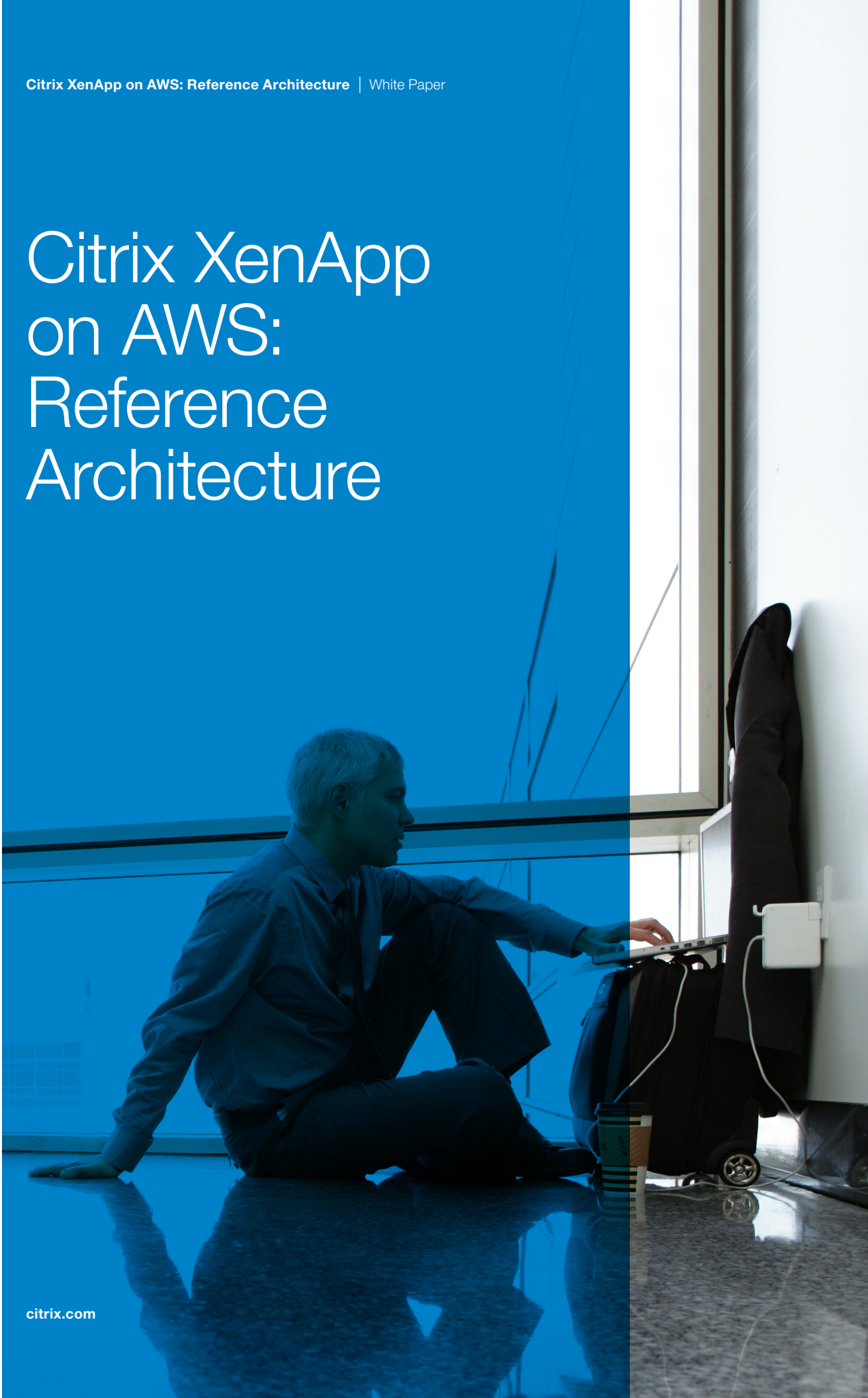
Citrix XenApp on AWS: Reference Architecture



amazon web services | Partner Network
ADVANCED TECHNOLOGY PARTNER

CITRIX®

citrix.com

Amazon Web Services (AWS) provides a complete set of services and tools for deploying Windows® workloads and NetScaler VPX technology, making it a perfect fit for deploying or extending a Citrix XenApp farm, on its highly reliable and secure cloud infrastructure platform. This white paper discusses general concepts regarding how to use these services and provides detailed technical guidance on how to configure, deploy, and run a XenApp farm on AWS. The white paper illustrates reference architecture for the two most common Citrix XenApp deployment scenarios and discusses their network, security, and deployment configurations so you can run XenApp workloads in the cloud with confidence.

This white paper is targeted to IT infrastructure decision-makers and administrators. After reading it, you should understand the requirements to set up and deploy the components of a typical XenApp farm on AWS. Included in the discussion are the artifacts to use and how to configure the various infrastructure details, such as compute instances, storage, security, and networking.

Enterprises need to grow and manage their global computing infrastructures rapidly and efficiently while simultaneously optimizing and managing capital costs and expenses. AWS's computing and storage services meet this need by providing a global computing infrastructure. The AWS infrastructure enables companies to rapidly spin up compute capacity or quickly and flexibly extend their existing on-premises infrastructure into the cloud. AWS provides a rich set of services and robust, enterprise-grade mechanisms for security, networking, computation, and storage.

Citrix XenApp 6.5 provides advanced management and scalability, a rich multimedia experience over any network, and self-service applications with universal device support from PC to Mac to smartphone. With full support for Windows Server® 2008 R2 and seamless integration with Microsoft® App-V,

XenApp 6.5 provides session and application virtualization technologies that make it easy for customers to centrally manage applications using any combination of local and hosted delivery to best fit their unique requirements.

AWS is a perfect complement to Citrix XenApp, because it enables organizations to rapidly provision the necessary computing infrastructure to power Citrix XenApp solutions.

AWS and Citrix have partnered to enable customers to deploy enterprise-class workloads involving Windows Server® and Citrix NetScaler on a pay-as-you-go, on-demand elastic infrastructure, thereby eliminating the capital cost for server hardware and greatly reducing the provisioning time required to create or extend a XenApp farm. This partnership has resulted in the ability to license and run NetScaler on AWS in an hourly charge fashion.

XenApp Reference Architecture and scenarios

To understand how XenApp and associated components can be hosted on AWS and connected to an existing on-premises deployment, let's first review the architecture and components of a typical XenApp server farm and explore the common scenarios and topologies.

XenApp Farm Reference Architecture

Citrix provides considerable guidance for architecting XenApp farm topologies for many scenarios and scales. This section reviews the typical XenApp farm architecture as recommended by Citrix and identifies a couple of common deployment scenarios and associated topologies that we will map onto AWS later in this paper.

XenApp has evolved over several versions to provide a rich set of capabilities and services for application and hosted shared desktop delivery. XenApp architecture has also evolved to support a service-based architecture, enabling specific services or application sets to be scaled out to individual servers and worker groups. In addition, XenApp Reference Architecture defines distinct roles and worker groups that you can create and scale out independently. This model fits nicely within AWS's scale-out approach.

The XenApp reference architecture layers and services are illustrated in Figure 1.

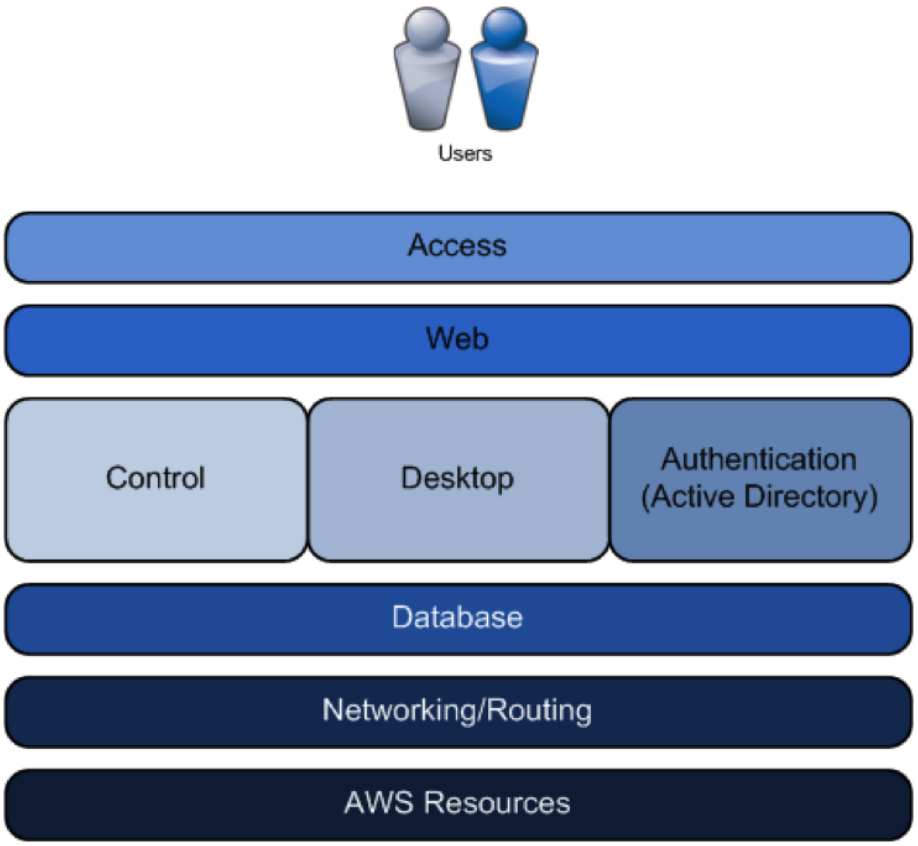


Figure 1: XenApp Layers and Services

Common XenApp on AWS deployment scenarios

XenApp can support a variety of application and hosted shared desktop delivery goals. This paper discusses two of the most common scenarios in relation to leveraging AWS: Hybrid XenApp Farm Extension and XenApp Cloud Hosted Farm. The primary difference between the two models lies in the location of the database and access layer resources.

