Mobilizing Windows apps

CITRIX®

citrix.com

About FlexCast Services design guides

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

Today's workers expect greater levels of flexibility as they do their jobs, particularly the types of devices they work on and the locations they work from.

While on mobile devices, especially tablets and smartphones, people are growing accustomed to having instant access to their personal applications with the push of a button. They want the same experience when accessing their business applications, which are predominantly Windows based.

People also find working outside of the office to be beneficial for productivity and improved quality of life. To be successful, they need a way to access their Windows applications from remote locations.

These demands pose great challenges for IT organizations. Somehow, IT must find ways to provide users with the required Windows business applications on mobile devices and in remote locations without massive rewrites. At the same time, IT must adhere to corporate information security guidelines by preventing corporate data from leaving secure storage locations.

Objective

The objective of the FlexCast Services design guide is to construct and demonstrate an efficient way of delivering Windows-based applications to remote users while properly optimizing them for different types of endpoints, which could be the latest touch-enabled mobile devices, including tablets and smartphones, or traditional laptops and workstations.

This is the challenge impacting WorldWide Corporation (WWCO), a hypothetical consulting organization. WWCO would like improve the user experience by allowing access to corporate applications from remote locations across multiple

types of endpoint devices, including mobile and traditional. The IT organization needs to support any mobile device type and brand, any type of laptop or workstation and any operating system. In addition, IT needs an efficient way to make Windows apps more accessible on smaller displays and usable on touch-enabled screens.

To address these challenges, IT decided to implement a XenApp environment to provide remote access to Windows-based business applications from employee- and corporate-owned devices. To properly validate the solution, IT identified a 500-user division for the first phase of the rollout.

WWCO business objectives

- Efficiently provision Windows apps for multiple devices per user and multiple device types (mobile and traditional)
- Reduce the costs of application rewrites and new application development
- Centralize delivery of applications and data to any device, on any network, from a single platform
- Enable secure, remote access to Windows applications on the latest mobile devices
- Ensure information security across employee- and corporate-owned mobile devices

WWCO technical objectives

- Support mobile devices, which include iOS, Android and Windows tablets and phones
- Support traditional laptops and workstations running operating systems such as Windows, Mac and Linux
- Build a solution that scales from a few hundred users to thousands
- Utilize virtualized components, where possible, to reduce costs and complexity
- Implement an N+1 highly available solution without incurring large cost increases
- Define a public access point for external users
- Secure all traffic crossing public network links
- Design a strong, multi-factor authentication solution

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 workload will consist of standard office productivity apps, web-based apps, occasional multimedia viewing and local printing.

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.

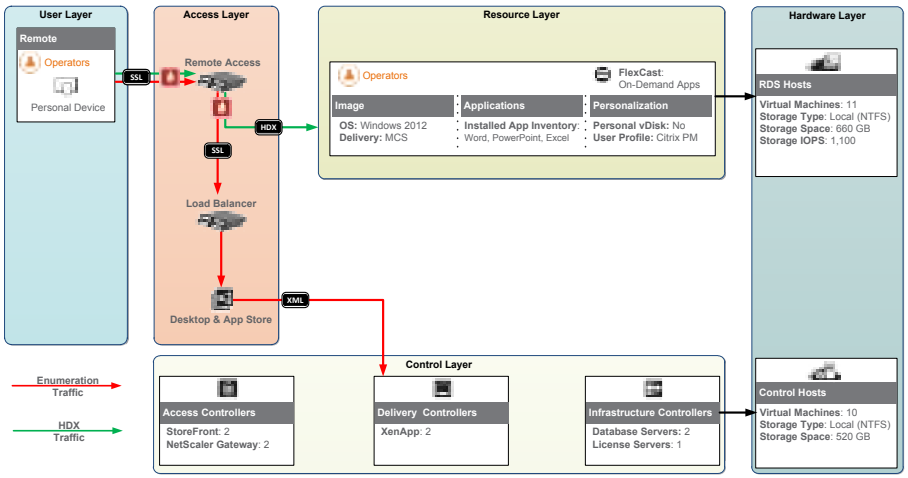

Figure 1: Conceptual architecture

This architecture is suitable for 500 users requiring secure access to Windows apps from various mobile devices and locations.

