

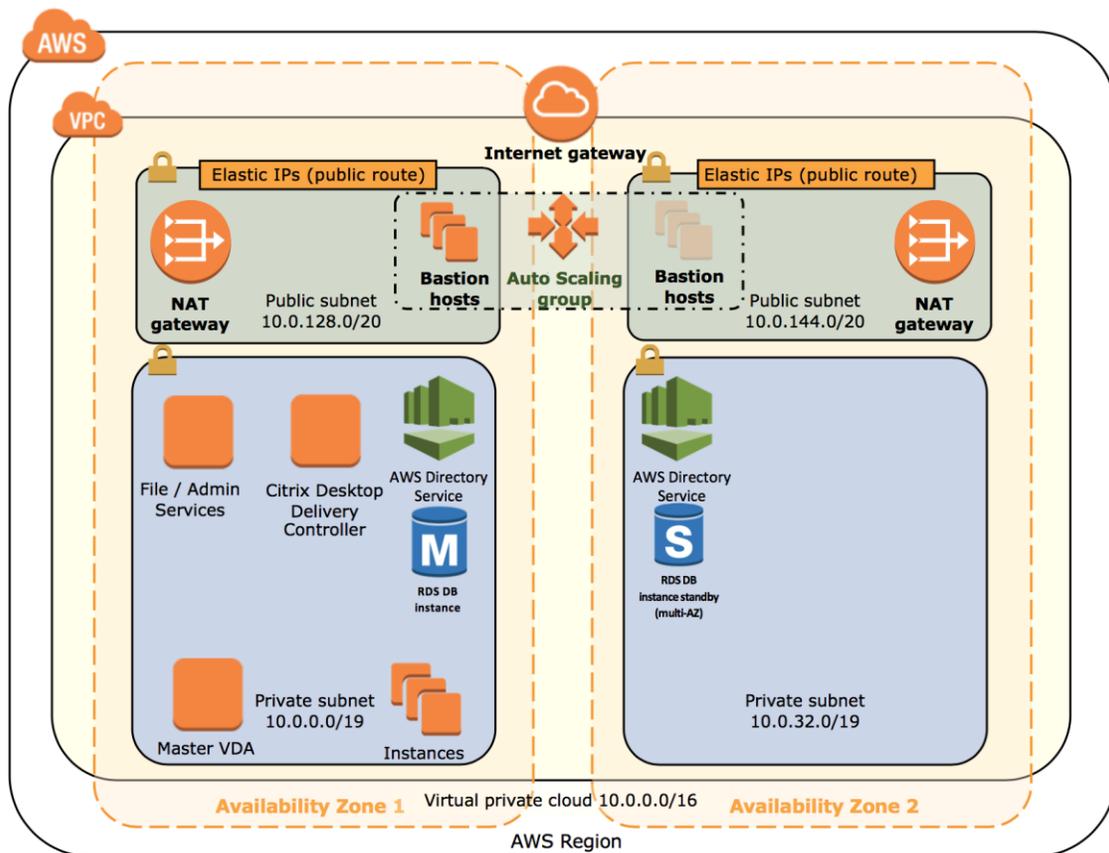
Deploying Citrix Virtual Apps and Desktop with AWS Directory Service and Amazon RDS – Version 1.0

Introduction

This deployment guide covers how to provision and deploy Citrix Virtual Apps and Desktop using AWS Directory Services and Amazon Relational Database Service (Amazon RDS) as a proof of concept (POC). Citrix NetScaler configuration will not be included but can be added later if needed.

For more information on deploying the Citrix NetScaler Access Gateway on AWS check out this [Validated Reference Design NetScaler and Amazon AWS](#). Citrix is an AWS Partner Network (APN) Advanced Technology Partner.

Please be aware that any AWS services used outside of the Free Tier may incur charges. This article uses Citrix XenApp and XenDesktop interchangeably with Citrix Virtual Apps and Desktops. This guide deploys Citrix within a single Availability Zone (AZ) for simplicity. The diagram below shows a multiple-AZ deployment which is suggested for pilot and production environments.



What you'll accomplish

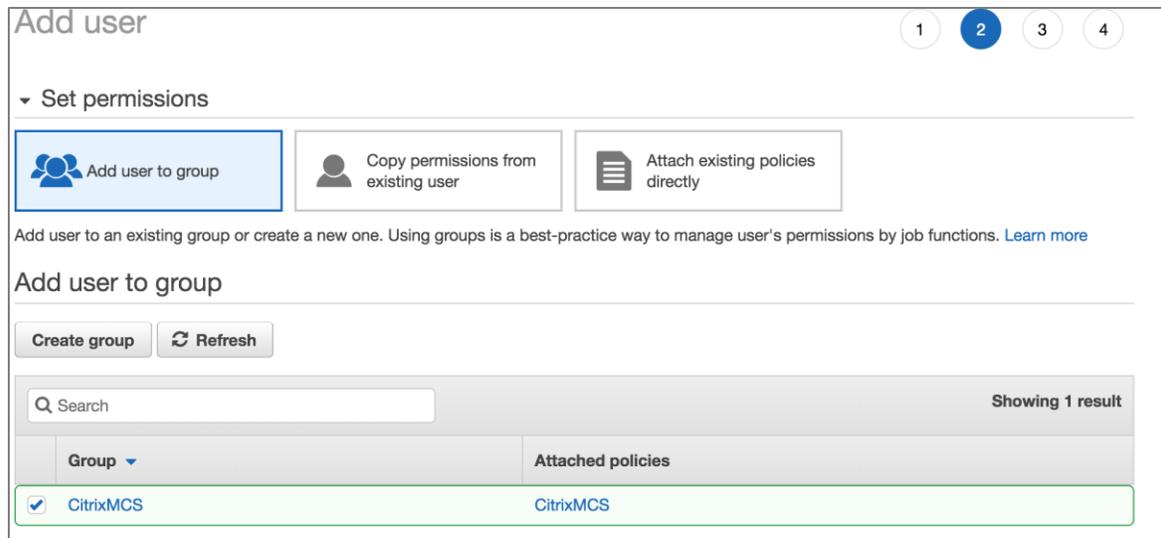
- Deploy an AWS CloudFormation template, which creates the following:
 - A new Amazon Virtual Private Cloud (Amazon VPC) with two public and two private subnet for redundancy and security.
 - Active Directory Service for Microsoft Active Directory to support the Citrix environment.
 - A Remote Gateway instance (bastion) so you can access the environment.
- Deploy Amazon RDS and configure Citrix to use it.
- Deploy and configure the Citrix Virtual Apps and Desktops.

What you need before starting

- An AWS account. You need an AWS account to deploy the services described in this guide. The instructions to sign up for an AWS account can be found [here](#).
- A basic understanding of AWS services is beneficial for this deployment guide, but not required.
- A Citrix.com account with access to Citrix Virtual Apps and Desktops evaluation licensing and media for installation.
- Plan your Security Groups. This deployment guide does not go into detail on how to configure your Security Groups. For more information, check out [Amazon EC2 Security Groups for Windows Instances](#).

Step 1: Prepare your AWS Account

- Log into the AWS Management Console with your AWS account.
- Select a region. All AWS operations will be done within selected region, so please make a note of it.
- IAM service steps:
 - Create a user called CitrixMCS.
 - Only programmatic access is necessary.
 - Create a password. Click Next: Permissions.
 - Click Create Group > Create Policy and follow this article to configure the policy: [How to Define Identity Access Management Permissions Running XenDesktop on AWS](#).



- Click Next: Review.
- Click Create User.

Download and make note of the Access Key ID and Secret Access Key on the next screen:

- Create EC2DomainJoin role:
 - Follow the instructions [here](#) in Section 6e to create an EC2DomainJoin role.
 - If the role doesn't work correctly, you can still deploy instances and join them to the domain manually. Instructions for how to join an instance to a Windows domain can be found [here](#).
- Create Security Groups:
 - Plan and create your Security Groups to fit the needs of your environment.
 - Learn more: [Amazon EC2 Security Groups for Windows Instances](#).

Step 2: Execute the Quick Start

The next step is to execute the Active Directory Domain Services on AWS Quick Start – Scenario 3 found [here](#). Please familiarize yourself with the instructions.

First, follow step 1 [outlined here](#) to create a Key Pair and increase service limits.

We will be launching Scenario 3 into a new VPC. Launch the Quick Start [here](#). Follow the steps below to configure and launch the Quick Start:

- Confirm you are in the correct region of the AWS Console, and click Next.
- Enter the following values. Leave default values for other fields.
 - Stack Name: CitrixPOC-AD-RDS-QS, or your own unique name.
 - Availability Zones: click the field twice to add only two AZs. Any two AZs are acceptable. Make note of the availability zones you chose.

- Allowed Remote Desktop Gateway External Access CIDR: 0.0.0.0/0, or provide the public IP of the device you'd like to connect with to the RDGW. This will be used as a bastion host for the environment.
- Key Pair Name: select the Key Pair you created earlier.
- Domain DNS Name: use the default of example.com.
- Domain NetBIOS Name: use the default of example.
- Domain Admin Password: create a password and make note of it.
- Click Next.
- In the following window, review and click Next again.
- Click the checkbox acknowledging AWS CloudFormation might create resources with custom names.
- Click Create.

The Quick Start will take at least 30 minutes to complete. Do not proceed with the deployment until the Quick Start is complete.

CloudFormation > Stacks > Create Stack

Create stack

- Select Template
- Specify Details**
- Options
- Review

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more.](#)

Stack name:

Parameters

Network Configuration

Availability Zones:
List of Availability Zones to use for the subnets in the VPC. Note: The logical order is preserved and only 2 AZs are used for this deployment.

VPC CIDR: CIDR Block for the VPC

Private Subnet 1 CIDR: CIDR block for private subnet 1 located in Availability Zone 1.

Private Subnet 2 CIDR: CIDR block for private subnet 2 located in Availability Zone 2.

Public Subnet 1 CIDR: CIDR Block for the public DMZ subnet 1 located in Availability Zone 1

Public Subnet 2 CIDR: CIDR Block for the public DMZ subnet 2 located in Availability Zone 2

Allowed Remote Desktop Gateway External Access CIDR: Allowed CIDR Block for external access to the Remote Desktop Gateways

Amazon EC2 Configuration

Key Pair Name: Public/private key pairs allow you to securely connect to your instance after it launches.

Remote Desktop Gateway Instance Type: Amazon EC2 instance type for the Remote Desktop Gateway instances

Microsoft Active Directory Configuration

Domain DNS Name: Fully qualified domain name (FQDN) of the forest root domain e.g. example.com

Domain NetBIOS Name: NetBIOS name of the domain (up to 15 characters) for users of earlier versions of Windows e.g. EXAMPLE

Microsoft Active Directory Configuration

Domain DNS Name: Fully qualified domain name (FQDN) of the forest root domain e.g. example.com

Domain NetBIOS Name: NetBIOS name of the domain (up to 15 characters) for users of earlier versions of Windows e.g. EXAMPLE

Domain Admin Password: Password for the domain admin user. Must be at least 8 characters containing letters, numbers and symbols

Microsoft Remote Desktop Gateway Configuration

Number of RDGW hosts: Enter the number of Remote Desktop Gateway hosts to create

AWS Quick Start Configuration

Quick Start S3 Bucket Name: S3 bucket name for the Quick Start assets. Quick Start bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).

Quick Start S3 Key Prefix: S3 key prefix for the Quick Start assets. Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).

