure that the following fields are deselected:  
  - HTTP(S) Secure Tunnel  
  - PCoIP Secure Gateway  
  If HTML Access is not being used, select the option for Do not use **Blast Secure Gateway under Blast Secure Gateway**.  
  If HTML Access is to be used, we can tunnel through the Connection Server and have it provide the SSL certificate. This can remove the requirement for each virtual desktop to have a trusted SSL certificate.  
  - In the Blast Secure Gateway section, select the option **Use Blast Secure Gateway for only HTML Access connections to machine**.  
  - Set the Blast External URL to https://horizon.example.com:8443 |
| Authentication              | Follow the steps in **Configure a SAML Authenticator in Horizon Administrator** to set up the VMware Identity Manager as a SAML authenticator. |
| Backup                      | Define a backup schedule and location for the Connection Server configuration according to **Backing Up and Restoring Horizon 7 Configuration Data**. |
| Origin checking             | With multiple Connection Servers fronted by a load balancer, it is necessary to change origin checking on each server. If origin checking is left enabled, the load balanced name used to initiate a connection would not match the actual server name. This can cause the connection server to reject the request. One indication of this is when using HTML Access or the Horizon Administrator console from Google Chrome or Safari browsers.  
  To disable origin checking, create a locked.properties file in the |
Table 224: Connection Server Configuration Tasks (Continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>C:\Program Files\VMware\VMware View\Server\sslgateway\conf directory. Enter the following entries as detailed in Cross-Origin Resource Sharing. checkOrigin=falsebalancedHost=horizon.example.comportalHost.1=unified-access-gateway-name-1.example.comportalHost.2=unified-access-gateway-name-2.example.com</td>
</tr>
<tr>
<td></td>
<td>Restart the Connection Server services.</td>
</tr>
</tbody>
</table>

Certificates

When you first install Horizon 7, it uses self-signed certificates. VMware does not recommend that you use these in production. At a high level, the steps for replacing the certificates on the Connection Servers and the Composer server are:

1. Create a certificate signing request (CSR) configuration 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 7 to use the signed certificate.

For the full process, see Configuring TLS Certificates for Horizon 7 Servers.

Cloud Pod Architecture

If multiple Horizon 7 pods are being used, Cloud Pod Architecture (CPA) should be configured. This is especially useful when configuring multiple sites, where each site should have its own separate pod.

More detail on Cloud Pod Architecture can be found in "Component Design: Horizon 7 Architecture" on page 132.

Create the Pod Federation

1. Connect to the Horizon Administrator console on one of the Connection Servers in the first pod (Site 1).
2. Choose the task to initialize the Cloud Pod Architecture feature.
3. Rename the pod federation if desired.
4. Rename the site.
5. Rename the pod if desired.

Join Another Pod to the Federation

1. Connect to the Horizon Administrator console on one of the Connection Servers in the that pod (Site 2).
2. Choose the option to join the pod federation.
3. Enter the FQDN of a Connection Server from the first pod, along with credentials.
4. If this pod is in another physical location, create a new site.
5. Edit the newly added pod.
   a. Rename the pod if desired.
   b. Move the pod to the appropriate site.

See [Setting Up a Cloud Pod Architecture Environment](#) for full instructions.

**Desktop Pool Settings**

The following table lists specific desktop pool settings that were used in this reference architecture.

**Table 225: Configuration Settings for Instant-Clone Desktop Pools**

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Settings for Instant-Clone Pools</th>
</tr>
</thead>
</table>
| Desktop Pool Definition     | • Type: Automated
                               | • User Assignment: Floating
                               | • vCenter Server: Instant clones                                    |
| Desktop Pool Settings       | • Remote Machine Power Policy: N/A
                               | • Delete or refresh machine on logout: N/A
                               | • Default display protocol: VMware Blast
                               | • 3D renderer: N/A or NVIDIA GRID vGPU (depending on use case)      |
                               | • HTML access: Enabled                                                |
| Provisioning Settings       | Provision all machines up-front: Selected                             |
| Guest Customization         | AD container: Dedicated OU for this type of desktop                   |

**RDS Farm Settings**

The following table lists specific RDSH server farm settings that were used in this reference architecture.
**Table 226: Configuration Settings for RDSH Server Farms**

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Settings for RDSH Server Farms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Pool Definition</td>
<td>Type: Automated</td>
</tr>
<tr>
<td>Identification and Settings</td>
<td>• Default display protocol: VMware Blast</td>
</tr>
<tr>
<td></td>
<td>• HTML access: Enabled</td>
</tr>
<tr>
<td></td>
<td>• Max sessions per RDS host: 30 or greater, depending on server</td>
</tr>
<tr>
<td></td>
<td>hardware and VM specifications</td>
</tr>
<tr>
<td>Guest Customization</td>
<td>AD container: Dedicated OU for this type of desktop</td>
</tr>
<tr>
<td></td>
<td>Predefined specification</td>
</tr>
</tbody>
</table>

**Setting Up True SSO for Horizon 7**

The high-level steps that need to be completed are:

1. Configure Horizon 7 and VMware Identity Manager™ Integration.
2. Install and configure Microsoft Certificate Authority service.
3. Set up a certificate template for use with True SSO.
4. Install and configure the enrollment servers.
5. Add VMware Identity Manager as a SAML Authenticator to the Connection Servers.
6. Add the Horizon 7 pods to VMware Identity Manager.

For more information on how to install and configure True SSO, see [Setting Up True SSO](#).

**Horizon 7 and VMware Identity Manager Integration**

As a prerequisite, integrate Horizon 7 and VMware Identity Manager. This consists of three high-level steps:

1. Deploy VMware Identity Manager Connectors and configure Active Directory synchronization.
2. Create one or more virtual apps collections in VMware Identity Manager.
3. Configure SAML authentication on the Horizon 7 Connection Servers.

Full details on this is given in "Platform Integration" on page 244.

**Set Up a Microsoft Enterprise Certificate Authority**

1. Add the Active Directory Certificate Services Server role using the Add Roles and Features Wizard. The only role service required is Certification Authority.
2. Once installed, configure Active Directory Certificate Services using the following values.
Table 227: Settings for Active Directory Certificate Services

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Services</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>Setup Type</td>
<td>Enterprise CA</td>
</tr>
<tr>
<td>CA Type</td>
<td>Root CA or Subordinate CA, depending on your preference for PKI deployments. Choose Root CA if you are not integrating into an existing PKI.</td>
</tr>
<tr>
<td>Private Key</td>
<td>Create a new private key</td>
</tr>
</tbody>
</table>
| Cryptology         | - Key length: 2048 (recommended)  
                     - Hash algorithm: SHA256 (recommended) |
| CA Name            | Change if desired. |
| Validity Period    | Leave as default of 5 years. |

3. The final configuration is done by opening a command prompt, as an Administrator, and running the following commands:
   a. Enable non-persistent certificate processing and help reduce the CA database growth rate:
      ```
      certutil -setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
      ```
   b. Ignore offline CRL (certificate revocation list) errors on the CA:
      ```
      certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE
      ```
   c. Restart the Certificate Authority Service so that these changes can take effect.
      ```
      sc stop certsvc sc start certsvc
      ```

Repeat these steps (1 to 3) on each Certificate Authority server. Also see Set Up an Enterprise Certificate Authority.

Create and Issue a Certificate Template

As preparation, create an active directory security group for the enrollment server computer accounts. This will be used when creating the certificate template and assigning permissions to the enrollment servers. A group makes adding new enrollment servers easier.

1. Create a new certificate template by first opening the Certification Authority administrative tool.
a. Expand the tree in the left pane, right-click **Certificate Templates** and select **Manage**. Right-click the **Smartcard Logon** template and select **Duplicate Template**.

b. Do not click **OK** until you have completed all the configurations listed in the following table.

### Table 228: Configuration Settings for the Certificate Template

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Setting</th>
</tr>
</thead>
</table>
| **Compatibility**  | • Certification Authority: **Windows Server 2008 R2**  
                     • Certificate recipient: **Windows 7 / Server 2008 R2** |
| **General**        | • Template display name: True SSO  
                     • Template name: TrueSSO  
                     • Validity period: 1 hour  
                     • Renewal period: 0 hours |
| **Request Handling** | • Purpose: **Signature and smartcard logon**  
                         • Select **Allow private key to be exported**.  
                         • Select **For automatic renewal of smart card certificates**. |
| **Cryptography**   | • Provider category: **Key Storage Provider**  
                     • Algorithm name: **RSA**  
                     • Minimum key size: **2048**  
                     • Request hash: **SHA256**  
                     Can be different depending on the security standards. |
| **Server**         | • Select **Do not store certificates and requests in the CA database**.  
                     • De-select **Do not include revocation information in issued certificates**. |
| **Issuance Requirements** | • Select **This number of authorized signatures**.  
                            • Value: 1  
                            • Policy type required in signature: **Application Policy**  
                            • Application Policy: **Certificate Request Agent** |
Table 228: Configuration Settings for the Certificate Template (Continued)

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● Require the following for enrollment: <strong>Valid existing certificate</strong></td>
</tr>
<tr>
<td>Subject Name</td>
<td>Leave as is.</td>
</tr>
<tr>
<td>Security</td>
<td>Add the group you created for the enrollment servers in preparation and give this read and enroll permissions.</td>
</tr>
</tbody>
</table>

2. Before closing the Certificate Template console, change the permissions on the **Enrollment Agent (Computer)** template. Add the security group that you created for the enrollment server computer accounts and give it read and enroll permissions.


4. Issue the True SSO certificate template.
   a. Right-click **Certificate Templates** and select **New > Certificate Template to Issue**.
   b. Select the new True SSO template you just created. This step is required for all certificate authorities that issue certificates based on this template. Repeat the issuance on all certificate authority servers.

5. Issue the Enrollment Agent (Computer) certificate template.
   a. Right-click **Certificate Templates** and select **New > Certificate Template to Issue**.
   b. Select the **Enrollment Agent (Computer) Template**. This step is required for all certificate authorities that issue certificates based on this template. Repeat the issuance on all certificate authority servers.

See [Create Certificate Templates Used with True SSO](#).

**Enrollment Server Setup**

The next steps are to install the Horizon enrollment service, enable it to request certificates, and pair it the Connection Servers. See [Install and Set Up an Enrollment Server](#).

**Install the Enrollment Server Service**

1. Run the Horizon 7 Connection Server executable.
2. Select the **Enrollment Server** role.
3. Indicate the authentication mode and whether you are configuring Horizon 7 or Horizon Cloud.
Appendix B: VMware Horizon Configuration

Install the Enrollment Agent (Computer) Certificate.

This authorizes this enrollment server to act as an Enrollment Agent and generate certificates on behalf of users.

1. Open the Microsoft Management Console (MMC) and select Add/Remove Snap-in > Certificates > Computer account > Local computer.
2. Expand Certificates > Personal folder.
3. Right-click All tasks > Request New Certificate.
4. Request and enroll the Enrollment Agent (computer) certificate.

Configure Connection Server Pairing

Next, configure Connection Server pairing so that the enrollment service will trust the Connection Server when it prompts the enrollment servers to issue the short-lived certificates for Active Directory users.

1. Export certificate from Connection Server:
   a. On one of the Connection Servers, open the Microsoft Management Console (MMC) and select Add/Remove Snap-in > Certificates > Computer account > Local computer.
   b. Expand Certificates > VMware Horizon View Certificates > Certificates folder.
   c. Right-click the certificate file with the friendly name vdm.ec, and select All Tasks > Export.
   d. In the Certificate Export wizard, accept the defaults, including leaving the No, do not export the private key radio button selected.
   e. Save the file with a meaningful name such as s1-pl-enrollclient.cer.
2. Import the certificate to the enrollment server:
   a. On the enrollment server, open the Microsoft Management Console (MMC) and select Add/Remove Snap-in > Certificates > Computer account > Local computer.
   b. Expand Certificates > VMware Horizon View Enrollment Server Trusted Roots folder.
   c. Right-click All tasks > Import and browse to the file you saved from the Connection Server export.
   d. Ensure that the certificate will be placed in the VMware Horizon View Enrollment Server Trusted Roots store.
3. Configure the enrollment service to give preference to the local certificate authority when they are co-located:
   a. Edit the registry using regedit.exe as an administrator.
   b. Browse to the following location: HKLM\SOFTWARE\VMware, Inc\VMware VDM\Enrollment Service. You must create the Enrollment Service key if it does not already exist.
   c. Right-click and add a new String Value (REG_SZ)
      Name: PreferLocalCa
      Value data: 1
d. Repeat this process on each Enrollment Server. Also see Enrollment Server Configuration Settings.

Connection Server Configuration

The last configuration is to add the enrollment servers to the Horizon Connection Servers, and to enable the authenticators. On one of the Connection Servers in the pod, open a command prompt, as an administrator, and browse to C:\Program Files\VMware\VMware View\Server\tools\bin. You will use the vdmutil.exe command tool in the following steps.

1. Add the enrollment servers to environment.
2. List enrollment servers to confirm their details.
3. Create the connectors.
4. List the SAML authenticator details.
5. Enable TrueSSO for the SAML Authenticator

The parameters are case-sensitive.

In each of the commands you need to specify credential parameters:

- --authAs <administrator>
- --authDomain <domain>
- --authPassword <Password>

The following tables provide the syntax and examples for performing each of these steps. For more information about these steps, also see Configure Horizon Connection Server for True SSO.

