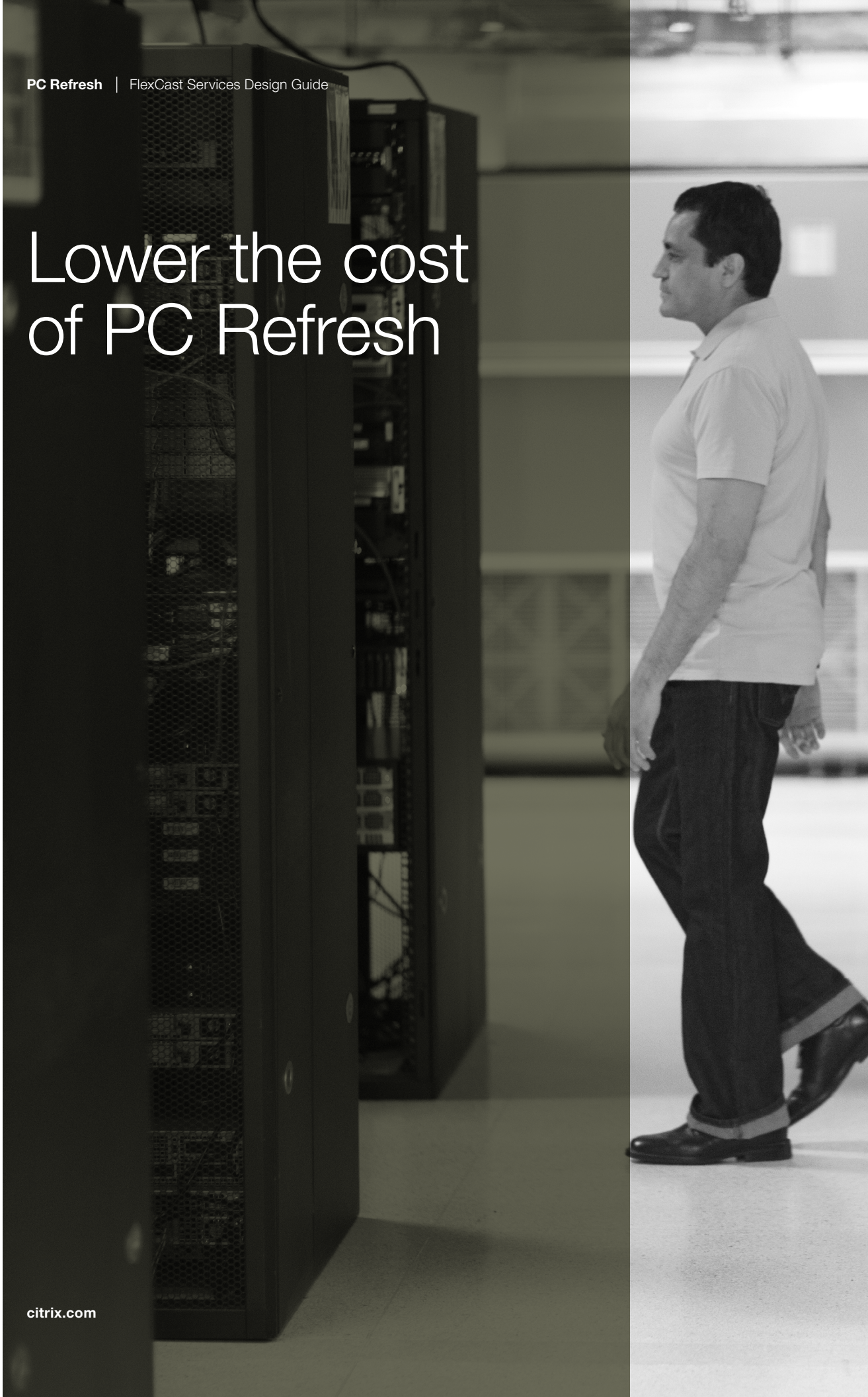
Lower the cost of PC Refresh



CITRIX®

citrix.com

Table of contents

Click on the section names above to navigate to that portion of the book and the arrow icon to return to the table of contents from any page.

About the FlexCast Services design guide

Citrix FlexCast Services design guides provide an overview of a validated architecture based on many common scenarios. Each design guide relies on Citrix Consulting best practices and in-depth validation by the Citrix Solutions Lab to provide prescriptive design guidance on the overall solution.

