VMware Workspace Portal Reference Architecture

VMware Workspace Portal 2.1

TECHNICAL WHITE PAPER

vmware®

Table of Contents

Executive Summary

This reference architecture provides guidance for implementing a VMware Workspace™ Portal 2.1 deployment of 30,000 users and 40 applications of various types using an existing server and storage infrastructure. You can scale the architecture for larger deployments or high availability by adding Workspace Portal virtual appliances (VA).

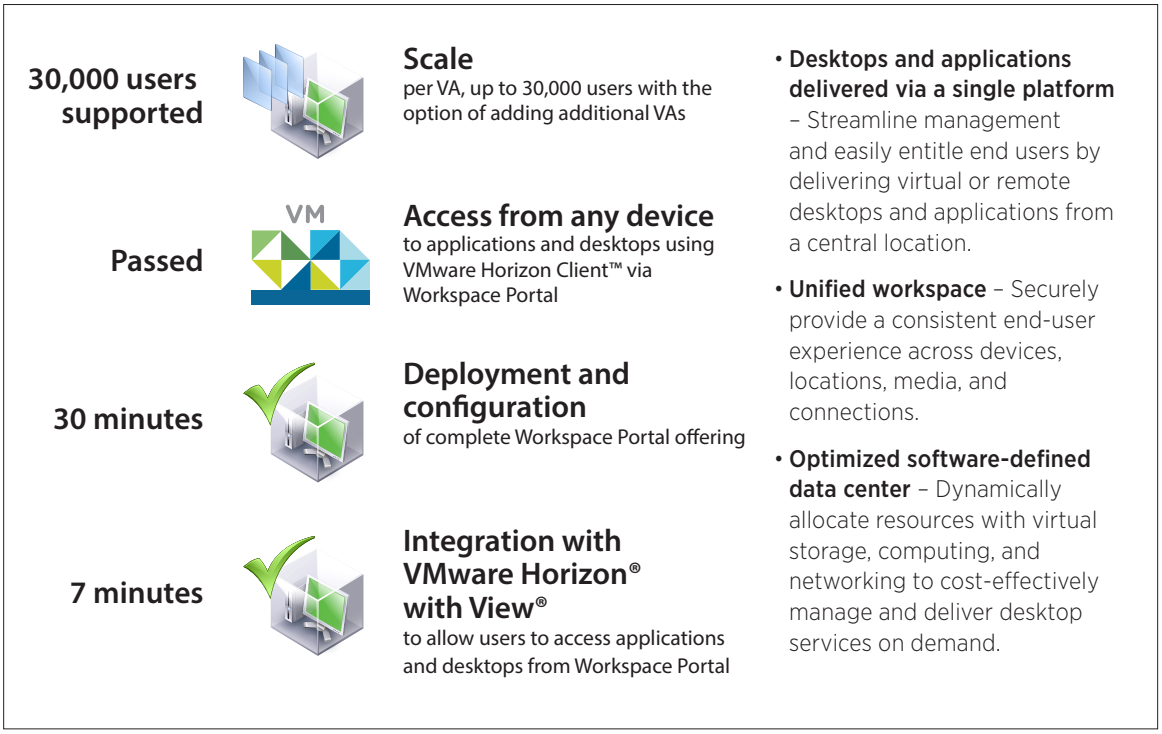

Figure 1: Test Results

This document includes information on VMware Horizon (6.0) with View, VMware ThinApp® 5.0, and Workspace Portal 2.1 running on top of VMware vSphere® 5.x. It describes how you can integrate Workspace Portal 2.1 in existing infrastructures and addresses performance characteristics.

As part of the architecture validation, VMware performed functional tests to highlight how easy it is to deploy, integrate, and manage Workspace Portal.

Overview

VMware Workspace Portal combines applications and desktops in a single, aggregated workspace. Employees can then access the desktops and applications regardless of where they are based. With fewer management points and flexible access, Workspace Portal reduces the complexity of IT administration.

Workspace Portal is delivered as a virtual appliance (VA) that is easy to deploy onsite and integrate with existing enterprise services. Organizations can centralize assets, devices, and applications and manage users and data securely behind the firewall. Users can share and collaborate with external partners and customers securely when policy allows.

