Dr. D. Y. Patil Pratishthan's

DR. D. Y. PATIL INSTITUTE OF ENGINEERING, MANAGEMENT & RESEARCH

Approved by A.I.C.T.E, New Delhi , Maharashtra State Government, Affiliated to Savitribai Phule Pune University
Sector No. 29, PCNTDA , Nigidi Pradhikaran, Akurdi, Pune 411044. Phone: 020–27654470, Fax: 020-27656566
Website :www.dypiemr.ac.in Email : principal.dypiemr@gmail.com

---

Department of Artificial Intelligence and Data Science

LAB MANUAL
Cyber Security
(TE)
Semester II

Prepared by:
Mrs. Sneha Kanawade

Mini Project(Cyber Security) Laboratory

Course Code	Course Name	Teaching Scheme (Hrs./ Week)	Credits
317536	Mini Project(Cyber Security)	2	1

Course Objectives:

- To understand threats/vulnerabilities to networks and countermeasures.
- To provide understanding of cryptography and its applications.
- To explain various approaches to Encryption techniques.
- To understand working of firewall and IDs.

Course Outcomes:

On completion of the course, learner will be able to–

- CO1: Identify basic security attacks and services.
- CO2: Analyze the vulnerabilities and design a security solution.
- CO3: Implement symmetric and asymmetric key algorithms.
- CO4: Demonstrate network security applications, Firewall, IDs.

Operating System recommended: 64-bit Open source Linux or its derivative

Table of Contents

Lab Assignment No.	1
Title	Implementation of S-DES
Roll No.	
Class	TE
Date of Completion	
Subject	Mini Project(Cyber Security)
Assessment Marks	
Assessor's Sign	

ASSIGNMENT No: 01

Title: Implementation of S-DES (Data Encryption Standard)

Problem Statement: Implementation of S-DES

Prerequisite:

Basics of Computer networking and Python

Software Requirements:

Python 3

Hardware Requirements:

PIV, 2GB RAM, 500 GB HDD

Learning Objectives:

Learn Data Encryption Standard Algorithm (DES)

Outcomes:

After completion of this assignment students are able to understand the Data Encryption Standard.

Theory:

Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a Symmetric-key block cipher issued by the national Institute of Standards & Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration −

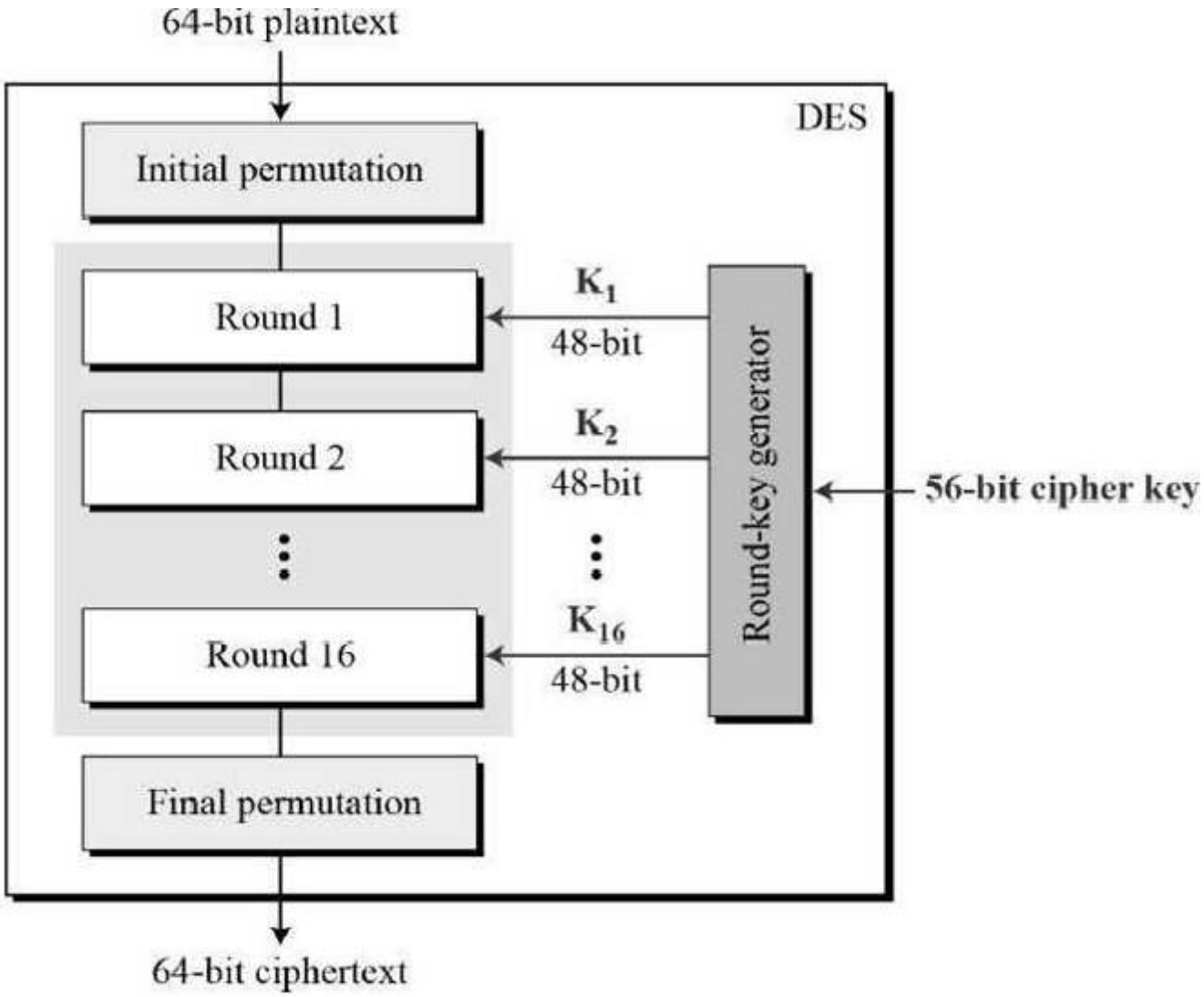


Figure 5.1: General Structure of DES

Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows

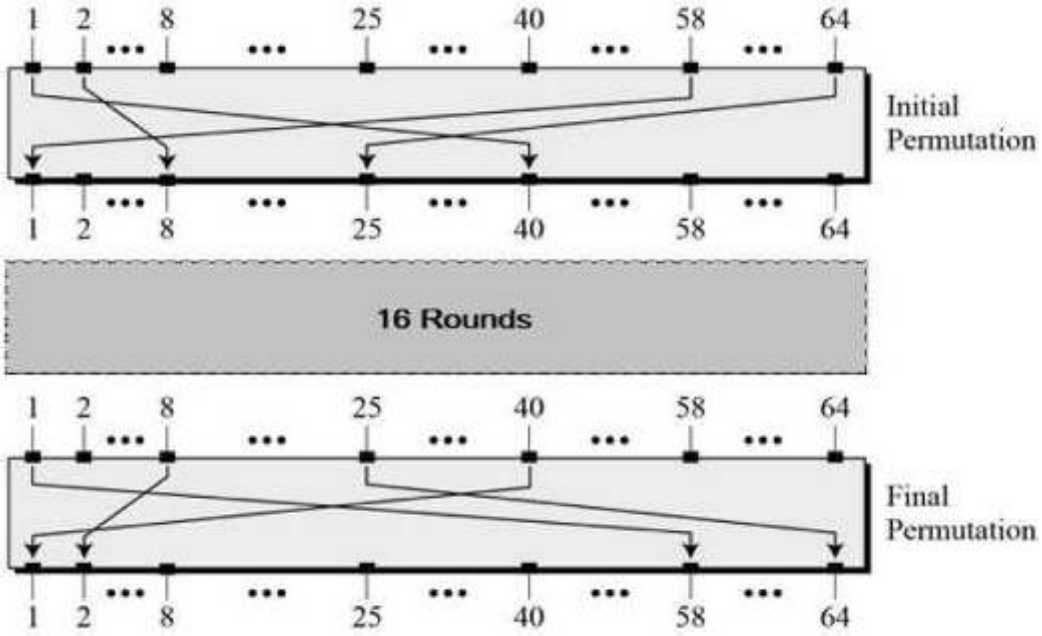


Figure 5.2 initial and final permutations

Round Function

The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

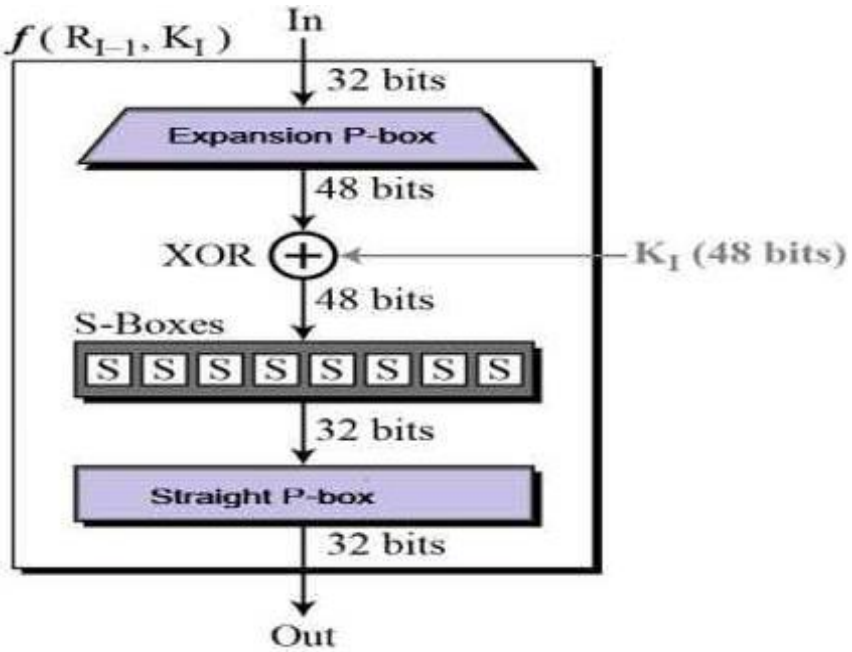
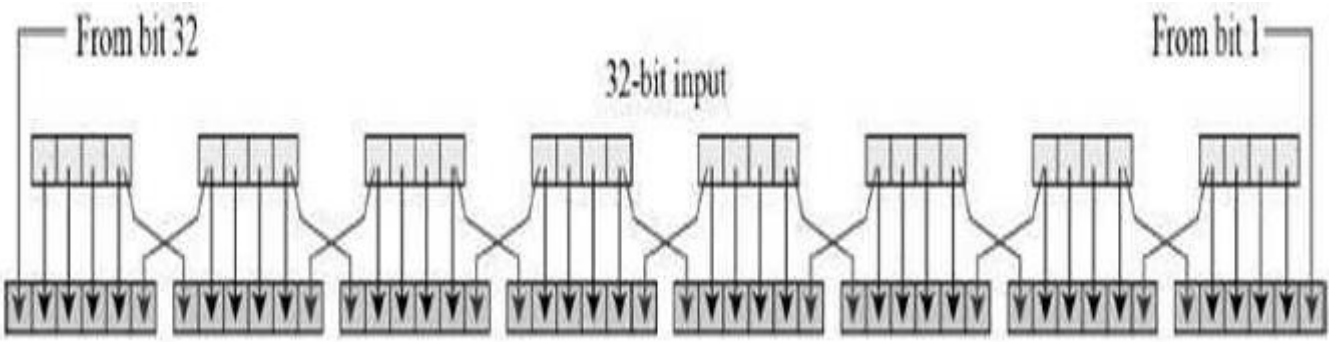


Figure 5.3 Round Functions

Expansion Permutation Box

Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits.



Permutation logic is graphically depicted in the following illustration:

Figure 5.4 Permutation logic

The graphically depicted Permutation logic is generally described as table in DES specification illustrated as shown:

Table 5.1 Permutation logic

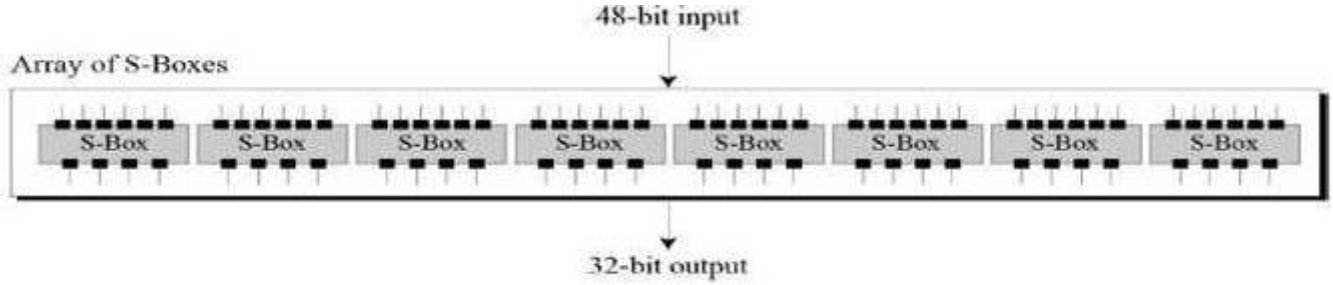
32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

XOR(Whitener)

After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.

Substitution Boxes

The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and



a 4-bit output. Refer the following illustration –

Figure 5.5 S-Boxes

The S-box rule is illustrated below –

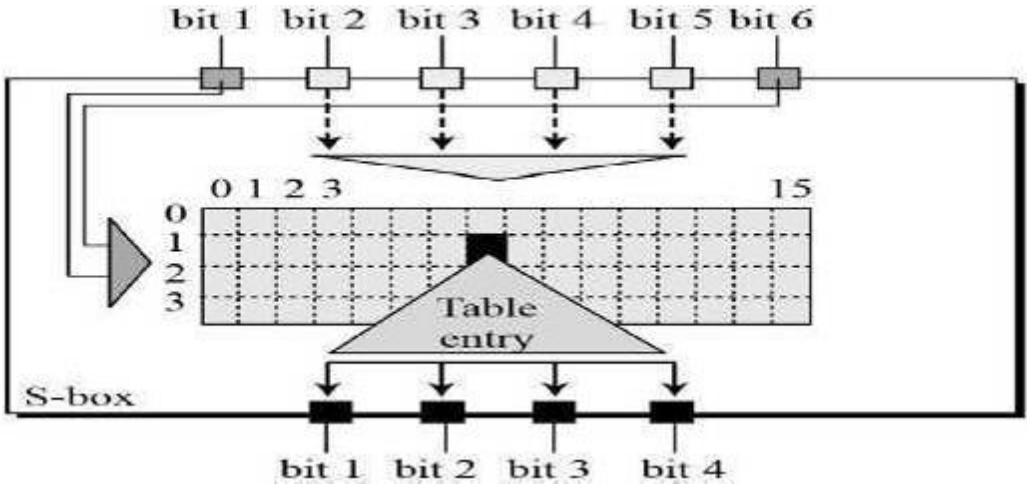


Figure 5.6 S-Box Rules

There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.

Straight Permutation − The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration:

Table 5.2 Straight Permutation

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration −

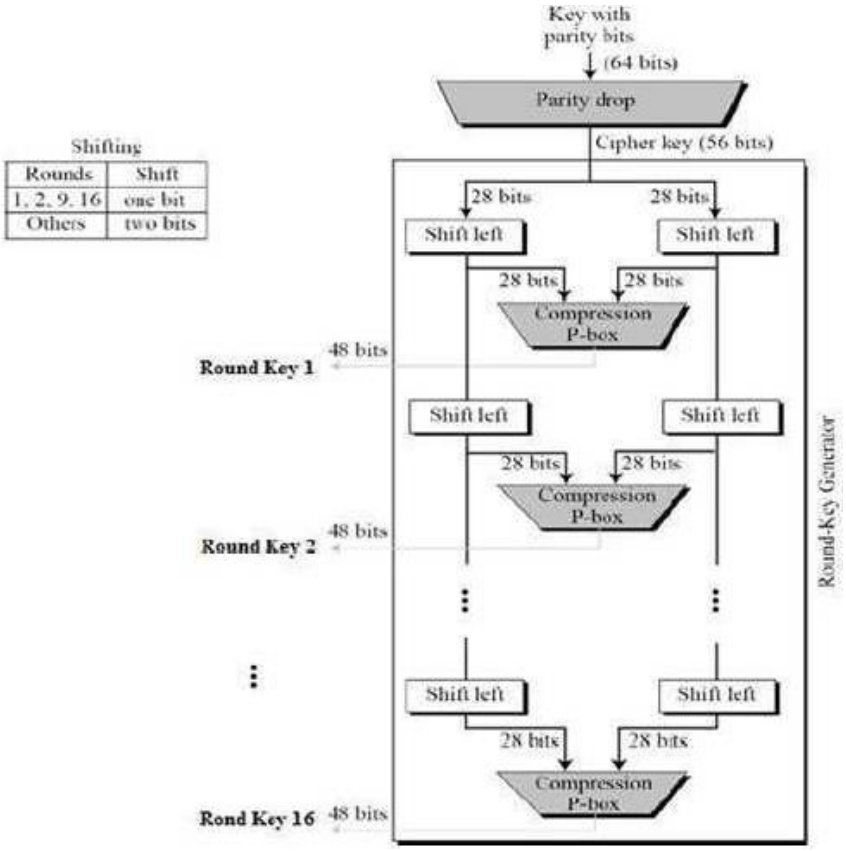


Figure 5.7 the process of key generation

The logic for Parity drops, shifting, and Compression P-box is given in the DES description.

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

- **Avalanche effect** − A small change in plaintext results in the very great change in the cipher text.
- **Completeness** − Each bit of cipher text depends on many bits of plaintext.

During the last few years, cryptanalysis has found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

Lab Assignment No.	2
Title	Implementation of S-AES
Roll No.	
Class	TE
Date of Completion	
Subject	Mini Project(Cyber Security)
Assessment Marks	
Assessor's Sign	

ASSIGNMENT No: 02

Title: Implementation of S-AES (Advanced Encryption Standard)

Problem Statement: Implementation of S-AES

Prerequisite:

Basic of Python3, Concept of Advanced Encryption Standard

Software Requirements:

Python 3

Hardware Requirement:

PIV, 2GB RAM, 500 GB HDD

Learning Objectives:

Learn How to Apply Advanced Encryption Standard Algorithm to encryption of given data.

Outcomes:

After completion of this assignment students are able Implement code for **Advanced Encryption Standard Algorithm** for given data and find the encrypted data of the given data.