Hybrid XenApp Farm Extension

In this scenario, a company wants to run XenApp within its enterprise to support internal users. The company extends its on-premises deployment to the cloud to increase capacity, improve performance, or scale the resource-intensive components in the cloud, when needed. This model also provides higher availability for business continuity and disaster recovery provided the user data is available during the event. Connectivity for this model relies on the NetScaler CloudBridge Connector functionality which creates a secure and optimized for XenApp deployments VPN tunnel between the on-premises deployment and the AWS availability zones. Figure 2 illustrates this scenario.

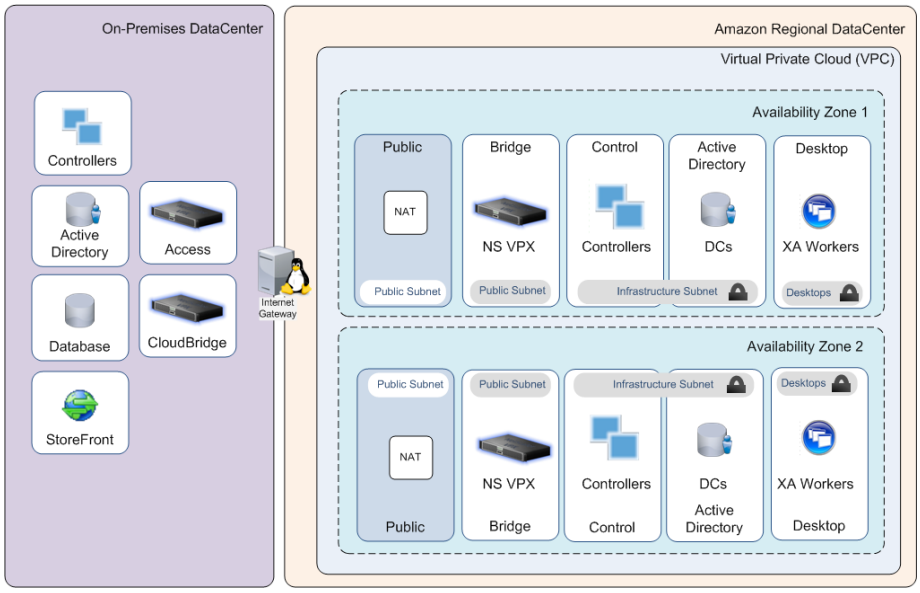


Figure 2: Hybrid XenApp Farm Extension Model

XenApp Cloud Hosted Farm

In this scenario, XenApp is used by a service-oriented IT organization as the basis for delivering hosted-shared desktops and applications as a service. All XenApp services and user data are kept completely in the AWS cloud using multiple availability zones within one single AWS region. Corporate application data and user authentication will remain on-premises. This model also relies on the NetScaler CloudBridge Connector functionality to create secure tunnels for corporate data with the AWS region and its availability zones. Figure 3 depicts this scenario.

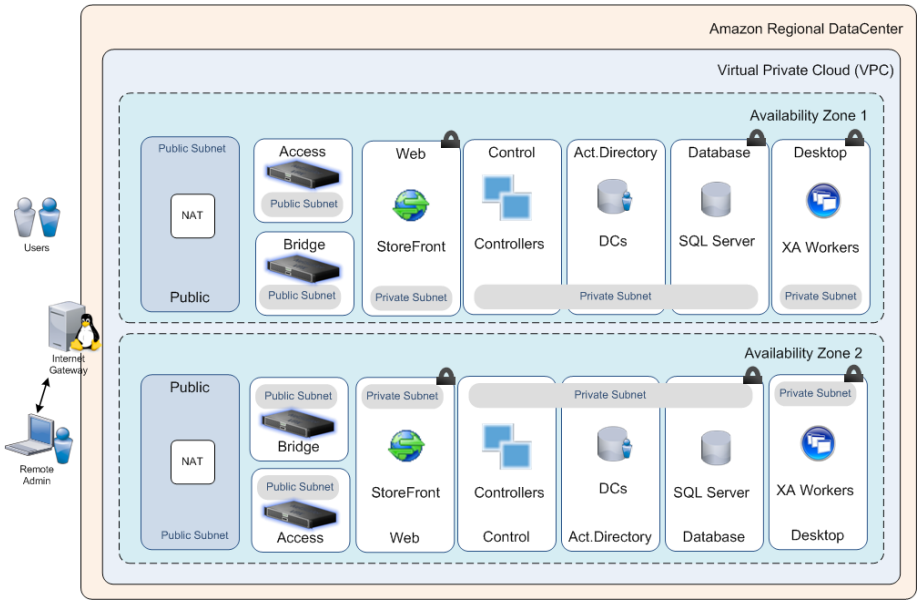


Figure 3: XenApp Cloud Hosted Farm Model

Key elements that distinguish this scenario from the previous Hybrid scenario are:

- Access and Web layer located in AWS cloud
- Active Directory domain controllers resident within the farm (not associated with the user environment)

Microsoft components

Additional infrastructure components are required or recommended to support XenApp farms:

- Active Directory® Domain Services (AD DS). XenApp requires AD DS to serve as the authoritative identity store and authentication mechanism. AD DS (with one or more domain controllers) must reside within the same network as the XenApp farm and be accessible to XenApp farm instances.
- Distributed File System (DFS)
- Group Policies
- SQL Server
  XenApp farms must have an associated data store. The data store provides a repository of persistent information, including:
  - Farm configuration information, such as zones, worker groups etc.
  - Published application configuration
  - Printer configurations
  - Etc.

For larger enterprise deployments it is advised to use the high-availability and replication features or Microsoft SQL Server. XenApp 6.5 supports the transactional replication with immediate updating subscribers' model. See "Using SQL Database Mirroring to Improve Citrix XenApp Server Farm Disaster Recovery Capabilities" as well as "Design and Scalability Considerations for Enterprise XenApp Deployments".

Citrix components

This section introduces the various Citrix components and their responsibilities within the reference architecture.

NetScaler

NetScaler is an ideal choice for front-ending a XenApp desktop and application virtualization infrastructure. An advanced solution for delivering both applications and services, it provides extensive high-availability, security and performance optimization capabilities, tightly integrated with XenApp and XenDesktop.

Ensuring availability

High availability for dependable access If a component such as a XenApp Zone Data Collector fails, core load-balancing algorithms within NetScaler dynamically route virtual desktop traffic to available services and servers. NetScaler configures and manages these as part of a pool of resources to automatically address both unanticipated failures and scheduled outages. NetScaler also helps ensure high availability of other elements in your desktop virtualization solution, including:

- Front-end components, such as StoreFront and NetScaler Gateway virtual servers
- Supporting services, such as file transfer, licensing, provisioning and management servers
- Downstream components, such as the StoreFront and XML broker servers of Citrix XenApp, that you can use to enable application virtualization

Health monitoring for proactive failure management. In conjunction with load balancing capabilities, NetScaler health checks proactively determine the status of key solution components such as the StoreFront and Zone Data Collectors. NetScaler monitoring includes extended content verification checks to establish both the availability and proper operation of numerous software routines and system-level components, including ASP.net and essential logon, XenApp Farm operation, Zone Data Collector and database services.

GSLB for disaster recovery. NetScaler includes a robust GSLB capability that provides seamless disaster recovery for desktop virtualization. If an availability zone or region site becomes unavailable for any reason, NetScaler automatically directs users to an alternate zone or region, helping to ensure continuity of access to their desktops.

Strengthening security

Secure access from any location and device. An integral component of NetScaler, NetScaler Gateway™ is a full-featured secure sockets layer (SSL) virtual private network (VPN). As such, it provides your organization several security capabilities important to a virtual desktop operating model, without the need to deploy any additional devices.

The NetScaler Gateway module accounts for remote users by providing an encrypted tunnel and supporting multiple methods for user authentication. This protects desktop sessions traversing public networks from eavesdropping while enabling your enterprise to leverage its existing identity infrastructure.

With NetScaler Gateway, you can control on a granular lever which users get access to which resources based on attributes including user role, location, strength of authentication, sensitivity of the resource and ownership and security posture of the client device. As well as its intimate knowledge of virtual channels to control local printing, copy, paste, save-to-disk and other functionality.

Streamlining the user experience

Performance optimization. Leading virtual desktop solutions employ optimized display protocols to help ensure adequate performance over wide area networks (WANs). ICA, the display protocol that both XenDesktop and XenApp use, is unmatched in this regard. Still, one or more of the NetScaler performance enhancement mechanisms can improve performance further, especially if your organization is using a desktop virtualization solution other than XenDesktop.

