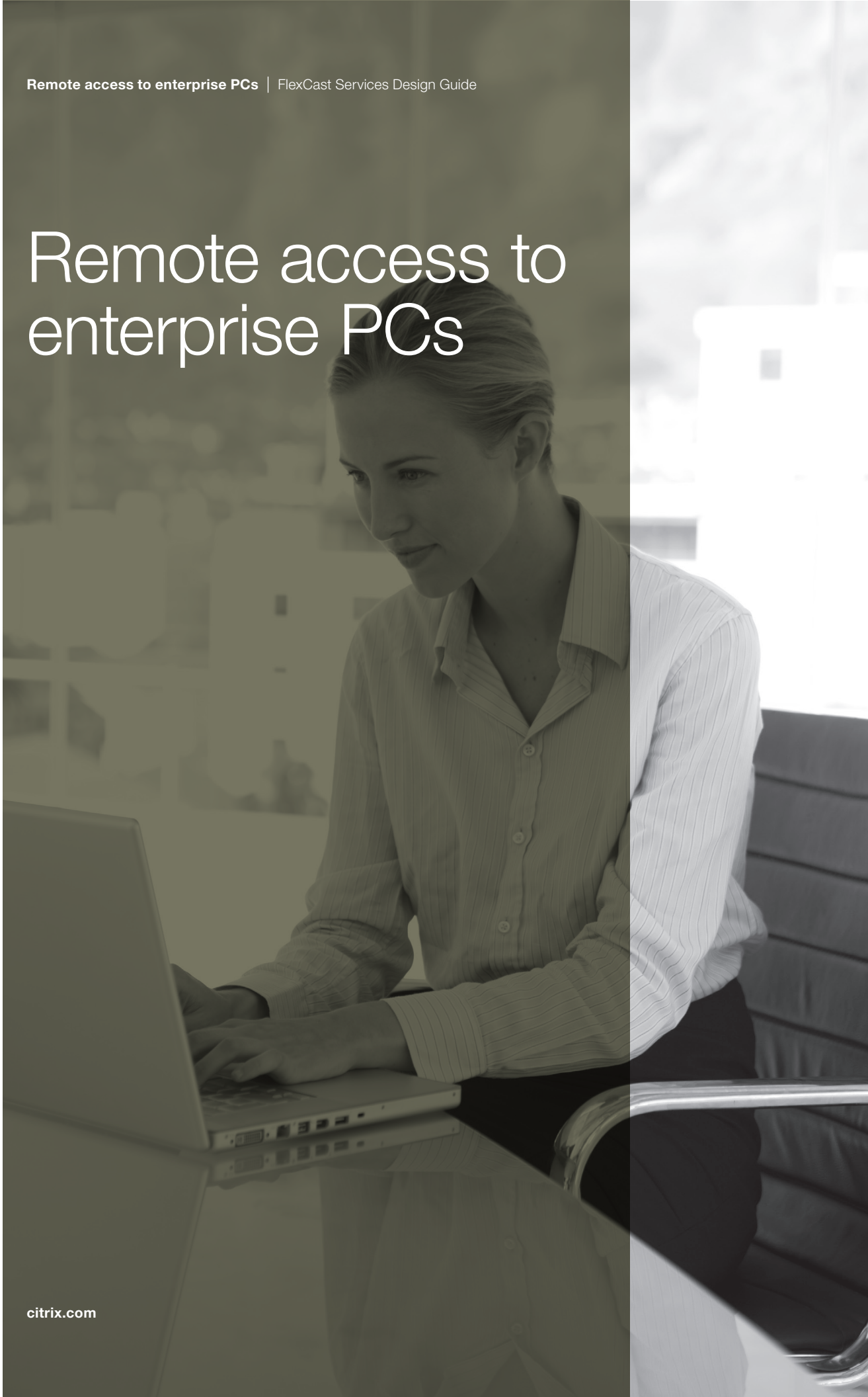
# Remote access to enterprise PCs



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 relies on Citrix Consulting best practices and in-depth validation by the Citrix Solutions Lab to provide prescriptive design guidance on the overall solution.