Theory: The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details

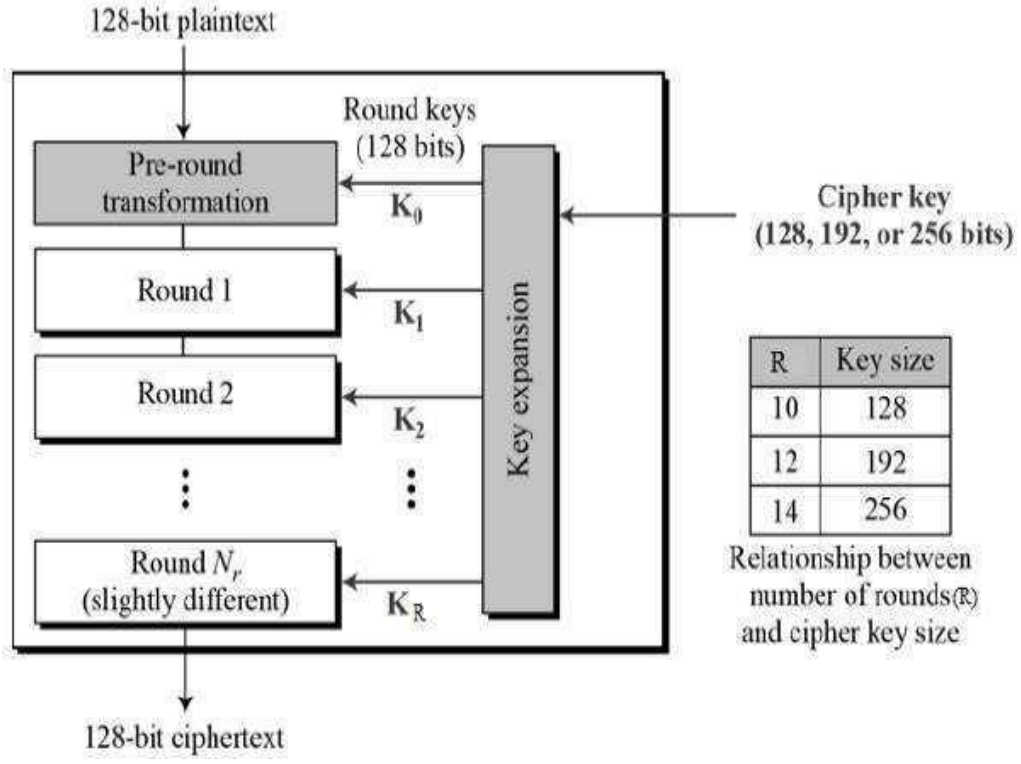
- Software implementable in C ,Java and Python

Operation of AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).
Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration −



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below −

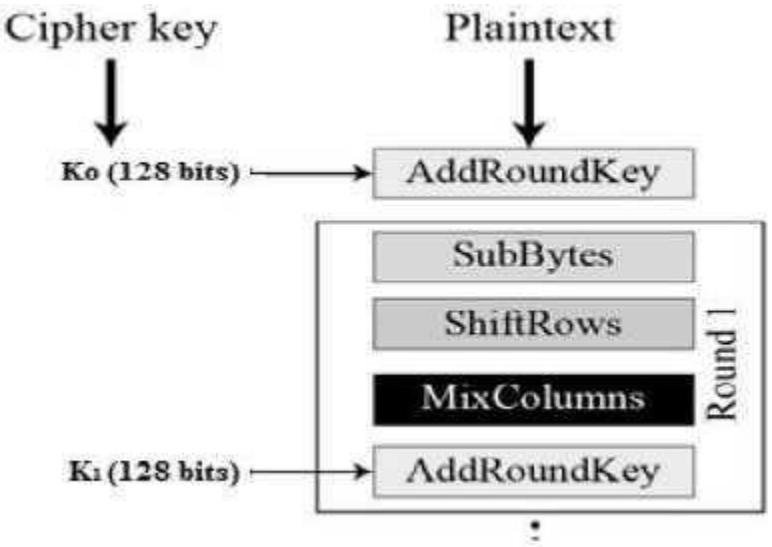


Figure 6.2 Encryption Process

Lab Assignment No.	03
Title	Implementation of Diffie-Hellman key exchange
Roll No.	
Class	TE
Date of Completion	
Subject	Mini Project(Cyber Security)
Assessment Marks	
Assessor's Sign	

ASSIGNMENT No: 03

Title: Implementation of Diffie-Hellman key Exchange (DH)

Problem Statement: Implementation of Diffie-Hellman key Exchange (DH)

Prerequisite:

Basics of Computer Networking and Python

Software Requirements:

Python 3

Hardware Requirements:

PIV, 2GB RAM, 500 GB HDD

Learning Objectives:

Learn Diffie-Hellman key Exchange (DH)

Outcomes:

After completion of this assignment students are able to understand the Diffie-Hellman key Exchange

Theory Concepts:

Diffie-Hellman key Exchange (DH)

In the mid- 1970's, Whitefield Diffie, a student at the Stanford University met with Martin Hellman, his professor &the two began to think about it. After some research & complicated mathematical analysis, they came up with the idea of AKC. Many experts believe that this development is the first & perhaps the only truly revolutionary concept in the history of cryptography.

Silent Features of Diffie-Hellman key Exchange (DH)

1. Developed to address shortfalls of *key distribution* in symmetric key distribution.
2. A *key exchange algorithm*, not an encryption algorithm
3. Allows two users to share a *secret key* securely over a public network
4. Once the key has been shared Then both parties can use it to encrypt and decrypt messages using symmetric cryptography
5. Algorithm is based on "difficulty of calculating discrete logarithms in a finite field"
6. These keys are mathematically related to each other.
7. ''Using the public key of users, the session key is generated without transmitting the private key of the users.''

Diffie-Hellman Key Exchange/Agreement Algorithm with Example

1. Firstly, Alice and Bob agree on two large prime numbers, n and g. These two integers need not be kept secret. Alice and Bob can use an insecure channel to agree on them.

   Let n = 11, g = 7.

2. Alice chooses another large random number x, and calculates A such that:
   $A = g^x \bmod n$

   Let x = 3. Then, we have, $A = 7^3 \bmod 11 = 343 \bmod 11 = 2$.

3. Alice sends the number A to Bob.

   Alice sends 2 to Bob.

4. Bob independently chooses another large random integer y and calculates B such that:
   $B = g^y \bmod n$

   Let y = 6. Then, we have, $B = 7^6 \bmod 11 = 117649 \bmod 11 = 4$.

5. Bob sends the number B to Alice.

   Bob sends 4 to Alice.

6. A now computes the secret key K1 as follows:
   $K1 = B^x \bmod n$

   We have, $K1 = 4^3 \bmod 11 = 64 \bmod 11 = 9$.

7. B now computes the secret key K2 as follows:
   $K2 = A^y \bmod n$

   We have, $K2 = 2^6 \bmod 11 = 64 \bmod 11 = 9$.

Diffie-Hellman Key exchange

1. Public values:
    - large prime p, generator g (primitive root of p)
2. Alice has secret value x, Bob has secret y

   Discrete logarithm problem: given x, g, and n, find A
3. A → B: $g^x \pmod n$
4. B → A: $g^y \pmod n$
5. Bob computes $(g^x)^y = g^{xy} \pmod n$
6. Alice computes $(g^y)^x = g^{xy} \pmod n$
7. Symmetric key= $g^{xy} \pmod n$

Limitation: Vulnerable to "man in the middle" attacks*

Man-in-the-Middle Attack:

Alice	Tom	Bob
n = 11, g = 7	n = 11, g = 7	n = 11, g = 7

Figure 7.1 Man-in-the-Middle Attack Part-I

Alice	Tom	Bob
x = 3	x = 8, y = 6	y = 9

Figure 7.2 Man-in-the-Middle Attack Part-II

Alice	Tom	Bob
$A = g^x \bmod n$ $= 7^3 \bmod 11$ $= 343 \bmod 11$ $= 2$	$A = g^x \bmod n$ $= 7^8 \bmod 11$ $= 5764801 \bmod 11$ $= 9$ $B = g^y \bmod n$ $= 7^6 \bmod 11$ $= 117649 \bmod 11$ $= 4$	$B = g^y \bmod n$ $= 7^9 \bmod 11$ $= 40353607 \bmod 11$ $= 8$

Figure 7.3 Man-in-the-Middle Attack Part-III

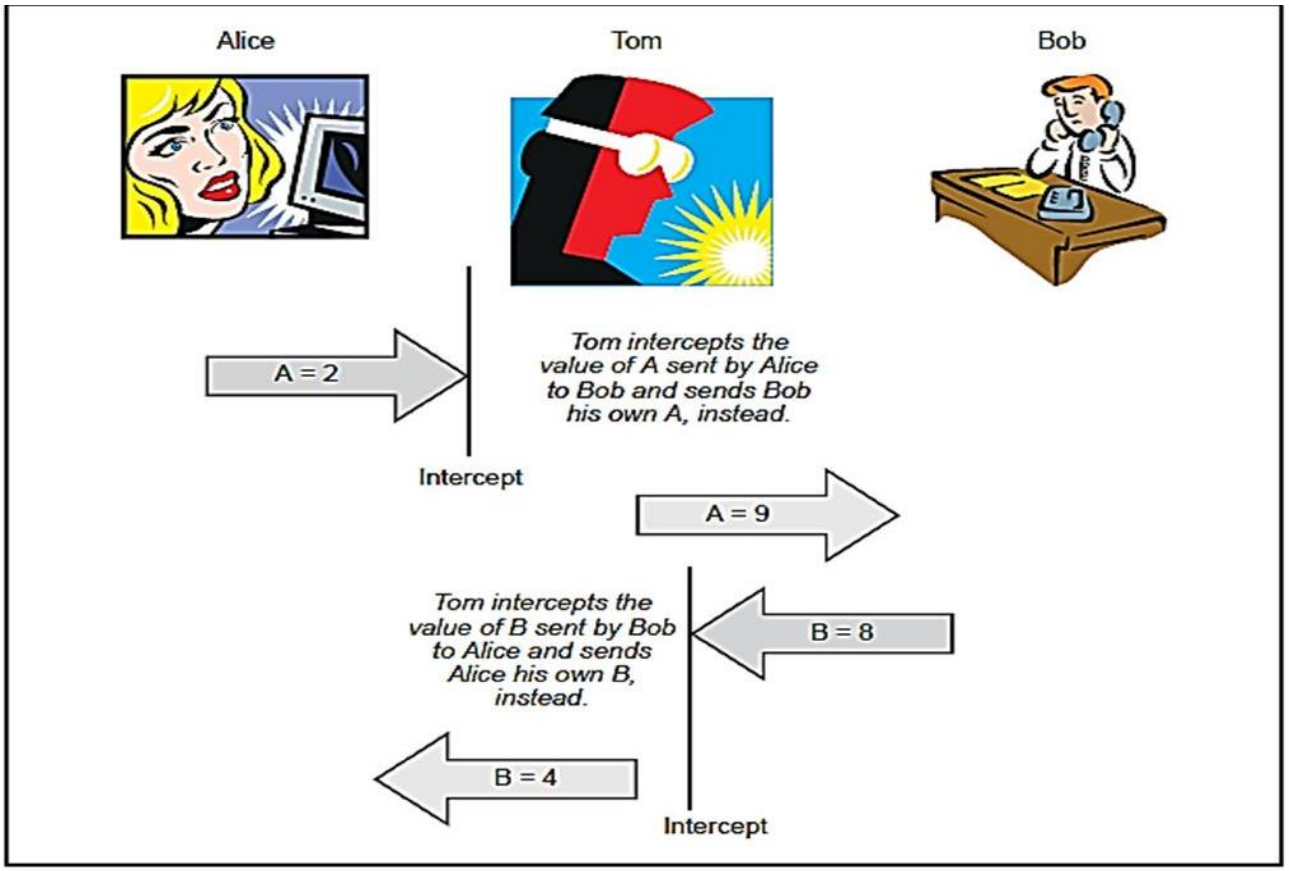


Figure 7.4 Man-in-the-Middle Attack Part-IV

Alice	Tom	Bob
A = 2, B = 4*	A = 2, B = 8	A = 9*, B = 8

(Note: * indicates that these are the values after Tom hijacked and changed them.)

Figure 7.5 Man-in-the-Middle Attack Part-V

Alice	Tom	Bob
K1 = B^x mod n	K1 = B^x mod n	K2 = A^y mod n
= 4^3 mod 11	= 8^8 mod 11	= 9^9 mod 11
= 64 mod 11	= 16777216 mod 11	= 387420489 mod 11
= 9	= 5	= 5
	K2 = A^y mod n	
	= 2^6 mod 11	
	= 64 mod 11	
	= 9	

Figure 7.6 Man-in-the-Middle Attack Part-VI

Preventing a Man-in-the-Middle Attack with Hashing

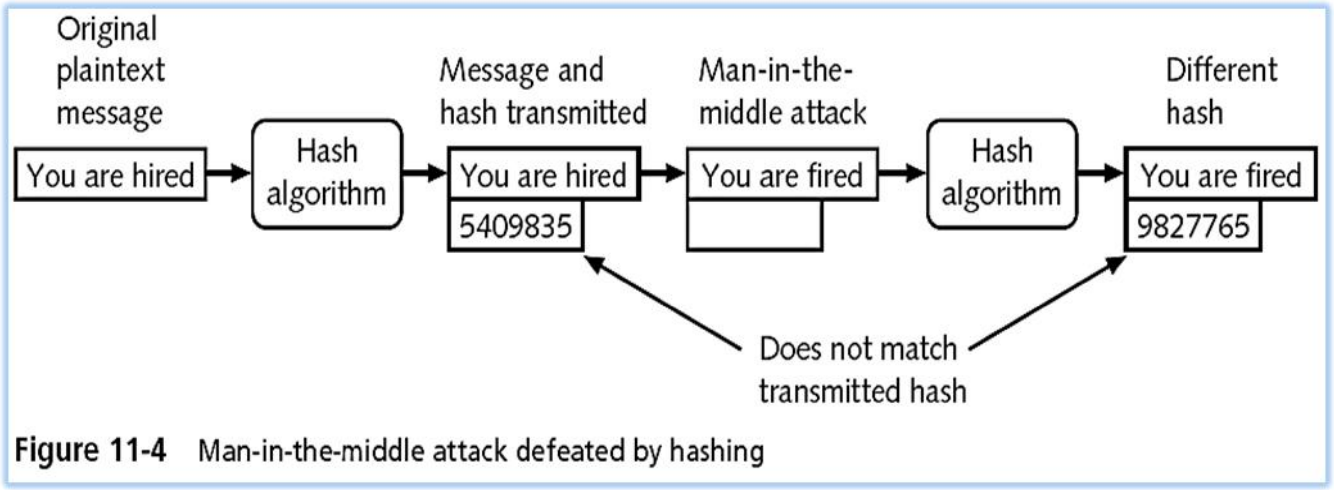


Figure 11-4 Man-in-the-middle attack defeated by hashing

Lab Assignment No.	04
Title	Implementation of RSA.
Roll No.	
Class	TE
Date of Completion	
Subject	Mini Project(Cyber Security)
Assessment Marks	
Assessor's Sign	

ASSIGNMENT No: 04

Title: Implementation of RSA.

Problem Statement: Implementation of RSA Algorithm

Prerequisite:

Basic of Python, Information security Algorithm

Software Requirements:

Python 3.7

Hardware Requirement:

2GB RAM, 500 GB HDD

Learning Objectives:

Learn RSA Algorithm

Outcomes:

After completion of this assignment students are able to understand the How asymmetric cryptographic algorithm is used

Theory Concepts:

RSA(Rivest, Shamir & Adleman)

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a large composite number is difficult: when the integers are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator.

- RSA makes the public and prívate keys by multiplying two large prime numbers *p* and *q*
    - It's easy to find & multiply large prime No. (*n*=*pq*)
    - It is very difficult to factor the number *n* to find *p* and *q*
    - Finding the private key from the public key would require a factoring operation
    - The real challenge is the selection & generation of keys.
- RSA is complex and slow, but secure
- 100 times slower than DES on s/w & 1000 times on h/w

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secures public- key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

Using an encryption key (*e*,*n*), the algorithm is as follows:

1. Represent the message as an integer between 0 and (*n*-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2. Encrypt the message by raising it to the *e*th power modulo *n*. The result is a ciphertext message C.
3. To decrypt ciphertext message C, raise it to another power *d* modulo *n*

The encryption key (*e*,*n*) is made public. The decryption key (*d*,*n*) is kept private by the user.

How to Determine Appropriate Values for *e*, *d*, and *n*

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as *p* and *q*.
2. Set *n* equal to *p* * *q*.
3. Choose any large integer, *d*, such that GCD(*d*, ((*p*-1) * (*q*-1))) = 1
4. Find *e* such that *e* * *d* = 1 (**mod** ((*p*-1) * (*q*-1)))

Rivest, Shamir, and Adleman provide efficient algorithms for each required operation[4].

How secure is a communication using RSA?

Cryptographic methods cannot be proven secure. Instead, the only test is to see if someone can figure out how to decipher a message without having direct knowledge of the decryption key. The RSA method's security rests on the fact that it is extremely difficult to factor very large numbers. If 100 digit numbers are used for *p* and *q*, the resulting *n* will be approximately 200 digits. The fastest known factoring algorithm would take far too long for an attacker to ever break the code. Other methods for determining *d* without factoring *n* are equally as difficult.

Any cryptographic technique which can resist a concerted attack is regarded as secure. At this point in time, the RSA algorithm is considered secure.

How Does RSA Works?

RSA is an **asymmetric** system, which means that a key pair will be generated (we will see how soon) , a **public** key and a **private** key , obviously you keep your private key secure and pass around the public one.

The algorithm was published in the 70's by Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman, hence RSA, and it sort of implement's a trapdoor function such as Diffie's one.

RSA is rather slow so it's hardly used to encrypt data, more frequently it is used to encrypt and pass around **symmetric** keys which can actually deal with encryption at a **faster** speed.

RSA Security:

- It uses prime number theory which makes it difficult to find out the key by reverse engineering.
- Mathematical Research suggests that it would take more than 70 years to find P & Q if N is a 100 digit number.

Algorithm

The RSA algorithm holds the following features −

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.

You will have to go through the following steps to work on RSA algorithm −

Step 1: Generate the RSA modulus

The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N, as shown −

N=p*q

Here, let N be the specified large number.

Step 2: Derived Number (e)

Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1). The primary condition will be that there should be no common factor of (p-1) and (q-1) except 1

Step 3: Public key

The specified pair of numbers **n** and **e** forms the RSA public key and it is made public.

Step 4: Private Key

Private Key **d** is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows −

ed = 1 mod (p-1) (q-1)

The above formula is the basic formula for Extended Euclidean Algorithm, which takes p and q as the input parameters.

Encryption Formula

Consider a sender who sends the plain text message to someone whose public key is **(n,e).** To encrypt the plain text message in the given scenario, use the following syntax −

C = Pe mod n

Decryption Formula

The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver **C** has the private key **d**, the result modulus will be calculated as −

Plaintext = Cd mod n

Example

1. P=7, Q=17
2. 119=7*17
3. (7-1)*(17-1)= 6*16 =96 factor 2 & 3, so E=5
4. (D*5) mod (7-1)*(17-1)=1, so D=77
5. CT=10^5 mod 119 =100000 mod 119 =40
6. Send 40
7. PT=40^{77} mod 119 = 10

Lab Assignment No.	05
Title	Implementation of ECC algorithm
Roll No.	
Class	TE
Date of Completion	
Subject	Mini Project(Cyber Security)
Assessment Marks	
Assessor's Sign	

ASSIGNMENT No: 05

Title: Implementation of ECC algorithm

Problem Statement: Implementation of ECC algorithm

Prerequisite:

Basic of Python, Information security Algorithm

Software Requirements:

Python 3.7

Hardware Requirement:

2GB RAM, 500 GB HDD

Learning Objectives:

Learn ECC Algorithm

Outcomes:

After completion of this assignment students are able to understand the How ECC algorithm is used to encrypt and decrypt messages.

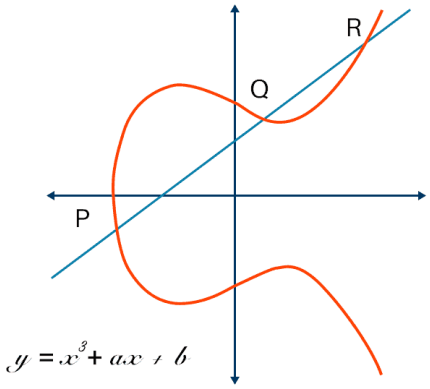
Theory:

ECC, as the name implies, is an asymmetric encryption algorithm that employs the algebraic architecture of elliptic curves with finite fields.

