VMware Design Guide for Retail Branch Banking Transformation

Table of Contents

About Design Guides ................................................................. 3
  Introduction ................................................................. 3
  Audience ................................................................. 3
  Revisions and Additions .................................................. 3

Business Case ........................................................................ 4
  What Is the AlwaysOn Digital Workspace for Financial Services? ........................................ 5
  What Is the AlwaysOn Digital Workspace? ........................................................................ 5
  Availability ........................................................................ 5
  Mobility .............................................................................. 6
  Security .............................................................................. 6

AlwaysOn Digital Workspace Architecture ......................................................... 7
  Virtual Infrastructure Services .................................................. 8
  Single Data Center Design ...................................................... 9
  Dual Data Center Design ........................................................ 10
  Single Data Center Design in N+1 Configuration .................................................. 11
  Multiple Data Center Design in N+1 Configuration .................................................. 12

AlwaysOn Digital Workspace Supported Functions .......................................... 13

AlwaysOn Digital Workspace Availability Analysis ........................................... 15
  Virtual Application and Desktop Sessions .................................................. 15
  Virtual Infrastructure Services .................................................. 16

AlwaysOn Digital Workspace Service Redundancy Analysis ................................ 20
  AlwaysOn Virtual App/Desktop Cluster ........................................ 20
  AlwaysOn Digital Workspace Pod .............................................. 20
  AlwaysOn Digital Workspace Private Cloud Instance ........................................ 20
  AlwaysOn Digital Workspace Service .............................................. 20
  Storage Infrastructure ............................................................ 21
  View Connection Server ......................................................... 21
  Local Load Balancer .............................................................. 21
  Global Load Balancer .............................................................. 21
  VMware NSX for Horizon ......................................................... 21

AlwaysOn Digital Workspace Failure Scenario Analysis ..................................... 22

About the Author and Contributor ................................................................. 24
About Design Guides

VMware design guides are created through architectural design development and review by subject matter experts. The guides provide overviews of solution architectures and general implementation guidance. As a reference asset, each document illustrates a design framework to support proof-of-concept, pilot, and full implementations. In each case, customer-specific detailed design documentation should be developed.

Design guides incorporate generally available products into the design and employ repeatable processes for the deployment, operation, and management of components within the solution.

Design guides ensure the viability of logical designs or concepts in real-world practices. This document complements product specifications and installation guidelines published for each product. All detailed technical and functional product-level questions should be referred to the appropriate product documentation.

Introduction

Based on financial services requirements with a special focus on branch banking, this design guide provides an overview of the VMware AlwaysOn Digital Workspace solution, its logical architecture, and validation of the capabilities by VMware experts. Based on products from VMware, this architecture represents the foundation on which customers and partners can build comprehensive workspace solutions that require high availability for end-user-computing (EUC) services.

The term workspace refers to a software environment within which end users access and interact with one or more applications that they are entitled to access. A workspace includes a traditional Windows desktop, but it also includes browser applications and published applications.

The solution described here is not exclusive to the third-party products referenced within the architecture. Consult your VMware representative on how to implement this architecture with your preferred vendors and supported products. This document will be updated as newer capabilities are incorporated in the AlwaysOn Digital Workspace solution.

Audience

This document is for enterprise architects, solution architects, sales engineers, field consultants, advanced services specialists, and customers who plan to design, configure, and deploy an AlwaysOn Digital Workspace solution.

Revisions and Additions

This version of the VMware Design Guide for Retail Branch Banking Transformation includes the following additions and revisions as compared with Version 2.2.

- Functionality based on the VMware Horizon® 7 platform (including an RDSH application delivery platform)
- Incorporated VMware multi-site Horizon reference architecture white paper
- Incorporated VMware Identity Manager™ reference architecture white paper
- Added latest Cloud Pod Architecture (CPA) functionality
Business Case

Financial services organizations consider their distributed branches as a critical link in the customer relationship management chain. Similar to the retail industry, a bank branch must represent and deliver the entire portfolio of products and services, ranging from cash dispensing through ATMs to mortgage services.

