Partner and Customer Toolkit
XenDesktop 2.0

Worldwide Consulting Solutions

Pilot Reference Architecture

Overview

Properly delivering desktops to users is a core requirement for just about any business. If users are unable to use their desktops or applications, the business cannot function at full utilization. Every few years, just about every business undergoes a massive rollout of a new operating system, new hardware or new applications requiring a swarm of individuals to build, test and rollout the newest systems to the masses. Because of this enormous undertaking, many organizations hold off on beneficial upgrades, which oftentimes limit how fast the organization can turn to changing market demands.

There are automated tools from numerous vendors to help in the deployment of new applications and operating systems, but the question should be raised if deploying applications out to the user population is still the best approach. This type of approach incurs numerous consequences impacting the user and the business like:

- Loss of end-user device opens up significant security concerns for lost data
- Corruption of the operating system or application by malicious or inadvertent acts requires extensive troubleshooting and administrative time resulting in end-user downtime
- System upgrades are delayed due to the costs associated with the procurement of new hardware

Instead of going down the old approach of deploying operating systems and applications to thousands of physical workstations, a dynamically provisioned virtual desktop environment will offer organizations the ability to provide their users that latest environments without the time and costs associated with a large-scale desktop rollout. Before the rollout begins, it is recommended a pilot program is launched that validates the recommended design based on business and user requirements. This document provides a reference architecture for a XenDesktop Pilot. It is broken up into the following components:

- Virtual Desktop Requirements
- Solution Overview
- Technical Architecture

Virtual Desktop Requirements

The pilot is the last stage of testing and validating the design and environment build before moving towards a full-scale production rollout. A small set of users will work with the production-level environment and validate the solution is functional and meets the overall virtual desktop requirements. For the architecture defined throughout this document, the following requirements are used:

- Users should be able to personalize their virtual desktop environment with application configurations, environment settings and user preferences. The personalization settings should follow the user from system-to-system.

- Users should be able to continue working within their virtual desktop even if there is a failure of a component within the environment.
- Users should be able to get access to their virtual desktop securely and over remote connections without relying on a VPN client
- A single base standard image should be used for all users within the pilot group.
- Updating the operating system with the latest security patches should only be required on a single image. Those changes should be propagated to all users' virtual desktops.
- Users should only see the applications they have been assigned as seeing all applications causes confusion.

Solution Overview

The XenDesktop solution is comprised of a number of components to allow for the best solution for each organization's unique demands. Based on the requirements of the pilot, the overview architecture of the solution is identified in Figure 1.