Table 229: Step 1: Add Enrollment Servers (ES) to Environment

<table>
<thead>
<tr>
<th>Syntax</th>
<th>vdmutil --authAs &lt;administrator&gt; --authDomain &lt;domain&gt; --authPassword &lt;Password&gt; --trueSSO --environment --add --enrollmentServer &lt;enrollment Server FQDN&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example 1: Add first enrollment server</td>
<td>vdmutil --authAs administrator --authDomain vmweuc --authPassword Password --trueSSO --environment --add --enrollmentServer s1-enr1.vmweuc.com</td>
</tr>
<tr>
<td>Example 2: Add second enrollment server</td>
<td>vdmutil --authAs administrator --authDomain vmweuc --authPassword Password --trueSSO --environment --add --enrollmentServer s1-enr2.vmweuc.com</td>
</tr>
</tbody>
</table>

Table 230: Step 2: List Enrollment Servers (ES)
### Syntax

```
vdmutil --authAs <administrator> --authDomain <domain> --authPassword <Password> --truesso --environment --list --enrollmentServers
```

```
vdmutil --authAs <administrator> --authDomain <domain> --authPassword <Password> --truesso --environment --list --enrollmentServer <enrollment Server FQDN> --domain <domain FQDN>
```

#### Example 1: List enrollment servers
```
vdmutil --authAs administrator --authDomain vmweuc --authPassword Password --truesso --environment --list --enrollmentServers
```

#### Example 2: List detail of first enrollment server
```
vdmutil --authAs administrator --authDomain vmweuc --authPassword Password --truesso --environment --list --enrollmentServer s1-enr1.vmweuc.com --domain vmweuc.com
```

#### Example 3: List detail of second enrollment server
```
vdmutil --authAs administrator --authDomain vmweuc --authPassword Password --truesso --environment --list --enrollmentServer s1-enr2.vmweuc.com --domain vmweuc.com
```

### Table 231: Step 3: Create Connectors

```
vdmutil --authAs <administrator> --authDomain <domain> --authPassword <Password> --truesso --create --connector --domain <domain FQDN> --template "True SSO" --primaryEnrollmentServer <enrollment Server FQDN> --certificateServer <Domain-CA> --mode enabled
```

#### Example: Create connector with primary and secondary servers and both certificate authorities
```
vdmutil --authAs administrator --authDomain vmweuc --authPassword Password --truesso --create --connector --domain vmweuc.com --template TrueSSO --primaryEnrollmentServer s1-enr1.vmweuc.com --secondaryEnrollmentServer s1-enr2.vmweuc.com --certificateServer vmweuc-S1-ENR1-CA,vmweuc-S1-ENR2-CA --mode enabled
```

### Table 232: Step 4: List SAML Authenticator

```
vdmutil --authAs <administrator> --authDomain <domain> --authPassword <Password> --truesso --list --authenticator
```

#### Example
```
vdmutil --authAs administrator --authDomain vmweuc --authPassword Password --truesso --list --authenticator
```

### Table 233: Step 5: Enable TrueSSO for the SAML Authenticator

```
vdmutil --authAs <administrator> --authDomain <domain> --authPassword <Password> --truesso --list --authenticator
```

#### Example
```
vdmutil --authAs administrator --authDomain vmweuc --authPassword Password --truesso --list --authenticator
```
Finally, in any pod with two enrollment servers, change load balancing to round robin instead of the default active/passive. This only needs to be done on one Connection Server per pod.

1. On one of the Connection Servers, from Windows Administrative Tools, open ADSI Edit.
2. Right-click Connect to and define the Connection Settings.
3. For the Connection Point setting, choose the option for Select or type a Distinguished Name and type DC=vdi, DC=vmware, DC=int
4. For the Computer setting, type localhost:389
5. Expand OU=Properties, select OU=Global, and double-click CN=Common in the right pane.
6. Edit the pae-NameValuePair attribute.
7. Add a new value cs-view-certsso-enable-es-loadbalance=true and click OK.

See Connection Server Configuration Settings.

Setting Up True SSO for Horizon Cloud Service on Microsoft Azure

For detailed information on how to install and configure True SSO, see Configure True SSO for Use with Your Horizon Cloud Environment.

The high-level steps that need to be completed are:

1. Install and configure a Certificate Authority. See "Set Up a Microsoft Enterprise Certificate Authority" on page 349.
3. Download the Horizon Cloud pairing bundle from the Administration Console’s Active Directory page.
   a. The pairing bundle is used when setting up the Enrollment Server.
   b. See Download the Horizon Cloud Pairing Bundle.
4. Set up the Enrollment Server. See Set up the Enrollment Server.
5. Configure the Enrollment Server to prefer to use the local Certificate Authority service. See Enrollment Server Configuration Settings.
a. Edit the registry on the Enrollment servers using regedit.exe as an administrator.
b. Browse to the following location: HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Enrollment Service. You must create the Enrollment Service key if it does not already exist.
c. Right-click and add a new String Value (REG_SZ):
   - Name: PreferLocalCa
   - Value data: 1
d. This process needs to be repeated on each enrollment server.

**VMware vRealize Operations for Horizon Deployment and Configuration**

To deploy VMware vRealize® Operations for Horizon® there are two main tasks.

1. Deploy and configure a vRealize Operations cluster and remote collector nodes.
2. Install and configure the Horizon solution components.

**Deploy vRealize Operations Manager**

Deploy vRealize Operations appliances, form the cluster, and configure remote collectors. See [Installing vRealize Operations Manager](#).

1. Deploy a vRealize Operations appliance for each of the cluster nodes required.
   a. Use the **Deploy OVF Template** wizard in vSphere Client.
   b. Power on the appliances.
2. Install and configure the cluster.
   a. Complete the initial setup of the cluster by following the wizard on the first node. Open a browser and navigate to https://<first-node-FQDN-or-IP-address>/admin. The first node will become the master.
   b. On the Get Started page, select **New Installation**.
   c. Enter and re-enter a password for the admin user account.
   d. Install a certificate if available. If a certificate is not available, use the default certificates that are generated.
   e. Enter a name for **Cluster Master Node**.
   f. For **NTP Server Addresses**, add addresses to allow the nodes of the cluster to synchronize time.
      
      **Note**: If you leave the NTP blank then vRealize Operations Manager will manage its own synchronization by having all nodes synchronize with the master node and replica node.
   g. In **Add Nodes**, add the second cluster node, which will become a replica. **Enable high availability for this cluster** and select the second mode as a **Master Replica**.
On completion of the new installation wizard, the cluster will perform the configuration. The cluster might take from 10 to 30 minutes to start, depending on the size of your cluster and nodes. Do not make changes or perform any actions on cluster nodes while the cluster is starting.

3. Add the remote collector nodes. See Run the Setup Wizard to Create a Remote Collector Node.
   a. Deploy the remote collectors using the Deploy OVF Template wizard.
   b. Add the remote collector to the cluster using a browser, and navigate to https://<collector-FQDN-or-IP-address>/admin.
   c. On the Get Started page, select Expand an Existing Installation.
   d. Give the node a name and select Remote Collector for the node type.
   e. Enter the master node IP address or FQDN, validate the certificate, and accept the certificate.
   f. Authenticate to the cluster using the administrator user account and password specified during the cluster installation.
   g. Repeat this process for each additional remote collector.

4. Apply the security patch by following the knowledge base article vRealize Operations Manager 6.6.1, 6.7 and 7.0 Security Patch (60301).
   a. This takes the build version to 7.0.0.11287812
   b. The above patch is required to support vRealize Operations for Horizon 6.6 running on vRealize Operations Manager version 7.0 See vRealize Operations for Horizon compatibility with vRealize Operations Manager 7.0 (59651) for instructions on upgrading licenses through My VMware.

5. Apply vRealize Operations Manager licensing.
   Open a browser, navigate to https://<first-node-FQDN-or-IP-address>/ and follow the first-run wizard, entering your vRealize Operations Manager license key.

6. Complete the vRealize Operations Manager setup. Tasks include configuring the vCenter Server adapter by following the instructions in VMware vSphere Solution in vRealize Operations Manager. If you are using VMware vSAN™, configure the vSAN adapter. Consider configuring access control and external authentication sources.

**Deploy vRealize Operations for Horizon**

When vRealize Operations Manager is installed, configured, and licensed, you can progress with the installation of the Horizon adapter and the broker agent. See Installing and Configuring vRealize Operations for Horizon for full instructions.

1. Install the vRealize Operations for Horizon solution:
   a. Open a browser, and navigate to https://<first-node-FQDN-or-IP-address>/
   b. Navigate to Administration > Solutions and select the + (Add) icon to add the new solution.
c. **Browse** to the VMware-vrops-viewadapter-6.6.0-buildnumber.pak file and click **Upload**.

2. Create a vRealize Operations Adapter instance:
   a. Navigate to **Administration > Solutions**.
   b. Select **VMware Horizon** and select the gear (configure) icon.
   c. In the Adapter Type column, select **Horizon Adapter**.
   d. Define the instance settings, which include name and adapter ID.
   e. Define credentials to be used in pairing the Horizon adapter to the Horizon Broker.
   f. Under Advanced Settings, select the appropriate remote collector.
   g. Test the connection and click **Save Settings**.
   h. Select the + (Add) icon to add a new adapter instance for each remote site, selecting the remote collector for that site.

3. Apply licensing:
   a. Add a license key by navigating to **Administration > Management > Licensing**.
   b. Select the + (Add) icon to add a new license key.
   c. Select **VMware Horizon** from the drop-down list and enter your vRealize Operations for Horizon license key. Validate and save the settings.
   d. Next, follow the instructions in **Associate Objects with Your License Key**
   e. Click the **License Groups** tab.
   f. Edit the membership criteria for the **VMware Horizon Solution Licensing** group to include the objects used by Horizon.
   g. Edit the membership criteria for the **Product Licensing** group to exclude the objects.
4. Follow the instructions in **Import vGPU Dashboards** (optional).

5. Install and configure the vRealize Operations for Horizon Broker Agent:
   
a. Log on to a Connection Server and run the `VMware-v4vbrokeragent-x86_64-6.6.0-buildnumber.exe` executable to install the Horizon Broker Agent.  
   **Note:** The broker agent is installed on only one Connection Server per pod.

b. Pair the broker agent with a Horizon Adapter instance using the Broker Agent Config Utility for Horizon wizard. For instructions, see **Configure the vRealize Operations for Horizon Broker Agent**.

c. Repeat this step for each additional pod, pairing each broker agent with the respective Horizon Adapter instance.

6. Install the vRealize Operations for Horizon desktop agents on the parent virtual machine, RDS hosts, or desktops that are to be monitored.
   
a. The vRealize Operations for Horizon desktop agent can be installed as a part of the Horizon Agent installation. It can also be installed separately if required.

b. See the table in **Desktop Agent** to find the version included with the Horizon Agent being used and to determine whether you need to install another version separately.

7. Follow the instructions in **Verify Your vRealize Operations for Horizon Installation**.

**Cloud Pod Architecture Global Entitlement Settings**

For this reference architecture, the following global entitlements were used.
### Table 234: Global Entitlement Settings for Roaming User Use Case

<table>
<thead>
<tr>
<th>GE Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Roaming</td>
</tr>
<tr>
<td>Scope</td>
<td>All Sites (ANY)</td>
</tr>
<tr>
<td>Entitlements</td>
<td>VMWEUC\All_Sales_People</td>
</tr>
<tr>
<td>Use home site</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

This configuration allows anyone connecting to the federation through the global namespace, https://horizon.vmweuc.com for this environment, to get a desktop no matter which pod they get connected to.

This fits with our requirements because our global load balancer (F5 BIG-IP DNS/GTM) is configured to point the user to an available pod closest to their current geographical location.

If a member of the group VMWEUC\All_Sales_People is closest to Site 1, a session is brokered with the pod in Site 1. The same logic applies if that same member is closest to Site 2.

### Table 235: Global Entitlement Settings for Power User Use Case

<table>
<thead>
<tr>
<th>Global Entitlement Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>PowerUser</td>
</tr>
<tr>
<td>Scope</td>
<td>Within Site</td>
</tr>
<tr>
<td>Entitlements</td>
<td>VMWEUC\Site1-PowerUsers</td>
</tr>
<tr>
<td></td>
<td>VMWEUC\Site2-PowerUsers</td>
</tr>
<tr>
<td>Use home site</td>
<td>Enabled</td>
</tr>
<tr>
<td>Entitled user must have home site</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

This global entitlement configuration splits a group of users, PowerUsers, into two groups. This allows for initial user placement by making sure all the members of PowerUsers are not working from the same data center.

This configuration also enables and forces the presence of a home site for the entitled groups in conjunction with defining the scope to be **Within Site**. This effectively means that the two groups are associated with a home site that dictates their preferred placement.
Home Site Configuration When Both Sites Are Operational

The home site configuration for the two groups is as shown in the following table.

Table 236: Initial Placement in Different Data Centers

<table>
<thead>
<tr>
<th>Group</th>
<th>Domain</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site1-PowerUsers</td>
<td>VMWEUC</td>
<td>Site 1</td>
</tr>
<tr>
<td>Site2-PowerUsers</td>
<td>VMWEUC</td>
<td>Site 2</td>
</tr>
</tbody>
</table>

With this configuration, and under normal operating conditions,

- A member of Site1-PowerUsers is always given a desktop resource in Site 1.
- A member in Site2-PowerUsers always gets a desktop resource in Site 2.

Home Site Override – Preparing for Failover

The configuration shown in the preceding section is suitable when both sites are online and fully operational. But using just this global entitlement would cause issues because, in the event of either of the sites being unavailable, part of the user base would not be able to log in.

Additional configuration is required to reverse the logic so that users associated with a site that is currently offline can be temporarily allowed to connect and log in to another site.

For a given global entitlement, it is possible to configure a home site override option that does exactly this.

Table 237: Override Configurations to Use During an Outage

<table>
<thead>
<tr>
<th>Group</th>
<th>Domain</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site1-PowerUsers</td>
<td>VMWEUC</td>
<td>Site 2</td>
</tr>
<tr>
<td>Site2-PowerUsers</td>
<td>VMWEUC</td>
<td>Site 1</td>
</tr>
</tbody>
</table>

Notice how this effectively overrides the home site configuration for those groups at the global entitlement level to reverse the logic, allowing members from group Site1-PowerUsers to connect to Site 2 and members from group Site2-PowerUsers to connect to Site 1.

Note: This change should only be made for the group impacted by a data center outage. At no point in time would both the override options be configured as depicted in the preceding table; the override should be configured only for the group impacted.
The home site override configuration should only be changed after a failed site's resources have been fully failed over. The reverse-logic configuration is of no use if users access the site before their resources are available.

**Horizon Group Policies**

You can use standard Microsoft Group Policy Object (GPO) settings to configure VMware Horizon® virtual desktops and applications, and also use VMware-provided GPO administrative templates for fine-grained control of access to features.