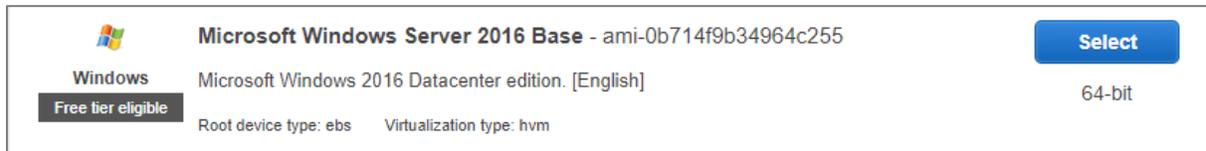
Step 3: Launch the Amazon EC2 resources

In this section, we will launch four identical Amazon EC2 instances. We will rename them and configure them after deployment for the roles they play in this guide:

- DDC01 – Desktop Delivery Controller and other components.

- FileAdmin01 – a file share for the software installers, and admin use of Active Directory Tools, and Microsoft SQL Studio Management Tools.
- TestVDA01 – used to test the VDA.
- GoldVDA01 – used to create a gold image in the Machine Catalog.

In the AWS Management Console, navigate to the Amazon EC2 service and click Launch Instance. Select Microsoft Windows Server 2016 Base and then select the M4 Large type.



- Click Next: Configure Instance Details.
- Set Number of Instances to 4.
- Click the Network pop-up menu and select the VPC created by the Quick Start.
- Click the Subnet pop-up and select the Private Subnet 1A.
- Click the Domain join directory pop-up and select the example.com domain.
- Click the IAM Role pop-up and select EC2 Domain Join you created.
- Click Next: Add Storage.
- Click Next: Add Tags.
- Click Next: Configure Security Group.
- Click Review and Launch.
- Click Launch.
- Select the key pair you created earlier and launch the instances.

Return to the Instances view in the AWS Console. In the Name column, edit the names of the four instance we just launched to match the list below:

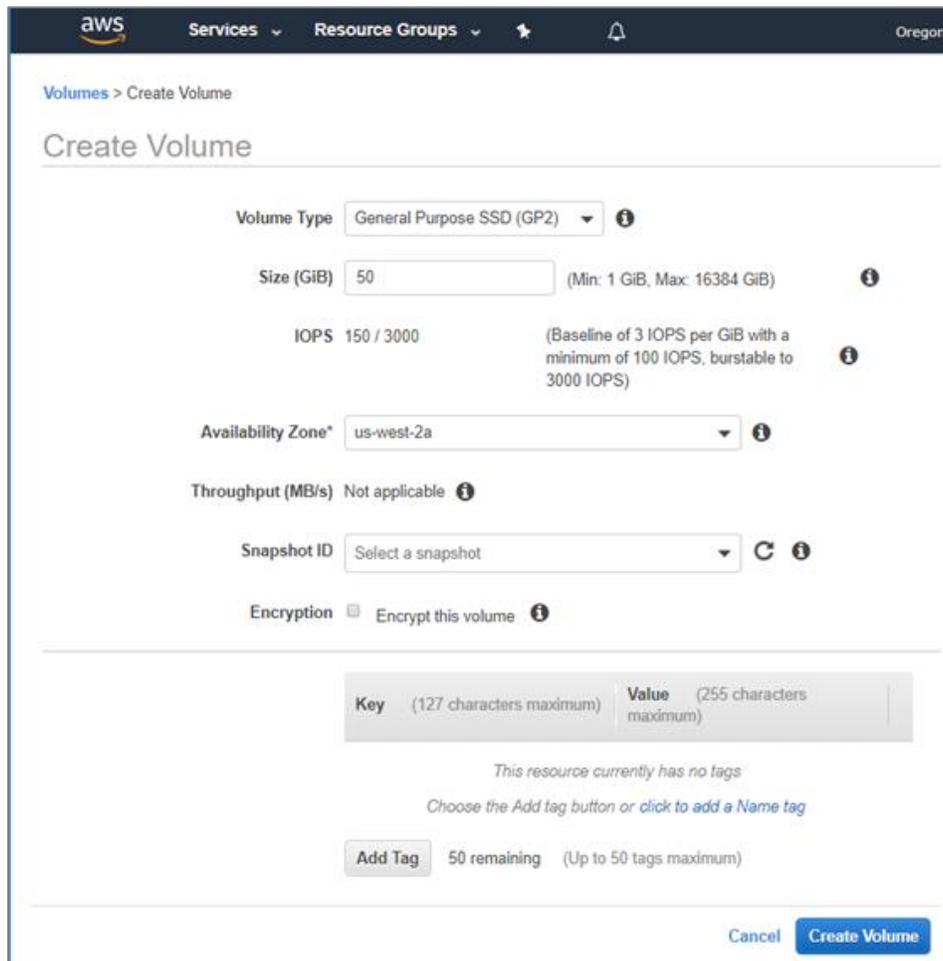
- DDC01
- FileAdmin01
- TestVDA01
- GoldVDA01

Step 4: Add a 50 GB volume to FileAdmin01:

This will be used for software installers and other files needed for this installation:

- Go to the EC2 Instances Dashboard in the AWS Console and select Volumes. Make sure you are in the correct region.
- Select Create Volume.

- Set Volume Type to General Purpose SSD (GP2).
- Set the size to 50 GB.
- Set the Availability Zone to the AZ for Private Subnet 1A or where the instances were launched.
- Click Create Volume.

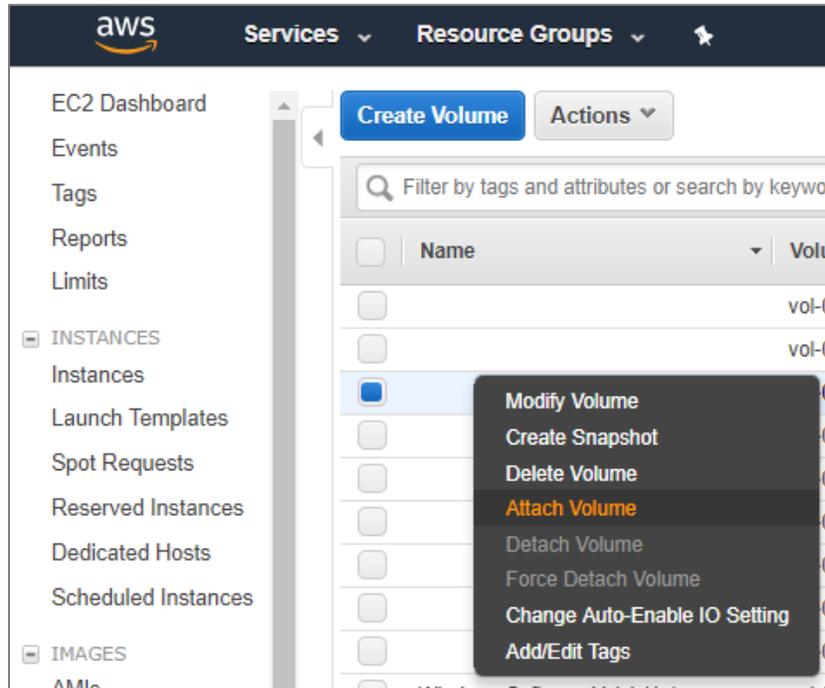


The screenshot shows the 'Create Volume' page in the AWS console. The configuration is as follows:

- Volume Type:** General Purpose SSD (GP2)
- Size (GiB):** 50 (Min: 1 GiB, Max: 16384 GiB)
- IOPS:** 150 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)
- Availability Zone:** us-west-2a
- Throughput (MB/s):** Not applicable
- Snapshot ID:** Select a snapshot
- Encryption:** Encrypt this volume

At the bottom, there is a section for tags with an 'Add Tag' button and a 'Create Volume' button.

- Return to the Volumes page in the AWS Console.
- Right-click the new volume and select Attach Volume.



- Click the Instance field and select FileAdmin01.
- Click Attach.



Step 5: Configure the EC2 instances and connect using Remote Desktop

In this section, we will decrypt the Administrator password for the Gateway instance called RGDW and the four Amazon EC2 instances we launched earlier. We will connect to each instance with Windows Remote Desktop. The gateway instance is created by the Quick Start and has a public IP address.

The four instances we launched do not have public IP addresses. We will connect to the RDGW over the internet and then use Windows Remote Desktop on the RDGW instance to connect to the four instances.

It's important to note each instance has a local Administrator account (`{Instance NetBIOSname\Administrator}`) and a Domain Admin account (`{example.com\admin}`). The password for the local Administrator account is decrypted with the Amazon EC2 Key Pair you used in the Quick Start and when you launched the four instances. The domain admin account is an Active Directory Domain admin used for all Citrix, Microsoft SQL, and Active Directory operations. In Production, you would use separate domain accounts for each service.

The domain admin account uses the password you supplied for the Domain Admin Password parameter in the Quick Start. You will enter "example.com\admin" in the user name field of Remote Desktop whenever you use this account.

Step 5A: Decrypt the local Administrator Passwords

Follow the instructions [here](#) to decrypt the password for the RDGW instance. Make a note of the password.

Follow the same instructions [here](#) to connect to the RDGW. Once connected to the RDGW instance then connect to each of the instances within the private subnet using MSTSC.

If your instances were launched with "domain join" configured, login using the domain administrator account. If not, follow the instructions above to decrypt the local administrator password, login, and join to the domain.

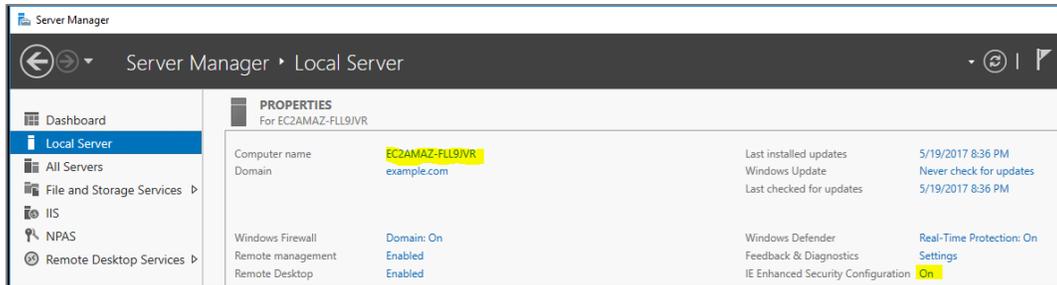
Step 5B: Configure the Amazon EC2 Instances

Execute the steps below on the instances you just created before proceeding with Step 5 in the deployment guide. You may change the name of the RDGW instance if you'd like, but do not add it to the domain. Connect to each of these instances using Remote Desktop using the domain admin account:

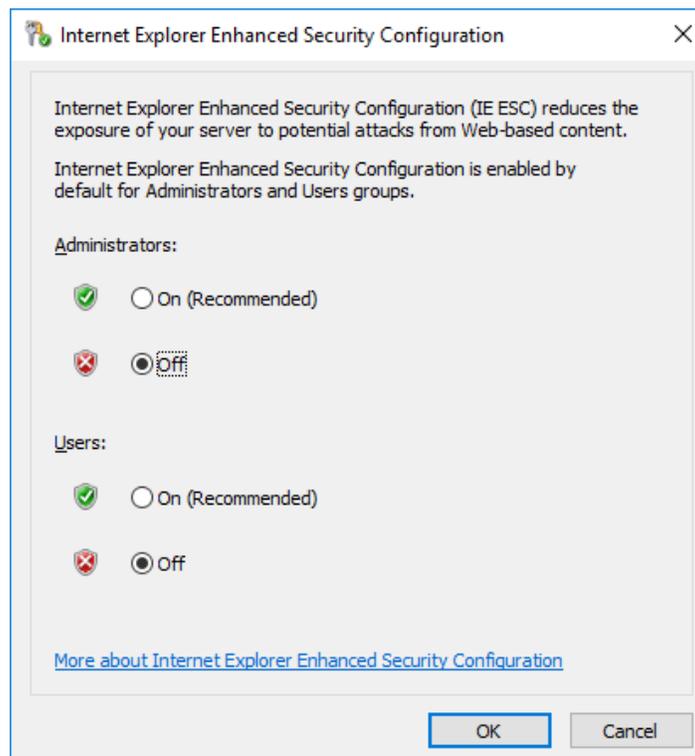
- DDC01 – Desktop Delivery Controller and other components.
- FileAdmin01 – a file share for the software installers, and admin use of Active Directory Tools, and Microsoft SQL Studio Management Tools.
- TestVDA01 – used to test the VDA.
- GoldVDA01 – used to create a gold image in the Machine Catalog.

