VMware AlwaysOn Desktop Design Guide

Version 2.1

WHITE PAPER

vmware®

Table of Contents

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 implementations. As a reference asset, each document illustrates a design framework to support proof-of-concept, pilot, and full implementations.

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 appropriate product documentation.

Introduction

This guide provides an overview of the VMware AlwaysOn Desktop 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 desktop solutions that require high availability for end-user computing (EUC) services.

The solution is not exclusive to the products described 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 Desktop 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 Desktop solution.

Business Case

Organizations across all industries recognize that a legacy desktop service model based on physical machines no longer meets their end users' increasing demands for mobility, device choice, security, and agility in application delivery and life cycle management. Moreover, as end-user productivity grows due to the increasing adoption of technology, the net cost of downtime in EUC services continues to increase as a result.

While virtual desktop technologies offer a highly desirable alternative for next-generation EUC services, the infrastructure delivering those services must be highly resilient. Resiliency requires a foundational architecture that is designed to eliminate planned and unplanned downtimes that impact end-user productivity.

In other words, next-generation EUC services must be designed with an always-on capability built into the core architecture. Enterprise IT architects must ensure that the selected solution has a built-in design for ultra-high availability. This design guide details a VMware solution that meets and exceeds these requirements.

What Is the AlwaysOn Desktop?

VMware AlwaysOn Desktop is a complete, end-to-end solution for a virtual-desktop, private (on-premises) cloud infrastructure based on the VMware Horizon® 6 platform. The solution offers critical capabilities in three areas:

- Availability
- Mobility
- Security

Availability
The AlwaysOn Desktop solution incorporates end-to-end redundancy as the primary design premise for delivering non-stop desktop service. By providing high resilience through redundancy, the solution infrastructure has no single point of failure.

The system delivers a Windows desktop to each end user by selecting from multiple available paths to access virtual desktop clouds running in the customer's data centers. If a path becomes unavailable due to component outages or planned maintenance, the system intelligently routes around all unavailable path and continues delivering desktop services to the enterprise.

Mobility
Desktop mobility is a core capability in the Horizon platform. As end users move from device to device and across locations, the AlwaysOn Desktop solution reconnects end users to the virtual desktop instances that they are already logged in on, even when they access the enterprise from a remote location through the firewall.

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

Security
Security is an ever-increasing concern in the EUC space. The AlwaysOn Desktop solution delivers single sign-on (SSO) authentication and policy management, in addition to integration with third-party products, using proximity cards. The solution also delivers added security measures for data in transit.

The solution includes the following security features.

- **Safe-harbor data protection** – Communication protocol between a client device and the View virtual desktop infrastructure (VDI) is based on PCoIP. Designed for real-time streaming of the graphical user interface (GUI), no data content is included in the PCoIP communication to the user device. Therefore, traditional data protection measures, such as endpoint encryption, are not necessary. Similarly, loss of the end-user device is no longer a security issue because no data is locally stored or cached.
- **User authentication** – The AlwaysOn Desktop solution is compatible with several authentication platforms designed to simplify the end-user experience. In addition to authentication based on VMware Identity Manager™, the AlwaysOn Desktop solution can also work with third-party platforms such as Imprivata OneSign. OneSign is capable of automatically launching access to the View virtual desktops upon user authentication. Using proximity cards for access, the OneSign component offers users tap-and-go functionality, which can yield significant workflow and compliance benefits, especially in healthcare use cases.
- **Antivirus protection** – The AlwaysOn Desktop 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 using VMware vShield™ APIs, thereby offloading that task from the virtual desktops, which yields higher capacity and better virtual desktop density.

AlwaysOn Desktop Industry-Specific Solutions

The AlwaysOn Desktop design can be configured and adapted to deliver specific solutions for healthcare (VMware AlwaysOn Point of Care™), financial services (AlwaysOn Branch Compute), education, and retail. These solutions can include third-party products to satisfy industry-specific use cases.

AlwaysOn Desktop Software Stack

The following functions and associated products are incorporated in the AlwaysOn Desktop design guide.

COMPONENT	DETAILS
End-user authentication and SSO	VMware Identity Manager (third-party products with similar capabilities are also supported)
Application portal	VMware Identity Manager
VDI platform	View in Horizon 6
Application delivery	VMware App Volumes™ (third-party products with similar capabilities are also supported)
Application isolation	VMware ThinApp® (third-party products with similar capabilities are also supported)
Profile management	VMware User Environment Manager™ (third-party products with similar capabilities are also supported)
Storage platform	VMware Virtual SAN™ (third-party storage platforms with similar capabilities are also supported)
Desktop pool security and segmentation	VMware NSX™

COMPONENT	DETAILS
Intelligent load balancer	BIG-IP Local Traffic Manager (LTM) and Global Traffic Manager (GTM) from F5 (products with similar capabilities are also supported)
Card-based authentication and SSO	Imprivata OneSign, either in conjunction with VMware Identity Manager for authentication or as an alternative to end-user authentication (third-party products with similar capabilities are also supported)

Table 1: AlwaysOn Desktop Software Stack

AlwaysOn Desktop Architecture and Topology

This design guide covers four separate designs for AlwaysOn Desktop:

- Option A: AlwaysOn Desktop with VMware Identity Manager
- Option B: AlwaysOn Desktop with VMware Identity Manager plus proximity card access platform
- Option C: AlwaysOn Desktop with Cloud Pod Architecture (CPA) and proximity card access platform, without VMware Identity Manager
- Option D: N+1 redundancy configuration for scenarios A and B

For easy reference, the following matrix shows the above design options:

	VMWARE IDENTITY MANAGER	CPA	PROXIMITY CARD ACCESS	N+1
Option A	Yes	No	No	No
Option B	Yes	No	Yes	No
Option C	No	Yes	Yes	No
Option D	Yes	No	No	Yes
	Yes	No	Yes	Yes

Table 2: AlwaysOn Desktop Design Options

The following sections describe the four design options, with each illustrated in two perspectives:

- **Logical stack** – Shows all layers in a typical implementation as well as interconnections between layers in terms of dependencies
- **Component-level architecture** – Shows products required within the layers identified in the logical stack

Option A: AlwaysOn Desktop with VMware Identity Manager

In this design, VMware Identity Manager functions as the primary entry point for all end users as shown in the following illustrations.