Elliptic Curve Cryptography (ECC) is an encryption technology comparable to RSA that enables public-key encryption.

While RSA's security is dependent on huge prime numbers, ECC leverages the mathematical theory of elliptic curves to achieve the same level of security with considerably smaller keys.

Victor Miller and Neal Koblitz separately proposed elliptic curve ciphers in the mid-1980s. On a high level, they are analogs of actual public cryptosystems in which modular arithmetic is substituted by elliptic curve operations.



Components of Elliptic Curve Cryptography

Below are the components of elliptic curve cryptography:

1. ECC keys:

- **Private key:** ECC cryptography's private key creation is as simple as safely producing a random integer in a specific range, making it highly quick. Any integer in the field represents a valid ECC private key.
- **Public keys:** Public keys within ECC are EC points, which are pairs of integer coordinates x, and y that lie on a curve. Because of its unique features, EC points can be compressed to a single coordinate + 1 bit (odd or even). As a result, the compressed public key corresponds to a 256-bit ECC.

2. Generator Point:

- ECC cryptosystems establish a special pre-defined EC point called generator point G (base point) for elliptic curves over finite fields, which can generate any other position in its subgroup over the elliptic curve by multiplying G from some integer in the range [0…r].
- The number r is referred to as the "ordering" of the cyclic subgroup.
- Elliptic curve subgroups typically contain numerous generator points, but cryptologists carefully select one of them to generate the entire group (or subgroup), and is excellent for performance optimizations in calculations. This is the "G" generator.

Elliptic Curve Cryptography Algorithms

Based on the arithmetic of elliptic curves over finite fields, Elliptic-Curve Cryptography (ECC) provides numerous sets of algorithms:

Digital signature algorithms:

- **Elliptic Curve Digital Signature Algorithm. (ECDSA):** ECDSA, or Elliptic Curve Digital Signature Algorithm, is a more highly complicated public-key cryptography encryption algorithm. Elliptic curve cryptography is a type of public key cryptography that uses the algebraic structure of elliptic curves with finite fields as its foundation. Elliptic curve cryptography is primarily used to generate pseudo-random numbers, digital signatures, and other data.
- **Edwards-curve Digital Signature Algorithm (EdDSA):** The Edwards-curve Digital Signature Algorithm (EdDSA) was proposed as a replacement for the Elliptic Curve Digital Signature Algorithm

for performing fast public-key digital signatures (ECDSA). Its primary benefits for embedded devices are higher performance and simple, secure implementations. During a signature, no branch or lookup operations based on the secret values are performed. Many side-channel attacks are foiled by these properties.

Encryption algorithms:

- **Elliptic Curve Integrated Encryption Scheme (ECIES):** ECIES is a public-key authenticated encryption scheme that uses a KDF (key-derivation function) to generate a separate Medium Access Control key and symmetric encryption key from the ECDH shared secret. Because the ECIES algorithm incorporates a symmetric cipher, it can encrypt any amount of data. In practice, ECIES is used by standards such as Intelligent Transportation Systems.
- **EC-based ElGamal Elliptic Curve Cryptography:** ElGamal Elliptic Curve Cryptography is the public key cryptography equivalent of ElGamal encryption schemes that employ the Elliptic Curve Discrete Logarithm Problem. ElGamal is an asymmetric encryption algorithm that is used to send messages securely over long distances. Unfortunately, if the encrypted message is short enough, the algorithm is vulnerable to a Meet in the Middle attack.

Key Agreement algorithm:

- **Elliptic-curve Diffie–Hellman (ECDH):** Elliptic-curve Diffie-Hellman (ECDH) is a key agreement protocol that enables two parties to establish a shared secret over an insecure channel, each with an elliptic-curve public-private key pair. This shared secret can be used directly as a key or to generate another key. Following that, the key, or the derived key, can be used to encrypt subsequent communications with a symmetric-key cipher.
- **Fully Hashed Menezes-Qu-Vanstone(FHMQV):** Fully Hashed Menezes-Qu-Vanstone is an authenticated key agreement protocol based on the Diffie-Hellman scheme. MQV, like other authenticated Diffie-Hellman schemes, protects against an active attacker. The protocol can be adapted to work in any finite group, most notably elliptic curve groups, in which it is recognized as elliptic curve MQV (ECMQV).

Application of Elliptic Curve Cryptography

- **Diffie-Hellman:** The basic public-key cryptosystem suggested for secret key sharing is the Diffie-Hellman protocol. If A (Alice) and B (Bob) initially agree on a given curve, field size, and mathematical type. They then distribute the secret key in the following manner. We can see that all we need to build the Diffie-Hellman protocol is scalar multiplication.
- **Elliptic Curve Digital Signature Algorithm (ECDSA):** ECC is one of the most widely utilized digital signature implementation approaches in cryptocurrencies. In order to sign transactions, both Bitcoin and Ethereum use the field inverse multiplication, but also arithmetic multiplication, inverse function, and modular operation.
- **Online application:** Moreover, ECC is not limited to cryptocurrencies. It is an encryption standard that will be utilized by most online apps in the future due to its reduced key size and efficiency. Most commonly used in cryptocurrencies such as Bitcoin and Ethereum, along with single-way encryption of emails, data, and software.
- **Blockchain application:** The cryptocurrency Bitcoin employs elliptic curve cryptography. Ethereum 2.0 makes heavy use of elliptic curve pairs with BLS signatures, as stated in the IETF proposed BLS specification, to cryptographically ensure that a specific Eth2 validator has really verified a specific transaction.

Lab Assignment No.	06
Title	Enable/Configure (windows/ubuntu) firewall. Create rules to filter network traffic and to block unauthorized network traffic.
Roll No.	
Class	TE
Date of Completion	
Subject	Mini Project(Cyber Security)
Assessment Marks	
Assessor's Sign	

ASSIGNMENT No: 06

Title: Enable/Configure (windows/ubuntu) firewall. Create rules to filter network traffic and to block unauthorized network traffic.

Problem Statement: Enable/Configure (windows/ubuntu) firewall. Create rules to filter network traffic and to block unauthorized network traffic.

Prerequisite:

Basic of Python, Information security Algorithm

Software Requirements:

Python 3.7

Hardware Requirement:

2GB RAM, 500 GB HDD

Learning Objectives:

Learn ECC Algorithm

Outcomes:

After completion of this assignment students are able to understand the How to create rules to filter network traffic and to block unauthorized network traffic.

Theory:

Windows Firewall

Windows Firewall is a packet filter and stateful host-based firewall that allows or blocks network traffic according to the configuration. A packet filter protects the computer by using an access control list (ACL), which specifies which packets are allowed through the firewall based on IP address and protocol (specifically the port number). A stateful firewall monitors the state of active connections and uses the information gained to determine which network packets are allowed through the firewall. Typically, if the user starts communicating with an outside computer, it remembers the conversation and allows the appropriate packets back in. If an outside computer tries to start communicating with a computer protected by a stateful firewall, those packets are dropped automatically unless access was granted by the ACL.

Exam Alert

Windows Firewall is on by default. Any program or service that needs to communicate on a network must be opened in a firewall, including sharing files, pinging the server, or providing basic services, such as DNS and DHCP.

Compared to Windows Firewall introduced with Windows XP SP2, the Windows Firewall used with Windows Server 2008 has some major improvements, including the following:

Windows Firewall supports IPv6 connection filtering.

By using outbound packet filtering, you can help protect the computer againt spyware and viruses that attempt to contact outside computers.

With the advanced packet filter, rules can also be specified for source and destination IP addresses and port ranges.

Rules can be configured for services by the service name chosen from a list, without needing to specify the full path filename.

IPSec is fully integrated with Windows Firewall, allowing connections to be allowed or denied based on security certificates, Kerberos authentication, and so on. Encryption can also be required for any kind of connection.

A new management console snap-in named Windows Firewall with Advanced Security provides access to many advanced options and enables remote administration.

You can use separate firewall profiles for when computers are domain-joined or connected to a private or public network.

Basic Configuration

Windows Firewall is on by default. When Windows Firewall is on, most programs are blocked from communicating through the firewall. If you want to unblock a program, you can add it to the Exceptions list (on the Exceptions tab). For example, you might not be able to send photos in an instant message until you add the instant messaging program to the Exceptions list. To add a program to the Exceptions list, click the Add program button and select it from the available list or browse for it by clicking the Browse button.

To turn on or off Windows Firewall, follow these steps:

Open Windows Firewall by clicking the Start button, clicking Control Panel, clicking Security, and then clicking Windows Firewall.

Click Turn Windows Firewall On or Off (see Figure 5.3). If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

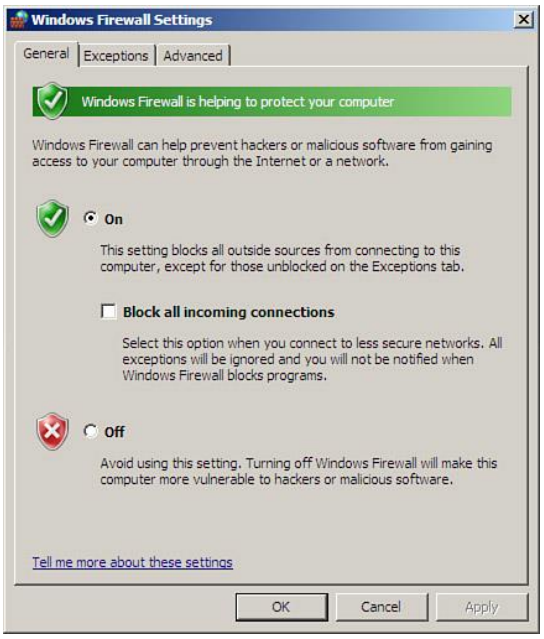


Figure 5.3 Windows Firewall options in the Control Panel.

Click On (recommended) or Off (not recommended) and then click OK.

If you want the firewall to block everything, including the programs selected on the Exceptions tab, select the Block All Incoming Connections check box. Block All Incoming Connections blocks all unsolicited attempts to connect to your computer. Use this setting when you need maximum protection for your computer, such as when you connect to a public network in a hotel or airport, or when a computer worm is spreading over the Internet. With this setting, you are not notified when Windows Firewall blocks programs, and programs on the Exceptions list are ignored.

The Windows Firewall Settings interface has three tabs:

General: Enables you to turn Windows Firewall on and off, as well as to block all incoming connections, no matter how you have configured the exceptions.

Exceptions: Enables you to configure programs and ports for which you want to allow communication into and out from your Windows Vista computer. Only create an exception that is specifically required, and remove exceptions that you no longer need. Never create an exception for a program when you are unsure of the functionality of that program.

Advanced: Enables you to select the network interfaces that you want Windows Firewall to protect.

To configure programs as exceptions,

Open Windows Firewall by clicking Start > Control Panel > Security > Windows Firewall.

Click Allow a program through Windows Firewall. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

In the Windows Firewall dialog box, select the Exceptions tab and then click Add Program.

In the Add A Program dialog box, select the program in the Programs list or click Browse to use the Browse dialog box to find the program.

By default, any computer, including those on the Internet, can access this program remotely. To restrict access further, click Change Scope.

Click OK three times to close all open dialog boxes.

To open a port in Windows Firewall,

Open Windows Firewall by clicking the Start button, clicking Control Panel, clicking Security, and then clicking Windows Firewall.

Click Allow a program through Windows Firewall. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

Click Add port.

In the Name box, type a name that will help you remember what the port is used for.

In the Port number box, type the port number.

Click TCP or UDP, depending on the protocol.

By default, any computer, including those on the Internet, can access this program remotely. To change scope for the port, click Change scope, and then click the option that you want to use. (“Scope” refers to the set of computers that can use this port opening.)

Click OK two times to close all open dialog boxes.

Windows Firewall with Advanced Security

Similar to the Windows Firewall with Advanced Security introduced in Windows Vista, the Windows Firewall with Advanced Security in Windows Server 2008 is a Microsoft Management Console (MMC) snap-in that allows you to set up and view detailed inbound and outbound rules and integrate with Internet Protocol security (IPSec).

The Windows Firewall with Advanced Security management console enables you to configure:

Inbound rules: Windows Firewall will block all incoming traffic unless solicited or allowed by a rule.

Outbound rules: Windows Firewall will allow all outbound traffic unless blocked by a rule.

Connection security rules: Windows Firewall uses a connection security rule to force two peer computers to authenticate before they can establish a connection and to secure information transmitted between the two computers. Connection security rules use IPsec to enforce security requirements. Connection security rules will be explained more in the next chapter.

Monitoring: Windows Firewall uses the monitoring interface to display information about current firewall rules, connection security rules, and security associations.

Windows Firewall is on by default. When Windows Firewall is on, most programs are blocked from communicating through the firewall. If you want to unblock a program, you can add it to the Exceptions list (on the Exceptions tab). For example, you might not be able to send photos in an instant message until you add the instant messaging program to the Exceptions list. To add a program to the Exceptions list, see Allow a program to communicate through Windows Firewall.

To turn on or off Windows Firewall:

Open Windows Firewall with Advanced Security located in Administrative Tools.

Click the Windows Firewall Properties.

Under Firewall state, Select either On (recommended) or Off (not recommended) and click the OK button. See Figure 5.4.

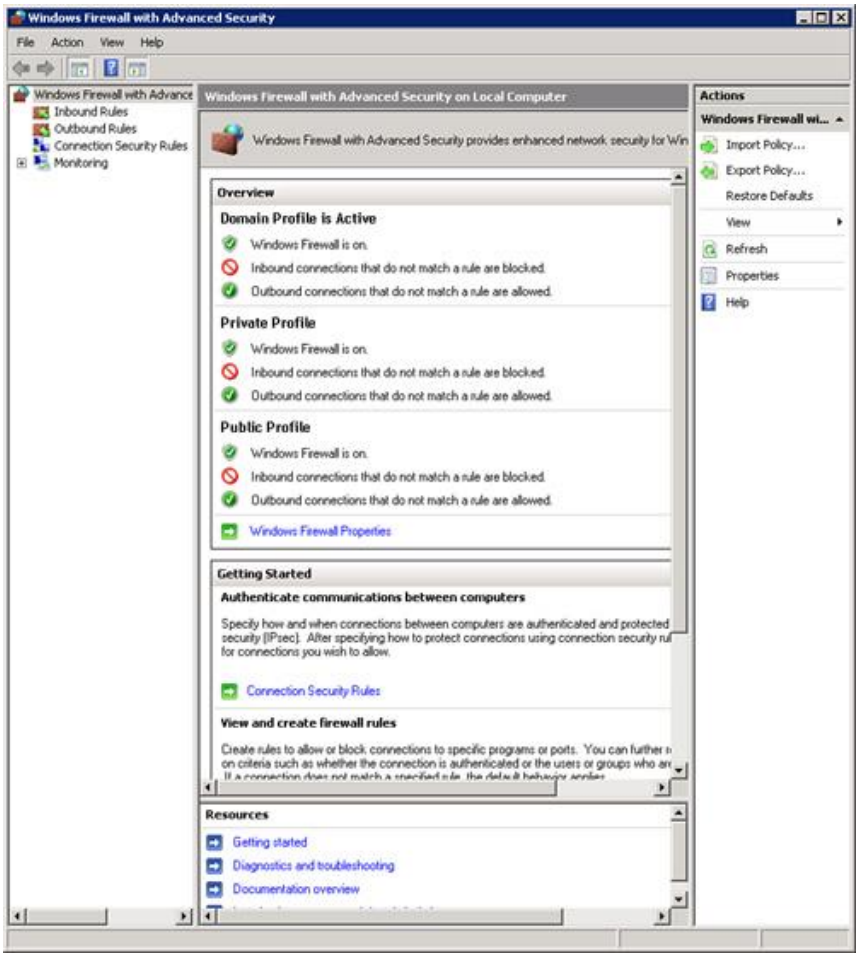


Figure 5.4 Windows Firewall properties.

Creating Inbound and Outbound Rules

You create inbound rules to control access to your computer from the network. Inbound rules can prevent

Unwanted software being copied to your computer

Unknown or unsolicited access to data on your computer

Unwanted configuration of your computer from remote locations

To configure advanced properties for a rule using the Windows Firewall with Advanced Security, follow these steps:

Right-click the name of the inbound rule and click Properties.

From the properties dialog box for an inbound rule, configure settings on the following tabs:

General: The rule's name, the program to which the rule applies, and the rule's action (allow all connections, allow only secure connections, or block).

Programs and Services: The programs or services to which the rule applies.

Users and Computers: If the rule's action is to allow only secure connections, the computer accounts that are authorized to make protected connections.

Protocols and Ports: The rule's IP protocol, source and destination TCP or UDP ports, and ICMP or ICMPv6 settings.

Scope: The rule's source and destination addresses.

Advanced: The profiles or types of interfaces to which the rule applies.

You can also use the Windows Firewall with Advanced Security to create outbound rules to control access to network resources from your computer. Outbound rules can prevent:

Utilities on your computer accessing network resources without your knowledge.

Utilities on your computer downloading software without your knowledge.

Users of your computer downloading software without your knowledge.

Determining a Firewall Profile

A firewall profile is a way of grouping settings, such as firewall rules and connection security rules that are applied to the computer, depending on where the computer is connected. On computers running this version of Windows, there are three profiles for Windows Firewall with Advanced Security. Only one profile is applied at a time.

The available profiles are

Domain: Applied when a computer is connected to a network in which the computer's domain account resides.

Private: Applied when a computer is connected to a network in which the computer's domain account does not reside, such as a home network. The private settings should be more restrictive than the domain profile settings.

Public: Applied when a computer is connected to a domain through a public network, such as those available in airports and coffee shops. The public profile settings should be the most restrictive because the computer

is connected to a public network where the security cannot be as tightly controlled as within an IT environment.

Using netsh Command to Configure the Windows Firewall

To view the current firewall configuration, including ports that have been opened, use the following command:

netsh firewall show state

NOTE

If the Firewall status shows that the Operational mode is set to Enable, this means that the Windows Firewall is enabled but no specific ports have been opened.

To open ports at the firewall for DNS (port 53), use the following command:

netsh firewall add portopening ALL 53 DNS-server

To view the firewall configuration, use the following command:

netsh firewall show config

To enter the netsh advfirewall context, at the command prompt, type

netsh

When you enter the netsh context, the command prompt displays the >netsh prompt. At the >netsh prompt, enter the advfirewall context type:

advfirewall

After you are in the advfirewall context, you can type commands in that context.

Commands include the following:

Export: Exports the current firewall policy to a file.

Help: Displays a list of available commands.

Import: Imports a policy from the specified file.

Reset: Restores Windows Firewall with Advanced Security to the default policy.

Set: Supports the following commands:

set file: Copies the console output to a file.

set machine: Sets the current machine on which to operate.

show: Shows the properties for a particular profile. Examples include show allprofiles, show domainprofile, show privateprofile and show publicprofile.

In addition to the commands available for the advfirewall context, advfirewall also supports several subcontexts. To enter a subcontext, type the name of the subcontext at the netsh advfirewall> prompt. The available subcontexts are

consec: Enables you to view and configure computer security connection rules

Firewall: Enables you to view and configure firewall rules

Monitor: Enables you to view and set monitoring configuration

Managing Windows Firewall with Advanced Security via Group Policy

To centralize the configuration of large numbers of computers in an organization network that uses the Active Directory directory service, you can deploy settings for Windows Firewall with Advanced Security through Group Policy. Group Policy provides access to the full feature set of Windows Firewall with Advanced Security, including profile settings, rules, and computer connection security rules.