This reference architecture describes the sizing and connectivity requirements for a 30,000-user Workspace Portal application management and desktop access solution.

The high-level infrastructure consists of

- VMware ESXi™ hosts with two 2.0 GHz Intel E5-2650 processors (2x8 cores)
- 192 GB RAM per ESXi host
- NFS-based storage
- 10 Gigabit Ethernet (GbE) networking

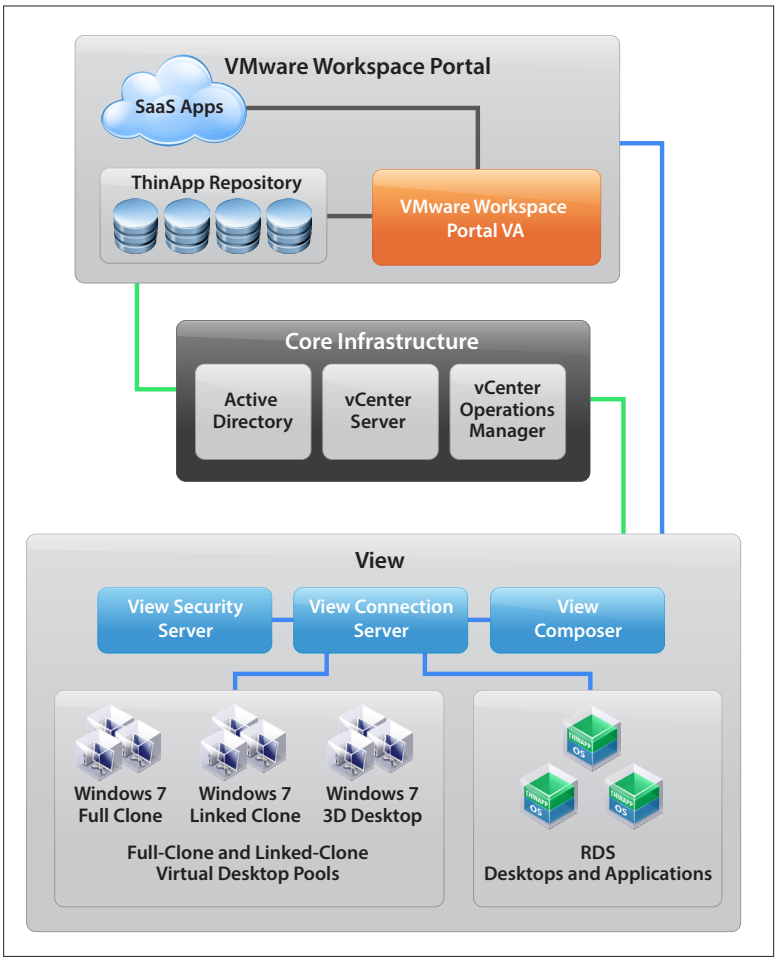

Figure 2: Workspace Portal Solution

Hardware Components

The server system used in this solution includes the following components:

- Two Intel E5-2650 processors (16 physical cores)
- 192 GB DDR3 ECC registered memory
- Two 10 GbE NICs

All components required to set up and support Workspace Portal run on NFS-based storage attached to the hosts. See the Workspace Portal Configuration and VA Sizing sections for sizing guidance.

The internal infrastructure was based on 10 GbE to connect the ESXi hosts, VMware Horizon 6 components, and Workspace Portal. Virtual desktops connected to the same 10 GbE network provided user access. The functional tests were performed on different network types, such as Wi-Fi and 1 Gb.

VMware vSphere

VMware vSphere is the industry-leading virtualization platform for building cloud infrastructures. It enables users to run business-critical applications with confidence and respond quickly to business needs. vSphere accelerates the shift to cloud computing for existing data centers and underpins compatible public cloud offerings, forming the foundation for the industry's best hybrid cloud model.

VMware Workspace Portal 2.1

Workspace Portal, part of Horizon 6, allows users to access desktops and applications in a central location. Workspace Portal also provides IT a central place to entitle and deliver Windows applications, desktops, software-as-a-service (SaaS) applications, ThinApp packaged applications, and XenApp applications to users.