Follow these steps for each instance separately:

- Open Server Manager.
- Select Local Server from the left navigation window.



- Click the word On next to IE Enhanced Security Configuration.
- In the next window click Off twice and click OK.



- Click the Computer Name.
- Click Change.
- Change the Computer Name on each instance to match the Name Field in the AWS Management console.
- Click OK.
- Click Close in the System Properties window and you will be prompted to reboot. Reboot the instance.

Step 6: Format the 50 GB volume on FileAdmin01 and share it to the domain

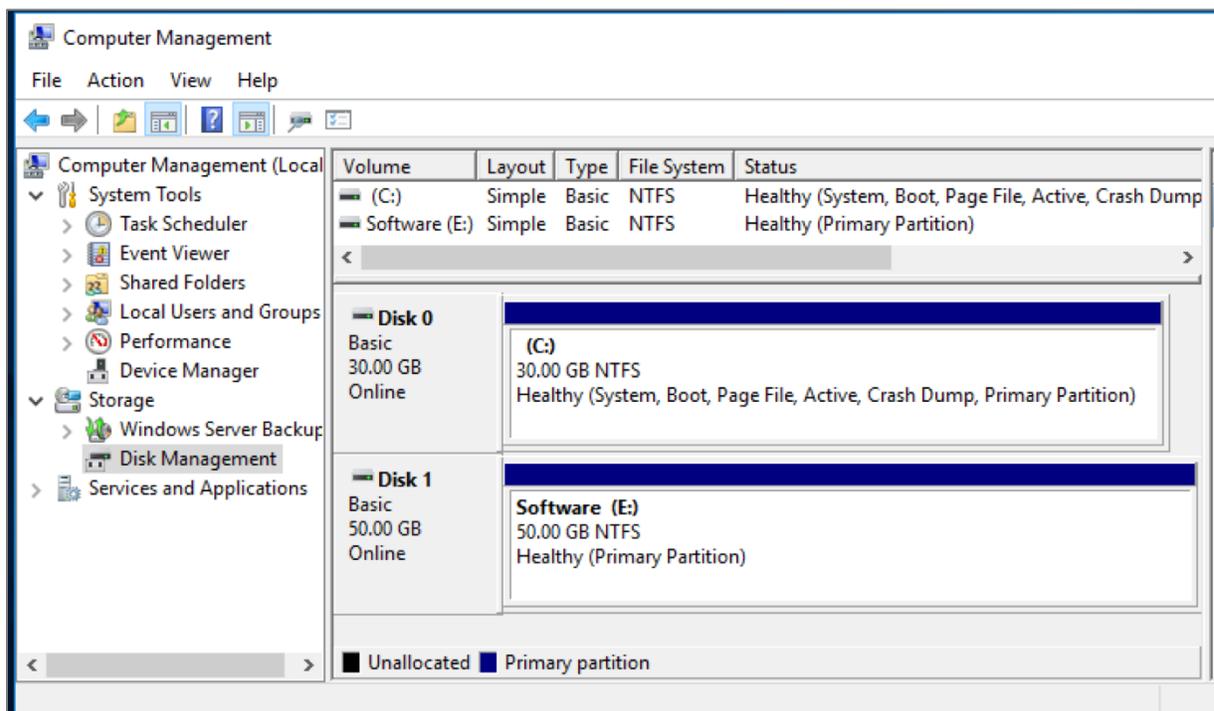
In this section, we will format the 50 GB volume on FileAdmin01 that is needed for the software installers mount it as a E:\ drive and share it.

Connect to the FileAdmin01 as domain Administrator from the RDGW instance. Open Computer Management then expand Storage:

- Select Disk Management.
- Right Click the offline disk and select Bring Online.
- In the next warning dialog box, click OK.
- Right-click the disk again and select Initialize.

Follow steps to create a New Volume:

- Leave the default disk sizes.
Configure the drive letter as E: Click Next. If you mount the disk on a different drive letter, please make note of it.
- Leave the NTFS default values and click Next.
- Click Create.



- Open a File Explorer.
- The E:\ drive should now be visible.
- Create a folder on the E:\ drive called Software.
- Right-click on the Software directory.
- In the context menu click Share, select Specific People.
- Type Everyone in the box and click Add.
- Click Share.

Test the share from another instance (not the RDGW) and type \\FileAdmin01.example.com in a Windows File Explorer.

Step 7: Download and install items onto the FileAdmin01 Instance.

In this section, we will download and install items onto the FileAdmin01 Instance:

- Connect to FileAdmin01 as Domain Administrator using RDP.
- Install the Active Directory Administration Tools by following this [guide](#).
- Download SQL Server Management Studio [here](#) and save it to the E:\Software folder.
- Follow the instructions on the download page to install Management Studio on the FileAdmin01.
- Install the SQL Server PowerShell module. Follow the instructions [here](#) to install the module.
 - Open PowerShell as in administrator “run as administrator.”
 - Type Install-Module -Name SqlServer.
- In a browser, go to the Citrix Downloads page [here](#) and download the Xenapp 7.18 / XenDesktop 7.18 installer to the E:\Software directory. You may need to create a free account to download it.
- Create a folder called XAXD_7_18 within the Software directory.
- Once downloaded, mount .iso and copy contents into e:\software\XAXD_7_18\.

Step 8: Configure Group Policy Objects for Drive Mapping

This will help ease the installation of the software being installed.

Follow the steps outlined in this Microsoft Blog article: [Using Group Policy Preferences to Map Drives Based on Group Membership](#).

Moving forward in this guide, I will refer to the [\\fileadmin01\Software](#) location as the “Mapped Drive” shown in screenshots as Z:\.

Step 9: Create Domain Users

Depending on your success criteria of your POC, you will need a set of users accounts for testers to access the environment.

[Follow these steps](#) to learn more about the user account permissions needed for RDS.

Open Active Directory Users and Computers within the FileAdmin01 instance:

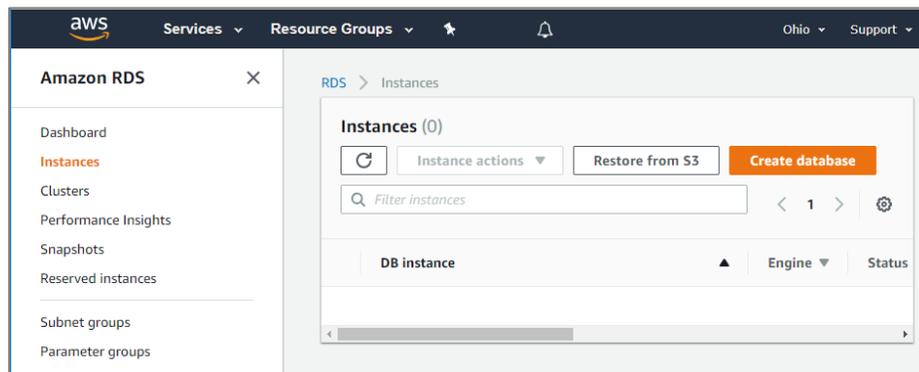
- Create additional Domain admin accounts.

- Create additional Test user accounts

Step 10: Install the database

In this section, we will install the Amazon RDS for Microsoft SQL Database:

- Log into the AWS Management Console and select Amazon RDS.
- Select Instances from the left navigation window.
- Click Create Database.



- Select Microsoft SQL Server.
- Select SQL Server Standard Edition and click Next.
- Select Production and click Next.
- Select either Yes or No for multi-AZ deployments depending on your requirements.
- Change the DB Instance class to db.r4.large. Use the Citrix Database Sizing tool [here](#) for guidance.
- Review the Estimated Monthly Costs box to make sure you are aware of the costs associated with deploying Amazon RDS.

Settings

DB instance identifier [Info](#)
Specify a name that is unique for all DB instances owned by your AWS account in the current region.

DB instance identifier is case insensitive, but stored as all lower-case, as in "mydbinstance". Must contain from 1 to 63 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Cannot end with a hyphen or contain two consecutive hyphens.

Master username [Info](#)
Specify an alphanumeric string that defines the login ID for the master user.

Master Username must start with a letter. Must contain 1 to 64 alphanumeric characters.

Master password [Info](#) **Confirm password** [Info](#)

Master Password must be at least eight characters long, as in "mypassword". Can be any printable ASCII character except "/", "", or "@".

- For DB Instance Identifier, enter CitrixOnAWS.
- Create a Master username of “dbadmin” and enter a password, and then click Next.

Network & Security

Virtual Private Cloud (VPC) [Info](#)
VPC defines the virtual networking environment for this DB instance.

Only VPCs with a corresponding DB subnet group are listed.

Subnet group [Info](#)
DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

Public accessibility [Info](#)

Yes
EC2 instances and devices outside of the VPC hosting the DB instance will connect to the DB instances. You must also select one or more VPC security groups that specify which EC2 instances and devices can connect to the DB instance.

No
DB instance will not have a public IP address assigned. No EC2 instance or devices outside of the VPC will be able to connect.

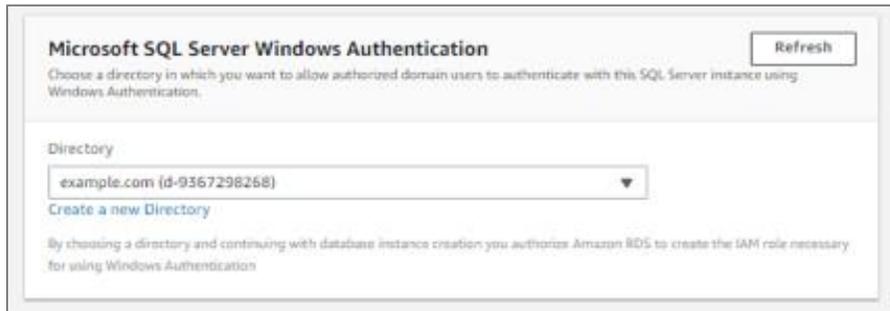
Availability zone [Info](#)

VPC security groups
Security groups have rules authorizing connections from all the EC2 instances and devices that need to access the DB instance.