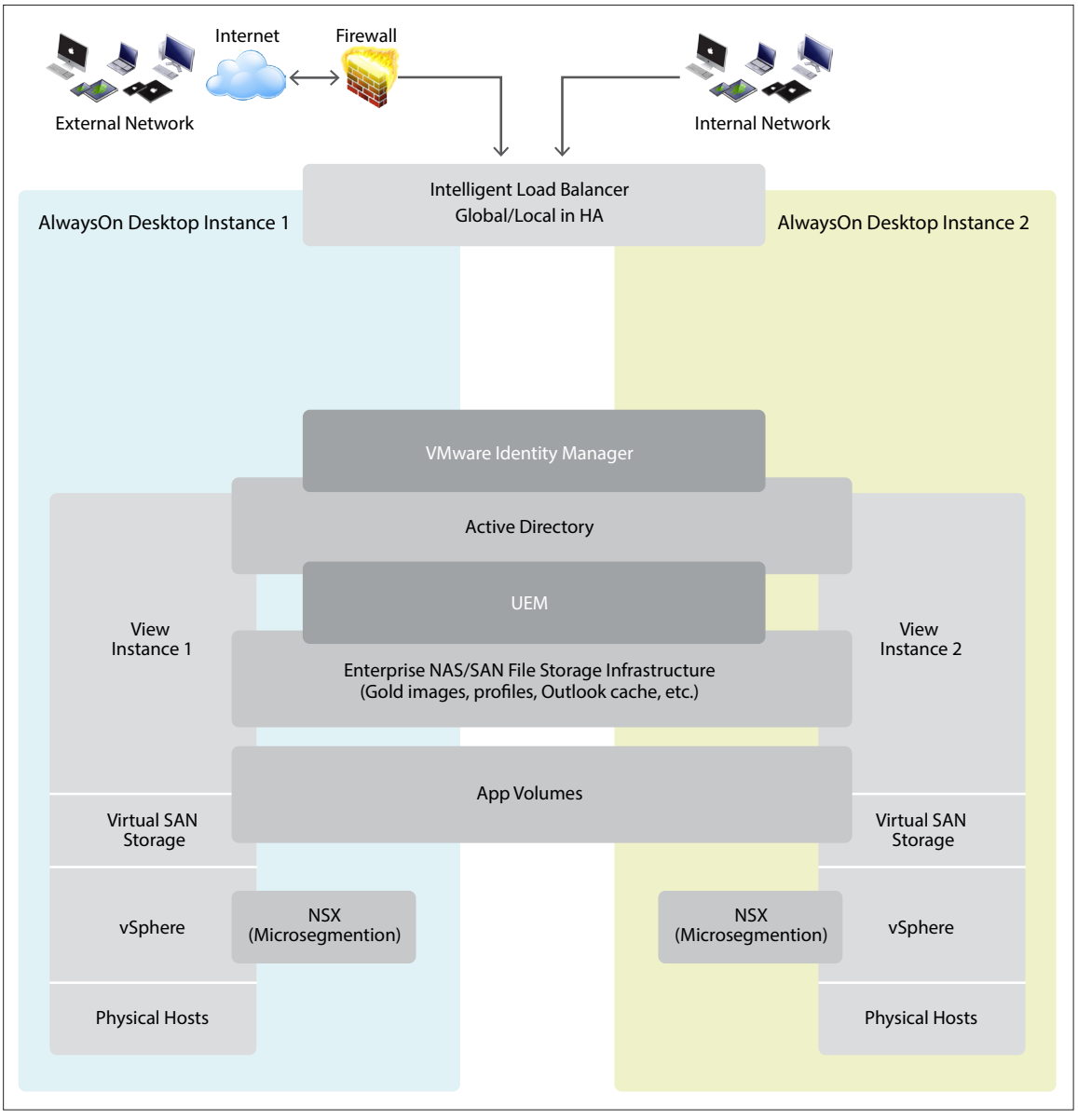

Figure 1: Logical Stack Based on VMware Identity Manager

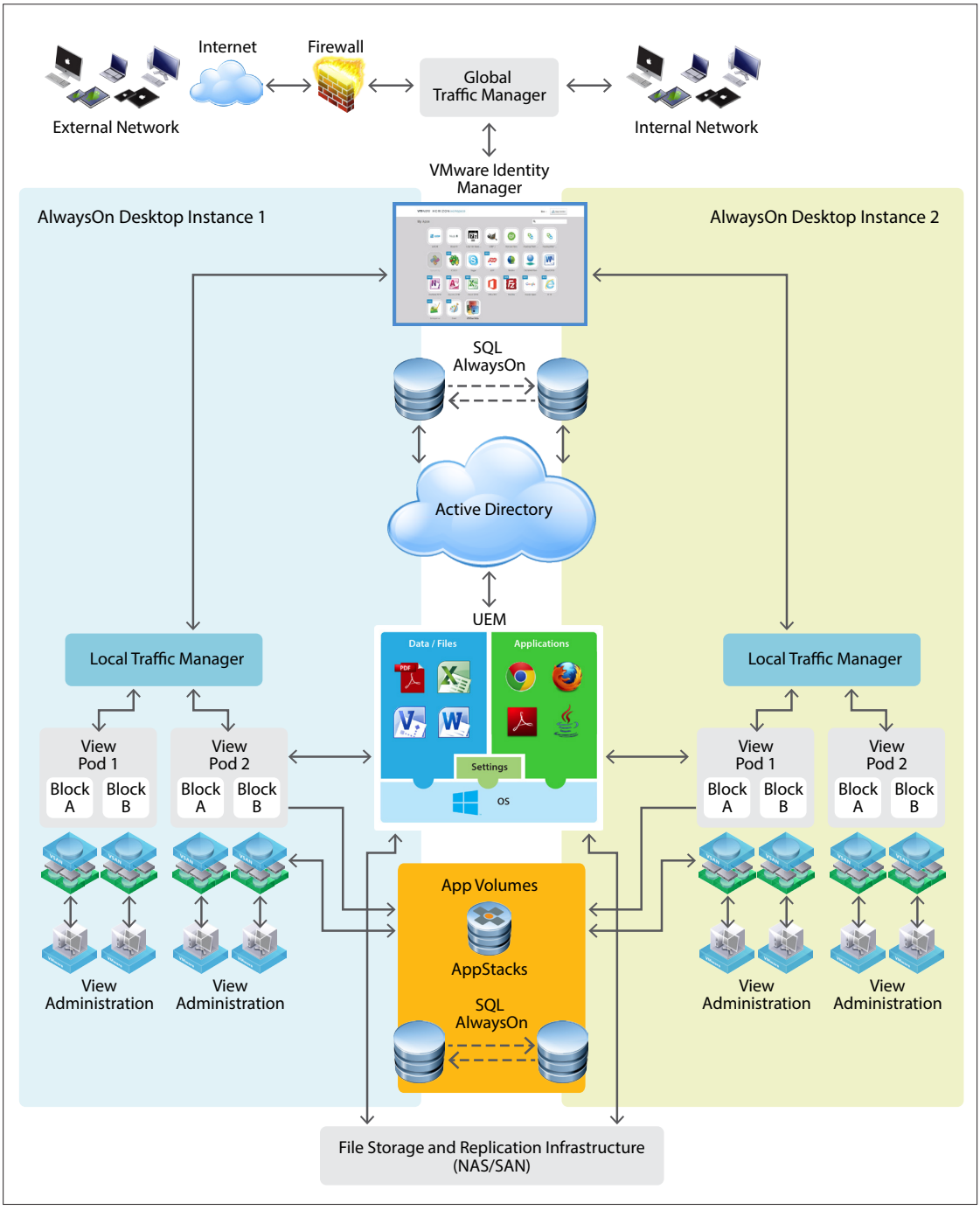

Figure 2: Component-Level Architecture – Minimum Topology for AlwaysOn Desktop with VMware Identity Manager

Option B: AlwaysOn Desktop with VMware Identity Manager Plus Proximity Card Access Platform
In this design a proximity card platform, such as Imprivata OneSign, functions as the primary authentication for end users. The platform logs into the user's respective VMware Identity Manager portal page as shown in the following illustrations.