End-to-end user experience visibility XenApp or XenDesktop deployments provided by HDX Insight. This add-on tool for NetScaler delivers compelling user experience with powerful business intelligence and failure analysis.

Simplifying scalability

Choice of platform. Whereas the highly popular NetScaler MPX hardware appliances are ideally suited for single-instance, high-capacity use cases, the recently introduced NetScaler SDX platform can also support multi-tenancy requirements by running multiple, isolated NetScaler instances on a single physical device. Either one can provide you a combination of hardware and system-level software that has been constructed and optimized for service delivery for on-premises deployments.

In comparison, NetScaler VPX is a full-featured virtual appliance version of NetScaler that you can deploy on AWS or on any hardware platform running a compatible Citrix XenServer, Microsoft Hyper-V, or VMware ESXi hypervisor. Because there is no physical appliance to deal with, you can deploy NetScaler service delivery capabilities on demand, anywhere within your enterprise or AWS.

CloudBridge

Move to the cloud securely and efficiently

CloudBridge lowers the risk and reduces the effort and cost for enterprises to leverage cloud resources for production workloads by:

- Encrypting the connection between the enterprise premises and the cloud provider so that all data in transit is secure
- Making the cloud provider network look like a natural extension of the enterprise datacenter network, minimizing the need to make major network changes and reducing application configuration drift
- Empowering enterprises to interconnect datacenters over public and private networks to cost effectively replicate critical data

Improved virtual experience for branch offices

CloudBridge with integrated HDX technologies accelerates, controls and optimizes virtual desktops and virtual applications delivered by XenApp, Combined with NetScaler Gateway, CloudBridge improves user experience and productivity by providing fast, secure remote access. This enables enterprises to support up to

four times more users of virtual apps and desktops by caching, optimizing ICA and storing streamed application packages on appliances on-premises or within AWS. Resulting in up to 25 times bandwidth saving per virtual desktop and reduction therefore in traffic between on-premises and AWS.

XenApp

Citrix XenApp 6.5 provides advanced management and scalability, a rich multimedia experience over any network, and self-service applications with universal device support from PC to Mac to smartphone. With full support for Windows Server® 2008 R2 and seamless integration with Microsoft® App-V, XenApp 6.5 provides session and application virtualization technologies that make it easy for customers to centrally manage applications using any combination of local and hosted delivery to best fit their unique requirements.

XenApp 6.5 introduces significant enhancements that simplify application management and bring unprecedented levels of scalability to increase cost savings and datacenter efficiency. XenApp gives corporations the ability to centrally manage heterogeneous applications and deliver Software as a Service (SaaS) to their workforce.

StoreFront

Citrix StoreFront, which is the successor to Citrix Web Interface, authenticates users to XenDesktop sites, XenApp farms, and AppController (SaaS Apps), enumerating and aggregating available desktops and applications into stores that users access through Citrix Receiver for Android, iOS, Linux, Windows, Win8/RT or Receiver for Web sites. It has been built on a modern, more flexible and powerful framework which enables Storefront to provide next generation features, such as:

- Unified StoreFront that delivers SaaS & Native Mobile applications (through AppController) as well as XenApp and XenDesktop resources
- Simplified Account Provisioning, which enables users to connect to assigned desktops and applications by simply entering their email or server address, or by opening a Provisioning File in Receiver
- Access from any Receiver with a consistent user experience, including automatic fall-back to an HTML 5 client if a native client isn't available locally and can't be installed
- Synchronization of resource subscriptions across all platforms and devices (Follow-me Apps & Data)

StoreFront functionality and architecture

The following diagram depicts a typical StoreFront infrastructure:

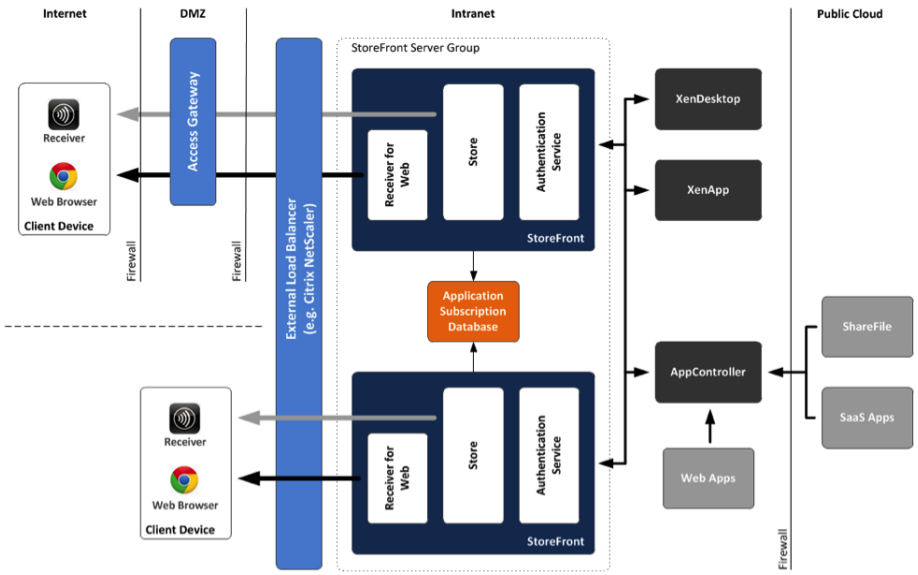


Figure 4: Typical StoreFront Infrastructure

Implementing XenApp Architecture scenarios in AWS

The reminder of this white paper provides step-by-step mapping for each XenApp farm scenario discussed earlier to an equivalent setup in AWS, including similar resources, network and security setup, and configuration. To implement the XenApp scenarios in AWS, the following elements are discussed:

- **Network setup and configuration.** This section covers the setup of the network for the XenApp farm within AWS, including subnets to support the logical server groups for different layers and roles within the XenApp reference architecture. It also covers the Cloudbridge architecture to connect the on-premises datacenter and the AWS availability zones.
- **Server setup and configuration.** This section covers the services and artefacts involved in the design of the various servers for each layer and role in the XenApp farm. It also includes the architecture of XenApp, Active Directory and SQL Server for high availability.
- **Security.** This section discusses security mechanisms in AWS, including how to configure the instance and network security to enable authorized access to the overall XenApp farm as well as between layers and instances within the farm.
- **Deployment and management.** This section provides details on packaging, deployment, monitoring, and management of the XenApp farm components.

Network setup

Let's start with the network setup to provide the environment in which you instantiate and configure your servers and database.

The Citrix reference architecture is organized around a multi-layered (Access, Web, Desktop, Control, Database and Authorization) approach, allowing you to independently scale and configure each layer. Our first task is to define a network environment that supports this type of layered structure and enables you to deploy the various server roles in each layer with suitable security configuration.

Amazon Virtual Private Cloud

A key component of AWS networking is the Amazon Virtual Private Cloud (Amazon VPC). Amazon VPC provides the ability to reserve an isolated portion of the AWS cloud in which to deploy and manage a XenApp farm. Amazon VPC supports the creation of public and private subnets within the virtual network, allowing you to host the different layers and roles within the XenApp architecture.

Amazon VPC also supports the ability to establish a hardware virtual private network (VPN) connection between a VPC and an external location, such as a corporate data center. Customers use a hardware or software VPN appliance (the customer gateway) and connect that gateway to the VPC (the virtual private gateway) to provide seamless integration between on-premises compute infrastructure and resources within the VPC. Leveraging this VPN–VPC connectivity extends the corporate network data center to the cloud. Corporate users can interact with cloud instances and applications in a relatively transparent way, effectively supporting the notion of an "extended enterprise" in the cloud.

To map your XenApp reference architectures and scenarios to AWS, you must first structure your VPC and subnets to mirror the same organizational layers, server groups, and access requirements defined there. VPC subnets that need to be accessible from the Internet through the VPC Internet gateway need to be public; otherwise, you can designate them as private, and they will not be accessible from outside the VPC. In the case of a VPN-connected VPC, connections through the VPN occur through the virtual private gateway; therefore, instances can be in private subnets but still reachable (as long as the security configuration allows it). Thus, VPN-only scenarios do not require public subnets (e.g., for NetScaler Gateway deployments). However, the public-facing XenApp scenario does need to be accessible from outside of AWS, so each NetScaler Gateway instance must be in a public subnet to be reached via the Internet gateway.

Fault tolerance and scalability for our XenApp farm scenarios is critical to ensure they can provide sufficient performance through changes in load, and be resilient to any unforeseen issues within the farm infrastructure. Although the AWS Elastic Load Balancing (ELB) web service can be used to distribute internet-based requests to internal web servers, it doesn't have intelligence to check the health of an application. Of course ELB will not direct any incoming requests to servers that crash, but what is StoreFront itself crashes? Consider a situation where the instance is network accessible via ICMP/TCP but the IIS service is malfunctioning. Users would be directed to a non-functioning StoreFront. Intelligent load balancing within NetScaler prevents users from being directed to servers with inactive or not correctly functioning services. Before NetScaler directs a user request to a StoreFront or XenApp XML Broker server, NetScaler users its built-in health checks or monitors that are application specific.