- "OU GPO Best Practices" below
- "Common GPO Settings for Desktop and RDSH Server VMs" on the next page
- "Desktop Settings" on the next page
- "RDSH Server OU-Level Settings" on page 365
- "User Configuration Settings" on page 366
- "User Environment Manager – Group Policy Settings " on page 367

**OU GPO Best Practices**

Use the following guidelines when applying GPO settings to organizational units (OUs):

- Consider blocking inheritance on the OUs where Horizon desktops or RDSH servers will be provisioned.
- Re-use GPOs.
- Create separate OUs for users and computers.
- Ensure that each GPO is enabled or disabled for **Computer Settings** and **User Settings**.
- Group similar settings into one GPO.
- Understand the difference between monolithic and functional GPOs:
  - Monolithic GPOs contain settings for many different areas and are quite large. All settings are in one place. Use monolithic GPOs for generic settings that apply to all users or computers.
    - Monolithic GPOs are typically applied at the domain level or relatively high in the Active Directory hierarchy.
  - Functional GPOs contain a limited number of settings for a specific area. Functional GPOs are smaller GPOs that facilitate settings being defined for particular users or VMs.
    - Functional GPOs are typically applied lower in the Active Directory hierarchy.
- 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 the settings for the VM’s OU are applied to the session.
This appendix contains a list of group policy settings that would typically be applied (this is not an exhaustive list). Most other settings can be applied through VMware User Environment Manager™ policies. As part of the Horizon 7 and VMware Horizon® Cloud Services™ downloads, there is a VMware-Horizon-Extras-Bundle ZIP file that contains a set of group policy templates to assist in defining additional GPO settings.

**Common GPO Settings for Desktop and RDSH Server VMs**

The settings in this section apply to both VDI desktops and RDSH servers.

**Table 238: Settings for Computer Configuration > Policies > Administrative Templates > System > Group Policy**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure user Group Policy loopback processing mode</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td><strong>Mode</strong>: Replace</td>
</tr>
<tr>
<td>Configure Logon Script Delay</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Table 239: Settings for Computer Configuration > Policies > Administrative Templates > System > Logon**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<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>

**Desktop Settings**

The following settings apply only to VDI desktops.
### Table 240: Settings for Computer Configuration > Policies > Administrative Templates > System > User Profiles

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set roaming profile path for all users logging onto this computer</td>
<td>Enabled (Specify the mandatory profile path. This can be local or on a remote network share.)</td>
</tr>
<tr>
<td>Delete cached copies of roaming profiles</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

### RDSH Server OU-Level Settings

The following settings apply only to RDSH servers.

### Table 241: Settings for Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Licensing

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

### Table 242: Settings for Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Profiles

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
Table 243: Settings for Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use mandatory profiles on the RD Session Host server</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

User Configuration Settings

Various settings can be used to optimize the user experience while protecting the system. The following tables list a few basic, initial settings that would normally be applied. Because these are user settings, you must also use the loopback processing setting.

Table 244: Settings for User Configuration > Policies > Administrative Templates > Start Menu and Taskbar

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

Table 245: Settings for User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically activate newly installed add-ons</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Table 246: Settings for User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site to Zone Assignment List</td>
<td>Enabled</td>
</tr>
<tr>
<td>Zone assignments</td>
<td>&lt;URL of Identity Manager&gt; 1</td>
</tr>
<tr>
<td></td>
<td>Example: <a href="https://workspace.vmweuc.com">https://workspace.vmweuc.com</a> 1</td>
</tr>
<tr>
<td></td>
<td>&lt;URL of ThinApp Share&gt; 1</td>
</tr>
<tr>
<td></td>
<td>Example: &gt;\vmweuc.com\files 1</td>
</tr>
</tbody>
</table>

User Environment Manager – Group Policy Settings

The following instructions are excerpted from the User Environment Manager Administration 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 and create a new GPO or select an existing GPO that is applied to the users for which you want to configure FlexEngine.

3. Open the Group Policy Management Editor by right-click the selected GPO and clicking Edit. The FlexEngine ADMX template is available under User Configuration\ Administrative Templates\VMware UEM\FlexEngine.

4. 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** – Setting that enables the FlexEngine agent (recommended). 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 is:
     
     "C:\Program Files\VMware\Horizon Agents\User Environment Manager\FlexEngine.exe" -s

The group policy settings to use are listed in the following tables.
**Table 247**: User Environment Manager GPO Settings for **User Configuration > Policies > Administrative Templates > VMware UEM > FlexEngine**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

**Table 248**: User Environment Manager GPO Settings for **User Configuration > Policies > Windows Settings > Scripts**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
</table>
| Logoff    | Script Name = C:\Program Files\VMware\Horizon Agents\User Environment Manager\FlexEngine.exe  
Script Parameters = -s |

**User Environment Manager Smart Policies**

The following tables contain some simple sample Horizon Smart Policies. Adapt them to suit the use case and environment.

The following policies are defined in the User Environment Manager Management Console.

**Table 249**: Horizon Smart Policies – External

<table>
<thead>
<tr>
<th>Policy settings</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• USB redirection: Disable</td>
<td>Horizon Client property <strong>Client location</strong> is equal to <strong>External</strong></td>
</tr>
<tr>
<td>• Printing: Disable</td>
<td></td>
</tr>
<tr>
<td>• Clipboard: Disable</td>
<td></td>
</tr>
<tr>
<td>• Client drive redirection: Disable</td>
<td></td>
</tr>
<tr>
<td>• PCoIP profile: Not set</td>
<td></td>
</tr>
</tbody>
</table>
Table 250: Horizon Smart Policies – Internal

<table>
<thead>
<tr>
<th>Policy settings</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB redirection: Enable</td>
<td>Horizon Client property <strong>Client location</strong> is equal to <strong>Internal</strong></td>
</tr>
<tr>
<td>Printing: Enable</td>
<td></td>
</tr>
<tr>
<td>Clipboard: Enable</td>
<td></td>
</tr>
<tr>
<td>Client drive redirection:Enable</td>
<td></td>
</tr>
<tr>
<td>PCoIP profile: Not set</td>
<td></td>
</tr>
</tbody>
</table>

Table 251: Horizon Smart Policies – ZContractor

<table>
<thead>
<tr>
<th>Policy settings</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB redirection: Disable</td>
<td>Horizon Client property <strong>Client location</strong> is equal to <strong>Internal</strong></td>
</tr>
<tr>
<td>Printing: Enable</td>
<td>and <strong>User is a member of an Active Directory group Contractor</strong></td>
</tr>
<tr>
<td>Clipboard: Disable</td>
<td></td>
</tr>
<tr>
<td>Client drive redirection:Disable</td>
<td></td>
</tr>
<tr>
<td>PCoIP profile: Not set</td>
<td></td>
</tr>
</tbody>
</table>

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. See Configure Triggered Tasks for more information.

Table 252: Triggered Task – Horizon Smart Policies

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

Additional Configuration for User Environment Manager

There are several enhancements to the folder redirection feature of User Environment Manager. See User Environment Manager 9.6 Folder Redirection Enhancements Feature Walk-Through for more information.
Table 253: Folder Redirection – User Environment Policies

<table>
<thead>
<tr>
<th>Policy Settings</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Remote path: User’s Home drive share using the %username% variableExample: <code>\vmweuc.com\share\Users\%username%</code></td>
<td>None</td>
</tr>
<tr>
<td>• Folders to redirect: Documents</td>
<td></td>
</tr>
<tr>
<td>Note: Depending on your needs, you might also want to select Downloads, Music, Pictures, and Videos. Be aware that selecting these folders places a larger load on your file servers, requiring additional disk space and higher performance requirements.</td>
<td></td>
</tr>
</tbody>
</table>

Configure application blocking to prevent users from running `cmd.exe`. See Configure Application Blocking to enable and configure the application-blocking rules.

Configure User Environment settings to map the \H: drive to the user’s home drive and to map location-based printers. See Using the User Environment Tab for more information.
Appendix C: VMware Identity Manager Configuration for Multi-site Deployments

Use the procedures in this appendix to create SQL Server clustered instances that can fail over between sites and to set up a highly available database for VMware Identity Manager. The following diagram shows the architecture.

**Figure 170**: On-Premises Multi-site VMware Identity Manager Architecture

The tasks you need to complete are grouped into the following procedures:

1. "Create a Windows Server Failover Cluster" on the next page
2. "Configure Cluster Quorum Settings" on page 374
3. "Install the SQL Server" on page 375
4. "Create the VMware Identity Manager Database" on page 376
5. "Sync the Database Account Across the Availability Group Replicas" on page 376
6. "Create and Configure the Availability Group" on page 377
7. "Create a SQL Server Maintenance Job to Back Up the Database" on page 381
8. "Deploy and Set Up VMware Identity Manager Appliances" on page 383
9. "Configure Failover and Redundancy for VMware Identity Manager" on page 386
10. "Deploy and Set Up the Connectors Inside the Corporate Network" on page 387
11. "Finalize Failover Preparation" on page 390
Create a Windows Server Failover Cluster

A Windows Server Failover Cluster (WSFC) is a group of Windows Servers that have the same software installed on them and work together as one instance to provide high availability for a service, such as a Microsoft SQL Server database. If a VM, or cluster node, in the cluster fails, another node in the cluster begins to provide the service.

To create a Windows Server Failover Cluster (WSFC):

1. In Site 1, create and configure two Windows 2016 VMs and then do the same in Site 2. Ensure that the VMs have the same virtual hardware version and the same Windows Server patch levels.

2. In each site, use VMWare vSphere® Web Client to create VMDKs for each of the SQL Server VMs. Format and mount the drives in Windows.

   For our configuration, we used the following dedicated drives:
   - Windows
   - SQL_Binaries
   - SQL_Data
   - SQL_Logs
   - SQL_Temp
   - SQL_Backup

   The WSFC configuration we used does not rely on clustered shared volumes, but it is essential that each of the individual VM disks and volumes in Windows are presented in the same order with the same drive letters.

3. Because two servers in each site form part of the WSFC, VMware recommends that you configure VMware vSphere® Storage DRS™ anti-affinity rules to separate the VMs on different VMware ESXi™ hosts. See Storage DRS Anti-Affinity Rules.

4. Follow the guidelines in the Microsoft article Pre-stage cluster computer objects in Active Directory Domain Services.

5. Install the Windows Failover Clustering feature on each of the SQL Server VMs (two in Site 1 and two in Site 2), using Windows Server Add Roles and Features Wizard.

6. Use the Windows Create Cluster Wizard to add each of the servers to the new cluster:
7. Add a client access point IP for a subnet in Site1 and a subnet in site 2.

8. Because the WSFC spans two sites and subnets, ensure that the cluster heartbeat thresholds are set appropriately.

Four WSFC settings control the behavior of the cluster service regarding missed heartbeat probes:
- **SameSubnetDelay** controls how often a node sends heartbeat probe packets within the same subnet.
- **SameSubnetThreshold** controls how many probe misses the node will tolerate before taking action within the same subnet.
- **CrossSubnetDelay** controls how often a node sends heartbeat probe packets across different subnets.
- **CrossSubnetThreshold** controls how many probe misses the node will tolerate before taking action across different subnets.

Use the PowerShell commands shown in the following screenshot to verify and configure the cluster settings on one of the cluster member servers.

```
PS C:\> (get-cluster).samesubnetThreshold=10
PS C:\> (get-cluster).crosssubnetThreshold=20
PS C:\> get-cluster | fl *subnet*

CrossSubnetDelay : 1000
CrossSubnetThreshold : 20
PlumbAllCrossSubnetRoutes : 0
SameSubnetDelay : 1000
SameSubnetThreshold : 10
```

We recommend setting **SameSubnetThreshold** to 10 and setting **CrossSubnetThreshold** to 20.

### Configure Cluster Quorum Settings

A quorum is required for the WSFC to prevent split-brain scenarios. In this reference architecture, a Windows file share in a third site was used to make a quorum, but it is also possible to use a cloud witness in Azure.

You must configure cluster quorum settings and specify which cluster nodes (VMs) each cluster instance can run on. Each node in a WSFC can cast one “vote” to determine which site is up and thus which node is the primary owner.

To configure the cluster quorum settings:

1. Configure quorum votes for Site 1:
   a. Open Failover Cluster Manager and select **More Actions > Configure Cluster Quorum Settings**.
   b. Complete the Configure Cluster Quorum Wizard, using the following guidelines:
      - **Select Quorum Configuration Option** page – Select **Advanced Quorum Configuration**.
      - **Select Voting Configuration** page – Click **Select Nodes** and select the check boxes for the SQL Server VMs.
• Select Quorum Witness page – Select Configure a file share witness, click Next, and enter the path to the file share; for example, \\S3-FS1\mswsfc1-fsw

The Microsoft article Configure and manage quorum covers this in more detail.

2. To verify that the quorum is configured correctly, in Failover Cluster Manager, select Nodes and examine the Assigned Vote column.

Install the SQL Server

In this procedure, you run the Setup.exe program from the SQL Server installation media and select New SQL Server stand-alone installation. Repeat this procedure for each of the SQL Server VMs in each site.

In Site 1, on the first SQL Server VM, complete the SQL Server installation wizard, using the following guidelines:

• Installation page – Select New SQL Server stand-alone installation.
• Feature Selection page – Select Database Engine Services feature.
• Instance Configuration page – Select Default Instance.
• Database Engine Configuration page – On the Data Directories tab, for each item, select the disk that you created for that type of file. For example, place the data root directory, system database directory, and user data directory on the VMDK disk you created for SQL data. For the database log directory, select the VMDK disk you created for SQL logs, and so on. On the TempDB tab, configure the Data directories and Log directory field with the path to the SQL Temp disk.
On the Server Configuration tab, select Mixed Mode (SQL Server authentication and Windows authentication), and enter credentials for a user account that will be part of the SQL Server administrators.

Repeat the procedure for each of the three other SQL Server VMs. Ensure SQL installation paths are identical for each for four SQL Server VMs in the WSFC. An unattended installation is possible using the ConfigurationFile.ini file generated from the SQL Server installation on the first server.

Now we have a WSFC with four SQL Server nodes.

We are now ready to create the database and configure an Always On availability group for the VMware Identity Manager database.

Create the VMware Identity Manager Database

In this procedure, you create the database in Site 1 and make a backup. You also create the horizon login user.

To create the database and login user:

1. Log in to Microsoft SQL Server Management Studio as the sysadmin or as a user account with sysadmin privileges.
2. Connect to the first SQL Server in Site 1.
3. Follow the procedure provided in the product documentation to create a new saas database for VMware Identity Manager, along with a login user named horizon.
   See Create the VMware Identity Manager Service Database. This provides a script with SQL commands you must run to create the database and login user.
   
