Flexing to the Cloud with Citrix XenDesktop and Amazon Web Services

CITRIX®

citrix.com

Table of contents

Introduction 4
- The hybrid cloud explained 4
- Private cloud versus public cloud 4
- Benefits of a hybrid cloud for applications and desktops 4

The Citrix cloud continuum 5

Hybrid cloud use cases 5
- Commodity applications and desktops 5
- Q&A test/development 6
- Enterprise IT/Outsourced data center 6
- Business partner and/or temporary workforce 6
- Application disaster recovery and redundancy 6

Virtual workspace considerations 6
- Profile and user data 6
- Domain authentication 7

How does Citrix enable a flexible hybrid cloud architecture? 7
- XenDesktop 7.5 / XenApp 7.5 8
- StoreFront 8
- NetScaler VPX 8
- NetScaler CloudBridge connector 9
- CloudBridge VPX/MPX 9
- Citrix Cloud formation templates 9

Solution overview 10
- Meeting business demand and users needs 10
- Extending resources to the cloud 10

Solution deep dive 11
- Introduction 11
- The customer cloud environment – Amazon Web Services 12
- Start connecting to the cloud 14
- Amazon AWS CloudBridge connector pre-requisites 16
- On-premise CloudBridge connector pre-requisites 18
- Install and configure CloudBridge connector 18
- AWS XenDesktop site pre-requisites 20
- Creating the desktop server base image 21
- AWS XenDesktop site creation 21
- Machine catalog creation 25
- Delivery group creation 27
- On-premise StoreFront integration 29
- Conclusion 30

Resources and tools **30**
Citrix related information 30
Amazon AWS related information 31
3rd party resources 31
Key contributors 32

Click on the section names above to navigate to that portion of the book and the arrow icon to return to the table of contents from any page.

Introduction

The hybrid cloud explained

With the recent surge in interest around cloud service technologies, customers are exploring what a cloud-based strategy can provide them. With a typical public cloud infrastructure platform, the service provider only lays the foundation: an operating system, server management platform, and supporting services. The customer then installs applications and/or develops the necessary user workspaces.

With the virtualization movement and subsequent cloud-era dramatically changing the way IT protects and delivers applications, desktops, and data to an ever-increasing mobile workforce, increased adoption of virtualization technologies and cloud-based solution architectures have brought about a myriad of benefits. With these benefits however have come additional layers of complexity for each new variation in the provisioning and delivery process.

Advancements in virtualization technology have added layers of complexity as both physical servers, virtual servers and (as both physical server and virtual servers along with associated storage associated storage now need to be configured, managed and monitored independently. To reap the larger benefits, the once simple service delivery workflow has been expanded to account for the additional layers, including physical or virtual, and locations, including private, public or hybrid cloud, that are now integrated within solution architecture. Ideally hybrid cloud solution should be a seamless extension of the data center, consisting of desktop and application resources from private and public clouds, hosted on or off-premise.

Private cloud versus public cloud

The integrated platform for provisioning hybrid clouds using XenDesktop and XenApp enables IT admins to deliver a complete range of apps and desktops, whether in the private cloud or in the public cloud, while consolidating management, monitoring and maintenance tasks. The private cloud is the collection of on-premise infrastructure, desktops, applications and data delivered on demand by enterprise IT. Private clouds can also be hosted off-premise. In this case, a service provider offers a portion of its public infrastructure for exclusive use by a single customer, also known as a tenant.

The public cloud is the collection of off-premise, multi-tenant infrastructure, storage and computing resources, as well as SaaS applications and data, which are delivered on demand by external cloud service providers. Public clouds allow multiple customers, or tenants, to share the underlying resources with each paying only for the resources it consumes.

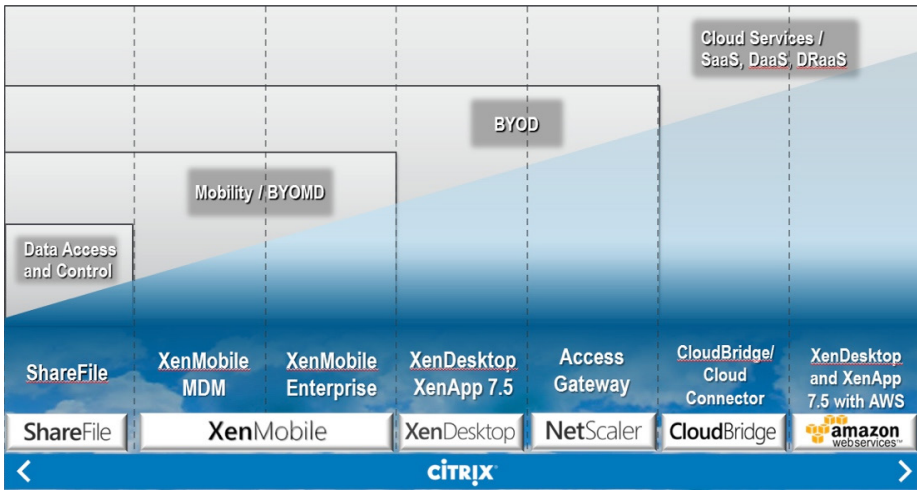
Benefits of a hybrid cloud for applications and desktops

Citrix is changing the role of IT as enterprises transition into the cloud-era through products and solutions that transform any Windows application or desktop into a cloud service delivered across any network, to any device. Citrix XenDesktop 7.5 and XenApp 7.5 provide cloud-ready application and desktop service delivery from any type of private, public and hybrid cloud enabling enterprises to couple cloud

computing with application and desktop virtualization to realize the combined resource optimization, infrastructure agility and economic benefits from a single platform. Citrix XenDesktop and XenApp are the industry's only cloud-ready software platforms to deliver mobile, secure access to a complete collection of app and desktop virtualization solutions. Citrix provides a hybrid cloud solutions that gives organizations the freedom to deploy applications when and where they make the most sense to meet an organization's security, performance, and availability requirements.

The Citrix cloud continuum

As we have seen, many enterprises are increasingly turning to hybrid clouds to combine the benefits of building private and public clouds as well as leveraging existing IT infrastructure to cut costs, maximize value and modernize the way IT services are delivered. The Citrix enterprise product portfolio is built such that no matter what stage a customer is at during this transformation to leverage cloud, Citrix has the products, technologies and reach to make switching to the cloud easier as the industry's only integrated end-to-end cloud platform. Furthermore, due to Citrix's high level of product integration, at no point in the process does a customer waste resources on point-based or stop-gap solutions.



Hybrid cloud use cases

Commodity applications and desktops

Generally the best practice when it comes to hosting applications is to keep the application logic next to the data. While this is accurate with respect to mission critical or line of business applications; sometimes there are general use or commodity applications than can function equally well no matter where their logic resides. Often the moving of these applications to the cloud brings along with it various cost savings as well as business agility benefits through the rapid provisioning and de-provisioning of applications.

Q&A test/development

Ramping up resources for application testing and development can be a costly endeavor. Providing cloud access to testers allows for the rapid provisioning of necessary resources for the testing phase, and then the destruction of them upon completion of the project. The ability to rapidly scale up an environment and only pay for the resources that are being used can be a rather large savings in not only time, but also on-going administrative and support overhead.

Enterprise IT/Outsourced data center

Many companies are exploring the benefits of outsourcing data center functionality. These include the ability to avoid the heavy costs and requirements involved in building an entirely new data center. A cost-effective option would be one that allows for a seamless increase capacity with linear cost curve. The on-demand capacity and dynamic enterprise scalability of a Citrix cloud solution would meet these requirements perfectly.

Business partner and/or temporary workforce

Companies require rapid deployments of corporate resources to contract and other “non-employees”. The use of a hybrid model allows for the flexibility of supplying the contract working a desktop in the cloud that meets company standards, while securely accessing applications located in the company’s datacenter. Upon completion of the contract, a company can simply terminate the instance that resides in the cloud as to no incur any additional cost.

Application disaster recovery and redundancy

Increasingly more companies are discovering and starting to leverage cloud services for disaster recovery. A cloud-based service model is an attractive alternative for companies that may be strapped for IT resources; most common these days in SMB’s. Cloud service’s usage-based costing model is often a great fit for disaster recovery because the expensive secondary infrastructure spends most of its time sitting idle while on-premise resources are used in the everyday course of business. Having an organizations disaster recovery site(s) in the cloud reduces the need for data center space, IT infrastructure and IT resources, which can lead to significant, cost reductions. These reductions often enable small and medium sized companies to deploy disaster recovery solutions that were usually only found in large enterprise.