However, branches present a unique set of challenges to IT infrastructure services:

- **Primary customer touch-point** – Directly impacts customer experience perception
- **Security a major concern** – Security ‘attack surface’ is very broad
- **Extreme cost of downtime** – Must meet very high uptime SLAs
- **Widely dispersed / small cluster of end users** – Large number of locations with small cluster of varied workflows (tellers, bankers, ATMs)
- **Low-bandwidth connectivity** – Highly limited communication bandwidth not suitable for multimedia and rich application experience
- **Total dependence on telecommunication infrastructure** – Any outage in the communication services renders the branch non-operational (limited DR)

These challenges combine to make end-user-computing services in branches one of the IT segments that is most in need of transformation.

In addition to solving these shortcomings, visionary CIOs are looking for ways to improve banker productivity, enhance customer experience, significantly reduce operating costs, and eliminate the nagging threat of cybersecurity breaches in branches. They are also looking for a new model to deliver end-user-computing services as part of acquiring new entities—the current model is too costly and takes too long to implement.

Bankers are looking for new ways to improve customer service and customer engagement at branches in an effort to grow revenue. A modern, secure end-user-computing solution drives a competitive advantage by giving bankers, relationship managers, and brokers, as well as customer service representatives, an “always on” and available desktop or workspace. With instant access to the right information at the right time, bankers can uncover new customer opportunities, review portfolios, make real-time decisions, and more effectively serve clients.

While banks are investing heavily in business continuity and disaster recovery, branches by their nature often are left out of the total scope of these projects. More holistic approaches to business continuity and disaster recovery are needed, especially when branches are the primary touchpoint and the face of the institution to the customer.

New branch solutions for managing end-user-computing services must be designed with an always-on capability built into the core architecture. The use of secure digital workspaces featuring virtual desktop technologies, and centralized desktop image and application management, is a modern solution for delivering and managing end-user-compute services at the branch.

A new on-premises, cloud-based model addresses all of these operational challenges and offers CIOs a platform to implement their next-generation end-user-computing vision. Without changing the existing telecommunication infrastructure, the solution enables new mobile workflows, eliminates data security risks, and offers lines of business much higher velocity in lifecycle management of applications for bankers.

The solution even offers a DR capability in the realm of branch connectivity to data centers. The latter would require tremendous additional investment if done through traditional upgrade of network infrastructure.
What Is the AlwaysOn Digital Workspace for Financial Services?
This design guide describes the underlying infrastructure to support the distinct workflows and use cases within a typical financial services branch operation. Specific use cases include:

- Teller workspace
- Mobile banker
- Banker station
- ATM image management
- Banking kiosk

Typical outcomes delivered by AlwaysOn deployments include:

- **Transform end-user compute at the branch** – Gain operational efficiencies by centralizing and automating desktop, application, and device management costs. Provide real-time application delivery and user management for all branch end users. Shift IT resources from lower-value tasks to higher-value service management.

- **Improve employee productivity and customer experience with mobile workflows** – Provide secure and efficient access to sensitive client portfolio data, investments, and trades—where and when customers need it. Enhance the customer experience by “taking the bank to the customer.” Improve employee retention, engagement, and productivity with BYOD—any app, any OS, any device.

- **Support business continuity with high availability of services** – Support remote branch locations with high levels of service and continuity of operations. Reduce unnecessary outages or disruption in service from failed software updates or device hardware failure. Provide continuous service to the branch with AlwaysOn Desktop design and multipath access to desktops or workspaces.

- **Secure data, stay compliant, and reduce risk** – Protect sensitive applications and restricted data by keeping them centralized within the data center. Immediately apply software updates and security patches to protect the edge from malware or cyber threats. Ensure compliance in the U.S. with the Financial Industry Regulatory Authority (FINRA) and the Gramm-Leach-Bliley Act through policy and role-based access control with a complete audit trail—logging and reporting. Reduce risk by tracking, locking, and remote wiping compromised or lost devices.