   **Note:** The default database name used in the script is saas. The default login user name is horizon. You can modify the script to use different names, but if you use a different name, write the name down.
4. After the database has been created, right-click the saas database (or, if you modified the database script to use a different name, select that name) and select Tasks > Back Up to create a full backup.
5. Use SQL Server Configuration Manager on each SQL Server to set the default port for all IPs to 1433.
   a. Under SQL Server Network Configuration, right-click Protocols for <Instance-name> in the left pane, and double-click TCP/IP in the right pane.
   b. In the TCP/IP Properties dialog box, on the IP Addresses tab, scroll down to the IP All section.
   c. Set TCP Port to 1433.

Sync the Database Account Across the Availability Group Replicas

It is important for us to have consistent SQL Server configurations across Always On availability group nodes because we need database logins to be able to connect to the database after failover.
Consistency across the SQL Server cluster nodes can be ensured through scripts, stored procedures, or manual commands. In this example, the focus is on ensuring account synchronization only.

In this reference architecture, we leveraged `Copy-DbaLogin` and `Sync-DbaSqlLoginPermission` commands to ensure consistency across both SQL Server instances. These are a part of the `dbatools` PowerShell module available on GitHub.

1. Ensure that `dbatools` is installed on all SQL servers.
   
   **Note:** To install `dbatools`, you can open PowerShell and enter the following command:
   
   ```powershell
   install-module -Name dbatools
   ```

2. Use the `copy-dbalogin` and `sync-dbaloginpermission` cmdlets to synchronise SQL Server instances:

   **Syntax:**
   ```powershell
   Copy-DbaLogin -source <SQL_server> -Destination <SQL_server>
   ```
   
   Where the `source` server is the SQL Server instance where the IDM SQL Server account was created, and the `destination` server is the additional SQL Server Always On replica server we plan to use in the Always On availability group.

3. Use the `Sync-DbaSqlLoginPermission` PowerShell command to sync account permissions across all Always On instances.

   **Syntax:**
   ```powershell
   Sync-DbaSqlLoginPermission -source <SQL_server> -Destination <SQL_server>
   ```

4. Run `copy-dbalogin` and `sync-dbaloginpermission` from the source server to each of the replica servers.

### Create and Configure the Availability Group

In this procedure, you create an Always On availability group, add the SQL Server from Site 1 as the primary replica, and add the other three SQL Server instances as secondary replicas. Replication between both SQL Server instances in the Site 1, where the primary node resides, will be synchronous and have automatic failover. Replication between the secondary-site nodes in Site 2 will be asynchronous, with manual failover.

To create the availability group:

1. In preparation for creating the availability group listener, choose a listener name and obtain a corresponding static IP address for Site 1 and a static IP for Site 2. For example, in this reference architecture, the listener name is `idm-agl`, to designate VMware Identity Manager availability group listener.
2. In Site 1, in the Management Studio, right-click **Always On High Availability** in the left pane, and select **New Availability Group Wizard**.

3. Complete the New Availability Group wizard, using the following guidelines:
   - **Specify Name** page – Use the name that you selected in Step 1.
   - **Select Databases** page – Select the check box for the VMware Identity Manager database; for example, **saas**.
   - **Specify Replicas > Replicas** tab – The cluster instance from Site 1 should already be listed. Click **Add Replica** to connect to and add the cluster instance from Site 2.
     - **Specify Replicas > Backup Preferences** tab – Select **Any Replica**. The two server instances are listed and they both have a backup priority of 50 (out of 100).
     - **Specify Replicas > Listener** tab – Select **Create an availability group listener**, enter the listener name, set the port to 1433, and click **Add** to add the IP addresses of the two IP
After you complete these pages, the Validation page, the Summary page, and the Results page take you through the process of creating the availability group, the listener, and adding the replicas.

When the process is complete, you can view the new availability groups using the Management Studio.

5. In Microsoft SQL Management Studio, connect to one of the SQL Server nodes in the WSFC and expand the availability groups. You can see that the availability group (idm-ag) with primary and secondary replicas.
6. Because the SQL Always On listener spans two sites and subnets, modify the parameters to change default behavior. Open a PowerShell prompt and use the following PowerShell commands to configure the listener:

   a. Use the Get-ClusterResource and Get-ClusterParameter cmdlets to determine the name of the resource (`idm-ag_agl-idm`) and its settings, as shown in the following example.

   ![PowerShell Command Example](image)

   b. Change the following settings:

      - Use `Set-ClusterParameter HostRecordTTL 120` to change `HostRecordTTL` to a lower value than the default in multi-site deployments. A generally recommended value is 120 seconds, or 2 minutes, rather than the default of 20 minutes. Changing this setting reduces the amount of time to connect to the correct IP address after a failover for legacy clients that cannot use the `MultiSubnetFailover` parameter.

      - Use `Set-ClusterParameter RegisterAllProvidersIP 0` to change `RegisterAllProvidersIP` to false in multi-site deployments. With this setting, the active IP address is registered in the client access point in the WSFC cluster, reducing latency for legacy clients.

   For instructions on how to configure these settings, see RegisterAllProvidersIP Setting and HostRecordTTL Setting. For sample scripts to configure the recommended settings, see Sample PowerShell Script to Disable RegisterAllProvidersIP and Reduce TTL.
c. Use `stop-clusterresource` and `start-clusterresource` to restart the `idm-agl_agl-idm` resource so that the new settings can take effect.

Now that the database is set up and the SQL Server Always On availability groups are configured, you can deploy and configure VMware Identity Manager to point to the Always On availability group for the database.

**Create a SQL Server Maintenance Job to Back Up the Database**

VMware recommends creating a SQL maintenance job that makes frequent backups of the Identity Manager transaction log. This job can truncate the transaction log, to guard against filling up the disk with log entries.

Database backup frequency is a matter of operational policy for your organization, but in the following procedure, we provide an example of a SQL maintenance job that backs up transaction logs for a SQL Always On database. These scripts use Ola Hallengren's `MaintenanceSolution.sql` script and the stored procedures and objects it generates. The `MaintenanceSolution.sql` script was run on the WSFC SQL servers prior to performing the following steps.

1. Verify the backup preference that is set on the SQL availability group for VMware Identity Manager database.
2. Launch Microsoft SQL Management Studio and log in to the primary SQL node (or secondary node, if the backup preference is set to this) using SA or the appropriate admin credentials.

3. Expand SQL Server Agent, right-click Jobs in the left pane, and select New Job.

4. Provide a Name for the job, set Category to Database Maintenance, and set Owner to SA. Click OK.

5. In the left pane, click Steps, and click New to open the Job Step Properties page, which is shown in the next step.

6. Provide a Step name and populate the Command pane with script that follows the screenshot.

```
EXECUTE [dbo].[DatabaseBackup]
@AvailabilityGroups = 'ag-idm',
@Directory = 'I:\Backups',
@BackupType = 'LOG',@Verify = 'Y',@CleanupTime = NULL,@CheckSum = 'Y',
```
@LogToTable = 'Y'

In the script:

- Replace ‘ag-idm’ with the name of your SQL Always On availability group. To back up all SQL availability groups on the server, replace ‘ag-idm’ with ‘ALL_AVAILABILITY_GROUPS’.
- Replace ‘I:\Backups’ with your backup path.
- To make a FULL backup instead of just backing up the transaction log, change the @BackupType to ‘FULL’.

7. In the left pane, click Schedule, click New, and complete the Job Schedule Properties page:
   a. Provide a Name and edit the schedule to suit your requirements.
   b. Click OK to close this Window.

This example schedule creates a new SQL agent job to back up transaction log of the VMware Identity Manager Always On database once every hour.

**Deploy and Set Up VMware Identity Manager Appliances**

For this reference architecture, we used the Linux-based VMware Identity Manager virtual appliance, which is a standard VMware virtual appliance, with all the usual deployment wizard prompts.

After deploying VMware Identity Manager instances, you point the appliance to the availability group listener you configured in the previous procedure. The VMware Identity Manager appliances reside in the DMZ within each site.

**Important:** As part of the following procedure, you will need to enter the fully qualified domain name (FQDN) of the global load balancer you are using (the VMware Identity Manager Service URL). Most administration tasks will be undertaken from the VMware Identity Manager administration console.
using the service URL (https://<global-LB-URL>/admin). At a minimum, you should also configure the local load balancer for Site 1.

Before starting the procedure, complete the load balancer prerequisites:

- Verify that you have set up the local and global load balancers according to the vendor’s instructions, that the FQDN for each load balancer is configured in DNS, and that each load balancer server is assigned a static IP address.

- On the global load balancer, obtain and install a TLS/SSL certificate. You can use a wildcard certificate or a Subject Alternate Name (SAN) certificate.

- On the local load balancer, install the TLS/SSL certificate described in the preceding bullet item. The VMware Identity Manager appliances must trust the certificate used. If not, the root from the Certificate Authority must be loaded in VMware Identity Manager. For more information see Installing Trusted Root Certificates.

- Configure the load balancer settings to enable X-Forwarded-For headers, increase the request timeout, and enable sticky sessions. For more information, see the topic Using a Load Balancer or Reverse Proxy to Enable External Access to VMware Identity Manager.

- To the local load balancer, add the FQDNs and IP addresses of the three VMware Identity Manager appliances you plan to create for Site 1.

If you are using F5, see Load Balancing VMware Identity Manager. This document provides instructions for integrating VMware Identity Manager nodes with the local load balancer. Also see Managing Horizon Traffic Across Multiple Data Centers with BIG-IP for guidance on how to implement global load balancing.

To set up VMware Identity Manager:

1. In vSphere Web Client, use the Deploy OVF Template wizard to deploy the VMware Identity Manager virtual appliance in Site 1.

   In the wizard, set a static IP address. See the topic Install the VMware Identity Manager OVA File. For network port requirements, see Deploying VMware Identity Manager in the DMZ.

   Note: In our example, the name of this first VMware Identity Manager appliance is s1-idm1 (s1-idm1.vmweuc.com). Make sure you specify the appliance’s FQDN in the Hostname field in the OVF Template wizard.

2. After deployment is complete, log in to the VMware Identity Manager browser-based console and follow the prompts to complete the Appliance Setup wizard.

   This involves entering the JDBC URL string and entering the credentials for the horizon database login user. The syntax of the JDBC URL is:

   jdbc:sqlserver://<hostname-of-availability-group-listener>;DatabaseName=saas;multiSubnetFailover=true

   Important: When deploying in a multi-subnet setup, be sure to add multiSubnetFailover=true as part of the JDBC connection string. This option enables faster failover. For more information, see MultiSubnetFailover Keyword and Associated Features.
**Database Connection Setup**

Database Type
- Internal Database
- External Database

JDBC URL: `jdbc:sqlserver://agl-idm.vmweuc.com;DatabaseName=saas,m`

*Consult documentation for supported JDBC URLs*

Database Username*

Database Password*

[Test Connection]

**Note**: When you test the connection, if you get a connection failed error, verify that you set the database port for all IP addresses to 1433, as described in Step 5 of "Create the VMware Identity Manager Database" on page 376.

For more information about the Appliance Setup wizard, see the topic Configure VMware Identity Manager Settings.

3. When the Setup Complete page appears, click the link on the page to continue with other VMware Identity Manager configuration tasks.

4. If you are not using a certificate from a trusted Certificate Authority, download the root certificate for the global load balancer and install it, as described in Installing Trusted Root Certificates.
5. Configure the VMware Identity Manager FQDN by using the FQDN of the top-level, global load balancer.

Important: You need a minimum of three VMware Identity Manager appliances in a cluster. We use a local load balancer for our pool of VMware Identity Manager appliances in Site 1 (s1-idm.vmweuc.com). We use another local load balancer for our pool of VMware Identity Manager appliances in Site 2 (s2-idm.vmweuc.com). We then use a global load balancer named my.vmweuc.com, which is in place above s1-idm and s2-idm.

For more information about configuring the FQDN, see the topic Modifying the VMware Identity Manager Service URL. As part of this procedure, after you change the FQDN to that of the global load balancer, you will enable the new self-service catalog UI.

6. If your load balancer requires to trust the certificate of the VMware Identity Manager nodes, copy the root certificate of the VMware Identity Manager appliance to the local load balancer, as described in Apply VMware Identity Manager Root Certificate to the Load Balancer.

Configure Failover and Redundancy for VMware Identity Manager

You use the VMware Identity Manager appliance you just created to create additional appliances in both Site 1 and Site 2. After giving each appliance its own IP address and DNS name, you configure the built-in Elasticsearch and Ehcache clusters.

1. Clone the VMware Identity Manager appliance twice, to create two clones of the VMware Identity Manager appliance in Site 1, as described in Configuring Failover and Redundancy in a Single Datacenter.

For our example, the original VMware Identity Manager appliance is named s1-idm1.vmweuc.com. The two clones for Site 1 are named s1-idm2.vmweuc.com and s1-idm3.vmweuc.com.

2. Give the cloned appliances static IP addresses and verify that an Elasticsearch cluster is created, as described in Assign a New IP Address to Cloned Virtual Appliance.

3. When all nodes are up and running, use the System Diagnostic Dashboard to verify that all nodes are using the same cluster ID. Also verify that Elasticsearch and Ehcache are up and run-
ning and everything else has a green status. If there are any issues, make sure to resolve these before moving on to deploying the second data center.

4. To provide site resilience, set up a separate cluster in the second data center. To implement this strategy, you must perform all the tasks described in: Deploying VMware Identity Manager in a Secondary Data Center for Failover and Redundancy.

5. Export the VMware Identity Manager appliance and use it to create a new cluster of three appliances in Site 2, as described in Create VMware Identity Manager Virtual Appliances in Secondary Data Center. Make sure to change the cluster ID on the three nodes in the second data center.

Change the VMware Identity Manager appliances in the secondary data center to read-only access. See Edit runtime-config.properties File in Secondary Data Center.

6. After all the nodes are up and running, make sure everything is green in the Systems Diagnostic Dashboard.

**Deploy and Set Up the Connectors Inside the Corporate Network**

After you set up the VMware Identity Manager instances inside the DMZ, you deploy four VMware Identity Manager Connectors inside the local area network (LAN)—two connectors in Site 1 and two connectors in Site 2. The connectors use the VMware Identity Manager’s built-in identity provider for load balancing.

There is no need for an external load balancer when using the built-in identity provider. The only authentication method that needs external load balancing of the connectors is Microsoft Active Directory Kerberos. The connectors sync users and groups from your enterprise directory to the VMware Identity Manager Service.

1. In preparation for establishing a connection to VMware Identity Manager Connectors, navigate to the global load balancer URL (https://<global-LB-URL>/admin), log in to the VMware Identity Manager administrative console, and generate an activation code for the two connectors you will create, using the connector names sl-idmconn1 and sl-idmconn2.
For instructions on generating the activation code, see the topic Generate Activation Code for Connector.

