AWS Technical Essentials
Lab Guide
Version 3.7A

AWS-100-ESS-37A-EN

Corrections or feedback on the course, please email us at:
aws-course-feedback@amazon.com.
For all other questions, contact us at:
https://aws.amazon.com/contact-us/aws-training/.

Table of Contents

Lab 1: Amazon S3

Overview	**Amazon Simple Storage Service** (**Amazon S3**) is a scalable object storage service designed for the Internet. In this lab you will create an Amazon S3 bucket and configure access logging. You will then upload an object and manage its permissions. When this is done, you can access the object via a web browser. You will have a chance to modify the object metadata, encrypt objects with Server Side Encryption, create folders, apply bucket-wide security with a bucket policy, and enable lifecycle policies to archive and delete logs.

Objectives	After completing this lab, you will be able to: • Create an Amazon S3 bucket and manage properties. • Upload objects and manage object-level permissions. • Access objects in an Amazon S3 bucket from a web browser. • Create folders and apply bucket-wide security using bucket policies.

Pre-requisites	This lab requires: • Access to a notebook computer with Wi-Fi running Microsoft Windows, Mac OS X, or Linux (Ubuntu, SuSE, or Red Hat). ○ **Note** The qwikLABS lab environment is not accessible using an iPad or tablet device, but you can use these devices to access the student guide. • For Microsoft Windows users: Administrator access to the computer. • An Internet browser such as Chrome, Firefox, or Internet Explorer 9 (previous versions of Internet Explorer are not supported).

Command Reference File	At various points, this lab will instruct you to copy and paste text as part of lab procedures. This text should be copied from the lab's associated **command reference file**, which is available on the Instructions tab of your lab in qwikLABS. It is not recommended to copy and paste text from this lab manual, as the manual's rich formatting may inject characters that cannot properly be parsed by the command line

Scenario	As the operations-focused individual in a start-up business, you are tasked with coming up with a low cost, high availability solution for your customer-facing website. Your website will host a myriad of documents for your customers, as well as video and static content. Your global team will contribute and update the content on your site.

Task 1-1: Amazon S3 Basics	
Overview	You need to build the public-facing website. In this section, you will access the Amazon S3 Console, create a new Amazon S3 bucket to contain Asperatus Tech's website content, configure logging, upload an object, and then access that object.

Step	Instruction
1.1.1	Log in to your **AWS Management Console**. Use the instructions in **Appendix A** of this lab manual to log in to the AWS Management Console using the pre-configured student account.
1.1.2	In the **AWS Management Console**, on the **Services** menu, click **S3**.
1.1.3	Click **Create Bucket** to create a new bucket. **Note**: There is already a bucket named "*QLtrail-Lab…*". This is just for the sandbox environment. You will be creating a new bucket.
1.1.4	In the **Create a Bucket – Select a Bucket Name and Region** dialog box, enter the following values: • **Bucket Name**: Type a bucket name that will be unique across Amazon S3. We recommend that you name your bucket with your initials and today's date to ensure uniqueness. This value will be referred to as *s3-bucket-name* in subsequent procedures. • **Region**: Choose a region closest to your location. If unsure, choose **Oregon**.
1.1.5	Click **Create**.
1.1.6	In the **S3 Console**, click the name of your bucket to view its contents. You will receive a message indicating that the bucket is empty.

1.1.7	Click **Upload** to add a new file object to your bucket.
1.1.8	In the **Upload – Select Files and Folders** dialog box, click **Add Files**.
1.1.9	Select a file (e.g. picture from My Pictures folder) from your local machine to use as an object. **Note**: We will refer to this uploaded file as *the object* in subsequent procedures
1.1.10	Click **Start Upload**. You can see the progress of the upload in the **Transfers** pane.

Task 1-2: Working with Objects	
Overview	Data for the company website will have various permissions and security associated with it. In this section, you will use the Amazon S3 Management Console to modify object attributes, including permissions, encryption, and Reduced Redundancy Storage options.

Step	Instruction
1.2.1	In the **S3 Console**, click on the name of the object that you uploaded earlier. **Note**: On selecting an object, the check box next to its name turns blue.
1.2.2	Click **Properties** to display the properties of the object.
1.2.3	In the **Properties** pane, click the **Link** to open the object. You will receive an Access Denied error message on clicking the link. **Note**: Notice the lock icon next to the link. It implies that the link to the object is a private link. Objects in Amazon S3 are private by default.
1.2.4	In the **S3 Console**, right-click the object and click **Make Public**.
1.2.5	Click **OK** on the dialog box to confirm.
1.2.6	Let us try to access the object again. In the **S3 Console**, with the object selected, click **Properties**.
1.2.7	In the **Properties** pane, click the **Link** again. The object should open this time without any error. **Note**: Notice the icon next to the link implying that it is a public link.
1.2.8	In the **Properties** pane, expand the **Details** section.

1.2.9	In the **Details** section, use the following values: • **Storage Class**: **Reduced Redundancy** The Reduced Redundancy Storage class reduces costs by storing noncritical, reproducible data at lower levels of redundancy than the Standard Storage class. • **Server Side Encryption**: **AES-256** Encryption provides added security for the object data stored in your Amazon S3 buckets.
1.2.10	Click **Save**.

Task 1-3: Folders and Bucket Policies	
Overview	As you are uploading the company documents, you begin to realize the need to better organize your documents and to simplify the management of security. In this section, you will use the Amazon S3 Console to organize your objects into folders. You will then create a Bucket Policy that defines permissions based on folders.

Step	Instruction
1.3.1	In the **S3 Console**, make sure you are in the bucket that you created earlier. **Hint**: The path in the top-left corner of the **S3 Console** should be **All Buckets / <Your S3 Bucket name>**
1.3.2	Click **Create Folder.**
1.3.3	In the **Name** field type **images** and click the check mark.
1.3.4	Repeat this procedure to create two more folders with the names **pages**, and **logs**.
1.3.5	In the **S3 Console**, make sure you are in the bucket that you created earlier. **Hint**: The path in the top-left corner of the S3 Console should be **All Buckets / <Your S3 Bucket name>**
1.3.6	Click **Properties**.
1.3.7	In the **Properties** pane, expand the **Permissions** section.
1.3.8	Click **Add bucket policy** to create a new policy for your bucket. Bucket policies define the permissions structure for your Amazon S3 bucket.

1.3.9	In the **Bucket Policy Editor** dialog box, click the **AWS Policy Generator** link.
1.3.10	In the **AWS Policy Generator** page, use the following values: • **Select Type of Policy: S3 Bucket Policy** • **Effect: Allow** • **Principal: *** • **AWS Service: Amazon S3** • **Actions: GetObject** • **Amazon Resource Name (ARN):** **arn:aws:s3:::<Your-S3-Bucket-Name>/images/*** **Note**: You are creating this policy only for the **images** folder in your S3 bucket.
1.3.11	Make sure you specified the correct bucket name in the Amazon Resource Name (ARN) field.
1.3.12	Click **Add Statement.**
1.3.13	Click **Generate Policy** to generate the policy.
1.3.14	In the **Policy JSON Document** dialog box, **copy** the generated policy text to your clipboard.
1.3.15	Click **Close**.
1.3.16	Go back to the **S3 Management Console** and in the **Bucket Policy Editor** dialog box, **paste** the policy text you copied earlier.
1.3.17	Click **Save**. **Note**: If the **Save** button is not active, type an extra space at the end of the policy text to activate it.