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 the Operators. This group will utilize personal devices to connect to the environment from a remote location. These devices include laptops, workstations, tablets and smartphones.
- Traffic will pass through the remote access device where users receive their resources from the desktop & app store.
- The allocated resources for the Operators user group are a set of on-demand apps, which simply provides the application interface while hiding the underlying operating system interface.
- The base operating system, Windows 2012, is delivered to the appropriate virtual machines via Machine Creation Services.
- User personalization is integrated into the desktops through the use of Citrix Profile Management.
- The total hardware allocation requirement for the solution is three 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, providing a framework for the technical architecture. At a high level, the 5-layer 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. Focuses on secure access policies and desktop/application stores.
3. Resource layer – Defines the virtual resources, which could be desktops or applications, assigned to each user group.
4. Control layer – Defines the underlying infrastructure required to support the 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.

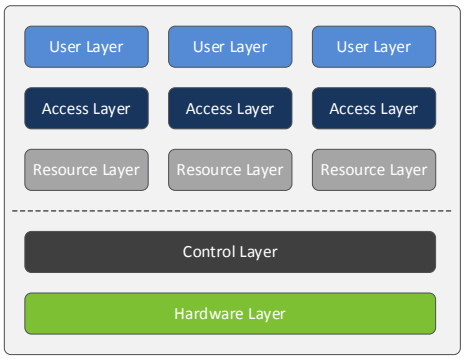

Figure 2: Virtual desktop model

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 business applications, 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 could be smartphones, tablets, laptops, desktops, thin clients, etc. Users download and install the Citrix Receiver client from their device's app store or directly from Citrix.com.
- Location – The Operators user group will work from remote locations, over unsecure network connections, requiring all authentication and session traffic to be secured.

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…	Remote, untrusted network
Authentication point	NetScaler Gateway
Authentication policy	Multi-factor authentication (username, password and token)
Session policy	Mobile Traditional
Session profile	ICA Proxy
User group	Operators

- Authentication – Allowing users to access the environment from a remote location without authenticating would pose security risks to WWCO. When users access the environment, the external URL will direct requests to Citrix NetScaler Gateway, which is deployed within the DMZ portion of the network. NetScaler Gateway will accept user multi-factor authentication credentials and pass them to the appropriate internal resources (Active Directory domain controllers and token authentication software such as RADIUS).
- Session policy – NetScaler Gateway can detect the type of endpoint device and deliver a specific access experience based on device properties. WWCO policies are:
  - Mobile – When users connect with a mobile device, a separate policy will be applied to improve usability of the Windows applications. By using the following expression within the NetScaler Gateway session policy configuration, this policy will only be applied to mobile devices: "REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver"
  - Traditional – This policy will be applied to all non-mobile devices by using the following expression within the NetScaler Gateway session policy configuration: "ns_true"

- Session profile – As the Operators group members only require access to their respective applications, regardless of endpoint, the session profile will be configured as ICA Proxy instead of full VPN mode. ICA Proxy only allows HDX traffic to pass from the endpoint to the on-demand app through NetScaler Gateway. Using an ICA Proxy session profile helps protect the environment by allowing only session-related traffic to pass, while blocking all other traffic.

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 Server 2012 - Standard
Delivery	Machine Creation Services
CPU	8 vCPU
Memory	16 GB RAM
Disk	60 GB
Application(s)	Microsoft Office (Word, Excel, PowerPoint)
Profile	Citrix Profile Management
Policy(s)	Optimized for WAN Optimized for mobile
User group	Operators

- Based on WWCO requirements, users do not require access to or interaction with the underlying desktop; they simply need access to a set of applications. XenApp utilizes Microsoft Remote Desktop Shared Hosted (RDSH) technology to provide delivery of on-demand applications via session virtualization, where multiple user sessions share the applications and resources of a single Windows Server instance. Even though resources are shared, session virtualization protects one user's session from impacting others or the underlying operating system.

- 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.