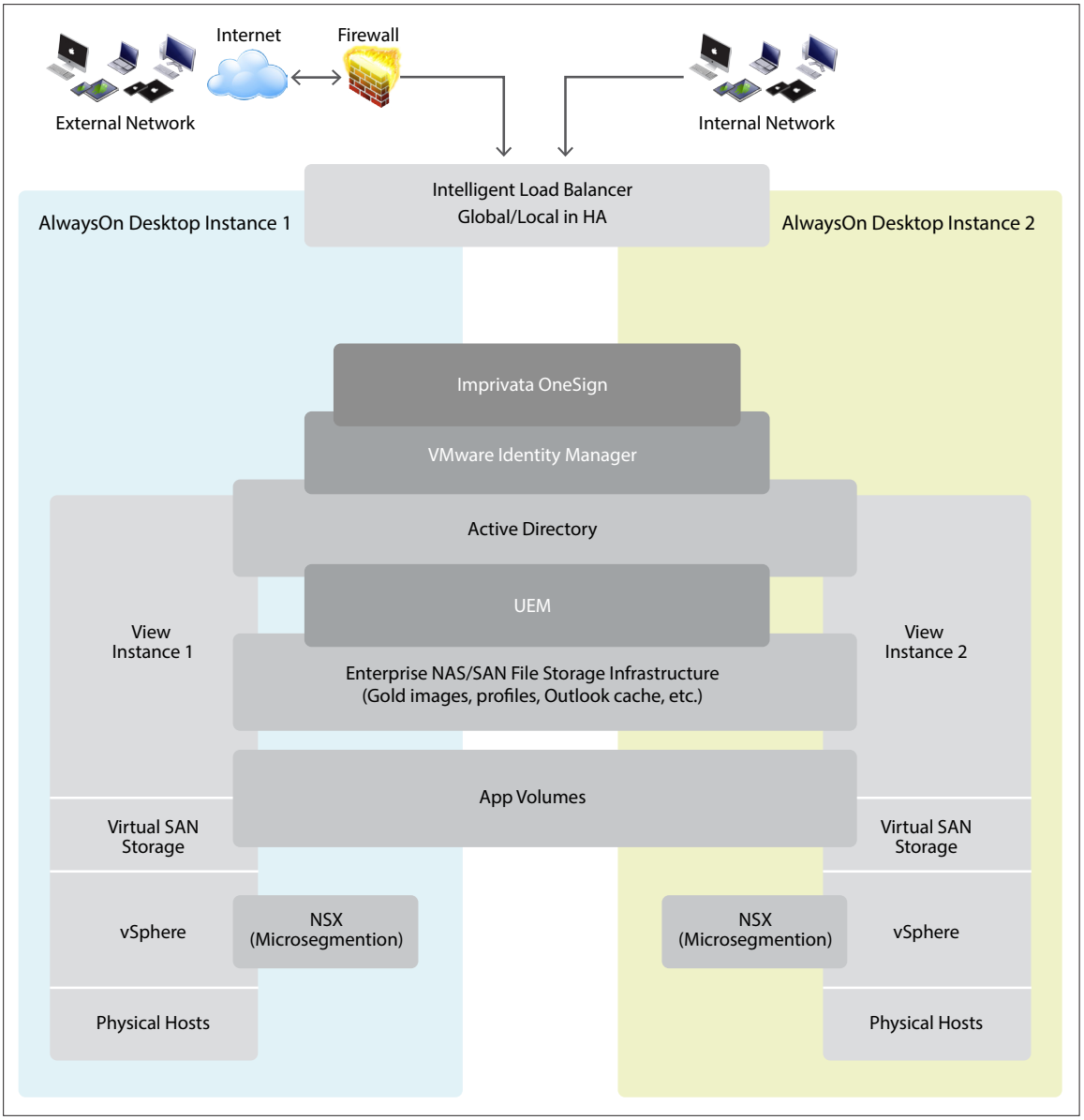

Figure 3: Logical Stack with Imprivata OneSign Platform for Proximity Card Access Plus VMware Identity Manager

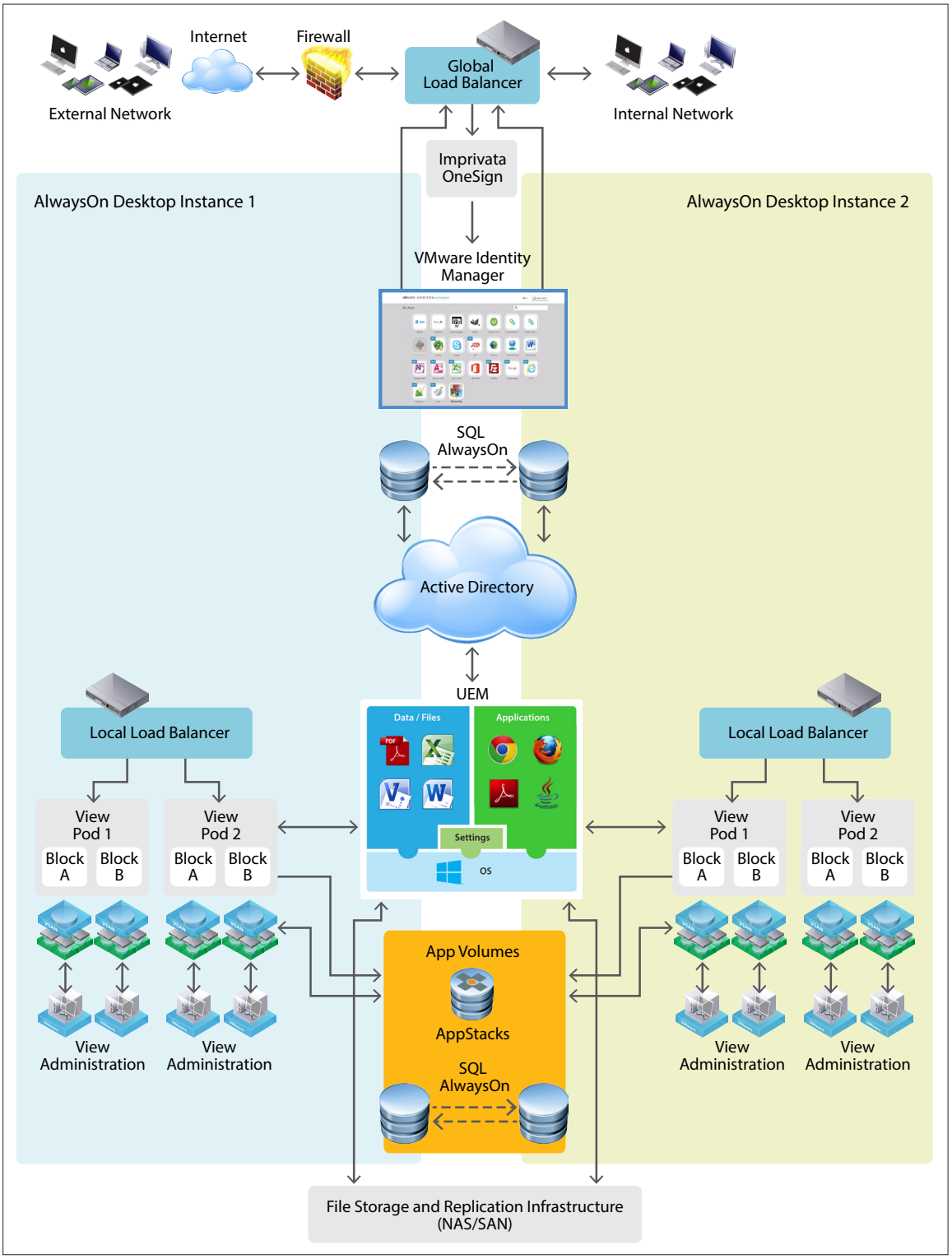

Figure 4: Component-Level Architecture – Minimum Topology for AlwaysOn Desktop with Imprivata OneSign for Proximity Card Authentication and VMware Identity Manager for Application Portal

Option C: AlwaysOn Desktop with Cloud Pod Architecture and Proximity Card Access Platform (Without VMware Identity Manager)

This design leverages proximity card access platforms such as Imprivata OneSign to function as the primary authentication mechanism for directly launching virtual Windows desktops.