Each FlexCast Services design guide incorporates generally available products and employs a standardized architecture, allowing multiple design guides to be combined into a larger, all-encompassing solution.

Project overview

Every year, a portion of the IT budget is allocated towards refreshing the aging PC environment. Although the retired PCs are still functional, the user experience starts to degrade while using the latest applications, which often require additional computing resources.

Unfortunately, tightening budgets is forcing IT to balance business-critical projects against routine operational projects, like PC refresh. IT must find innovative ways to successfully deliver business projects while still maintaining the current end user computing environment.

With Citrix XenDesktop, an IT organization can extend the life of user endpoint devices and still provide a great user experience while utilizing the latest operating system and applications.

Objectives

The objective of the FlexCast Services Design Guide is to construct and demonstrate a cost-effective way of delivering a high-performance Windows desktop to local users with low-cost and repurposed endpoints.

This is the challenge impacting WorldWide Corporation (WWCO), a hypothetical organization that would like to repurpose aging PCs while moving desktops to a central location to reduce management costs and increase data security.

To address these challenges, IT decided to implement a Citrix XenDesktop 7 environment to deliver high-performing, Windows-based virtual desktops to repurposed endpoint devices. To properly validate the solution, IT identified a 500-user division for the project.

WWCO business objectives

- Reduce the PC hardware refresh budget with repurposed endpoint devices
- Streamline PC support efforts and troubleshooting cycles
- Centrally manage a single master image and deploy desktops to all users to help reduce troubleshooting and support incidents
- Protect intellectual property

WWCO technical objectives

- Allow users to fully customize their desktop while IT manages a single desktop image
- Build a solution that scales from a few hundred users to thousands with minimal changes to the infrastructure
- Implement an N+1 highly available solution without large cost increases, excluding user-managed apps
- Centrally manage and control employee access and permissions
- Utilize virtualized components, where possible, to reduce costs

Assumptions

The following assumptions played a role in defining the overall strategy for WWCO:

- All resources (physical servers, virtual servers, Windows applications) will be hosted from a single datacenter.
- High availability is required for all critical components in N+1 mode, where enough spare capacity will be built into the system to allow for the failure of one component without impacting user access.
- WWCO's existing Microsoft Active Directory and DNS/DHCP will be reused.
- The master image will consist of standard office productivity and browser apps. Users can add additional apps as needed.

Conceptual architecture

Figure 1, based on the overall business and technical objectives for the project as well as the assumptions, provides a graphical overview of the solution architecture.

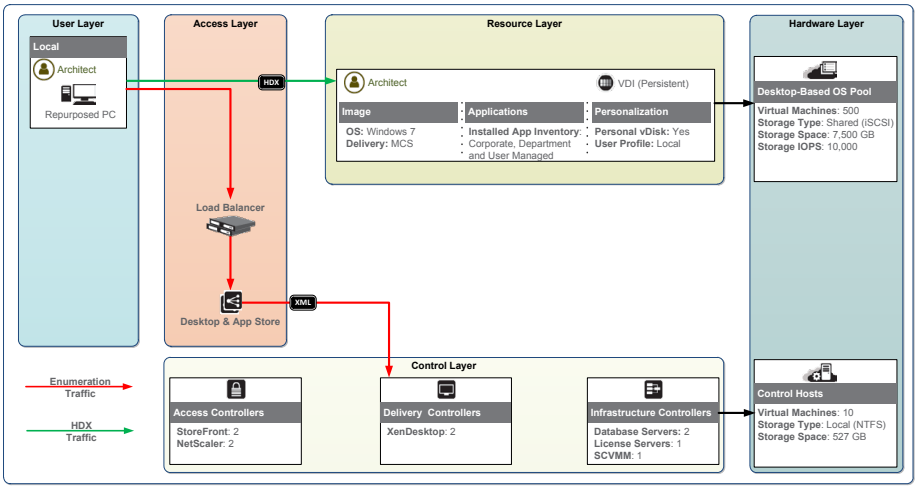


Figure 1: Conceptual architecture

This architecture is suitable for 500 users requiring local access to a fully customized Windows desktop from repurposed endpoint devices.

At a high level, the following information can be ascertained from the conceptual architecture:

- The 500-user division used in the first phase of the rollout is called Architect. This group will utilize repurposed PCs to connect to the environment from the local office. These devices are older desktop PCs, locked-down and configured to connect to a virtualized environment.
- The allocated resources for the Architect user group is a single, persistent desktop pre-configured with a set of standardized applications.