1.3.18	In the **S3 Console**, click the **images** folder in your bucket to view its contents.
1.3.19	Click **Upload** to upload a new object to your **images** folder.
1.3.20	In the **Upload – Select Files and Folders** dialog box, click **Add Files**.
1.3.21	Select a file (e.g. picture from My Pictures folder) from your local machine to use as an object. **Note**: We will refer to this uploaded file as *the object* in subsequent procedures
1.3.22	Click **Start Upload**. You can see the progress of the upload in the **Transfers** pane.
1.3.23	**Select** the object and click **Properties** to display its properties.
1.3.24	In the **Properties** pane, click the **Link** to open the object. Unlike in task 1-2, you will be able to access the object without any error because the Bucket Policy granted access to all objects in the **images** folder. **Note**: If you try to open objects in other folders, you will still get the access denied error. This is because you defined the Bucket Policy only for the **images** folder.

Task 1-4: Lifecycle Policies (Optional Task)	
Overview	Now that you have the business needs taken care of, you want to take care of the technical needs. It is important to have logs stored in an easy location, but it is also important to move them to a lower-cost location for long-term storage and then eventually remove them. In this section, you will use the S3 Console to define lifecycle policies for your bucket. The rules will move objects from your logs folder to Amazon Glacier storage after 30 days, and will delete them after 90 days.

Step	Instruction
1.4.1	In the **S3 Console**, click **All Buckets.**
1.4.2	Click **Create Bucket** to create a new bucket for storing logs.
1.4.3	In the **Create a Bucket – Select a Bucket Name and Region** dialog box, use the following values for the new bucket: • **Bucket Name: serverlogs** (add some unique identifier such as your initials at the end of the bucket name to make it unique). • **Region**: Check with your instructor for the region to choose. **Note**: Amazon Glacier service is currently not available in all regions. For this lab exercise, we will use a region where this service is available. If unsure, choose **Oregon**.
1.4.4	Click **Create**.
1.4.5	In the **S3 Console**, click the **serverlogs** bucket that you created.
1.4.6	Click **Properties.**

1.4.7	In the **Properties** pane, expand the **Lifecycle** section.
1.4.8	In the **Lifecycle** section, click **Add rule**.
1.4.9	In the **Lifecycle Rules** dialog box, on **Step 1: Choose Rule Target**, choose the following value: • **Apply the Rule to: Whole Bucket:<Your-serverlogs-bucket>**
1.4.10	Click **Configure Rule**.
1.4.11	On **Step 2: Configure Rule**, choose the following values: • **Action on Objects: Archive and then Permanently Delete** • **Archive to the Glacier Storage Class: 30 days** • **Permanently Delete: 90 days** **Note:** If you do not have the **Archive and then Permanently Delete** option, then you might have created your **serverlogs** bucket in a Region where Amazon Glacier service is not available. Please create a new bucket in a different region, for example: **Oregon**.
1.4.12	Select the acknowledgement check box.
1.4.13	Click **Review**.
1.4.14	On **Step 3: Rule**, use the following value: • **Rule Name: archive-logs**
1.4.15	Click **Create and Activate Rule**. The contents of the bucket will now automatically move from Amazon S3 to Glacier 30 days after creation, thereby lowering your storage costs. After 90 days, the objects will be automatically deleted from Amazon Glacier and Amazon S3.

1.4.16	**Congratulations!** You now have successfully: • Created an Amazon S3 bucket and configured its properties. • Uploaded objects and managed object-level permissions. • Accessed objects in an Amazon S3 bucket from a web browser. • Created folders and applied bucket-wide security using bucket policies.
1.4.17	Close the **Amazon S3 Management Console** window/tab.
1.4.18	On the qwikLABS page, click **End** to end your lab session.

Lab 2: Amazon EC2

Overview	**Amazon Elastic Compute Cloud** (**Amazon EC2**) is a web service that provides resizable compute capacity in the cloud. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity as your computing requirements change. In this lab you will launch an Amazon EC2 instance, connect to the instance, and create Elastic Block Store (EBS) volumes.

Objectives	After completing this lab, you will be able to: • Create an EC2 key pair and a security group. • Launch an Amazon EC2 Windows Instance. • Activate Termination Protection for an Amazon EC2 instance. • Create EBS volumes and snapshots.

Pre-requisites	This lab requires: • Access to a notebook computer with Wi-Fi running Microsoft Windows, Mac OS X, or Linux (Ubuntu, SuSE, or Red Hat). ○ **Note** The qwikLABS lab environment is not accessible using an iPad or tablet device, but you can use these devices to access the student guide. • For Microsoft Windows users: Administrator access to the computer. • An Internet browser such as Chrome, Firefox, or Internet Explorer 9 (previous versions of Internet Explorer are not supported).

Mac Users	This lab requires you to access a Windows instance by using Remote Desktop Connection software. Please check whether your computer has Remote Desktop Connection already installed. If not, then the software can be downloaded using this link: https://itunes.apple.com/us/app/microsoft-remote-desktop/id715768417

Command Reference File	At various points, this lab will instruct you to copy and paste text as part of lab procedures. This text should be copied from the lab's associated **command reference file**, which is available on the Instructions tab of your lab in qwikLABS. It is not recommended to copy and paste text from this lab manual, as the manual's rich formatting may inject characters that cannot properly be parsed by the command line

Scenario	As the operations-focused individual in a start-up business, you are tasked with coming up with a low cost, high availability solution for your customer-facing website. Your website will host a myriad of documents for your customers, as well as video and static content. Your global team will contribute and update the content on your site.

Task 1-1: Amazon EC2 Key Pairs	
Overview	In this lab, you are going to create a new key pair that will be used to launch your EC2 instance and also to retrieve your Windows Administrator password for the EC2 instance.

Step	Instruction
1.1.1	Log in to your **AWS Management Console**. Use the instructions in **Appendix A** of this lab manual to log in to the AWS Management Console using the pre-configured student account.
1.1.2	In the **AWS Management Console**, on the **Services** menu, click **EC2**.
1.1.3	In the navigation pane of the **EC2 Management Console**, click **Key Pairs**.
1.1.4	Click **Create Key Pair**.
1.1.5	In the **Create Key Pair** dialog box, use the following value: • **Key pair name: asperatus**
1.1.6	Click **Create**.
1.1.7	Save the file **asperatus.pem** to your local computer. This file contains the 'private' half of your key pair. You do not have to open the file; just remember where you saved the file (for example, the Downloads folder), because the file will be used later.

Task 1-2: Security Groups	
Overview	In preparation for launching an EC2 instance, you will now create a security group that will permit network access for web traffic and remote administration.