Lab Assignment No.	07
Title	Configure and demonstrate an Intrusion Detection System (IDS) to detect suspicious activities and generate alerts when detected.
Roll No.	
Class	TE
Date of Completion	
Subject	Mini Project(Cyber Security)
Assessment Marks	
Assessor's Sign	

ASSIGNMENT No: 07

Title: Configure and demonstrate an Intrusion Detection System (IDS) to detect suspicious activities and generate alerts when detected.

Problem Statement: Configure and demonstrate an Intrusion Detection System (IDS) to detect suspicious activities and generate alerts when detected.

Prerequisite:

Basic of Python, Information security Algorithm

Software Requirements:

Python 3.7

Hardware Requirement:

2GB RAM, 500 GB HDD

Learning Objectives:

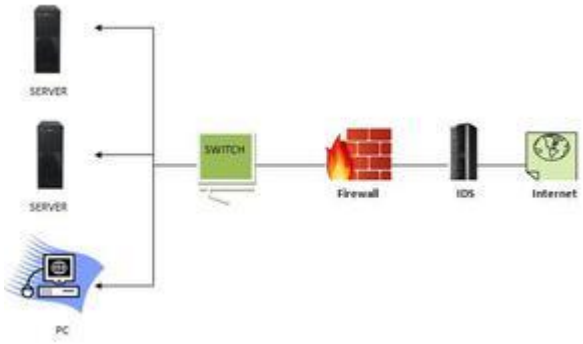
Learn ECC Algorithm

Outcomes:

After completion of this assignment students are able to understand the How detection of suspicious activity is done and how alerts are generated.

Theory:

A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between ‘bad connections’ (intrusion/attacks) and ‘good (normal) connections.



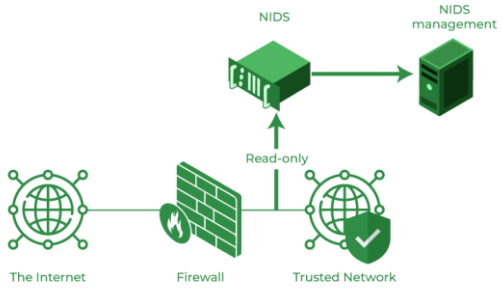
How does an IDS work?

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

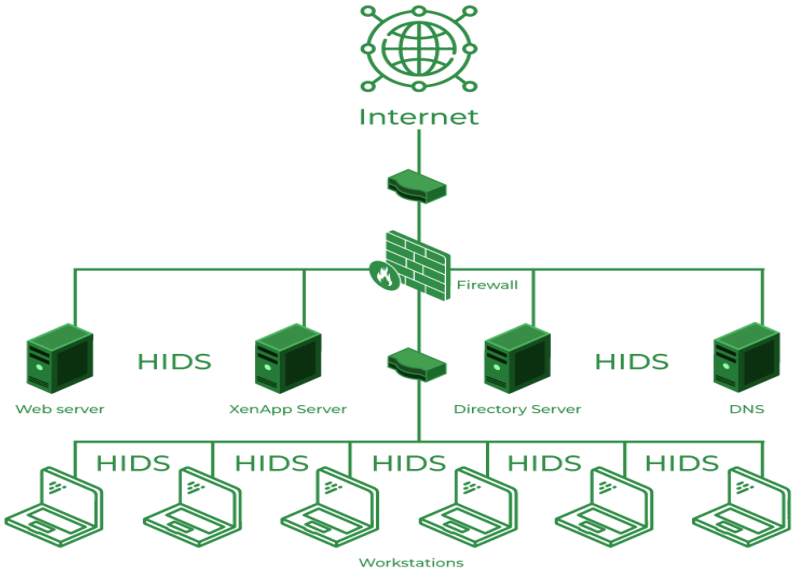
Classification of Intrusion Detection System

IDS are classified into 5 types:

- **Network Intrusion Detection System (NIDS):** Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.



- **Host Intrusion Detection System (HIDS):** Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.



- **Protocol-based Intrusion Detection System (PIDS):** Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accepting the related HTTP protocol. As HTTPS is unencrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.
- **Application Protocol-based Intrusion Detection System (APIDS):** An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.
- **Hybrid Intrusion Detection System**: Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system. In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system. The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Benefits of IDS

- Detects malicious activity: IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.
- Improves network performance: IDS can identify any performance issues on the network, which can be addressed to improve network performance.
- Compliance requirements: IDS can help in meeting compliance requirements by monitoring network activity and generating reports.
- Provides insights: IDS generates valuable insights into network traffic, which can be used to identify any weaknesses and improve network security.

Detection Method of IDS

1. **Signature-based Method**: Signature-based IDS detects the attacks on the basis of the specific patterns such as the number of bytes or a number of 1s or the number of 0s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in the system but it is quite difficult to detect new malware attacks as their pattern (signature) is not known.
2. **Anomaly-based Method**: Anomaly-based IDS was introduced to detect unknown malware attacks as new malware is developed rapidly. In anomaly-based IDS there is the use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in the model. The machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Comparison of IDS with Firewalls

IDS and firewall both are related to network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it doesn't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

Conclusion:

Intrusion Detection System (IDS) is a powerful tool that can help businesses in detecting and prevent unauthorized access to their network. By analyzing network traffic patterns, IDS can identify any suspicious activities and alert the system administrator. IDS can be a valuable addition to any organization's security infrastructure, providing insights and improving network performance.

Mini Project(Any one) 1

Lab Assignment No.	**8**
Title	Mini Project 4: This task is to demonstrate insecure and secured website. Develop a web site and demonstrate how the contents of the site can be changed by the attackers if it is http based and not secured. You can also add payment gateway and demonstrate how money transactions can be hacked by the hackers. Then support your website having https with SSL and demonstrate how secured website is.
Roll No.	
Class	TE
Date of Completion	
Subject	Mini Project(Cyber Security)
Assessment Marks	
Assessor's Sign	

ASSIGNMENT No: 08

Aim: This task is to demonstrate insecure and secured website. Develop a web site and demonstrate how the contents of the site can be changed by the attackers if it is http based and not secured. You can also add payment gateway and demonstrate how money transactions can be hacked by the hackers. Then support your website having https with SSL and demonstrate how secured website is.

Problem Statement: This task is to demonstrate insecure and secured website. Develop a web site and demonstrate how the contents of the site can be changed by the attackers if it is http based and not secured. You can also add payment gateway and demonstrate how money transactions can be hacked by the hackers. Then support your website having https with SSL and demonstrate how secured website is.

Prerequisite:

Basic of Python, Information security Algorithm

Software Requirements:

Python 3.7

Hardware Requirement:

2GB RAM, 500 GB HDD

Learning Objectives:

Learn ECC Algorithm

Outcomes:

After completion of this assignment students are able to understand the How detection of suspicious activity in secure and unsecured sites

Theory:

Introduction to SSL/TLS

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are technologies which allow web browsers and web servers to communicate over a secured connection. This means that the data being sent is encrypted by one side, transmitted, then decrypted by the other side before processing. This is a two-way process, meaning that both the server AND the browser encrypt all

traffic before sending out data.

Another important aspect of the SSL/TLS protocol is Authentication. This means that during your initial attempt to communicate with a web server over a secure connection, that server will present your web browser with a set of credentials, in the form of a "Certificate", as proof the site is who and what it claims to be. In certain cases, the server may also request a Certificate from your web browser, asking for proof that *you* are who you claim to be. This is known as "Client Authentication,"although in practice this is used more for business-to-business (B2B) transactions than with individual users. Most SSL-enabled web servers do not request Client Authentication.

Following diagram depicts dynamic web server system three tiers. In case of two tier, only browser and web server will be available client server model.

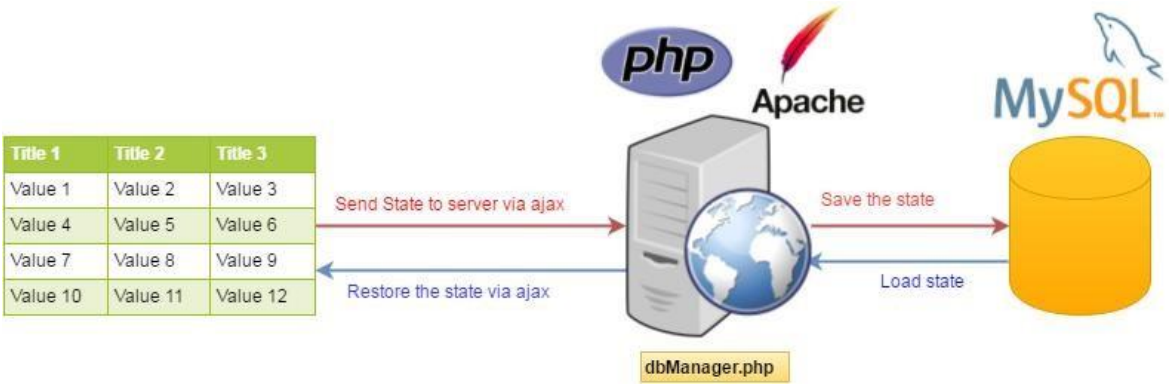


Figure 1: Ref: http://refreshmymind.com/wp-content

Above diagram shows three components of web server system. Presentation layer on left side i.e. browser, middle layer that is tomcat server and data layer is implemented with mysql.

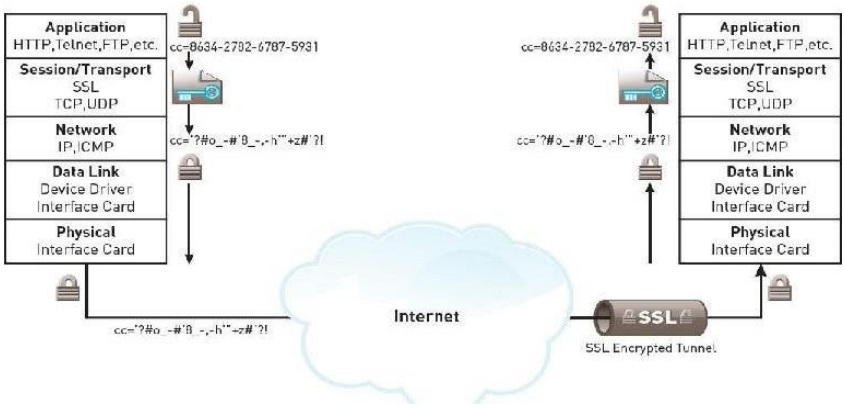
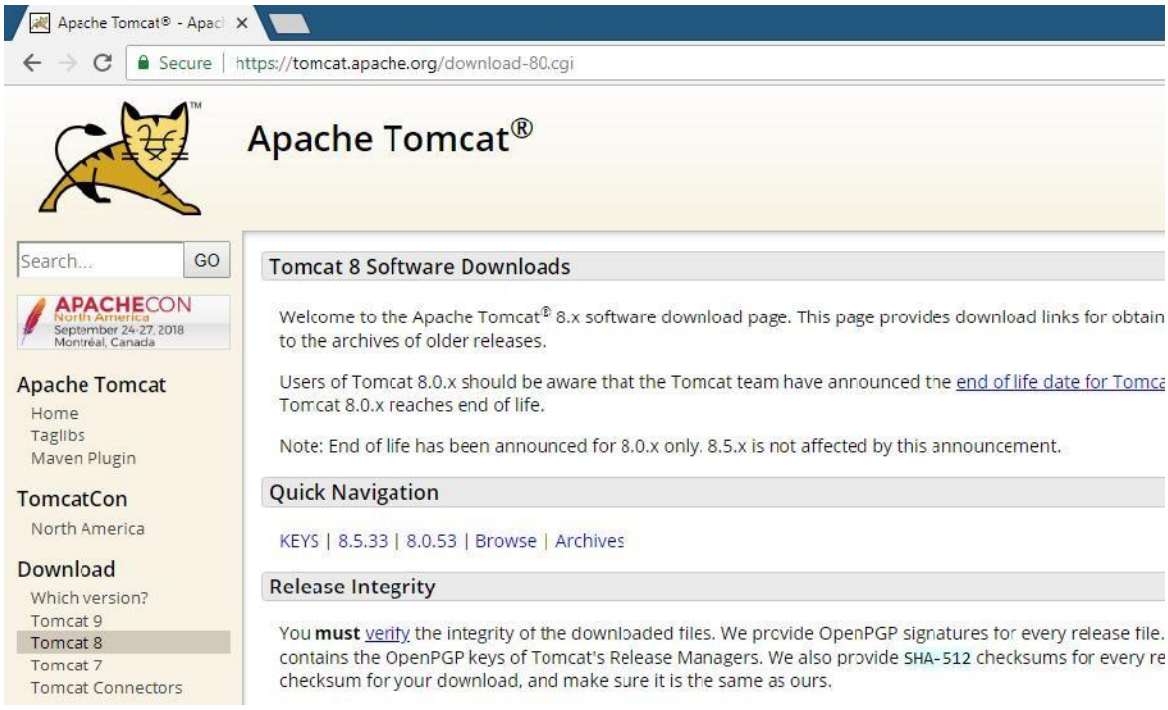


Figure 2: Client server protocol stack with SSL functionality

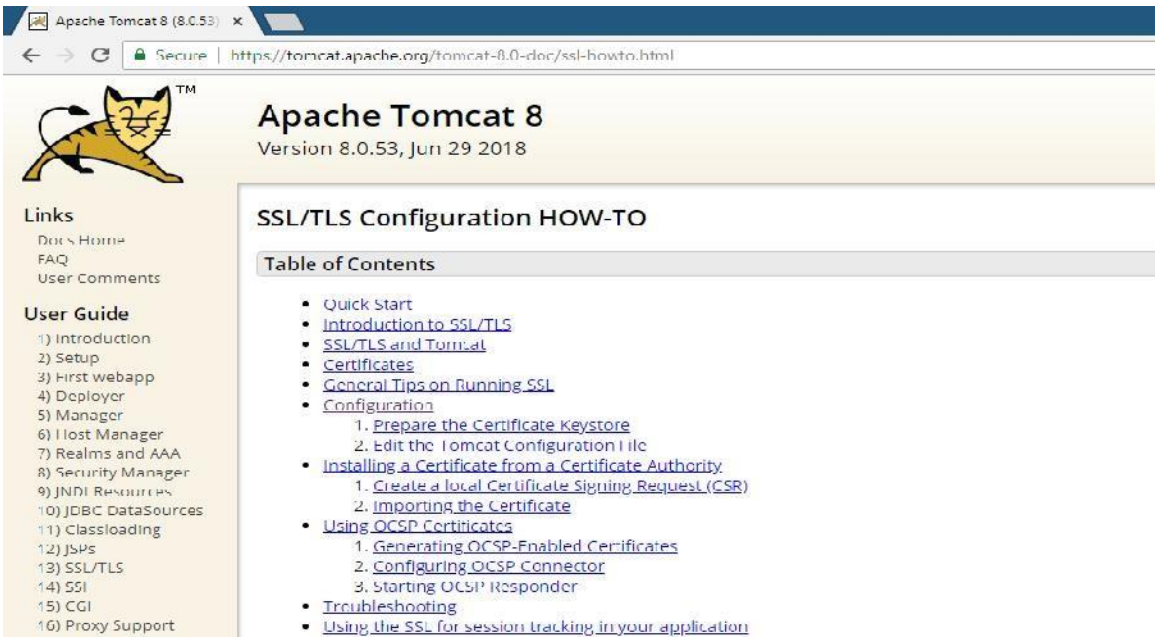
Now let us have practical steps of demonstration on Ubuntu system.

1. First prerequisite is install jdk on Ubuntu. (Preferably latest version) and add JAVA_HOME path in .bashrc which is available as in home directory. Also add jdk bin path in .bashrc so that you can access java command from any working directory.
2. Download the apache tomcat 8.55.33 application tar file from apache site. And extract it in your home directory. Also add CATALINA_HOME in .bashrc as follows.

   export CATALINA_HOME=/home/bnjagdale/web/apache-tomcat-8.5.33



3. **Documentation:** Additionally you may refer the SSL/TLS manual of securing web sites



4. **Start the Tomcat**. Go to the apache bin directory and run following command

   …/bin$sh startup.sh

   Stop tomcat: And you can shutdown tomcat server with following command.

   …/bin$sh shutdown.sh

   Note: Every time you change configuration files of tomcat, make sure to restart the tomcat server to adopt the changes

5. Access the Web Interface of tomcat server (Testing Web server)

Now that we have create a user, we can access the web management interface again in a web browser. Once again, you can get to the correct interface by entering your server's domain name or IP address followed on port 8080 in your browser:

Open in web browser

http://server_domain_or_IP:8080 OR

http://127.0.0.1:8080/

The page you see should be the same one you were given when you tested earlier:

6. Web server Manager interface

In order to use the manager web app that comes with Tomcat, we must add a login to our Tomcat server. We will do this by editing the tomcat-users.xml file:

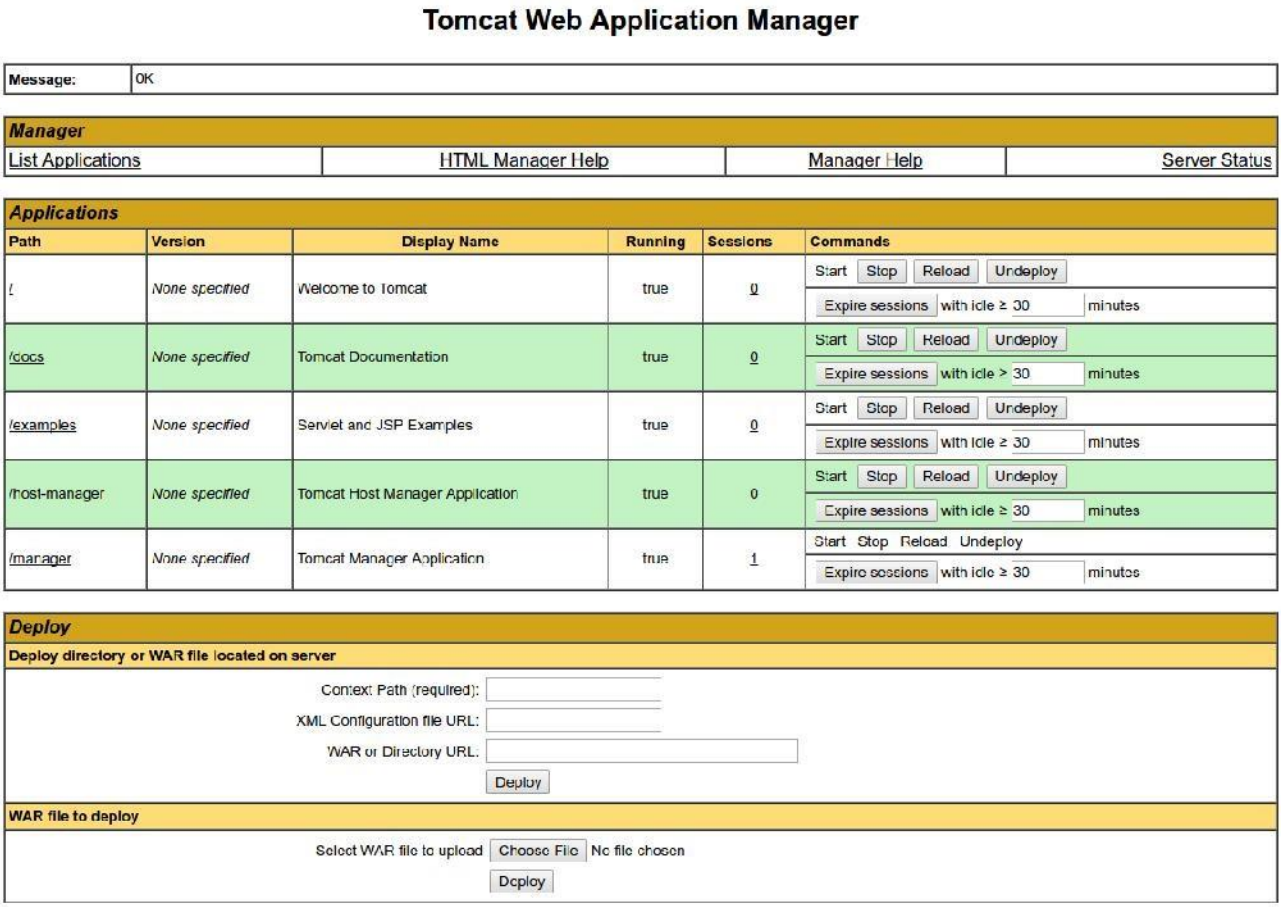
```
sudo nano  …./conf/tomcat-users.xml
```

You will want to add a user who can access the manager-gui and admin-gui (web apps that come with Tomcat). You can do so by defining a user, similar to the example below, between the tomcat-users tags. Be sure to change the username and password to something secure:

```
                    tomcat-users.xml – Admin User
<tomcat-users . . .>

  <user username="admin" password="password" roles="manager-gui,admin-gui"/>

</tomcat-users>
```

Save and close the file when you are finished. You need to restart the tomcat to adopt the changes.