This configuration takes advantage of Horizon Cloud Pod Architecture (CPA) functionality with the following key benefits:

- CPA enables View Pods to act as a single View environment – Pods are federated (they "know about each other").
- Single URL for user access – Unified namespace approach when used with global load balancing.
- Simplified administration – Global entitlement (entitle users across pods and pools).

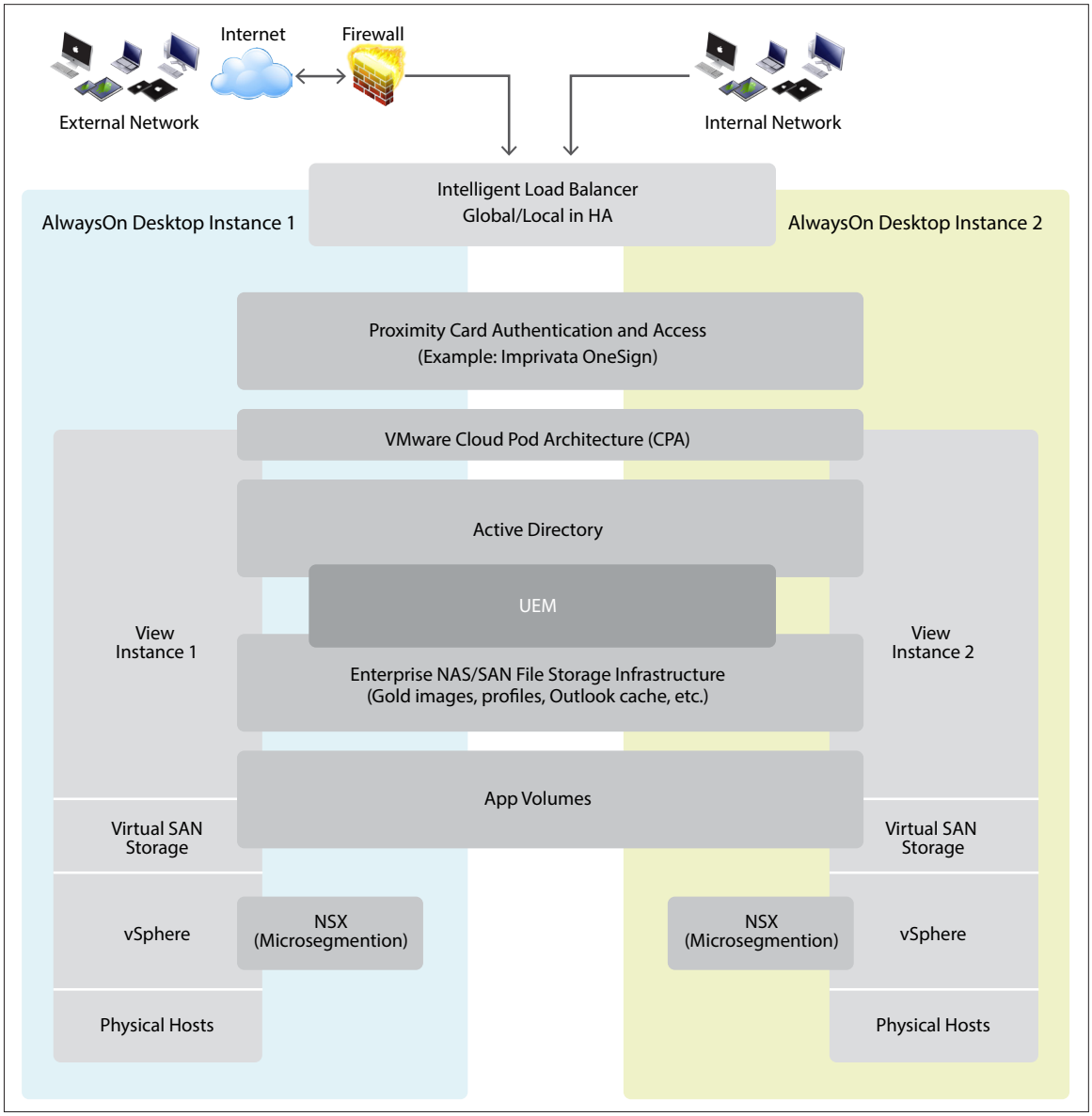

Figure 5: Logical Stack Based on Imprivata OneSign Platform for Proximity Access and SSO Functionality (Without VMware Identity Manager)