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

Today's workers seek improvements in their work-life balance. The implementation of a teleworking program allows them to work from home full-time, part-time or when commuting is less than ideal, such as during snowstorms or transit strikes.

IT must find the right tools and resources to provide remote access for teleworkers without compromising security. Typical security concerns include protecting corporate data used by remote workers and preventing unprotected endpoint devices from infecting the corporate network, all without radically changing users' workstyles.

Many products can address a portion of these remote access requirements, but only Citrix XenDesktop with Remote PC Access provides a comprehensive solution. XenDesktop with Remote PC Access, available in Enterprise or Platinum editions, is simple to deploy and secure by design. It delivers access to corporate resources without dramatically changing the user experience or IT footprint.

### Objective

The objective of the FlexCast Services Design Guide is to construct and demonstrate an efficient way of delivering remote access to enterprise PCs that is secured and optimized regardless of network type, worker location and endpoint device.

This is the challenge impacting WorldWide Corporation (WWCO), a hypothetical organization that has always issued each of its employees a physical desktop to ensure standardization and security compliance across the enterprise.

To improve employee morale, WWCO wants to enable remote access through a teleworking initiative that ensures employees can successfully perform their jobs without compromising the security of corporate data. In addition, the IT leadership team wants to capitalize on existing investments in physical desktops.

To address these challenges, IT decided to implement a XenDesktop 7 environment utilizing Remote PC Access to provide employees with secure remote access to their physical desktops located in the office. To properly validate the solution, IT identified a 500-user division for the first phase of the rollout.

WWCO business objectives

- Enable a remote access solution for a select number of employees
- Ensure that all corporate resources and data remain secure within the office when accessed remotely
- Leverage the existing physical desktop investment and security procedures
- Support remote access from personal devices, which can include mobile devices

WWCO technical objectives

- Quickly design and implement the remote access environment as the first step towards justifying a larger deployment
- Implement an N+1 highly available solution without large cost increases
- Centrally manage and control employee access and permissions
- Support access to physical enterprise PCs from employee-owned devices with different form factors, including tablets, phones, desktops and laptops, and different operating systems, which include iOS, Mac, Android, Linux and Windows.
- Build a solution that scales from a few hundred users to thousands
- Utilize virtualized components, where possible, to reduce costs
- Secure all traffic crossing public network links
- Support a strong, multi-factor authentication solution

## Assumptions

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

- All infrastructure resources (physical and virtual servers) will be hosted from a single datacenter.
- All enterprise PCs will remain in their current locations and continue to be utilized when users are on premise.
- High availability (HA) is required for all critical components in N+1 mode, where enough spare capacity will be built into the system to accommodate the failure of one component without impacting user access.
- WWCO's existing Microsoft Active Directory and DNS/DHCP will be reused.