The AlwaysOn Digital Workspace for Financial Services delivers several operational benefits as compared with legacy end-user management practices. These benefits are described in the next section.

What Is the AlwaysOn Digital Workspace?
VMware AlwaysOn Digital Workspace is a complete, end-to-end solution for a private (on-premises) cloud infrastructure for virtual applications and desktops based on the VMware Identity Manager platform. The solution offers critical capabilities in three areas:

- Availability
- Mobility
- Security

**Availability**
In support of more flexible work environments, the AlwaysOn Digital Workspace solution incorporates end-to-end redundancy as the primary design premise for delivering non-stop service availability. By providing high resilience through redundancy, the solution eliminates potential single points of failure in delivering the workspace experience to end users.

The system delivers a Windows desktop to each end user by selecting from multiple available paths to access virtual desktop cloud(s) running in the data centers. If a path becomes unavailable due to component outages or planned maintenance, the system intelligently routes around the unavailable component or path and maintains delivery of desktop services to the organization’s end users.
Mobility

Desktop mobility that delivers immediate access to information is a core capability of the platform. As end users move from device to device and across locations, the AlwaysOn Digital Workspace solution securely reconnects end users to the workspace and virtual desktop instances that they are already logged in on, even when they access the organization from a remote location through the firewall.

From an end user’s viewpoint, this functionality is sometimes referred to as a “follow-me desktop.” This type of session persistence can yield significant employee benefits and productivity gains because it allows users to move across devices and between locations while keeping their desktops and applications in the same state.

Security

Security is an ever-increasing concern for all organizations. The AlwaysOn Digital Workspace solution delivers single sign-on (SSO) authentication and policy management, in addition to integration with third-party products for proximity card access and multi-factor authentication. The solution also delivers added security measures for data in transit.

The solution includes the following security features:

• **Data loss prevention** – Communication between a client device and the Horizon virtual desktop infrastructure (VDI) is based on Blast Extreme or PCoIP protocols. Designed for real-time streaming of the graphical user interface (GUI), no data content is included in the communication stream to the user device. Therefore, traditional data protection measures, such as endpoint encryption, are not necessary. Similarly, loss of the end-user device has minimal security consequence because no data is locally stored or cached.

• **User authentication** – The AlwaysOn Digital Workspace solution is compatible with several authentication platforms designed to simplify the end-user experience. In addition to authentication based on VMware Identity Manager, the solution works with Active Directory and other third-party identity provider platforms. Proximity cards and smart cards can also be incorporated in the access framework for multi-factor authentication and single sign-on across Windows applications.

• **Antivirus protection** – The AlwaysOn Digital Workspace solution is compatible with most of the top antivirus protection platforms, such as Trend Micro, McAfee, Symantec, and Sophos. These platforms are capable of running their services in VMware vSphere® hypervisors, thereby offloading that task from the virtual desktops, which yields higher capacity and better virtual desktop performance.

• **Cybersecurity and compliance** – The solution significantly reduces risks due to zero-day vulnerabilities. Security patches can be applied to centrally managed “gold” images and become immediately available to end users’ virtual desktop sessions.

VMware Horizon 7 meets the following compliance standard requirements:

• PCoIP protocol is compliant with FIPS 140-2.
• VMware is SOC 2, Type I certified.
• Supports Criminal Justice Information Services (CJIS) 5.3.
• Supports PCI DSS version 3.0.
**AlwaysOn Digital Workspace Architecture**

At the core of AlwaysOn Digital Workspace architecture is the notion of multi-pathing. This concept ensures that each end-user request for a virtual application or desktop session can be fulfilled by at least two resources. By eliminating single points of failure, even if an entire instance of View in Horizon 7 becomes unavailable, end users are assured of getting a functioning session at all times. The following illustration shows this architecture at a high level.

Each instance of virtual app/desktop cloud is comprised of View desktops as well as RDSH hosts running published applications—in any combination based on capacity requirements. The instances are independent of each other and operate in an active-active mode. Incoming session requests are routed by the intelligent load balancer layer-2 network appliance based on pre-defined routing logic as well as service availability.