Workspace Portal is delivered as a SUSE Linux-based Open Virtual Appliance (OVA) file consisting of a single VA deployed through VMware vCenter™ or any other solution supporting Open Virtualization Format (OVF) or OVA format.

VMware Horizon 6 with View

Horizon 6 with View delivers hosted virtual desktops and applications to end users through a single platform. These desktop and application services—including RDS-hosted applications, ThinApp packaged applications, SaaS applications, and virtualized applications from Citrix—can all be accessed from one unified workspace across devices, locations, media, and connections. Leveraging closed-loop management and optimized for the software-defined data center, Horizon helps IT control, manage, and protect the Windows resources that end users want at the speed they expect and with the efficiency that business demands.

For more information, see the VMware Horizon 6 Reference Architecture.

Workspace Portal Reference Architecture

This reference architecture supports a 30,000-user Workspace Portal deployment, including 40 enterprise and Web applications, View desktops, and RDS-hosted applications.

The architecture leverages the benefits of the VMware software-defined data center (SDDC) stack to provide an enterprise-class virtualization platform and ensure performance, security, manageability, scalability, availability, and reliability.

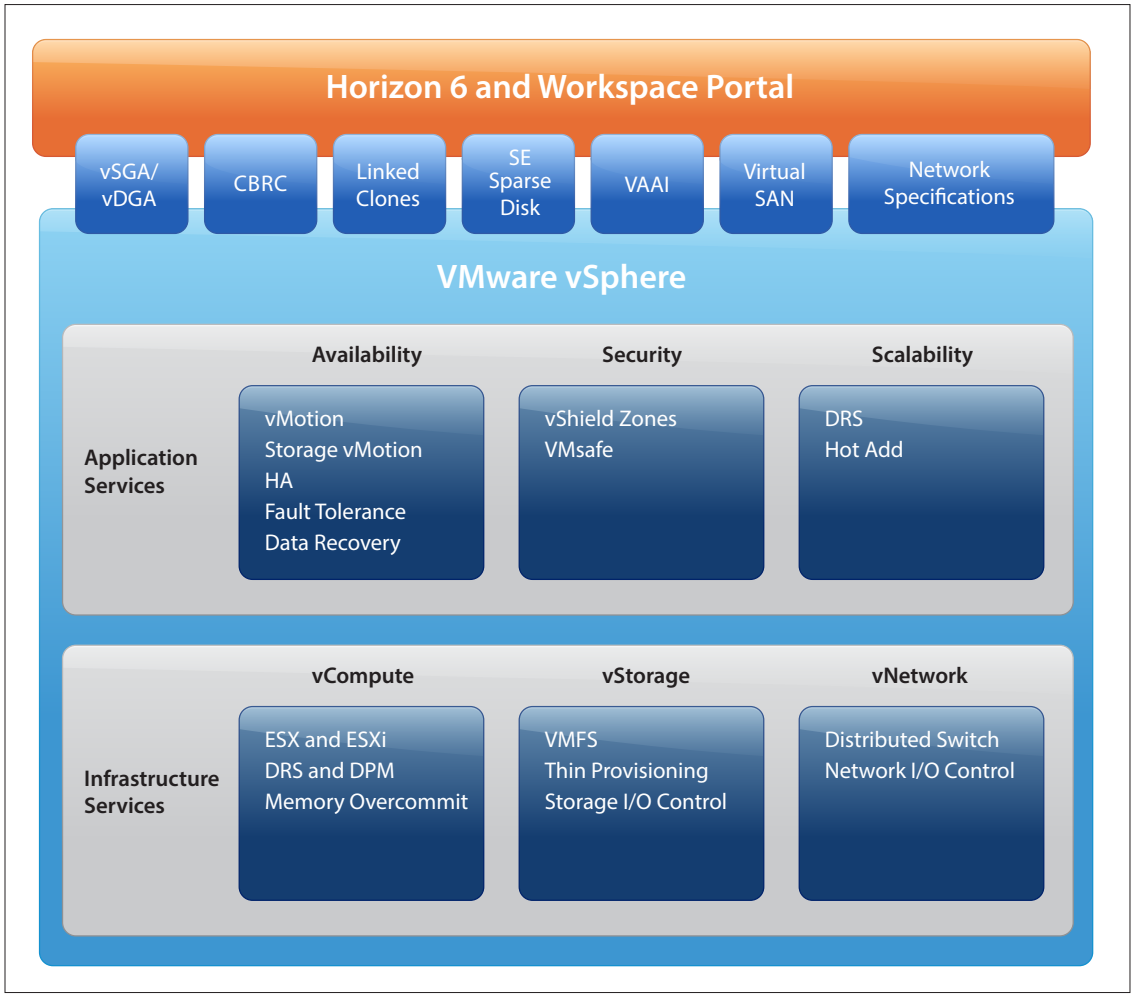

Figure 3: VMware Software-Defined Data Center

Workspace Portal benefits from proven vSphere features, such as a distributed resource scheduler, high availability, thin provisioning, transparent page sharing, and memory compression.