2. Deploy two VMware Identity Manager Connectors in Site 1.

You install the VMware Identity Manager Connector by running a Windows installation wizard on an already up and running Windows machine.

The VMware Identity Manager Connectors run inside your trusted enterprise network. For instructions, see the topic Deploying the VMware Identity Manager Connector.

**Important:** For this reference architecture, we used the Windows-based VMware Identity Manager Connector.

3. (Optional) To replace the TLS/SSL certificate for the VMware Identity Manager Connector, go to this URL: https://<FQDN>:8443/cfg/ssl.
4. Use the VMware Identity Manager administration console (at the global load balancer URL) to add a directory.
   a. Click the link on the Setup is Complete page, which is displayed after you activate the connector.
   b. On the Identity & Access Management > Directories tab, click Add Directory and select the type of directory you want to add.
   c. Follow the wizard prompts, and add the first connector (s1-idmconn1) as your Sync Connector.

Adding a directory allows VMware Identity Manager to sync users and groups from your enterprise directory to the VMware Identity Manager Service. For more information, see the topic Integrating Your Enterprise Directory with VMware Identity Manager.

<table>
<thead>
<tr>
<th>Add Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Directory Name</strong></td>
</tr>
<tr>
<td>Active Directory over LDAP</td>
</tr>
<tr>
<td>Active Directory (Integrated Windows Authentication)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Directory Sync and Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sync Connector</strong></td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td><strong>Directory Search Attribute</strong></td>
</tr>
<tr>
<td>Enter the account attribute that contains the user name.</td>
</tr>
</tbody>
</table>

**Note:** Create activation codes for all four connectors and deploy them. The result is that you will have four connectors—two in Site 1 and two in Site 2—and the sync connector will be the s1-idmconn1 connector in Site 1.

If the s1-idmconn1 connector ever becomes unavailable, you will need to select a different connector as the sync connector. If Site 1 has a failure event, you will need to select a connector in Site 2. For more information, see the topic Enabling Directory Sync on Another Connector in the Event of a Failure.

5. Enable the connectors’ authentication methods to operate in outbound-only mode.

For instructions, see the topic Enable Outbound Mode for the Connector. For more information, also see the topic Configure High Availability for Authentication.
At this point, we have

- 3 VMware Identity Manager appliances for Site 1: s1-idm1, s1-idm2, s1-idm3
- 1 load balancer virtual server for site 1: s1-idm
- 2 VMware Identity Manager Connectors for Site 1: s1-idmconn1, s1-idmconn2
- 3 VMware Identity Manager appliances for Site 2: s2-idm1, s2-idm2, s2-idm3
- 1 load balancer virtual server for site 2: s2-idm
- 2 VMware Identity Manager Connectors for Site 2: s2-idmconn1, s2-idmconn2
- 1 master load balancer virtual server: my.vmweuc.com

**Finalize Failover Preparation**

To complete the setup, follow the instructions provided in the following topics from Installing and Configuring VMware Identity Manager documentation:

- Configure Failover Order of Horizon View and Citrix-based Resources
- Clear Cache in Secondary Data Center

To perform a failover, refer to the following topics:

- Follow the steps in Failover to Secondary Data Center.
- Configure the VMware Identity Manager appliances in the secondary data center for read-write mode. See Promoting Secondary Data Center to Primary Data Center.
Troubleshoot Elasticsearch

The most common issue that arises when running a VMware Identity Manager cluster has to do with Elasticsearch health.

You can check the health of the Elasticsearch cluster using the System Diagnostic Dashboard, by monitoring `https://hostname/AUDIT/API/1.0/REST/system/health`, or, when logged in on console, you can run the following command:

```
curl 'http://localhost:9200/_cluster/health?pretty'
```

The command should return a result similar to the following.

```
{
"cluster_name" : "horizon",
"status" : "green",
"timed_out" : false,
"number_of_nodes" : 3,
"number_of_data_nodes" : 3,
"active_primary_shards" : 20,
"active_shards" : 40,
"relocating_shards" : 0,
"initializing_shards" : 0,
"unassigned_shards" : 0,
"delayed_unassigned_shards" : 0,
"number_of_pending_tasks" : 0,
"number_of_in_flight_fetch" : 0
}
```

If Elasticsearch does not start correctly or if its status is red, follow these steps to troubleshoot:

1. Ensure port 9300 is open between all nodes.
2. Restart Elasticsearch on all nodes in the cluster by running the following command:
   
   ```
   service elasticsearch restart
   ```

3. Check the logs for more details by running the following commands:
   
   ```
   cd /opt/vmware/elasticsearch/logstail -f horizon.log
   ```
Appendix D: Workspace ONE UEM Configuration for Multi-site Deployments

Use the procedures in this appendix to create SQL Server clustered instances that can fail over between sites and to set up a highly available database for VMware Workspace ONE® UEM. The following diagram shows the architecture.

![On-Premises Multi-site VMware Workspace ONE UEM Architecture](image)

The tasks you need to complete are grouped into the following procedures:

1. Create a Windows Server Failover Cluster
2. Configure Cluster Quorum Settings and Possible Owners for Each Cluster Instance
3. Install the SQL Server on each server in the Windows Server Failover Cluster
4. "Create the Workspace ONE UEM Database" on the next page
5. "Create the Workspace ONE UEM SQL Service Account and Assign Database Owner Roles" on page 394
6. "Sync the Workspace ONE UEM Database Account Across SQL Server Availability Group Replicas" on page 398
7. "Create an Always On Availability Group for the Workspace ONE UEM Database" on page 399
8. "Set Advanced Always On Availability Group Listener Parameters for Multi-site or Multi-subnet Failover" on page 404

For steps 1, 2, and 3, which involve creating a Windows Server Failover Cluster with Microsoft SQL Server, follow the procedures detailed in "Appendix F: Horizon 7 Active/Passive Service Using VMware vSAN Stretched Cluster" on page 429.
The rest of this appendix details the procedures that begin with step 4 in the preceding list.

**Create the Workspace ONE UEM Database**

After you finish creating the Windows Server Failover Cluster (WSFC), you are ready to create the database and configure an Always On availability group for Workspace ONE UEM.

1. Open SQL Server Management Studio and connect to your SQL Server database instance in Site 1.
2. Log in as the sysadmin or as a user account with sysadmin privileges.
3. Click **Connect**.
4. Right-click **Databases** and select **New Database**.
5. Enter `wsouemDB` as the database name.
6. Scroll to the right side of **Database files** section, select the ellipses (…) for the DATABASE file in the **Autogrowth** column, and in the dialog box:
   a. Change **File Growth** to **In Megabytes**.
   b. Set the size to **128**.
   c. Click **OK**.
7. Select **Options** in the left pane, set **Collation** to **SQL_Latin1_General_CS_AS**, and let other options use the defaults.

<table>
<thead>
<tr>
<th>Collation:</th>
<th>SQL_Latin1_General_CP1_CI_AS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery model:</td>
<td>Full</td>
</tr>
<tr>
<td>Compatibility level:</td>
<td>SQL Server 2016 (130)</td>
</tr>
<tr>
<td>Containment type:</td>
<td>None</td>
</tr>
</tbody>
</table>

8. Select **OK** to create the database.

9. Expand **Databases** and verify that the database is created.

**Create the Workspace ONE UEM SQL Service Account and Assign Database Owner Roles**

After you create the Workspace ONE UEM database, you must configure the SQL service account that will be used to connect to the Workspace ONE UEM database.

1. Open SQL Server Management Studio.
2. Log in to the database server that contains the Workspace ONE UEM database.
3. Navigate to **Security > Login**, right-click **Login**, and select **New Login** to give the account a login name.
4. Select whether to use your **Windows** account or the local **SQL Server** account for authentication.
5. If you select **SQL Server authentication**, enter the password to be used.
6. Select `wsouemDB` as the default database.
7. Navigate to the Server Roles page and select public as the server role.

8. Navigate to the User Mapping page and make the following selections:
   a. In the Users mapped to this login list, select wsouemDB, and in the Database role membership list, select the db_owner role.
   Important: The db_owner role must be selected for the SQL Server user account that
you plan to use for running the Workspace ONE UEM database script.
b. In the **Users mapped to this login** list, select the **msdb** database, and in the **Database role membership** list, select the **SQLAgentUserRole** and **db_datareader** roles.

---

**Sync the Workspace ONE UEM Database Account Across SQL Server Availability Group Replicas**

In this reference architecture, we leveraged `Copy-DbaLogin` and `Sync-DbaSqlLoginPermission` commands to ensure consistency across both SQL Server instances. These are a part of the `dbatools` PowerShell module available on GitHub.

1. Use the `Copy-DbaLogin` PowerShell command to sync the SQL wsouemDB account across all Always On instances.

   **Syntax:** `Copy-DbaLogin -source <SQL_server> -Destination <SQL_server>`

   Where the `source` server is the SQL Server instance where the Workspace ONE UEM SQL Server account was created, and the `destination` server is the additional SQL Server Always On replica server we plan to use in the Always On availability group.
2. Use the `Sync-DbaSqlLoginPermission` PowerShell command to sync account permissions across all Always On instances.

**Syntax:** `Sync-DbaSqlLoginPermission -source <SQL_server> -Destination <SQL_server>`

Where the *source* server is the SQL Server instance where the Workspace ONE UEM SQL Server account was created, and the *destination* server is the additional SQL Server Always On replica server we plan to use in the Always On availability group.

**Create an Always On Availability Group for the Workspace ONE UEM Database**

1. Open SQL Server Management Studio and connect to the server where the wsouemDB database was created.

2. Navigate to **Always On High Availability**, right-click, and select **New Availability Group Wizard**.
3. Give the availability group for the wsouemDB database a name; for example, wsouem-AG.
4. Select the **wsouemDB** database for the availability group.
   If you have not already done so, make a full backup of the database before you proceed.

5. Click **Add Replica** and enter the credentials of the additional SQL Server instance to join the availability group.
6. Configure synchronous replication with automatic failover for the primary and secondary replicas within Site 1, and configure asynchronous replication for the replicas in Site 2.

![Specify Replicas](image)

7. On the Listener tab select Create an availability group listener, enter the Listener DNS Name and Port, and click Add, to add the listener IP addresses.

**Note:** There are two subnets, one from each of site. Enter one unused IP address from each subnet. SQL Server will create the DNS record for the availability group listener.
8. On the Select Initial Data Synchronization page, select **Automatic Seeding**.

**Important**: Automatic seeding requires that data and log file paths be consistent across both availability replica SQL Server instances. If your configuration uses different data and log file paths, choose another data synchronization method.
Click **Next** and the Validation page, the Summary page, and the Results page take you through the process of creating the availability group, the listener, and adding the replicas.

When the process is complete, you can view the new availability groups using the Management Studio.

9. Expand the Availability Group in SQL Server Management Studio and verify settings.

![Availability Group in SQL Server Management Studio](image)

**Set Advanced Always On Availability Group Listener Parameters for Multi-site or Multi-subnet Failover**

1. Open a PowerShell prompt and use the `Get-ClusterResource` and `Get-ClusterParameter` cmdlets to determine the name of the resource (wsouem-ag_wsouem-agl) and its settings, as shown in the following example.

![PowerShell Output](image)
2. Change the `HostRecordTTL` to a lower value than the default using the following command:

   ```powershell
   Set-ClusterParameter HostRecordTTL 120
   ```

   A generally recommended value is 120 seconds, or 2 minutes, rather than the default of 20 minutes. Changing this setting reduces the amount of time to connect to the correct IP address after a failover for legacy clients that cannot use the `MultiSubnetFailover` parameter.

3. Use the following command to change `RegisterAllProvidersIP` to `false` in multi-site deployments:

   ```powershell
   Set-ClusterParameter RegisterAllProvidersIP 0
   ```

   With this setting, the active IP address is registered in the Client Access Point in the WSFC cluster, reducing latency for legacy clients.

For instructions on how to configure these settings, see `RegisterAllProvidersIP Setting` and `HostRecordTTL Setting`. For sample scripts to configure the recommended settings, see `Sample PowerShell Script to Disable RegisterAllProvidersIP and Reduce TTL`. 
4. Stop and restart the `wsouem-ag_wsouem-agl` resource so that the new settings can take effect. Enter the following commands:

```
stop-clusterresource
start-clusterresource
```

Now that the database is set up and the SQL Server Always On availability group is configured, you can deploy and configure VMware Workspace ONE UEM components to point to the Always On availability group for the database.
Appendix E: App Volumes Configuration

This appendix provides detailed instructions for configuring VMware App Volumes™ across multiple sites, implementing redundancy both within and across sites.

As is described in the Multi-site Design section of "Component Design: App Volumes Architecture " on page 172, the recommended deployment option for App Volumes across multiple sites is to use separate databases.

Configuration of the Non-Attachable Datastore and Storage Group

This design uses an NFS datastore to replicate AppStacks between sites. Though NFS is not a requirement, it provides low-cost storage replication that works with both VMware vSphere® VMFS and VMware vSAN™ implementations of VMware vSphere®.

To use this setup, perform the procedures described in the sections that follow:

1. “Configure a Non-Attachable NFS Datastore for Site 1 and Site 2” below.
2. “Create a Storage Group” on page 409.
3. “Replicate AppStacks from Site 1 to Site 2” on page 410.

Configure a Non-Attachable NFS Datastore for Site 1 and Site 2

Note: The screenshots in this section were taken from Site 1. The process was repeated for Site 2.

To configure a non-attachable datastore for replication purposes:

1. Use the App Volumes Manager console to configure a machine manager for the VMware vCenter Server®.

   App Volumes–managed storage locations are available based on the vCenter Server selected in the App Volumes machine manager configuration. For example, the following screenshot shows a machine manager configured for the vCenter Server whose host name is s1-vc-vdi.vmweuc.com.
2. Mount the NFS datastore to the hosts in the selected vCenter Server, to make them available as App Volumes managed storage locations.

For example, in the following screenshot, the NFS datastore AppVolumes-Unattached is added to vSphere hosts in the sl-vc-vdi.vmweuc.com cluster.
3. After the NFS datastore has been added to the vSphere hosts, select **Rescan** to make it available as a managed storage location.

![Managed Storage Locations](image)

4. Select the datastore, and select **Make As Not Attachable**. This option allows AppStacks to replicate to and from this datastore, but prevents AppStacks on this datastore from being mounted for use.

