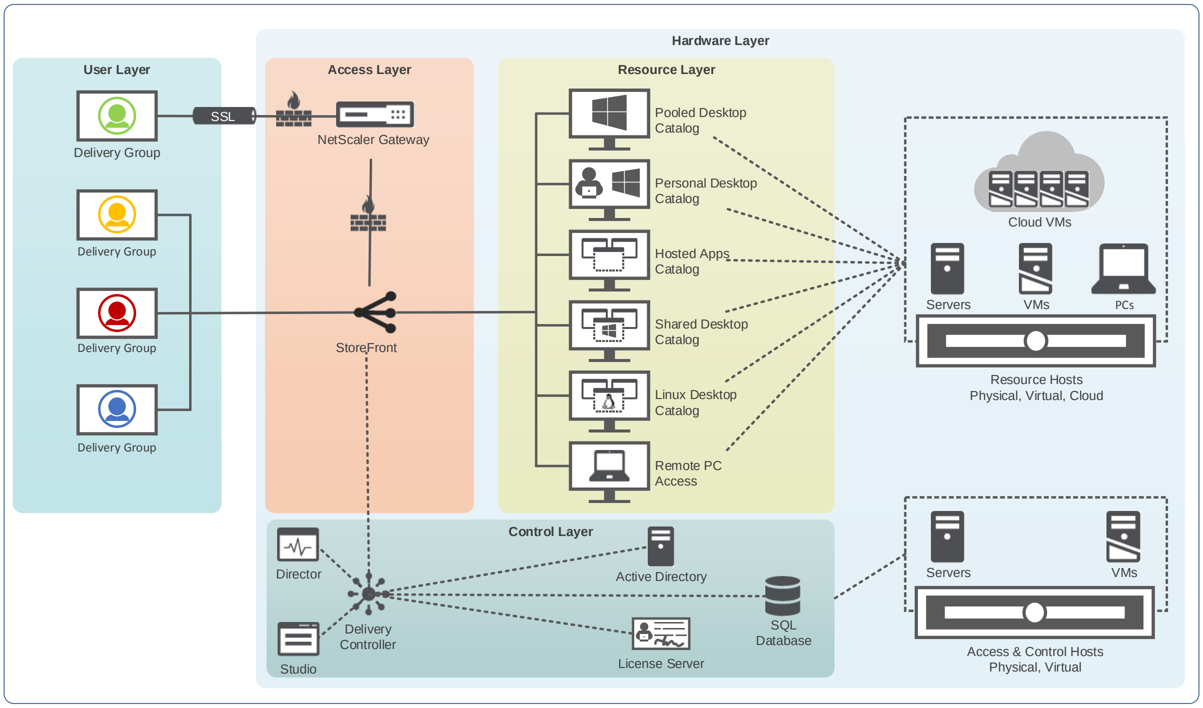
Citrix XenDesktop 7.6 Feature Pack 2 Blueprint

TABLE OF CONTENTS

Overview

Creating a virtual desktop design is often considered a complex activity where hundreds of decisions must be made that directly and indirectly affects other decisions leading to confusion. Because XenDesktop 7.6 Feature Pack 2 is an end-to-end, enterprise desktop virtualization solution, it encompasses desktop models to meet every user scenario.



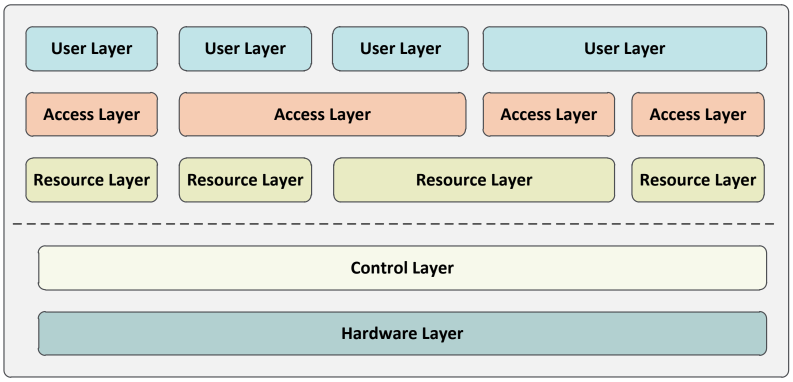
However, when focusing on the common use cases, which typically accounts for the largest percentage of users, many of the decisions simply follow best practices, which are based on years of real-world implementations.

The Citrix XenDesktop 7.6 Feature Pack 2 Blueprint provides a unified framework for developing a virtual desktop and application solution. The framework provides a foundation to understand the technical architecture for the most common virtual desktop/application deployment scenarios.

At a high-level, a virtual desktop solution is based on a unified and standardized 5-layer model.

1. User Layer – Defines the unique user groups, endpoints and locations.
2. Access Layer – Defines how a user group gains access to their resources. Focuses on secure access policies and desktop/application stores.
3. Resource Layer – Defines the virtual desktops, applications and data provided to each user group
4. Control Layer – Defines the underlying infrastructure required to support the users accessing their resources
5. Hardware Layer – Defines the physical implementation of the overall solution

The power of this model is that it is extremely flexible in that each user group can have their own set of access policies and resources or they can be shared, but regardless how the user, access and resource layers are defined, they are all managed by a single, integrated control layer, as shown in the following figure.