Step	Instruction
1.2.1	In the navigation pane of the **EC2 Management Console**, click **Security Groups**.
1.2.2	Click **Create Security Group**.
1.2.3	In the **Create Security Group** dialog box, use the following values: • **Security group name: Remote access** • **Description: Grant RDP Access** • **VPC:** From the drop-down list, click **Lab VPC** if it is not already selected **Note:** The VPC ID starts with "**vpc-**" with CIDR range of 10.1.0.0/16.
1.2.4	In the **Security group rules** section, click **Add Rule** to add a rule to your security group.
1.2.5	For your security rule, specify the following values: • **Type: RDP** • **Source: Anywhere** **Note**: It is normally a best practice to **NOT** enable RDP access directly to production servers. Rather, it is best to use a Bastion Server ('Jump Box') as the entry point for RDP and SSH connections. Creating a wide-open security rule in this step is done for lab purposes only.
1.2.6	To add a second rule, click **Add Rule**.

1.2.7	You will need HTTP access to the instance. Use the following values to include HTTP access: • **Type: HTTP** • **Source: Anywhere** **Note**: Creating a wide-open security rule in this step is done for lab purposes only.
1.2.8	Click **Create** to create the Remote access security group.
1.2.9	You have now configured a security group to permit inbound access for Remote Desktop Protocol (port 3389) and HTTP (port 80) web traffic. Later in the lab you will attach this security group to your EC2 instance so you access the instance via RDP and HTTP.

Task 1-3: Launching an Amazon EC2 Windows Instance	
Overview	Now that you have created a key pair and defined a Security Group, it is time to launch your web server. In this section, you will launch an Amazon EC2 instance which will be your web server.

Step	Instruction
1.3.1	In the navigation pane of the **EC2 Management Console**, click **Instances**.
1.3.2	Click **Launch Instance**.
1.3.3	On the **Step 1: Choose an Amazon Machine Image (AMI)** page, select the first **Microsoft Windows Server 2012 R2 Base** distribution in the list by clicking **Select**.
1.3.4	On the **Step 2: Choose an Instance Type** page, choose **t2.medium**.
1.3.5	Click **Next: Configure Instance Details**.
1.3.6	On the **Step 3: Configure Instance Details** page, select the following values: • **Network:** From the drop-down list, click **Lab VPC** • **Auto-assign Public IP:** Enable Leave the rest as its default values. **Note:** If you see an error message, “No default subnet found. Please choose another subnet in your default VPC, or choose another VPC,” click the **Don’t show me this again** link to close this message. You can safely ignore this message for this lab environment; in an actual customer environment you would contact AWS support to resolve this issue.
1.3.7	Click **Next: Add Storage**.

1.3.8	On the **Step 4: Add Storage** page, leave the default selections and click **Next: Tag Instance**.
1.3.9	On the **Step 5: Tag Instance** page, specify a new name value for your instance as follows: • **Key: Name** • **Value: Web Server**
1.3.10	Click **Next: Configure Security Group**.
1.3.11	On the **Step 6: Configure Security Group** page, use the following values: • **Assign a security group: Select an existing security group** • **Security group name: Remote access**
1.3.12	Click **Review and Launch**.
1.3.13	On the **Step 7: Review Instance Launch** page, review the configuration for your instance. When done, click **Launch**.
1.3.14	In the **Select an existing key pair or create a new key pair** dialog box, use the following values: • **First dropdown (unlabeled): Choose an existing key pair** • **Select a key pair:** Select the **asperatus** key pair • **I acknowledge that I have access to…:** Enable this checkbox **Note**: Make sure you selected the **asperatus** key pair that you created previously.
1.3.15	Click **Launch Instances**.
1.3.16	On the **Launch Status** page, click **View Instances**. Observe the **Status Checks** field of your **Web Server** instance until it shows that both status checks have completed successfully. Ignore the **Alarm Status** field in this lab environment.

Task 1-4: Termination Protection	
Overview	Now that you have launched your Amazon EC2 instance, it is worth knowing how to keep the instance from being deleted accidentally. In this section, you will enable termination protection for your instance which will protect it from accidental terminations.

Step	Instruction
1.4.1	In the navigation pane of the **EC2 Management Console**, click **Instances**.
1.4.2	Select the **Web Server** instance that you just created. **Note**: On selecting an instance, the check box next to its name turns blue.
1.4.3	In the **Actions** menu, go to **Instance Settings** and click **Change Termination Protection**.
1.4.4	In the **Enable Termination Protection** dialog box, click **Yes, Enable**. This will protect the instance from accidental termination.
1.4.5	To verify termination protection, in the **Actions** menu, go to **Instance State** and click **Terminate**.
1.4.6	In the **Terminate Instances** dialog box, you will notice that the **Yes, Termination** option is inactive.
1.4.7	Click **Cancel**.

Task 1-5: Creating an EBS Volume	
Overview	In this section, you will use the Amazon EC2 Management Console and the Windows disk management utility to create, attach, and manipulate an Elastic Block Store (EBS) volume. EBS volumes must be created in the same Availability Zone as the Amazon EC2 instance to which they connect.

Step	Instruction
1.5.1	In the navigation pane of the **EC2 Management Console**, click **Instances**.
1.5.2	Make a note of the **Availability Zone** in which your **Web Server** instance is running. **Hint**: Look at the **Availability Zone** field value for your **Web Server** instance.
1.5.3	In the navigation pane, click **Volumes**.
1.5.4	Click **Create Volume** to create a new volume.
1.5.5	In the **Create Volume** dialog box, use the following values for the new volume: • **Type: General Purpose (SSD)** • **Size (GiB): 10** • **Availability Zone:** Select the same availability zone that you identified in step 1.5.2 **Note**: Make sure you selected the size of the new volume to be 10GiB.
1.5.6	Click **Create**. An empty 10GiB volume is created.

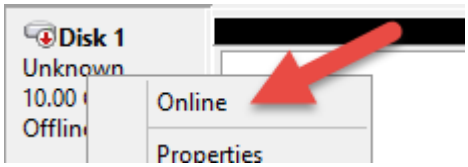
1.5.7	You can give a name to the new volume to identify it more easily. **Select** the 10GiB volume that you just created. **Hint**: Click the  icon to refresh the pane and get the latest status. **Note**: Make sure only the 10GiB volume is selected.
1.5.8	In the **Actions** menu, click **Add/Edit Tags**.
1.5.9	In the **Add/Edit Tags** dialog box, click **Create Tag**.
1.5.10	Use the following values to create a new tag for the 10GiB volume: • **Key: Name** • **Value: Small Volume**
1.5.11	Click **Save**. The name of the volume will now appear in the **Name** column of the 10GiB volume.
1.5.12	You can now attach the new EBS volume to your Amazon EC2 instance. Select the **Small Volume** that you just created. **Note**: Make sure only the **Small Volume** is selected.
1.5.13	In the **Actions** menu, click **Attach Volume**.
1.5.14	In the **Attach Volume** dialog box, click in the **Instance** field and select your **Web Server** instance.
1.5.15	Click **Attach**. This will attach the Small Volume to the Web Server instance. We will verify this by connecting to the Web Server instance in the next section.