Create new VPC security group

Choose existing VPC security groups

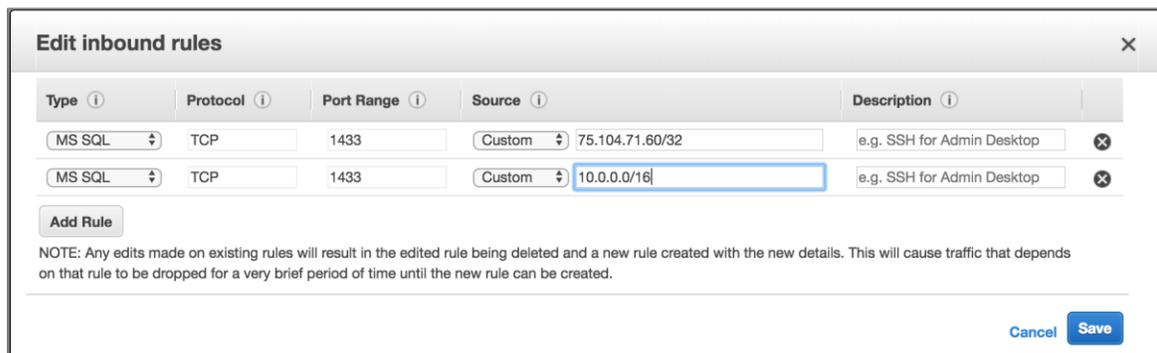
- Select the VPC deployed by the Quick Start.
- Select Create new DB Subnet Group.
- Set Public Accessibility to No.
- Select the AZ where DDC01 is deployed.
- Select Configure as needed for Security Groups or select the default.



- For Microsoft SQL Server Windows Authentication, select the domain we created with the Quick Start (example.com).
- You can leave the rest of the options in this wizard as default.
- Scroll to the bottom of the page and Click Create Database.
- This will take some time.
- When the database has been created, make a note of the FQDN for the endpoint. You can find it in the Connect section of the database instance information window.

Open the AWS Management Console and select VPC > Security Groups:

- Select the Security Group created by the RDS Launch Wizard.
- Select the Inbound rules tab.
- Click Edit.

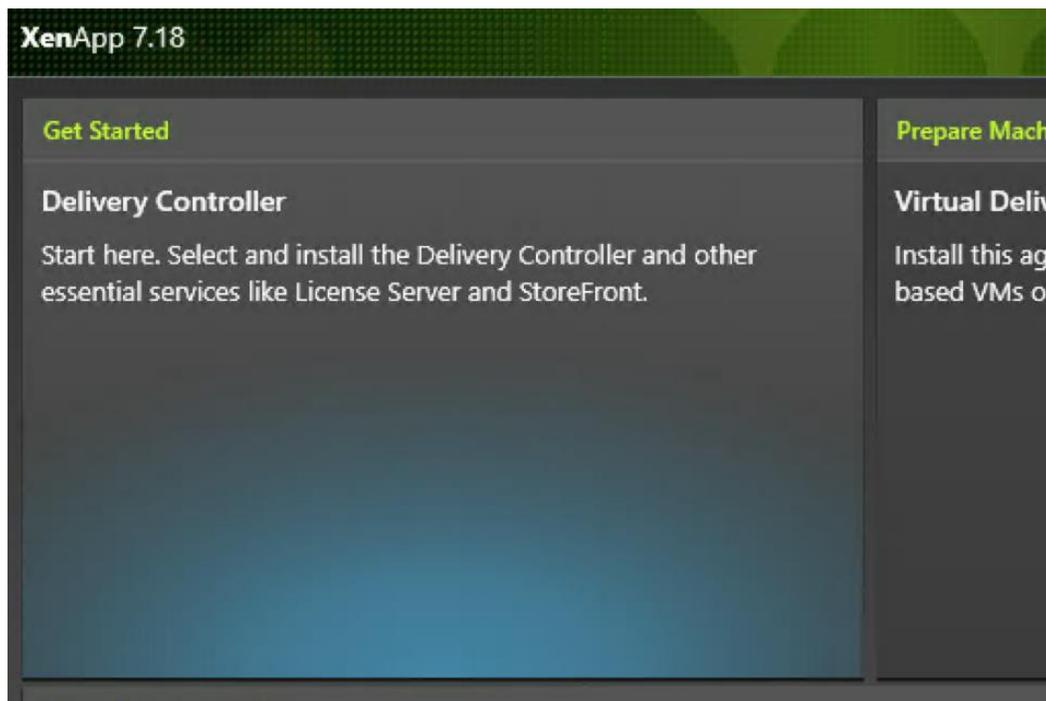


- Depending on your security requirements, configure so the DDC01 & FileAdmin01 instances have access.
- Click Save.

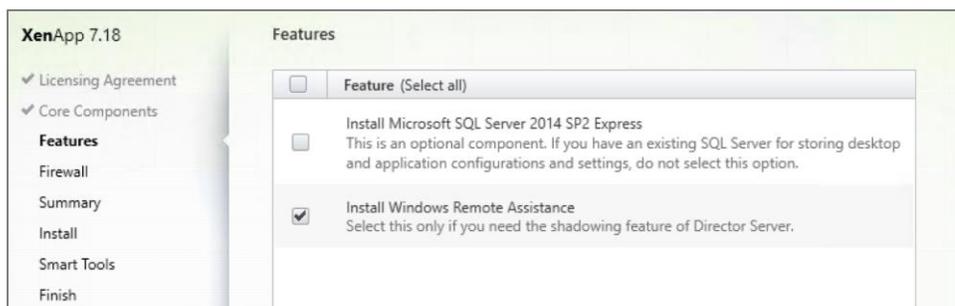
Step 11: Create a Desktop Delivery Controller

In this section, you will install the Citrix Desktop Delivery Controller:

- Connect to DDC01 as the Domain Admin (example.com\admin) via the RDGW instance using Remote Desktop.
- Open Windows File Explorer and go to the mapped drive location Z:\software\XAXD_7_18
- Execute Autoselect.exe
- Click Start for XenApp.

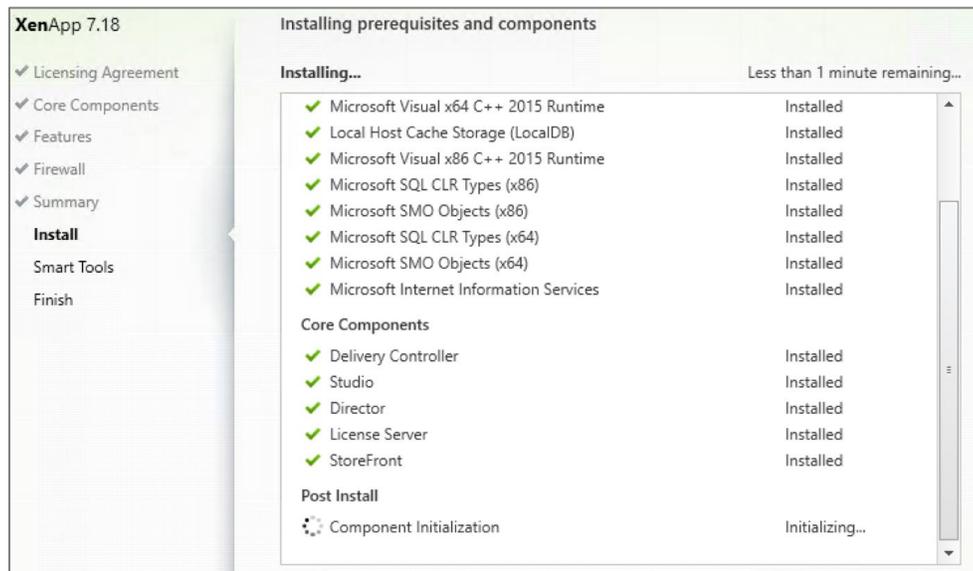


- Click the upper left hand pane that says Delivery Controller.
- Accept terms and click Next.
- Accept all default values Except in Features.

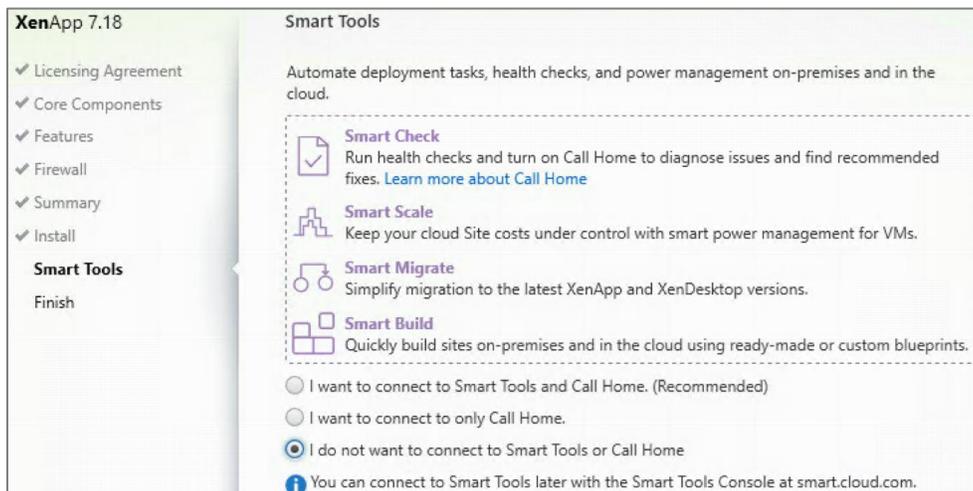


- Uncheck "Install Microsoft SQL Server 2014 SP2 Express."

- Click Next until you see the Install button.
- Click Install. This will take some time to complete.



- The installer will stop at a prompt to use Smart Tools and Call Home. Select “I do not want to use Smart Tools” and click OK.



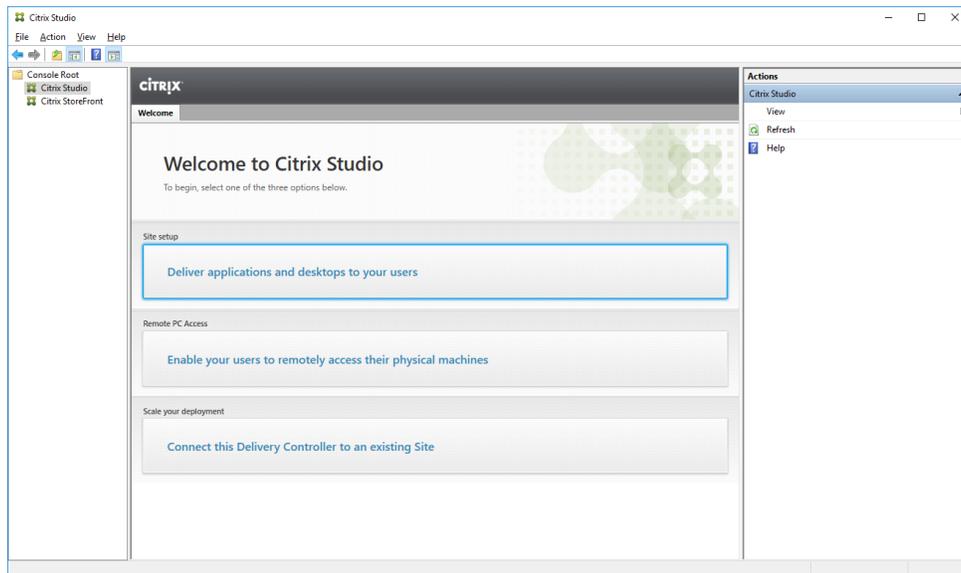
- Check Launch Studio on the next screen and click Finish.

Step 12: Citrix Site setup

In this section, we will setup our Citrix Site.

Step 12A: Generate Scripts

- Connect to DDC01 as Domain Administrator.
- In the Citrix Studio window, select “Deliver applications and desktops to your users.”