Let's take a look at the Manager App, accessible via the link or http://server_domain_or_IP:8080/manager/html. You will need to enter the account credentials that you added to the tomcat-users.xml file. Afterwards, you should see a page that looks like this:



Tomcat Web Application Manager

Message:	OK

Manager			
List Applications	HTML Manager Help	Manager Help	Server Status

Applications					
Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

Context Path (required):
XML Configuration file URL:
WAR or Directory URL:
Deploy

WAR file to deploy

Select WAR file to upload Choose File No file chosen
Deploy

The Web Application Manager is used to manage your Java applications. You can Start, Stop, Reload, Deploy, and Un install here. You can also run some diagnostics on your apps (i.e. find memory leaks). Lastly, information about your server is available at the very bottom of this page.

7. Let us test the web pages / JSP pages

   Now let us deploy jsps and html and test them. Switch to webapps directory of tomcat and create you won folder like ….

   ..webspps$mkdir myapps

   ..webspps$cd myapps

   ..webspps$gedit login1.html

```
<html>
     <head>
       <title>SSL demonstration</title>
     </head>
     <body>
     <h3>Web communicaton in plain text- NO SSL</h3>
     <br>
     <form action="http://127.0.0.1:8080/myapps/action.jsp"
     method=post>
```

```
        User Name:<br>
        <input type="text" name="username" value=""><br>
        Password:<br>
        <input type="password" name="password"
     value=""><br><br>
        <input type="submit" value="Submit">
     </form>
     </body>
</html>
```

One more file to respond to above html as action.jsp as follows

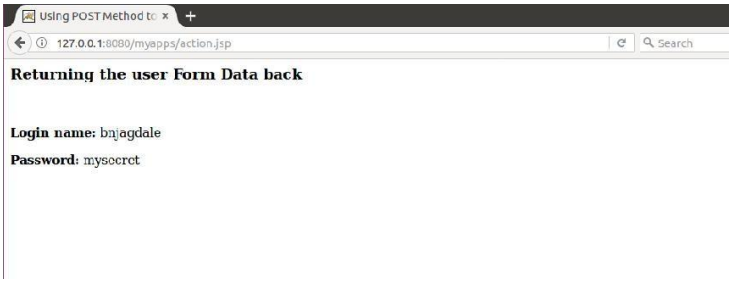
```
<html>
         <head>
            <title>Using POST Method to Read Form Data</title>
         </head>

         <body>
            <h3>Returning the user Form Data back</h3>
            <br>

               <p><b>Login name:</b>
                  <%= request.getParameter("username")%>
               </p>

               <p><b>Password:</b>
                  <%= request.getParameter("password")%>
               </p>
         </body>
</html>
```

…webapps/myapps$ls

login1.html
action.jsp

Create two files. First file of html is to demonstrate the web form login page. action file is jsp program for response for login html file

8. Now test the web pages as follows.
   You will observe that all traffic is plain in format. So far we have not talked about SSL or TLS between client and server.



9. SSL/TLS installation (Java keytool)

SSL/TLS and Tomcat

It is important to note that configuring Tomcat to take advantage of secure sockets is usually only necessary when running it as a stand-alone web server. Details can be found in the Security Considerations Document. When running Tomcat primarily as a Servlet/JSP container behind another web server, such as Apache or Microsoft IIS, it is usually necessary to configure the primary web server to handle the SSL connections from users. Typically, this server will negotiate all SSL-related functionality, then pass on any requests destined for the Tomcat container only after decrypting those requests. Likewise, Tomcat will return clear text responses, which will be encrypted before being returned to the user's browser. In this environment, Tomcat knows that communications between the primary web server and the client are taking place over a secure connection (because your application needs to be able to ask about this), but it does not participate in the encryption or decryption itself.

Certificates

In order to implement SSL, a web server must have an associated Certificate for each external interface (IP address) that accepts secure connections. The theory behind this design is that a server should provide some kind of reasonable assurance that its owner is who you think it is, particularly

before receiving any sensitive information. While a broader explanation of Certificates is beyond the scope of this document, think of a Certificate as a "digital passport" for an Internet address. It states which organization the site is associated with, along with some basic contact information aboutthe site owner or administrator.

This certificate is cryptographically signed by its owner, and is therefore extremely difficult for anyone else to forge. For the certificate to work in the visitors browsers without warnings, it needs to be signed by a trusted third party. These are called *Certificate Authorities* (CAs). To obtain a signed certificate, you need to choose a CA and follow the instructions your chosen CA provides to obtain your certificate. A range of CAs is available including some that offer certificates at no cost.

Java provides a relatively simple command-line tool, called keytool, which can easily create a "self-signed" Certificate. Self-signed Certificates are simply user generated Certificates which have not been signed by a well-known CA and are, therefore, not really guaranteed to be authentic at all. While self-signed certificates can be useful for some testing scenarios, they are not suitable for any form of production use.

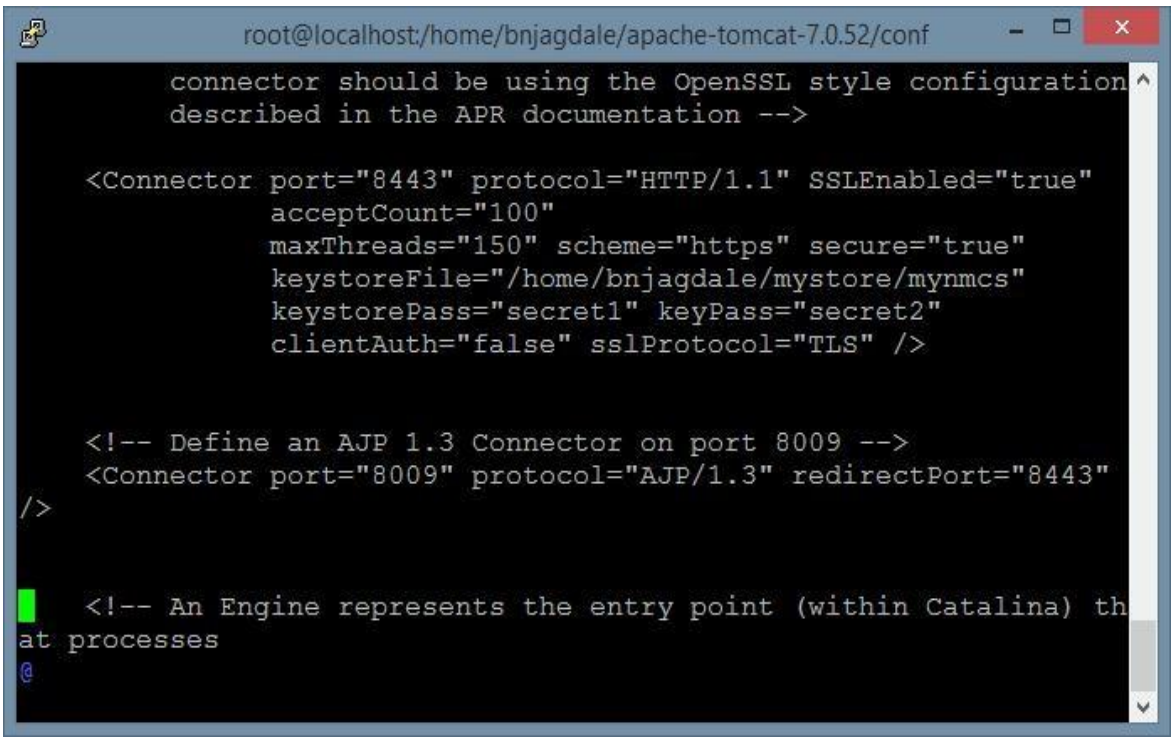
10. Above traffic between server and client is without SSL implementation

1. Now create the digital certificate using java keytool in jdk/bin
2. Issue command as follows.

   [root@localhost ~]# keytool -genkey -alias mykeys -keyalg RSA -keystore mynmcs

   In this example keynamed mynmcs is created in working directory and public key pair is also generated in keystore supported by passwords.

3. Now configure the digital certificate in server.xml file available in conf directory under apache tomcat directory. As follows

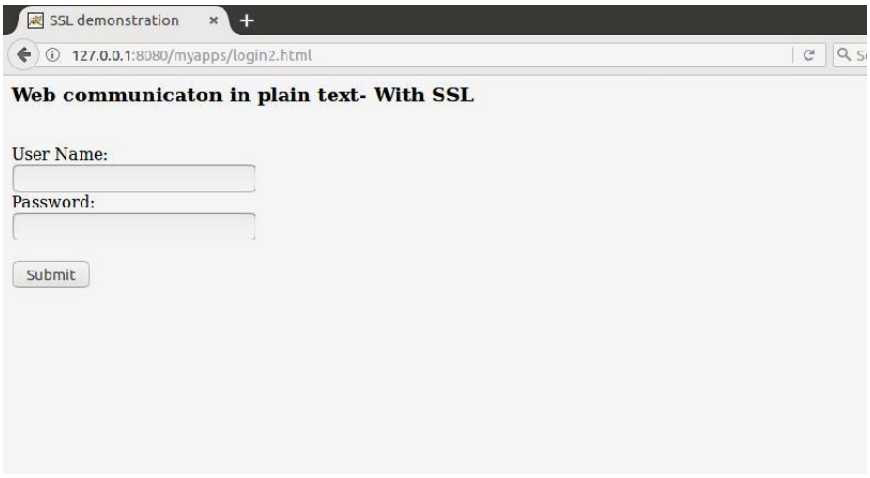


4. Restart the tomcat server by using command as under tomcat 8 bin directory

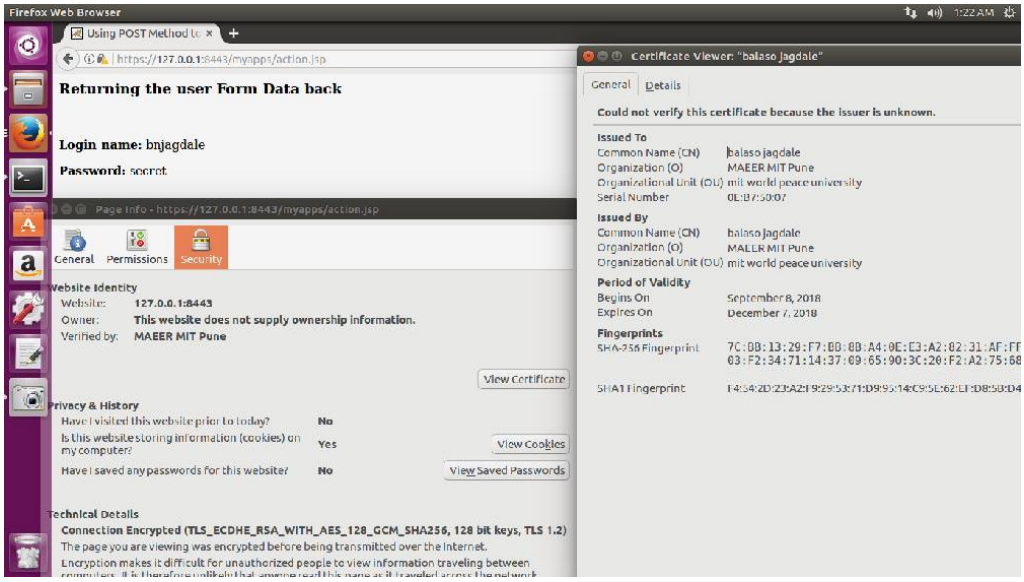
   ```
   $sh shutdown.sh
   $sh startup.sh
   ```

5. Now issue the url in client browser as follows

   ```
   https://172.20.1.121:8443/myapps/login2.html
   ```



6. Now this form will (submit) initiate ssl dialog and hence communication will be secured now.

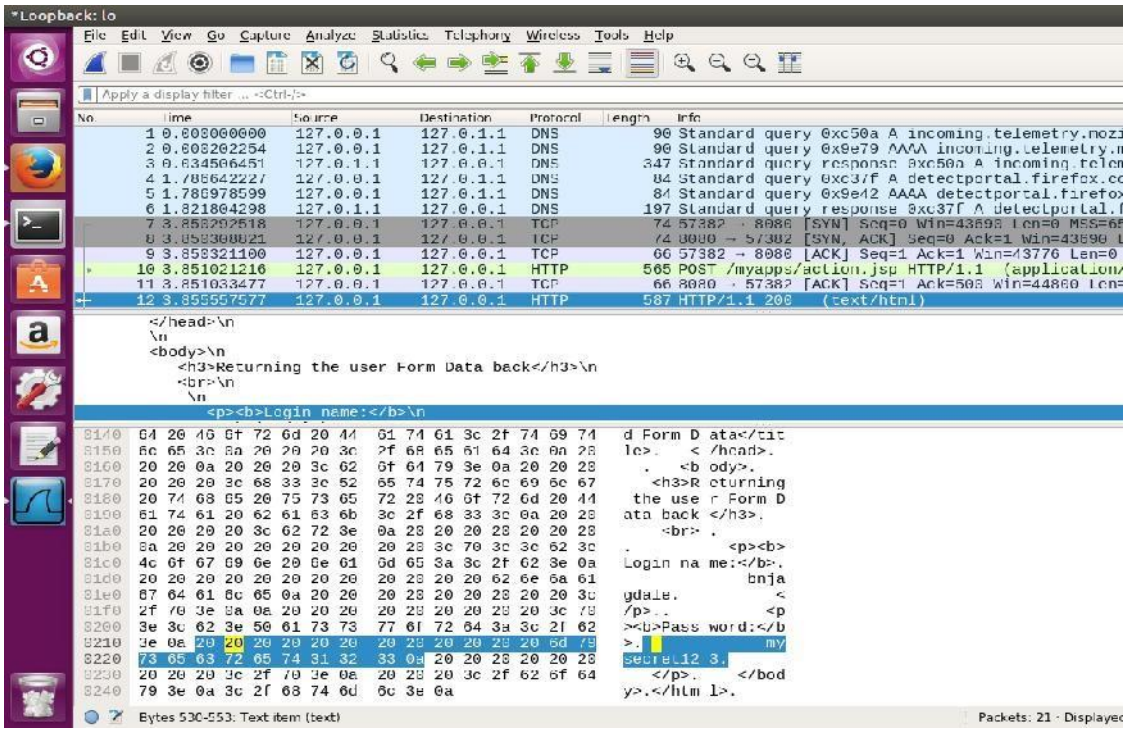


Certificate warning error is shown as certificate is self-signed. Accept certificate and check the output.

So now traffic is secured with SSL between transport and application.

Click on certificate error and see the details. Certificates installed in tomcat server for SSL security are self-signed. If signed by CA like VeriSign, even legality of this communication is applicable. Thus by deploying SSL in tomcat server, websites can be secured to achieve Authentication, integrity and secrecy goals in the communication between web client and web server.

Now check the plain traffic by deploying sniffer such as tcpdump or wireshark etc. and verify that traffic is plain without SSL and with https://localhost:8443/... Traffic is secured in term of authentication, secrecy and integrity.



As you can see that wire shark has sniffed the web traffic and found what server and client are talking. Here, toward the bottom of screen capture, you can see password in plain format, whichyou will not be able to sniff after https SSL is deployed.

Wish you joy while experimenting…

Part B : Elective II : Cloud Computing

Lab Assignment No.	**9**
Title	Setting up AWS Environment: Create a new AWS account, Secure the root user, Create an IAM user to use in the account Set up the AWS CLI, Set up a Cloud9 environment.
Roll No.	
Class	TE
Date of Completion	
Subject	Mini Project(Cyber Security)
Assessment Marks	
Assessor's Sign	

ASSIGNMENT No: 09

Title: Setting up AWS Environment: Create a new AWS account, Secure the root user, Create an IAM user to use in the account Set up the AWS CLI, Set up a Cloud9 environment.

Problem Statement: Setting up AWS Environment: Create a new AWS account, Secure the root user, Create an IAM user to use in the account Set up the AWS CLI, Set up a Cloud9 environment.

Prerequisite:

Basic of Cloud

Software Requirements:

AWS

Hardware Requirement:

2GB RAM, 500 GB HDD

Learning Objectives:

Learning AWS Environment

Outcomes:

After completion of this assignment students are able to how to create IAM user to use in the account setup the AWS CLI

Theory:

Create an EC2 environment with the AWS CLI
Install and configure the AWS CLI, if you have not done so already. To do this, see the following in the AWS Command Line Interface User Guide:

Installing the AWS Command Line Interface

Quick configuration

You can configure the AWS CLI using credentials for one of the following:

The IAM user you created in Team setup for AWS Cloud9.

An IAM administrator in your AWS account, if you will be working regularly with AWS Cloud9 resources for multiple users across the account. If you cannot configure the AWS CLI as an IAM administrator, check with your AWS account administrator. For more information, see Creating your

first IAM admin user and group in the IAM User Guide.

An AWS account root user, but only if you will always be the only one using your own AWS account, and you don't need to share your environments with anyone else. We don't recommend this option as it isn't an AWS security best practice. For more information, see Creating, Disabling, and Deleting Access Keys for Your AWS Account in the Amazon Web Services General Reference.

For other options, see your AWS account administrator or classroom instructor.

In the following AWS Cloud9 command, provide a value for --region and --subnet-id. Then run the command and make a note of the "environmentId" value for later cleanup.

aws cloud9 create-environment-ec2 --name my-demo-environment --description "This environment is for the AWS Cloud9 tutorial." --instance-type t2.micro --image-id resolve:ssm:/aws/service/cloud9/amis/amazonlinux-1-x86_64 --region MY-REGION --connection-type CONNECT_SSM --subnet-id subnet-12a3456b
In the preceding command:

--name represents the name of the environment. In this tutorial, we use the name my-demo-environment.

--description represents an optional description for the environment.

--instance-type represents the type of Amazon EC2 instance AWS Cloud9 will launch and connect to the new environment. This example specifies t2.micro, which has relatively low RAM and vCPUs and is sufficient for this tutorial. Specifying instance types with more RAM and vCPUs might result in additional charges to your AWS account for Amazon EC2. For a list of available instance types, see the create environment wizard in the AWS Cloud9 console.

--image-id specifies the identifier for the Amazon Machine Image (AMI) that's used to create the EC2 instance. To choose an AMI for the instance, you must specify a valid AMI alias or a valid AWS Systems Manager (SSM) path. In the example above, an SSM path for an Amazon Linux 2 AMI is specified.

For more information, see create-environment-ec2 in the AWS CLI Command Reference.

--region represents the ID of the AWS Region for AWS Cloud9 to create the environment in. For a list of available AWS Regions, see AWS Cloud9 in the Amazon Web Services General Reference.