- Although users do not have to install their own applications in the virtualized environment, they want to customize and personalize these applications as they see fit. The Citrix Profile Management solution allows WWCO to create a profile solution that fits the needs for the current user group, but can also expand to support additional groups. In addition, enabling profile streaming and folder redirection within Profile Management increases logon speed, helping to improve the end user experience.
- While authentication and security policies applied when users connect from a remote location support IT security goals, a satisfying experience must be provided for users. As the network link between user and resource is dynamic and uncontrolled, policies are needed to optimize the user experience for the WAN and mobile devices.

Policy	Settings	Applied to…
Optimized for WAN	Based on the template "Optimized for WAN"	Any user connecting through NetScaler Gateway
Optimized for mobile	Mobile experience • Automatic keyboard display: Allowed • Launch touch-optimized desktop: Allowed • Remote the combo box: Allowed	Any user connecting through NetScaler Gateway where Access Control = "Mobile", which corresponds to a NetScaler Gateway Session Policy defined in the Access Layer

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.

The decisions for the Operators group are met by correctly incorporating and sizing the control layer components, which include access controllers, delivery controllers and infrastructure controllers.

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	NetScaler Gateway	StoreFront
Instances	2 virtual servers	2 virtual servers
CPU	2 vCPU	2 vCPU
Memory	2 GB RAM	4 GB RAM
Disk	3.2 GB	60 GB

Parameter	NetScaler Gateway	StoreFront
Citrix product version	NetScaler VPX for Hyper-V 10 Build 71.6	StoreFront 2.0
Microsoft product version	Not applicable	Windows Server 2012 Standard
Network ports	443	443
Redundancy	High-availability pair	Microsoft Network Load Balancing (MAC spoofing)

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	XenApp Delivery Controller
Instances	2 virtual servers
CPU	2 vCPU
Memory	4 GB RAM
Disk	60 GB
Citrix product version	XenApp
Microsoft product version	Windows Server 2012 Standard
Network ports	80, 443
Redundancy	Load balanced via StoreFront
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 SCVMM
Instances	2 virtual servers	1 virtual servers	1 virtual server
CPU	2 vCPU	2 vCPU	2 vCPU
Memory	4 GB RAM	4 GB RAM	4 GB RAM
Disk	60 GB	60 GB	100 GB
Version(s)	Not Applicable	Citrix License Server 11.12	Not applicable
Microsoft product version	Windows Server 2012 Standard 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 XenApp 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 XenApp 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 XenApp 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
Server model	HP DL380P G8	3	3 servers
Processor(s)	Intel Xeon E5-2690 @2.9GHz	2	16 cores
Memory	8GB DDR3-1333	24	192 GB

Component	Description	Quantity	Total
Disk(s)	300GB SAS @ 15,000RPM	8	2.4 TB
Microsoft product version	Windows Server 2012 datacenter	3	3

To provide fault tolerance within the solution, 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.

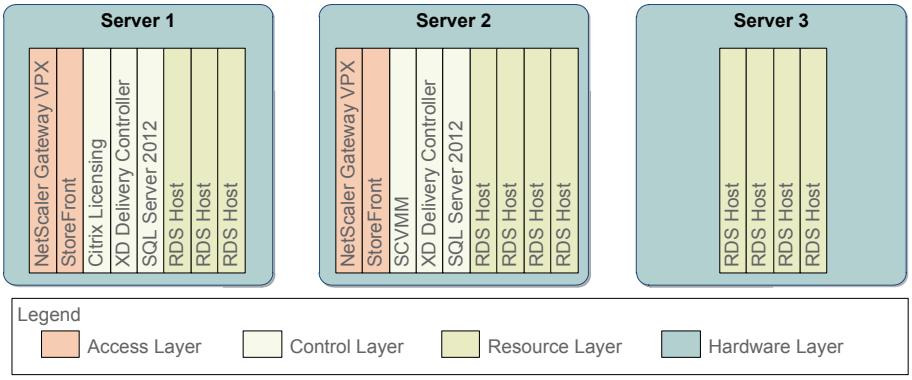

Figure 3: Virtual machine server allocation

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 RDS servers.