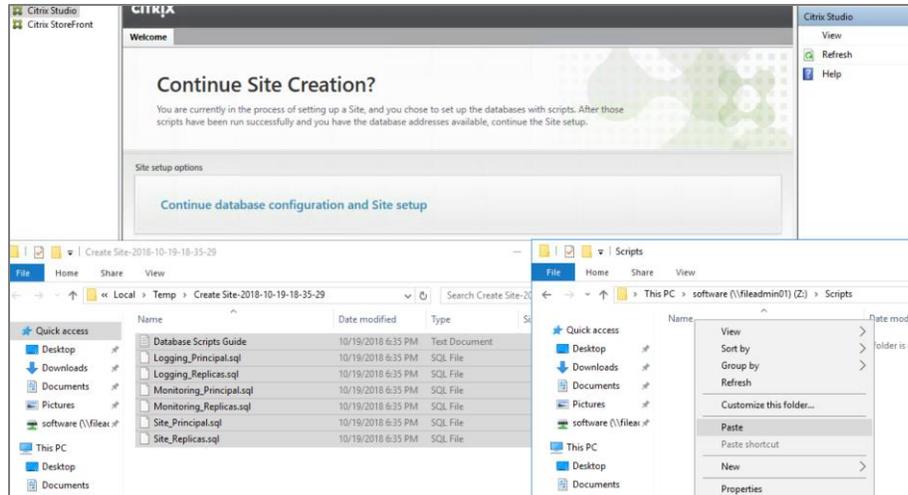


- Check the option for a fully configured site and name the Site MyPOC. Click Next.

Since Amazon RDS doesn't support the “dbcreator” role, you will need to have the Desktop Delivery Controller generate scripts and “hand scripts to Database Administrator.” You will be acting as a Database Administrator to complete this guide.

For more information on this requirement check out this document for [Amazon RDS permissions](#).

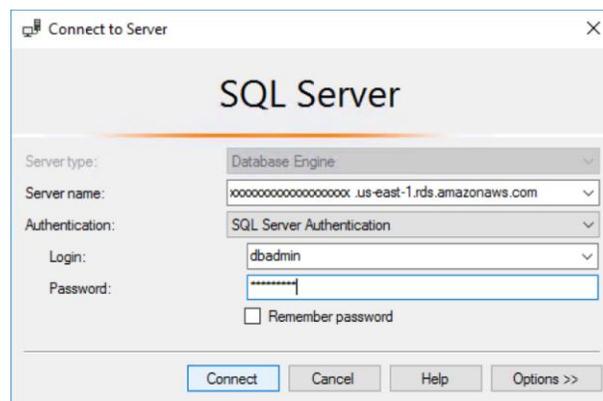
- Select the “Generate scripts to manually set up databases on the database server” option and click Next.
- Click Generate Scripts.
- Make note of the three database names—CitrixMyPOCSite, CitrixMyPOCLogging, and CitrixMyPOCMonitoring—created by the installation wizard. We will need them later to create the databases with Microsoft SQL Management Studio.
- A File Explorer window will open with the path to the scripts.
- Open a separate File Explorer Window and connect to the Mapped Drive.
- Create a Folder called Scripts Z:\Scripts.
- Copy the scripts created by the Citrix installation wizard on the DDC01 to the mapped drive folder.



Step 12B: Create Databases

Connect to the FileAdmin01 as Domain Administrator:

- Launch Microsoft SQL Server Management Studio:
 - In the Connect to Server window, enter the Amazon RDS instance endpoint.
 - Select SQL Server Authentication.
 - Enter the Master DB user name of dbadmin and the password.
 - Click Connect.



We will create three databases with the names we created in Citrix installation wizard:

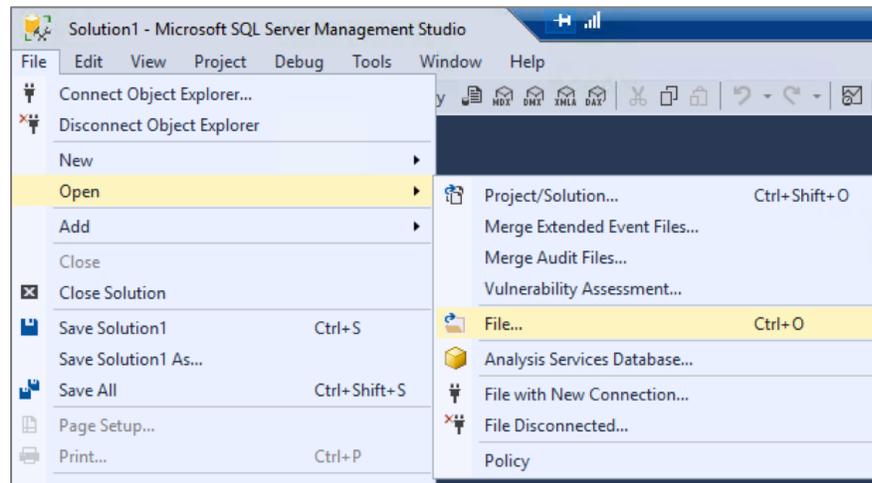
- CitrixMyPOCSite
- CitrixMyPOCLogging
- CitrixMyPOCMonitoring

Follow these steps for each Database being created:

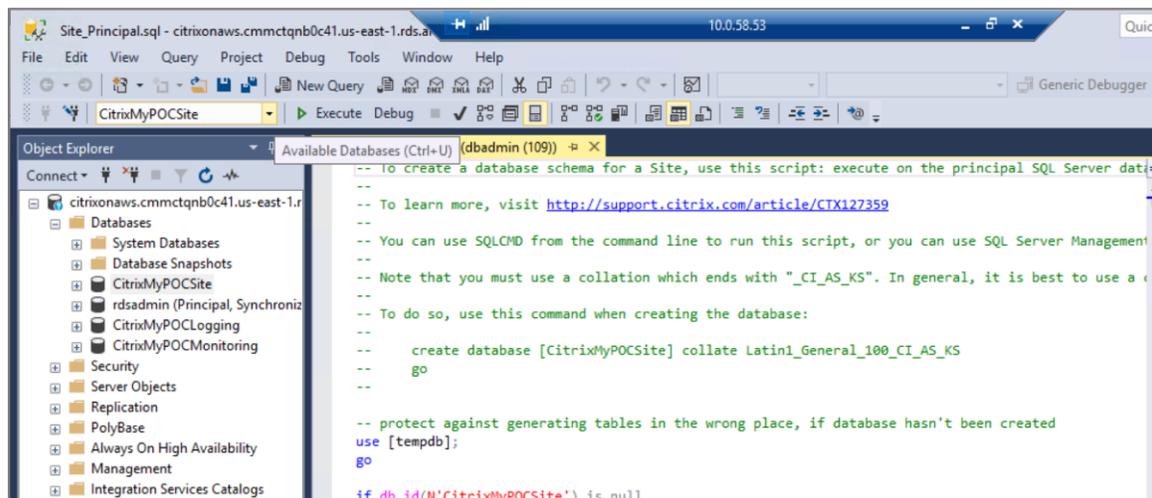
- Right-click on Databases in the left navigation window and select New Database.

- Enter the database name.
- Select Options from the New Database Window.
- Change Collation to “Latin1_General_100_CI_AS_KS.” Please note that you must use a collation which ends with “_CI_AS_KS.” In general, it’s best to use a collation which ends with “_100_CI_AS_KS.” This is outlined within the text of the site principal script.
- Set Recovery Model to Full.

Step 12C: Execute Scripts



- In Microsoft SQL Server Management Studio, navigate to File, Open, File.
- Open the mapped drive location and under scripts.
- select “Site_Principal.”



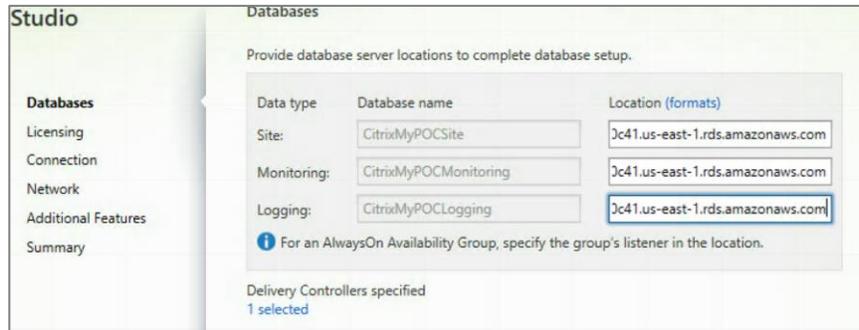
- Select CitrixMyPOCSite and click Execute.
 - Please note errors about “login already exists” or “Syntax error” can be ignored.

- Repeat these steps for the “Logging_Principal” and “Monitoring_Principal” scripts.

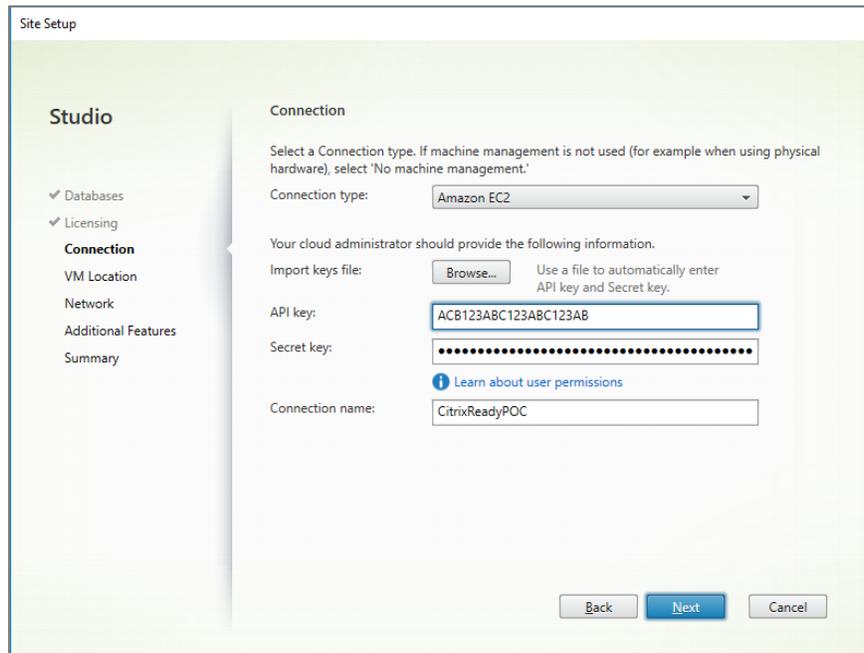
Step 12D: Complete Citrix installation:

Switch back to your RDP connection to the DDC01 instance:

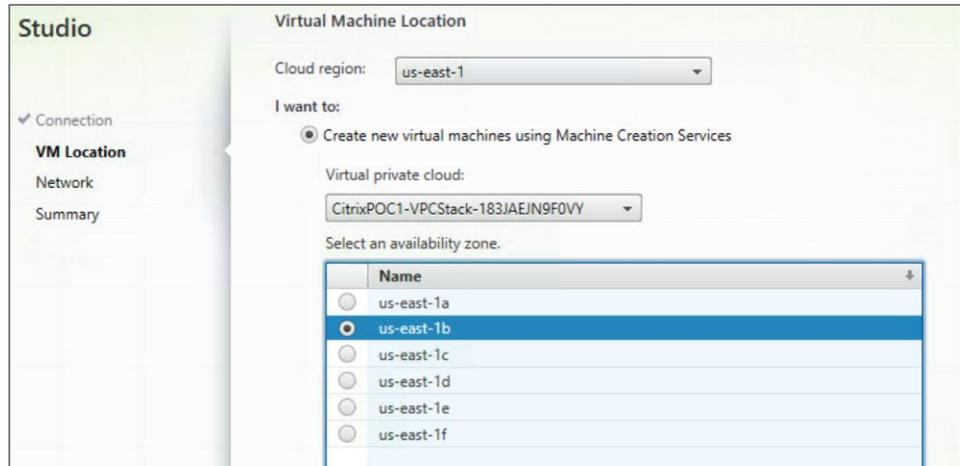
- In Citrix Studio, click “Continue database configuration and Site setup.”
- Enter the Amazon RDS endpoint URL for each database, and click Next.