Virtual workspace considerations

Profile and user data

In general it is a Citrix delivery model best practice to separate the applications from the desktops. In doing so, users are provided a seamless workspace where applications appear to be locally installed within the client operating system or virtual desktop and can communicate with one another natively. Additionally since applications are not physically installed into the golden image, image sizes are kept to a minimum which increases performance and helps control storage

costs. In a typical hybrid cloud VDI deployment, where the shared virtual desktops are hosted in the cloud and the applications are hosted on-premise, there are no user data or profile implications as no architectural changes to the application hosting are required. Cloud-based desktop users will leverage a mandatory profile, enforced by Active Directory OU membership and the user's roaming profile will be accessible through the application session.

Domain authentication

When designing a Hybrid cloud solution for desktops and/or applications an important consideration will be your domain authentication topology. Active Directory domain controllers can run within an AWS cloud environment and be replicated from existing on-premise domain controllers using the CloudBridge Connector. This allows the servers to authenticate to local domain controllers, but still authenticate to corporate user identities and credentials. Often replicating these services in the cloud provides for better authentication performance. It is recommend to replicate domain controllers across Availability Zones (as with other resources) to provide high availability.

If security or compliance issues prohibit placing a read/write domain controller off premise, it is also possible to directly connect to existing on-premise domain controllers through the CloudBridge Connector. Some considerations with this approach however include making sure the cloud-based server resources are properly joined to the domain and can complete successful DNS name resolution with the domain. Additionally, the organization's physical connection to the Internet should be of adequate size and quality to support all possible domain authentication traffic along with all ICA traffic from user sessions. Refer to the Resources section for more information on sizing of links for ICA traffic as well details on configuring a read-only domain controller.

How does Citrix enable a flexible hybrid cloud architecture?

XenDesktop 7.5 / XenApp 7.5

Citrix XenDesktop is a desktop virtualization and VDI solution that delivers a complete Windows desktop experience as an on-demand service to any user, anywhere. Whether users are task workers, knowledge workers, or mobile workers, XenDesktop can quickly and securely deliver individual applications or complete desktops while providing a high-definition user experience. The recently released XenDesktop 7.5 simplifies virtual desktop delivery and Windows app delivery to an increasingly mobile workforce by leveraging the elasticity of hybrid clouds and the security of mobile device management. Only XenDesktop can provision application or desktop workloads to private or public cloud infrastructure alongside a traditional virtual infrastructure deployment. Support through Amazon Web Services or any Citrix cloud platform-based public cloud or a private cloud infrastructure. Support for Windows Azure will be available in the near future.

Citrix XenDesktop and XenApp have been redesigned as cloud ready solutions for delivering both applications and desktops on any type of cloud infrastructure by integrating with any virtual infrastructure technology, storage infrastructure and

complex network topologies to deliver a single, unified platform. XenDesktop and XenApp now enable enterprise IT to build a common service delivery architecture for all Windows apps and desktops leveraging common policies and tools that simplify deployment and management. By delivering Windows apps and desktops as a cloud-like service, XenDesktop and XenApp can handle multiple versions and instances of both Windows Server and desktop operating systems from a single platform. XenDesktop and XenApp are built to leverage any virtual infrastructure or cloud management platform.

Whether using the included Citrix XenServer, leveraging the performance and rising popularity of Microsoft Hyper-V, or building on an existing VMware vSphere infrastructure, XenDesktop is built to be hypervisor, storage and network agnostic. Citrix XenDesktop and XenApp are the first solutions to be fully integrated for cloud solutions. Virtual apps and desktops can be deployed on popular cloud platforms including Apache CloudStack based Citrix CloudPlatform or Amazon Web Services (AWS) making it easier than ever to dynamically expand the infrastructure footprint. For details refer to the XenDesktop and XenApp administration guide in the Resources section.

StoreFront

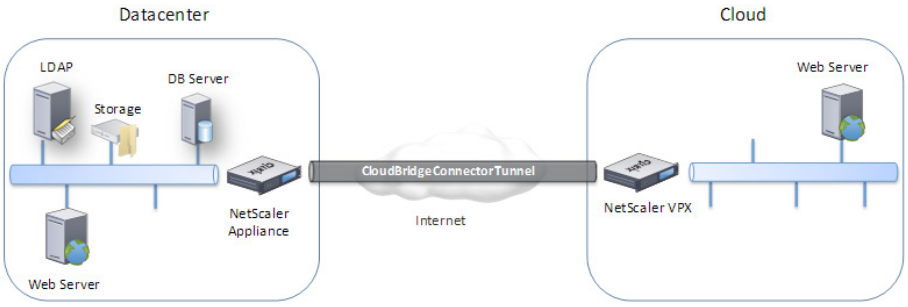
This increase in mobile activity has led to the concept of the app store, providing users with one centralized access point for all the applications available for a particular platform delivered leveraging a self-service model. App stores are popular with users because applications are easy to access and users can select applications to meet their individual needs, not to mention synchronize their applications across multiple devices. The user experience is both personal and consistent. With Citrix StoreFront you can bring that same on-demand app store experience to your enterprise. StoreFront enables you to create universal enterprise app stores to facilitate your users' mobile workstyles while giving you centralized control. Like consumer app stores, StoreFront stores provide users with on-demand, self-service access to their business resources. However, StoreFront expands the experience across all your users' devices, including their mobile devices. Users get a single, consistent point of access to their desktops and applications from all their devices, enabling them to work wherever and whenever they want. For details refer to the StoreFront administration guide in the Resources section.

NetScaler VPX

The Citrix NetScaler product line optimizes delivery of applications over the Internet and private networks, combining application-level security, optimization, and traffic management into a single, integrated appliance. You install a NetScaler appliance in your server room and route all connections to your managed servers through it. The NetScaler features that you enable and the policies you set are then applied to incoming and outgoing traffic. For details refer to the Netscaler administration guide in the Resources section.

NetScaler CloudBridge connector

The CloudBridge connector is a feature of the Citrix NetScaler and Citrix CloudBridge appliances that seamlessly connects enterprise datacenters to external clouds and hosting environments. This secure connectivity is accomplished through a secure GRE tunnel and makes the cloud a secure seamless extension of your enterprise network.



CloudBridge VPX/MPX

Citrix CloudBridge appliances optimize your WAN links, giving your users maximum responsiveness and throughput at any distance. A CloudBridge appliance is easy to deploy, because it works transparently. You do not have to change your applications, servers, clients, or network infrastructure. CloudBridge delivers industry leading advanced TCP protocol acceleration, which reduces delays on congested or high-latency links. Additionally, protocol acceleration for Windows network file systems (CIFS), XenApp (ICA and CGP, including the new multi-session ICA standard), Microsoft Outlook (MAPI), and SSL. On top of this, CloudBridge can provide bandwidth saving multi-session compression with compression ratios of up to 10,000:1. The CloudBridge is an optional component of the Citrix flex cloud solution and its integration will be covered in detail in a subsequent whitepaper.

Citrix Cloud formation templates

The AWS EC2 cloud not only provides the on-demand resources (compute, database, network etc.) you need to deploy a XenApp 7.5 solution but also provides a way to script the provisioning and configuration steps so you can deploy it easily. AWS CloudFormation enables you to create and provision AWS infrastructure deployments predictably and repeatedly. It helps you deploy AWS services such as Amazon Elastic Compute Cloud (EC2), Amazon Elastic Block Store (EBS), and Auto Scaling groups to build reliable, scalable, and cost-efficient applications. In addition, we've provided some basic Windows PowerShell scripts for a more detailed configuration of the Windows-based Amazon EC2 instances.