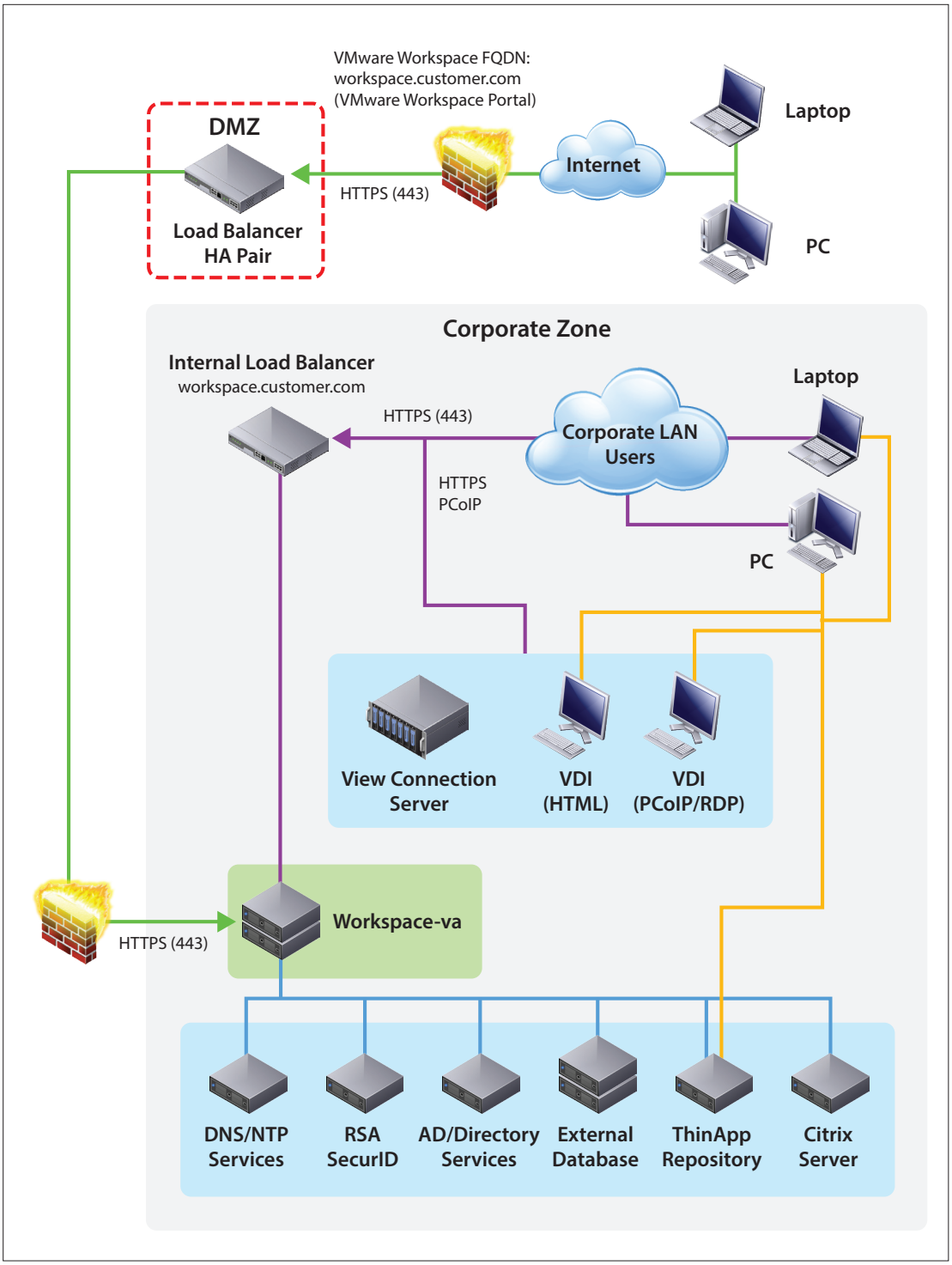

Figure 4: Workspace Portal Architecture Design

SaaS and Web Applications

Enabling the Web Applications module allows you to add Web and SaaS applications to your Workspace Portal catalog and to entitle users and groups to access those applications.

Workspace Portal also provides an application catalog with preconfigured SaaS applications. Workspace Portal supports Security Assertion Markup Language (SAML) 1.1 and 2.0.

Note: To integrate Workspace Portal with Horizon 6 with View, use SAML 2.0 as detailed in the Horizon 6 documentation.

ThinApp Configuration

Workspace Portal integrates with ThinApp 4.7 and later to stream or download ThinApp applications to Windows endpoints. To support ThinApp packages in Workspace Portal requires the following:

1. Install Workspace Portal Client on the Windows machines targeted for using ThinApp packages via Workspace Portal.
2. Enable the ThinApp packages module from the Workspace Portal Administrative Console.
3. Log in to Connector Services Admin and click **Packaged Apps** – **ThinApp**.
4. Connect to the ThinApp share (Windows CIFS share) and provide the requested information. Only EXE files are supported.
5. Log back in to the Workspace Portal Administrative Console and verify that ThinApp packages have been added to the catalog.

Horizon with View Configuration

To integrate Workspace Portal with Horizon with View, do the following:

1. Install VMware View Agent® in the virtual desktops to provide HTML5 access to View desktops.
2. Make sure that Workspace Portal User Directory Sync has been configured to sync the User Principle Name (UPN) attributes.
3. Make sure that forward and reverse DNS records exist for View servers.
4. Enable the View module in Workspace Portal.
5. Join the VA used for Horizon with View integration, or verify that it has been joined to the domain.
6. Configure SAML 2.0 authentication in View, and enable SAML 2.0 authentication for all brokers in the View pods used for the integration.

Note: SAML 1.1 does not support Horizon with View and Workspace Portal integration.

The SAML authentication configuration applies to desktops and applications, so both are functional after the integration has been set up.

To configure other options for the Horizon with View and Workspace Portal integration, use the Connector Admin Web interface. For more information, see Installing and Configuring Workspace Portal.

Network Deployment Considerations

The VAs communicate between each other using host names, so forward and reverse DNS records for the VAs and IP addresses are necessary. The initial deployment requires one IP address. For a typical production scenario, two VAs are deployed to allow for high availability.

By default, the Workspace Portal VA is accessible only to users inside the corporate network. To provide external access from outside the firewall to Workspace Portal, install a reverse proxy or load balancer using SSL termination to sit in front of one or more VAs.