Active session states are shared across the instances through the Cloud Pod Architecture (CPA) functionality. This means that an end user with an existing active (logged-in) session is automatically routed to the instance with that session when accessing the environment.

The AlwaysOn Digital Workspace architecture can include multiple instances of virtual app/desktop clouds as determined by maximum CPA configuration. Each instance is made up of one or more View pods with a maximum size of 10,000 sessions per pod. Figure 2 illustrates the components within each pod.
Virtual Infrastructure Services
The AlwaysOn Digital Workspace design leverages a set of infrastructure services to provide end-to-end functionality. These services include:

- **VMware Identity Manager** – Unifying platform for global user authentication and entitlement. It includes an application catalog and conditional access policies.
- **VMware App Volumes™** – An application and user management platform.
- **VMware User Environment Manager** – Offers personalization and dynamic policy configuration across any virtual, physical, and cloud-based Windows desktop environment. It simplifies end-user profile management by providing organizations with a single, lightweight, and scalable solution that leverages existing infrastructure. User Environment Manager maps environmental settings (such as networks and printers), and dynamically applies end-user security policies and personalization.
- **CIFS File Shares** – Existing infrastructure for accessing and sharing files.
- **Microsoft Active Directory** – Existing LDAP infrastructure for authentication and access policies.

![Component Stack for a Single Horizon App/Desktop Pod](image)

The final configuration of each instance must be developed during the design phase. This architecture can be implemented in several ways as described in the following sections.
Single Data Center Design
The architecture can contain two instances in one data center.

**Figure 3: Single Data Center Design**
Dual Data Center Design

The architecture can be set up with two instances split between two data centers.
Single Data Center Design in N+1 Configuration

In this configuration, each app/desktop cloud instance is sized for 50 percent of the total required session capacity. In the event that any one of the instances becomes unavailable, the remaining two instances continue delivering service at 100 percent required capacity—resulting in no service outage and no capacity impact.

The advantage of the N+1 configuration is reduced hardware costs, since the total hardware required for 100 percent session redundancy is only 1.5X (as compared to 2X).

![Diagram showing Single Data Center N+1 Configuration](image)

*Figure 5: Single Data Center N+1 Configuration*
Multiple Data Center Design in N+1 Configuration

This design is an adaptation of the single data center N+1 configuration where Horizon instances are spread across multiple data centers. The advantage remains the same (that is, 1.5X hardware instead of 2X), however, this configuration also provides data center disaster recovery capability.

The same approach can be applied to the scenario where there are only two data centers: primary and secondary. In this case, the N+1 configuration would be comprised of two Horizon instances in the primary data center and one in the secondary data center. The design remains exactly the same, where all instances are in active state and delivering application and desktop sessions.

![Diagram of Multiple Data Center N+1 Configuration](image)