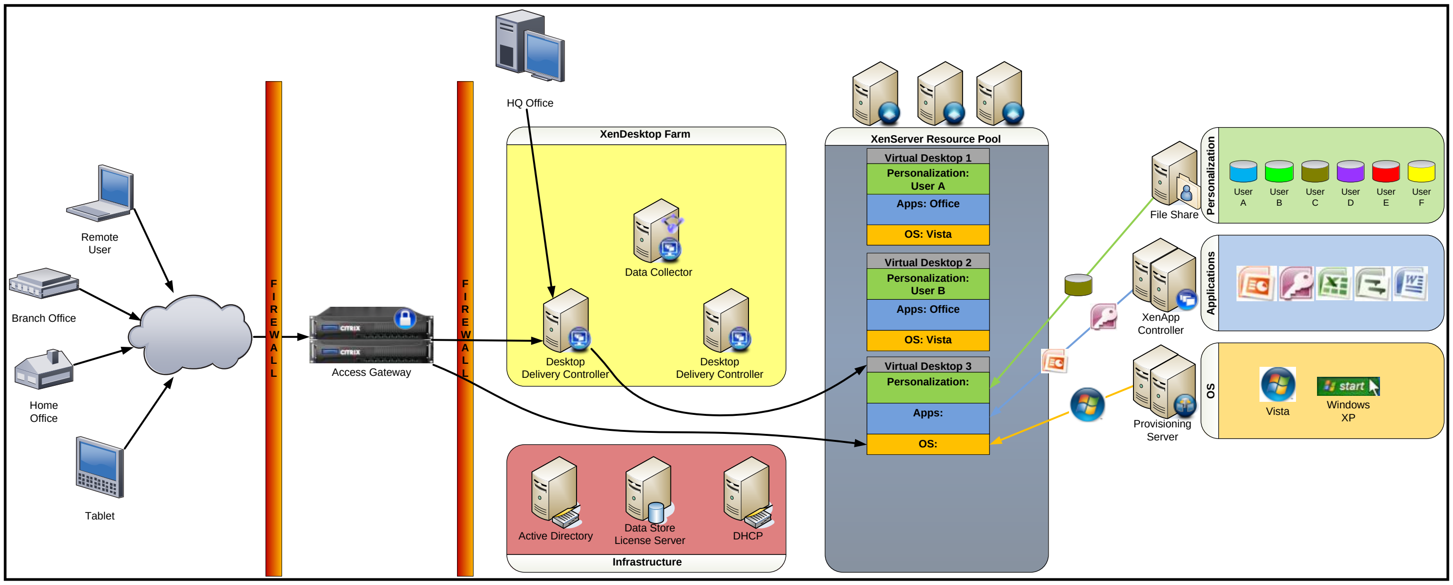

Figure 1: Overall Architecture

The architecture can be broken down into six core components:

1. Virtualization Infrastructure: The virtualization infrastructure allows for the dividing of a single physical server into multiple virtual servers all sharing resources. The virtualization infrastructure for this pilot architecture is based on XenServer as it is included as part of the XenDesktop overall solution. The virtualization infrastructure could also leverage Microsoft Hyper-V or VMware ESX.
2. Virtual Desktop Delivery Controller: The virtual desktop delivery controller is responsible for the registration of new virtual desktops and directing requests for virtual desktops to available systems. Users interact indirectly with the controller via the integrated Web Interface component. Through a web-based site, or through a locally installed receiver, users will be delivered their virtual desktop.
3. Virtual Desktop Provisioning: The provisioning server aspect of the XenDesktop solution delivers an operating system image to the virtual desktop instance on the virtualization infrastructure. A base operating system image is created that contains all operating system-level configurations as dictated by the organization's policies. The base image, however, does not contain applications. As each virtual desktop boots, the operating system is streamed over the network to the virtual desktop. The power of this solution is identified when updates are

required as only the base image requires updating and all virtual desktops will utilize the latest image upon next reboot. By stripping out the applications, a single instance of each operating system version is required for an organization.

4. Application Delivery Controller: The application delivery controller is responsible for identifying the user's assigned applications and delivering them to the virtual desktop. Application delivery is the first part of personalizing the user's desktop based on their needs. By separating the applications from the base desktop image, fewer desktop images are required, which simplifies maintenance.
5. Personalization: The personalization aspect of the solutions allows the user to customize their work environment as their needs dictate. With user personalization, the user settings are stored and travel with the user regardless of desktop they access. User personalization is more than roaming profiles, as the Citrix User Profile Manager strips out all unwanted settings and only keeps those items of value to the user. Also, the delivery of the personalization settings is optimized so the user is not left waiting for their virtual desktop to load.
6. Access Gateway: The Access Gateway component allows users to work remotely while keeping the connection secure. When used with XenDesktop, the communication to the virtual desktop is encapsulated inside of SSL communication, which does not require the opening of any additional ports on the external firewall besides the common port of SSL (443). Also, Access Gateway does not require the use of a client-side agent when users access XenDesktop virtual desktops. This greatly simplifies the end-user experience.

This is just a high-level overview of the entire architecture. The following section will go into more detail as to how the system works together to deliver a virtualized desktop for the identified pilot environment.

Technical Architecture

Every component works together to deliver a dynamic virtual desktop environment to a user. Depending on the requirements, certain components can be removed of modified. All six aspects of the solution will be used based on this particular scenario. Looking into the architecture a little deeper, the following services are utilized:

End-Point

- Desktop Receiver: The Citrix client installed on the end-point, which allows connections to the virtual desktop using the Citrix ICA protocol.

Access Gateway

- SSL-VPN: Acts as a secure proxy from the external end-point to the virtual desktop. Traffic leaving the SSL-VPN and destined for the public network is encapsulated within SSL. The SSL-VPN website is where users enter in their logon credentials.
- Authentication Service: Responsible for providing Web Interface with credentials. This process allows the user to authenticate once to the SSL-VPN and have the remaining authentication challenges provided automatically.