You also want to distribute multiple instances to each Availability Zone to provide redundancy and failover in the case of an Availability Zone failure. VPC subnets do not span Availability Zones, so you must set up a separate but similar subnet structure within each zone. NetScaler GLBS load balancing can be used to distribute requests to servers in multiple Availability Zones.

Next to local and global smart load balancing the Citrix NetScaler Application Delivery Controller (ADC) also provides remote access and is the best SSL VPN solution to deliver access to virtualized applications and desktops. This NetScaler Gateway functionality tightly integrates with XenApp providing granular controlled access to the correct set of resources required by users with integrated HDX SmartAccess capabilities while enforcing access control and corporate security policies.

The same Citrix NetScaler ADC also incorporates cloud connectivity between on-premises AWS VPCs through its CloudBridge capabilities—seamlessly extending our enterprise datacenter to the AWS cloud with IPSEC VPN security, WAN optimization and advanced networking. Where other VPN solutions exist that would create a VPN connection between our enterprise datacenter and the AWS Availability zones, they don't provide the combination of TCP Flow Control, data compression and de-duplication, in a streamlined physical and virtual model enabling these functions for enterprise network and AWS VPCs. This also includes the industry leading acceleration of the Citrix HDX protocol by monitoring and accelerating data in five key ICA channels. For these five channels, data is compressed and de-duplicated, and TCP flows are optimized to ensure that our VPN connection is fully utilized. The net result is a 50% decrease in VPN bandwidth required for HDX traffic per user, especially important in our Hybrid XenApp Scenario.

NOTE: The IP address ranges for the VPC and subnets are defined using a single Classless Inter-domain Routing (CIDR) IP address block, such as 10.16.0.0/16, providing an internal IP address space of 65,536 unique IP addresses. Subnets can then be created with their own unique CIDR block ranges within the overall VPC address range.

VPC setup for the Hybrid scenario

Let's look at the specific steps for setting up a VPC instance for the Hybrid XenApp scenario.

The AWS Management Console provides a wizard-based approach to setting up Amazon VPC environments for a few typical Amazon VPC configurations. For this XenApp scenario, the goal is to set up the AWS environment to enable corporate users to use XenApp resources located in AWS via the NetScaler CloudBridge VPN; the NetScaler CloudBridge does require access to the public internet to establish the VPN tunnel, but you do not need to allow access to or from the public Internet for any of the resources deployed in the AWS cloud. The VPC Creation Wizard option VPC with a Single Public Subnet Only initiates the setup you are looking for.

NOTE: Servers within the farm may need to exit of AWS for things like software updates. Such actions can be accomplished either by adding a network address translation (NAT) instance in the VPC and configuring it to be public or by having the servers traverse the VPN tunnel to use the Internet access through the corporate datacenter. Amazon VPC includes a default route table that guides communications to and from instances, and the VPC Creation Wizard enables the route tables to allow instances to communicate with each other (using the internal VPC IP addresses) and externally out of the VPC (for all other IP addresses) through the NAT instance.

Based on the specifics of your XenApp Hybrid scenario, you must add several components into the results of the VPC Single Public Subnet setup:

- **One VPC created within a specific AWS region that has components spanning multiple Availability Zones. Your XenApp infrastructure will be deployed across multiple Availability Zones to provide high availability.**
- **Private subnets in each Availability Zone to hold Desktop, Control and Authentication layers. These subnets are not directly accessed by users (everything goes through the NetScalers) and hence do not need to be accessible outside of the VPC.**
- **One Internet gateway and one CloudBridge VPN per Availability Zone. These provide VPN connectivity between the corporate datacenter and the VPC.**

Putting together everything discussed thus far, Figure 4 shows the network configuration defined for the XenApp Hybrid scenario.

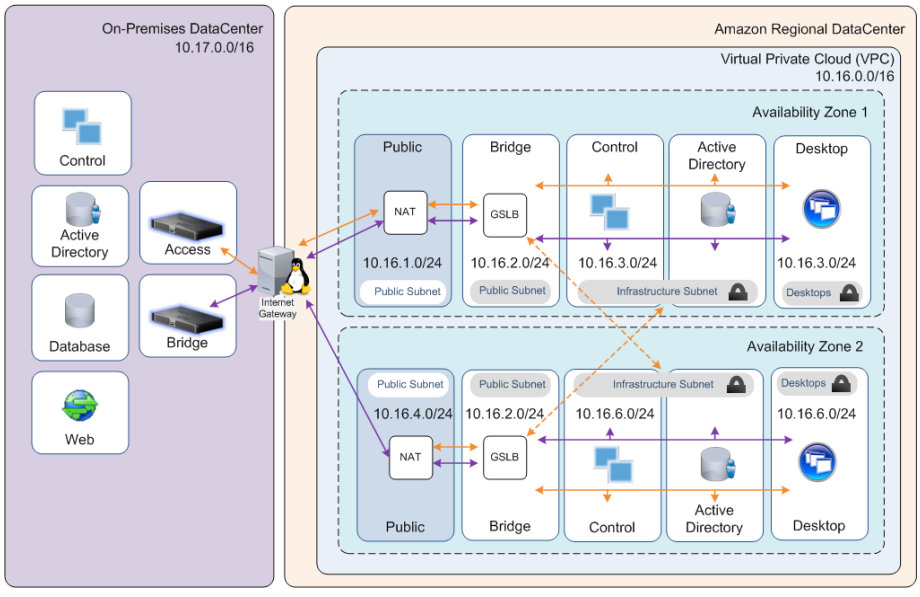


Figure 5: Hybrid Extension Network Configuration

VPC setup for the cloud scenario

For the XenApp Cloud Farm scenario, there are different requirements and setup configurations.

The cloud XenApp scenario most resembles the VPC Creation Wizard scenario "VPC with Public and Private Subnets." The differences between the cloud scenario and the hybrid scenario are:

- **With a cloud XenApp deployment, the Access and Web layers have to be deployed in AWS.**
- **In this scenario, NetScaler Load-balancing is deployed in AWS for Storefront and XML Broker Service high availability.**
- **In a cloud XenApp deployment, the NetScaler Gateway functionality will be activated for the public subnets so that users can access the resources over the Internet.**
- **Public subnets in each Availability Zone hold the public facing interfaces of the NetScaler. A VPC can have multiple subnets in which each subnet resides in a separate Availability Zone. Each subnet must reside entirely within one Availability Zone.**
- **You still want to place the Desktop, Control, Database and AD layers in private subnets; users only need to get at the NetScaler Gateway.**
- **The cloud scenario adds NAT instances in each Availability Zone to facilitate servers in private subnets communicating out to the Internet (to get operating system software updates, for example).**

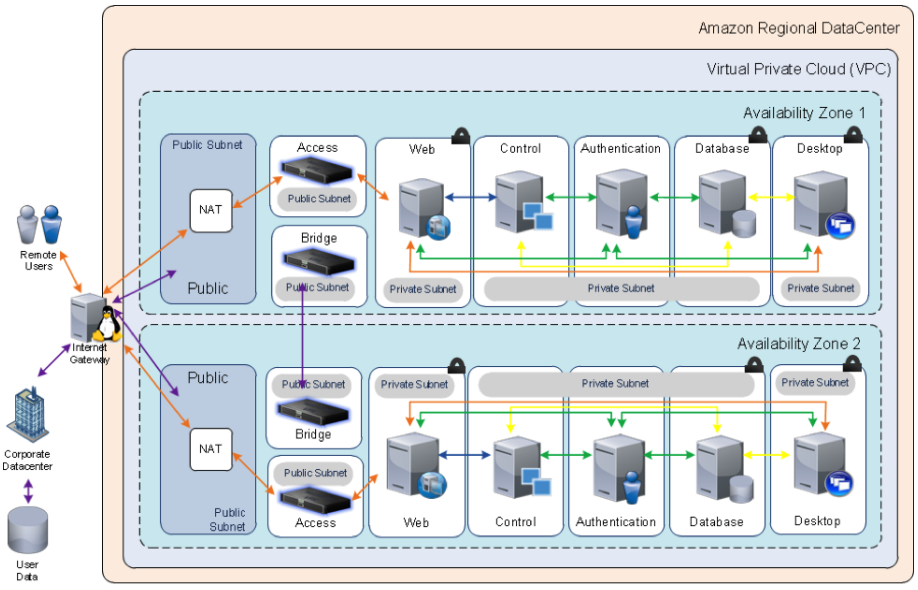


Figure 6: Complete XenApp Cloud Scenerio Neywork Configuration

Given these differences, Figure 5 shows the network setup for the XenApp cloud scenario.

AD DS setup and DNS configuration

XenApp requires AD DS for user authentication. However, you also want to leverage AD DS to provide Domain Name System (DNS) functionality within the VPC among the various server instances.

For your XenApp farm to operate, you need connectivity to one or more domain controllers to facilitate user authentication and DNS resolution across servers within the farm. In the hybrid scenario, you want the XenApp instances to authenticate to users' corporate credentials (effectively an extension of their corporate network). There are two different ways to support this configuration:

- XenApp instances could traverse the NetScaler CloudBridge connection back to the corporate data centre and authenticate to on-premises domain controllers.
- Domain controllers could be hosted in AWS and replicated from on-premises domain controllers via the NetScaler CloudBridge connection. This action allows the servers to authenticate to local (within AWS) domain controllers but still authenticate to corporate user identities and credentials.