**Figure 6:** Multiple Data Center N+1 Configuration
AlwaysOn Digital Workspace Supported Functions

The following functions and associated products are incorporated in this design guide.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-user authentication</td>
<td>Three modes are supported:</td>
</tr>
<tr>
<td></td>
<td>• VMware Identity Manager (supports Active Directory and other identity provider platforms)</td>
</tr>
<tr>
<td></td>
<td>• Via Horizon Client (supports Active Directory)</td>
</tr>
<tr>
<td></td>
<td>• Via HTML5 browser (supports Active Directory)</td>
</tr>
<tr>
<td>Proximity card access</td>
<td>Imprivata OneSign. Two modes are supported:</td>
</tr>
<tr>
<td></td>
<td>• Active Directory authentication to VMware Identity Manager portal. Requires secondary authentication to access VMware Identity Manager portal.</td>
</tr>
<tr>
<td></td>
<td>• Active Directory authentication and launch Horizon Client. Single sign-on to entitled desktops and applications. Other third-party access products with similar functionality can be included.</td>
</tr>
<tr>
<td>Single sign-on (SSO)</td>
<td>Four modes are supported (in any combination):</td>
</tr>
<tr>
<td></td>
<td>• SAML integration within VMware Identity Manager portal</td>
</tr>
<tr>
<td></td>
<td>• HTML password vault accessed from VMware Identity Manager portal</td>
</tr>
<tr>
<td></td>
<td>• TrueSSO for Windows desktops accessed from VMware Identity Manager portal</td>
</tr>
<tr>
<td></td>
<td>• Imprivata OneSign Windows agent for Windows application sign-on</td>
</tr>
<tr>
<td>Application portal and catalog</td>
<td>Two modes are supported:</td>
</tr>
<tr>
<td></td>
<td>• VMware Identity Manager – Shows all applications entitled to authenticated end user</td>
</tr>
<tr>
<td></td>
<td>• Direct through Horizon Client – Shows all applications entitled to end user in Active Directory</td>
</tr>
<tr>
<td>Virtual desktop platform (VDI)</td>
<td>View in Horizon 7</td>
</tr>
<tr>
<td>Application publishing platform</td>
<td>RDSH in Horizon 7</td>
</tr>
<tr>
<td>Federated entitlement</td>
<td>VMware Cloud Pod Architecture (CPA)</td>
</tr>
<tr>
<td></td>
<td>• Enables multiple View pods to act as a single View environment for entitlement purposes</td>
</tr>
<tr>
<td></td>
<td>• Single URL for user access – Unified namespace when used with global load balancing</td>
</tr>
<tr>
<td></td>
<td>• Simplified administration – Global entitlement (entitle users across pods and pools)</td>
</tr>
<tr>
<td>Application management and</td>
<td>Multiple methods are supported (in any combination):</td>
</tr>
<tr>
<td>delivery</td>
<td>• VMware App Volumes in Horizon 7</td>
</tr>
<tr>
<td></td>
<td>• Directly installed in gold image(s)</td>
</tr>
<tr>
<td></td>
<td>• Via VMware Identity Manager as SaaS applications</td>
</tr>
<tr>
<td></td>
<td>• Via VMware Identity Manager as XenApp published applications</td>
</tr>
<tr>
<td></td>
<td>• As ThinApp® packaged applications:</td>
</tr>
<tr>
<td></td>
<td>- Via App Volumes in a View desktop</td>
</tr>
<tr>
<td></td>
<td>- In gold image in a View desktop</td>
</tr>
<tr>
<td></td>
<td>- As icon on VMware Identity Manager portal</td>
</tr>
<tr>
<td>COMPONENT</td>
<td>DETAILS</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Application isolation</td>
<td>VMware ThinApp (third-party products with similar capabilities are also supported)</td>
</tr>
<tr>
<td>User profile management</td>
<td>VMware User Environment Manager (third-party products with similar capabilities are also supported)</td>
</tr>
<tr>
<td>Storage platform</td>
<td>VMware vSAN™ (third-party storage platforms with similar capabilities are also supported)</td>
</tr>
<tr>
<td>Security and micro-segmentation</td>
<td>VMware NSX®</td>
</tr>
</tbody>
</table>

*Table 1: AlwaysOn Digital Workspace Functional Stack*
AlwaysOn Digital Workspace Availability Analysis
The availability analysis is described across two functional layers: Virtual Application and Desktop Sessions, and Virtual Infrastructure Services.

Virtual Application and Desktop Sessions
VMware Identity Manager functions as the primary entry point for all end users. Independent Horizon instances function in an active-active mode to service incoming requests for virtual desktop and application services. Using the VMware Cloud Pod Architecture (CPA) feature, these instances operate in unison and present a common (single namespace) interface to the end users.

Upon authentication via VMware Identity Manager, end users with already running desktop (View) or application (RDSH) sessions are automatically routed to their sessions. End users requesting new desktop (View) or application (RDSH) sessions are routed to the appropriate Horizon instance based on their policies in CPA.