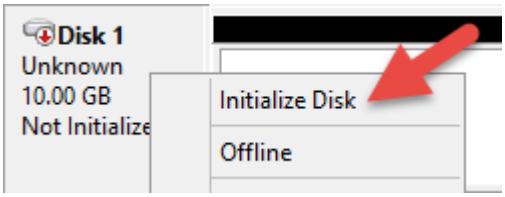
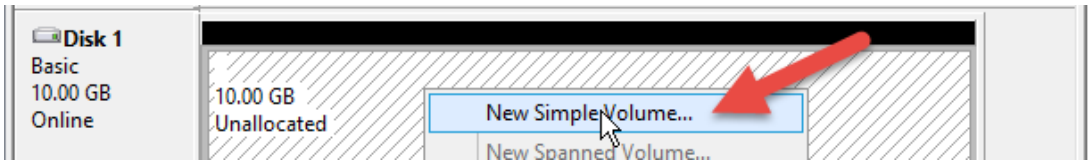
Task 1-6: Connection to your Amazon EC2 Instance	
Overview	The Web Server instance that you created previously is now running and has an additional EBS volume that you attached in the previous procedure. Since this Amazon EC2 instance is running Microsoft Windows, you can now connect to it by using the Remote Desktop Connection application. In order to do this, you will require the IP address and password of your instance. A random Administrator password has been created for your instance. To retrieve it, you will need to use the **asperatus.pem** file, the 'private' half of your **asperatus** key pair, you saved earlier.

Step	Instruction
1.6.1	In the navigation pane of the **EC2 Management Console**, click **Instances**.
1.6.2	Select your **Web Server** instance.
1.6.3	In the **Description** tab, copy the **Public IP** value to a text editor like Notepad. You will need this IP address to establish a Remote Desktop Connection to the Web Server.
1.6.4	On the **Actions** menu, click **Get Windows Password**.
1.6.5	On the **Retrieve Default Windows Administrator Password** page, click **Browse**, and select the **asperatus.pem** file that you downloaded in step 1.1.7.
1.6.6	Click **Decrypt Password**.
1.6.7	Copy the **Password** to a text editor as you will need this to login to your Web Server instance.

1.6.8	In the **Retrieve Default Windows Administrator Password** dialog box, click **Close** to close the dialog box.
1.6.9	Launch a Remote Desktop Connection (RDP) to your Web Server using the **Public IP** of your Web Server instance and the **Password** you obtained in the previous steps. Make sure to login as the **Administrator**. **Note**: If you are using Mac to remote desktop into the Web Server instance, check if your machine has Remote Desktop Connection already installed. If not, you can download this software using this link: https://itunes.apple.com/us/app/microsoft-remote-desktop/id715768417
1.6.10	Do **NOT** close the RDP session as you will use it in the next section of the lab.

Task 1-7: Using EBS Volumes	
Overview	You can use the Windows Server Management tool to format your EBS volume. In this section, you will configure and use the EBS volume from your Web Server instance.

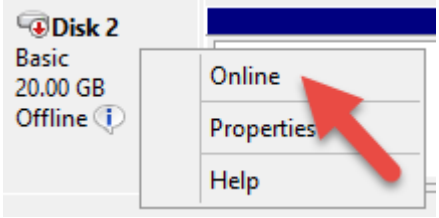
Step	Instruction
1.7.1	In the RDP session to the Web Server, click the **Server Manager** icon in the taskbar 
1.7.2	In the **Server Manager** window, on the **Tools** menu, click **Computer Management**.
1.7.3	In the **Computer Management** window, in the left navigation pane, click **Disk Management**.
1.7.4	You will notice the 10GiB EBS volume is already attached to your Web Server and is in an offline state. In order to use this disk, you will first need to bring it online. Right-click **Disk 1** and click **Online**. 

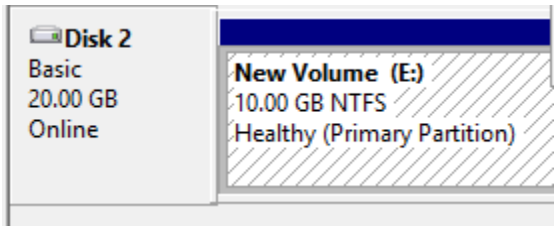
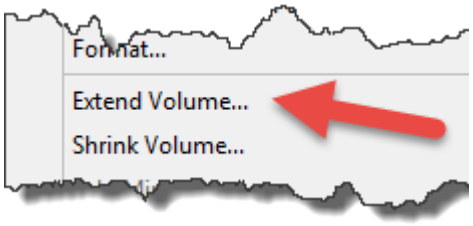
1.7.5	Next the disk needs to be initialized. Right-click **Disk 1** and click **Initialize Disk**. 
1.7.6	In the **Initialize Disk** dialog box, accept the default values and click **OK**.
1.7.7	Right-click the unallocated volume and click **New Simple Volume…** 
1.7.8	In the **New Simple Volume Wizard**, accept the defaults for all steps (click **Next** four times) and click **Finish**. The disk will now be formatted and added as a new drive (D:)
1.7.9	Close the **Computer Management** window and the **Server Manager** window.
1.7.10	In the RDP session, launch Windows Explorer and navigate to the new drive (D:) that you just added. 
1.7.11	Create a new folder on the drive (D:) called **Asperatus**.
1.7.12	Keep the RDP session open as you will use it in the next section of the lab.

Task 1-8: EBS Snapshots	
Overview	While performing your work for Asperatus, you realize that a larger EBS volume is required. In this section, you will create a new, larger EBS volume by taking a snapshot of your existing Small Volume. An EBS snapshot is a backup copy of an EBS volume. Snapshots are stored in Amazon S3 to ensure high durability. New EBS volumes can then be created from EBS snapshots.

Step	Instruction
1.8.1	In the navigation pane of the **EC2 Management Console**, click **Volumes**.
1.8.2	Select the **Small Volume** that is currently attached to your Web Server instance.
1.8.3	In the **Actions** menu, click **Create Snapshot**.
1.8.4	In the **Create Snapshot** dialog box, use the following values: • **Name: Asperatus data**
1.8.5	Click **Create** to create a snapshot of the Small Volume.
1.8.6	In the **Create Snapshot** dialog box, click **Close**. You can now use this snapshot to create a new, larger EBS volume.
1.8.7	In the navigation pane of the **EC2 Management Console**, click **Snapshots**. This will display all your EBS snapshots.
1.8.8	Select the **Asperatus data** snapshot that you created previously.

1.8.9	In the **Actions** menu, click **Create Volume**.
1.8.10	In the **Create Volume** dialog box, use the following values: • **Type: General Purpose (SSD)** • **Size (GiB): 20** • **Availability Zone:** Select the same availability zone that you identified in step 1.5.2 **Note**: You are now creating a 20GiB volume using the **Asperatus data** snapshot. You might remember that the original source volume (**Small Volume**) is only 10GiB.
1.8.11	Click **Create** to create the new volume from the Snapshot.
1.8.12	In the **Create Volume** dialog box, click **Close**. The new, larger volume can now be attached to an EC2 instance.
1.8.13	First name the new volume so it is easy to identify. In the navigation pane of the **EC2 Management Console**, click **Volumes**.
1.8.14	Select the new **20GiB volume**.
1.8.15	In the **Actions** menu, select **Add/Edit Tags**.
1.8.16	In the **Add/Edit Tags** dialog box, click **Create Tag**.
1.8.17	Use the following values to create a new tag for the 20GiB volume: • **Key: Name** • **Value: Large Volume**
1.8.18	Click **Save**. The name **Large Volume** will now appear in the **Name** column of the 20GiB volume.