## 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.

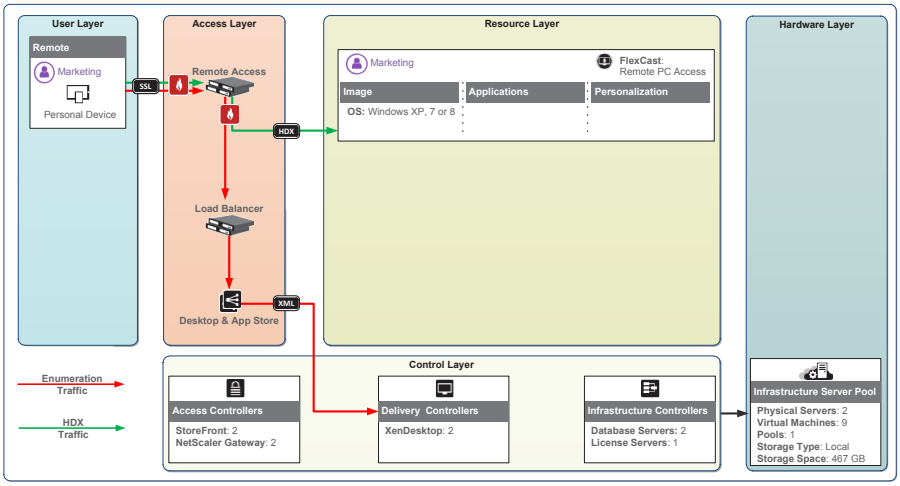



**Figure 1:** Conceptual architecture

This architecture is suitable for 500+ users requiring secure access to their physical desktop 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 WWCO's rollout is called Marketing. This group will utilize personal devices to connect to their physical desktop from a remote location. Personal devices include laptops, workstations, tablets and smartphones.
- Traffic will pass through a highly available pair of remote access appliances (Citrix NetScaler Gateway appliances) where users receive their resources from the desktop and app store, provided by StoreFront.
- The allocated resource for members of the Marketing user group is their office-based physical desktop.
- This resource, which is a Windows XP, Windows 7 or Windows 8 physical desktop, is managed as it was before XenDesktop 7 was integrated into the environment.
- The total hardware allocation requirement for the solution is two physical servers and 10 virtual machines (VMs). Although the entire infrastructure could be delivered with fewer than 10 VMs and two physical servers, additional VMs and physical servers are used to provide N+1 HA.

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

## Detailed architecture

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

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

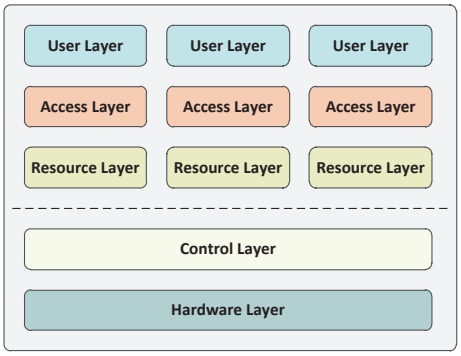



**Figure 2.** Virtual desktop model

### User layer

The user layer focuses on the logistics of the user groups, which include 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 data.

- **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. 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 Marketing 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 resources 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<br>Traditional |
| Session profile | ICA Proxy |
| User group | Marketing |

- **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 NetScaler Gateway, which is deployed within the DMZ portion of the network. NetScaler Gateway will accept multi-factor authentication credentials from users 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 and policy. WWCO policies are:
  - **Mobile** – When users connect with a mobile device, a separate policy will be applied to improve usability of the physical Windows desktop. 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 Marketing group members only require access to their respective physical desktops, regardless of endpoint, the session profile will be configured as ICA proxy instead of full VPN mode. ICA proxy allows only HDX traffic to pass from the endpoint to the user's physical desktop through NetScaler Gateway, while full VPN mode makes the endpoint act as if it is physically on the internal network. 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 and how to deliver it to the associated VMs, which applications to deliver and how to provide the right level of personalization and user experience for the respective user group.

Based on WWCO's decision to use Remote PC Access, there is no change to the Marketing users' physical desktops. This solution simply provides a secure, remote connection to the desktop.

While the enterprise desktop will not change, WWCO still needs to design the user experience through the use of XenDesktop policies. While authentication and security policies 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. Based on these requirements, the following policies will be used for the environment:

| Policy | Settings | Applied to… |
|---|---|---|
| Optimized for WAN | Based on the template "Optimized for WAN" | Any user connecting through NetScaler Gateway |
| Optimized for mobility | Mobile Experience<br>• Automatic keyboard display: Allowed<br>• Launch touch-optimized desktop: Allowed<br>• 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 |
| Secure resources | Based on the template "Secure and Control" | Delivery group |

## Control layer

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

### Access controllers

The access controllers provide users with connectivity to their resources as defined within the access layer. 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 |
| 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 of StoreFront virtual servers is responsible for resource enumeration.