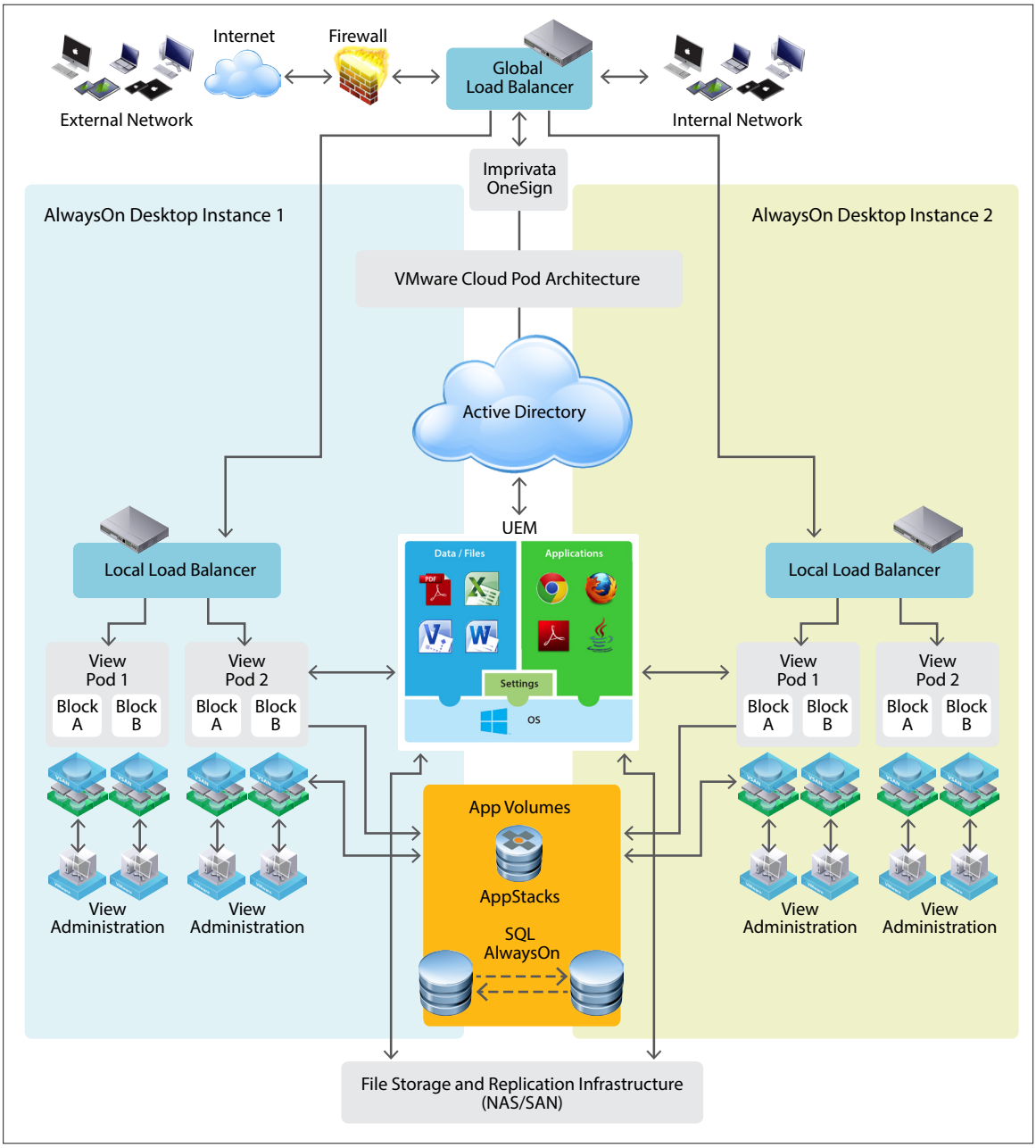

Figure 6: Component-Level Architecture Based on Imprivata OneSign for Proximity Card Authentication and SSO (Without VMware Identity Manager)

Option D: N+1 Redundancy Configuration for Scenarios A and B

Redundancy is a core concept in the AlwaysOn Desktop architecture. N+1 is a term applied to a configuration in which instead of two redundant View private cloud instances, a third instance is added to deliver 100 percent capacity in the event one of the instances is out of service.

In an N+1 configuration, each View private cloud instance is sized for 50 percent of the required concurrent session capacity. Any one of the three instances can fail and the overall available capacity remains at 100 percent, as illustrated in the following figure.

The component-level architecture is the same as Figure 2 or Figure 4, except the N+1 equivalent has three separate instances of View private cloud.