Amazon and Citrix recommend the second option for better performance and reliability. The domain controllers can be replicated across Availability Zones (as with your other resources) to provide high availability. Microsoft provides guidance on Active Directory Replication Over Firewalls.

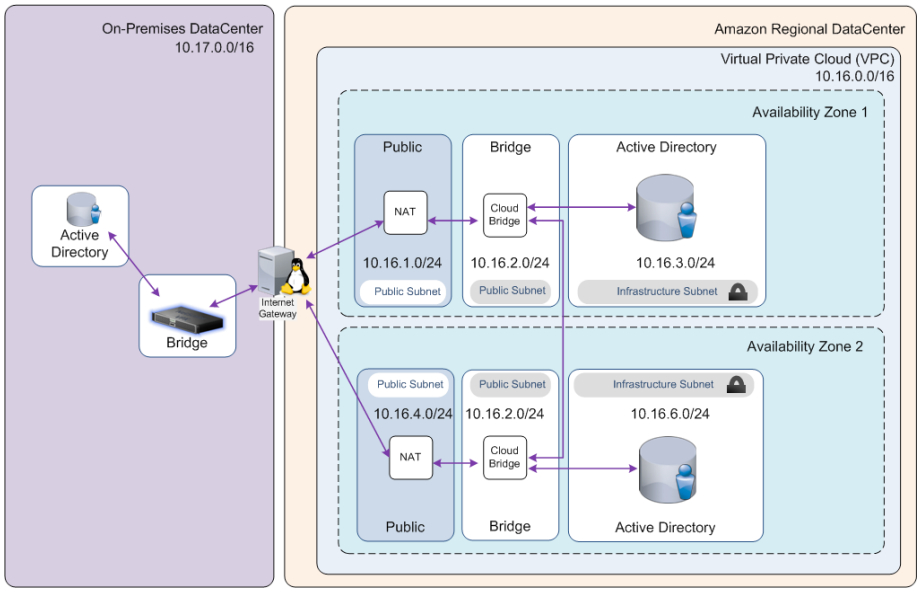


Figure 7: Microsoft Active Directory Replication

In the cloud scenario, the XenApp farm is still connected to a corporate infrastructure via VPN, but the Access and Web Layers (NetScaler Gateway and Citrix StoreFront) are located within the AWS environment. Instead, it requires AD DS to be instantiated within the AWS environment to facilitate user registration

and authentication for the NetScaler Gateway, StoreFront and XenApp instances running there. As in the hybrid scenario, Amazon and Citrix suggest hosting domain controllers in multiple Availability Zones to provide redundancy and high availability, as illustrated in Figure 7.

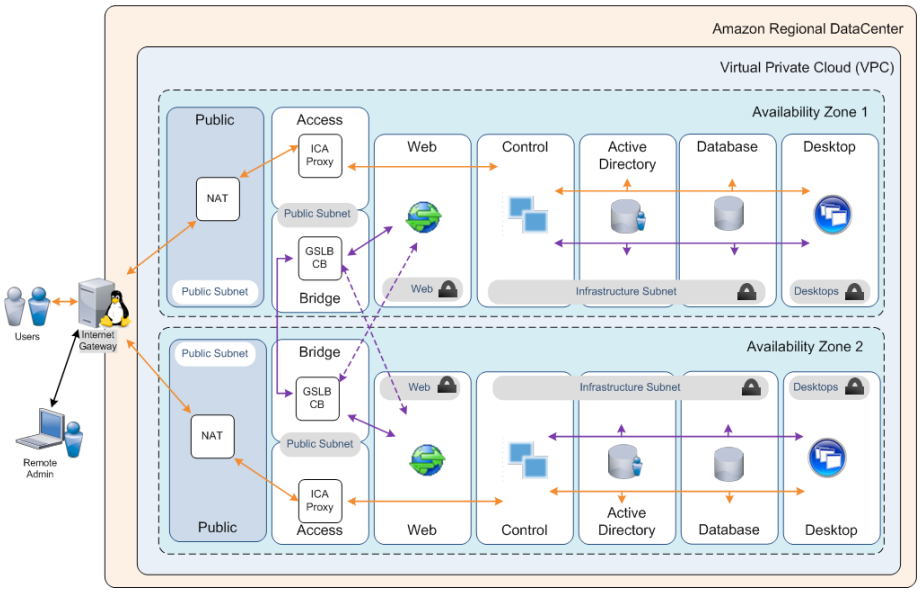


Figure 8: XenApp Cloud Scenerio

AD DS is typically run in on-premises, static environments, and there are certain typical configuration details and assumptions that are different when AD DS runs in AWS. For AD DS domain controllers to be used for DNS in AWS and across Availability Zones, each needs to be in a security group that opens User Datagram Protocol (UDP) ports 0–65,535. (Security groups are discussed in detail in a later section.)

Server setup and configuration

Now that your network is set up in the structure you need, let's tackle the task of setting up and instantiating the various server instances within the VPC to support your XenApp reference architectures.

At the heart of AWS is the Amazon Elastic Compute Cloud (Amazon EC2) web service, a cloud computing infrastructure that supports a variety of operating systems and machine configurations (e.g., CPU, RAM). AWS provides preconfigured virtual machine (VM) images (Amazon Machine Images, or AMIs) with guest operating systems (Linux®, Windows, etc.) and may have additional software (e.g., SQL Server) used as the basis for virtualized instances running in AWS. You can use these AMIs as starting points to instantiate and install or configure additional software, data, and more to create application- or workload-specific AMIs. This includes preconfigured Citrix NetScaler and CloudBridges VPXes.

To implement the various layers and roles in the XenApp reference architecture, start out with AMIs that are based on Windows Server 2008 R2, and look at the software running each one to determine which AMIs are applicable to Access, Desktop, Control, Database or AD layer servers. At this time, several AMIs support some version of Windows Server. Some AMIs include components like Microsoft Internet Information Services (IIS) for the StoreFront roles; others include SQL Server Standard (for the Database layer when located in AWS).

XenApp is not preinstalled in any of the Windows-based AMIs because of Microsoft RDS licensing model restrictions. Citrix XenApp is layered on top of the Microsoft RDS technology.

AWS, Citrix and Microsoft provide a comprehensive collection of information, tools, and resources for running Windows-based applications and XenApp workloads on AWS. You can find details on the specific AMIs that include Windows, SQL Server, etc., within the Amazon EC2 AMI catalogue. Information on AMIs for XenApp on AWS usage can be found in this blog series: http://blogs.citrix.com/authors/peterb.

Mapping XenApp server roles and servers to Amazon EC2 AMIs and instance types

A key aspect of implementing your AWS solution is choosing the appropriate AMI and instance type for each role within the farm. Each role in the XenApp reference architecture has distinct requirements for software and infrastructure resources, such as CPU, RAM, and disk storage. Microsoft and AWS have partnered to publish a number of Windows-based AMIs that include additional software components for supporting typical roles (e.g. IIS for web server, SQL Server for database server, Windows core for domain controller) that run on a variety of Amazon EC2 instance types. Citrix has also made guidance available in selecting instances in the Scalability and economics of XenApp on AWS whitepaper.

In terms of machine capacity and sizing, Citrix provides detailed guidance for various components within a XenApp farm, which can be found here so that topic is not covered in this paper. However, the basic details of typical system requirement minimums for various components within a XenApp farm are summarized in the tables that follow. For more information on this topic, please see Design and Scalability Considerations for Enterprise XenApp Deployments, StoreFront Planning Guide and Scalability and economics of XenApp on AWS whitepaper

Table 1 presents the minimum system requirements Citrix recommends for the different layers and roles within a XenApp farm.

Layer/role	Scenario	Processor	RAM	Hard disk
Access Layer (StoreFront)	Cloud	64-bit, 1 core	1 GB	80 GB
Application Layer (Workers)	All	64-bit, 4 core	16 GB	80 GB
Control Layer (Data Collector)	All	64-bit, 4 core	8 GB	80 GB
Database server	Small deployment	64-bit, 4 core	8 GB	80 GB
Database server	Medium deployment	64-bit, 8 core	16 GB	80 GB
Domain controller	All	64-bit, 4 core	8 GB	80 GB

Table 1: Minimum Resource Requirements

Table 2 shows how to map these requirements to Amazon EC2 AMIs and Windows instance types.

Tier	Applicable Amazon EC2 instance type and range	AMI to use
StoreFront	Medium (m1.medium)	Windows Server 2008 R2 + IIS
Worker server	Compute optimized Extra Large (cc2.8xlarge)	Windows Server 2008 R2
Controller server	Large (m1.large)	Windows Server 2008 R2 + IIS
Database server	General Purpose Extra Large (m3. xlarge)	Optimized SQL Server 2008 R2 AMIs from Microsoft
Domain controller	Large (m1.large)	Windows Server (in the role of a domain controller)

Table 2: Amazon EC2 Instance Types

The AMIs listed in Table 2 include the default configuration for Amazon EBS volumes (formatted as Windows file systems) for boot drive and associated data storage applicable to the role. The SQL Server 2008 R2 AMIs indicated have been configured with multiple EBS volumes to support distinct SQL Server storage components (data, logs, temp files), optimizing for storage requirements and I/O patterns of each component. Amazon EC2 also supports the ability to customize an instance, allowing you to attach additional Amazon EBS volumes or resize an existing Amazon EBS volume by taking a snapshot, and then creating a new, larger volume from the snapshot. You can then use this customized instance as the basis for a new, customized AMI. Figure 8 provides an overview of the reference model introduced earlier combined with the information from the above table.