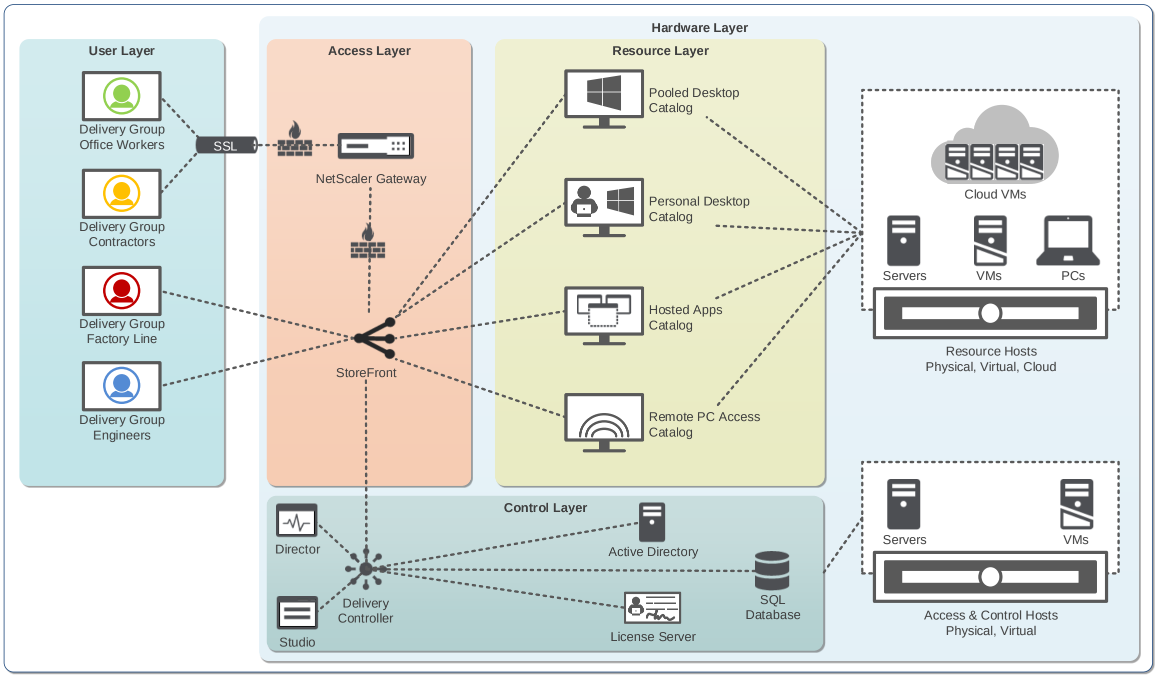


The XenDesktop 7.6 Feature Pack 2 blueprint details the recommended architecture for four common scenarios:

1. A standardized (pooled) Windows desktop
2. A fully customizable (personal) Windows desktop
3. Windows-based applications
4. Remote access to enterprise PCs

Conceptual Architecture

When put into practice, the 5-layer virtual desktop model results in a conceptual architecture like the following:



Based on the conceptual architecture, the following can be discerned:

- User Layer: There are four distinct delivery groups corresponding to different sets of users.
- Access Layer: Users access a list of available resources through StoreFront. For users not on the internal, protected network, like the Office Workers and Contractors user groups, must establish a SSL encrypted tunnel across public network links to the NetScaler Gateway, which is deployed within the DMZ area of the network.
- Resource Layer: Four types of resources are provided to the users:
  - Pooled Desktops: A hosted desktop-based Windows operating system where the desktop interface is remotely displayed, the virtual machine is individually shared amongst a pool of users and is reset to a clean state after each use.
  - Personal Desktops: A hosted desktop-based Windows operating system where the desktop interface is remotely displayed, the virtual machine is permanently assigned to a single user and all changes persist for the lifetime of the desktop.
  - Hosted Apps: A hosted server-based Windows operating system where the virtual machine is shared amongst a pool of users simultaneously while each user is encapsulated within their own session and only the application interface is remotely displayed.
  - Remote PC Access: A traditional, local Windows desktop, assigned to a single user and can be physically accessed locally or accessed remotely.
- Control Layer: The Delivery Controller authenticates users and enumerates resources from StoreFront while creating, managing and maintaining the virtual resources. All configuration information about the XenDesktop site is stored within the SQL database.
- Hardware Layer: The corresponding hosts provides compute and storage resources to the Resource Layer workloads. One set of hosts centrally delivers virtual servers and virtual desktops

from the data center while a second set of hosts correspond to the Access and Control layer servers.

Detailed Architecture

The high-level design for a standard virtual desktop solution is fairly straightforward by following the 5-layer model, which guides an organization to define the user groups before determining how they will access their resources. Once these aspects are defined, the design is finalized by detailing how the solution is controlled and managed and how the hardware will support the defined solution.

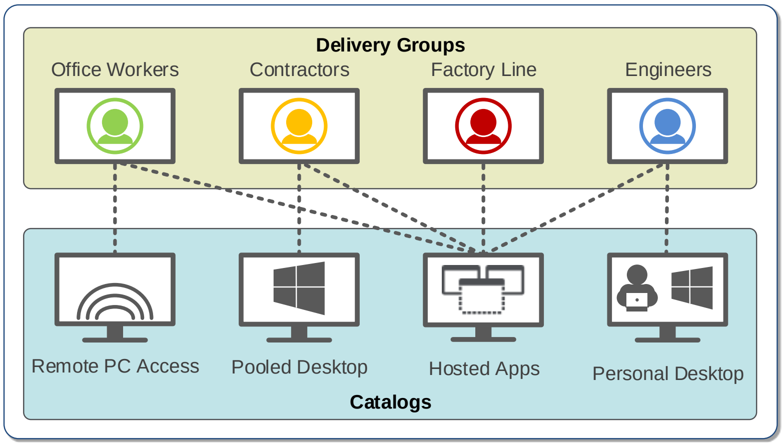
User Layer

Aligning the user requirements with an appropriate virtual desktop is the initial step in creating a complete, end-to-end solution.

Most environments typically have more than one type of user group with different requirements that must be met. However, even though there are many user groups within an organization, a large majority often fit into one of the following scenarios.

Users need access to…	Users include…	Endpoints include…	Common location(s) include…	IT Delivers…
Only Line-of-Business applications	Factory line workers Retail clerks Bank tellers Nurses’ station users Call centers	Thin clients PCs (new and old) Kiosks	Local, trusted network	Hosted applications
A standardized desktop environment	Contractors Partners	Personal devices	Local, trusted network or Remote, untrusted network	Shared desktop or Pooled desktop
A fully customizable desktop environment	Office Workers Consultants Engineers Designers	Thin clients PCs (new and old) Laptops	Local, trusted network or Remote, untrusted network	Personal desktop Or Remote PC Access
Line-of-Business and a fully customizable desktop environment	Road Warriors Executives	Tablets Smartphones Laptops	Local, trusted network or Remote, untrusted network	Hosted applications and Personal desktop

An important design element with XenDesktop 7.6 Feature Pack 2 is that user groups (delivery groups) can access more than one resource (catalog). Based on the conceptual architecture, the following defines the Delivery Group to Catalog allocation:

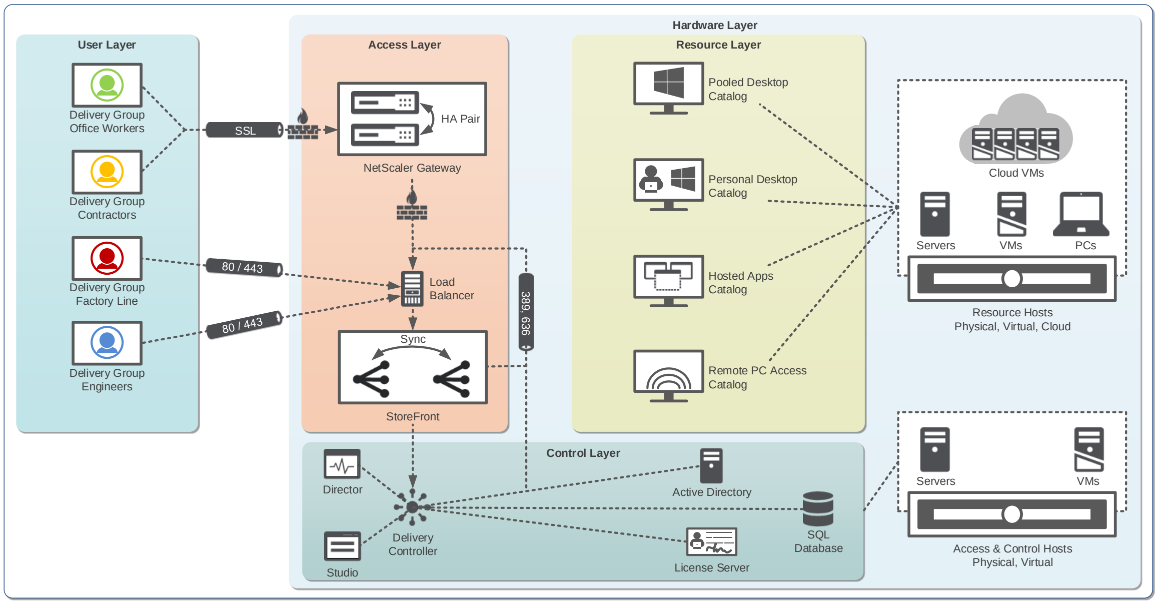


- Office Workers typically work from the office but require the ability to work from home on occasion.
- Contractors are hired to work on an internal project. A pooled desktop is provided because their endpoint devices are untrusted and they will require certain levels of access.
- Engineers require the ability to fully customize their desktop, which includes user-based applications.
- A set of line-of-business applications, required by every user group, are provided as a hosted app model, which allows an organization to centrally deliver a Windows-based application while guaranteeing a proper configuration.

Access Layer

Providing access to the environment includes more than simply making a connection to a resource. Providing the proper level of access is based on where the user is located as well as the security policies defined by the organization.

Based on the locations defined for each user group, the following diagram depicts the Access Layer for the solution along with design recommendations:



- StoreFront: Internal users access a StoreFront store either directly through Citrix Receiver or via the StoreFront web page. StoreFront not only provides a complete list of available resources for each user, but it also allows users to "favorite" certain applications, which makes them appear prominently. The subscriptions are synchronized to the other StoreFront servers automatically. Upon successful authentication, StoreFront contacts the Delivery Controller to receive a list of available resources (desktops and/or applications) for the user to select. Redundant StoreFront servers should be deployed to provide N+1 redundancy where in the event of a failure, the remaining servers have enough spare capacity to fulfill any user access requests.
- NetScaler Gateway: Remote users access and authenticate to the NetScaler Gateway, which is located within the network's DMZ. Upon successful validation against Active Directory, NetScaler Gateway forwards the user request onto StoreFront, which generates a list of available resources. This information is passed back to the user through NetScaler Gateway. When a user launches a resource, all traffic between the user and NetScaler Gateway is encapsulated within SSL en-route to the virtual resource. Redundant NetScaler Gateway devices should be deployed to provide N+1 redundancy.
- Load Balancers: Based on the "N+1" recommendations for many of the control layer components, it is advisable to have an intelligent load balancing solution in place, which is capable of not only identifying if the server is available, but also that the respective services and functioning and responding correctly. Implementing an internal and light-weight pair of NetScaler VPX virtual servers can easily accommodate the load balancing requirements for the solution.

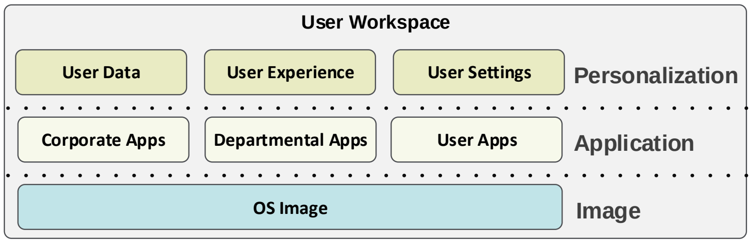
It is important to note that users might access the environment from different locations, requiring policies to be intelligent enough to detect and respond appropriately. In most environments, tougher security policies are put into place when users access the environment from a remote, untrusted network as compared to a local, trusted network. This often includes tougher authentication policies (like multi-factor authentication) and greater protocol protection with encryption and encapsulation.

Users connecting from…	Local, trusted network	Remote, untrusted network
Authentication Point	StoreFront	NetScaler Gateway
Authentication Policy	Simple authentication (username and password)	Multi-factor authentication (username, password and token)
Session Policy	Not applicable	Mobile and Non-Mobile
Session Protocol (Profile)	ICA	ICA Proxy

***Note**: For "Remote, untrusted network" two different session policies are used to provide the correct user experience based on being on a mobile device (smartphone or tablet) versus a non-mobile device (laptop or desktop). The details for the session policies are detailed in* Appendix: Session Policy Details*.*

Resource Layer

Users need access to their resources, whether those resources are desktops or applications. The configuration of the resources must align with the overall needs of the user groups. In order to align each resource with each user group, the resource is defined across three separate but integrated layers, creating a user workspace.

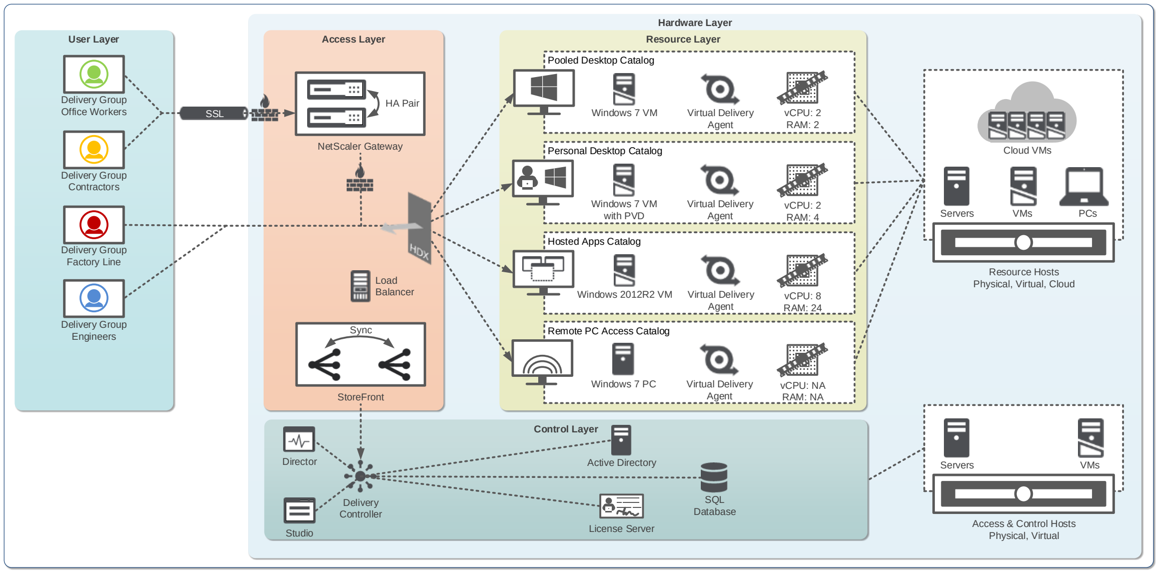


Each layer and component within the layer must be delivered appropriately.