--connection-type CONNECT_SSM specifies that AWS Cloud9 connects to its Amazon EC2 instance through Systems Manager. This option ensures no inbound traffic to the instance is allowed. For more information, see Accessing no-ingress EC2 instances with AWS Systems Manager.

Note
When using this option, you need to create the AWSCloud9SSMAccessRole service role and AWSCloud9SSMInstanceProfile if they aren't already created. For more information, see Managing

instance profiles for Systems Manager with the AWS CLI.

--subnet-id represents the subnet you want AWS Cloud9 to use. Replace subnet-12a3456b with the ID of the subnet of an Amazon Virtual Private Cloud (VPC), which must be compatible with AWS Cloud9. For more information, see Create an Amazon VPC for AWS Cloud9 in VPC settings for AWS Cloud9 Development Environments.

AWS Cloud9 shuts down the Amazon EC2 instance for the environment after all web browser instances that are connected to the IDE for the environment have been closed. To configure this time period, add --automatic-stop-time-minutes and the number of minutes. A shorter time period might result in fewer charges to your AWS account. Likewise, a longer time might result in more charges.

By default, the entity that calls this command owns the environment. To change this, add --owner-id and the Amazon Resource Name (ARN) of the owning entity.

After you successfully run this command, open the AWS Cloud9 IDE for the newly created environment. To do this, see Opening an environment in AWS Cloud9. Then return to this topic and continue with Step 2: Basic tour of the IDE to learn how to use the AWS Cloud9 IDE to work with your new environment.

If you try to open the environment, but AWS Cloud9 doesn't display the IDE after at least five minutes, there might be a problem with your web browser, your AWS access permissions, the instance, or the associated VPC. For possible fixes, see Can't open an environment.

Lab Assignment No.	**10**
Title	Setup, Create and visualize data in an Amazon Relational Database (Amazon RDS) MS SQL Express server using Amazon Quick Sight.
Roll No.	
Class	TE
Date of Completion	
Subject	Mini Project(Cyber Security)
Assessment Marks	
Assessor's Sign	

ASSIGNMENT No: 10

Title: Setup, Create and visualize data in an Amazon Relational Database (Amazon RDS) MS SQL Express server using Amazon Quick Sight.

Problem Statement: Setup, Create and visualize data in an Amazon Relational Database (Amazon RDS) MS SQL Express server using Amazon Quick Sight.

Prerequisite:

Basic of Cloud

Software Requirements:

AWS

Hardware Requirement:

2GB RAM, 500 GB HDD

Learning Objectives:

Learning AWS Environment

Outcomes:

After completion of this assignment students are able to how to create IAM user to use in the account setup the AWS CLI

Theory: Amazon RDS for SQL Server makes it easy to set up, operate, and scale SQL Server deployments in the cloud.

Amazon QuickSight is a scalable, serverless, embeddable, machine learning-powered Business Intelligence (BI) service built for the cloud. Using the Amazon RDS connector in Amazon QuickSight, organizations can seamlessly gather insights from RDS data without a single line of code.

In this tutorial, you learn how to:

- Create a Microsoft SQL Server Express Edition database in Amazon RDS.
- Download and connect to a Microsoft SQL Server client.
- Create a sample database and tables, and load sample data to be accessed in Amazon QuickSight.
- Enable the security groups on Amazon RDS for Amazon QuickSight to connect to RDS datasets.

- Create an Amazon QuickSight account.
- Enable Amazon QuickSight to connect to Amazon RDS, and create a dataset for visualization.
- Clean up resources.

The AWS services you use in this tutorial are AWS Free Tier eligible.

About this Tutorial

Time	20 minutes
Cost	AWS Free Tier Eligible
Use Case	Analytics
Products	Amazon QuickSight, Amazon RDS for SQL Server
Audience	Developer
Level	Beginner
Last Updated	May 26, 2021

Step 1. Create an AWS Account
The resources created and used in this tutorial are AWS Free Tier eligible.
Sign-up for AWS

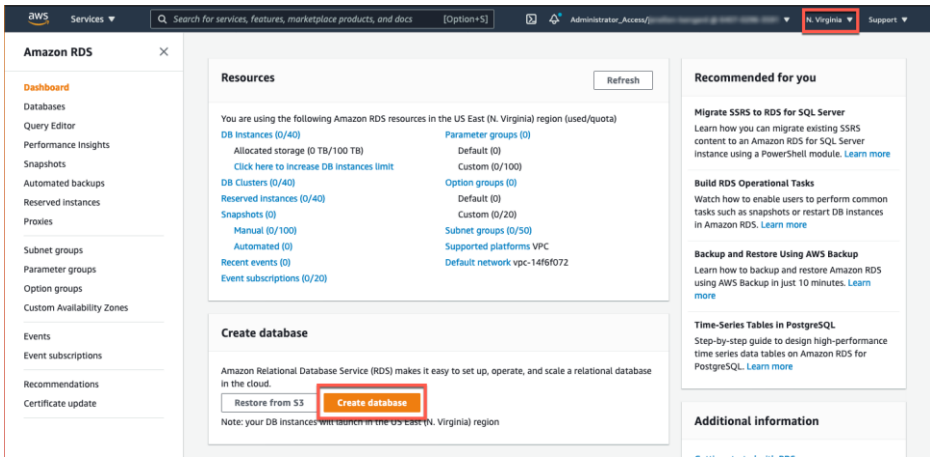
Already have an account? Sign-in

Step 2. Create a Microsoft SQL Server Express Edition database in Amazon RDS
Complete the following steps to connect to a Database Engine in Amazon RDS.

---

a. Open the Amazon RDS console and choose the Region where you want to create the Database.

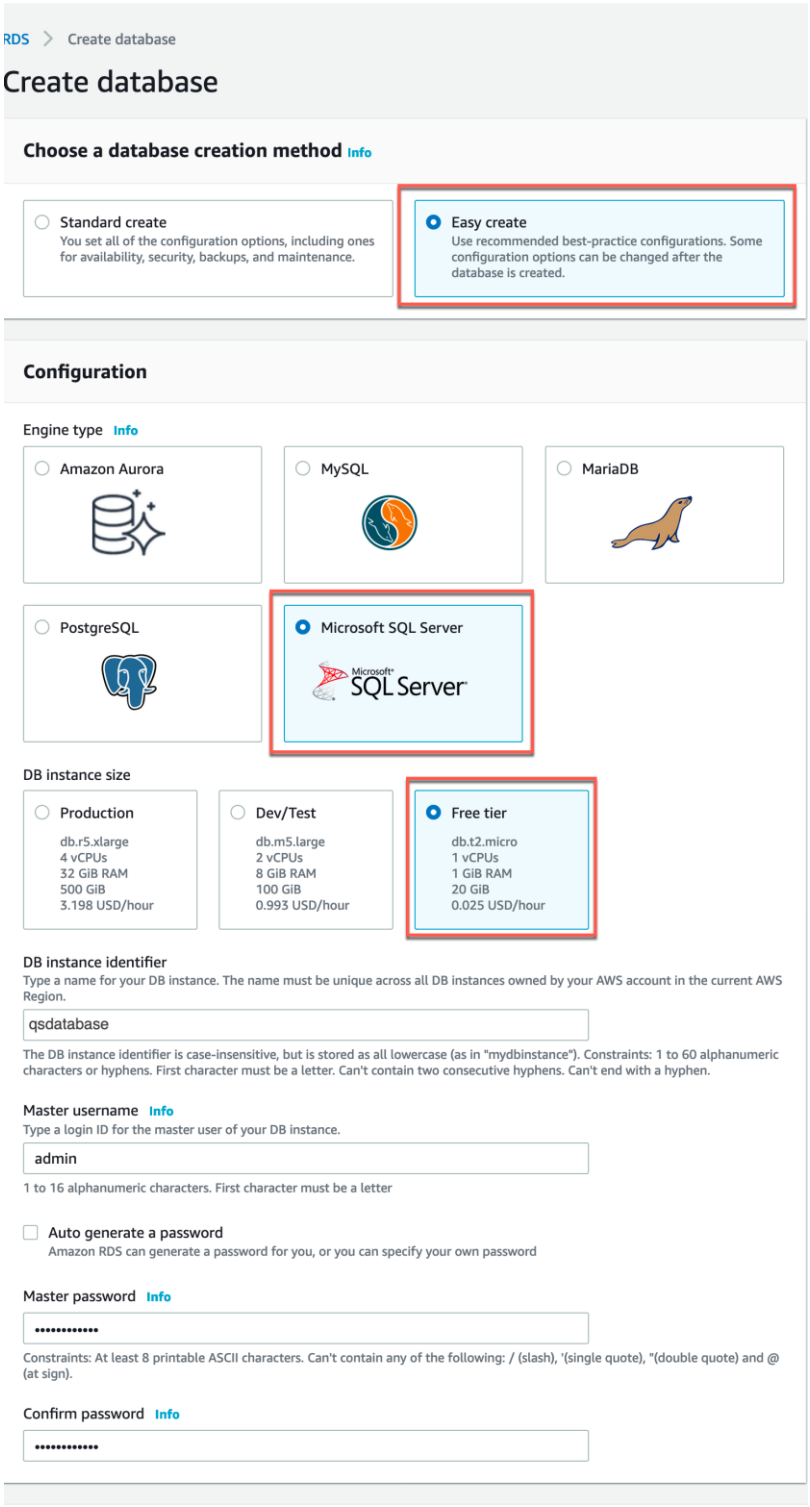
b. In the Create Database section, choose Create Database.



c. On the Create database page, in the Choose a database creation method section, choose Easy Create.

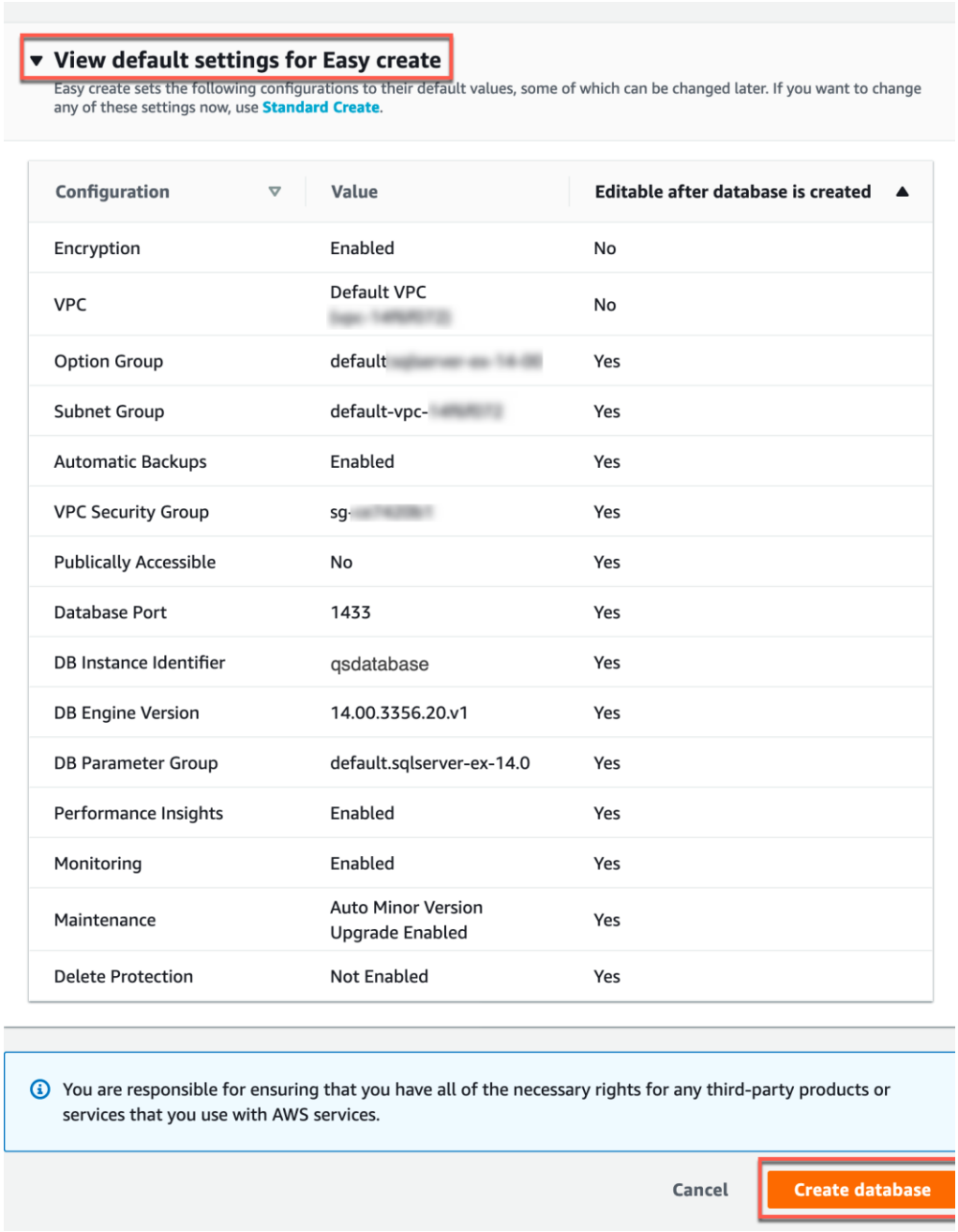
d. In the Configuration section, make the following changes:

- For Engine type, choose Microsoft SQL Server.
- For DB instance size, choose Free tier.
- For DB instance identifier, type qsdatabase.
- For Master username, enter admin.
- For Master password, type a unique password, and confirm password.



e. In the View default settings for Easy create drop down, leave the default settings. Then, choose Create database.

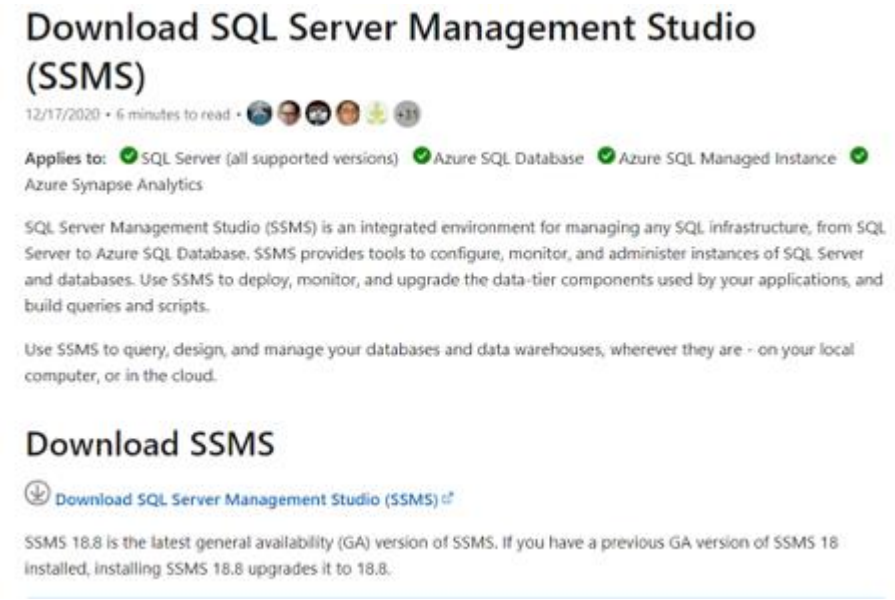
Note: It may take several minutes for the database to be created.



Step 3. Download and connect to a Microsoft SQL Server client
Complete the following steps to download Microsoft SQL Server Management Studio, and create tables to run queries against the database.

---

a. Open the Download Microsoft SQL Server Management Studio page, choose the link under the Download SSMS section.



Download SQL Server Management Studio (SSMS)

12/17/2020 • 6 minutes to read •

Applies to: SQL Server (all supported versions) Azure SQL Database Azure SQL Managed Instance Azure Synapse Analytics

SQL Server Management Studio (SSMS) is an integrated environment for managing any SQL infrastructure, from SQL Server to Azure SQL Database. SSMS provides tools to configure, monitor, and administer instances of SQL Server and databases. Use SSMS to deploy, monitor, and upgrade the data-tier components used by your applications, and build queries and scripts.

Use SSMS to query, design, and manage your databases and data warehouses, wherever they are - on your local computer, or in the cloud.

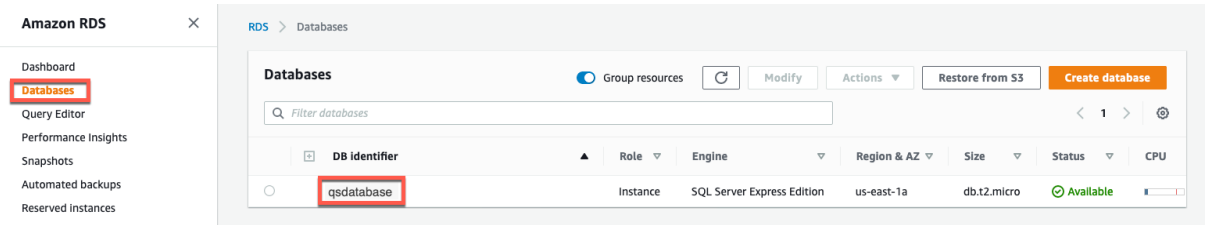
Download SSMS

Download SQL Server Management Studio (SSMS)

SSMS 18.8 is the latest general availability (GA) version of SSMS. If you have a previous GA version of SSMS 18 installed, installing SSMS 18.8 upgrades it to 18.8.

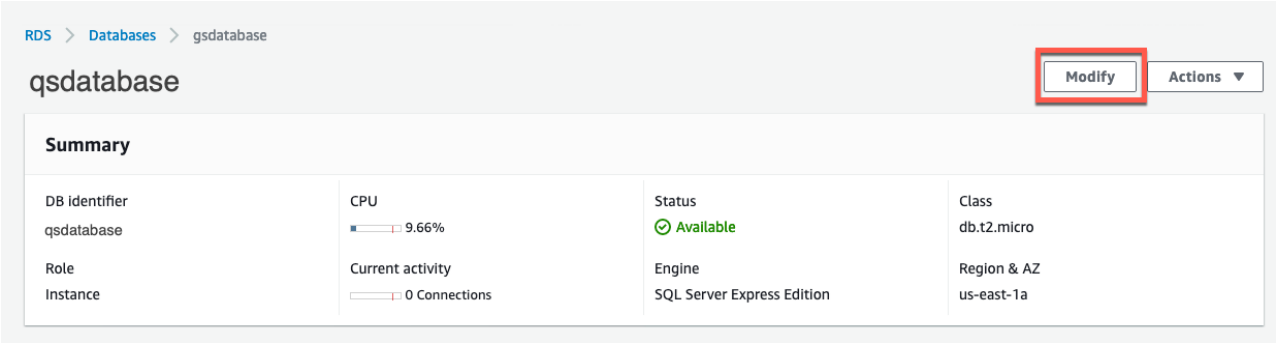
---

b. Open the Amazon RDS console, in the left-hand navigation pane, choose Databases. Then, choose the qsdatabase.