1.8.19	You can now attach the new EBS volume to your Amazon EC2 instance. Select the **Large Volume** that you just created. **Note**: Make sure only the 20GiB volume is selected.
1.8.20	In the **Actions** menu, click **Attach Volume**.
1.8.21	In the **Attach Volume** dialog box, click in the **Instance** field and select your **Web Server** instance.
1.8.22	Click **Attach**. This will attach the Large Volume to the Web Server instance.
1.8.23	Return to the Remote Desktop Connection session to the Web Server instance that you previously established.
1.8.24	In the RDP session, click the **Server Manager** icon in the taskbar. 
1.8.25	In the **Server Manager** window, in the **Tools** menu, click **Computer Management**.
1.8.26	In the **Computer Management** window, in the left navigation pane, click **Disk Management**.
1.8.27	You will notice the 20GiB EBS volume is added as Disk 2 and is in an offline state. In order to use this disk, you will first need to bring it online. Right-click **Disk 2** and click **Online**. 

1.8.28	You will notice that Disk 2 (Large Volume) was added only as a 10GB volume and the remaining 10GB is unallocated. This is normal behavior. To help Windows recognize the entire 20GB volume, you must extend the volume. Right-click **New Volume (E:)** and click **Extend Volume…**  
1.8.29	In the **Extend Volume Wizard**, accept the default values (click **Next** two times) and click **Finish**. Disk 2 is now available as a new drive (E:) of 20GB size.
1.8.30	Close the **Computer Management** window and the **Server Manager** window.
1.8.31	Launch Windows Explorer and navigate to the new drive (E:) that you just added. 
1.8.32	You will notice that the new drive (E:) contains the Asperatus folder you created earlier on the Small Volume (D:). This folder was copied into the snapshot, and then restored when you created the Large Volume from that snapshot.
1.8.33	Close the Remote Desktop Connection session to the Web Server instance.

1.8.34	**Congratulations!** You now have successfully: • Created an EC2 key pair and a security group to allow remote access to an Amazon EC2 instance. • Launched an Amazon EC2 Windows Instance. • Activated Termination Protection for an Amazon EC2 instance. • Created EBS volumes and snapshots.
1.8.35	Close the **AWS Management Console** window or tab.
1.8.36	On the qwikLABS page, click **End** to end your lab session.

Lab 3: Elastic Load Balancing

Overview	**Elastic Load Balancing** is used to distribute incoming application traffic across multiple Amazon EC2 instances. It enables you to achieve even greater fault tolerance in your applications, seamlessly providing the amount of load balancing capacity needed in response to incoming application traffic. In this lab you will create an elastic load balancer for HTTP traffic.

Objectives	After completing this lab, you will be able to: • Create a load balancer for HTTP traffic. • Test the load balancer configuration.

Pre-requisites	This lab requires: • Access to a notebook computer with Wi-Fi running Microsoft Windows, Mac OS X, or Linux (Ubuntu, SuSE, or Red Hat). ○ **Note** The qwikLABS lab environment is not accessible using an iPad or tablet device, but you can use these devices to access the student guide. • For Microsoft Windows users: Administrator access to the computer. • An Internet browser such as Chrome, Firefox, or Internet Explorer 9 (previous versions of Internet Explorer are not supported).

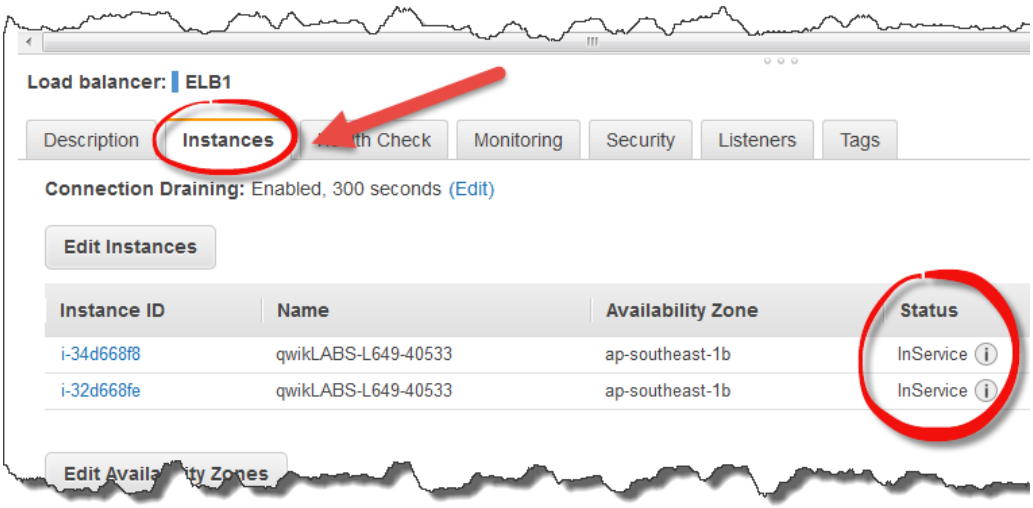
Command Reference File	At various points, this lab will instruct you to copy and paste text as part of lab procedures. This text should be copied from the lab's associated **command reference file**, which is available on the Instructions tab of your lab in qwikLABS. It is not recommended to copy and paste text from this lab manual, as the manual's rich formatting may inject characters that cannot properly be parsed by the command line

Scenario	As the operations-focused individual in the start-up business, you previously configured some Amazon S3 buckets and a pair of EC2 instances in preparation for your website. Now, it is time to tie your Amazon EC2 instances together using the Elastic Load Balancing service for traffic distribution and high availability.

Task 1-1: Elastic Load Balancing Basics	
Overview	Two web servers are already running in Asperatus Tech's environment. In this procedure you will create and configure a load balancer to serve traffic to these two web servers.

Step	Instruction
1.1.1	Log in to your **AWS Management Console**. Use the instructions in **Appendix A** of this lab manual to log in to the AWS Management Console using the pre-configured student account.
1.1.2	In the **AWS Management Console**, in the **Services** menu, click **EC2**.
1.1.3	In the navigation pane of the **EC2 Management Console**, click **Load Balancers**.
1.1.4	Click **Create Load Balancer**.
1.1.5	In the **Create Load Balancer** wizard, on the **Step 1: Define Load Balancer** page, use the following values: • **Load Balancer name: ELB1**
1.1.6	Click **Next: Assign Security Groups**.
1.1.7	On the **Step 2: Assign Security Groups** page, use the following values: • **Assign a security group: Create a new security group** • **Security group name: HTTP Only** • **Type: HTTP** • **Source: Anywhere**
1.1.8	Click **Next: Configure Security Settings**.

1.1.9	On the **Step 3: Configure Security Settings** page, click **Next: Configure Health Check**.
1.1.10	On the **Step 4: Configure Health Check** page, use the following values: • **Ping Protocol: TCP** • **Health Check Interval: 6** • **Healthy Threshold: 2**
1.1.11	Click **Next: Add EC2 Instances**.
1.1.12	On the **Step 5: Add EC2 Instances** page, select both the EC2 instances. **Note**: Make sure you selected both the instances to add to the load balancer.
1.1.13	Click **Next: Add Tags**.
1.1.14	On the **Step 6: Add Tags** page, click **Review and Create.**
1.1.15	On the **Step 7: Review** page, review the settings. To create the load balancer, click **Create**.
1.1.16	Once your load balancer is created successfully, in the **Load Balancer Creation Status** page, click **Close**. Your load balancer will now appear in the console.
1.1.17	Select **ELB1** in the list.