- The base operating system, Windows 7, is delivered to the appropriate virtual machines via Machine Creation Services.
- Complete user personalization, including user installed applications, is integrated into the desktops through the use of Personal vDisk.
- The total hardware allocation requirement for the solution is 7 physical servers.

Each layer of the architecture diagram and the relevant components are discussed in greater detail below.

Detailed architecture

The overall solution for WWCO is based on a standardized five-layer model that provides a framework for the technical architecture. At a high level, the model comprises:

1. User layer. Defines the unique user groups and overall endpoint requirements
2. Access layer. Defines how user groups will gain access to their resources and focuses on secure access policies and desktop/application stores
3. Resource layer. Defines the resources, which could be desktops, applications or data, assigned to each user group
4. Control layer. Defines the underlying infrastructure required to support users in accessing their resources
5. Hardware layer. Defines the physical implementation of the overall solution with a focus on physical servers, storage and networking

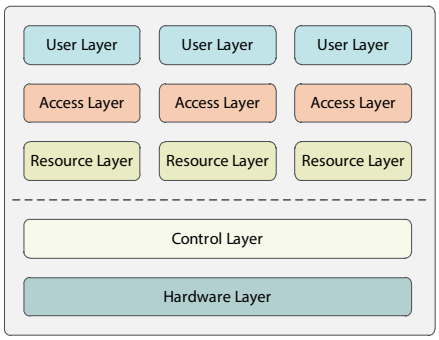


Figure 2: Virtual desktop model

User layer

The user layer focuses on the logistics of the user groups, which includes client software, recommended endpoints and office locations. This information helps define how users will gain access to their resources, which could be desktops, applications or documents.

- Citrix Receiver client. This client software, which runs on virtually any device and operating platform, including Windows, Mac, Linux, iOS and Android, must be downloaded onto user endpoints to access virtual desktops, which are hosted in the datacenter. Citrix Receiver provides the client-side functionality to secure, optimize and transport the necessary information to/from the endpoint/host over Citrix HDX, a set of technologies built into a networking protocol that provides a high-definition user experience regardless of device, network or location.
- Endpoints. The physical devices used by the Architect user group are repurposed desktop PCs configured with Citrix Receiver and Desktop Lock. The Desktop Lock utilizes a replacement Windows shell, in which no local Start menu is displayed to prevent users from accessing the local operating system. Upon boot up and login, the user's local desktop is hidden and the virtual desktop is seamlessly delivered.
- Location. The Architect user group will work from local offices, over secure network connections. Although the network is private, traffic must still be encrypted.

Access layer

The access layer defines the policies used to properly authenticate users to the environment, secure communication between the user layer and resource layer and deliver the applications to the endpoints.

The following displays access layer design decisions based on WWCO requirements.

Users connecting from…	Local, trusted network
Authentication point	StoreFront
Authentication policy	Single-factor authentication (username and password)
User group	Architect

- Authentication. Users must authenticate to their virtual desktop before being allowed access. As each user will only access the environment from an internal location, single-factor authentication using a username and password will be satisfactory.

Resource layer

The resource layer defines the underlying image, how to deliver the image to the associated virtual machines, which applications to deliver and how to provide the right level of personalization for the respective user group.

Based on the requirements, the following displays the resource layer design decisions based on WWCO requirements.

Criteria	Decision
Operating system	Windows 7
Delivery	Machine Creation Services
CPU	8 vCPU

Memory	2 GB RAM
Image size	35 GB
Disk cache	Differencing Disk: 5 GB (Shared storage) PVD Disk: 10 GB (Shared storage)
Page file size	2 GB (contained within differencing disk)
Application(s)	Office productivity Departmental apps User installed apps (via Personal vDisk
Profile	Local profile
Policy(s)	Hi-def experience
User group	Architect