Image

The first part of the image definition is selecting the right operating system and size of the virtual instance, which is based on the type of desktop IT delivers to the user as well as the standards for the organization.

Based on the types of resources defined for each user group, the following diagram depicts the resource configurations:



Properly sizing the virtual desktops and virtual servers are based on the Citrix best practices, which are defined in the following table:

Resource Type	OS	vCPU	RAM	Image Size	Cache Size	Users per VM	VMs per Server
XenDesktop - Personal or Pooled desktop	Windows 7	2 vCPU	2 GB	35 GB	5 GB	1	140-200
	Windows 8	2 vCPU	2 GB	35 GB	5 GB	1	135-190
	Windows 8.1	2 vCPU	2 GB	35 GB	5 GB	1	135-190
XenApp - Hosted Apps or Shared desktops	Windows 2008R2	4 vCPU	12 GB	60 GB	15 GB	20-30	8
	Windows 2012	8 vCPU	24 GB	60 GB	30 GB	48-68	4
	Windows 2012R2	8 vCPU	24 GB	60 GB	30 GB	48-68	4

***Note:** vCPU recommendations for hosted apps and shared desktop are based on dual processor servers with 8 cores each (16 total cores).*

***Note:** The recommendations are based on a normal workload for office-based user.*

***Note**: Hypervisor based on Windows Server 2012R2 with Hyper-V.*

The second aspect of the image definition is the delivery fabric, which is independent of the selected operating system. XenDesktop 7.6 Feature Pack 2 includes two integrated solutions focused on providing different benefits to an organization. These options are:

- Machine Creation Services (MCS): Utilizes the hypervisor and storage infrastructure (local or shared storage) to create unique, thin provisioned clones of a master image, which can either be a desktop-based OS or a server-based OS. Due to the focus on simplicity, MCS requires no extra hardware and utilizes functionality within the hypervisor. Due to the simplicity of MCS, it is the recommended option for deployments that do not require desktop delivery to physical targets or image update automation.
- Provisioning Services (PVS): Provides advanced image delivery technology by utilizing the network infrastructure to deliver required portions of an image, just-in-time, to a physical or virtual machine with either a desktop-based OS or a server-based OS. Although this model does require additional virtual servers to provide the image streaming technology, it is a full image life-cycle solution that includes functionality to reduce storage throughput to near 0 IOPS per user, consolidate storage space, automate image maintenance activities, and provide fast rollback capabilities.

Applications

The most important aspect of the resource layer are the applications, which is what the users are trying to access. In order to have a successful application delivery solution, an application delivery strategy must be defined:

- Installed: The applications are installed in the master desktop image. Even though this option can result in a greater number of master desktop images if the application sets between user groups greatly differ, it is the recommended approach due to its simplicity and familiarity. This is the best approach for applications used by 75%+ of the user population.
- Hosted: The applications are installed and published from a server-based OS running XenApp 7.6. Each application is published to a set of user groups. When accessed, the application executes on the central hosting server and then remotely displaying the user interface on the user’s desktop. This is the best approach for line of business applications that are used by 50-75% of the user population.
- Streamed: The applications are dynamically delivered to the virtual/physical desktop/server when requested, with a solution like Microsoft App-V. This solution requires additional products and infrastructure, but is the most dynamic option resulting in the fewest number of master images.
- User-based: Many applications are not managed or maintained by IT, and are considered user-based applications. Due to the small percentage of users who use these applications, it is not justified to make these applications IT-managed applications. Users who require user-based applications can either
    - Receive a personal desktop where they can install and maintain their own set of applications through XenDesktop Personal vDisk technology.
    - Receive a pooled desktop and seamlessly access applications installed on their physical endpoint within their virtualized desktop session with the use of “Local App Access” policy.

Personalization

The final component of the resource layer is focused on the personalization of the user’s workspace: defining how customized each group can make their workspace while providing the right user experience. Each user group/resource combination typically results in one of three options:

- Locked: Changes are discarded

- Basic: Basic application setting changes persist
- Complete: All changes persist

The three options are implemented with the use of XenDesktop policies and are configured as follows:

Personalization Profile	Locked	Basic	Complete
Enable Profile Management	Enabled	Enabled	Enabled
Path to user store	UNC path	UNC path	UNC path
Process logons for local admins	Enabled	Enabled	Enabled
Process Internet cookie files on logoff	Enabled	Enabled	Enabled
Exclusion list – Directories	See Appendix: Profile Policy Details	See Appendix: Profile Policy Details	See Appendix: Profile Policy Details
Directories to synchronize	See Appendix: Profile Policy Details	See Appendix: Profile Policy Details	See Appendix: Profile Policy Details
Files to synchronize	See Appendix: Profile Policy Details	See Appendix: Profile Policy Details	See Appendix: Profile Policy Details
Folders to mirror	See Appendix: Profile Policy Details	See Appendix: Profile Policy Details	See Appendix: Profile Policy Details
Delete locally cached profiles on logoff	Enabled	Enabled	Disabled
Local profile conflict handling	Delete local profile	Delete local profile	Delete local profile
Migration of existing profiles	None	None	None
Profile streaming	Disabled	Disabled	Disabled
Grant administrator access	Enabled	Enabled	Enabled
Profile Folder Redirection (Do not add these to exclusion list)	None	AppData(Roaming) Contacts Desktop Documents Downloads Favorites Music Pictures Videos	AppData(Roaming) Contacts Desktop Documents Downloads Favorites Music Pictures Videos

The XenDesktop policies determine how much personalization a user can do to their workspace. Regardless of the user's personalization, the right user experience must be delivered in all scenarios. XenDesktop user and computer policies help define how the session is configured based on the user's end point device, location or accessed resource. Recommended policies are as follows:

- Unfiltered: The unfiltered policy is the system-created default policy providing a baseline configuration for an optimal experience. Each user group receives this policy with additional policies incorporated to customize the experience based on use case or access scenario.