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

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
Drive count	8
Drive speed	15,000 RPM
RAID	RAID 10
IOPS per user	4
Read/write ratio	10/90
Characteristics	Random, 4K blocks

Based on tests, each user accessing an on-demand application will generate roughly 4 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.

As the overall solution is more write intensive, it is recommended to utilize a RAID 10 configuration across the eight hard disk drives, as RAID 10 provides fault tolerance and better write performance than RAID 5.

Networking

Integrating the solution into the network requires proper configuration to have the right components communicate with each other. This is especially important for NetScaler Gateway, which resides in the DMZ. 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	DMZ VLAN	1 Gbps	3
4	Disabled		

The three VLANs are divided among the physical servers, NetScaler Gateway and remaining virtual servers as shown in Figure 4.

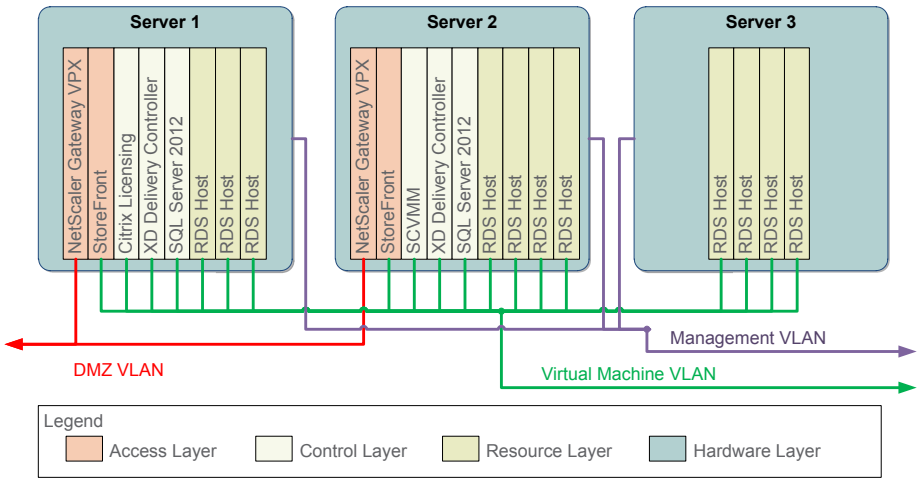

Figure 4: Networking architecture

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

- NetScaler Gateway is configured to use the DMZ VLAN. This VLAN does not connect with any other internal networks, which helps keep the DMZ and internal traffic separated.

- 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 RDS hosts supported 560 users across 11 virtual machines, with each virtual machine hosting an average of 51 users.
- The control layer components of SQL Server, StoreFront and delivery controllers consumed less than 30 percent of CPU and had over 20 percent of available memory.
- The NetScaler Gateway CPU, memory and network utilization was under 10 percent for the 500-user load.
- Based on the overall solution, a 1 Gbps switch would provide sufficient network capacity.

Measuring resource utilization was but one part of the overall validation for the solution, as resource utilization does not provide information about the user experience. As resource utilization increases, user experience decreases to a point where the solution becomes unacceptable. Therefore, the Citrix Solutions Lab utilizes a metric based on the Login VSI 3.7 test tool that takes the user experience into account.

Login VSI measures response times for opening and clicking within the UI of applications including Microsoft Word, PowerPoint, Excel and Internet Explorer and Adobe Flash video. The results of the Login VSI testing are given as VSIMax, the point at which response times exceed the acceptable limit. Information about Login VSI and details about administering the test environment can be found at loginvsi.com.