- Machine Creation Services is not limited by scale, but rather by the type of delivery target: physical or virtual machine. As the project is based on resource delivery to virtual machines, Machine Creation Services is the ideal solution. Machine Creation Services does not require additional hardware or resources as it simply utilizes the hypervisor and local storage to create unique, thin, provisioned clones of a master image, resulting in a solution that is simple to deploy and easy to scale.
- As the users often require unique and custom applications in order to perform their job, personalization will be provided with Personal vDisk. Personal vDisk captures and stores the user-level changes in a virtual disk that is separate from the master image. All changes, not explicitly ignored, persist across reboots and master image updates. Administrators are able to update redeploy the master image to all users while preserving all user-level changes, including user installed applications.
- Storage space is a critical factor when designing a fully personalized desktop. Although the personal vDisk can be thin provisioned, which will greatly reduce storage space requirements, the actual size of the disk will continue to grow through the lifetime of the virtual desktop. As users continue to customize their desktop, those changes are captured and stored within the Personal vDisk. If thin provisioning storage calculations are too aggressive, there is a risk of exhausting storage space.
- As users only access the environment from internal locations where adequate bandwidth exists and latency is low, a high definition user experience will be provided that offloads, to the repurposed PCs, certain graphical and multimedia operations from the hosting servers. Instead of the hosting servers fetching and rendering flash, windows media and other multimedia content, the physical endpoint will utilize local computing resources, which will help improve capacity on the hosting infrastructure. The user experience configuration and optimizations are provided by the following XenDesktop policies:

Policy	Settings	Applied to…
Hi-Def experience	Based on the template “High Definition User Experience”	Delivery group

Control layer

The control layer of the solution defines the virtual servers used to properly deliver the prescribed environment detailed in the user, access, and resource layers of the solution, including required services, virtual server specifications and redundancy options.

Access controllers

The access controllers are responsible for providing users with connectivity to their resources, as defined within the access layer. In order to support the access layer design, the following components are required:

Parameter	StoreFront	NetScaler VPX Express
Instances	2 virtual servers	2 virtual servers
CPU	2 vCPU	2 vCPU
Memory	2 GB RAM	2 GB RAM
Disk	60 GB (local storage)	3.2 GB (local storage)
Citrix product version	StoreFront 2.0	NetScaler VPX for Hyper-V 10 Build 71.6
Microsoft product version	Windows Server 2012 Standard	NetScaler VPX for Hyper-V 10 Build 71.6
Network ports	443	443, 80
Redundancy	Load balanced via NetScaler VPX Express	High-availability pair

The redundant pair of NetScaler Gateway virtual servers is responsible for providing secure, remote access while the redundant pair or StoreFront virtual servers is responsible for resource enumeration.

Delivery controllers

The delivery controllers manage and maintain the virtualized resources for the environment. In order to support the resource layer design, the following components are required:

Parameter	XenDesktop delivery controller
Instances	2 virtual servers
CPU	2 vCPU
Memory	4 GB RAM
Disk	60 GB
Citrix product version	XenDesktop 7
Microsoft product version	Windows Server 2012 Standard
Network ports	80, 443
Redundancy	Load balanced via NetScaler VPX Express
Notes	System Center Virtual Machine Manager (SCVMM) management console installed

A single delivery controller can easily support the load of 500 users. However, to provide N+1 fault tolerance, a second virtual server will provide redundancy in case one virtual server fails.

Infrastructure controllers

In order to have a fully functioning virtual desktop environment, a set of standard infrastructure components are required.

Parameter	SQL server	License server	Hyper-V SCVMM4
Instances	2 virtual servers	1 virtual servers	2 virtual servers
CPU	2 vCPU	2 vCPU	2 vCPU
Memory	4 GB RAM	4 GB RAM	4 GB RAM
Disk	60 GB (local storage)	60 GB (local storage)	100 GB
Version(s)	Not applicable	Citrix License Server 11.12	Not applicable
Microsoft product version	Windows Server 2012 Standared SQL Server 2012	Windows Server 2012 Standard	Windows Server 2012 Standard SCVMM 2012 SP1
Network ports	1433	27000, 7279, 8082	135, 443, 2179, 3389, 5985-5986, 8100-8013
Redundancy	SQL Server AlwaysOn	None due to 30 day grace period	None

To provide fault tolerance, the following options were used:

- The XenDesktop database was deployed on an HA pair of Microsoft SQL Server 2012 servers utilizing the AlwaysOn availability group with primary and secondary instances spread across two virtual servers.
- Once active, a XenDesktop environment can continue to function for 30 days without connectivity to the Citrix License Server. Due to the integrated grace period, no additional redundancy is required.
- Only a single Hyper-V SCVMM server is used, as the loss of the server has minimal impact on a XenDesktop environment. Without the SCVMM server, only the power functions of the virtual machine are affected. All virtual servers that are currently running will continue to run, any connected user will notice no service disruption and any user who tries to connect to a session will succeed. Power functions can still be managed manually from the local console if needed.