Desktop Delivery Controllers (XenDesktop Servers)

- Web Interface: Responsible for providing a graphical display for users to see their available virtual desktops.
- XML Service: Responsible for communications between the Web Interface component and the XenDesktop farm. The XML Service authenticates users, provides a list of available virtual desktops, and generates the information to allow the end-point to make a connection to the virtual desktop.
- Controller Service: Responsible for communicating with the Virtual Desktop Service on the virtual desktops. The Controller Service registers the virtual desktops and maintains the virtual desktop state.
- Pool Service: Based on the XenDesktop farm configuration, the Pool Service contacts the virtualization infrastructure to spin up/down a virtual desktop.
- IMA Service: The IMA Service is responsible for all inter-server communication between Desktop Delivery Controllers. This includes the traffic going to and coming from the data collector.

Virtual Desktop

- Virtual Desktop Service: Responsible for registering with a Desktop Delivery Controller and maintaining a heartbeat with the controller. If the heartbeat fails, the Virtual Desktop Service will re-register with another available Desktop Delivery Controller.
- Application Receiver: With appropriate credentials, the Application Receiver contacts the Application Delivery Controller to receive a list of available applications. The Application Receiver also is responsible for making requests to the Application Delivery Controllers for application launches.

Application Delivery Controllers (XenApp Servers)

- Web Interface: Responsible for providing a set of available applications to the Application Receiver based on user credentials.
- XML Service: Responsible for communications between the Application Delivery Controller's Web Interface component and the XenApp farm. The XML Service authenticates users, provides a list of available applications, and generates the information to allow the virtual desktop to make a connection to the application (hosted or streamed).
- IMA Service: The IMA Service is responsible for all inter-server communication between Application Delivery Controllers. This includes the traffic going to and coming from the data collector.

Provisioning Servers

- TFTP: When a new virtual desktop boots, it contacts DHCP to find an IP address and the location of the boot file. The boot file comes from the Provisioning Server via the TFTP service.
- Streaming Service: After the virtual desktop receives the boot file with instructions, it contacts the provisioning server and provides its MAC address. Provisioning Server identifies the correct virtual disk based on the MAC address and uses the Streaming Service to send portions of the virtual disk to the virtual desktop as needed.

Each component is utilized during different periods of the virtual desktop connection process. The following subsections goes into greater details of what occurs and the components used:

- Virtual Desktop Startup
- Authentication
- Virtual Desktop Connection
- Virtual Desktop Personalization

Virtual Desktop Startup

The first stage of the XenDesktop architecture is getting virtual desktops online. The Data Collector refers to the Idle Desktop thresholds and determines current availability. When a new virtual desktop is required to meet the idle threshold limits, the Data Collector implements the startup procedure with the following process:

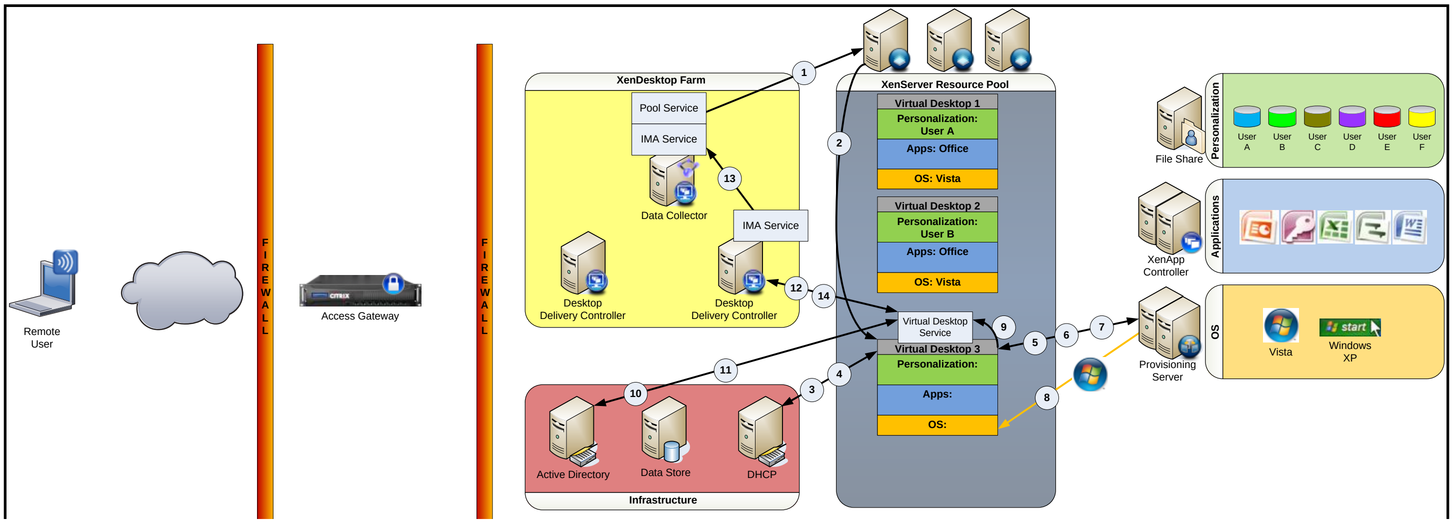

Figure 2: Virtual Desktop Startup Process

Step	Source	Destination	Port	Description
1	Pool Service (Desktop Delivery Controller)	XenServer	80	The Pool Service, on the desktop delivery controller, tells XenServer to start a specific virtual machine.
2	XenServer	Virtual Desktop	Local	XenServer starts the appropriate virtual desktop through a local API call.
3	Virtual Desktop	DHCP	67	The virtual machine boots via the network with PXE boot. The virtual machine requests IP information from the DHCP server
4	DHCP	Virtual Desktop	67	The DHCP server tells the virtual machine the IP address and any other configured DHCP options.
5	Virtual Desktop	Provisioning Server (Bootstrap Server)	68	The virtual machine was given an address for a bootstrap server, which corresponds to the Provisioning Server. Also, the Virtual Machine was given a boot filename.
6	Provisioning Server (Bootstrap Server)	Virtual Desktop	TFTP	Provisioning Server receives the bootstrap request from the virtual machine and the appropriate boot filename. The TFTP service on the Provisioning Server sends the boot file.
7	Virtual Desktop	Provisioning Server	6910-6930	The virtual desktop executes the bootstrap file and receives instructions for obtaining its streamed image. The request is made to the Provisioning Server.
8	Provisioning Server	Virtual Desktop	6910-6930	Provisioning Server looks into its database for the appropriate virtual disk to stream based on the virtual machines MAC address. Upon identifying the correct virtual disk, the Provisioning Server starts streaming the Operating System.
9	Virtual Desktop	Virtual Desktop Service (Virtual Desktop)	Local	Once the virtual desktop starts, it tells its local virtual desktop service to start.
10	Virtual Desktop Service (Virtual Desktop)	Active Directory	LDAP	The Virtual Desktop Service validates the farm ID with Active Directory.
11	Active Directory	Virtual Desktop Service (Virtual Desktop)	LDAP	Upon success validation of the farm ID, Active Directory sends the virtual desktop service a list of desktop delivery controllers for the farm.
12	Virtual Desktop Service (Virtual Desktop)	Desktop Delivery Controller		The Virtual Desktop Service tries, at random, to connect with the desktop delivery controller.
13	IMA Service (Desktop Delivery Controller)	IMA Service (Data Collector)	IMA: 2512	Once a Desktop Delivery Controller has been contacted, the virtual desktop is registered with the controller. The controller is now responsible for this particular virtual desktop. The registration information of a virtual desktop with a desktop delivery controller is sent to the data collector of the XenDesktop farm.

Step	Source	Destination	Port	Description
14	Virtual Desktop Service (Virtual Desktop)	Desktop Delivery Controller	8080	The virtual desktop continues to send a 30 second heartbeat to the desktop delivery controller informing that it is still available for a connection.

Authentication

Users will need delivery of a virtual desktop. This requires proper authentication. For external users, the authentication happens initially at the Access Gateway, which prevents unauthorized users from gaining access to the internal network. The authentication process happens as follows:

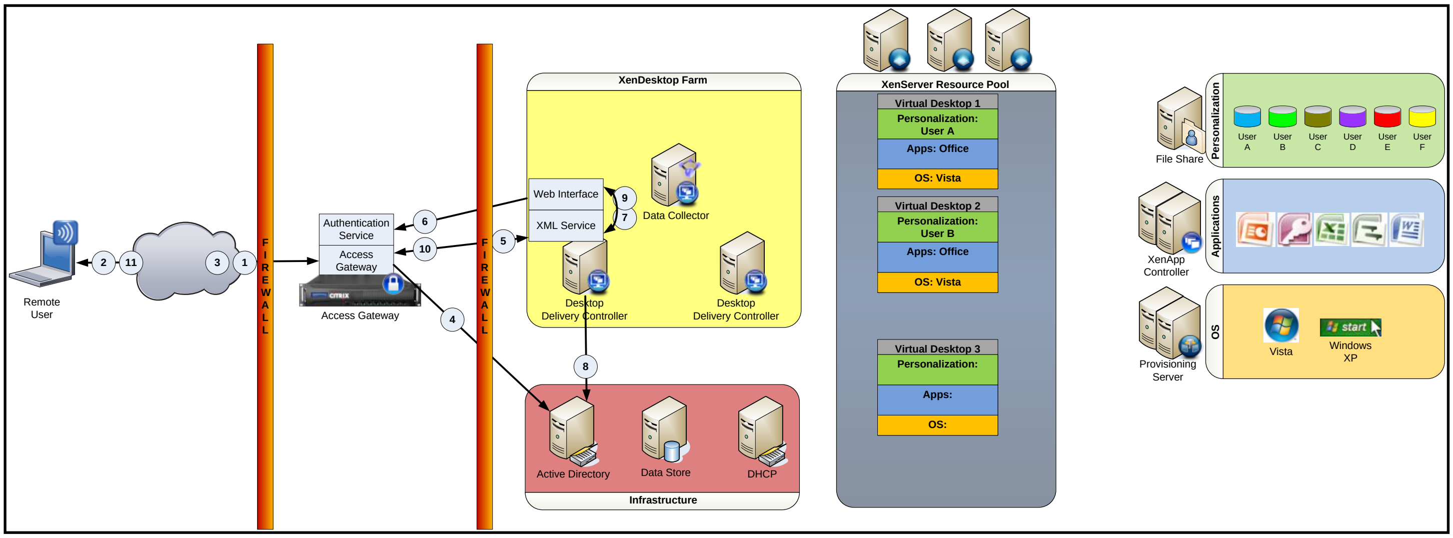

Figure 3: Authentication

Step	Source	Destination	Port	Description
1	End-Point	Access Gateway	443	User starts a browser and makes a request to the fully qualified domain name of the Access Gateway.
2	Access Gateway	End-Point	443	Access Gateway presents the user with a logon screen.
3	End-Point	Access Gateway	443	User enters in the logon credentials into the logon page
4	Access Gateway	Active Directory	389	Access Gateway authenticates the user’s credentials with the configured Active Directory server.
5	Access Gateway	Web Interface	80	Upon successful authentication, Access Gateway requests the Web Interface site.
6	Web Interface	Authentication Service (Access Gateway)	443	Web Interface receives the request and retrieves the credentials from the Authentication Service on the Access Gateway
7	Web Interface	XML Service (Desktop Delivery Controller)	80	With the credentials obtained from the authentication service, Web Interface passes the user’s credentials to the XML Service.
8	XML Service (Desktop Delivery Controller)	Active Directory	LDAP	The XML Service authenticates the user against Active Directory.
9	XML Service (Desktop Delivery Controller)	Web Interface	80	After successful authentication, the XML Service determines which virtual desktops are available for the user. The information is sent to Web Interface.
10	Web Interface	Access Gateway	443	Web Interface creates a web page containing a list of virtual desktops for the user.
11	Access Gateway	End-Point	443	Access Gateway proxies the Web Interface information back to the end-point’s browser.

Virtual Desktop Connection

Once users have properly authenticated, they must make a request for an available virtual desktop. This requires the user to select a single icon or the environment could be configured to auto-launch the desktop upon completion of the authentication process. Regardless of the solution selected, the process flows as follows:

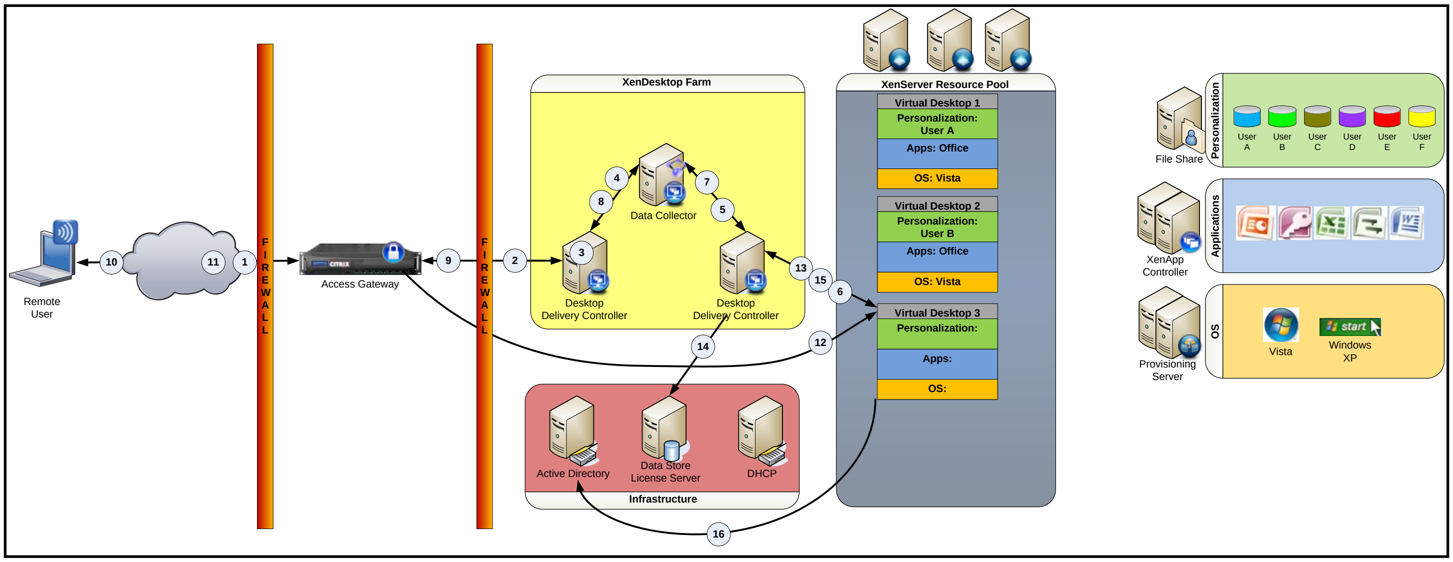

Figure 4: Virtual Desktop Connection

Step	Source	Destination	Port	Description
1	End-point	Access Gateway	443	User selects an icon representing a virtual desktop.
2	Access Gateway	Web Interface	80	The icon selection information is sent to Web Interface for processing.
3	Web Interface	XML Service & IMA Service (Desktop Delivery Controller)	80	Web Interface forwards the request onto the XML Service and then onto the IMA Service.
4	XML Service (Desktop Delivery Controller)	Data Collector	IMA: 2512	The request is forwarded onto the Data Collector for processing.
5	IMA Service (Data Collector)	Controller Service via the IMA Service (Desktop Delivery Controller)	IMA: 2512	The data collector will determine if the user currently has a virtual desktop disconnected, connecting or active. If there is an available virtual desktop, the user will be directed to it. However, if no virtual desktops are available, the Controller service will tell the Pool Service to contact the XenServer and tell it to start up a new virtual desktop. Once a virtual desktop has been identified, the data collector tells the controller to prepare the virtual desktop.
6	Controller Service (Desktop Delivery Controller)	Virtual Desktop Service (Virtual Desktop)	8080	The controller tells the virtual desktop to start listening on ICA and CGP ports for an incoming session.
7	Controller Service (Desktop Delivery Controller)	IMA Service (Data Collector)	IMA: 2512	The controller forwards the virtual desktop connection information to the data collector through IMA.
8	XML Service (Data Collector)	Web Interface	80	The data collector forwards the virtual desktop connection information onto Web Interface via the XML broker.
9	Web Interface	Access Gateway	443	Web Interface creates a launch file (ICA file) for the virtual desktop. The file is forwarded onto Access Gateway.
10	Access Gateway	End-Point	443	Access Gateway forwards the ICA file onto the end-point.
11	End-Point	Access Gateway	File type association	The end-point receives the ICA file and executes it. Based on file type associations, the ICA file is launched by the desktop receiver. The connection request is sent to Access Gateway
12	Access Gateway	Virtual Desktop	ICA or CGP	Access Gateway proxies the launch request between the end-point