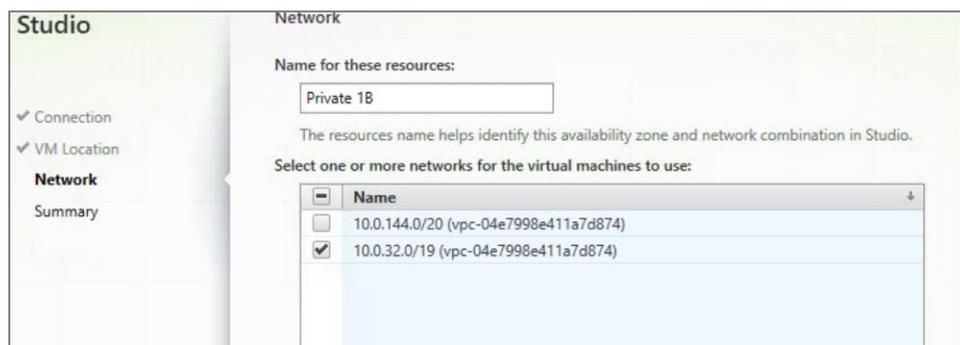
- Select the 30-day free license or enter a Citrix license if available, and click Next.



- Set the Connection type to Amazon EC2.
- Enter the API Key and Secret Key of the CitrixPOCAdmin IAM User we created earlier, and then click Next.
- Select the “Cloud region”, Virtual Private Cloud and Availability Zone for this deployment.

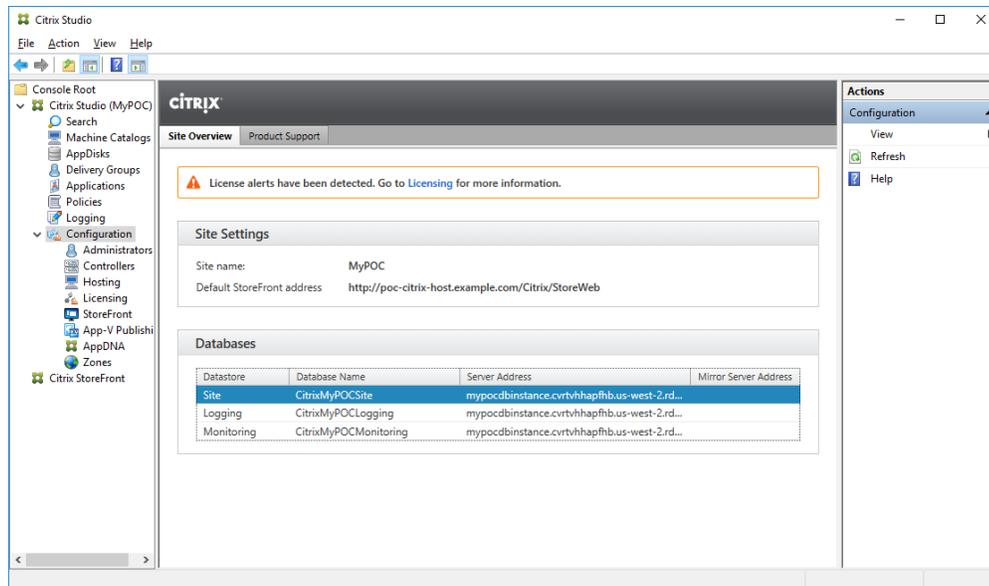


- Then Select the Private subnet you'd like your Amazon EC2 Instances deployed into.



- Check the AWS Management Console if you are not sure which AWS Region, Availability Zone, VPC, or subnet to select.
- Do not select AppDNA or App-V Publishing. Click Next.
- Click Finish.

You can check the configuration by clicking Configuration in the left navigation window.



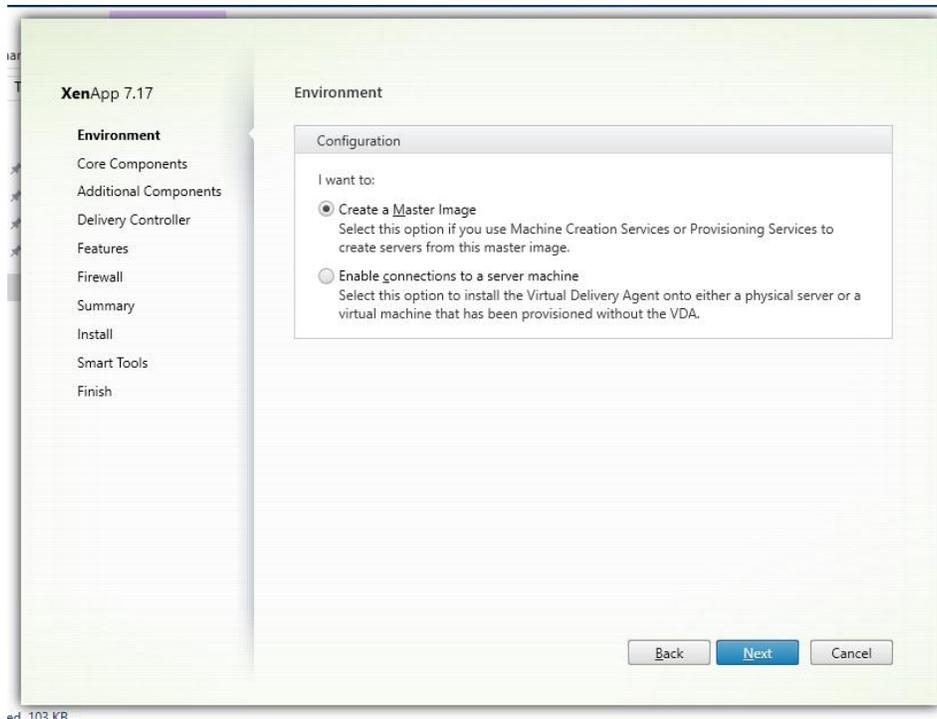
Step 13: Create a gold image VDA for use with Machine Creation Services

In this section, we will create a gold master VDA image to use with Machine Creation Services.

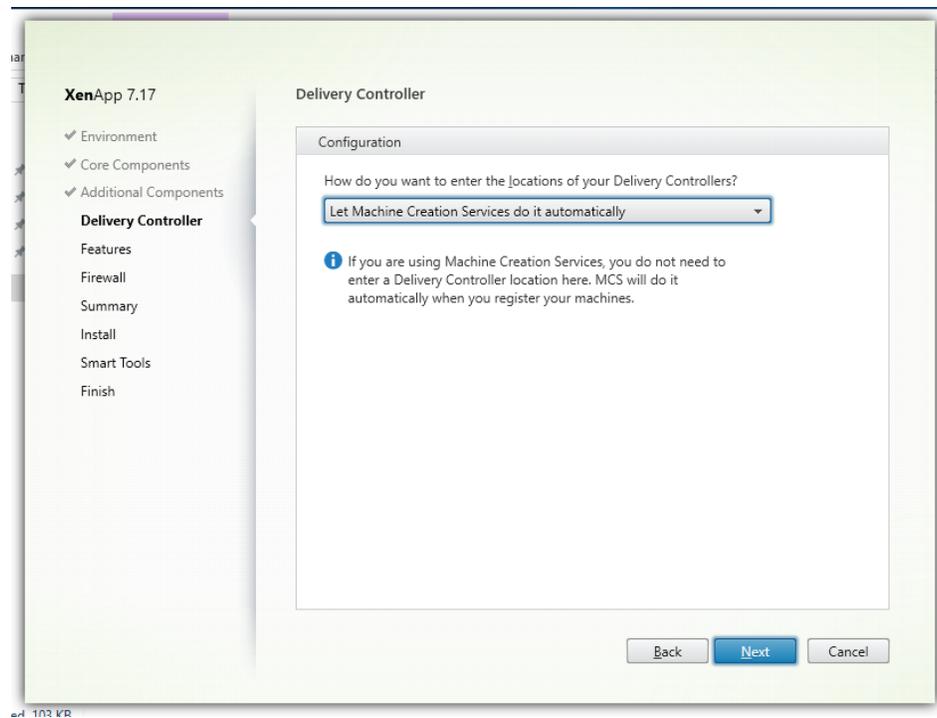
Connect to GoldVDA01 as Domain Admin (example.com\admin) account from the RDGW instance using Remote Desktop.

Navigate to the file share from FileAdmin01 in Windows Explorer:

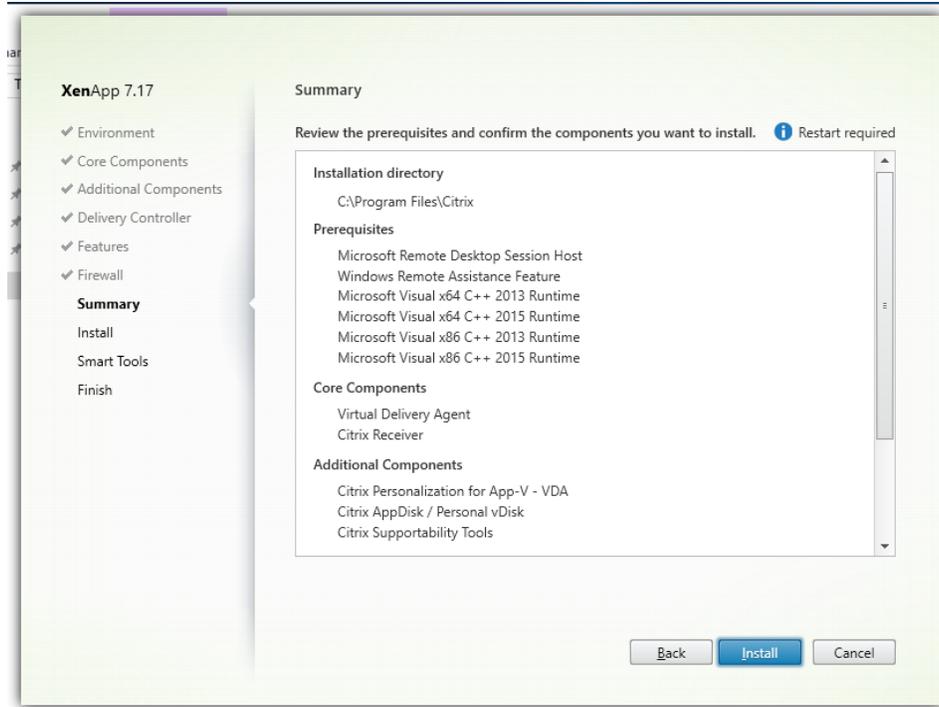
- Navigate to the XAXD_7_18 Folder
- Launch the AutoSelect installer.
- Click the Start button for XenApp.
- Select Prepare Machines and Images.
- Select Create a Master Image.