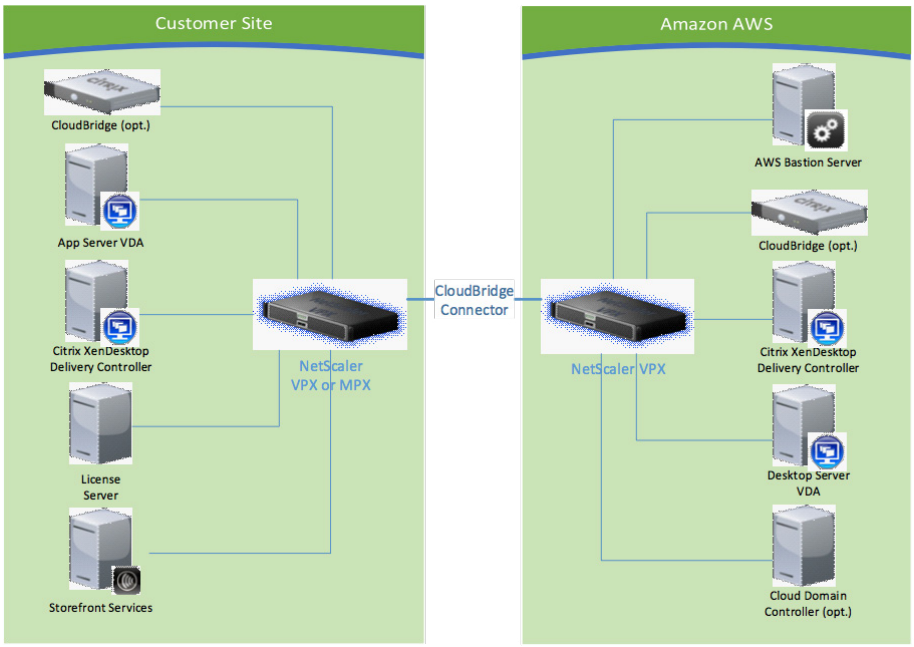
These Windows PowerShell scripts provide limited functionality and are not meant to represent a final solution. The scripts are built from samples freely available on the usual Windows PowerShell community sites and are meant to show how you can use AWS CloudFormation and Windows PowerShell to reach deep into your

instances at provisioning time and perform the necessary configuration steps. This CloudFormation template constructs a VPC, with a NetScaler Gateway, temporary Domain Controller, Bastion Host, Delivery Controller and a VDA Master Image. When deploying a production environment, you will want to replace the scripts with your own. To download the template, refer to the Resources section in this paper.

Solution overview

Meeting business demand and users needs

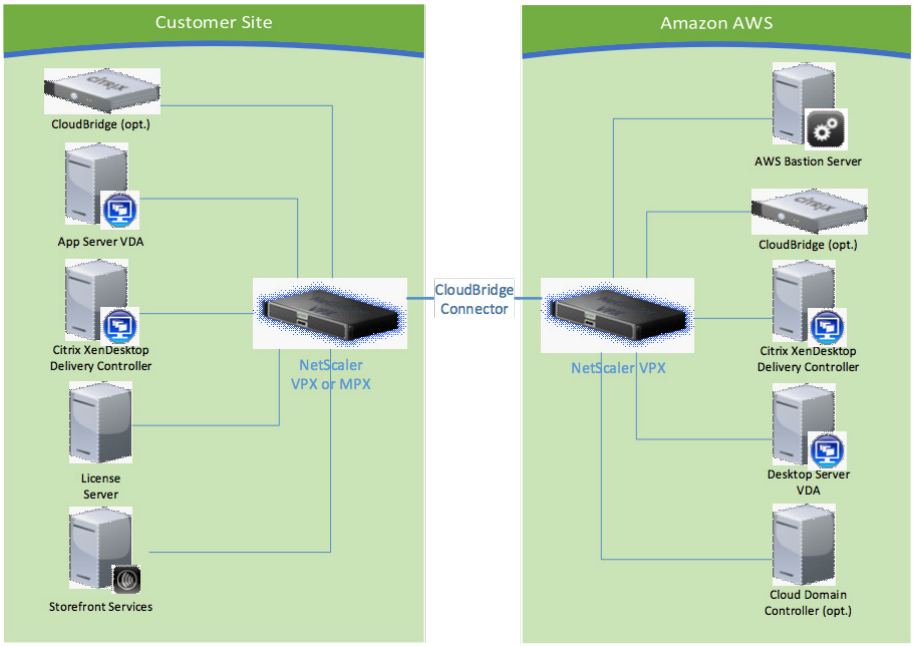
Public clouds provide seemingly unlimited scale, making them appropriate for situations with unpredictable demand. Users demand a seamless, reliable, high performance experience from the desktop to the data center to the cloud. Citrix meets these demands by powering mobile workstyles through solutions that address people, data and apps while powering public and private cloud services through solutions for unifying, bridging and building cloud environments. The cornerstone of the Citrix solution set is the XenDesktop delivery platform, featuring the FlexCast Architecture. XenDesktop meets these demands and provides business agility by separating the applications from the desktop. Refer to the Resources section for more details on the benefits of the Flexcast architecture.



Extending resources to the cloud

Extending application and desktop resources, otherwise known as flexing to the cloud, involves the deployment and integration of a parallel XenDesktop site located in the cloud. This parallel site provides customers a high-performance environment that can grow and change in an on-demand fashion based on current user and business needs. Desktops, applications or both can be quickly provisioned and

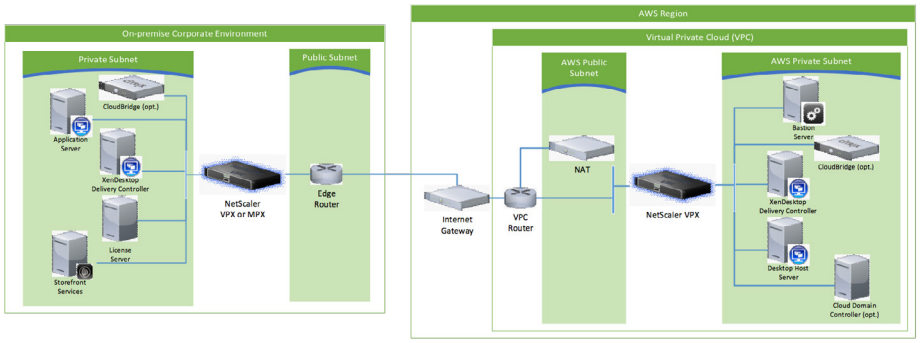
deployed via this cloud environment and then leveraged transparently through existing access methods that users are familiar with. Citrix licensing, management and authentication can be integrated with existing on-premise tools, while seamless, secure connectivity between the cloud and on-premise resources is provided via the CloudBridge Connector.



Solution deep dive

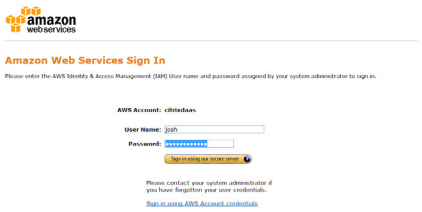
Introduction

The Citrix XenDesktop flex cloud solution consists of a parallel XenDesktop site positioned inside a VPC (virtual private cloud) in AWS (Amazon Web Services). Server-based VDI desktops will be hosted from the cloud with the option of providing applications as well. This new site shares domain authentication, licensing and Citrix StoreFront access with an existing on-premise corporate site. Secure connectivity between the AWS site and on-premise site is provided by the Citrix CloudBridge connector running on a pair of NetScaler VPX's. The following detailed steps outline the creation and configuration of the environment below and are intended primarily for demonstrations or proofs-of-concept environments.

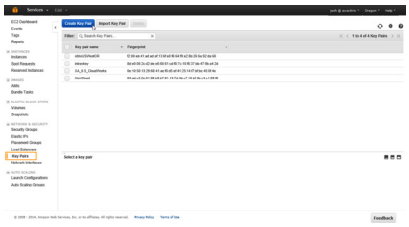


The customer cloud environment – Amazon Web Services

Log into the AWS Management Console.



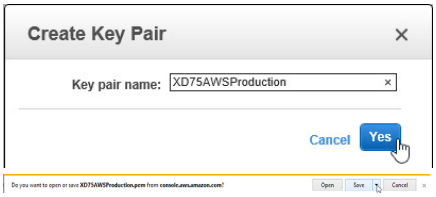
Under EC2, Create Key Pair.



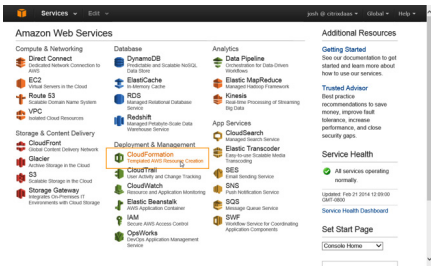
Give the Key Pair a friendly name.

Click Yes.

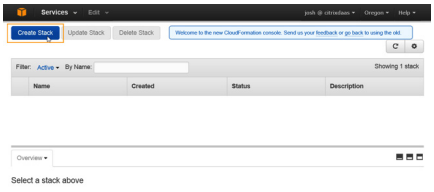
Save private key created in a safe location.



Create Cloud Formation.

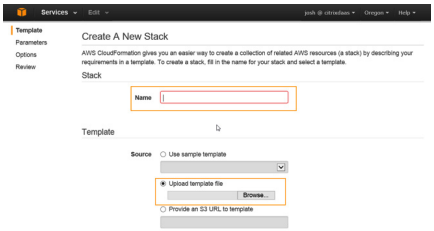


Click Create Stack.



Enter a friendly name for the newly created stack.

Upload the cloud formation template and run the script.