## Delivery controllers

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

| Parameter | XenDesktop Delivery Controller |
|---|---|
| Instances | 2 virtual servers |
| CPU | 2 vCPU |
| Memory | 4 GB RAM |
| Disk | 60 GB |
| Citrix product version | XenDesktop 7 |
| Microsoft product version | Windows Server 2012 Standard |
| Network ports | 80, 443 |
| Redundancy | Load balanced via StoreFront |

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

### Infrastructure controllers

A fully functioning virtual desktop environment requires a set of standard infrastructure components:

| Parameter | SQL Server | License Server |
|---|---|---|
| Instances | 2 virtual servers | 1 virtual servers |
| CPU | 2 vCPU | 2 vCPU |
| Memory | 4 GB RAM | 4 GB RAM |
| Disk | 60 GB | 60 GB |
| Citrix product version(s) | Not Applicable | Citrix License Server 11.12 |
| Microsoft product version | Windows Server 2012 Standard<br>SQL Server 2012 | Windows Server 2012 Standard |
| Network ports | 1433 | 27000, 7279, 8082 |
| Redundancy | SQL Server AlwaysOn | None due to 30-day grace period |

To provide fault tolerance, the following options will be used:

- The XenDesktop database will be deployed on an HA pair of Microsoft SQL Server 2012 servers utilizing the AlwaysOn availability group with primary and secondary instances spread across two virtual servers.
- Once active, a XenDesktop environment can continue to function for 30 days without connectivity to the Citrix license server. Due to the integrated grace period, no additional redundancy for the license server is required.

### 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 | 2 | 2 servers |
| Processor(s) | Intel Xeon E5-2690 @2.9GHz | 2 | 16 cores |
| Memory | 8GB DDR3-1333 | 4 | 32 GB |
| Disk(s) | 300GB SAS @ 15,000RPM | 4 | 1.2 TB |
| Microsoft product version | Windows Server 2012 Datacenter | 2 | 2 |

To provide fault tolerance for the solution, the virtual servers will be distributed so redundant components are not hosted from the same physical server. The virtual server allocation is depicted in Figure 3.

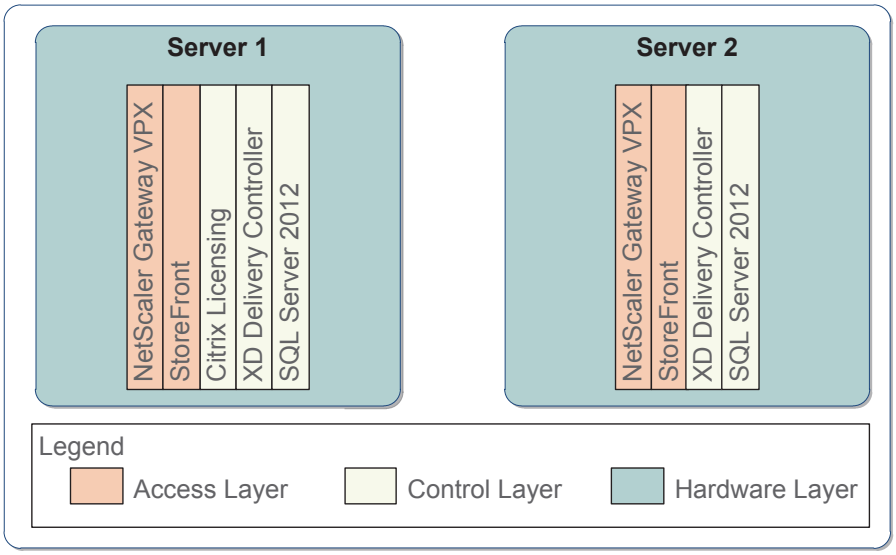



**Figure 3:** Virtual machine server allocation

**Note:** The resource load on the physical hardware for the access and control layer components is minimal.

**Note:** Although this environment was designed for 500 users, it can scale significantly higher without adding extra hardware.