Step	Source	Destination	Port	Description
				and virtual desktop.
13	Virtual Desktop	Controller Service (Desktop Delivery Controller)	8080	Virtual desktop tells the controller that the user has connected and this information is sent onto the data collector. The user's logon information is sent onto the controller for validation.
14	Controller Service (Desktop Delivery Controller)	License Server	27000	The controller does the following before authentication proceeds: • Validates the credentials • Checks out a license from the license server. • Determines the resultant set of policies for the virtual desktop
15	Controller Service (Desktop Delivery Controller)	Virtual Desktop	8080	If the credentials are valid and there is an available license, then the credentials, license and policy are sent to the virtual desktop for processing.
16	Virtual Desktop	Active Directory	LDAP	Once the connection has been approved by the controller, the virtual desktop uses the transferred credentials to logon against Active Directory and applies the appropriate policies.
17	Virtual Desktop	Personalization	SMB	Based on the Active Directory policies applied, the Virtual Desktop contacts the file server holding the user's personalization settings. Those settings are applied to the virtual desktop.

Virtual Desktop Personalization

Once the virtual desktop has launched, the last item to accomplish is to integrate the applications into the virtual desktop. This process happens automatically as follows, when integrated with XenApp.

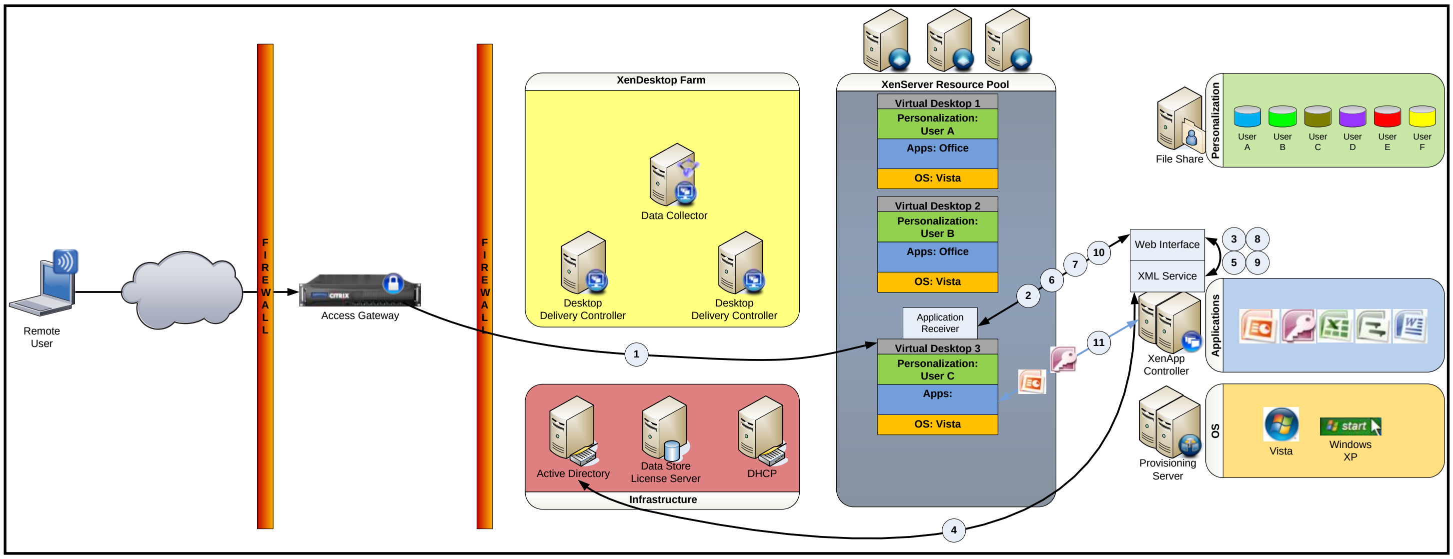

Figure 5: Virtual Desktop Personalization

Step	Source	Destination	Port	Description
1	End-point	Virtual Desktop	443 / ICA / CGP	A connection has already been made between the end-point to the virtual desktop through Access Gateway
2	Application Receiver (Virtual Desktop)	Web Interface	80	When the user is logged into the desktop, the Application Receiver starts automatically. Based on the configuration, the receiver contacts Web Interface and automatically passes the logon credentials.
3	Web Interface	XML Service	80	Web Interface passes the logon credentials onto the XML service
4	XML Service	Active Directory	LDAP	The XML Service validates the credentials against Active Directory.
5	XML Service	Web Interface	80	With validated credentials, the XML Service identifies the available applications for the user and passes this information on to Web Interface.