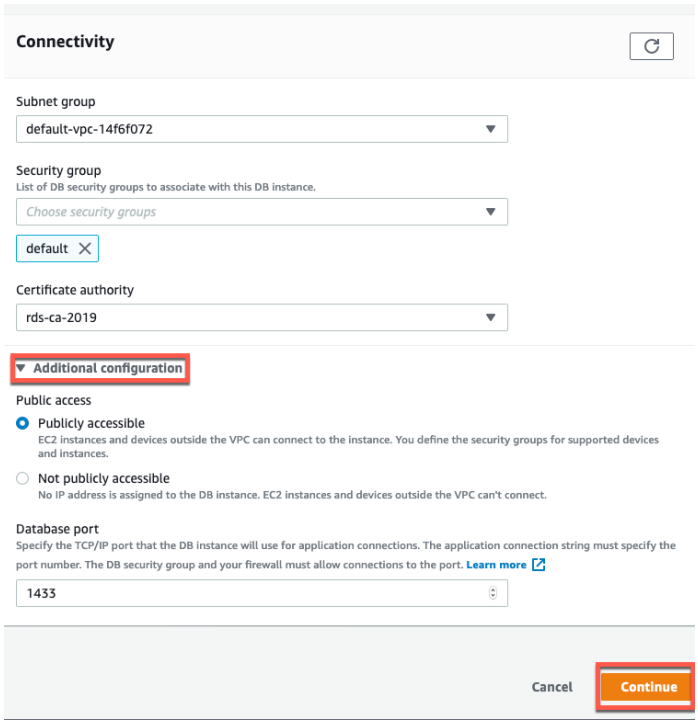


---

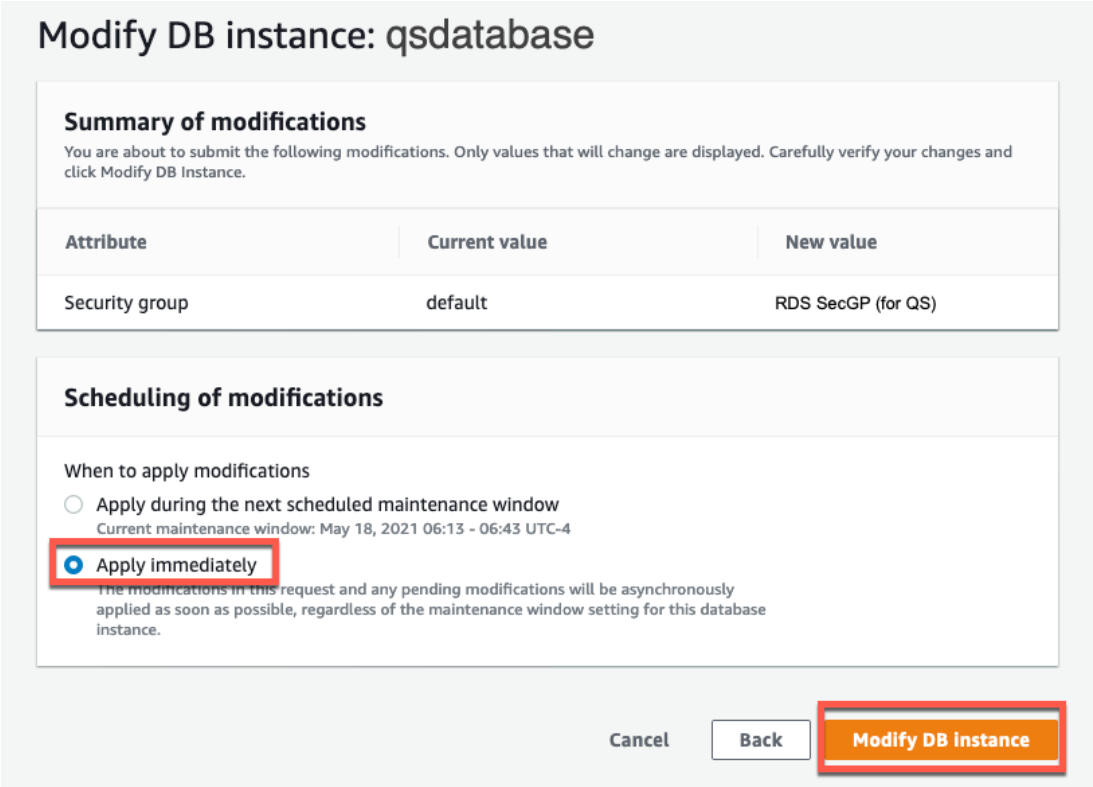
c. On the qsdatabase page, choose Modify.



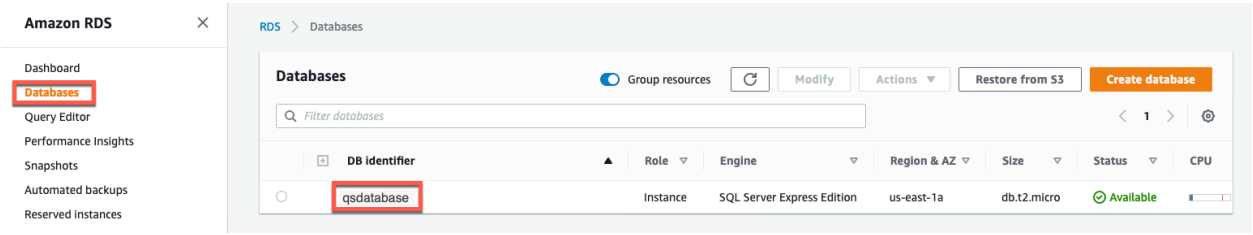
d. On the ModifyDB instance: qsdatabase page, in the Connectivity section, choose Additional Configuration. Then, choose Publicly accessible, and choose Continue.



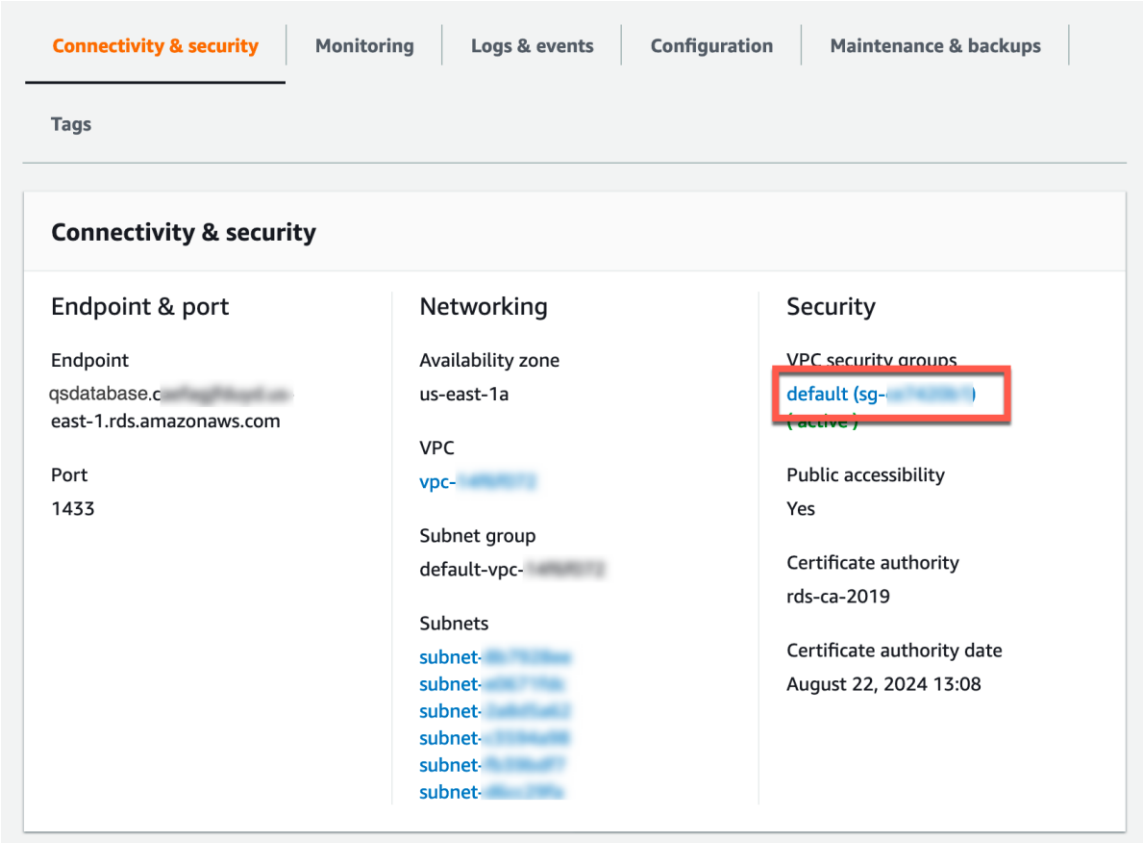
e. On the ModifyDB instance: qsdatabase page, in the Scheduling of modifications section, choose Apply immediately. Then, choose Modify DB instance.



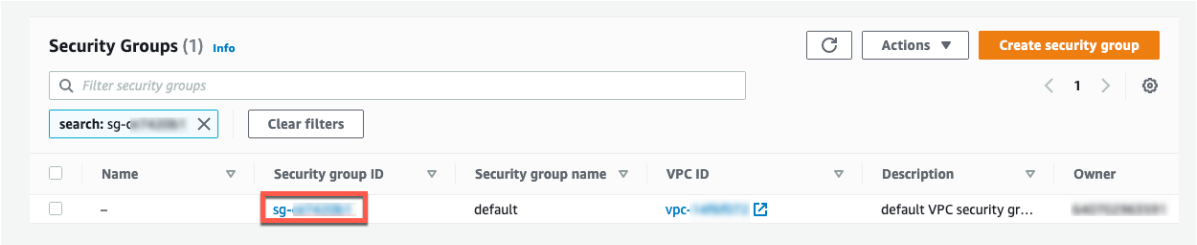
f. On the left-hand navigation, choose Databases. Then, choose qsdatabase.



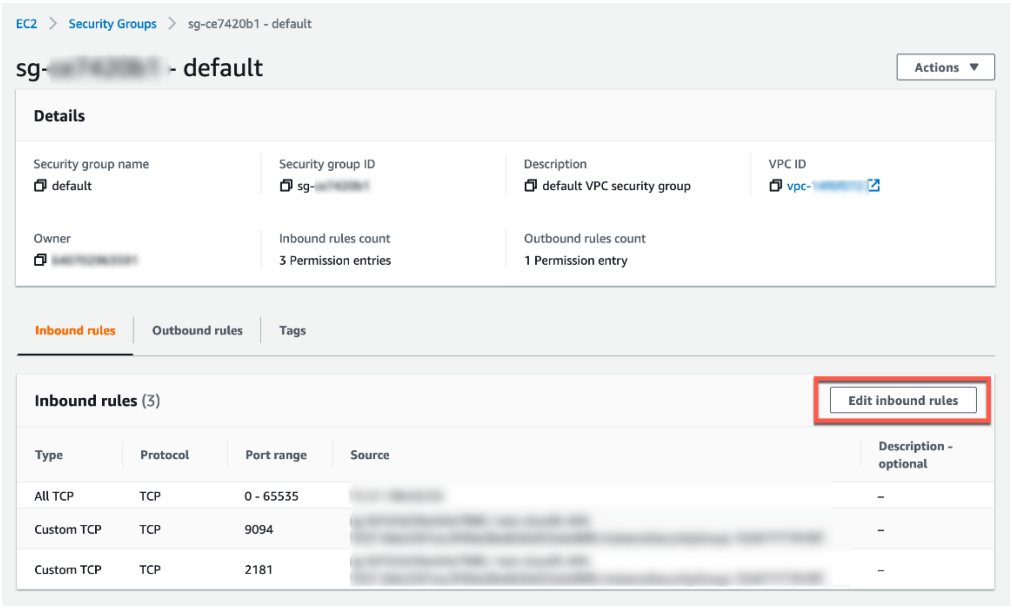
g. On the qsdatabase page, in the Connectivity & security section, choose the VPC security groups link.



h. On the Security groups page, choose the Security group ID.



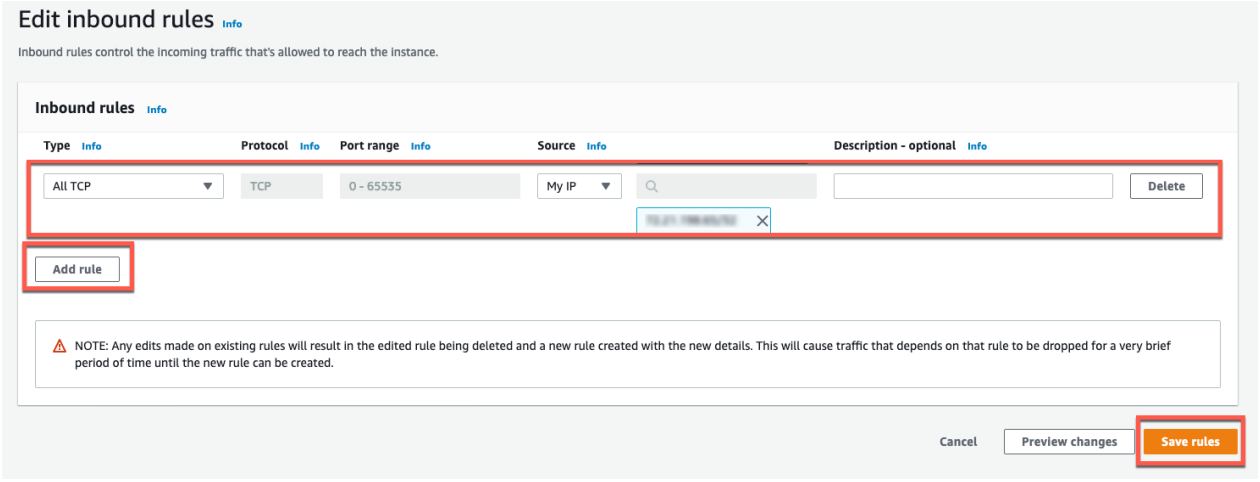
i. On the sg-default page, in the Inbound rules section, choose Edit inbound rules.



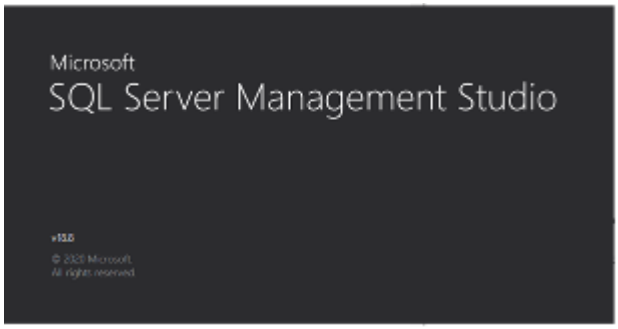
j. On the edit inbound rules page, in the Inbound rules section, choose Add rule, and make the following changes.

- For Type, choose All TCP from the drop-down list.
- For Source, choose My IP.

k. Then, choose Save rules.



l. Verify that the SSMS Client download has completed. Then, install and open the software.



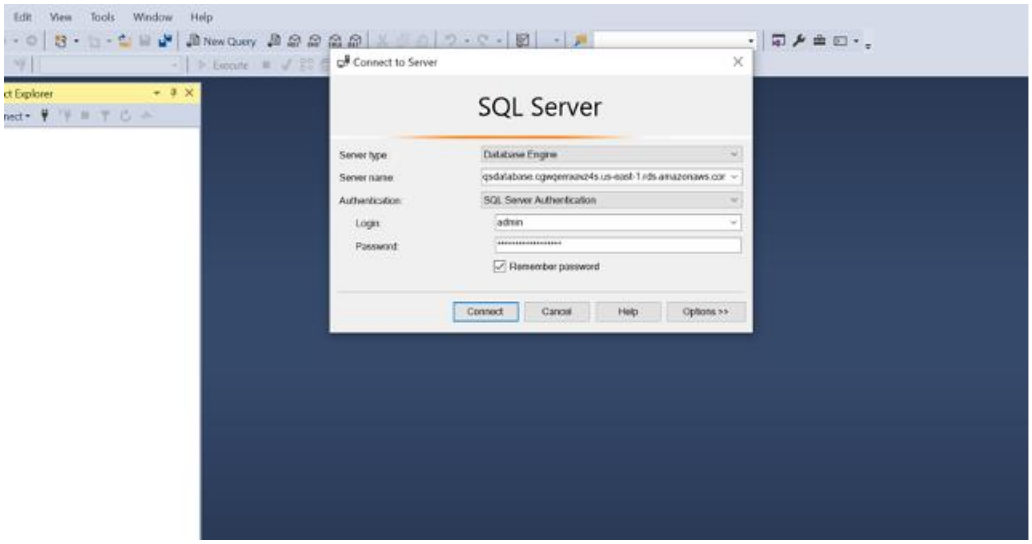
m. In the SQL Server pop up window, enter the following details.

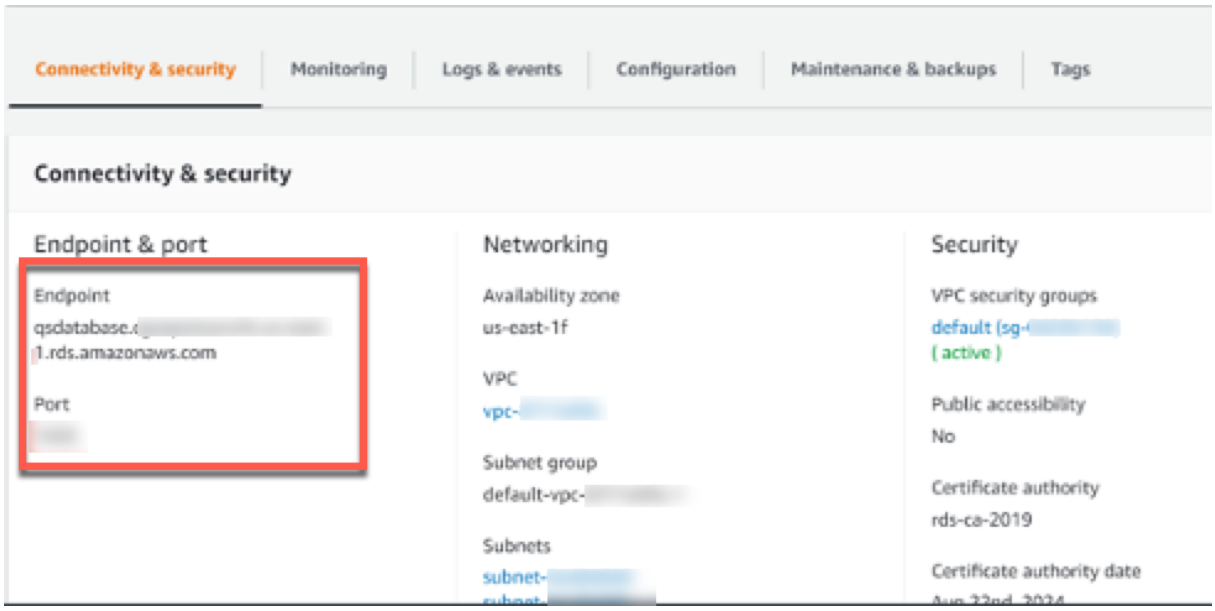
- For Server Name, paste the qsdatabase Endpoint and Port separated by commas. Example: qdatabase.abc.us-east-1.rds.amazonaws.com,1433.

  Note: To find the endpoint, open the Amazon RDS console, and choose qsdatabase. On the qsdatabase page, in the Connectivity & Security section, copy the Endpoint and Port.

- For Login, type the username you entered when creating the qsdatabase.
- For Password, type the password you entered when creating the qsdatabase.

n. Then, choose Connect.