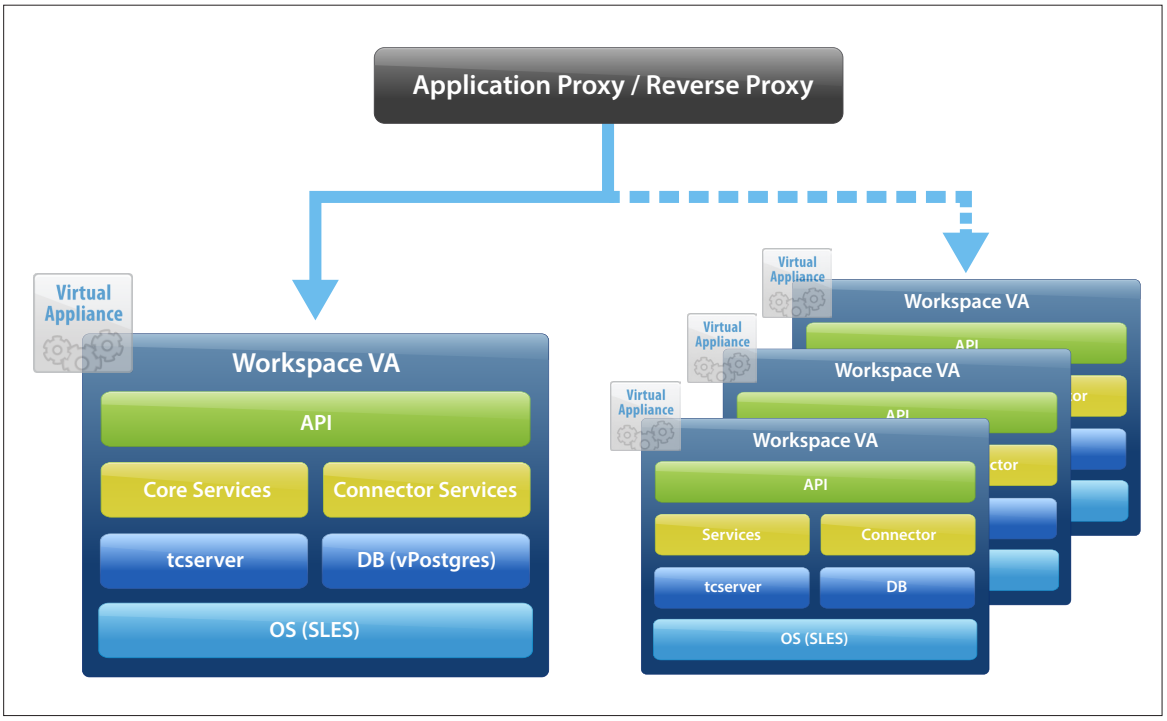

Figure 5: Setup for Application or Reverse Proxy

The following table lists the ports required for Workspace Portal.

NETWORK PATH	PORT	PROTOCOL
Horizon Client or app to VA	443 (HTTPS)	TCP
VA to Active Directory (user authentication)	389	TCP and UDP
VA to domain controller (domain join)	135	TCP and UDP
VA to time server (NTP)	123	UDP
VA ThinApp repository (SMB)	445	TCP
VA to domain controller and all Windows clients to connector-va (Kerberos authentication)	88	TCP and UDP
VA to global catalog server (user sync)	3268	TCP

NETWORK PATH	PORT	PROTOCOL
VA to domain controller (Kerberos password change)	464	TCP and UDP
All VAs to DNS server (DNS)	53	TCP and UDP
Load balancer to VA and VA to all other VAs (HTTPS)	443	TCP
VMware Workspace Portal Administrative Services links	8443	TCP
connector-va to SecureID server (SecureID)	5500	UDP
VAs to each other, if more than one (auditing)	9200–9400	TCP
VAs to each other, if more than one (auditing)	54328	UDP
VA to external database (if used)	5432	TCP and UDP
VA (connector service) to domain controller	749	TCP and UDP

Table 1: Workspace Portal Default Ports

External Infrastructure Components

The external infrastructure of this reference architecture consists of the following components:

- **Active Directory** – Workspace Portal requires Active Directory to sync users and groups. This reference architecture uses Windows Server 2008 R2 Active Directory.
- **DNS** – The VAs refer to each other by their host names. Both forward and reverse records are required for all VAs in the Workspace Portal vApp. Make sure that each machine can search for the Workspace Portal fully qualified domain name (FQDN).
- **Network Time Protocol (NTP)** – All VAs rely on time synchronization.
- **Load balancer or reverse or application proxy** – This reference architecture uses a software-based load balancer.
- **ThinApp** – The solution leverages the existing VMware application virtualization solution.
- **Horizon 6 with View** – The solution leverages the existing VMware virtual desktop solution and application solution.