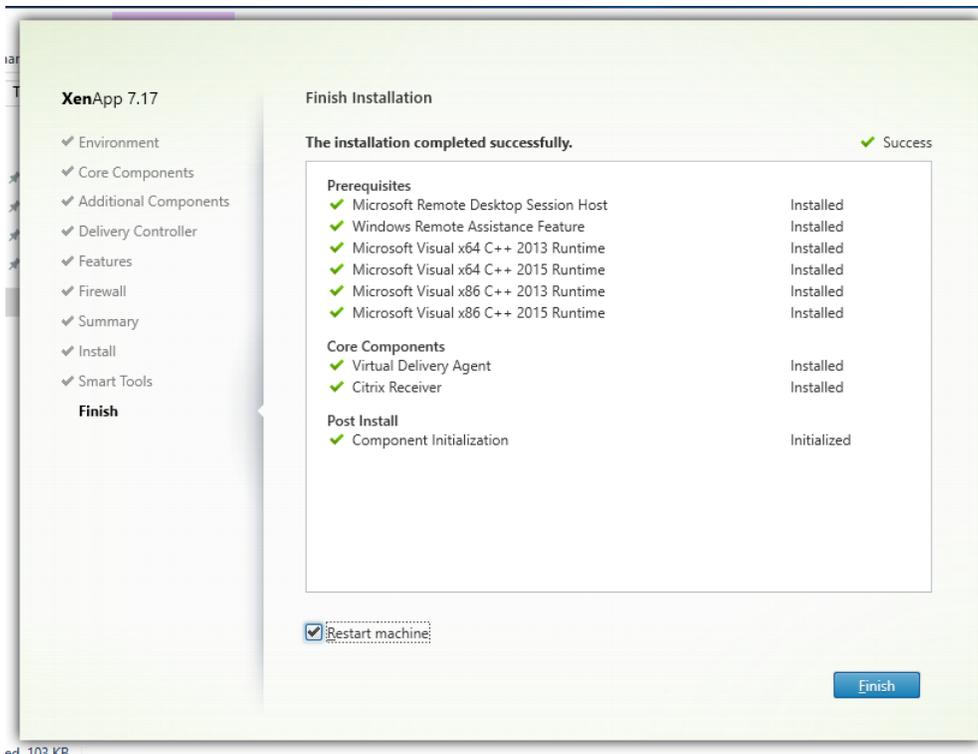
- Accept default options and click Next until you see the Delivery Controller Configuration screen. Select “Let Machine Creation Services do it automatically.”



- Click Next with default values until you see the Install button. Click Install.



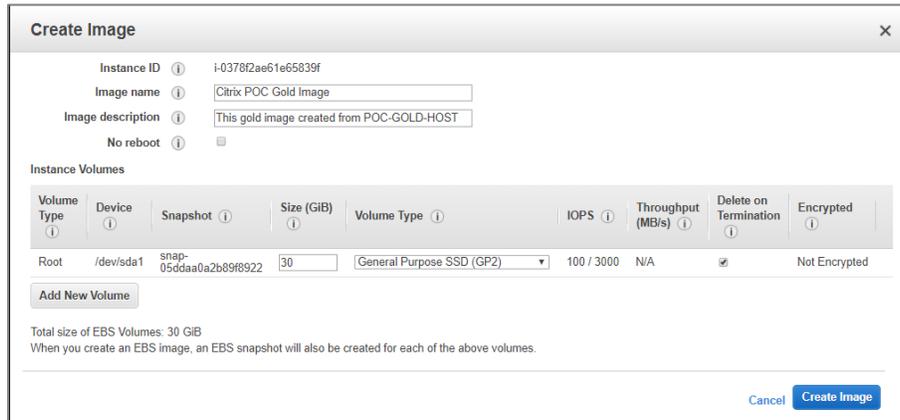
- When the installer finishes, select “I do not want to participate in Call Home.” Click Next.
- Click Finish. The instance will reboot when the installation is complete.



- The installer will finish and reboot the instance.

Open the AWS Console, go to the EC2 dashboard and view your Instances:

- Right-click GoldVDA01, and select Create Image from the Image sub-menu.
- Name the image Citrix POC Gold Image and enter a description.
- Click Create Image.



| Volume Type | Device | Snapshot | Size (GiB) | Volume Type | IOPS | Throughput (MB/s) | Delete on Termination | Encrypted |
|-------------|-----------|------------------------|------------|---------------------------|------------|-------------------|-------------------------------------|---------------|
| Root | /dev/sda1 | snap-05d0aa0a2b89f8922 | 30 | General Purpose SSD (GP2) | 100 / 3000 | N/A | <input checked="" type="checkbox"/> | Not Encrypted |

- Select AMIs in the AWS Management Console within the EC2 dashboard.
- The image is building and should be in Pending status. Wait for the image to be in Available status.



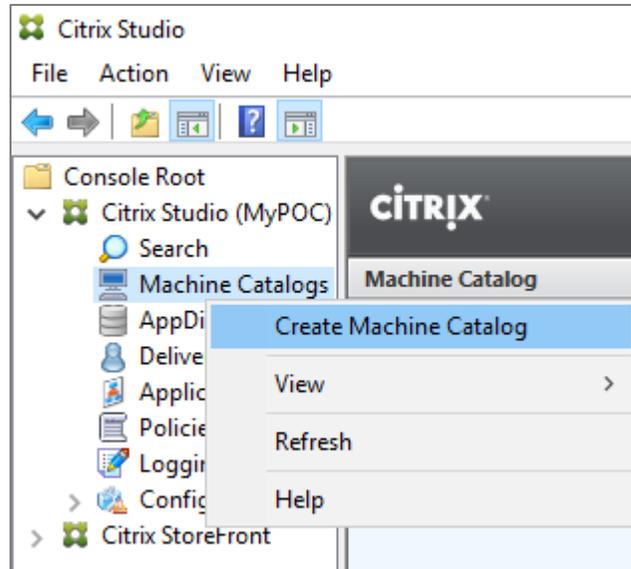
| Name | AMI Name | AMI ID | Source | Owner | Visibility | Status |
|--------------------------|-----------------------|-------------------------|------------------|--------------|------------|-----------|
| <input type="checkbox"/> | Citrix POC Gold Image | ami-0aa873d3d3412dea3e6 | 678451878732/... | 678451878732 | Private | available |

Step 14: Create the Gold Image VDA Machine Catalog and Delivery Group

In this section, we will make a new Machine Catalog and Delivery Group for the Citrix POC Gold Image we created earlier.

Connect to DDC01 as Domain Administrator via RDP:

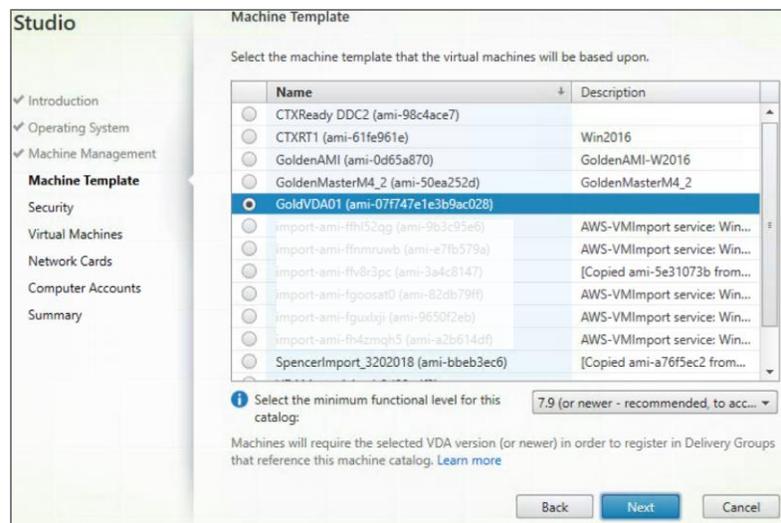
- Launch Citrix Studio.
- Right Click Machine Catalog and select Create Machine Catalog.



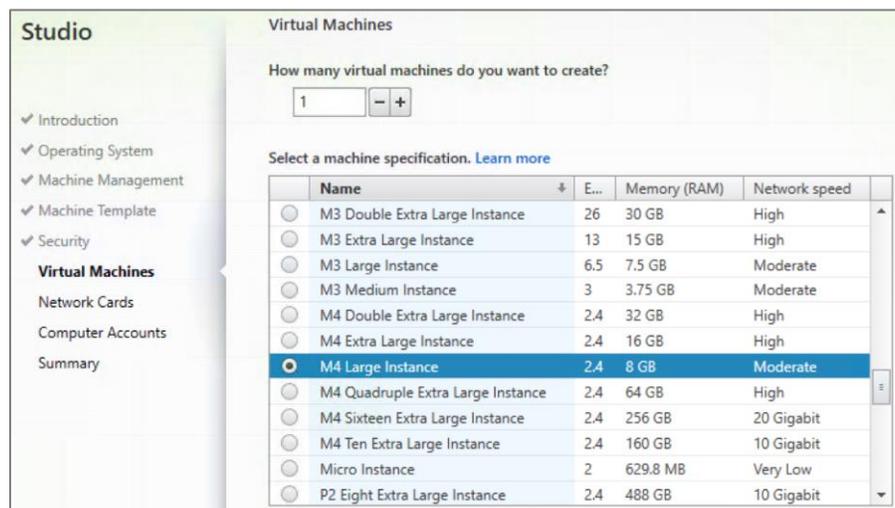
- Select Server OS, and click Next.
- Select “Machines that are power managed” and “Deploy Machines Using” Citrix Machine Creation Services (MCS).”



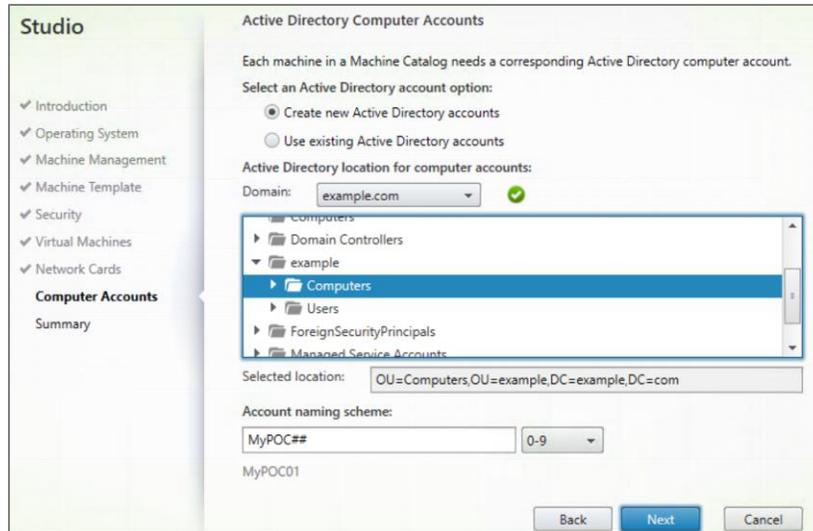
- Click Next.
- Select the Citrix POC Gold Image as the Machine Template. Click Next.