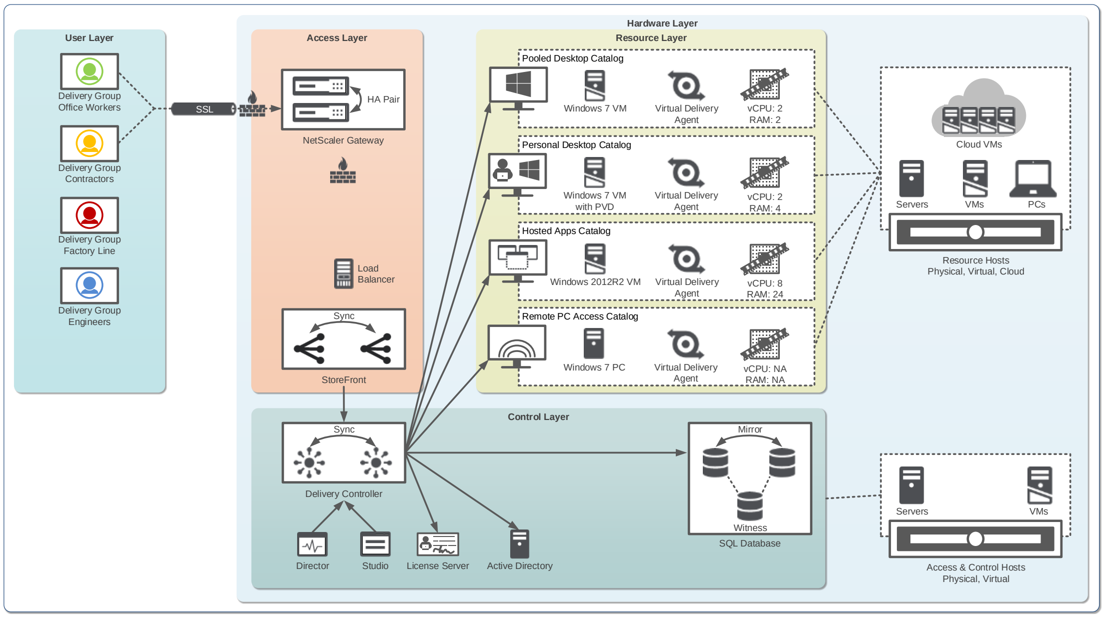
- Remote access policy - Optimized for WAN: The remote access policy includes settings to better protect the resources as they will be accessed from remote and potentially unsecure locations. Applied to all sessions coming through NetScaler Gateway.
- Local access policy - High Definition User Experience: The local access policy focuses on a high quality user experience at the expense of bandwidth, which should be plentiful on a local connection scenario.
- Mobile device policy: The mobile device policy helps improve the user experience for any user who utilizes a tablet, smartphone or other small form factor device.

Once defined, each policy must be properly applied to the right set of objects and scenarios. These policies are applied as follows:

Policy Name	Settings or Template	Assigned to…
Unfiltered	Not applicable	Not applicable
Remote access policy	Template: Optimized for WAN	Access Control – With NetScaler Gateway
Local access policy	Template: High Definition User Experience	Access Control – Without NetScaler Gateway
Mobile device policy	Mobile Experience • Automatic keyboard display: Allowed • Launch touch-optimized desktop: Allowed • Remote the combo box: Allowed	User group name

Control Layer

Every major design decision made within the User, Access and Resource layers are used to help design the control components of the overall solution. These components include delivery controllers, SQL databases, license servers and imaging controllers, which can be seen in the following figure:



Properly sizing the control layer is based on the Citrix best practices, which are defined as follows.

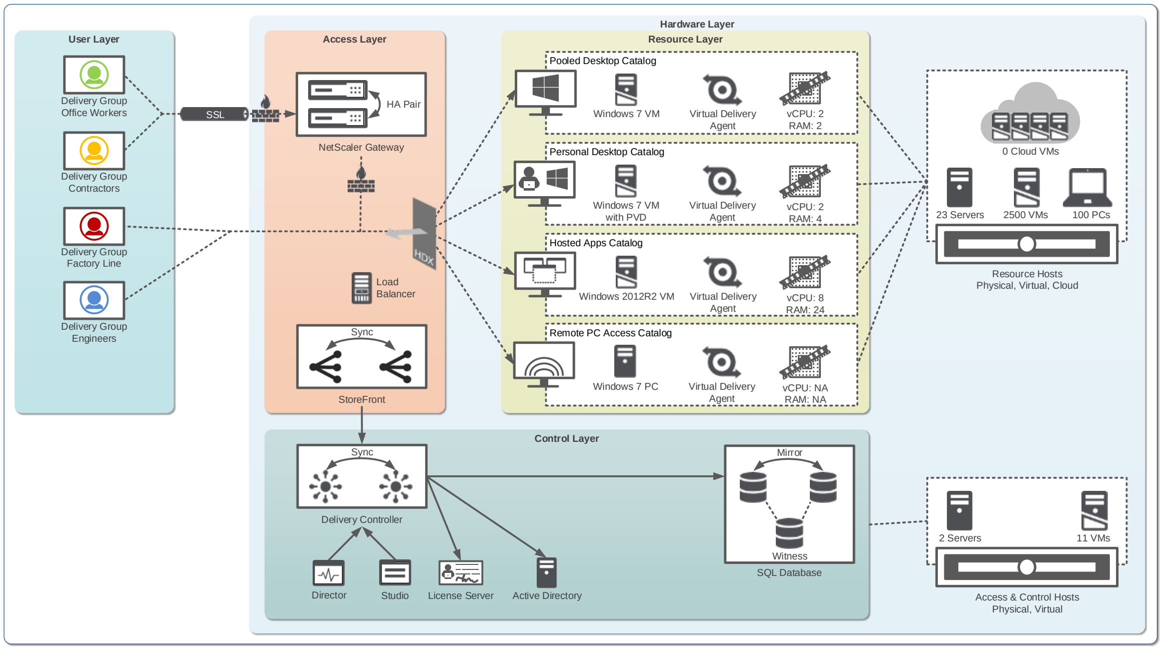
Component	Category	Best Practice
Delivery Controller	High-Availability	Use an “N+1” redundancy calculation, where “N” is the number of controllers required to support the environment.
License Server	High-Availability	Because the environment continues to function in a 30-day grace period if the license server is offline, no additional redundancies are required.
SQL Database	Mirroring	Due to licensing costs, a 3-node mirror configuration is typically recommended: • Node 1: Primary Mirror (SQL Standard) • Node 2: Secondary Mirror (SQL Standard) • Node 3: Witness (SQL Express)

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

- Network Services, like DNS and DHCP, for name resolution and IP address assignment.
- Active Directory for user authentication

Hardware Layer

The hardware layer is the physical implementation of the virtual desktop solution. It answers the fundamental question of “How many servers do I need to support my users?”



A set of hardware is defined for Resource layer hosts, which is broken up as follows:

- For the server hosted resources (pooled, personal and hosted apps), a set of physical servers that are often virtualized into a number of virtual machines. With XenDesktop 7.6 Feature Pack 2, the hardware layer can also include cloud hosted desktops and apps with the integration of Amazon AWS and CloudPlatform.
- For the client hosted resources (Remote PC Access), hardware is also required, but this hardware is located with the user, outside of the data center and takes the form of laptops and PCs.

A second set of hardware is defined to support the Access and Control layers of the solution. This will take the form of physical and virtual server workloads.

Completing the hardware layer framework includes additional decisions on the storage fabric and server footprint, which are often decisions made based on relationships organizations have with different vendors.