XenApp Worker configuration

As mentioned earlier, XenApp is not pre-installed in any publically available AMI, so you must obtain sufficient licensing for deploying Microsoft RDS and Citrix XenApp in AWS and then install XenApp into your instances. Typically, you will create your own private XenApp Worker AMI, by creating a Windows Server-based instance, installing and configuring XenApp, sealing and preparing the instance for provisioning and then turning that instance into an AMI as described in the XenApp Reference Architecture Implementation Guide. This private AMI will be the basis of the various XenApp Worker instances in your farm.

When building XenApp Worker instances, using the ephemeral storage or a provisioned-IOPs EBS volume will provide the best performance for end users when the user profiles and page file are stored on that volume.

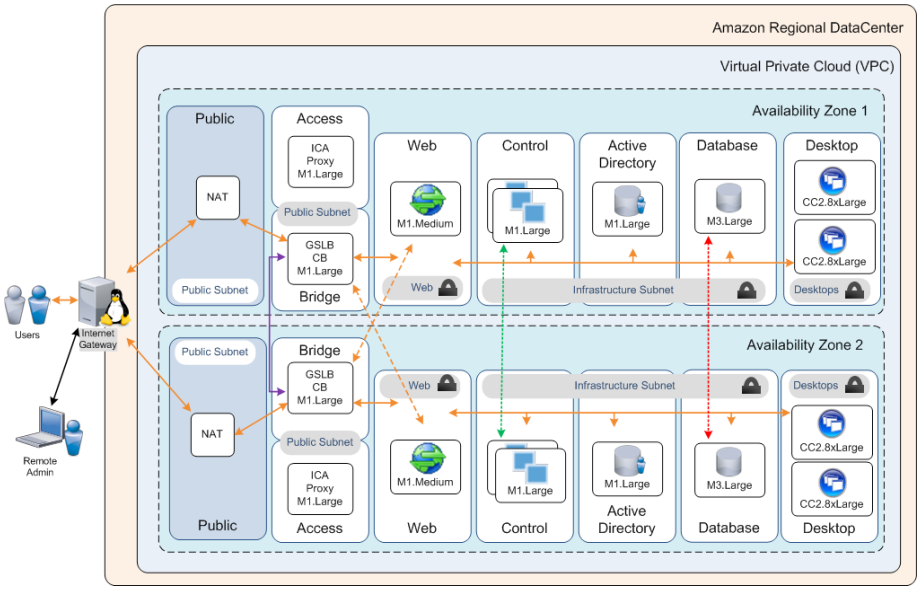


Figure 9: Complete Cloud Instance Type Recommendations

Security

Security setup is critical in the implementation of your XenApp farm to enable proper network access (in and out of the VPC, specific subnets, and the instances running each subnet) to facilitate user authentication and appropriate authorization, data privacy, and threat management (in the case of public-facing sites). These and other key elements have to be set up correctly to provide the necessary security measures and enable users to access their XenApp deployed applications and hosted shared desktops with the correct identity and authorization.

A cornerstone of your scenarios is the use of Amazon VPC for providing the overall isolation of the farm and segmenting parts of the farm (i.e., the server groups) to support the desired management and control. Within Amazon VPC and subnet isolation, there are security details that you must set up to enable proper access (and restrictions). The two main approaches at your disposal are:

- **Security groups.** A security group acts as a firewall that controls the traffic allowed in and out of a group of instances. When you launch an instance in a VPC, you can assign the instance to up to five VPC security groups. **Security groups act at the instance level, not the subnet level.**

  In general, it is a good idea to define distinct security groups for each layer. Doing so allows you to define the settings for each layer (and vary them independently) as well as restrict access to the "calling" layer (e.g., allowing the Control layer to be called only from the Desktop layer).

- **Network access control lists (ACLs).** A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. You might set up ACLs with rules similar to your security groups to add a layer of security to your VPC. **Network ACLs act at the subnet level, not the instance level.**

Security groups

Here are the two approaches discussed in greater detail:

Access Layer:

- Access Layer is the point of contact for users, so the Access Layer security group should be configured to support inbound client connection types of HTTPS/SSL (HDX is tunnelled in SSL). You can configure the Access Layer in many combination, but Citrix recommends using HTTPS for both inbound client connection types. You should create an outbound security rule that lists the Control and Desktop security group as the targets, restricting the NetScaler Gateway to sending requests out to the Control, Web and Desktop Layer instances only.

Web Layer:

- In the cloud scenario, the StoreFront instances are not directly exposed but receive requests via the NetScaler load balancer. You should configure the StoreFront instances to accept requests only from the NetScaler load balancer. Create a security rule for your access layer that restricts inbound access to the NetScaler interface (SNIP) that communicates with the StoreFront instances. Ensuring that only the NetScaler load balancers are allowed to send to and receive from the StoreFront instances. You can also set up an outbound rule to limit outgoing requests to the desktop layer instances.

Control Layer:

- The Control layer security group should be configured with an inbound rule listing the Access layer security group as an allowed sender and an outbound rule listing the database security group for outgoing messages.

Desktop Layer:

- As in the Control layer case, your Desktop layer security group should be configured with an inbound rule listing the Access layer security group as an allowed sender and an outbound rule listing the database security group for outgoing messages.

Database layer:

- You also want to restrict inbound access to the Desktop and Control layer instances, so create a security rule that restricts inbound access to the Desktop and Controller layer security groups.

The Appendix includes a chart detailing the various recommended security groups and settings for your XenApp farm scenarios.

Network ACLs

Network ACLs mirror the rules specified in security groups and add an extra layer of security to allow general access rules to be honored regardless of which instances are sending or receiving. Because network ACLs act at the network level (not the instance level), you can set up additional rules to handle certain networks, IP addresses, and address ranges in a specific way. For instance, you can set up a network ACL that defines a rule to deny ingress to a range of source IP addresses (blacklisted IP addresses). For detailed guidance on setting up Amazon VPC network ACLs, see the Amazon Virtual Private Cloud User Guide.

Administrator access

In this architecture, the Desktop, Control, AD and database layer instances are placed in private subnets, restricting access from outside the VPC. This placement reduces exposure and enhances security. However, it is still necessary to provide access to those instances for administrative purposes, such as configuration updates and troubleshooting.

To help manage the instances in the private subnet, an indirect (and secure) method is to set up one or more bastion servers in a public subnet to act as proxies, and then set up rules to allows access for these bastion servers to the Desktop, Control or Database layer instances. After bastion servers are set up, administrators can use RDP to gain access to the bastion host; they can then access other instances using RDP at their VPC private IP addresses.

Deployment

To set up your XenApp farm in AWS, you must establish and configure several complex and interrelated details to enable proper functions and the correct security settings. Furthermore, you will inevitably need to change the configuration over time to perform such actions as adding instances for scale out or updating instance configurations.

AWS provides a number of tools and approaches for facilitating deployment in AWS:

- **AWS Management Console.** The AWS Management Console is an interactive tool that is good for starting out or smaller deployments. However, for more complex scenarios or automated deployment sequences, consider one of the other options described below.

- **AWS application programming interface (API) tools.** AWS provides several command-line interface (CLI) commands and programmatic web service APIs that are typically built into scripts; these commands allow a set of actions to occur in a coordinated way.
- **AWS sample code and libraries.** AWS provides a Sample Code & Libraries Catalog to support application-based setup and configuration. Several programming languages are supported through software development kits (SDKs) that AWS provides.
- **AWS CloudFormation.** AWS provides an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. With AWS CloudFormation, you do not need to figure out the order in which AWS services need to be provisioned or the subtleties of how to make those dependencies work.

  You can use a tool called AWS CloudFormer to reverse-engineer an existing set of resources or settings running in an AWS account into an AWS CloudFormation template. So, a typical approach for a complex setup is to manually deploy or configure components of the SharePoint Server farm, and then use this tool to generate an appropriate AWS CloudFormation script.
- **Windows and .NET Developer Center.** These Windows and Microsoft .NET tools include the AWS SDK for .NET and the AWS Toolkit for Visual Studio.

A key approach to automating deployment of components within an AWS solution is to create custom AMIs for distinct roles that have additional software dependencies and configuration requirements. For the XenApp reference architecture, distinct roles are defined (StoreFront, XenApp Worker, XenApp Controller, and others) for which you can create custom AMIs. Custom AMIs for the XenApp farm architecture can be based on public Windows-based AMIs (as indicated earlier) or Windows-based AMIs that you create as a starting point.

Monitoring and management

You must be able to monitor a number of core dimensions within a XenApp farm to enable corrections and updates when issues occur or performance suffers. Amazon CloudWatch is an AWS service that monitors various health metrics associated with AWS resources. You can use it to collect, analyze, and view system and application metrics so that you can make operational and business decisions more quickly and with greater confidence. Amazon CloudWatch sets several predefined metrics, such as CPUUtilization and disk I/O performance, that AWS measures and that you can view and act upon. You can also publish your own metrics directly to Amazon CloudWatch to allow statistical viewing in the AWS Management Console and to issue (and react on) custom alarms.