1.1.18	In the bottom pane, click **Instances** tab to view the status of the instances. You must now wait until the instances have a status of **InService**. **Hint**: Click the icon to refresh the pane and get the latest status.  **Note**: If the instances have a status of OutOfService, point to the icon to see the details: • An *Instance registration is still in progress* message implies that the load balancer is still starting. Wait until the status changes. • If you receive a *health check message*, check your Health Check configuration or ask your instructor for assistance.
1.1.19	Click the **Description** tab.
1.1.20	In the **Description** tab, copy the **DNS Name** value to a text editor such as Notepad.
1.1.21	In the text editor, delete **(A Record)** at the end of the DNS Name. **Note**: Your DNS Name should now end with **amazonaws.com**.

1.1.22	Copy the modified DNS name from the text editor and browse to it using a web browser. **Note**: Make sure you are using the modified DNS name, ending with **amazonaws.com**. If the page returns a DNS error and does not display, this is likely because the DNS name for the load balancer is not registered yet in the global DNS system. Wait a few minutes, and then refresh the page. You should see a Web page being served from one of the instances. The page will display details about the instance that is serving the request, including its public IP address and the instance ID.
1.1.23	**Congratulations!** You now have successfully: • Created a load balancer to load balance HTTP traffic to your application. • Tested the load balancer configuration.
1.1.24	Close the **AWS Management Console** window/page**.**
1.1.25	On the qwikLABS page, click **End** to end your lab session.

Lab 4: Amazon RDS Driven Application

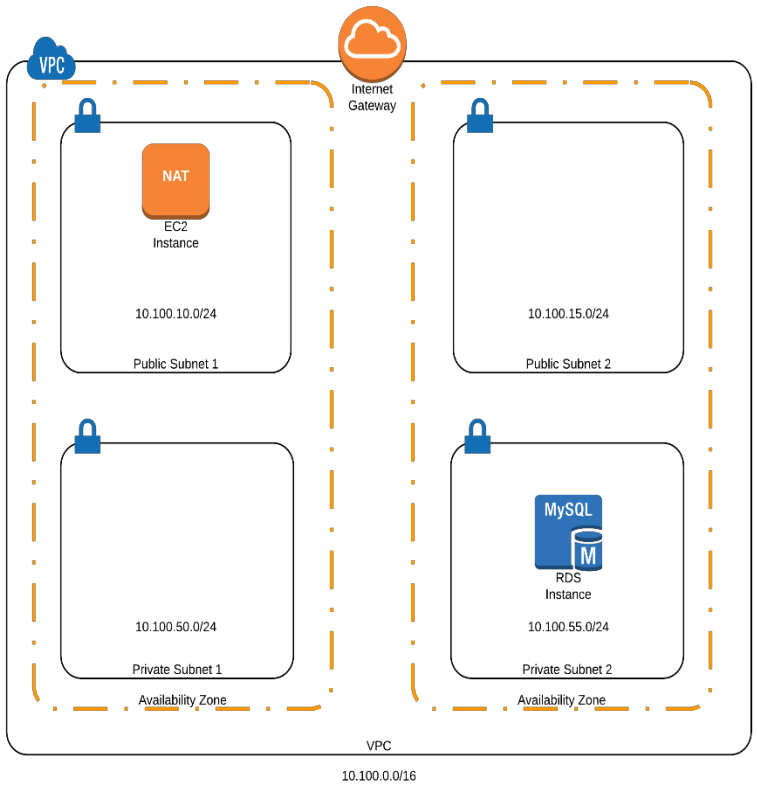
Overview	**Amazon Relational Database Service** (Amazon RDS) is a web service that makes it easy to set up, operate and scale a relational database in the cloud. In this lab you will be using Amazon RDS to launch a MediaWiki application. This is a free software open source wiki package written in PHP, originally for use on Wikipedia.

Objectives	After completing this lab, you will be able to: • Create an Amazon RDS instance. • Install an application on an Amazon EC2 instance. • Create an Amazon EC2 Security Group. • Create and use an Amazon S3 bucket for the application. • Launch the application.

Pre-requisites	This lab requires: • Access to a notebook computer with Wi-Fi running Microsoft Windows, Mac OS X, or Linux (Ubuntu, SuSE, or Red Hat). ○ **Note** The qwikLABS lab environment is not accessible using an iPad or tablet device, but you can use these devices to access the student guide. • For Microsoft Windows users: Administrator access to the computer. • An Internet browser such as Chrome, Firefox, or Internet Explorer 9 (previous versions of Internet Explorer are not supported).

Command Reference File	At various points, this lab will instruct you to copy and paste text as part of lab procedures. This text should be copied from the lab's associated **command reference file**, which is available on the Instructions tab of your lab in qwikLABS. It is not recommended to copy and paste text from this lab manual, as the manual's rich formatting may inject characters that cannot properly be parsed by the command line

Scenario	Your company wants to launch a public Wiki page to keep your customers informed and to give them the ability to edit, share, and voice their opinion and feedback. You have an application and some graphics you want to use and will be leveraging Amazon RDS, Amazon EC2, and Amazon S3 to get this new Wiki page up and running. The lab already has the script you need to get started as well as an Amazon EC2 and RDS instance. Below is a diagram showing the current state of your lab environment.



Task 1-1: Amazon RDS Instance	
Overview	In this section you will open the Amazon RDS instance that was created as part of the lab setup and copy the endpoint so you can use it for launching your MediaWiki application.

Step	Instruction
1.1.1	Log in to your **AWS Management Console**. Use the instructions in **Appendix A** of this lab manual to log in to the AWS Management Console using the pre-configured student account.
1.1.2	In the **AWS Management Console**, in the **Services** menu, click **RDS**.
1.1.3	In the navigation pane of the **RDS Console**, click **Instances**.
1.1.4	Click the **DB Instance** name to get more details about the instance.
1.1.5	In the details pane, copy the **Endpoint** to a text editor such as Notepad. The endpoint you copy should look similar to this: `qrmtnn51rjfpf0.cuf6s0ky2hzw.ap-southeast-1.rds.amazonaws.com:3306` **Note**: If your Endpoint says “Not available yet”, please wait for a few minutes and then refresh the page until the Endpoint is displayed.
1.1.6	In the text editor**, delete** the **:3306** at the end of the endpoint. Your endpoint should now end with **rds.amazonaws.com**. The modified endpoint should look similar to this: `qrmtnn51rjfpf0.cuf6s0ky2hzw.ap-southeast-1.rds.amazonaws.com`

1.1.7	Save the text file using the name **Modified RDS Endpoint** on your local machine.
1.1.8	Copy the entire contents of the **Command Reference File** for this lab to a text editor such as Notepad. In subsequent procedures, we will refer to this text as *the user data text*.
1.1.9	In the user data text, replace **<RDS ENDPOINT>** with the modified RDS endpoint from Step 1.1.6. **Note**: Make sure to delete the brackets around the endpoint.
1.1.10	In the user data text, your **RDS_ENDPOINT** variable should look similar to this: `RDS_ENDPOINT="qrmtnn51rjfpf0.cuf6s0ky2hzw.ap-southeast-1.rds.amazonaws.com"` **Note**: Make sure there is no **:3306** at the end of the endpoint, and the endpoint is enclosed in double quotes ("…").
1.1.11	In the user data text, do **NOT** edit anything else other than the RDS_ENDPOINT variable.
1.1.12	Keep the text editor window open as you will use this modified user data text in the next lab procedure.