In the event that one of the Horizon instances becomes non-responsive, the intelligent load balancer adjusts its routing logic and new incoming session requests are automatically sent to the other Horizon instance(s). This is the worst-case outage scenario, since each Horizon instance has built-in redundancies to handle various intra-instance component failures such as failures of Connection Servers, VMware vCenter Server®, physical hosts or clusters, and others.
Virtual Infrastructure Services

AlwaysOn Digital Workspace architecture uses several virtual infrastructure services as part of its operation (as shown in Figure 1). The following sections show how each of these services is designed with redundancy and fault-tolerance. This service is also available as a SaaS (off-premises) offering by VMware.

- **VMware Identity Manager** – Unifying platform for global user authentication and entitlement. It includes an application catalog and conditional access policies.

VMware Identity Manager consists of a redundant set of manager nodes and a SQL database implemented in a SQL AlwaysOn configuration, as shown in Figure 7. This design has built-in component and database redundancy for supporting a very-high-availability SLA.

![Figure 7: VMware Identity Manager AlwaysOn Configuration](image)

For the corresponding detailed technical information for implementing VMware Identity Manager on-premises in an AlwaysOn configuration, see [Configuring VMware Identity Manager for Multiple Data Centers](#).
• **VMware App Volumes** – An application and user management platform. App Volumes consists of a redundant set of manager nodes and a SQL database implemented in a SQL AlwaysOn configuration, as shown Figure 8:

![Diagram](image)

Figure 8: App Volumes Multi-Instance Configuration
This design has built-in component and database redundancy for supporting a very-high-availability SLA. Figure 9 shows App Volumes implemented across two physical data centers.

Figure 9: App Volumes Multi-Site Configuration
• **VMware User Environment Manager** – User Environment Manager offers personalization and dynamic policy configuration across any virtual, physical, and cloud-based Windows desktop environment. User Environment Manager does not require any database and all the user and application configuration information is maintained in a set of files stored in CIFS shares. As such, the overall availability of the User Environment Manager service is the same as the CIFS file storage infrastructure. For a reference architecture for a multi-site Horizon 7 implementation, including User Environment Manager, see the *VMware Horizon 7 Enterprise Edition Multi-Site Reference Architecture*.

• **Microsoft Active Directory** – A common infrastructure service for existing Windows-based workloads (desktops and servers). AD has built-in redundancy and fault tolerance. AD Domain Controllers are part of management blocks within each Horizon instance.

• **CIFS File Shares** – Similar to Active Directory, a CIFS-based file share service is a common infrastructure service with built-in redundancy and high availability across NAS/SAN and the associated fabric layer.
AlwaysOn Digital Workspace Service Redundancy Analysis

The AlwaysOn Digital Workspace design has three primary tenets.

- **Eliminate any single point of failure that can cause an outage in the service** – This design objective is accomplished by ensuring 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.

- **Configure virtual desktop pools to be nonpersistent (linked clones)** – The configuration allows the desktop service cloud to be managed as pools of homogenous virtual desktops without the complexity of managing user profiles or personas for every desktop. Any user can access any available virtual desktop pool based on entitlements and access policies.

- **Leverage the customer’s existing enterprise storage (NAS or SAN) environment** for storing persistent user data, such as profiles, data files, and Outlook cache, as well as enterprise desktop gold images. This data must be accessible from any of the Horizon instances.

The following sections examine and validate that the above design requirements are satisfied in the AlwaysOn Digital Workspace solution.

**AlwaysOn Virtual App/Desktop Cluster**

**Redundancy measure:** Multiple vSphere hosts are contained within each Horizon cluster.

In the event that a physical host goes down, other hosts in the cluster (also called a block) continue uninterrupted. The only impact of such an outage is a reduction in the concurrent session capacity of the cluster, measured by the virtual machine density of each host. Users with aborted sessions running on the malfunctioning host log back into the service to receive a new session. No reconfiguration is necessary, other than replacing the defective host.

**AlwaysOn Digital Workspace Pod**

**Redundancy measure:** Each pod includes at least two Horizon clusters (for both apps and desktops) and up to seven Connection Servers (five of which are always active).