Specify any custom/key parameters specific to the VPC or on-premise environment;

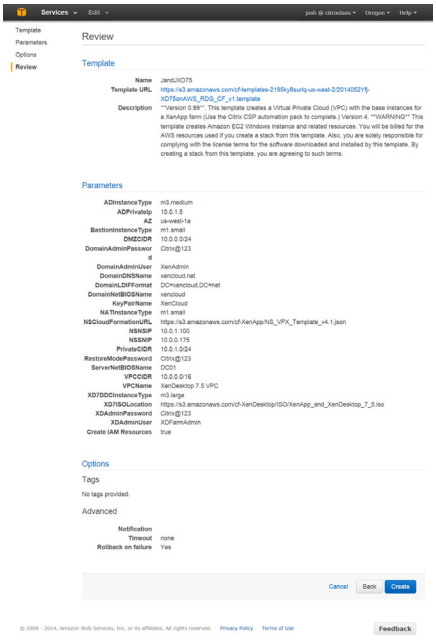
- Availability Zone
- User Access Key
- Key Pair Name
- Secret Access Key
- Custom IP address requirements
- XenDesktop ISO location
- Etc...

Note: Changing the Domain name for the auto-created server instances here is not required as it will be done in a later step when joining the on-premise corporate domain.

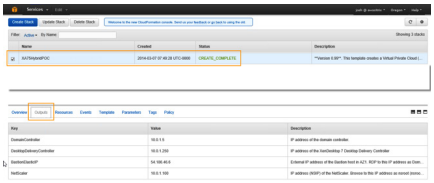
Click Next Step and run the creation script.

Review Template details and Parameters ensuring the accuracy of the Availability Zone, Key Pair names, and any other parameters that were modified from their defaults in the previous step.

Click Create.



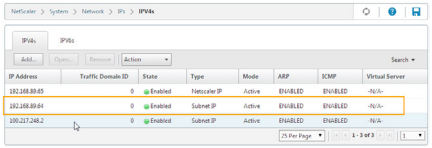
When completed, click the checkbox next to the newly created Stack. Then click on the Outputs tab to display the management IP addresses of the NetScaler and Bastion management server.



Start connecting to the cloud

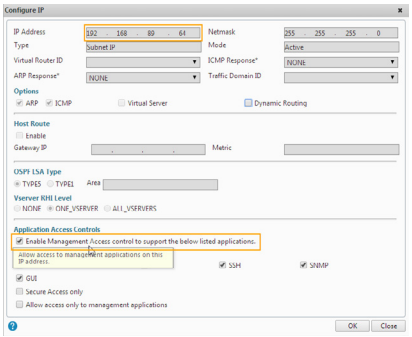
Install and Configure NetScaler VPX On-Premise (if not existing)

Only two nics/SNIPs required; private and public.



Click Enable Management Access when creating both interfaces.

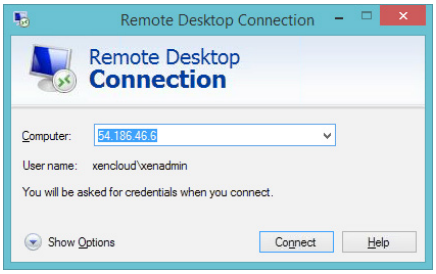
Keep management enabled on both if management from across the tunnel is required.



Create a Remote Desktop Services (RDS) connection to the Bastion management server in Amazon Web Services (AWS) by connecting to the Elastic IP (EIP).

Note: The Bastion management server also is pre-configured for RDS connectivity to the private subnet of the VPC.

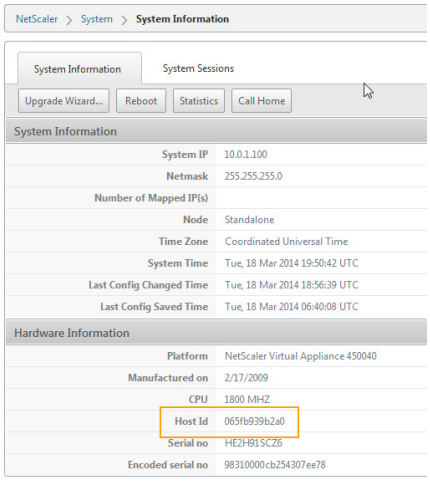
Note: To configure the AWS NetScaler, a second RDS connection must be made from the Bastion management server to the Domain controller in the private subnet in the cloud.



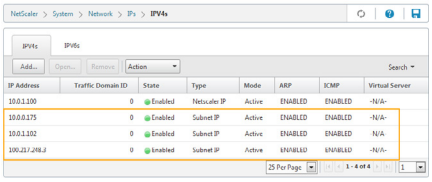
Install a valid license on the AWS NetScaler VPX.

Make note of the NetScaler Host ID which will be used during license activation and allocation on citrix.com.

Refer to the NetScaler Administration Guide in the Resources section for details on NetScaler licensing.

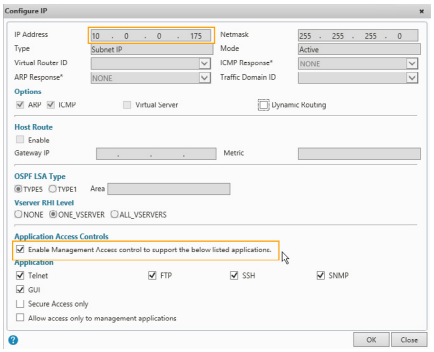


When configuring the AWS NetScaler VPX, three additional SNIPs required. These will correlate and connect to the private subnet, the public subnet and the CloudBridge network. In this example, the 10.0.0.175 IP correlates to the public subnet, the 10.0.1.102 IP to the private, and the 100.217.248.3 to the CloudBridge network.

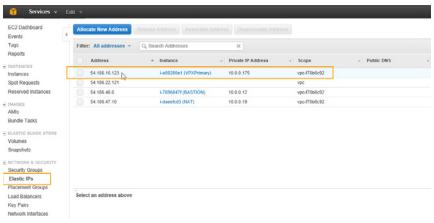


Enable management access on all three SNIPs.

When configuration is complete, management access is only required on the public SNIP for management access from the on-premise environment.



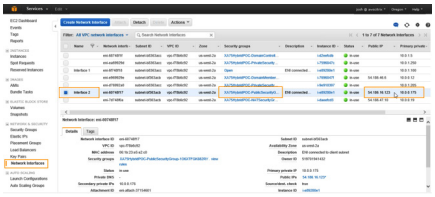
In AWS Management Console, bind the EIP to the Public SNIP of the NetScaler.



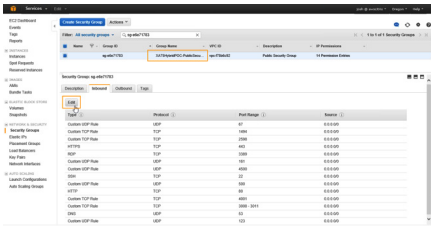
Amazon AWS CloudBridge Connector Pre-Requisites

Verify and configure the following AWS security groups as follows:

- XA75HybridPOC-NATSecurityGroup
- XA75HybridPOCPublicSecurityGroup
- XA75HybridPOCPrivateSecurityGroup



Confirm the inbound and outbound TCP and UDP rules for each security group. See below for specific ports and protocols.



For reference, ensure inbound TCP and UDP port rules for the Public and NAT Security Group match this table.

Note: This port configuration is the minimum requirement. Additional ports may be added as necessary. (i.e. ICMP for testing connectivity)

*These ports are optional for Active Directory LDAP. The only required LDAP is TCP/UDP 389. See Resources section for detailed information on Microsoft Active Directory port requirements.

**These ports are required only for DHCP. If DHCP is not required in the AWS XenDesktop site, they can be excluded.

Protocol	Port(s)	Src/Dest	Protocol	Port(s)	Src/Dest
TCP	22	0.0.0.0/0	TCP	3389	0.0.0.0/0
TCP	25	0.0.0.0/0	TCP	4001	0.0.0.0/0
TCP/UDP	53	0.0.0.0/0	TCP	7279	0.0.0.0/0
TCP	80	0.0.0.0/0	TCP	8008	0.0.0.0/0
TCP/UDP	88	0.0.0.0/0	TCP	8083	0.0.0.0/0
TCP	135	0.0.0.0/0	TCP	27000	0.0.0.0/0
TCP	139	0.0.0.0/0	TCP	3268	0.0.0.0/0
TCP/UDP	389	0.0.0.0/0	UDP**	67	0.0.0.0/0
TCP	445	0.0.0.0/0	UDP	123	0.0.0.0/0
TCP	464	0.0.0.0/0	UDP	138	0.0.0.0/0
TCP*	636	0.0.0.0/0	UDP	161	0.0.0.0/0
TCP	1494	0.0.0.0/0	UDP	500	0.0.0.0/0
TCP	443	0.0.0.0/0	UDP**	2535	0.0.0.0/0
TCP	2598	0.0.0.0/0	UDP	3003	0.0.0.0/0
TCP*	3008-3011	0.0.0.0/0	UDP	4500	0.0.0.0/0
TCP*	3269	0.0.0.0/0			

For reference, ensure inbound TCP and UDP port rules for the Private Security Group match this table.