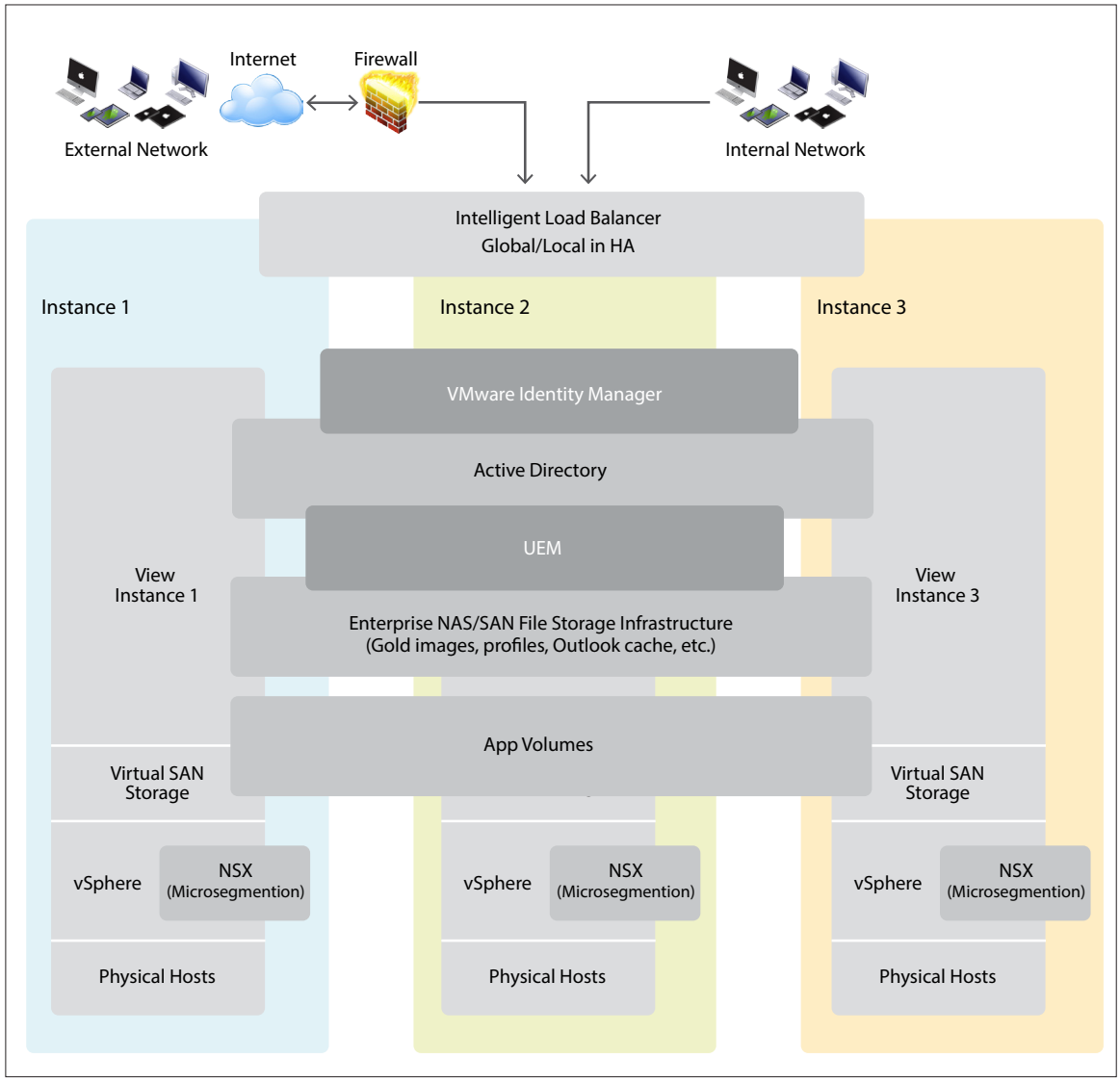

Figure 7: Logical Stack Based on VMware Identity Manager in the N+1 Redundancy Configuration (Without Cloud Pod Architecture)

AlwaysOn Desktop Product List

The following table lists the products and components supported in the AlwaysOn Desktop solution. Each deployment must be implemented using the appropriate configuration documentation.

	COMPONENT	DESCRIPTION
VMware components	vSphere	The AlwaysOn Desktop solution is built on top of the vSphere hypervisor layer that enables the virtual desktop clouds to be implemented on third-party host hardware. Each physical host runs vSphere as its core software.
	View in Horizon 6	View provides the VDI service.
	Virtual SAN	Virtual SAN provides the high-performance virtual storage infrastructure. It pools locally attached storage drives across the physical hosts and provides typical SAN functionality to the View infrastructure. Third-party products with similar capabilities are also compatible.
	VMware Identity Manager	VMware Identity Manager gives end users easy access on any device to all their business apps. It also provides IT a scalable, policy-based management platform to centrally govern and secure assets across devices. VMware Identity Manager includes a centralized catalog of all applications and data services that can be delivered to users based on their identity and needs. This user-centric management model enables IT to efficiently manage a diverse and evolving set of applications and devices. VMware Identity Manager requires SQL Server 2014 AlwaysOn in this solution.
	User Environment Manager	User Environment Manager offers personalization and dynamic policy configuration across any virtual, physical, and cloud-based environment. It simplifies end-user profile management by providing organizations with a single and scalable solution that leverages the existing infrastructure. Third-party products with similar capabilities are also compatible.
	App Volumes	App Volumes provides real-time application delivery with life cycle management. IT can use App Volumes to instantly deliver applications to users without compromising the user experience. Use of writable volumes in AlwaysOn Desktop should be addressed on a case-by-case basis.
	VMware vRealize™ Operations for Horizon	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 to devices. It enables desktop administrators to proactively optimize the end-user experience, avert incidents, and eliminate bottlenecks.

	COMPONENT	DESCRIPTION
VMware components (continued)	NSX	NSX improves desktop virtualization security and helps address east-west threats by enabling administrators to define policy centrally. The policy is then distributed to the hypervisor layer within every vSphere host and attached to each virtual desktop as soon as it is created. To secure virtual desktops and adjacent workloads within the data center, NSX implements microsegmentation, giving each desktop its own perimeter defense. This shrink-wrapped security uses the NSX distributed virtual firewall capability to police traffic to and from each virtual machine, eliminating unauthorized access between desktops and adjacent workloads.
Third-party components	Intelligent load balancer	Provides standard load-balancing and intelligent routing based on source IPs, geolocation, user ID, or latency. A user is always routed to the preferred site based on predefined rules and routed to the next available site in case of a site failure. Two levels of traffic routing are available: • Global level, which sits across the instances of AlwaysOn Desktop clouds • Local level within each instance of the AlwaysOn Desktop cloud Compatible third-party platforms include F5 BIG-IP GTM and LTM products (in redundant pairs). Other third-party products with similar capabilities are also compatible.
	Proximity card-based authentication	Enables direct authentication to the View desktop environment. These products deliver an enhanced user experience for ease of authentication, especially in healthcare settings where clinicians are always on the move and need to rapidly enter and exit their virtual desktops many times a day. The Imprivata OneSign platform is fully compatible with the AlwaysOn Desktop solution. Third-party products with similar capabilities are also compatible.
	Microsoft SQL Server Database Platform	App Volumes and VMware Identity Manager products use Microsoft SQL Server for their underlying database platform. Both of them support SQL Server AlwaysOn functionality that was introduced with SQL Server 2012 and designed specifically for high-availability through redundancy. Consult appropriate Microsoft documentation for further details.