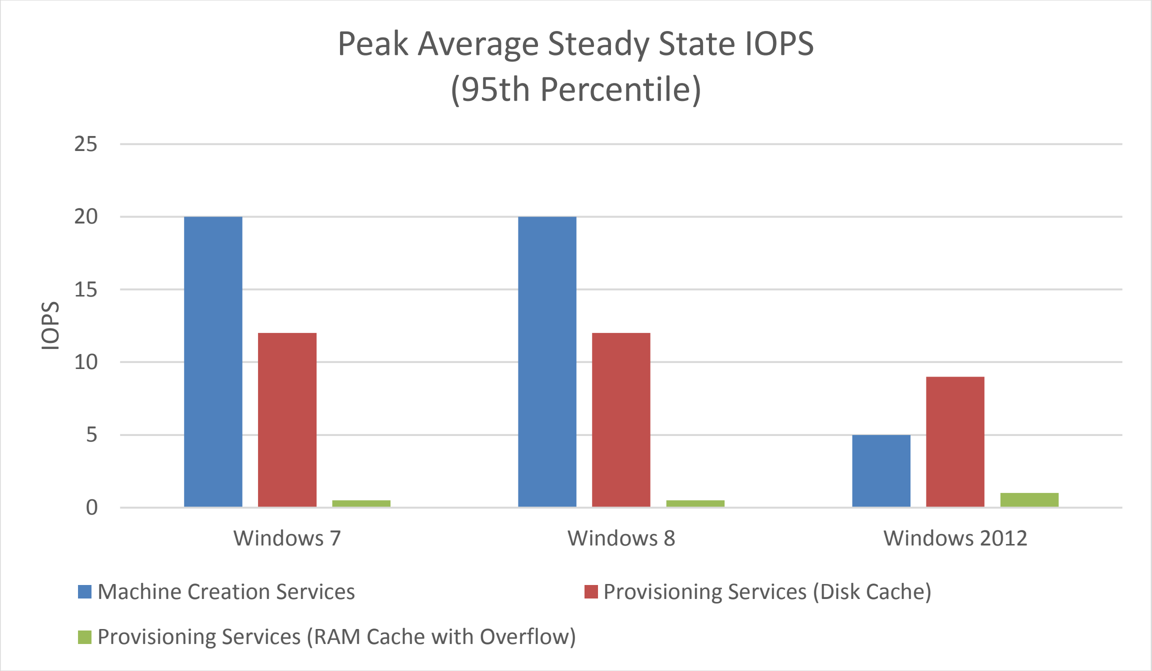
Storage Fabric

Storage is often considered one of the most important and complex decisions in a virtual desktop solution. In addition to impacting the cost of the solution, the selected storage fabric also impacts the available options for physical server footprint, which is why selecting a storage solution is the first step in the hardware layer design.

Storage Type	Benefits	Concerns	Appropriate for…
Local Storage	Inexpensive Simple to deploy	Virtual machines are inaccessible if physical server is offline Limited number of disk spindles (based on server design) Longer operational processes as each local store must be updated	Rack servers
Direct Attached Storage	Moderate expense Virtual machine migration when physical server is offline	Failure on DAS array can impact multiple physical servers DAS interconnects consume valuable space in a blade chassis Limited number of connections to a DAS array	Rack servers
Centralized Storage	Shared master image across physical servers Virtual machine migration when physical server is offline Simple expansion Advanced features to help offset costs	Expensive Complex Often requires storage tiers to control costs	Blade servers

Regardless of the storage fabric selected, an appropriate amount of storage resources (space and IOPS) must be available in order to provide an acceptable user experience. Each read/write operation to the disk must wait in line before it is serviced. If the capacity of the storage infrastructure is not high enough, an IO request wait time increases, negatively impacting the user experience.

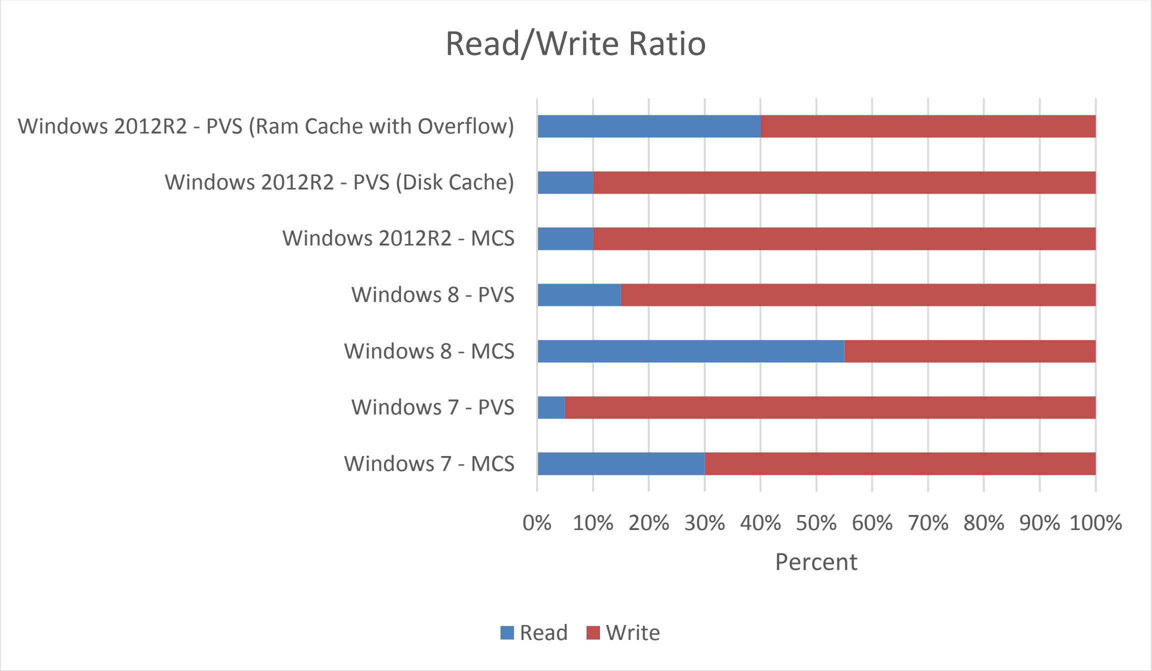
Using an average for IOPS activity could result in an under-scoped storage solution. In order to better accommodate peaks of storage activity, a peak average calculation is used that is based on the 95th percentile, which is depicted in the following graph:



***Note**: Based on Windows Server 2012 with Hyper-V and vSphere 5.5.*

***Note:** Peak average steady state IOPS for Windows 7 and Windows 8 utilizing the RAM Cache with Overflow feature of Provisioning Services is 0.01 IOPS per user.*

In addition to IOPS activity, the read/write ratio also must be taken into account, which is based on the following:



***Note**: Hypervisor optimizations, like Hyper-V CSV cache, XenServer IntelliCache, and vSphere CBRC can reduce read IOPS for Machine Creation Services delivered desktops.*