Figure 5 shows the overall performance of the entire solution utilizing Login VSI:

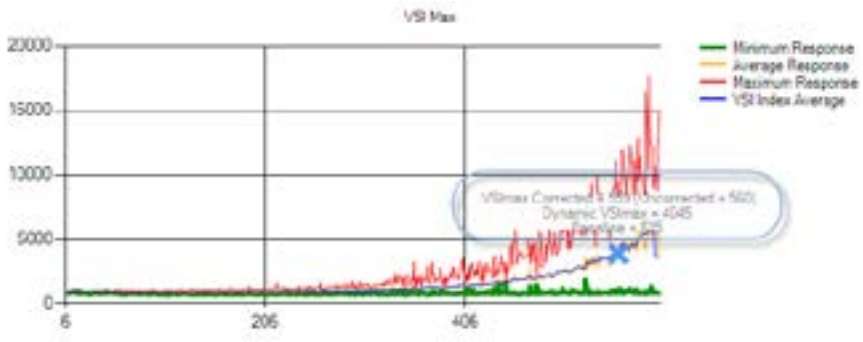

Figure 5: User experience validation

Based on the analysis, the user experience started to degrade above **559 users**.

Next steps

People expect instant access to their applications at the push of the power button, in large part because of the proliferation of smartphones and tablets. They are also used to working from a laptop or desktop regardless of location. In order to meet these mobility demands, IT organizations have three choices:

1. Damage satisfaction with IT by ignoring user requests
2. Rewrite applications for mobile platforms
3. Virtualize applications and deliver them seamlessly with XenApp

Providing on-demand application delivery with XenApp provides a way to quickly meet user demands without the long delays and high costs of application rewrites. It provides a foundation that can expand to include more users and additional requirements such as virtual desktops (VDI).

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

- XenApp 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:

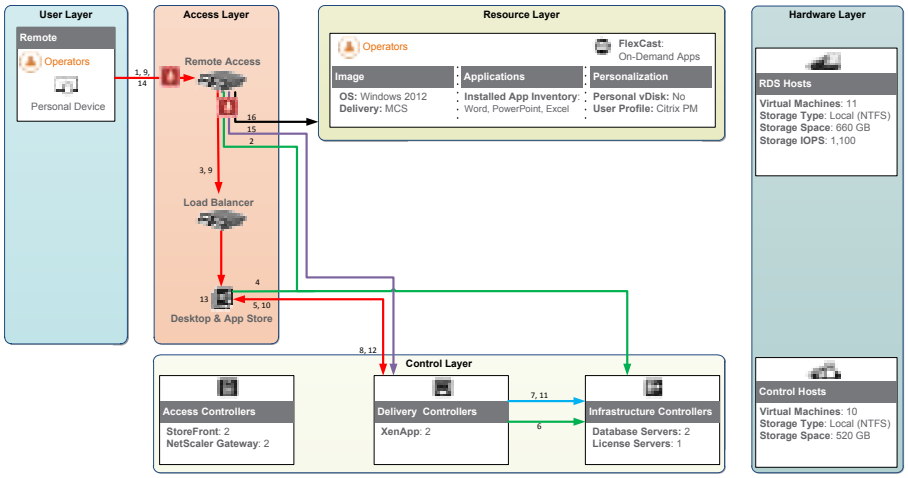

Figure 6: Authentication and enumeration process

Step	Remote users
1.	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.
2.	The credentials are validated against Active Directory (389).
3.	NetScaler Gateway forwards the validated user credentials to StoreFront, which can be a virtual address hosted by a load balancer (443).
4.	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.
5.	StoreFront forwards the user credentials to the Delivery Controllers (80 or 443), which could be a virtual address hosted by a load balancer.
6.	The Delivery Controller validates the credentials against Active Directory (389).
7.	Once validated, the XenApp Delivery Controller identifies a list of available resources by querying the SQL Database (1433).
8.	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).
9.	A resource is selected from the available list within Citrix Receiver or browser. The request is sent to StoreFront through NetScaler Gateway (443).
10.	StoreFront forwards the resource request to the Delivery Controller (80 or 443).

Step	Remote users
11.	The Delivery Controller queries the SQL Database to determine an appropriate host to fulfill the request (1433).
12.	The Delivery Controller sends the host and connection information to StoreFront (443).
13.	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).
14.	Citrix Receiver uses the launch file and makes a connection to the NetScaler Gateway (443).
15.	NetScaler Gateway validates the ticket with the STA (80 or 443)
16.	NetScaler Gateway initiates a connection to the resource (1494 or 2598) on the user's behalf.

CITRIX®

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.