In the event that a Horizon cluster becomes non-operational, the remaining cluster(s) continues to deliver full service. The Connection Servers in the pod work around the out-of-service cluster.

In the event that a Connection Server becomes unavailable, the other Connection Servers continue uninterrupted. Up to two (out of seven) Connection Servers can become unavailable before there is any impact to session request routing or brokering.

**AlwaysOn Digital Workspace Private Cloud Instance**

**Redundancy measure:** Many large implementations will have more than a single Horizon pod within an instance of AlwaysOn Digital Workspace. In such cases, service is still available in that instance, even if an entire pod becomes unavailable. The intelligent load balancer will be able to route new session requests to the other pod(s) in the instance.

**AlwaysOn Digital Workspace Service**

**Redundancy measure:** AlwaysOn Digital Workspace Service includes at least two private cloud instances.

In the event that one of the private cloud instances becomes non-operational or requires a planned outage, the remaining private cloud instance(s) continue to deliver full service. The global intelligent load balancer sends new requests to the functioning private cloud instance(s).
The AlwaysOn Digital Workspace solution can be designed so that private cloud instances can operate in either active-active or active-passive modes.

In active-active mode, loss of a private cloud instance in its entirety does not impact service availability, because the functioning private cloud instance(s) continues to operate independently.

In active-passive mode, loss of an active private cloud instance requires that the passive instance be promoted to active status, typically through a DNS update.

Storage Infrastructure

Redundancy measure: Using VMware vSAN technology enables the storage architecture for AlwaysOn Digital Workspace to be highly modular. This is ideally suited to the nonpersistent nature of virtual desktops in this solution.

Each vSAN datastore is limited to a single cluster of vSphere hosts. This means that the largest failure domain for a datastore is a single cluster. Additionally, since a vSAN datastore supports RAID configuration, at least two flash storage arrays must become defective before there is any impact on the cluster’s operation.

For implementation guidelines and best practices, see the vSAN Documentation.

View Connection Server

Redundancy measure: Each View pod supports up to seven Connection Servers that function as a single logical entity. Loss of a Connection Server does not impact the availability of the View pod.

For implementation guidelines and best practices, see the Horizon 7 Documentation.

Local Load Balancer

Redundancy measure: Each data center with an AlwaysOn Digital Workspace virtual cloud instance may include a redundant pair of local load balancers. In the event that one load balancer goes down, the other one continues to provide full service.

AlwaysOn Digital Workspace is agnostic to the load balancer platform. For implementation guidelines and best practices, see the vendor’s product documentation.

Global Load Balancer

Redundancy measure: The AlwaysOn Digital Workspace solution requires a redundant pair of global load balancers that provide a global namespace for all incoming desktop session requests. In the event that one load balancer is out of service, the other load balancer continues to provide full service.

For implementation guidelines and best practices, see the vendor’s product documentation.

VMware NSX for Horizon

Redundancy measure: Each NSX instance is bound to a single instance of VMware vCenter Server. Because AlwaysOn Digital Workspace has redundant vCenter Server instances, NSX is also redundant.

NSX is a layer of network security software in the vSphere platform for AlwaysOn Digital Workspace. It provides the capability to segregate desktop pools using security policies (also called micro-segmentation functionality).

For implementation guidelines and best practices, see the NSX Documentation.
### AlwaysOn Digital Workspace Failure Scenario Analysis

The following table lists potential failure scenarios and the associated impact.