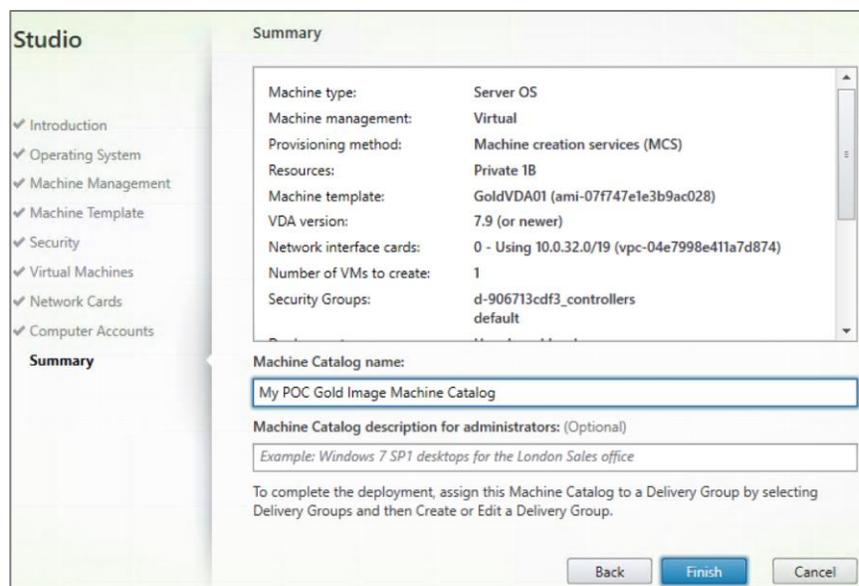
- Select the Domain Member Security Group and Default Security Groups (or your unique Security Group configuration) and click Next.
- Set Virtual Machine count to 1, or as many as you'd like.
- Select the same instance type we used (M4) for AMI image. Click Next.



- Select the subnet for Private 1A, and click Next.
- Select Create new Active Directory accounts.
- Set Domain to example.com.
- Select the Computers OU below example, not the top level Computers OU. The Domain Admin does not have permissions for the top level Computers OU. Make sure your Selected Location matches the screenshot below. Example OU then Computers OU.

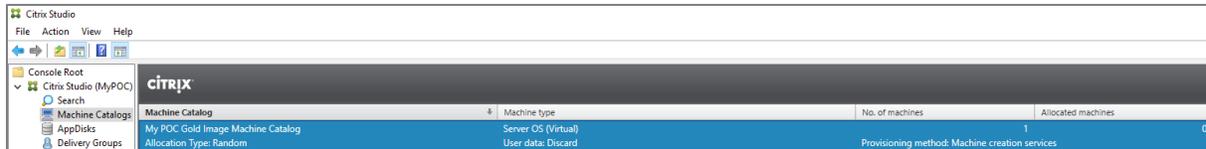


- Set Account Naming scheme to MyPOC##. Click Next.
- Name the Machine Catalog “My POC Gold Image Machine Catalog.” Click Finish.



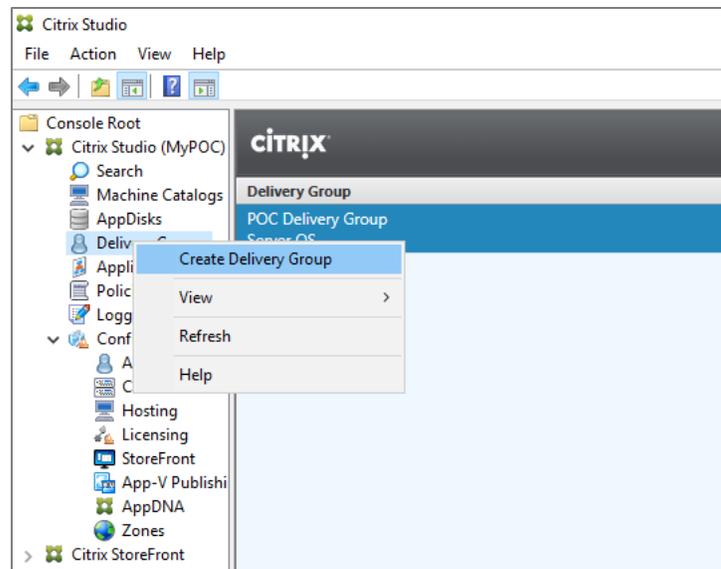
- Creation of the Machine Catalog will take at least 15 minutes. Do not proceed with the guide until the Machine Catalog creation has completed.
- You will see XenDesktop temp instance and Volume Worker instances start within your Amazon EC2 Dashboard. These instances are creating the identity Amazon EBS volumes for the catalog and will start and terminate throughout this process.

When Machine Creation Services is complete, you should see at least one machine in the catalog.

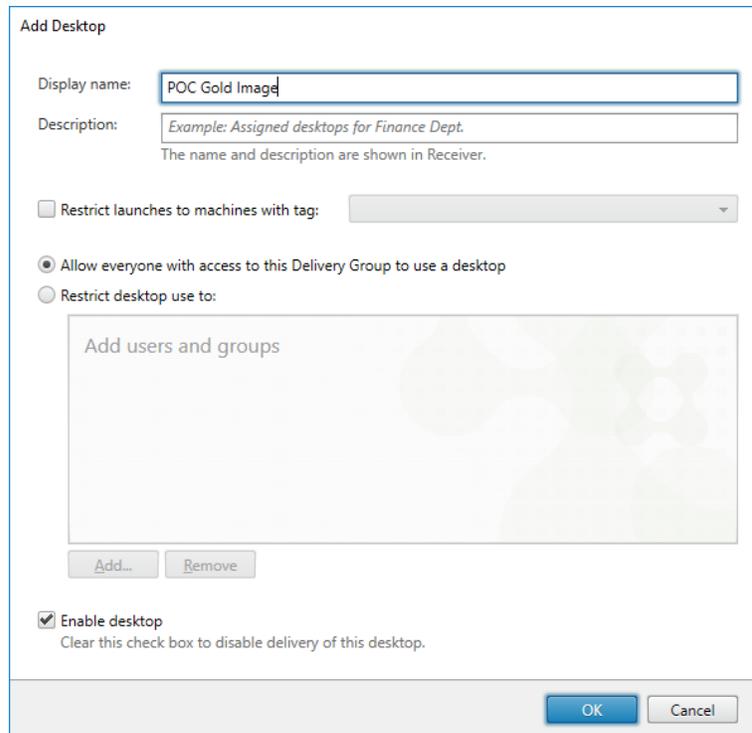


Create a Delivery Group for the Gold Image Machine Catalog:

- Expand Delivery Groups and select Create New Delivery Group.



- Select My POC Gold Image Machine Catalog, and click Next.
- Accept default values and click Next until the add Desktops Screen.
- Click Add.
- Set Display Name to POC Gold Image Delivery Group. Click OK.
- Click Next in the Desktops Windows.



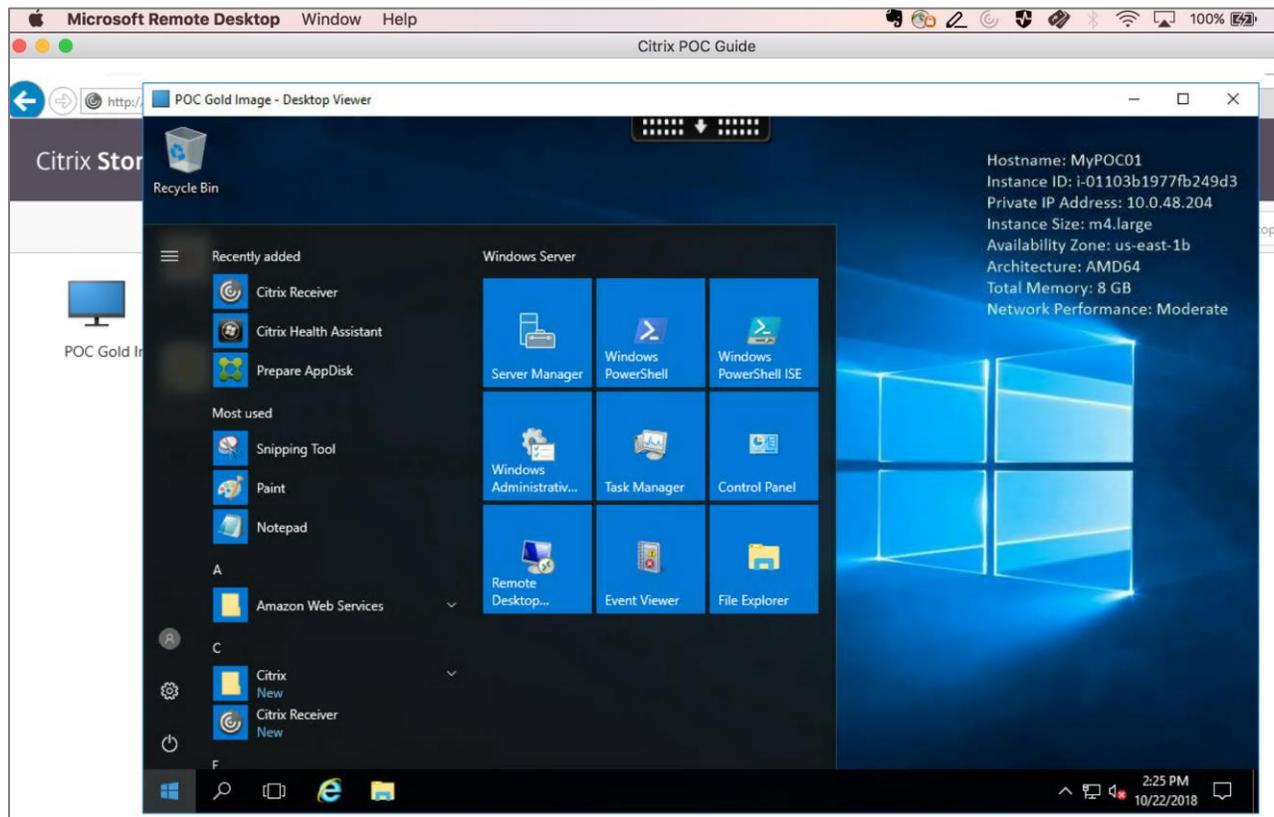
- Name the Delivery Group “POC Gold Image” Delivery Group. Click Finish.

Step 15: Launch a Gold Image VDA Session

In this section, we will test the Gold Image instance we created in the Machine Catalog by launching a session.

Connect to FileAdmin01 as Domain Administrator via RDP:

- Open a browser and enter <http://ddc01.example.com/Citrix/StoreWeb>
- Install the Citrix Receiver using the default values.
- Log in as Domain Administrator.
- Select the Desktops tab.
- Launch the POC Gold Image.



You've successfully completed a Citrix Virtual Apps and Desktops deployment within your AWS account!

This guide does not provide internet-based users access to these desktop resources. If you'd like to extend this environment to internet-based users follow this guide. [Validated Reference Design NetScaler and Amazon AWS](#).

If you require an HA configuration, deploy a second Desktop Delivery Controller (DCC02) and during the installation of XenApp, select, join an existing Farm.

Dive Deeper with Citrix Virtual Apps and Desktops

Check out [this reference documentation](#) from Citrix for more information on adding, removing, and moving Controllers.

[Understanding the Database requirements for XenApp & XenDesktop](#)

[How to use PowerShell to Change XenDesktop SQL Connection Strings](#)

Technical Articles and Support related to Citrix on AWS

[Configure the Volume Worker instance to use the Machine Catalog VPC and not the default VPC](#)

[MCS doesn't show the instance type or size you'd like to use for your deployment within a machine catalog](#)

[MCS fails with dedicated instances - Citrix switched the instance type of the Volume Service Worker to T2 which doesn't exist in dedicated environments](#)

[Amazon EC2 AMIs with Windows Server](#) require no Client Access Licenses (CALs). They also include two Microsoft Remote Desktop Services licenses for administrative purposes.

For RDSH or XenApp use cases, it's recommended to license additional Microsoft Remote Desktop Services licenses for additional users.