![Managed Storage Locations](image)

**Create a Storage Group**

Next, you create a storage group that includes one or more attachable datastores, and the non-attachable datastore, as shown in the following screenshot.
Figure 172. Creating a Storage Group

**Replicate AppStacks from Site 1 to Site 2**

After storage groups have been created on Site 1 and Site 2, you can import AppStacks for assignment at the secondary site, and you can replicate the AppStacks to the datastores that are members of the storage group. The following screenshot shows the **Import** and **Replicate** buttons you can use.

Figure 173. Import and Replicate AppStacks.
Configuration of Separate App Volumes Database Instances per Site

This design uses separate App Volumes database instances for each site. With this option, you can use SQL Always On availability groups within each site to achieve local high availability of the database. To make user-based entitlements for AppStacks available between sites, you must use a PowerShell script, which VMware provides. This setup is shown in the following figure.

To use this setup, perform the procedures in the following order:

1. "Create a Windows Server Failover Cluster in Each Site" below
2. "Install SQL Server 2016 Stand-Alone in All VMs" on page 413
3. "Create the App Volumes Databases and Enable Availability Groups for the Clusters" on page 415
4. "Create Always On Availability Groups for App Volumes Databases" on page 417
5. "Configure Cluster Quorum Settings" on page 421
6. "Install App Volumes to Use a Highly Available Database" on page 423

Create a Windows Server Failover Cluster in Each Site

A failover cluster is a group of VMs that have the same software installed on them and work together as one instance to provide high availability for a service, such as a Microsoft SQL Server database. If a VM, or cluster node, in the cluster fails, another node in the cluster begins to provide the service.

**Note:** For information about setting up F5 load balancers for use with App Volumes, see [F5 with App Volumes Configuration Guide](#). If you are using another type of load balancer, verify that you have set up this load balancer according to the vendor’s instructions.

To create a Windows Server Failover Clustering (WSFC) cluster:

1. On two ESXi hosts in Site 1, create and configure the two VMs that will be used as a clustered instance of Microsoft SQL Server, and then do the same in Site 2.
   - For this reference architecture, we used the Windows Server 2016 Standard operating system in the VMs that run SQL Server.
   - In this example, we named the VMs as follows: At Site 1, we created VMs named s1-sql4 and s1-sql5 on separate ESXi hosts. At Site 2, we created VMs named s2-sql4 and s2-sql5.
   - Set up each VM in the same way, with a total of five 20-GB hard disks: one disk for the Windows OS and five disks for the various types of SQL Server data.
Inside the OS, the disks are mapped to drive letters as follows.

2. In preparation for creating the failover cluster, choose a cluster name and obtain a corresponding static IP address for the cluster in Site 1 and in Site 2.

For example, in this reference architecture, for the cluster names, we use `s1-sqlclust-2` and `s2-sqlclust-2`.

3. To set up failover clustering on the SQL Server VMs, use Server Manager on each of the four VMs (two in Site 1 and two in Site 2), and use the Windows Server Add Roles and Features Wizard to add the Failover Clustering feature.

In the wizard, select to add the following features:
.NET Framework 3.5 features

Failover Clustering, including adding the Failover Clustering tools

For detailed instructions, see the Microsoft blog post Installing the Failover Cluster Feature and Tools in Windows Server 2012. One of the tools installed is the Failover Cluster Manager, which you will use for many of the steps that follow.

4. Use the Failover Cluster Manager to create a WSFC cluster that includes two SQL Server VMs in Site 1, and then do the same in Site 2.

For detailed instructions, see the Microsoft blog post Creating a Windows Server 2012 Failover Cluster, and see Create a Failover Cluster. The failover cluster for Site 1 includes the VMs s1-sql4 and s1-sql5. The cluster for Site 2 includes the VMs s2-sql4 and s2-sql5.

Install SQL Server 2016 Stand-Alone in All VMs

You install SQL Server Stand-Alone on each VM, rather than creating a SQL Server failover cluster. For App Volumes, you use stand-alone installations and then create Always On availability groups to achieve failover within a site.

To install SQL Server:

1. In Site 1, on the first SQL Server VM, complete the SQL Server installation wizard, using the following guidelines:
   - Feature Selection page – Select Database Engine Services and Management Tools - Basic.
   - Instance Configuration page – Select Default instance. The instance ID is MSSQLSERVER.
- **Server Configuration** page – The startup type is Automatic for the SQL Server Agent and SQL Server Database Engine.

- **Database Engine Configuration** page – On the Server Configuration tab, select Mixed Mode (SQL Server authentication and Windows authentication), and enter credentials for a user account that will be part of the SQL Server administrators. On the Data Directories tab, for each item, select the disk that you created for that type of file during VM creation. Use the following screenshot as a guide.

For more information about the setup wizard, see Install SQL Server from the Installation Wizard (Setup).

2. Repeat Step 1 to install SQL Server on the other VM in Site 1 and on the VMs in Site 2.

3. Create a shared folder on the first SQL Server VM in each site; for this example, the VMs are s1-sql4 and s2-sql4).
   a. Create a folder named Replication on the SQL_Binaries (E:) drive. You created this drive during Step 1 of "Create a Windows Server Failover Cluster in Each Site" on page 411.
b. Give the SQL service account full permissions on the folder.

Create the App Volumes Databases and Enable Availability Groups for the Clusters

This section provides detailed instructions for creating a highly available database but does not give recommendations regarding the sizing of the database for various sizes of deployments. For information about database sizing, see VMware App Volumes 2.x Database Best Practices.

To create the databases:

1. On first SQL Server VM in each site, use Microsoft SQL Server Management Studio to create an App Volumes database.

   For this example, the VMs are s1-sql4 and s2-sql4.
a. Log in to the Management Studio as the sysadmin or as a user account with sysadmin privileges.

b. Connect to the SQL Server instance on the VM, right-click the Databases folder, and select New Database.

c. Enter a database name and click OK.

For example, for Site 1, we named the database s1-appvolumes. For Site 2, we named the database s2-appvolumes.

2. Open SQL Server Configuration Manager and enable Always On availability groups for the Windows Failover cluster in Site 1 and Site 2.

For instructions, see Enable and Disable AlwaysOn Availability Groups (SQL Server).
The cluster names are the names you created in Step 2 of "Create a Windows Server Failover Cluster in Each Site" on page 411.

3. In each site, on the domain controller, open Active Directory Users and Groups, and create a new Computer object for the availability group.

For this example, for Site 1, the AD computer name for the group is s1-sqlclust2-ag1. For Site 2, the name is s2-sqlclust2-ag1.

Create Always On Availability Groups for AppVolumes Databases

In this procedure, you create an Always On availability group, adding the SQL Server stand-alone instances from Site 1 as the primary replica and secondary replicas. You then do the same for Site 2,
so that each site has its own Always On availability group to achieve automatic failover within each site (but not across sites).

To create the availability groups:

1. On the first SQL Server VM in Site 1, open the Management Studio, right-click **Always On High Availability** in the left pane, and select **New Availability Group Wizard**.

2. Complete the New Availability Group wizard, using the following guidelines:
   - **Specify Name** page – Use the name of the AD computer object you just created. For this example, the name is `s1-sqlclust2-ag1` for Site 1.
   - **Select Databases** page – Select the check box for the local database, which is `s1-appvolumes` in this example.
   - **Specify Replicas > Replicas** tab – The first SQL Server VM should already be listed. Click **Add Replica** to connect to and add the second SQL Server VM from this site.

   ![New Availability Group Wizard](image)

   **Important**: Select the **Synchronous Commit** and **Automatic Failover** check boxes. For the **Readable Secondary** setting, select **No** for the primary instance and **Yes** for the secondary instance.

   - **Select Data Synchronization** page – Select **Full**, and specify the shared **Replication** folder that you created in Step 3 "Install SQL Server 2016 Stand-Alone in All VMs" on page 413.
This share is used to synchronize the database on the secondary replica with that on the primary.

After you complete these pages, the Validation page, the Summary page, and the Results page take you through the process of creating the availability groups and listeners, and adding the replicas. On the Results page, you can see that the `s1-appvolumes` database is synchronized between both SQL servers.

When the process is complete, you can view the new availability groups using the Management Studio. The following screenshot shows the availability group with the primary replica on the `s1-sql4` VM.
The following screenshot shows the availability group with the secondary replica on the s1-sql5 VM.

3. Repeat Steps 1 and 2 for Site 2.
Configure Cluster Quorum Settings

At this point, you will configure cluster quorum settings to use a file share witness. Each element in a cluster can cast one “vote” to determine whether the cluster can run. Because you have two nodes in a cluster and you need an odd number of voting elements, create a file share quorum witness, which will cast the third vote. A file share witness is recommended when you need to consider multi-site disaster recovery with replicated storage.

To configure cluster quorum settings:

1. On a file server in each site, use Server Manager to open and complete the New Share wizard and create an SMB share, using the following guidelines:
   - **Select Profile** page – Select SMB Share – Quick.
   - **Share Location** page – For the share location, select Select by volume, and select the drive.
- **Permissions** page – Click **Customize permissions** and give the WSFC cluster object full control over the file share.

When you finish this step, you have two file shares: one for Site 1 and one for Site 2. For more details about accessing and using this wizard, see [12 Steps to NTFS Shared Folders in Windows Server 2012](#).

2. Configure the cluster quorum settings for each site:
   a. Open Failover Cluster Manager on the first VM in Site 1, right-click the cluster, and select **More Actions > Configure Cluster Quorum Settings**.
   b. Complete the Configure Cluster Quorum Wizard, using the following guidelines:
      - **Select Quorum Configuration Option** page – Select **Select the quorum witness**.
      - **Select Quorum Witness** page – Select **Configure a file share witness**.
      - **Configure File Share Witness** page – Enter the path to the file share you created in Step 1.
c. Repeat this procedure to set up a file share quorum witness in Site 2.

You are now ready to install App Volumes and point to the availability group we created.

**Install App Volumes to Use a Highly Available Database**

This procedure focuses on the specific settings required for connecting App Volumes to a highly available database. For details about other aspects of App Volumes installation, including system requirements, see the *VMware App Volumes Administration Guide*.

To install App Volumes:

1. In preparation for installing App Volumes and connecting to the availability group listener, use SQL Server Configuration Manager on each SQL Server VM to enable named pipes.

For instructions, see *Enable or Disable a Server Network Protocol*. 

---

For detailed instructions, see *Configure and Manage the Quorum in a Windows Server 2012 Failover Cluster*.
Important: Restart the SQL Server service so the new setting can take effect.

2. In Site 1, on the first VM on which you want to install App Volumes, download the App Volumes Manager installer, start the installation wizard, and follow the prompts to the Database Server page.

3. Complete the Database Server page, using the following guidelines:
   - **Choose local or remote database server to use** – Select the SQL Server Always On availability group listener that you created in "Create Always On Availability Groups for App Volumes Databases" on page 417.
   - **Name of database catalog to use or create** – Select the database that you created in "Create the App Volumes Databases and Enable Availability Groups for the Clusters" on page 415.

Important: If you see an error message such as the following one, it means you need to enable named pipes, as described in Step 1.
4. On the Choose Network Ports page, verify that the HTTP port is set to 80 and the HTTPS port is set to 443.

5. Follow the rest of the wizard prompts to complete the installation.

6. Repeat Steps 1–5 on the second App Volumes VM in Site 1, but on the Database Server page, be sure to leave the Overwrite existing database (if any) check box deselected. Both App Volumes Managers in Site 1 must point to the same highly available database.

7. Repeat this entire procedure in Site 2.

With App Volumes successfully installed, you can begin configuration. For detailed instructions see the VMware App Volumes Administration Guide. Also see the VMware App Volumes Reference Architecture.

The procedures in this appendix create a setup in which the App Volumes database can fail over automatically within each site. Site 1 and Site 2 have separate databases, but during a failover, users at Site 1 will be able to use replicated App Volumes AppStacks in Site 2 as long as the user entitlements are also replicated. For configuration details, see the next section, "PowerShell Script for Replicating App Volumes Application Entitlements" below.

PowerShell Script for Replicating App Volumes Application Entitlements

This script will append entitlements from the source server to the target server, but will not remove entitlements. The following summarizes the expected behavior:

- **Scenario**: User 1 is entitled to AppStack A in Site 1 (source server). AppStack A has been replicated to Site 2 (target server), but no entitlements exist.

  **Script behavior**: The script will add the User 1 entitlement to AppStack A at Site 2.

- **Scenario**: User 1 is entitled to AppStack B in Site 1 (source server). AppStack B has been replicated to Site 2 (target server). User 2 has been entitled to AppStack B at Site 2.

  **Script behavior**: The script will append the User 1 entitlement to AppStack B at Site 2. User 1 and User 2 are entitled to AppStack B at Site 2.

- **Scenario**: User 1 and User 2 are entitled to AppStack C in Site 1 (source server). AppStack C has been replicated to Site 2 (target server). The script has previously been run, so User 1 and User 2 are entitled to AppStack C at Site 1 and Site 2.

  **Script behavior**: Is as follows:

  - User 1 entitlement is deleted from AppStack C at Site 1.
  - The script does nothing. User 2 remains entitled to AppStack C at Site 1, and both User 1 and User 2 remain entitled to AppStack C at Site 2.

To use this script, you copy and paste the script, either to the database VM, to run the script locally on the server, or to another location, where you can run the script remotely as long as you have an account with the proper permissions and the machine meets the following software requirements:

- Windows Management Framework 4.0
- Microsoft .NET Framework 4.5
Next, open the script with a text editor and change the username, password, source server, and destination server to match your environment. These items are shown in bold text, in the first five lines of the following script. When you are finished, save the file with a .ps1 extension.