<table>
<thead>
<tr>
<th>SCENARIO NUMBER</th>
<th>FAILURE SCENARIO</th>
<th>IMPACT ON DESKTOP SERVICE AVAILABILITY</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A vSphere host malfunctions and goes out of service</td>
<td>None</td>
<td>View sessions that are running on the malfunctioning host are lost. However, the affected end users get a fresh View session upon logging in again. The operation of the View cluster to which the vSphere host belongs continues as normal.</td>
</tr>
<tr>
<td>2</td>
<td>A VMware vCenter Server goes out of service</td>
<td>None</td>
<td>Existing View sessions continue as normal. Logged-out sessions are not refreshed, and over time the capacity of the associated pool is reduced to zero. This draw-down effect is transparent to users because new login requests bypass the affected pool.</td>
</tr>
<tr>
<td>3</td>
<td>A Connection Server goes out of service</td>
<td>None</td>
<td>Each View pod includes up to seven Connection Servers. In this failure scenario, the remaining Connection Servers take over the load of the failed unit.</td>
</tr>
<tr>
<td>4</td>
<td>A local drive in a vSAN cluster goes out of service</td>
<td>None</td>
<td>The vSAN data store is configured as a RAID array with built-in protection against failure of individual drives.</td>
</tr>
<tr>
<td>5</td>
<td>An entire View cluster goes out of service</td>
<td>None</td>
<td>AlwaysOn Digital Workspace architecture requires at least two clusters in each pod. In this scenario, the remaining cluster(s) continue normal operation. Total available session capacity is reduced by the size of the malfunctioning cluster.</td>
</tr>
<tr>
<td>6</td>
<td>A View private cloud instance is unavailable</td>
<td>None</td>
<td>AlwaysOn Digital Workspace architecture requires at least two View cloud instances. In this scenario, the remaining View private cloud instance(s) continues normal operation. Total available session capacity can remain unaffected in a 2N or N+1 configuration. Services such as App Volumes, User Environment Manager, and VMware Identity Manager, are available from any of the View instances.</td>
</tr>
<tr>
<td>7</td>
<td>Component outage in the App Volumes SQL database</td>
<td>None</td>
<td>The SQL Server database supporting the App Volumes service within a View instance has multiple levels of redundancy, such as RAID arrays and a high-availability cluster that protects against component failures causing outages.</td>
</tr>
<tr>
<td>8</td>
<td>App Volumes SQL Server goes out of service</td>
<td>None</td>
<td>App Volumes supports SQL Server AlwaysOn. In the event that one of the SQL instances is down, service fails over to the other instance.</td>
</tr>
<tr>
<td>9</td>
<td>An App Volumes Manager goes out of service</td>
<td>None</td>
<td>App Volumes infrastructure service includes multiple App Volumes Managers operating in redundant mode</td>
</tr>
<tr>
<td>SCENARIO NUMBER</td>
<td>FAILURE SCENARIO</td>
<td>IMPACT ON DESKTOP SERVICE AVAILABILITY</td>
<td>DETAILS</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10</td>
<td>VMware Identity Manager database is unavailable</td>
<td>None</td>
<td>VMware Identity Manager service is configured with SQL Server AlwaysOn where the database service automatically fails over.</td>
</tr>
<tr>
<td>11</td>
<td>An Imprivata OneSign virtual appliance goes out of service</td>
<td>None</td>
<td>Imprivata OneSign platform includes multiple (up to 10) virtual appliances for authentication services. The OneSign agent maintains a list of available appliances and rolls over to the next available appliance in this scenario.</td>
</tr>
<tr>
<td>12</td>
<td>A vSphere host running the View admin services goes out of service</td>
<td>None</td>
<td>Existing View sessions continue as normal. Logged-out sessions are not refreshed. Over time, the capacity of the associated View pool is reduced to zero. This draw-down effect is transparent to users, because new login requests bypass the affected pool.</td>
</tr>
</tbody>
</table>

Table 2: AlwaysOn Desktop Solution Failover Scenarios
About the Author and Contributor

Farid Agahi is a Senior End-User-Computing Technical Strategist at VMware and a member of the Office of the CTO Team. Farid has over 30 years of experience in large-scale end-user-computing, solution engineering, and IT transformation. For the past 7 years, Farid has been focused on working with VMware enterprise customers to design and execute their IT strategies to transform end-user-computing services. This work includes engineering specific solutions based on virtualization technologies and cloud computing platforms.

Tisa Murdock, Director of Industry Solutions, VMware contributed content and review to this document.