Task 1-2: Launching an Amazon EC2 Instance	
Overview	In this procedure, you will create a new Amazon EC2 instance to install and run your MediaWiki application. As part of the instance creation, you will download and install the application, create a database on RDS, and configure your application to use the database.

Step	Instruction
1.2.1	In the **AWS Management Console**, in the **Services** menu, click **EC2**.
1.2.2	In the navigation pane of the **EC2 Management Console**, click **Instances**.
1.2.3	Click **Launch Instance**.
1.2.4	On the **Step 1: Choose an Amazon Machine Image (AMI)** page, select the first **Amazon Linux AMI** in the list by clicking **Select**.
1.2.5	On the **Step 2: Choose an Instance Type** page, make sure that **t2.micro** is selected.
1.2.6	Click **Next: Configure Instance Details**.
1.2.7	On the **Step 3: Configure Instance Details** page, use the following values: • **Network**: Select the VPC named **Lab VPC**. • **Subnet**: Select a subnet that starts with the name **Public Subnet**. • **Auto-assign Public IP**: **Enable** This will create your EC2 instance in the VPC called **Lab VPC**, which was built for you as part of your lab environment.
1.2.8	Scroll down the page and click **Advanced Details**.

1.2.9	Next, you will supply a user data field to the Amazon EC2 instance. In the **User data** section: • Verify that the **As text** radio button is checked. • **Paste the modified user data text,** from step 1.1.12, in the user data textbox. This text installs any necessary updates for the operating system; installs Apache, PHP, and MySQL client; downloads and installs the MediaWiki application; creates a database in RDS; and configures the database for your application.
1.2.10	Make sure you copied the modified user data text from step 1.1.12. The **RDS_ENDPOINT** variable in the text should look similar to this: `RDS_ENDPOINT="qrmtnn51rjfpf0.cuf6s0ky2hzw.ap-southeast-1.rds.amazonaws.com"` **Note**: Make sure there is no **:3306** at the end of the endpoint, and the endpoint is enclosed in double quotes ("…").
1.2.11	Click **Next: Add Storage**.
1.2.12	On the **Step 4: Add Storage** page, keep the default values and click **Next: Tag Instance**.
1.2.13	On the **Step 5: Tag Instance** page, use the following values to create a new tag: • **Key**: **Name** • **Value**: **Wiki**
1.2.14	Click **Next: Configure Security Group**.
1.2.15	In this step, you will configure a security group to allow you to access the Wiki EC2 instance using a Secure Shell (SSH) connection. On the **Step 6: Configure Security Group** page, use the following values: • **Assign a security group**: Select **Create a new security group** • **Security group name**: **Wiki Security Group**

1.2.16	Leave the default SSH rule as is. This will create a rule that allows Secure Shell (SSH) access from any location. **Note:** This security configuration is being used for lab purposes only, and is not recommended for use in a production environment. It is **highly recommended** that you restrict terminal access to the ranges of IP addresses (e.g., IPs assigned to machines within your company) that have a legitimate business need to administrate your Amazon EC2 instance.
1.2.17	Click **Add Rule** to add a second rule.
1.2.18	Specify the following values to add a rule enabling HTTP access to your instance: • **Type: HTTP** • **Source: Anywhere** This rule will allow HTTP requests from anywhere on the Internet. Since we want our Wiki server to be accessible to the general public, we can leave this rule as is without any further configuration.
1.2.19	Make sure the Security Group has two rules: one for SSH and one for HTTP.
1.2.20	Click **Review and Launch**.
1.2.21	On the **Step 7: Review Instance Launch** page, review the configuration for your instance. When done, click **Launch**.
1.2.22	You will now see a dialog named **Select an existing key pair or create a new key pair**. Whenever you create a new Amazon EC2 instance, you associate a key pair with the instance. You use the private key portion of your key pair in order to gain secure access to your instance using SSH/RDP. A key pair has already been created for you as part of your qwikLABS environment. To associate it with your new instance, use the following values: • First dropdown (unlabeled): Select Choose an existing key pair. • **Select a key pair**: Select the key pair that begins with the string qwikLABS-. • **I acknowledge that I have access to…**: Enable this checkbox.

1.2.23	Click **Launch Instances**.
1.2.24	On the **Launch Status** page, click **View Instances** (you might need to scroll down to find it). Observe the **Status Checks** field of your Wiki instance until it shows that both status checks have completed successfully. **Hint**: Click the  icon to refresh the pane and get the latest status.
1.2.25	Make sure your **Wiki** instance has launched completely before you move to the next lab procedure i.e. the two status checks for the instance must have completed successfully.

Task 1-3: Viewing Your Application	
Overview	In this procedure, you will access your MediaWiki application that is running in the Amazon EC2 instance, Wiki.

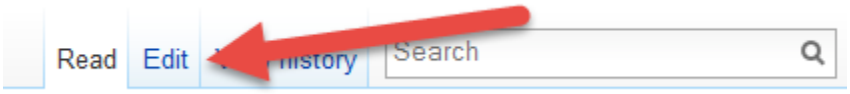
Step	Instruction
1.3.1	In the navigation pane of the **EC2 Management console**, click **Instances**.
1.3.2	Select the **Wiki** instance that you created previously. **Note**: Make sure only the Wiki instance is selected.
1.3.3	In the **Description** tab, copy the **Public IP** value to a text editor.
1.3.4	In the text editor, add **`/mediawiki`** to the end of the Public IP address. **Note**: Your URL should look similar to this: `11.22.33.44/mediawiki`
1.3.5	Copy the URL from the text editor and browse to it using a web browser. **Note**: Your URL should look similar to this: `11.22.33.44/mediawiki`
1.3.6	You will now see your MediaWiki application launched. In the next lab procedure, you will modify this webpage to use images from an Amazon S3 bucket. **Note**: Do not close the MediaWiki webpage as you will use it later.