Hardware layer

The hardware layer is the physical implementation of the solution. It includes server, networking and storage configurations needed to successfully deploy the solution.

Server

Following is the physical server implementation for the WWCO solution:

Component	Description	Quantity	Total
Servers	HP DL380P G8	7	7 servers
Processor(s)	Intel Xeon E5-2690 @2.9GHz	2	16 cores
Memory	8GB DDR3-1333	24	192 GB
Disk(s)	300 SAS @ 15,000RPM	4	1.2 TB
Storage Array Controller	300 SAS @ 15,000RPM	1	1 controller
Microsoft product version	Windows Server 2012 datacenter	7	7
Shared Storage	NetApp FAS2240-2	1	1
Disk(s)	600 GB SAS @ 15,000RPM	24	14 TB

When deploying a fully customizable virtual desktop where users can install any application, there must be a built in capacity buffer because the complete user workload is unknown. It is advisable to not design the solution so that the servers are at full capacity.

Taking into account a capacity buffer and N+1 fault tolerance, the virtual servers were distributed so redundant components were not hosted from the same physical server. The virtual server allocation is depicted in Figure 3.

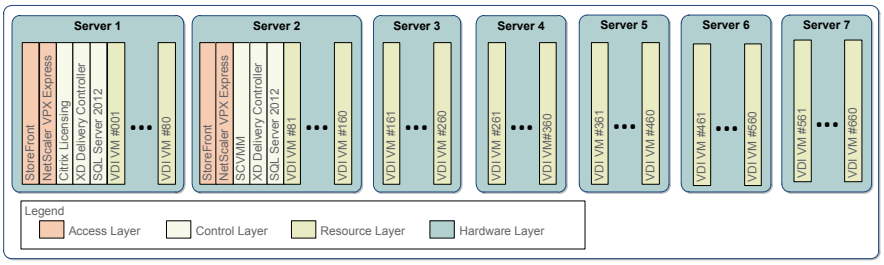


Figure 3: Virtual machine server allocation.

Note: The resource load on the physical hardware for the access and control layer components is minimal, which is why the hosts are also able to support VDI virtual machines.

Note: Although this environment was designed for 500 users, it can scale much higher by adding additional physical servers that mimic the configuration of Servers 3-7.

Storage

The storage architecture for the solution is based on the use of inexpensive local storage. To ensure an acceptable user experience, the storage architecture must have enough throughput capacity as well as fault tolerance to overcome the potential failure of a single drive.

Parameter	RDS hosts
Storage Solution	NetApp FAS2240-2
Drive count	24
Drive speed	15,000 RPM
Drive size	600 GB
RAID	RAID DP
IOPS per user	20
Read/write ratio	40/60
Characteristics	Random, 4K blocks

Based on tests, each user accessing a virtual desktop will generate roughly 20 IOPS (at max) during their steady state activity.

In addition to the resource layer virtual servers, the control and access layer systems generate IOPS activity. However, the impact on storage is minimal when compared to the active sessions generated by users.

Networking

Integrating the solution into the network requires proper configuration to have the right components communicate with each other. The network is configured based on each physical server's having four network ports:

NIC instance	Function	Speed	VLAN ID
1	Management VLAN	1 Gbps	1
2	Virtual machine VLAN	1 Gbps	2
3	Disabled		
4	Storage VLAN	1 Gbps	4

The two VLANs are divided among the physical and virtual servers as shown in Figure 4.

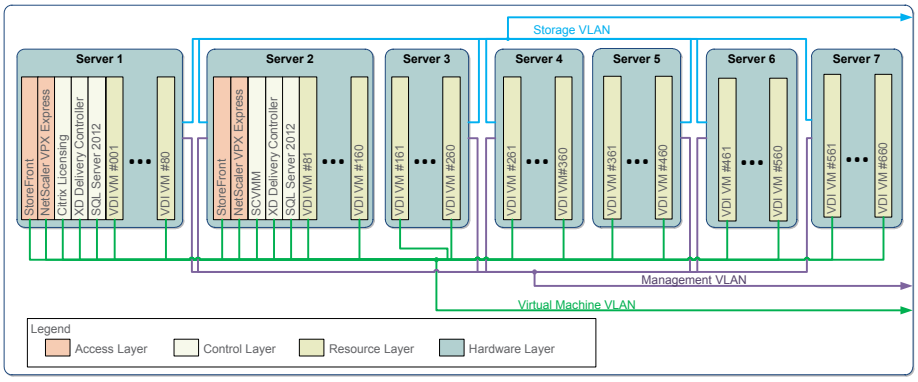


Figure 4: Networking architecture

As depicted in the diagram, the VLAN is configured as follows:

- The management VLAN is only connected to the physical hosts and not the virtual machines. This VLAN is for management calls to/from the physical server's hypervisor.
- The virtual machine VLAN, meant for all non-DMZ virtual machines, allows them to connect to the internal datacenter network.