Step	Source	Destination	Port	Description
6	Web Interface	Application Receiver	80	Web Interface sends the application information to the Application Receiver for display.
7	Application Receiver	Web Interface	80	When the user selects an application within the receiver, the request is sent to Web Interface
8	Web Interface	XML Service	80	The application launch request is forwarded on to the XML Service which identifies if the application is streamed or hosted.
9	XML Service	Web Interface	80	The XML Service sends the application information to Web Interface
10	Web Interface	Application Receiver	80	Web Interface takes the application information, creates a launch file, and sends the launch file to the Receiver.
11	Application Receiver	XenApp	1494 or SMB	The application receiver executes the launch file which contains application launching instructions • Streamed Applications: The launch file instructs the receiver to contact the server delivering the application. The application is streamed to the virtual desktop using SMB. • Hosted Applications: The launch file instructs the receiver to connect to the XenApp server hosting the application. The Receiver and the XenApp server create a direct connection over ICA port 1494.

Pilot Considerations

As the environment is being used with production data and with real users, it is advisable to build the environment with redundancy. The entire architecture can be made redundant with the duplication of key components.

- Access Gateway: Multiple Access Gateway devices can be added and setup in a high-availability pair. If one Access Gateway were to fail, the other would take over automatically.
- Desktop Delivery Controllers: Multiple Desktop Delivery Controllers should be used to provide redundancy.
    - Web Interface: In the default setup, each Desktop Delivery Controllers contains a Web Interface site. Multiple Web Interface servers should be used to continue to allow availability if one fails.
    - Data Collector: There is only one Data Collector in the XenDesktop Farm. If the Data Collector were to fail, another Desktop Delivery Controller would take on the role of the Data Collector automatically.
- Virtualization Infrastructure: The virtualization infrastructure is the base for desktop virtualization. When XenDesktop is implemented with XenServer, multiple XenServers should be used and added to the same resource pool. If one XenServer fails, the other XenServer will still provide virtualization infrastructure to the virtual desktops. And the virtual desktops hosted from the failed XenServer can be migrated to an available XenServer in a matter of seconds.
- Provisioning Servers: The Provisioning Servers stream the operating system to the virtual desktop. At least two Provisioning Servers should be deployed in a high-availability pair. Also, the virtual disk streamed out to virtual desktops should be stored on shared storage. Deploying the virtual disks on shared storage allows either Provisioning Server to stream the disk.
- Virtual Desktops: Based on XenDesktop’s architecture, if the number of available virtual desktops falls below a configurable threshold, new virtual desktops will be started automatically.
    - Application Receiver: The Application Receiver should be configured with backup Web Interface addresses to overcome a potential Application Delivery Controller failure.
- Application Delivery Controller (XenApp): Multiple XenApp servers should be used to provide redundancy for application delivery and the servers should be contained within the same XenApp farm.
    - Web Interface: Multiple servers should host the Web Interface sites for application delivery.

Summary

Providing a virtual desktop solution to an organization must be able to take into account the numerous requirements of the organization as well as providing the most flexible infrastructure that is easy to manage and maintain. The end-to-end solution must be tested in a small-scale production environment before the full rollout begins. This allows the organization to validate all requirements are met, all components function properly and the proper configuration and optimizations have been made.

The power of the XenDesktop solution is that the different components allow organizations to tailor the solution to meet their needs. And when all components are integrated together into a single virtual desktop delivery solution, an organization can simplify management and maintenance of the virtual desktop environment, provide the ability for users to personalize their virtual desktop and provide secure, remote access.

Notice

The information in this publication is subject to change without notice.

THIS PUBLICATION IS PROVIDED “AS IS” WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CITRIX SYSTEMS, INC. (“CITRIX”), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

This publication contains information protected by copyright. Except for internal distribution, no part of this publication may be photocopied or reproduced in any form without prior written consent from Citrix.

The exclusive warranty for Citrix products, if any, is stated in the product documentation accompanying such products. Citrix does not warrant products other than its own.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Version History

Author	Version	Change Log	Date
Daniel Feller	0.1	Document created	June 23, 2008
Daniel Feller	1.0	Document finalized	June 30, 2008

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