Note: This port configuration is the minimum requirement. Additional ports may be added as necessary. (i.e. ICMP for testing connectivity)

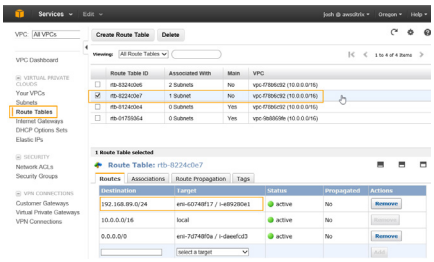
*These ports are optional for Active Directory LDAP. The only required LDAP is TCP/UDP 389. See Resources section for detailed information on Microsoft Active Directory port requirements.

**These ports are required only for DHCP. If DHCP is not required in the AWS XenDesktop site, they can be excluded.

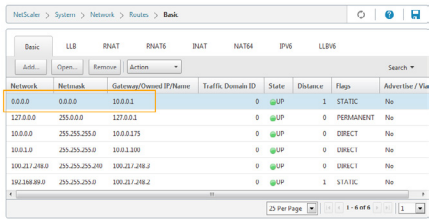
Protocol	Port(s)	Src/Dest	Protocol	Port(s)	Src/Dest
TCP	22	0.0.0.0/0	TCP*	3268	0.0.0.0/0
TCP	25	0.0.0.0/0	TCP*	3269	0.0.0.0/0
TCP/UDP	53	0.0.0.0/0	TCP	3389	0.0.0.0/0
TCP	80	0.0.0.0/0	TCP	4001	0.0.0.0/0
TCP/UDP	88	0.0.0.0/0	TCP	7279	0.0.0.0/0
TCP	135	0.0.0.0/0	TCP	8008	0.0.0.0/0
TCP	139	0.0.0.0/0	TCP	8083	0.0.0.0/0
TCP/UDP	389	0.0.0.0/0	TCP	27000	0.0.0.0/0
TCP	445	0.0.0.0/0	UDP**	67	0.0.0.0/0
TCP	464	0.0.0.0/0	UDP	123	0.0.0.0/0
TCP*	636	0.0.0.0/0	UDP	138	0.0.0.0/0
TCP	443	0.0.0.0/0	UDP	161	0.0.0.0/0
TCP	1494	0.0.0.0/0	UDP**	2535	0.0.0.0/0
TCP	2598	0.0.0.0/0	TCP*	3268	0.0.0.0/0
TCP	3008-3011	0.0.0.0/0	UDP	16500-16509	0.0.0.0/0

Edit the AWS route table for the private subnet as follows:

- Determine the VPC ID; in this example; vpc-f78b6392.
- Determine the route table ID for the private subnet; in this example rtb-8224c0e7.
- Determine the private ENI (Ethernet network interface) for the AWS NetScaler; in this example eni-60748f17.
- Create a new private route direction traffic destined for the private on-premise subnet, to the private ENI of the AWS NetScaler.



Verify that the default route on AWS NetScaler is pointing to the public gateway. In this example, the public gateway is 10.0.0.1.



On-premise CloudBridge connector pre-requisites

Configure on-premise internet router by creating the following routes:

- Inbound port 500 UDP traffic to the private SNIP on the on-premise NetScaler.
- Inbound port 4500 UDP traffic to the private SNIP on the on-premise NetScaler.
- Outbound traffic destined for the cloud bridge network routed to the private SNIP on the on-premise NetScaler.
- Outbound traffic destined for the AWS public subnet routed to the private SNIP on the on-premise NetScaler.
- Outbound traffic destined for the AWS private subnet routed to the private SNIP on the on-premise NetScaler.

Direction	Protocol	Destination	Port	Interface
IN	UDP	NetScaler Private SNIP	500	NA
IN	UDP	NetScaler Private SNIP	4500	NA
OUT	TCP	Cloud Bridge Network	ALL	NetScaler Private SNIP
OUT	TCP	AWS Public Subnet	ALL	NetScaler Private SNIP
OUT	TCP	AWS Private Subnet	ALL	NetScaler Private SNIP

In this example:

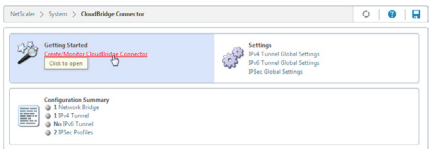
Direction	Protocol	Destination	Port(s)	Interface
IN	UDP	192.168.89.64	500	NA
IN	UDP	192.168.89.64	4500	NA
OUT	TCP	100.217.248.0	ALL	192.168.89.64
OUT	TCP	10.0.0.0	ALL	192.168.89.64
OUT	TCP	10.0.1.0	ALL	192.168.89.64

Install and configure CloudBridge connector

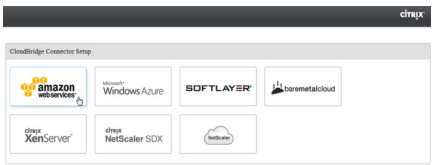
As a final step to enable the extension to the AWS cloud, a secure connection will be created between the on-premise network and the AWS public subnet. This will be accomplished by setting up a CloudBridge Connector between the on-premise and AWS NetScalers using the previously configured bridge network. In this example, the 100.217.248.2 SNIP on-premise and the 100.217.248.3 SNIP in AWS.

Log in to the on-premise NetScaler.

Create CloudBridge Connector.

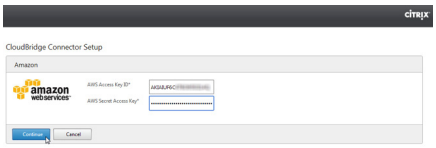


Select Amazon Web Services.



Enter the AWS Access Key ID and Secret Key ID.

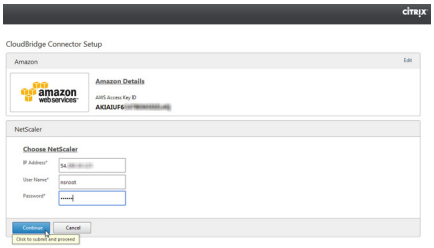
Click Continue.



Enter EIP address of the AWS NetScaler.

Enter NetScaler admin credentials.

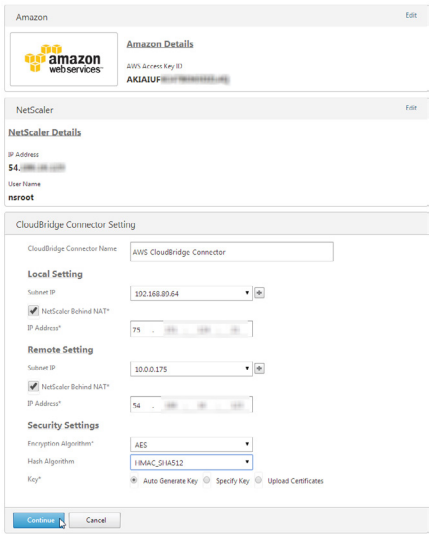
Note: The default NetScaler administrator username and password is nsroot/nsroot. This should be changed to a strong, unique password as soon as possible. Refer to the NetScaler Administration in the References section for details on Admin password changes.



Click Continue.

Verify the Access Key ID and NetScaler IP address.

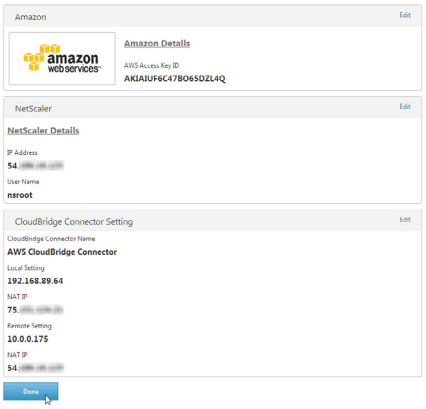
Configure the Connector Settings as follows:



- CloudBridge Connector Name
- Private SNIP of the on-premise NetScaler.
- Check the “NetScaler Behind NAT” checkbox
- Public (NAT or forwarded) SNIP of the on-premise NetScaler.
- Private SNIP of the AWS NetScaler.
- Check the “NetScaler Behind NAT” checkbox.
- Elastic IP that is bound to the public SNIP of the AWS NetScaler.
- Chose the AES Encryption Algorithm.
- Chose the SHA512 Hash Algorithm.
- Chose to Auto Generate Keys.
- Click Continue.