Table 3: AlwaysOn Desktop Supported Components

AlwaysOn Desktop Availability Analysis

AlwaysOn Desktop design has three primary tenets.

- Eliminate any single point of failure that can cause an outage in the desktop 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 private cloud instances.

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

AlwaysOn Desktop Cluster

Redundancy measure: Multiple vSphere hosts are contained within each View 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 working desktop. No reconfiguration is necessary, other than replacing the defective host.

AlwaysOn Desktop Pod

Redundancy measure: Each pod includes at least two View clusters.

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

AlwaysOn Desktop Private Cloud Instance

Redundancy measure: Each private cloud instance includes at least two pods.

In the event that a View pod becomes non-operational, the remaining pod continues to deliver full service. The View Connection Servers in the cloud instance work around the out-of-service pod.

AlwaysOn Desktop Service

Redundancy measure: AlwaysOn Desktop 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 continues to deliver full service. The global intelligent load balancer sends new requests to the functioning private cloud instance.

The AlwaysOn Desktop 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) continue(s) 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: Virtual SAN supports RAID-configured storage arrays in which loss of an individual local storage drive does not impact the operation of a View cluster with shared storage.

For implementation guidelines and best practices, see the Virtual SAN documentation.

View Connection Server

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

For implementation guidelines and best practices, see the Horizon 6 documentation.

Local Load Balancer

Redundancy measure: Each data center with an AlwaysOn Desktop 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.

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

Global Load Balancer

Redundancy measure: AlwaysOn Desktop solution includes 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 one continues to provide full service.

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

App Volumes

Redundancy measure: App Volumes architecture supports redundancy and high-availability features.

An instance of App Volumes can support multiple App Volumes Managers in a pooled configuration so that loss of one of them does not impact the overall service availability. Similarly, the SQL Server database platform must be implemented in an always-on clustered mode and configured for high availability.

The design includes an instance of App Volumes platform dedicated to each AlwaysOn Desktop private cloud instance. AppStacks must be duplicated across App Volumes instances as they are created and updated to ensure that AppStacks are available as local mounts for virtual desktops within each private cloud instance for optimal performance.

For implementation guidelines and best practices, see the App Volumes documentation.

User Environment Manager

Redundancy measure: User Environment Manager does not require a separate infrastructure. It consists of data and policy files that are stored in the enterprise NAS or SAN environment, therefore leveraging all the underlying high-availability and replication services of that environment. All file locations must be configured as referential (not absolute) paths to ensure access to User Environment Manager file objects from any View private cloud instance.

For implementation guidelines and best practices, see User Environment Manager.

VMware Identity Manager

Redundancy measure: VMware Identity Manager supports SQL Server AlwaysOn configuration that provides for a clustered SQL implementation with redundant instances of the database.

For implementation guidelines and best practices, see the VMware Identity Manager documentation.

NSX (Optional)

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

NSX is a layer of network security software in the vSphere platform for AlwaysOn Desktop. It provides the capability to segregate desktop pools using security policies, also called microsegmentation functionality. Although NSX is optional, it delivers significant security advantages in virtual desktop deployments with a large number of desktop pools.

For implementation guidelines and best practices, see the NSX documentation.

AlwaysOn Desktop Solution Failure Scenario Analysis

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

SCENARIO NUMBER	FAILURE SCENARIO	IMPACT ON DESKTOP SERVICE AVAILABILITY	DETAILS
1	A vSphere host malfunctions and goes out of service	None	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.
2	A VMware vCenter server goes out of service	None	Existing View sessions continue as normal. Logged-out sessions are not refreshed, and 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.
3	A View Connection Server goes out of service	None	Each View pod includes up to seven View Connection Servers. In this failure scenario, the remaining View Connection Servers take over the load of the failed unit.
4	A local drive in a Virtual SAN cluster goes out of service	None	The Virtual SAN data store is configured as a RAID array with built-in protection against failure of individual drives.
5	An entire View cluster goes out of service	None	AlwaysOn Desktop architecture requires at least two View clusters in each pod. In this scenario, the remaining View clusters continue normal operation. Total available session capacity is reduced by the size of the malfunctioning View cluster.
6	A View private cloud instance is unavailable	None	AlwaysOn Desktop architecture requires at least two View cloud instances. In this scenario, the remaining View private cloud instance(s) continue normal operation. Total available session capacity is reduced by the size of the malfunctioning View instance. Components such as App Volumes, User Environment Manager, and VMware Identity Manager, are available from any of the View instances.
7	Component outage in the App Volumes SQL database	None	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.

SCENARIO NUMBER	FAILURE SCENARIO	IMPACT ON DESKTOP SERVICE AVAILABILITY	DETAILS
8	App Volumes SQL Server database in a View private cloud instance goes out of service	None	App Volumes supports SQL Server AlwaysOn. In the event that one of the SQL instances is down, service fails over to the other instance.
9	VMware Identity Manager database is unavailable	None	VMware Identity Manager service is configured with SQL Server AlwaysOn where the database service automatically fails over.
10	A OneSign virtual appliance goes out of service	None	The 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.
11	A vSphere host running the View admin services goes out of service	None	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.

Table 4: AlwaysOn Desktop Solution Failover Scenarios

About the Author

Farid Agahi, Senior Business Strategist in End-User Computing, VMware, wrote this paper.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com