Validation

The defined solution was deployed and validated by the Citrix Solutions Lab. Here are the key findings from the validation:

- CPU was the limiting factor in scaling out the environment.
- The physical servers supported roughly 100 Windows 7 desktops.
- At peak, the control layer components of SQL Server, StoreFront and desktop delivery controllers consumed less than 30 percent of CPU and had over 20 percent of available memory.
- Based on the overall solution, a 1 Gbps switch would provide sufficient network capacity.

Figure 5 provides a graphical representation of the utilization of the control layer components as the user load increased.

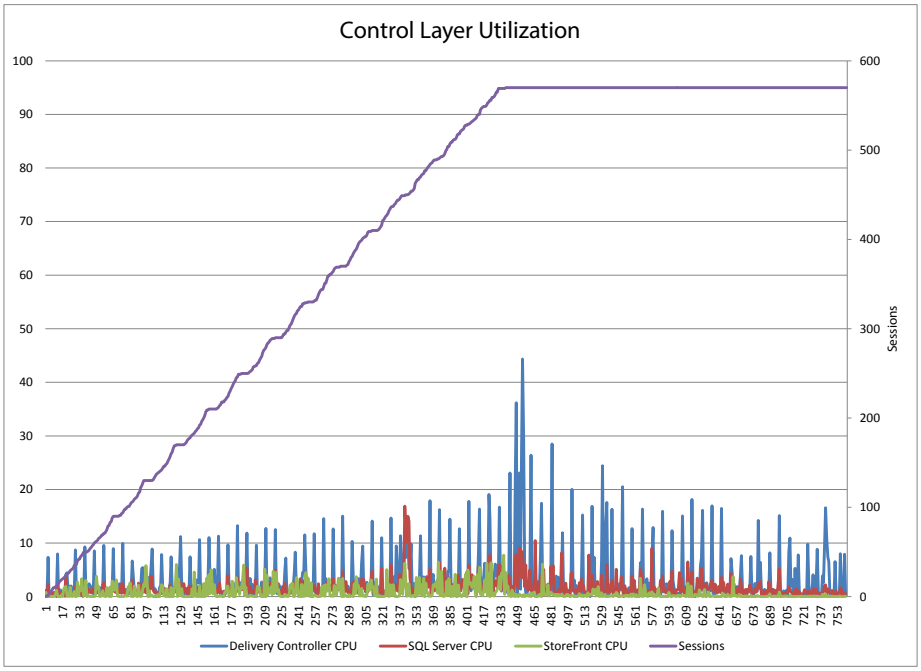


Figure 5: Processor Utilization for Control Layer Components

Although the solution was designed to only support 500 users, the control layer components, responsible for supporting and maintaining the environment, are minimally utilized and are capable of much higher user loads.

Next steps

While user demands for the latest resources continue to grow, IT must find ways to do more with less funding. If IT continues to follow old approaches where roughly every three years the endpoint devices are replaced with the latest PCs vendors have to offer, there will be significantly less funds available to take on new initiatives.

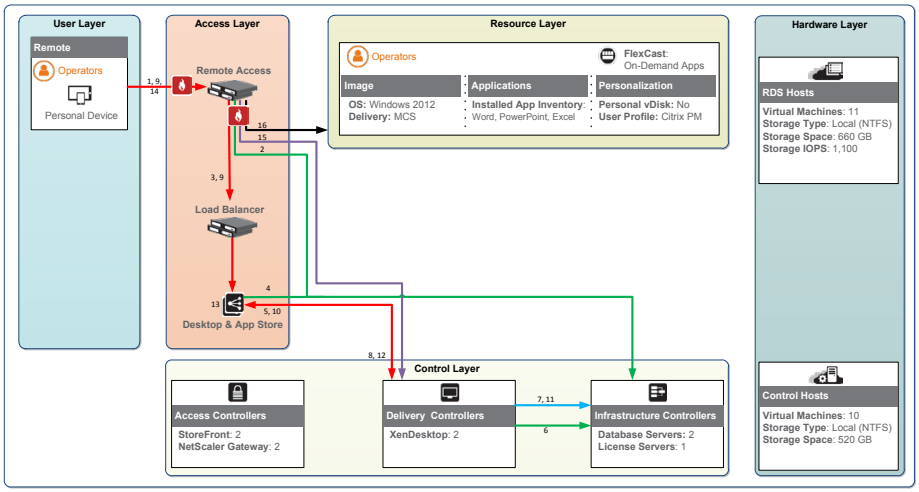
With Citrix XenDesktop 7, IT can deliver the latest applications to users without acquiring new endpoint devices. Citrix XenDesktop can offload some computing/graphical operations to the local endpoint device, which not only continues to provide each user with an exceptional experience but also allows higher user density on the data center servers.