Citrix EdgeSight for XenApp utilizes deep instrumentation from within the XenApp application and hosted shared desktop delivery environment to provide a comprehensive management solution for XenApp. EdgeSight captures, aggregates and visualizes fine-grained metrics from the instant a user attempts to access an application throughout the lifecycle of the session.

Figure 10: Citrix EdgeSight for XenApp

Citrix NetScaler Insight Center provides a 360-degree view for virtual desktop and application traffic as well as web applications such as Citrix StoreFront. Based on the popular industry standard AppFlow, Insight Center leverages existing NetScaler already in place in the application fabric such as our NetScaler ADCs deployed in our XenApp deployment scenarios. Being strategically situated at key focal points in the XenApp application path (Bridge and Access Layers), NetScaler appliances are uniquely positioned to capture the native intelligence from the network and application traffic passing through them.

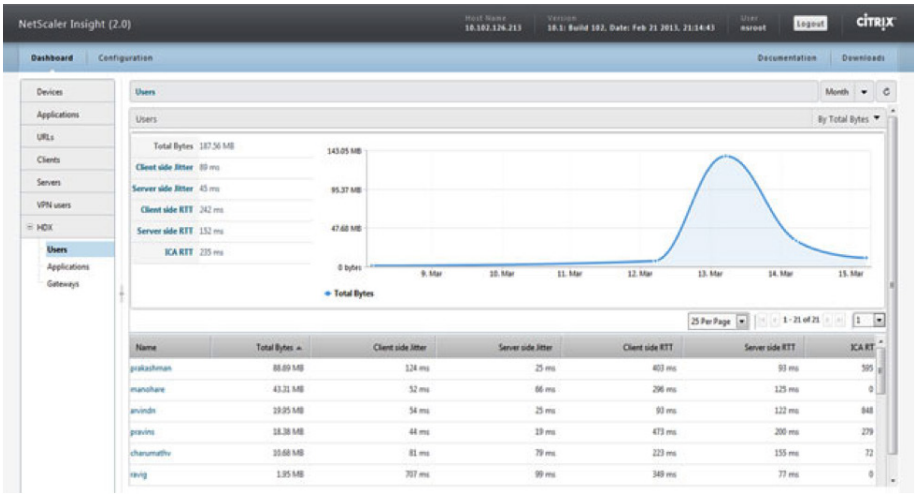


Figure 11: NetScaler Insight Center

Microsoft System Center Operations Manager is the typical tool used to monitor and manage a Microsoft-based infrastructure. Fortunately, Operations Manager can be used in AWS, too. The Windows-based infrastructure on AWS includes the standard Operations Manager agents for Windows Server, SharePoint Server, and SQL Server.

In the hybrid scenario, Operations Manager works as it does in an on-premises case, because your NetScaler CloudBridge effectively extends the enterprise network into the AWS cloud. In the cloud scenario, Operations Manager can be hosted in an instance and accessed as a published application via Citrix Receiver and provide monitoring and management against the other components of the XenApp farm.

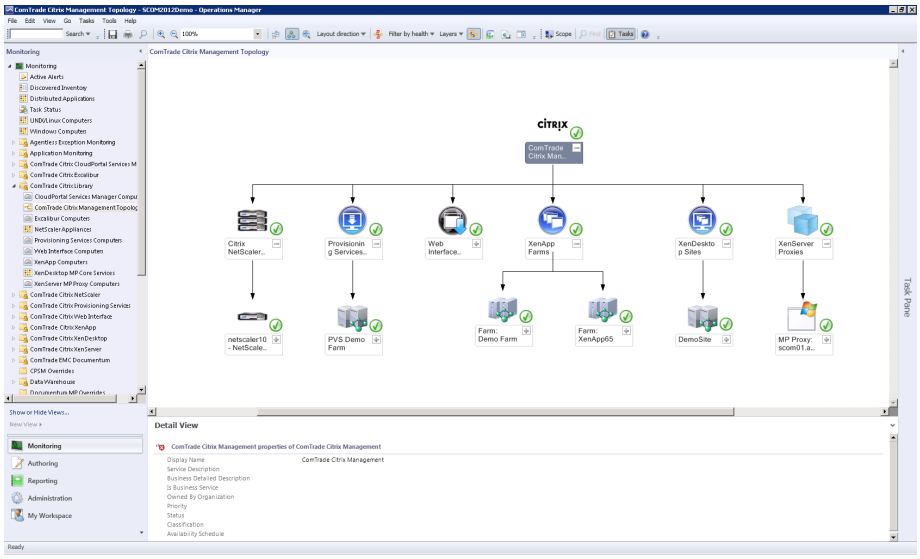


Figure 12: Microsoft System Center Operations Manager view of XenApp form

The ComTrade management pack for Citrix XenApp is an availability and performance management solution that extends the capabilities of Microsoft System Center Operations Manager to include Citrix XenApp infrastructure. The product fully integrates topology, health, and performance data into the Operations Manager console. Providing IT admins with XenApp performance and availability information integrated with other related back-end application layers such as Active Directory or SQL Server.

CA NimSoft is an IT monitoring and service management solution that spans traditional data centers such as our on-premises deployment as well as cloud environments such as AWS. It can be deployed in a SaaS or on-premises model.

The CA Nimsoft Monitor for Citrix XenApp provides insight from the end user's perspective into the availability and performance of applications and desktops delivered via the XenApp infrastructure. CA Nimsoft Monitor for AWS gives the required insights needed to proactively monitor AWS performance, offering visibility into resource utilization, operational issues and overall demand patterns for XenApp resources running in AWS.

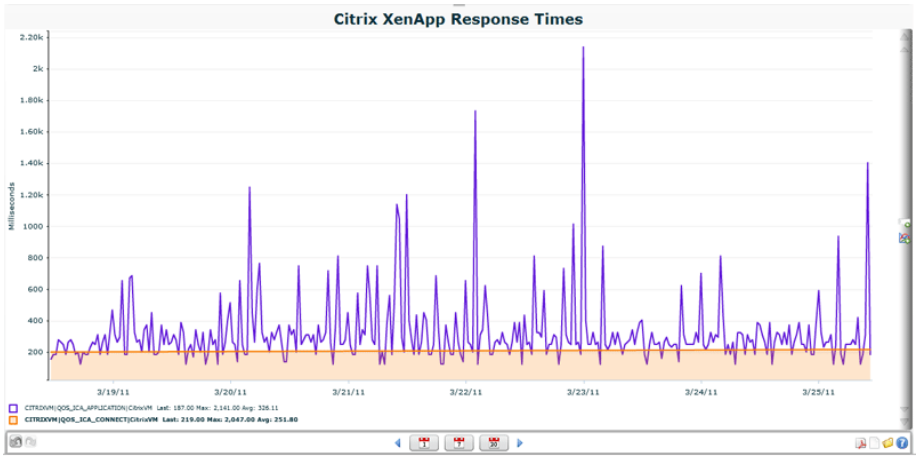


Figure 13: CA Nimsoft XenApp Monitoring

Putting it all together

With all the key topics covered, let's see how your XenApp deployment scenarios are ultimately set up in an AWS environment.

Hybrid XenApp Farm

Recall from the earlier discussions, the key components of the hybrid XenApp farm extended in an AWS environment scenario are as follows:

- Amazon VPC, with NetScaler CloudBridge VPN connection to the corporate datacenter Private subnets only, connected to the corporate network via CloudBridge
- At least two Availability Zones used to survive the low probability of an Availability Zone failure
- Resource Domain Controllers located in AWS
- StoreFront Load-balancing on-premises
- SQL Server in mirrored configuration on-premises

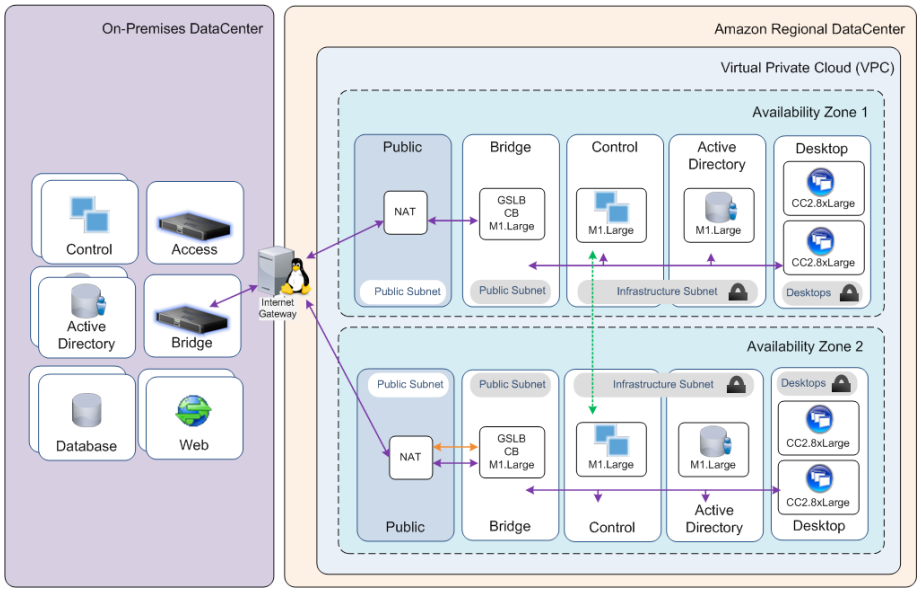


Figure 14: Hybrid Farm Model with Instance Types

Cloud XenApp Farm

From earlier discussions, recall that the key components for the XenApp Farm hosted in an AWS environment scenario are as follows:

- Amazon VPC, with public and private subnets
- NetScaler Gateway instances in the public subnet
- NetScaler GSLB across the NetScaler Gateway servers
- Bastion host in a public subnet, to provide administrative access to internal instances
- At least two Availability Zones used to survive the low probability of an Availability Zone failure
- Multiple StoreFront servers behind NetScaler Gateways within each Availability Zone in a private subnet
- SQL Server in mirrored configuration across Availability Zone private subnets
- AD DS domain controllers in AWS for user registration and authentication

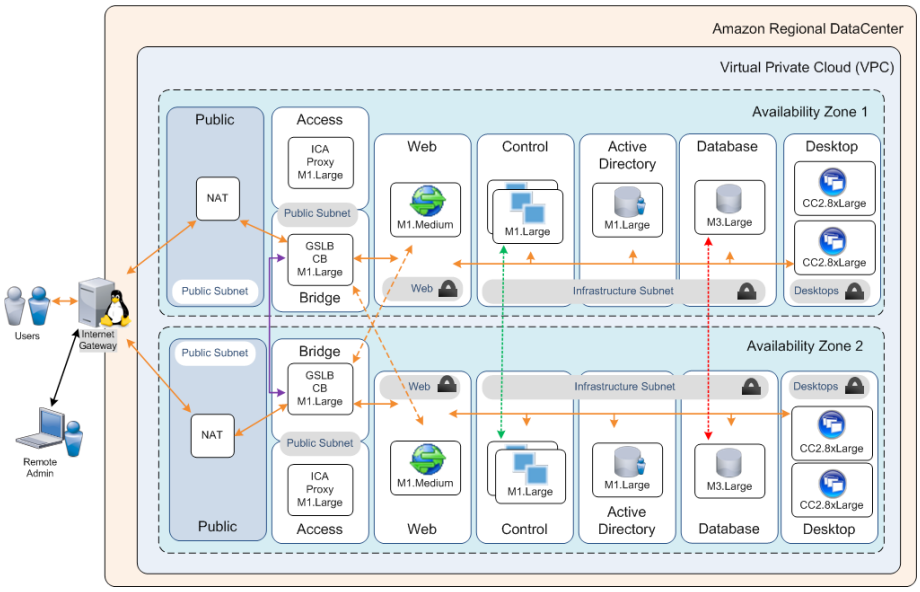


Figure 15: XenApp Cloud Model

Although you can use XenApp to support a variety of application and hosted shared desktop delivery goals, these scenarios are two of the most common. See the next section for information about other scenarios and additional resources.

Conclusion

This paper discusses two common deployment scenarios for XenApp—hybrid and cloud—and how to create them in an interconnected On-Premises - AWS cloud environment. We discussed how you can leverage different services that AWS provides (network setup, server setup, security, and deployment) and configure them specifically to run enterprise-class software like XenApp at scale in a secure fashion that is easier to maintain.

Further reading

Citrix on AWS:

- http://www.citrix.com/amazon
- http://blogs.citrix.com/author/peterb
- Scalability and economics of XenApp on Amazon Cloud
- XenApp on AWS Sizing and Economics costing model
- Setup Guide for the XenApp on AWS CloudFormation Template
- Three keys to building the best front-end network for virtual desktop delivery

Microsoft on AWS:

- http://www.awsmicrosite.com
- Amazon EC2 Windows Guide: http://docs.amazonwebservices.com/AWSEC2/latest/WindowsGuide/Welcome.html?r=7870
- Microsoft AMIs for Windows and SQL Server:
  - http://aws.amazon.com/windows
  - http://aws.amazon.com/amis/Microsoft?browse=1
  - http://aws.amazon.com/amis/6258880392999312 (SQL Server)

Appendix

Security group settings for a XenApp Farm

The following chart provides an example of the typical security group settings recommended for the XenApp reference architecture discussed in this document. For more information on the ports or their purpose, please see the Citrix Port Reference guide.

Source/Destination Security Group	Direction	Protocol	Port	Purpose
NAT Security Group (NatSG)				
PrivateSG	Inbound	ALL	ALL	ALL
WorkerSG	Inbound	ALL	ALL	ALL
0.0.0.0	Inbound	TCP	22	SSH
0.0.0.0	Outbound	ALL	ALL	ALL
NetScaler Security Group (NetscalerSG)				
Self	Inbound	ALL	ALL	ALL
0.0.0.0	Inbound	ICMP	ALL	Ping
0.0.0.0	Inbound	ICMP	Echo Reply	Ping
0.0.0.0	Inbound	TCP	22	SSH
0.0.0.0	Inbound	TCP	80	HTTP
0.0.0.0	Inbound	TCP	443	HTTPS
0.0.0.0	Inbound	TCP	3389	RDP
0.0.0.0	Inbound	TCP	4001	NetScaler
0.0.0.0	Inbound	TCP	3008-3011	NetScaler
0.0.0.0	Inbound	UDP	53	DNS
0.0.0.0	Inbound	UDP	67	DHCP
0.0.0.0	Inbound	UDP	123	NTP
0.0.0.0	Inbound	UDP	161	SNMP
0.0.0.0	Inbound	UDP	500	NetScaler

Source/Destination Security Group	Direction	Protocol	Port	Purpose
0.0.0.0	Inbound	UDP	3003	NetScaler
0.0.0.0	Inbound	UDP	4500	NetScaler
0.0.0.0	Outbound	ALL	ALL	ALL
0.0.0.0	Outbound	ICMP	ALL	Ping
0.0.0.0	Outbound	ICMP	Echo Reply	Ping
0.0.0.0	Outbound	UDP	53	DNS
Private Security Group (PrivateSG)				
Self	Inbound	ALL	ALL	ALL
Self	Inbound	ICMP	ALL	Ping
NetScalerSG	Inbound	TCP	3389	RDP
PublicSG	Inbound	TCP	80	HTTP
PublicSG	Inbound	TCP	389	LDAP
PublicSG	Inbound	TCP	443	HTTPS
PublicSG	Inbound	TCP	639	LDAP Secure
PublicSG	Inbound	TCP	1494	ICA/HDX
PublicSG	Inbound	TCP	2598	IMA
PublicSG	Inbound	TCP	5985	WinRM
PublicSG	Inbound	TCP	5986	WinRM
PublicSG	Inbound	TCP	7279	Licensing
PublicSG	Inbound	TCP	27000	Licensing
PublicSG	Inbound	UDP	53	DNS
0.0.0.0	Outbound	ALL	ALL	ALL
Self	Outbound	ALL	ALL	ALL
0.0.0.0	Outbound	ICMP	ALL	Ping
0.0.0.0	Outbound	TCP	3389	RDP
Public Security Group (PublicSG)				
0.0.0.0	Inbound	ALL	22	SSH
Self	Inbound	ALL	ALL	ALL
PrivateSG	Inbound	ALL	ALL	ALL
0.0.0.0	Inbound	TCP	22	SSH
0.0.0.0	Inbound	TCP	80	HTTP
0.0.0.0	Inbound	TCP	443	HTTPS
0.0.0.0	Inbound	TCP	1494	ICA/HDX
0.0.0.0	Inbound	TCP	2598	IMA
0.0.0.0	Inbound	TCP	3389	RDP

Source/Destination Security Group	Direction	Protocol	Port	Purpose
0.0.0.0	Inbound	TCP	80	HTTP
0.0.0.0	Inbound	TCP	443	SSL
0.0.0.0	Inbound	TCP	1494	ICA/HDX
0.0.0.0	Inbound	TCP	8080	HTTP/S
0.0.0.0	Outbound	ALL	ALL	ALL
PrivateSG	Outbound	ALL	ALL	ALL
WorkerSG				
MgmtSG	Inbound	ALL	ALL	ALL
PublicSG	Inbound	TCP	1494	ICA/HDX
PublicSG	Inbound	TCP	2598	IMA
0.0.0.0	Outbound	ALL	ALL	ALL
MgmtSG	Outbound	ALL	ALL	ALL
Management Security Group (MgmtSG)				
Self	Inbound	ALL	ALL	ALL
WorkerSG	Inbound	ALL	ALL	ALL
PublicSG	Inbound	TCP	80	HTTP
PublicSG	Inbound	TCP	389	LDAP
PublicSG	Inbound	TCP	443	HTTPS
PublicSG	Inbound	TCP	639	LDAP Secure
PublicSG	Inbound	TCP	1494	ICA/HDX
PublicSG	Inbound	TCP	2598	IMA
PublicSG	Inbound	TCP	3389	RDP
PublicSG	Inbound	TCP	5985	WinRM
PublicSG	Inbound	TCP	5986	WinRM
PublicSG	Inbound	TCP	7279	Licensing
PublicSG	Inbound	TCP	27000	Licensing
0.0.0.0	Outbound	ALL	ALL	ALL
Self	Outbound	ALL	ALL	ALL

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.

0613/PDF

citrix.com