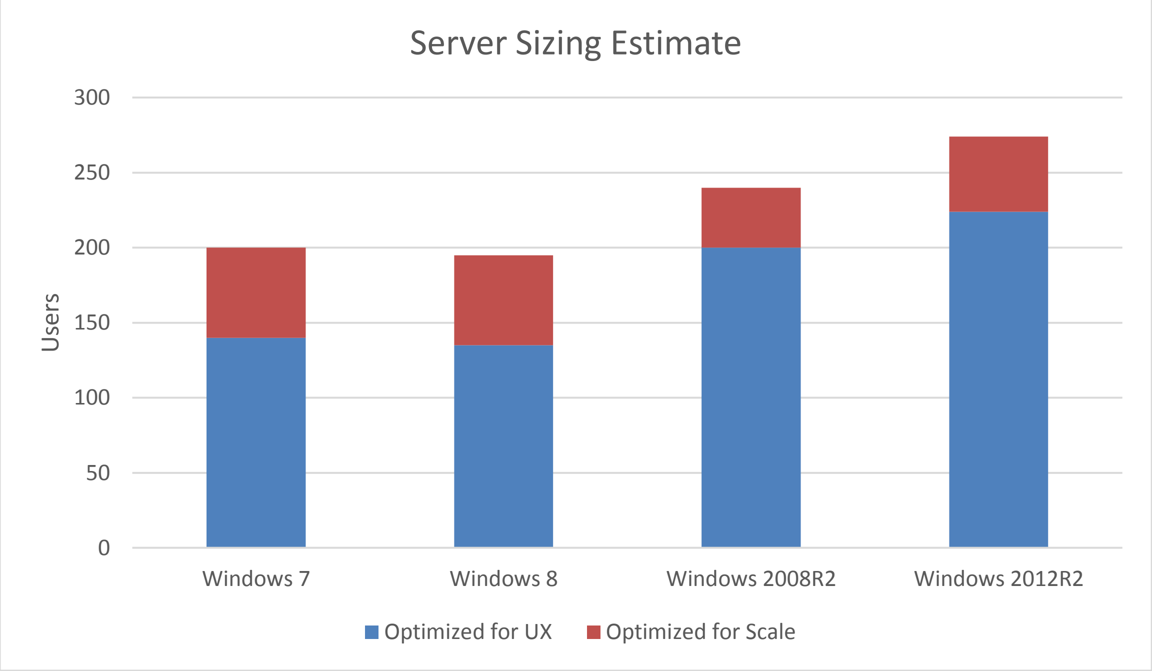
Server Footprint

At the hardware layer of the virtual desktop design, organizations must decide on the hardware footprint, which generally is a decision between blade servers and rack servers.

Server Type	Benefits	Concerns	Appropriate for…
Blade Servers	Higher density within same amount of rack space Consolidated network cabling requiring fewer core switch ports	Upfront costs are generally higher Limited amount of internal storage	Large deployments with shared storage
Rack Servers	Large amount of local storage Adding network capacity simply requires new network card	Greater power requirements Uses more switch ports Less density within a rack	Large or small deployments with local storage

Server Sizing

In order to start estimating the number of physical servers required to support a normal user workload of Office applications with minor Internet browsing and multimedia usage, the following can be used as a starting estimate:



***Note**: Based on dual Xeon E5-2690 2.9GHz processors running on Windows Server 2012R2 Hyper-V. The amount of RAM allocated to each server is based on the expected number of virtual machines multiplied by the amount of RAM required for each virtual machine.*

***Note**: Optimized for scale reduces vCPU allocation for the desktop OS from 2 to 1 and also reduces the graphics quality by utilizing legacy graphics.*

Agents, applications and configurations will play a big part in the overall density of a single server. For example, the following items have been shown to directly impact density and should be taken into account as part of the planning process:

- Antivirus: With antivirus added into the image, single server user density will decrease by 10-20%.
- Personal vDisk: For Windows 7 and Windows 8 desktops, the inclusion of Personal vDisk functionality will reduce single server user density by 5-15%.

- Microsoft Office 2013: Utilizing Microsoft Office 2013 versus previous versions (2007 and 2010) will reduce single server user density by 20%.

Next Steps

The XenDesktop 7.6 Feature Pack 2 blueprint is the first step towards delivering a virtual desktop solution within an organization. Based on the unified infrastructure of XenDesktop 7.6, there are few decisions that fundamentally impact the overall architecture. In fact, the two decisions that are unique for each organization are contained within the Hardware layer and are based solely on the organization's anticipated deployment size and existing relationships with storage and server vendors.

To learn more about the potential a solution like XenDesktop 7.6 Feature Pack 2 can provide, it is recommended to follow the prescribed roadmap in order to gain knowledge and firsthand experience.

- XenDesktop 7.6 Feature Pack 2 Blueprint: A layered solution for all successful designs & deployments, focusing on the common technology framework and core decisions.
- Reviewer's Guide: Prescriptive guide for getting 5-10 users deployed quickly and easily in a non-production environment.
- Design Guides: Recommended designs, with hardware layer planning numbers, for commonly used implementations, which can be combined together to form a more complete solution. Available design guides include
    - XenApp Design Guide: Mobilizing Windows Apps on vSphere
    - XenApp Design Guide: Mobilizing Windows Apps on Hyper-V
    - XenDesktop Design Guide: Secure Remote Access to Enterprise PCs
    - XenDesktop Design Guide: Pooled VDI on vSphere
    - XenDesktop Design Guide: Pooled VDI on Hyper-V

All of these materials, and more, are located on the Tech Info page of XenDesktop

Glossary

Hosted Shared Desktop: A type of virtual desktop based on a Windows server operating system. This type of virtual desktop is sometimes referred to as Remote Desktop Services (RDS) or Hosted Server Virtual Desktops (HSVD). With Hosted Shared Desktop, multiple users share the same desktop but their sessions are separated through session virtualization.

Machine Creation Services: An image delivery technology, integrated within XenDesktop that utilizes hypervisor APIs to create unique, read-only and thin provisioned clone of a master image where all writes are stored within a differencing disk.

Hosted Apps: A type of virtual desktop based on Windows server operating system. This type of virtual desktop is sometimes referred to as virtual applications, published applications or seamless applications. Hosted apps are similar in approach to Hosted Shared Desktops, except that the physical desktop interface is hidden from the user. When a user uses a Hosted App, they only see the application and not the underlying operating system, making Hosted Apps a powerful solution for mobile devices.

Personal Desktop: A type of virtual desktop based on a Windows desktop operating system. This type of virtual desktop provides a unique Windows desktop to each user either for the duration of the session or indefinitely.

Personal vDisk: A technology used on conjunction with Personal VDI desktops allowing for complete personalization while still utilizing a single, read-only master image. Any changes made the master image are captured and stored within a virtual hard disk attached to the virtual machine. Changes are cataloged in order to allow an administrator to update the master image without impacting user-level changes.

Provisioning Services: An image delivery technology, integrated within XenDesktop, which utilizes PXE booting and network streaming. A target device requests and receives appropriate portions of the master image from the provisioning server when needed. Any changes made during the duration of the session are stored in a temporary write cache.

Profile Management: A user profile solution, integrated with XenDesktop, that overcomes many of the challenges associated with Windows local, mandatory and roaming profiles through proper policy configuration. Profile Management improves the user experience by capturing user-based changes to the environment and by improving user logon/logoff speed.