**Note:** The first two lines of the script are required for App Volumes version 2.14 and later.

```powershell

$Credentials = @{
    username = 'domain\username'
    password = 'password'
}

$SourceServer = "SourceServerFQDN"

$TargetServer = "DestinationServerFQDN"


Invoke-RestMethod -SessionVariable TargetServerSession -Method Post -Uri "https://$TargetServer/cv_api/sessions" -Body $Credentials


$TargetAppStacks = Invoke-RestMethod -WebSession $TargetServerSession -Method Get -Uri "https://$TargetServer/cv_api/appstacks"

foreach ($Assignment in $SourceAssignments)
{
    $SourceAppStack = $SourceAppStacks.Where({$_ -eq $assignment.snapvol_id})[0]
    $TargetAppStack = $TargetAppStacks.Where({$_ -eq $SourceAppStack.name})[0]
    Invoke-RestMethod -WebSession $TargetServerSession -Method Post -Uri "https://$TargetServer/cv_api/assignments?action_type=assign&id=$($TargetAppStack.id)&assignments%5B0%5D%5Bentity_type%5D=$($assignment.entityt)&assignments%5B0%5D%5Bpath%5D=$($assignment.entity_dn)"
}

**Next Steps: Installing and Setting Up Other App Volumes Components**

After installation is complete, you must perform the following tasks to start using App Volumes:
Complete the App Volumes Initial Configuration Wizard (https://avmanager).

Install the App Volumes Agent on one or more clients and point the agent to the App Volumes Manager address (load-balanced address).

Select a clean provisioning system and provision an AppStack. See Working with AppStacks in the VMware App Volumes Administration 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.

Next Steps: Additional Configuration Options for Writable Volumes

This section describes how you can configure writable volumes so that end users can determine how much free disk space is available in their writable volume. It also describes how you can expand the amount of disk space if necessary.

Allowing End Users to See the Size of Writable Volumes

Administrators can use the App Volumes Manager console to view the disk space remaining in writable volumes. Administrators can also allow end users to see how much disk space is available on their writable volume by looking at their system volume. To do this, administrators must create a new registry key during the App Volumes Agent configuration:

1. Navigate to HKLM\System\CurrentControlSet\Services\svdriver.
2. From this location, create a new registry key called Parameters.
3. Within the Parameters key, create a new key called ReportSystemFreeSpace with a DWORD value of 0 (zero).

Alternatively, you can run a command from an elevated CMD prompt to create the correct key and value:

```
reg add hklm\system\currentcontrolset\services\svdriver\parameters /v ReportSystemFreeSpace /t REG_DWORD /d 0
```

This change requires a reboot to take effect. Logging out or logging in does not apply the changes.
**End-User Viewing of Writable Volume Space**

When end users look at available disk space through Windows Explorer *before* you make the registry changes, they can see the free space and total space reported for the C: drive.

![Actual Free Space on C:\](image1)

*Figure 175: Actual Free Space on C:\*

After you make the registry modifications and reboot the system, the C: drive reports the amount of free space on the user’s writable volume, which is 9.41 GB total in the following example.

![Free Space on User Writable Volume](image2)

*Figure 176: Free Space on User Writable Volume*

Notice the total space still reflects the C: drive value.

Configuring the registry so end users can view free space on their writable volumes is recommended any time you use writable volumes.

**Expanding Writable Volumes**

If a user’s writable volume has reached or is about to reach full capacity, it can be expanded. To expand the writable volume for each user from the App Volumes Manager console:

1. Locate the user’s writable volume on the *Volumes* tab under the *Writables* sub-tab, and expand the information on the specific writable volume.
2. Click the *Expand Volume* option and enter a larger value in 1-GB increments.
3. Have the user log out and log back in. The additional size is added to the writable volume after the user logs out and back in. Also, the free-space usage is not reflected in the App Volumes Manager until the user logs out and back in.
One infrastructure option for providing site resilience is to use a stretched cluster that extends a VMware vSAN™ cluster across the two data sites.

This architecture is achievable with data centers that are near each other, such as in a metro or campus network environment with low network latency between sites. A stretched cluster provides both the data replication required and the high-availability capabilities to recover the server components, desktops, and RDSH servers.

This use case uses full-clone desktop VMs to address existing VMware Horizon® 7 implementations that use full-clone persistent desktops and cannot easily transition to a nonpersistent use case for various business reasons.

**Recovery Service Definition for a vSAN Stretched Cluster**

**Active/Passive Service**

**Requirement**: The management servers are pinned to a specific data center but can be failed over to a second data center in the event of an outage.

**Overview**: This service builds on the replication capability of vSAN and the high-availability (HA) features of VMware vSphere® High Availability when used in a stretched cluster configuration between two data centers. The required Horizon 7 server components are pinned to the VMware vSphere® hosts in one of the data centers using VMware vSphere® Storage DRS™ VM DRS groups, host DRS groups, and VM-Host affinity rules on the vSAN stretched cluster. vSphere HA fails them over to the second data center in the event of an outage.

Although the Windows component of the user service could be composed of full clones, linked clones, instant clones, or RDSH-published applications, this reference architecture shows full-clone desktop VMs. This strategy addresses existing Horizon 7 implementations that use full-clone persistent desktops. Use cases involving floating desktop pools or RDSH-published applications are better served by adopting the active/active or active/passive use cases previously outlined. These use separate Horizon 7 pods per site with Cloud Pod Architecture for global entitlements.

**Horizon 7 services accommodated**: Legacy full clones, Developer Workspace service. The overall RTO (recovery time objective) is between 15 and 30 minutes with an RPO (recovery point objective) of 15 to 30 minutes.
### Table 254: Active/Passive Service Requirements for a vSAN Stretched Cluster

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full-clone Windows desktop VMs</td>
<td>Persistent use case with 1:1 mapping of a VM to a user. VMs are replicated with a vSAN stretched cluster.</td>
</tr>
<tr>
<td></td>
<td>- RTO = 15–30 minutes</td>
</tr>
<tr>
<td></td>
<td>- RPO = 15–30 minutes</td>
</tr>
<tr>
<td>Native applications</td>
<td>Applications are installed natively in a base Windows OS. Applications are replicated as part of the full-clone replication process described earlier.</td>
</tr>
<tr>
<td>IT settings (optional)</td>
<td>VMware User Environment Manager™ IT configuration is replicated to another data center.</td>
</tr>
<tr>
<td></td>
<td>- RTO = 30–60 seconds</td>
</tr>
<tr>
<td></td>
<td>- RPO = 30–60 seconds</td>
</tr>
<tr>
<td>User data and configuration (optional)</td>
<td>User Environment Manager user data is replicated to another data center.</td>
</tr>
<tr>
<td></td>
<td>- RTO = 30–60 seconds</td>
</tr>
<tr>
<td></td>
<td>- RPO = Approximately 2 hours</td>
</tr>
</tbody>
</table>

**vSAN Stretched Cluster Blueprint for the Active/Passive Service**

This service uses stretched cluster storage to replicate both desktops and infrastructure components from one data center to the other. Only one data center is considered active, and in the event of a site outage, all components would be failed over to the other site as a combined unit.
**Architectural Approach for the Stretched Cluster Active/Passive Service**

This architecture relies on a single Horizon 7 pod with all required services always running at a specific site and never stretched between geographical locations. Only desktop workloads can run actively in both sites. The Connection Servers and other server components can fail over to Site 2 as a whole unit in the event of an outage of Site 1. This architecture relies on vSAN stretched cluster technology.

**vSphere Infrastructure Design Using vSAN**

The stretched cluster active/passive service uses Horizon 7 hosted on a vSphere 6.7 environment with a vSAN stretched cluster and storage between the two sites.

In the validation of this design, a vSAN storage environment was deployed as a vSAN stretched cluster to provide high availability and business continuity for the virtual desktops in a metro cluster deployment. The vSAN stretched cluster also achieves the high availability and business continuity required for the management server VMs.
To protect against a single-site failure in a metro or campus network environment with low network latency between sites, a stretched cluster can synchronously replicate data between the two sites, with a short RTO time and no loss of data.

vSAN does support active/active data sites with desktops and RDSH VMs active in both sites. Although these virtual desktops and Horizon 7-published applications can operate in active/active mode, the supporting management machines, and especially the Connection Servers, must all run within the one data center at a given time. To achieve this, the management servers should all be pinned to the same site at all times. Horizon 7 management services are deployed in an active/passive mode on a vSAN stretched cluster, failing over to the secondary site in the event of a site failure.

**vSAN Stretch Cluster Fault Domains**

A vSAN stretched cluster is organized into three fault domains, referred to as *preferred*, *secondary*, and *witness*. Each fault domain denotes a separate, geographically dispersed site.

- Preferred and secondary fault domains are data sites that contain an equal number of VMware ESXi™ servers, with VMs deployed on them.
- The witness fault domain contains a single physical ESXi server or an ESXi virtual appliance whose purpose is to host metadata. It does not participate in storage operations. The witness host serves as a tie-breaker when the network connection is lost. If the network connection between the preferred and secondary sites is lost, the witness helps make the decision regarding the availability of datastore components. The witness host cannot run VMs, and a single witness host can support only one vSAN stretched cluster.

![vSAN Stretched Cluster Configuration](image)

**Figure 179: vSAN Stretched Cluster Configuration**

In vSAN 6.6 and later releases, an extra level of local fault protection is available for VM objects in stretched clusters. When a stretched cluster is configured, the following policy rules are available for objects in the cluster:

- **Primary level of failures to tolerate (PFTT)** – For stretched clusters, PFTT defines the number of site failures that a VM object can tolerate. For a stretched cluster, only a value of 0 or 1 is supported.
- **Secondary level of failures to tolerate (SFTT)** – For stretched clusters, SFTT defines the number of additional host failures that the object can tolerate after the number of site failures defined by PFTT is reached. If PFTT = 1 and SFTT = 2, and one site is unavailable, then the cluster can tolerate two additional host failures. The default value is 0, and the maximum value is 3.

- **Affinity** – This rule is available only if PFTT = 0. You can set the Affinity rule to **None**, **Preferred**, or **Secondary**. This rule enables you to restrict VM objects to a selected site in the stretched cluster. The default value is **None**.

**Horizon 7 Pod and Blocks in a vSAN Stretched Cluster**

In the validation of this design, a single vSAN stretched cluster was used for both the management block and the desktop block.

One VMware vCenter Server® was deployed for the management servers and the desktop resources. Three ESXi hosts were deployed in Site 1 and Site 2, and a witness virtual appliance deployed in Site 3.

Figure 180: Horizon 7 on vSAN Stretched Cluster

**vSAN Network Requirements**

Connectivity between vSAN data sites and the witness site must obey strict requirements. Both layer-2 (L2, same subnet) and layer-3 (L3, routed) configurations are used in a vSAN stretched cluster deployment.

vSAN communication between the data sites can be over stretched L2 or L3 networks, and vSAN communication between data sites and the witness site can be routed over L3.

vSAN traffic between data sites is unicast for vSAN versions 6.6 and later (multicast for versions 6.5 and earlier). Traffic between a data site and the witness site is unicast.
A critical requirement for a vSAN stretched cluster is the amount of latency between sites. Latency between data sites should not exceed 5 ms RTT (2.5 ms each way).

Maximum latency between data sites and the witness site depends on the number of objects in the vSAN cluster. In general, latency between a data site and witness site can be a maximum of 200 ms RTT (100 ms each way), for up to a 10+10+1 vSAN configuration (preferred + secondary + witness nodes). For configurations greater than 10+10+1, VMware requires a latency of less than or equal to 100 ms (50 ms each way).

VMware recommends having 10-Gbps network bandwidth between data sites.

Bandwidth requirements between data sites and the witness site depends on the number of components in the vSAN cluster.

For more detailed information on how to calculate the required bandwidth for vSAN stretched cluster, see the vSAN Bandwidth Calculation page.

**vSphere Virtual Networking and vSAN**

A single instance of VMware vSphere® Distributed Switch™ was created with two 10-Gb interfaces in a team.

Four port groups isolate network traffic:

- Virtual machines
- ESXi management network
Quality of service is enforced with network I/O control (NIOC) on the distributed virtual switch, guaranteeing a share of bandwidth for each type of traffic.

A vmkernel interface (vmknic) is created on the ESXi management port group, vSphere vMotion port group, and vSAN port group.

**vSAN Stretched Cluster Example Configuration**

In this example, the virtual witness is connected over L3 and static routes. vSAN data sites 1 and 2 are connected over a stretched L2 network for the management network, vSAN network, vMotion network, and VM network.

Because the physical routers do not automatically route traffic between sites 1, 2, and 3, it is necessary to add static routes so that vSAN traffic from the preferred and secondary sites can reach the witness host and vice versa. It is also necessary to add static routes so that vCenter Server can reach the management network of the witness ESXi host.
Static routes are added using `esxcfg-route -a` command that you run on the ESXi hosts. Run this command on all ESXi hosts in the cluster, both in the data sites and on the witness host.

Static routes:

- Site 1 data nodes (VLAN11) to witness vSAN vmkernel Site 3 (VLAN21)
- Site 3 witness vSAN vmkernel (VLAN21) to Site 1 data nodes (VLAN11)
- Site 2 data nodes (VLAN11) to witness vSAN vmkernel Site 3 (VLAN21)
- Site 3 witness vSAN vmkernel (VLAN21) to Site 2 data nodes (VLAN11)
- vCenter Server to Site 3 witness management vmkernel (VLAN20)
- Site 3 witness management vmkernel (VLAN20) to vCenter Server

Configure the physical network switches to have IP routing enabled between the vSAN network VLANs on the data sites and the witness site, in this example VLANs 11 and 21. Once requests arrive for the remote host (either witness-to-data or data-to-witness), the switch will route the packet appropriately.

For more details on network requirements for vSAN, including detailed requirements for the management network, VM network, vMotion Network, and vSAN network, see [vSAN Stretched Cluster Network Design Considerations](#).

**Prerequisites and Settings for the vSAN Stretched Cluster Service**

This section provides specifications for designing the infrastructure of the active/passive service using a vSAN stretched cluster, including settings for vSAN, vSphere, distributed switches, and storage.
The following table details the vSAN prerequisites.

### Table 255: vSAN Prerequisites

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Three dispersed sites</td>
<td>• Two data sites, each with an equal number of ESXi hosts</td>
</tr>
<tr>
<td></td>
<td>• One witness site with a dedicated ESXi physical server or virtual appliance, per vSAN stretched cluster</td>
</tr>
<tr>
<td>Network requirements</td>
<td>Data site to data site:</td>
</tr>
<tr>
<td></td>
<td>• &lt; 5 ms latency round-trip time over 10 Gbps</td>
</tr>
<tr>
<td></td>
<td>• Layer-2 or layer-3 network</td>
</tr>
<tr>
<td></td>
<td>• Connectivity with Unicast</td>
</tr>
<tr>
<td>Witness site to data site:</td>
<td>• 100–200 ms latency, depending on vSAN configuration</td>
</tr>
<tr>
<td></td>
<td>• Layer-3 network</td>
</tr>
<tr>
<td></td>
<td>• Connectivity with unicast</td>
</tr>
</tbody>
</table>

The vSphere HA settings are summarized in the following table.

### Table 256: vSphere High Availability Settings

<table>
<thead>
<tr>
<th>Name of Setting</th>
<th>Setting to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere HA</td>
<td>Turn on vSphere HA</td>
</tr>
<tr>
<td>Host Monitoring</td>
<td>Enabled</td>
</tr>
<tr>
<td>Heartbeat Datastores</td>
<td>Disabled (default)</td>
</tr>
<tr>
<td>Virtual Machine Monitoring</td>
<td>Disabled (default)</td>
</tr>
<tr>
<td>Admission Control</td>
<td>Set to 50%</td>
</tr>
</tbody>
</table>
Table 256: vSphere High Availability Settings (Continued)

<table>
<thead>
<tr>
<th>Name of Setting</th>
<th>Setting to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failures and Responses</td>
<td>Power off and restart VMs</td>
</tr>
<tr>
<td>Datastore Heartbeats</td>
<td>Select <strong>Use datastores only from the specified list</strong> – Do not select any of the datastores</td>
</tr>
</tbody>
</table>

Settings for VMware vSphere Distributed Resource Scheduler are summarized in the following table.

Table 257: vSphere Distributed Resource Scheduler Settings

<table>
<thead>
<tr>
<th>Name of Setting</th>
<th>Setting to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere DRS</td>
<td>Turn on vSphere DRS</td>
</tr>
<tr>
<td>DRS Automation</td>
<td>Partially Automated</td>
</tr>
<tr>
<td>Power Management</td>
<td>Off</td>
</tr>
<tr>
<td>VMHost Groups</td>
<td>For management servers only:</td>
</tr>
<tr>
<td></td>
<td>Add new VMHost Groups:</td>
</tr>
<tr>
<td></td>
<td>- Name: <strong>Preferred-Site-Host</strong></td>
</tr>
<tr>
<td></td>
<td>◦ Add ESXi hosts from Site 1</td>
</tr>
<tr>
<td></td>
<td>- Name: <strong>Secondary-Site-Host</strong></td>
</tr>
<tr>
<td></td>
<td>◦ Add ESXi hosts from Site 2</td>
</tr>
<tr>
<td></td>
<td>Add new VM Group:</td>
</tr>
<tr>
<td></td>
<td>- Name: <strong>Management-VM-Group</strong></td>
</tr>
<tr>
<td></td>
<td>◦ Add vSphere and Horizon 7 management VMs</td>
</tr>
</tbody>
</table>
Table 257: vSphere Distributed Resource Scheduler Settings (Continued)

<table>
<thead>
<tr>
<th>Name of Setting</th>
<th>Setting to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VMHost Rules</strong></td>
<td>Add a new VMHost rule:</td>
</tr>
<tr>
<td></td>
<td>• Name: <strong>ManagementVMs-to-Preferred-Site</strong></td>
</tr>
<tr>
<td></td>
<td>• Type: <strong>Virtual Machines to Hosts</strong></td>
</tr>
<tr>
<td></td>
<td>• VM Group: <strong>Management-VM-Group</strong></td>
</tr>
<tr>
<td></td>
<td>For <strong>Must run on hosts in group:</strong></td>
</tr>
<tr>
<td></td>
<td>• Host Group: <strong>Preferred-Site-Hosts</strong></td>
</tr>
<tr>
<td><strong>vSphere HA Rule Settings</strong></td>
<td>VM to Host affinity rules: vSphere HA should respect rules during failover.</td>
</tr>
</tbody>
</table>

**vSAN Stretched Cluster Storage Policies**

For the vSAN configuration of 3+3+1, the following vSAN storage policies were used:

- Primary level of failures to tolerate (PFTT) = 1
- Secondary level of failures to tolerate (SFTT) = 1;
- Failure tolerance method = RAID-1 (Mirroring).

**Steps for Building vSAN Stretched Cluster Recovery Services**

This section covers the high-level steps required to build out the active/passive service (using a vSAN stretched cluster), which can be seen from a blueprint perspective in the following figure.

![Blueprint for a Stretched Cluster Active/Passive Service](image)
The following table outlines the steps required for creating a vSAN stretched cluster.

**Table 258: Steps for Configuring a vSAN Stretched Cluster Active/Passive Service**

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>Review the Stretched Cluster Design Considerations and ensure the prerequisites listed in &quot;Prerequisites and Settings for the vSAN Stretched Cluster Service &quot; on page 436 are met.</td>
</tr>
</tbody>
</table>
| Witnesses | - Deploy a vSAN witness appliance on a vSphere HA/DRS cluster in witness Site 3.  
- Set the static network routes, if required.  
- Add the vSAN witness appliance to vCenter Server as a standalone ESXi host.  
- See Deploying a vSAN Witness Appliance. |
| vSphere clusters | - Create the required vSphere stretched cluster by adding the ESXi hosts from Site 1 and Site 2.  
- Enable vSAN for the cluster.  
- Configure the fault domains and select the relevant witness hosts created earlier. |
| DRS and HA | Configure DRS and HA settings as listed in "Prerequisites and Settings for the vSAN Stretched Cluster Service " on page 436. |
| Affinity | To pin the management servers as a unit to a particular site, you must create VMHost groups and VMHost rules.  
See "Prerequisites and Settings for the vSAN Stretched Cluster Service " on page 436 for details. |
| Complete | - Configure Horizon 7 servers and the VM template for the virtual desktops.  
- Provision Horizon 7 full-clone desktops. |
**Table 259**: Steps for Creating the Windows Component of a vSAN Stretched Cluster Active/Passive Service

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load balancing</td>
<td>Verify both global and local load balancing are functional.</td>
</tr>
<tr>
<td>Master VM</td>
<td>Build out a master VM image in Site 1 to meet requirements.</td>
</tr>
<tr>
<td>Create desktop pool</td>
<td>Create a desktop pool based on the master VM image.</td>
</tr>
<tr>
<td>Entitlements</td>
<td>Entitle the users to the desktop pool as required.</td>
</tr>
</tbody>
</table>

**Note**: With regards to the environmental infrastructure design, including Active Directory, distributed file systems, load balancing, and DHCP, you can use the same design as is used for the multi-site active/active and active/passive use cases, as described in "Environment Infrastructure Design" on page 221.

**Reference Architecture Validation for the Stretched Cluster Service**

This section details the impact to both users and services during failure and the behavior after failover for all the services.

**Table 260**: vSAN Stretched Cluster Active/Passive Service Failure Impact

<table>
<thead>
<tr>
<th>Type of Access</th>
<th>During Failure</th>
<th>After Failover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logged-in user</td>
<td>Some sessions are terminated (depends on the location where the desktop is running).</td>
<td>N/A</td>
</tr>
<tr>
<td>New user logging in</td>
<td>User cannot log in.</td>
<td>After management services have resumed, users can log in as normal.</td>
</tr>
<tr>
<td>Access to user data</td>
<td>If the desktop is not disconnected, a full-clone user has access to data.</td>
<td>User has access to data.</td>
</tr>
</tbody>
</table>
Test/Recovery Plan for Active/Passive Horizon 7 Service Failover

For this test, a whole site failure was simulated for one of the data sites in a vSAN stretched cluster configuration consisting of Horizon 7 management server VMs and virtual desktops running on a vSAN stretched cluster.

Users were logged in to full-clone virtual desktops when the failure occurred.

Figure 185: Active/Passive Horizon 7 Service Failover Test/Recovery Plan on vSAN Stretched Cluster

The following table lists the preliminary tests and checks to be performed.
Table 261: Active/Passive on vSAN Stretched Cluster Preliminary Tests

<table>
<thead>
<tr>
<th>Test</th>
<th>Name</th>
<th>Description</th>
<th>Expectation</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Identify candidate site for simulated failure</td>
<td>Select the site where all management VMs are running.</td>
<td>Management machines are pinned to the data site using DRS affinity rules.</td>
<td>Site 1 selected</td>
</tr>
<tr>
<td>0.2</td>
<td>Verify virtual desktops are ready for test</td>
<td>Check full-clone pool deployed across desktop vSAN stretched cluster.</td>
<td>Full-clone virtual desktops are available for login across both sites.</td>
<td>As expected</td>
</tr>
<tr>
<td>0.3</td>
<td>Verify vSAN fault domain, HA, and DRS settings</td>
<td>Verify that vSAN is operating effectively, with no errors. Also, verify that vSphere HA and DRS are enabled and configured correctly to support vSAN site failover.</td>
<td>vSAN reports no issues with configuration. vSphere HA and DRS settings are optimal.</td>
<td>As expected</td>
</tr>
<tr>
<td>0.4</td>
<td>Users log in to virtual desktops</td>
<td>Have test users log in to full-clone virtual desktops; one in each of Site 1 and Site 2.</td>
<td>Users are logged in to full-clone virtual desktops in Site 1 and Site 2.</td>
<td>As expected</td>
</tr>
<tr>
<td>0.5</td>
<td>Prepare to record the time period of the failover</td>
<td>Prepare a timer device to record the time it takes for failover of services from Site 1 to Site 2.</td>
<td>Time source starts recording time when failover occurs.</td>
<td>As expected</td>
</tr>
</tbody>
</table>

The following list of tests includes descriptions of occurrences during a vSAN stretched cluster active/passive service failover, the recovery steps required, and the test results.
### Table 262: Active/Passive on vSAN Stretched Cluster Test Results

<table>
<thead>
<tr>
<th>Test</th>
<th>Name</th>
<th>Description</th>
<th>Expectation</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Site failure simulation initiated</td>
<td>Power is killed to all ESXi servers in Site 1: one server for management VMs, three servers for hosting desktops.</td>
<td>The ESXi server that hosts the management VMs goes offline. Full-clone virtual desktops in Site 1 are unavailable. Virtual desktop sessions to full-clone desktops in Site 1 are disconnected. Virtual desktop sessions to full-clone desktops in Site 2 are unaffected.</td>
<td>As expected</td>
</tr>
<tr>
<td>2.0</td>
<td>vSphere HA fails the management VMs over to Site 2</td>
<td>vSphere HA starts up management VMs (vCenter Server, Connection Servers in Site 2.</td>
<td>vSphere HA restarts the management VMs within 30 seconds.</td>
<td>vSphere HA restarts management VMs within 25 seconds. Management VMs show vSAN storage policy non-compliance.</td>
</tr>
<tr>
<td>2.1</td>
<td>vSphere HA fails over full-clone desktops to Site 2</td>
<td>vSphere HA starts up all full-clone desktops that had been running in Site 1 before failure occurred.</td>
<td>vSphere HA restarts virtual desktops.</td>
<td>vSphere HA powers on all virtual desktops in 2 minutes. Desktop VMs show vSAN storage policy non-compliance.</td>
</tr>
</tbody>
</table>
Appendix G: NSX Data Center for vSphere Configuration

This appendix provides an overview of the VMware NSX® Data Center for vSphere® deployment process.

NSX Data Center for vSphere Installation

This section outlines the NSX Data Center for vSphere installation steps. This guide is not intended to replace the NSX Data Center for vSphere documentation.

Before starting, the NSX Manager requires other infrastructure components to be in place and configured:

- VMware vSphere® clusters
- VMware vSphere® Distributed Switch™
- VMware vCenter Server® and Platform Services Controller™
- DNS – Forward and reverse lookups
- NTP
- Active Directory
- Static IP addresses

Follow the relevant section of the NSX Installation Guide to install all of the following components:

1. **Install and set up ESXi hosts and vCenter Server** – See VMware ESXi Installation and Setup.
2. **Deploy an NSX Manager for each vCenter Server** – See Install the NSX Manager Virtual Appliance.
3. **Prepare ESXi hosts in the vSphere clusters for the Distributed Firewall feature** – See Prepare Host Clusters for NSX.
4. **Configure Distributed Firewall rules** – See Distributed Firewall.
5. **Consider implementing user-based Distributed Firewall rules.** See Identity Firewall Overview.

Post-Installation Configuration

Perform the following tasks for each NSX Manager:

1. **Register the vCenter Server for the management cluster with NSX Manager** – See Register vCenter Server with NSX Manager.
2. **Verify that the NSX plug-in is installed in vSphere Web Client** – See Register vCenter Server with NSX Manager.
4. **Configure Syslog** – See Configure a Syslog Server for NSX Manager.
5. **Apply the license** – See Add and Assign a License.
6. **Exclude the vCenter Server from firewall** protection – See *Exclude Virtual Machines from Firewall Protection*.

7. **Prepare the vSphere cluster for NSX** – See *Prepare Host Clusters for NSX*.

8. **Assign administrators** – The Enterprise Admin role must be assigned for all relevant functions, including DFW – See *User Management*.

9. **Define a backup schedule for the NSX Manager** – See *NSX Backup and Restore*.

### Replacing Certificates

When you first install NSX, self-signed certificates are used. It is not recommended that you use these in production. At a high level, the steps for replacing the certificates on the NSX Managers are:

1. Create a certificate signing request (CSR) configuration file. This file is used to generate the CSR to request a certificate.

2. Once you receive the signed certificate, import it.

3. Configure the NSX Manager to use the signed certificate.

For the full process, see *NSX Manager SSL Certification*.
Authors and Contributors

Graeme Gordon is a Senior Staff End-User-Computing (EUC) Architect in End-User-Computing Technical Marketing, VMware.

Andreano Lanusse is a Staff End-User-Computing (EUC) Architect in End-User-Computing Technical Marketing, VMware.

Donal Geary is a Reference Architect Engineer in End-User-Computing Technical Marketing, VMware.

Caroline Arakelian is a Senior Technical Marketing Manager in End-User-Computing Technical Marketing, VMware.

Josh Spencer is a Senior Technical Marketing Architect in End-User-Computing Technical Marketing, VMware.

Peter Bjork is a Senior Staff End-User-Computing (EUC) Architect in End-User-Computing Technical Marketing, VMware.

Rick Terlep is a Senior Technical Marketing Architect in End-User-Computing Technical Marketing, VMware.

Roger Deane is a Director in End-User-Computing Technical Marketing, VMware.

The following people contributed to content in previous papers whose content has been subsumed into this paper.

- Shardul Navare, Senior Technical Marketing Architect in End-User-Computing Technical Marketing, VMware
- Camilo Lotero, Senior Solution Engineer in End-User-Computing, VMware
- Adarsh Kesari, Staff Solutions Architect in End-User-Computing, VMware

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