Verify the Connector Name, Local IP settings, Remote IP settings.

Click Done.

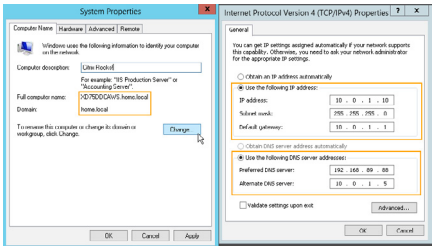


The CloudBridge Connector will now be created and the connector status page will appear. The connector status on the right side should be displayed with a green indicator.

If the status page does not appear, error messages are displayed, or the status indicator is red, see the CloudBridge Connector Admin Guide in the References section for troubleshooting steps.

AWS XenDesktop site pre-requisites

In preparation for the creation of the AWS XenDesktop site, the following steps need to be completed on the Delivery Controller.



- Assign a static IP address to the Delivery Controller within the private AWS subnet.
- Rename the Delivery Controller appropriately for your corporate domain naming convention.
- Configure DNS resolution between the Delivery controller and your corporate DNS infrastructure.
- Add the Delivery Controller to the corporate domain.

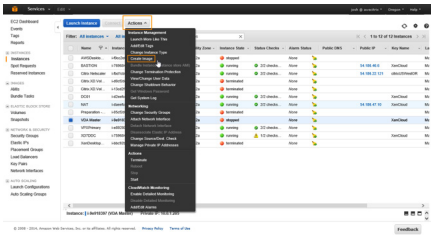
Note: Repeat the above steps for the Windows desktop server gold image (VDA Master) as well.

Creating the desktop server base image

Log into the AWS Management Console.

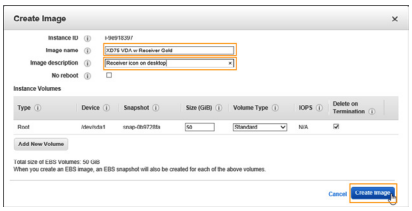
Select the VDA Master instance from the list.

Click the Actions menu and select Create Image.

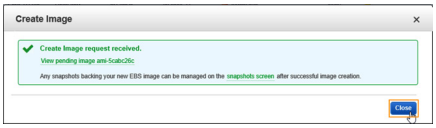


Enter a friendly name and description for this base image.

Click Create Image.

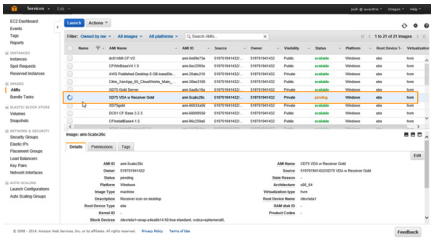


When the Create Image request dialog appears, click Close.



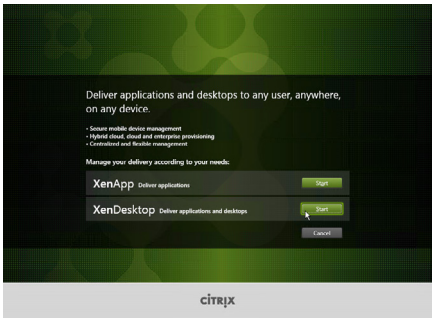
The newly created base image will appear in the AMI list.

Note: The new base image may display a Pending status for several minutes before becoming available. Note the AMI ID.



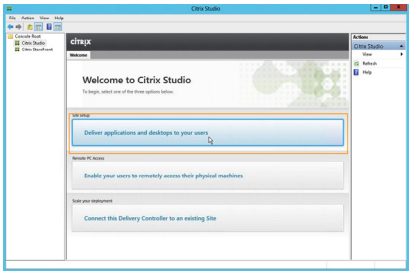
AWS XenDesktop site creation

Install XenDesktop 7.5 on the Delivery Controller server instance.



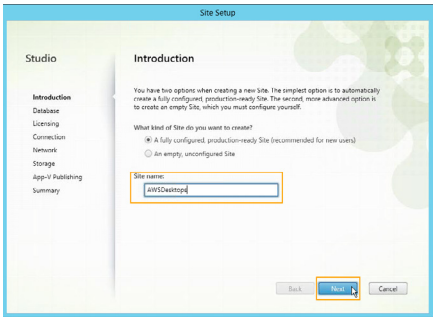
When XenDesktop is full installed on the Delivery Controller, launch Citrix Studio.

On the welcome screen, click the Deliver Applications bar under Site Setup.



Enter the desired AWS XenDesktop site name.

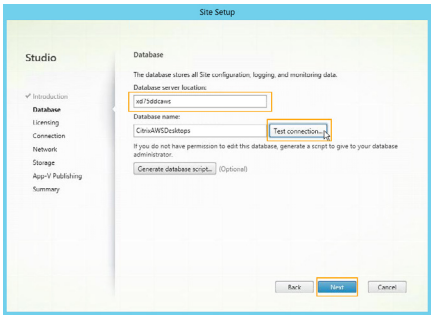
Click Next.



Enter the Delivery Controller's server name as the database server location. If an external SQL server is to be used in AWS, enter that server's name instead.

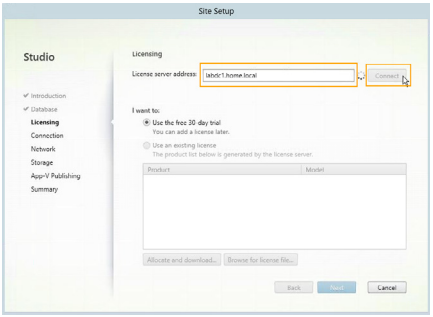
Click Test Connection to ensure proper communications.

Click Next.



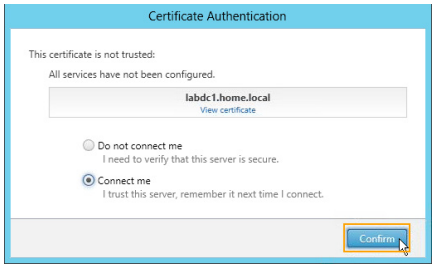
Enter the name of the on-premise Citrix licensing server.

Click Connect.



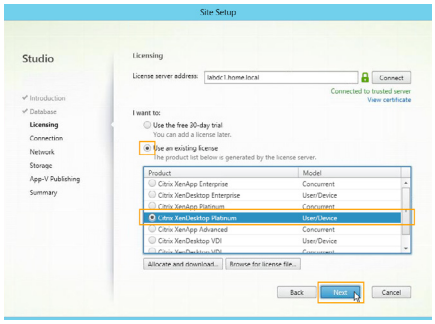
If prompted, select Connect Me to trust the certificate associated with the licensing server.

Click Confirm.



Select Use an Existing License, and chose the appropriate XenDesktop license for this site.

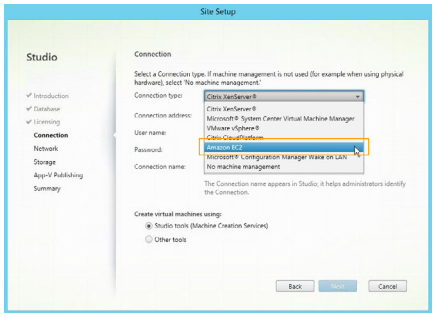
Click Next.



In the Connection Type pull down, select Amazon EC2.

Select to create virtual machines with Machine Creation Services.

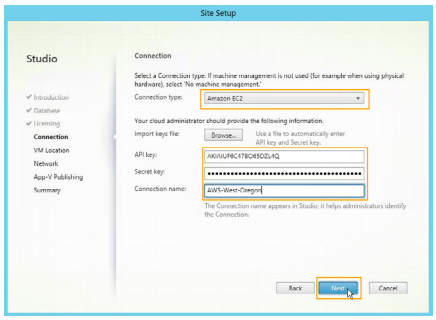
Click Next.



Enter the appropriate API Key (Access Key) and Secret Key.

Enter a name for this EC2 connection.

Click Next.

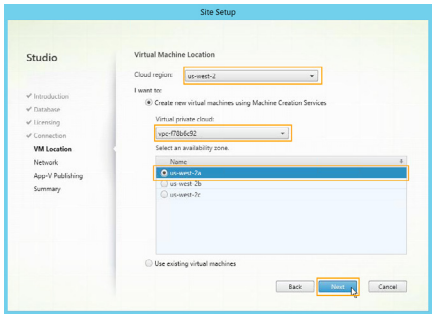


Select the appropriate Cloud Region and VPC.

Note the correct VPC ID.

Select the appropriate Availability Zone.