To learn more about the potential benefits that XenDesktop 7 can provide, it is recommended to follow the prescribed roadmap to gain knowledge and firsthand experience.

- XenDesktop 7 Blueprint: A layered solution for all successful designs and deployments, focusing on the common technology framework and core decisions
- Getting Started Guide: Prescriptive guide for deploying the solution to five or 10 users quickly and easily in a non-production environment
- FlexCast Services Design Guides: Recommended designs, with hardware layer planning numbers, for commonly used implementations, which can be combined to form a complete solution

Appendix: Authentication and enumeration process

The user authentication, enumeration and connection process is as follows:



Step	Remote users
	A user initiates a connection to the NetScaler Gateway URL (443) and provides logon credentials. This can either be done by using a browser or Citrix Receiver.
	The credentials are validated against Active Directory (389).
	NetScaler Gateway forwards the validated user credentials to StoreFront, which can be a virtual address hosted by a load balancer (443).
	StoreFront authenticates the user to Active Directory domain (389) it is a member of. Upon successful authentication, StoreFront checks the data store for existing user subscriptions and stores them in memory.
	StoreFront forwards the user credentials to the Delivery Controllers (80 or 443), which could be a virtual address hosted by a load balancer.
	The Delivery Controller validates the credentials against Active Directory (389).
	Once validated, the XenDesktop Delivery Controller identifies a list of available resources by querying the SQL Database (1433).
	The list of available resources is sent to StoreFront (443), which populates the user's Citrix Receiver or browser after passing through NetScaler Gateway (80 or 443).
	A resource is selected from the available list within Citrix Receiver or browser. The request is sent to StoreFront through NetScaler Gateway (443).
	StoreFront forwards the resource request to the Delivery Controller (80 or 443).
	The Delivery Controller queries the SQL Database to determine an appropriate host to fulfill the request (1433).
	The Delivery controller sends the host and connection information to StoreFront (443).
	StoreFront requests a ticket by contacting the Secure Ticket Authority (80 or 443), which is hosted on the Delivery Controller. The STA generates a unique ticket for the user, which is only valid for 100 seconds. The ticket identifies the requested resource, server address and port number thereby preventing this sensitive information from crossing public network links. StoreFront generates a launch file, including the ticket information, which is sent to the user through NetScaler Gateway (443).
	Citrix Receiver uses the launch file and makes a connection to the NetScaler Gateway (443).
	NetScaler Gateway validates the ticket with the STA (80 or 443)
	NetScaler Gateway initiates a connection to the resource (1494 or 2598) on the user's behalf.

Corporate Headquarters
Fort Lauderdale, FL, USA

India Development Center
Bangalore, India

Latin America Headquarters
Coral Gables, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

Online Division Headquarters
Santa Barbara, CA, USA

UK Development Center
Chalfont, United Kingdom

EMEA Headquarters
Schaffhausen, Switzerland

Pacific Headquarters
Hong Kong, China

About Citrix
Citrix (NASDAQ:CTXS) is the cloud company that enables mobile workstyles—empowering people to work and collaborate from anywhere, easily and securely. With market-leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration and data sharing, Citrix helps organizations achieve the speed and agility necessary to succeed in a mobile and dynamic world. Citrix products are in use at more than 260,000 organizations and by over 100 million users globally. Annual revenue in 2012 was $2.59 billion. Learn more at www.citrix.com.

Copyright © 2014 Citrix Systems, Inc. All rights reserved. Citrix, Citrix Receiver, NetScaler VPX, XenDesktop, NetScaler Gateway, FlexCast, ICA, and HDX are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.

0114/PDF **citrix.com**