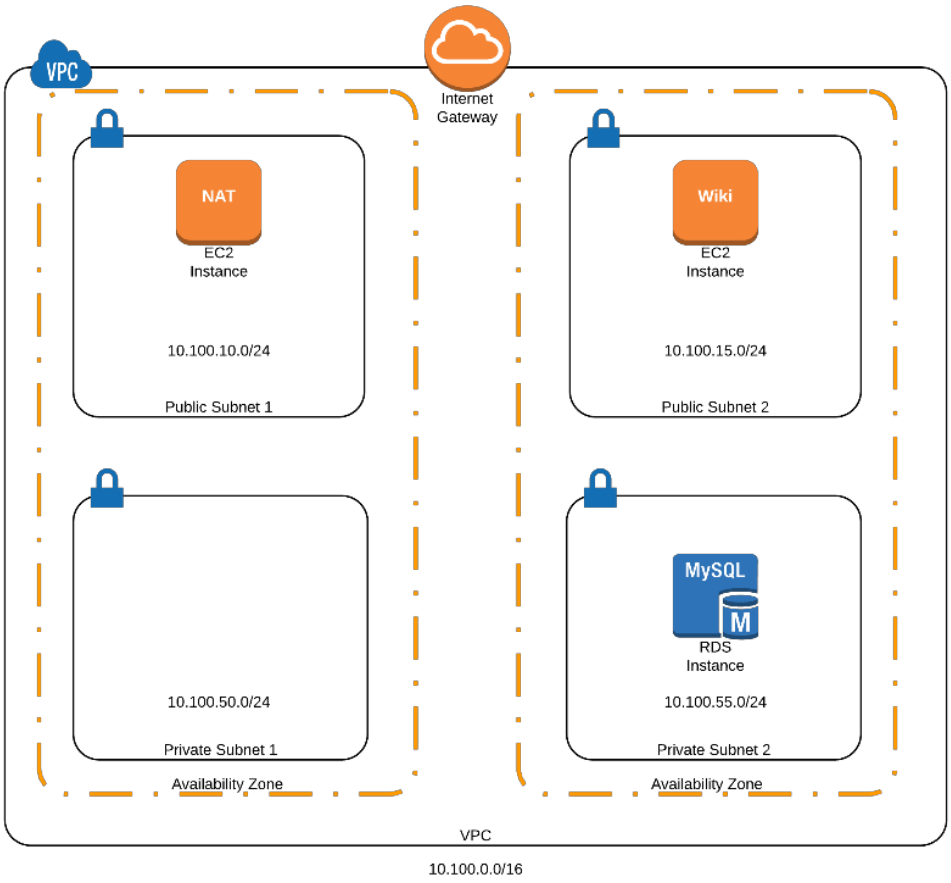
Task 1-4: Create an Amazon S3 Bucket and Upload an Object (Optional)	
Overview	If you have time and want to take this lab to the next step, follow the directions below to modify the User Interface of your application (MediaWiki) by adding a custom graphic. You can store graphics and other content for your application in an Amazon S3 bucket. In this procedure, you will create an Amazon S3 bucket to host your application graphics. Then, you will upload an image to this bucket and make it accessible to your application. In the next task, you will access this image from your MediaWiki site. **Note**: If you would like to skip this task and use an image that is already available in our training bucket skip to Task 1-5.

Step	Instruction
1.4.1	In the **AWS Management Console**, in the **Services** menu, click **S3**.
1.4.2	Click **Create Bucket** to create a new bucket.
1.4.3	In the **Create a Bucket – Select a Bucket Name and Region** dialog box, enter the following values: • **Bucket Name**: Type a bucket name that will be unique across Amazon S3. We recommend that you name your bucket with your initials and today's date to ensure uniqueness. This value will be referred to as *s3-bucket-name* in subsequent procedures. • **Region**: Choose a region closest to your location. If unsure, choose **Oregon**.
1.4.4	Click **Create**.
1.4.5	In the **S3 Console**, click the name of your bucket to view its contents. You will receive a message indicating that the bucket is empty.

1.4.6	Click **Upload** to add a new file object to your bucket.
1.4.7	In the **Upload – Select Files and Folders** dialog box, click **Add Files**.
1.4.8	Select a picture (e.g. picture from My Pictures folder) from your local machine. You will make this picture available on your MediaWiki webpage. **Note**: We will refer to this uploaded file as *the object* in subsequent procedures
1.4.9	Click **Start Upload**. You can see the progress of the upload in the **Transfers** pane.
1.4.10	In the **S3 Console**, right-click the object and click **Make Public**. **Note**: Objects in S3 are Private by default.
1.4.11	Click **OK** on the dialog box to confirm.
1.4.12	Click **Properties**.
1.4.13	In the **Object Properties** pane, copy the **Link** to a text editor like Notepad. Using this URL, you can access this object from anywhere on the Internet. **Note**: Make sure the URL does **NOT** have a Lock icon next to it. You will use this URL in the next lab procedure to add this picture to your MediaWiki webpage.

Task 1-5: Modifying Your Application	
Overview	Once you have your Amazon S3 URL for the graphic, you can modify your MediaWiki application to include that.

Step	Instruction
1.5.1	Make sure you have your Amazon S3 URL for the graphic you would like to add to your application. **Note**: If you did not complete Task 1-4, you can use an image that is already available in our training bucket. Copy the following URL for the image: https://d2lrzjb0vjvpn5.cloudfront.net/tech-essentials/v3.6-en/lab-4-rds/static/aws-training-and-certification.png
1.5.2	On your **Wiki** page, click **Edit**.  **Note**: If you need to open the Wiki page again, refer to Task 1-3.
1.5.3	In the **Editing Main Page** section, paste the Amazon S3 URL at the bottom of the text box.
1.5.4	Click **Save page** to save your changes**.**
1.5.5	You should now see your customized MediaWiki page with the picture from your S3 bucket. **Congratulations!** You have successfully launched your MediaWiki application using Amazon RDS and Amazon S3.

1.5.6	Below is a diagram of your lab environment at the completion of the lab procedures. 
1.5.7	Close the **AWS Management Console** window/tab.
1.5.8	On the qwikLABS page, click **End** to end your lab session.

Appendix A: Logging in to the AWS Management Console

Introduction	In this appendix, you will learn how to log in to the student account created for you as part of this course.

About Student Accounts	Each lab in this course has a corresponding lab environment that is launched from the qwikLABS page. (Your instructor should have already supplied you with instructions for creating a qwikLABS account.) Whenever you launch a new lab, the qwikLABS environment creates a new AWS account for you. Within this AWS account, it creates an IAM user named **awsstudent**. When you terminate your lab, this account is recycled, and all resources associated with it are terminated. Each time you start a new lab in this course, you will need to log in to your new lab environment as the user **awsstudent**, using the automatically-generated password provided for you on the qwikLABS page for that specific lab.

Step	Instruction
1	From the Class Lab page in qwikLABS, find the current lab, and click **Start Lab**.
2	On the lab page, wait until the text **Create in Progress...** disappears from the screen. For some labs, this may happen instantly; for other labs, it may take anywhere from five to 10 minutes for your lab to initialize. **Note**: Make sure to wait until the lab creation process has completed before you move on to the next step.
3	Near the bottom of the screen, find the **Lab Connection** section of the page. Below the text **AWS Management Console**, you will see the fields **User Name** and **Password**. These are your AWS account credentials. Select and copy the **Password** field.
4	Click **Open Console**. This will open the AWS Management Console, pre-populating it with the AWS account ID created for you by qwikLABS. **Note:** You can right-click on this button and use your Web browser's "open in new tab" function to prevent this page from opening in a separate window.
5	On the new window or tab containing the AWS Management Console, you should see the Account ID already filled in. In the Username field, type **awsstudent**. In the Password field, paste the password that you copied from Step 3. Finally, click the **Sign In** button. **Note**: On rare occasions, the Account ID on your signing page may be blank. Consult your instructor for assistance on how to locate your qwikLABS account ID.