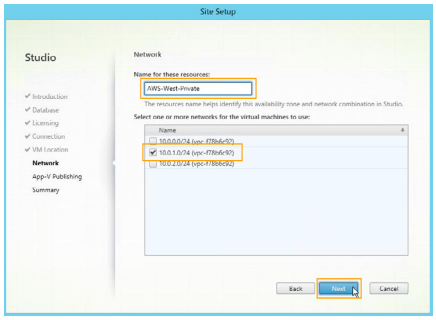
Click Next.



Enter a friendly name for these AWS-based network resources.

Select the AWS private subnet.

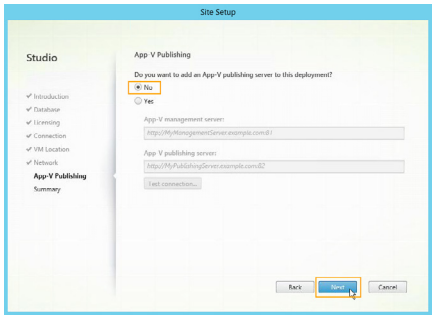
Click Next.



Select No to disable App-V publishing.

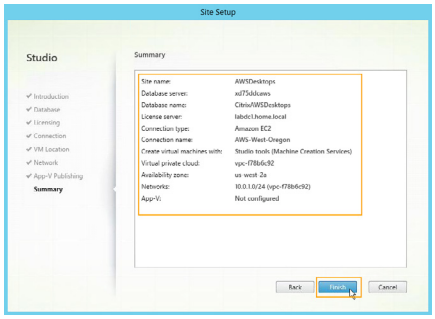
Click Next.

Note: This example does not include the publishing of App-V based applications. However, if App-V delivered applications are to be hosted in the cloud, the on-premise App-V management and publishing server information can be entered during this step.



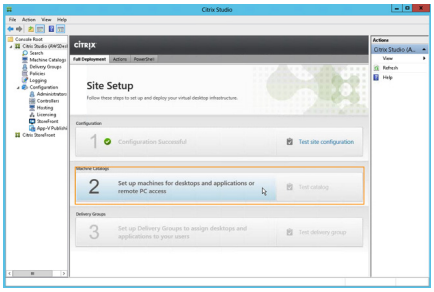
Review Site Summary details and ensuring the accuracy of all parameters.

Click Finish.



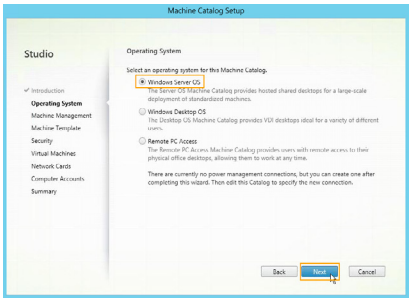
Machine catalog creation

On the welcome screen, click the Set-up Machines for Desktops and Applications bar under Machine Catalogs. Alternatively, right-click on the Machine Catalogs node and selecting Create Machine Catalog.



Select Windows Server OS.

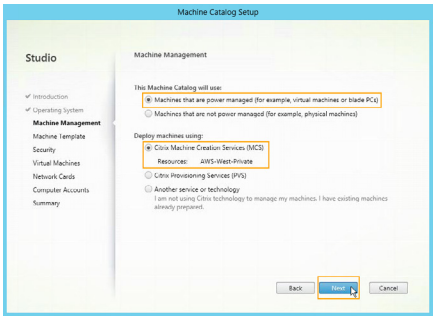
Click Next.



Select Machines that are Power Managed.

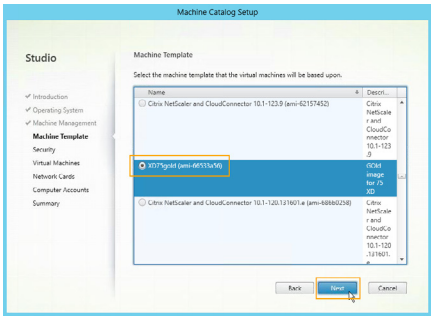
Select Machine Creation Services as the deployment method.

Click Next.



Select the base server image created in the previous section, from the list of machine templates. Note the AMI ID.

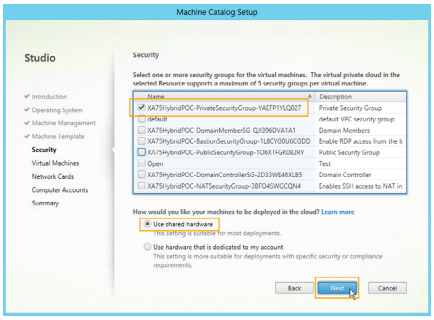
Click Next.



Select the appropriate AWS private security group.

In this example; XA75HybridPOC-PrivateSecurityGroup.

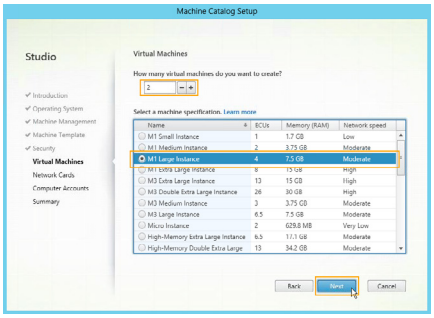
Click Next.



Enter the number of virtual machines to be created.

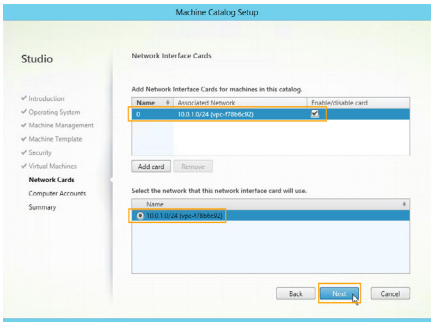
Select the desired virtual machine specification.

Click Next.



Select the network and network interface associated with the AWS private subnet.

Click Next.

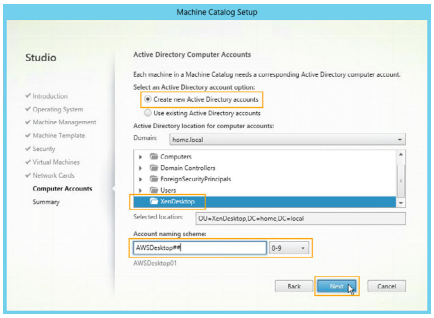


Select Create new Active Directory accounts.

Select an Active Directory OU for the newly created accounts.

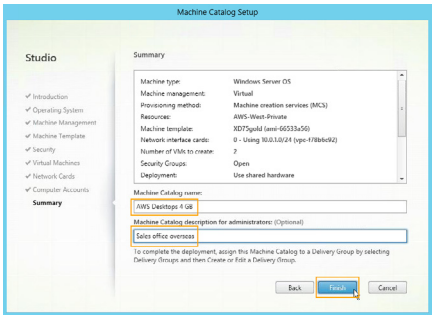
Enter a machine account naming convention.

Click Next.



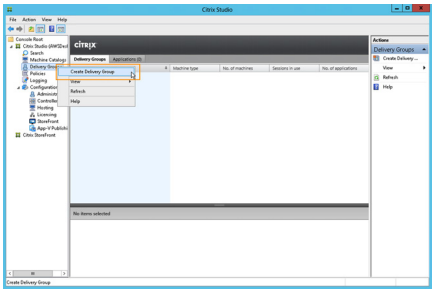
Enter a Machine Catalog friendly name and description.

Click Finish.



Delivery group creation

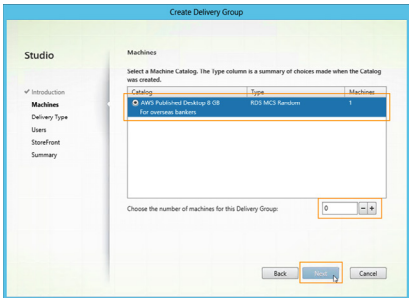
Right click on the Delivery Group node and select Create Delivery Group.



Chose the appropriate Machine Catalog.

Enter the desired number of virtual machines to allocate to this Delivery Group.

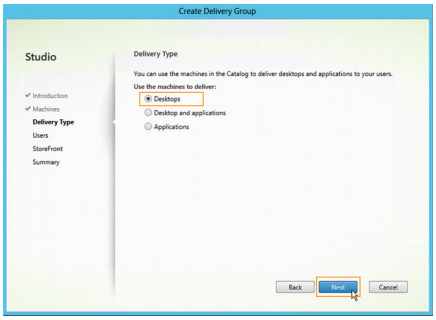
Select Next.



Select Desktops.