### Storage

The storage architecture for the solution is based on the use of inexpensive local storage. To ensure the solution is highly available, the storage architecture must be able to overcome the potential failure of a single drive.

| Parameter | Control Layer |
|---|---|
| Drive count | 4 |
| Drive speed | 15,000 RPM |
| RAID | RAID 10 |

Even though the control layer servers generate IO activity, this activity is minimal. The main storage requirement for the control layer servers is hard disk space, as defined in the control layer section.

RAID 10 is recommended because if future expansion of the solution includes hosted virtual desktop models, the servers will not require reconfiguration.

### 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.

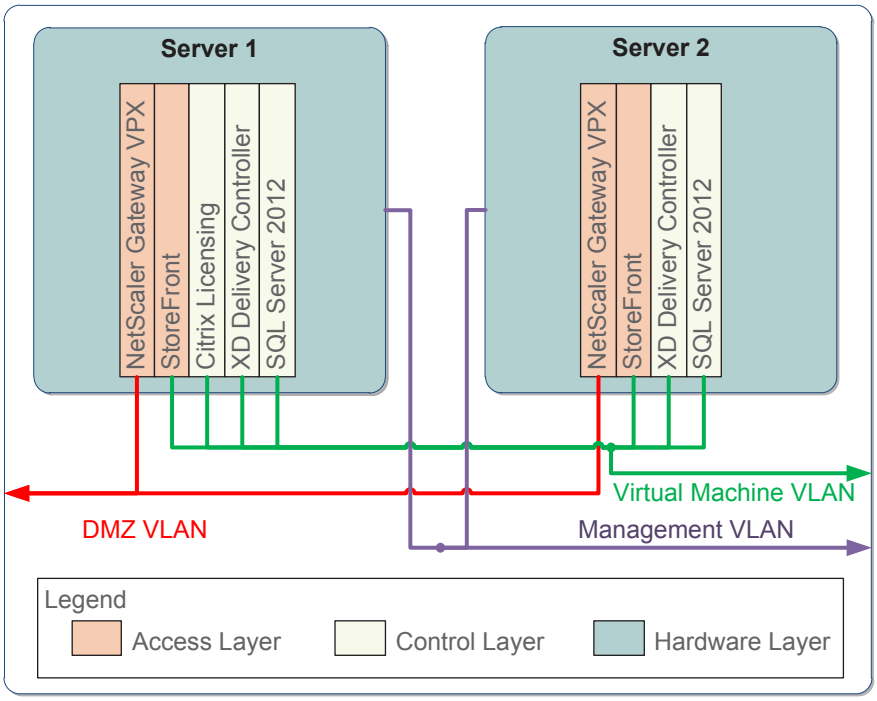



**Figure 4:** Networking architecture

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 VMs. This VLAN is for management calls to/from the physical server's hypervisor.

- The VM VLAN, meant for all non-DMZ VMs, allows them to connect to the internal network. The VM VLAN must be able to communicate with each user's enterprise desktop (default port: 80).

## Validation

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

- The control layer components of SQL Server, StoreFront and delivery controllers consumed less than 20 percent of CPU at maximum.
- 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.
- Users were able to effectively work on their traditional, physical desktop from a remote location.