Appendix: Profile Policy Details

The following outlines the initial inclusion/exclusion configurations recommended for an optimized user profile policy.

Policy	Setting(s)
Exclusion list - Directories	AppData\Local AppData\LocalLow AppData\Roaming\Citrix\PNAgent\AppCache AppData\Roaming\Citrix\PNAgent\Icon Cache AppData\Roaming\Citrix\PNAgent\ResourceCache AppData\Roaming\ICAClient\Cache AppData\Roaming\Microsoft\Windows\Start Menu AppData\Roaming\Sun\Java\Deployment\cache AppData\Roaming\Sun\Java\Deployment\log AppData\Roaming\Sun\Java\Deployment\tmp Application Data Citrix Java Local Settings UserData AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys AppData\Roaming\Macromedia\Flash Player\#SharedObject AppData\Roaming Saved Games
Synchronized Directories	AppData\Roaming\Microsoft\Credentials AppData\Roaming\Microsoft\Crypto AppData\Roaming\Microsoft\Protect AppData\Roaming\Microsoft\SystemCertificates AppData\Local\Microsoft\Credential
Synchronized Files	Microsoft Outlook • AppData\Local\Microsoft\Office\*.qat • AppData\Local\Microsoft\Office\*.officeUI Google Earth • AppData\LocalLow\Google\GoogleEarth\*.kml
Mirrored Folders	AppData\Roaming\Microsoft\Windows\Cookies

Appendix: Session Policy Details

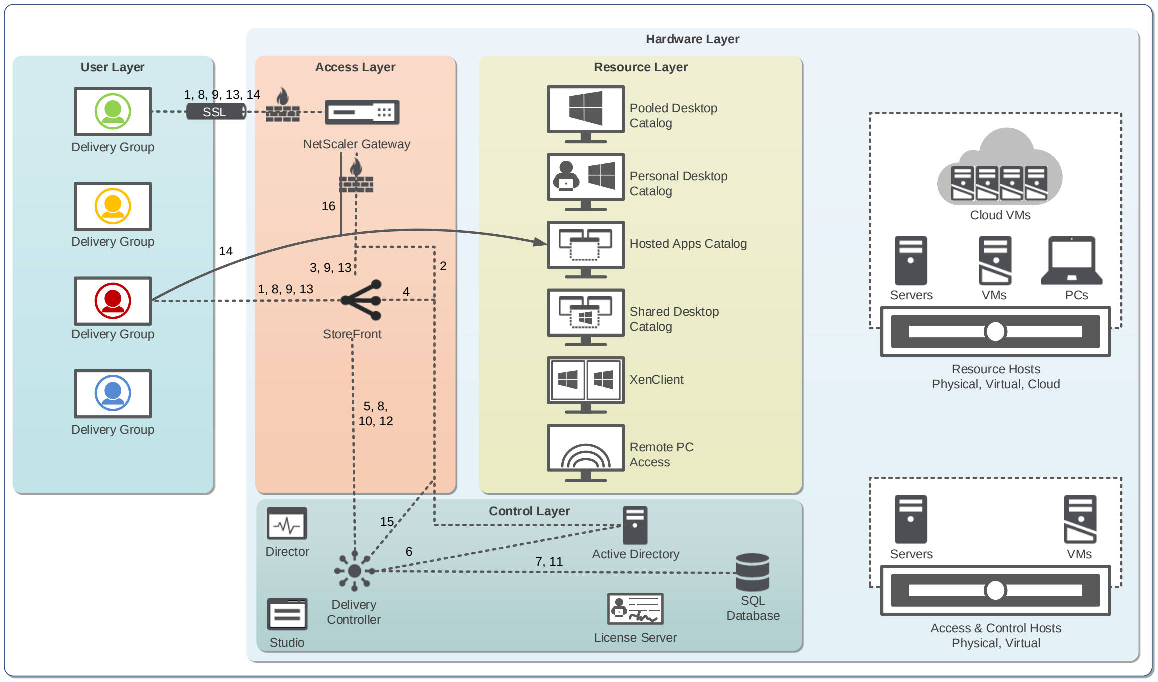
Devices are commonly grouped as either non-mobile (such as Windows desktop OS based), or mobile (such as iOS or Android). Therefore, a decision whether to provide support for mobile devices, non-mobile devices, or both should be made based on user group requirements.

To identify mobile and non-mobile devices, session policies defined on NetScaler Gateway should include expressions such as:

- **Mobile Devices:** The expression is set to “REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver” which is given a higher priority than the non-Mobile device policy to ensure mobile devices are matched while non-Mobile devices are not.
- **Non-Mobile Devices:** The expression is set to “ns_true” which signifies that it should apply to all traffic that is sent to it.

Appendix: Authentication Process

When a user authenticates to the environment to receive a list of available resources, the communication process is as follows:



Step	Local Users	Remote Users
1.	A user initiates a connection to the StoreFront URL (443), which can be a virtual address hosted by a load balancer, and provides logon credentials. This can either be done by using a browser or Citrix Receiver.	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 XenDesktop 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 (80 or 443).	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 (443).	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).	
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 creates a launch file, which is sent to the user (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).
14.	Citrix Receiver uses the launch file and makes a connection to the resource (1494 or 2598).	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.

The copyright in this report and all other works of authorship and all developments made, conceived, created, discovered, invented or reduced to practice in the performance of work during this engagement are and shall remain the sole and absolute property of Citrix, subject to a worldwide, non-exclusive license to you for your internal distribution and use as intended hereunder. No license to Citrix products is granted herein. Citrix products must be licensed separately. Citrix warrants that the services have been performed in a professional and workman-like manner using generally accepted industry standards and practices. Your exclusive remedy for breach of this warranty shall be timely re-performance of the work by Citrix such that the warranty is met. THE WARRANTY ABOVE IS EXCLUSIVE AND IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE WITH RESPECT TO THE SERVICES OR PRODUCTS PROVIDED UNDER THIS AGREEMENT, THE PERFORMANCE OF MATERIALS OR PROCESSES DEVELOPED OR PROVIDED UNDER THIS AGREEMENT, OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM, AND ALL IMPLIED WARRANTIES OF MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, OR AGAINST INFRINGEMENT. Citrix' liability to you with respect to any services rendered shall be limited to the amount actually paid by you. IN NO EVENT SHALL EITHER PARTY BY LIABLE TO THE OTHER PARTY HEREUNDER FOR ANY INCIDENTAL, CONSEQUENTIAL, INDIRECT OR PUNITIVE DAMAGES (INCLUDING BUT NOT LIMITED TO LOST PROFITS) REGARDLESS OF WHETHER SUCH LIABILITY IS BASED ON BREACH OF CONTRACT, TORT, OR STRICT LIABILITY. Disputes regarding this engagement shall be governed by the internal laws of the State of Florida.

851 West Cypress Creek Road Fort Lauderdale, FL 33309 954-267-3000 http://www.citrix.com