Workspace Portal Configuration

Workspace Portal requires additional configuration of vSphere hosts and vCenter servers, including NTP for vSphere hosts.

NTP

For time sync to work properly, NTP must be enabled and point to your enterprise NTP server on all vSphere hosts where the VA is deployed. Failing to do so can cause time drift between the VAs. It is also important to have proper time sync between all integration components, because the SAML artifacts used for authentication have a short lifespan, which could result in users not being able to access desktops or applications. Kerberos-enabled connectors sync time to the Primary Domain Controller role.

Database

The VA includes a vPostgres database to speed deployment and implementation. You can use an external database with two or more Workspace Portal VAs to provide high availability or scale the solution. The internal database supports production and high-availability deployments. For instructions on supportability and setup, see Using embedded vPostgres in Production for VMware Workspace Portal VA 2.1.

This reference architecture is based on using the internal vPostgres. If you are using an external database, Table 2 lists the recommendations for sizing the database.

RESOURCE	AMOUNT
vCPU	8
RAM	8 GB
Disk	120 GB

Table 2: Configuration for an External Database

VA Sizing

The Workspace Portal VA ships with a default sizing configuration. This configuration can work well for proof-of-concept and small deployments, but the configuration needs to be expanded to achieve a well-performing platform for the targeted 30,000 users. Table 3 lists the default and recommended configurations.

	VCPU	RAM	HARD DISK DRIVE
Default	2	6 GB	72 GB
Recommended	8	8 GB	72 GB

Table 3: VA Sizing Configuration

Test Results

Testing involved manual functional tests across a number of client devices to highlight usability and manageability. In addition, operational tests were conducted to verify entitlements, Active Directory sync tasks, and administration tasks.

After Workspace Portal is installed and configured, it takes 14 minutes to set up and provide access to RDS desktops and applications. An additional 18 minutes is needed to provision a pool of 100 desktops. It takes just 10 seconds for users to connect to desktops or applications after they have authenticated to View or Workspace Portal.

Functional Testing

The results of the functional testing are summarized in Table 4.

FUNCTIONAL TEST	TIME TO COMPLETE	VALIDATION	RESULT
Initial deployment and setup of Workspace Portal	30 minutes	An administrative account could access Workspace Portal for both admin and end-user experiences.	PASSED
Configure Workspace Portal to integrate with View	7 minutes	Entitled application and desktop appears in Workspace Portal.	PASSED
Access any RDS application from Workspace Portal	8–10 seconds (6–8 seconds to reconnect)	Clicked an RDS application entitled from View and synced to Workspace catalog.	PASSED
Access any virtual desktop from Workspace Portal	10 seconds (6–8 seconds to reconnect)	Clicking an RDS desktop in Workspace Portal after user login presents the desktop to the user.	PASSED
Access any RDS application from within a virtual desktop session	8–10 seconds (8–10 seconds to reconnect)	Clicking an RDS application in Workspace Portal after user login presents the application to the user.	PASSED
Create a group and filter members based on Active Directory attributes	2 minutes	After creating the group, validate that users in this group show the expected result.	PASSED

Table 4: Functional Test Results

Active Directory Synchronization and Entitlement Testing

Testing verified how well Active Directory sync operations performed as well as entitlement operations for 40 applications and 30,000 users.

All tests were performed using both the default and recommended configurations. The tests used only one Workspace Portal VA. The VA used the internally supplied database. The results show that expanding the resources improves entitlement operations.

	TOTAL ENTITLEMENT TIME	AVERAGE PER APPLICATION	ACTIVE DIRECTORY SYNC TIME
Default	4 hr, 9 min	7 min, 35 sec	34 min
Recommended	1 hr, 35 min	2 min, 35 sec	26 min

Table 5: AD Synchronization and Entitlement Test Results

References

Workspace Portal Datasheet

Workspace Portal FAQ

Workspace Portal Release Notes

Workspace Portal Administrator's Guide

Installing and Configuring Workspace Portal

Using embedded vPostgres in Production for VMware Workspace Portal VA 2.1

Workspace Portal 2.1 HA cluster using internal database

vmware®

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