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

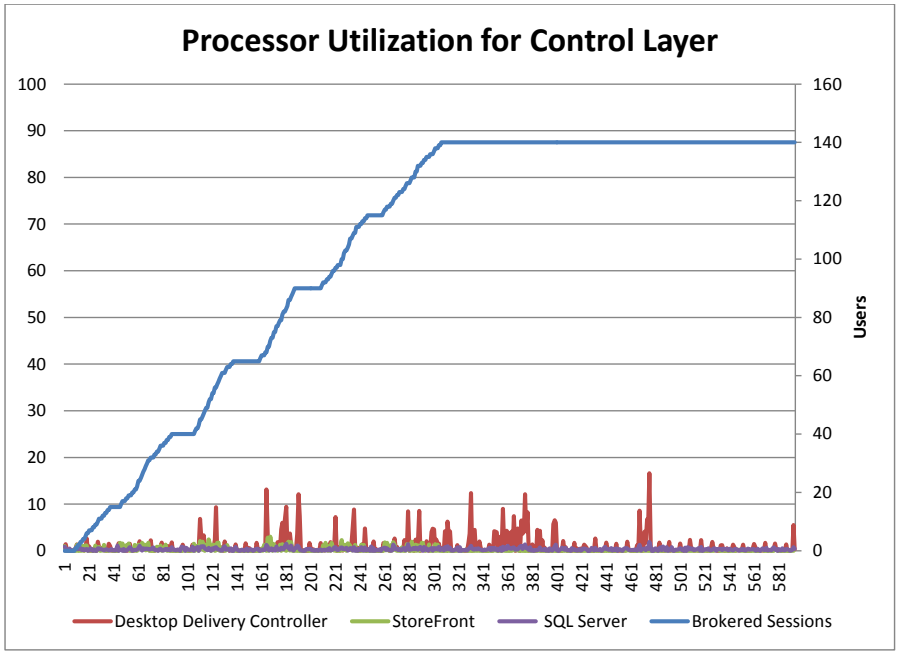



**Figure 5:** Processor utilization for control layer components

Although this solution was designed to support 500 Remote PC Access users, it can scale significantly higher without additional hardware.

## Next steps

When unforeseen events occur, making it difficult to commute to the office, workers may put their lives in danger because deadlines do not change and the job must get done. For many, an acceptable work-life balance is one of the most important aspects in ongoing career satisfaction.

XenDesktop 7 with Remote PC Access provides organizations with the ability to successfully implement a teleworking program without the complexity and risks typically associated with traditional remote access solutions.

Remote PC Access

- Eliminates the need for VPN tunnels, which often limit the types of endpoints that can be supported
- Utilizes Citrix HDX to provide a “in-the-office” experience even though the user’s enterprise desktop is far away
- Protects the corporate environment from exposure to the user’s environment by transmitting only screen, keyboard and mouse data and blocking everything else

To help you learn more about the potential benefits that XenDesktop 7 can provide, Citrix has prepared the following resources:

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

## Appendix: Authentication and enumeration process

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

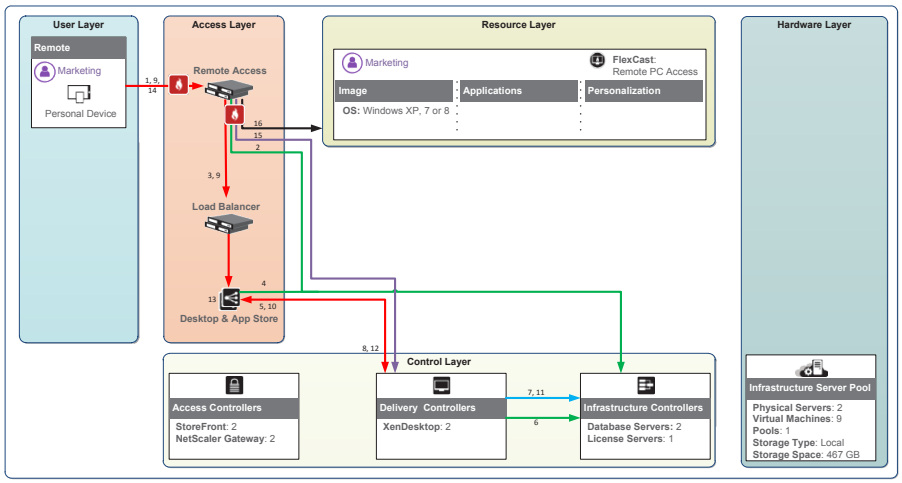



**Figure 6:** Authentication and enumeration process

| 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 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 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.<br><br>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.