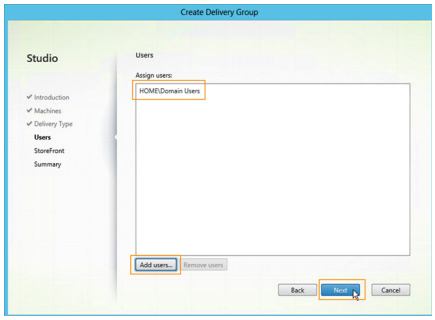
Click Next.

Note: If applications are to be delivered from the AWS site, either Desktop and Applications or Applications can be chosen here. In this example, only Desktops are being delivered.



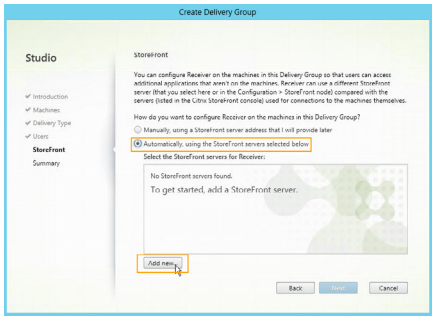
Click Add Users and select the Active Directory group(s) that contain the intended XenDesktop users.

Click Next.



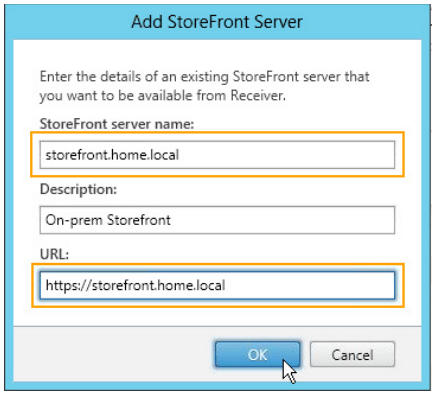
Select to Automatically configure Receiver with a list of StoreFront servers.

Click Add New.



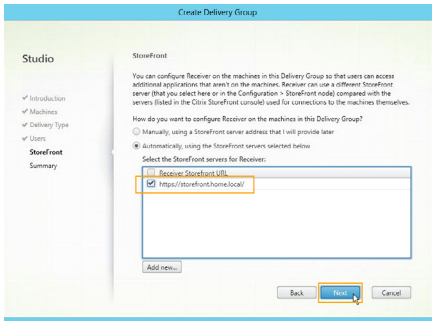
Enter the name and URL of at least one on-premise StoreFront server.

Click Ok.



Click the checkbox next to the newly added StoreFront server(s).

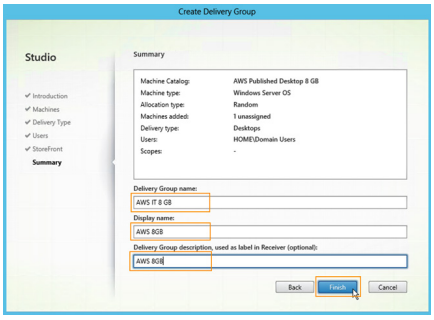
Click Next.



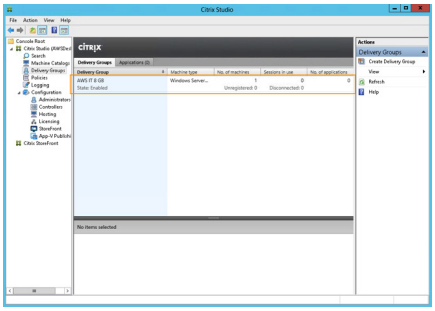
Enter a friendly name and display name for the Delivery Group.

Optionally, enter a description for the Delivery Group.

Click Finish.



Note: It may take several minutes for the newly created Delivery Group machines to register with the site.

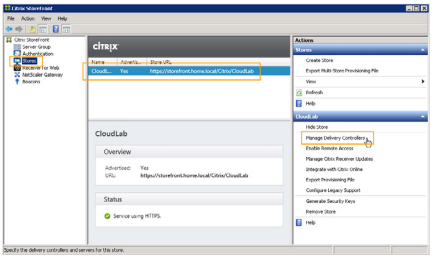


On-premise StoreFront integration

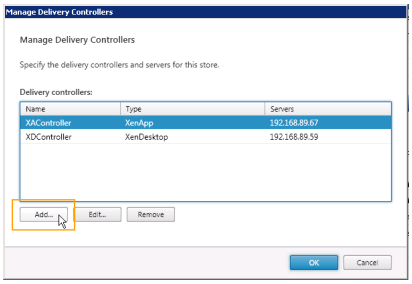
Open the on-premise StoreFront server Admin console.

Select the Stores node, and then click on the desired store URL.

In the right hand pane, select Manage Delivery Controllers.



Click Add.

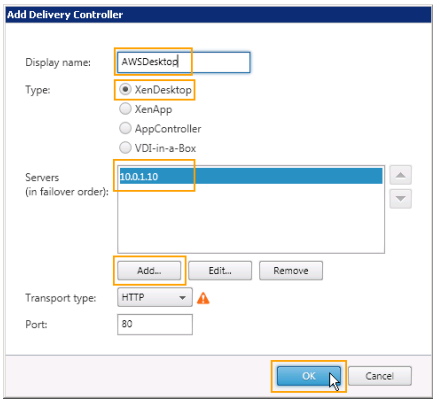


Enter a display name for this Delivery Controller.

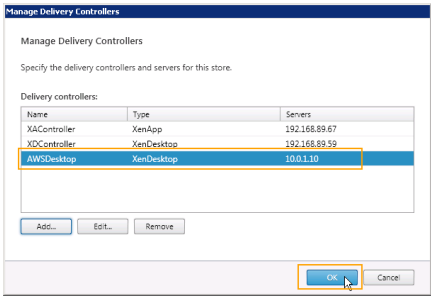
Select XenDesktop as the Delivery Controller type.

Click Add and enter the private IP address of the AWS Delivery Controller.

Click Ok.



Click Ok.



Conclusion

XenDesktop 7.5 and XenApp 7.5 have been redesigned as cloud ready solutions for delivering any Windows application or desktop into a cloud service delivered across any network, to any device. By deploying this expanded app and desktop delivery platform today, you will be positioned to leverage any virtual infrastructure or cloud management platform giving you the ability to take advantage of the automation and orchestration capabilities of cloud computing.

Resources and tools

Citrix related information

The Citrix CloudFormation template download

https://s3.amazonaws.com/cf-XenDesktop/XD75NSonAWS_CF_v1_2.json

XenDesktop 7.5 admin guide

http://support.citrix.com/proddocs/topic/xenapp-xendesktop/cds-xenapp-xendesktop-75-landing.html

Information on ICA bandwidth requirements

http://blogs.citrix.com/2013/08/27/get-up-to-speed-on-xendesktop-bandwidth-requirements

NetScaler VPX admin guide

http://support.citrix.com/proddocs/topic/netscaler-10-1/ns-gen-nsvpx-wrapper-con-10.html

Get Citrix product evaluation licenses

http://www.citrix.com/downloads/trials.html

CloudBridge connector admin guide

http://support.citrix.com/proddocs/topic/ns-system-10-1-map/CBC-wrapper-con.html

CloudBridge admin guide

http://support.citrix.com/proddocs/topic/cloudbridge/cb-wrapper-72-con.html

Citrix StoreFront planning guide

http://support.citrix.com/article/CTX136547

Installing CloudBridge VPX in AWS

http://support.citrix.com/article/CTX136046

Security guidelines for virtual desktops

http://support.citrix.com/article/CTX134780

Amazon AWS related information

Microsoft platform security whitepaper

http://media.amazonwebservices.com/AWS_Microsoft_Platform_Security.pdf

Creating a custom route table in AWS

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html#Add_IGW_Routing

AWS NAT instances

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html#nat-routing-table

3rd party resources

Windows Server 2012 read-only domain controller configuration

http://technet.microsoft.com/en-us/library/jj574152.aspx

Windows Server 2008 read-only domain controller configuration

http://technet.microsoft.com/en-us/library/cc772234.aspx

Active directory and active directory domain services port requirements:

http://technet.microsoft.com/en-us/library/dd772723%28WS.10%29.aspx

Key contributors

Jason Maynard, Senior Systems Engineer Author, Content Contributor, Reviewer

Josh Fleming, Senior Systems Engineer Author, Content Contributor, Reviewer

Peter Bats, Senior Solutions Architect Content Contributor, Reviewer

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix
Citrix (NASDAQ:CTXS) is a leader in virtualization, networking and cloud infrastructure to enable new ways for people to work better. Citrix solutions help IT and service providers to build, manage and secure, virtual and mobile workspaces that seamlessly deliver apps, desktops, data and services to anyone, on any device, over any network or cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive with mobile workstyles. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million people globally. Learn more at www.citrix.com.