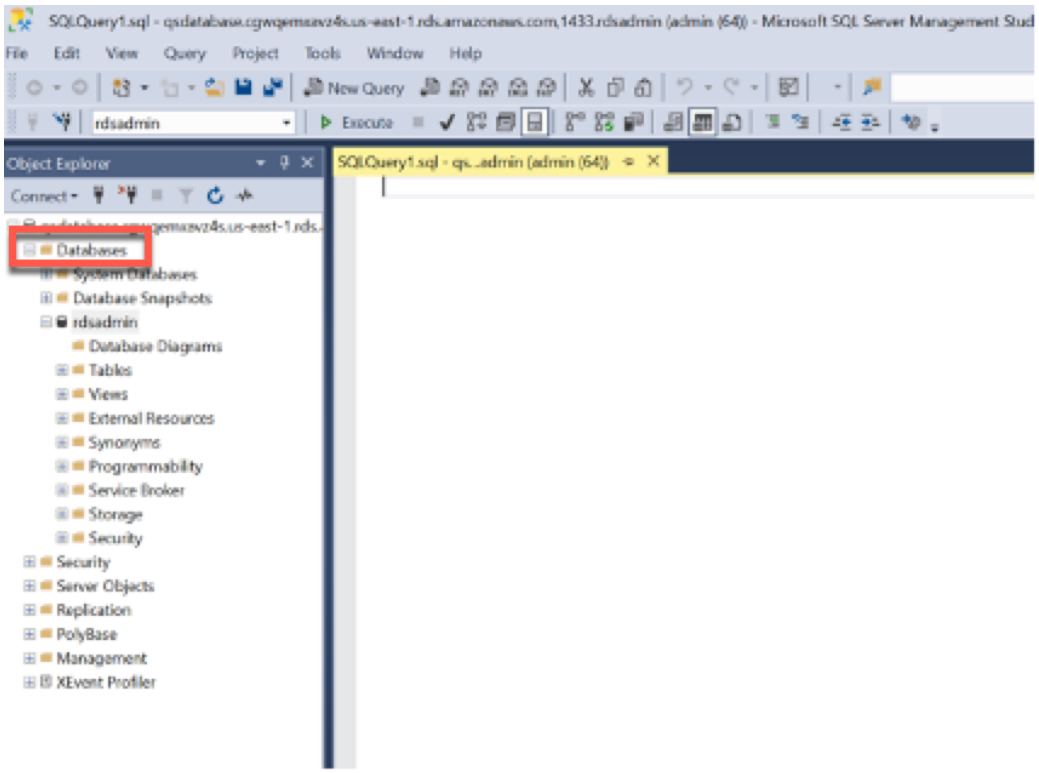




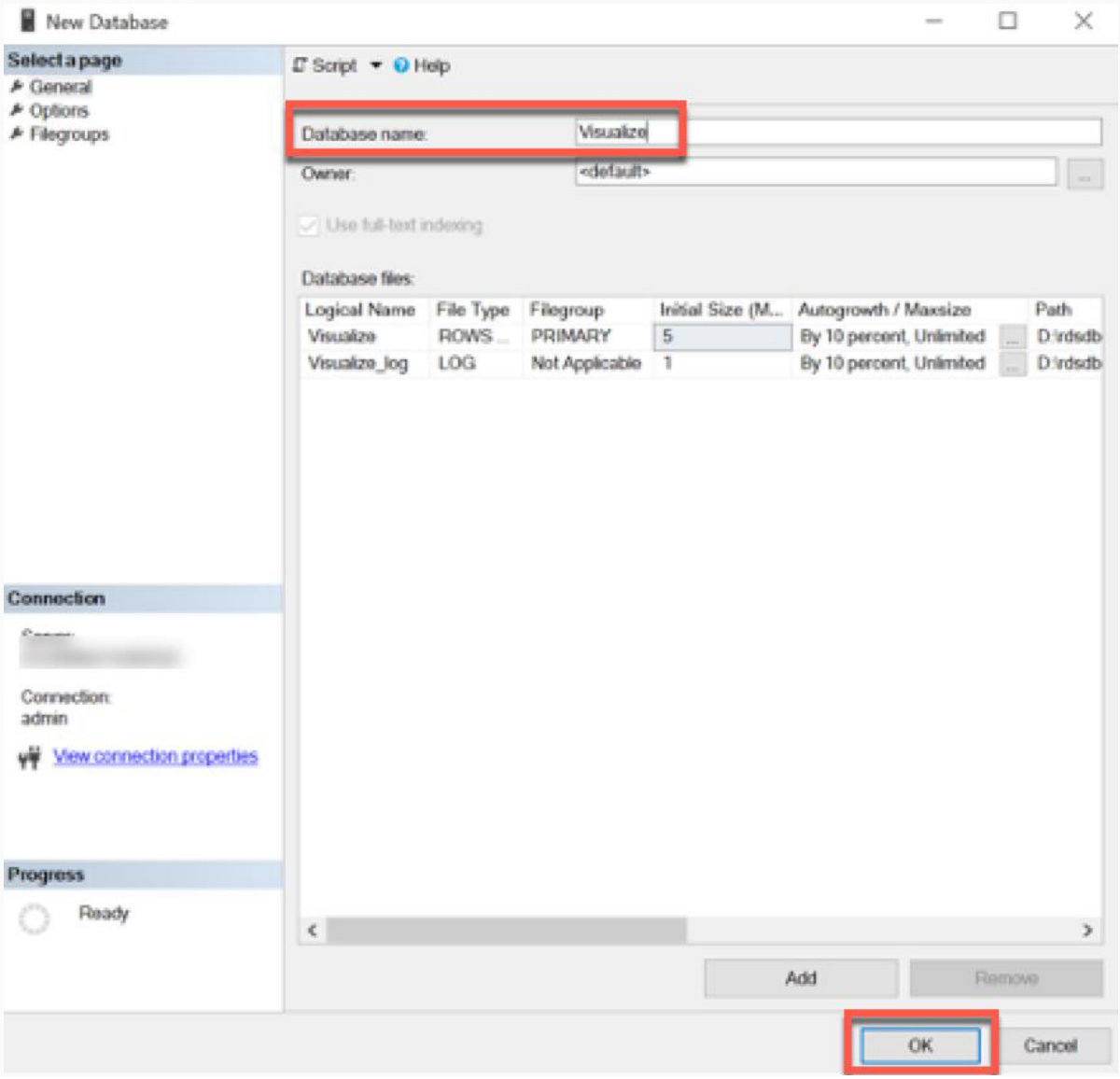
Step 4. Create a sample database and tables, and load sample data
Complete the following steps to create a sample database, create and load tables that can be accessed in Amazon QuickSight.

---

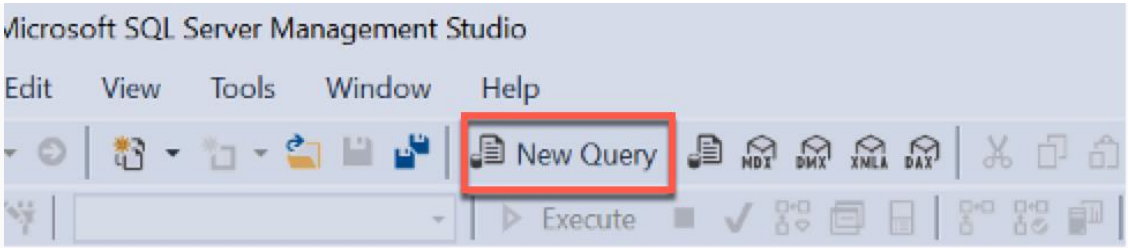
a. Open SQL Server Management Studio, in the left-hand navigation, choose Databases. Then, right click and choose Create Database.



b. On the New database page, for Database name, type Visualize. Then, choose OK.



c. Choose Visualize, and choose New Query.

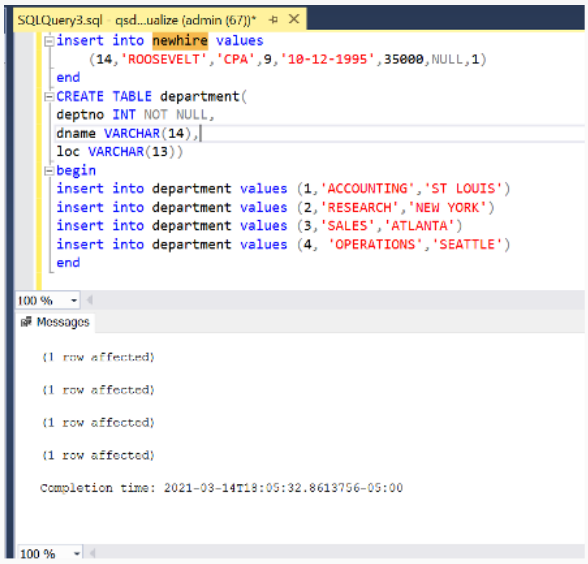


d. In the Query editor, copy and paste the following script.

Once the script is successfully run, the tables will be created and loaded with the sample data.

```
CREATE TABLE newhire(
empno INT PRIMARY KEY,
ename VARCHAR(10),
job VARCHAR(9),
manager INT NULL,
hiredate DATETIME,
salary NUMERIC(7,2),
comm NUMERIC(7,2) NULL,
department INT)
begin
insert into newhire values
   (1,'JOHNSON','ADMIN',6,'12-17-1990',18000,NULL,4)
insert into newhire values
   (2,'HARDING','MANAGER',9,'02-02-1998',52000,300,3)
insert into newhire values
   (3,'TAFT','SALES I',2,'01-02-1996',25000,500,3)
insert into newhire values
   (4,'HOOVER','SALES I',2,'04-02-1990',27000,NULL,3)
insert into newhire values
   (5,'LINCOLN','TECH',6,'06-23-1994',22500,1400,4)
insert into newhire values
   (6,'GARFIELD','MANAGER',9,'05-01-1993',54000,NULL,4)
insert into newhire values
   (7,'POLK','TECH',6,'09-22-1997',25000,NULL,4)
insert into newhire values
   (8,'GRANT','ENGINEER',10,'03-30-1997',32000,NULL,2)
insert into newhire values
   (9,'JACKSON','CEO',NULL,'01-01-1990',75000,NULL,4)
insert into newhire values
   (10,'FILLMORE','MANAGER',9,'08-09-1994',56000,NULL,2)
insert into newhire values
   (11,'ADAMS','ENGINEER',10,'03-15-1996',34000,NULL,2)
insert into newhire values
```

```
   (12,'WASHINGTON','ADMIN',6,'04-16-1998',18000,NULL,4)
insert into newhire values
   (13,'MONROE','ENGINEER',10,'12-03-2000',30000,NULL,2)
insert into newhire values
   (14,'ROOSEVELT','CPA',9,'10-12-1995',35000,NULL,1)
end
CREATE TABLE department(
deptno INT NOT NULL,
dname VARCHAR(14),
loc VARCHAR(13))
begin
insert into department values (1,'ACCOUNTING','ST LOUIS')
insert into department values (2,'RESEARCH','NEW YORK')
insert into department values (3,'SALES','ATLANTA')
insert into department values (4, 'OPERATIONS','SEATTLE')
end
Copy
```

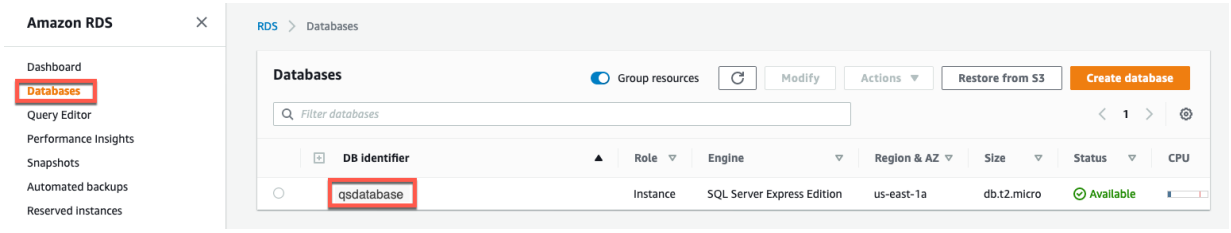


Step 5. Make the database instance Not publicly accessible
The database no longer needs to be publicly accessible; the previous script downloaded the required scripts from the client.

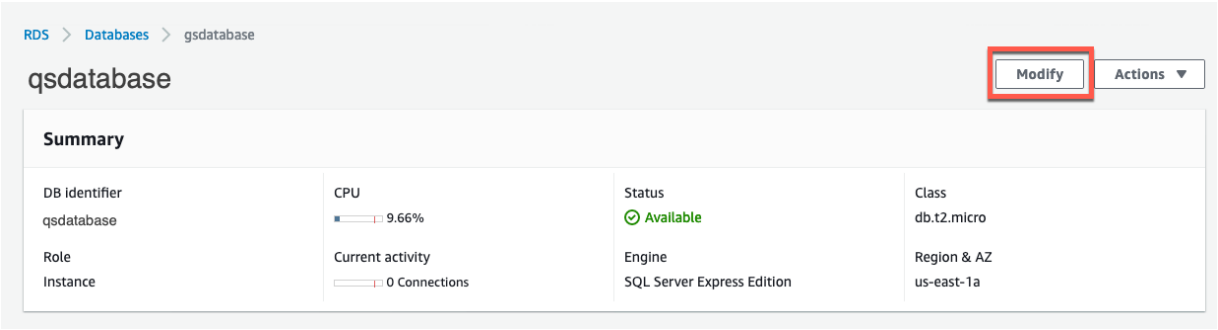
Complete these steps to connect Amazon QuickSight to RDS within a VPC.

---

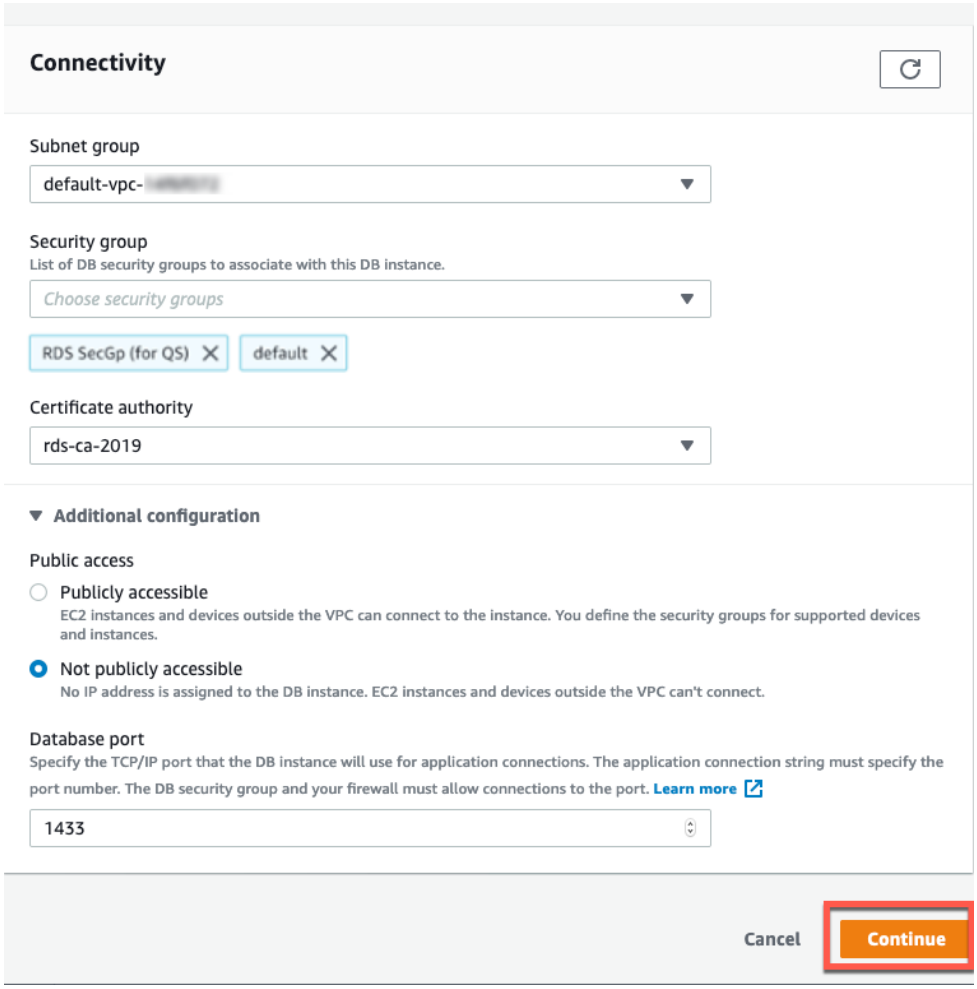
a. Open the Amazon RDS console, in the left-hand navigation, choose Databases. Then, choose the qsdatabase.



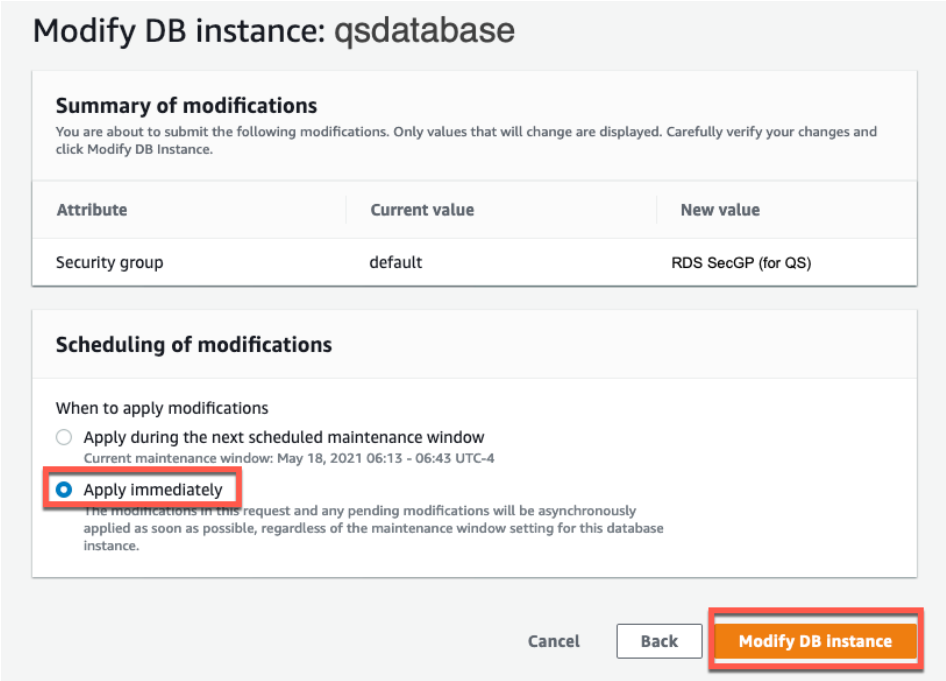
b. On the qsdatabase page, choose Modify.



c. On the ModifyDB instance:qsdatabase page, in the Connectivity section, choose Additional Configuration. Then, choose Not publicly accessible, and choose Continue.



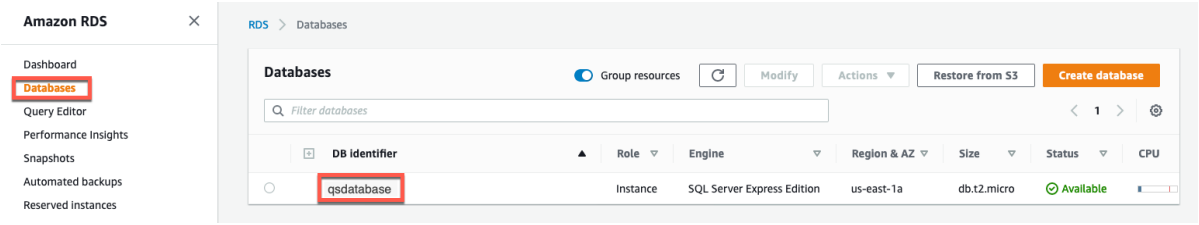
d. On the ModifyDB instance:qsdatabase page, in the Scheduling of modifications section, choose Apply immediately. Then, choose Modify DB instance.



Step 6. Enable the RDS database instance for access to Amazon QuickSight
Follow these steps to create a security group for Amazon QuickSight to access the RDS database in a VPC.

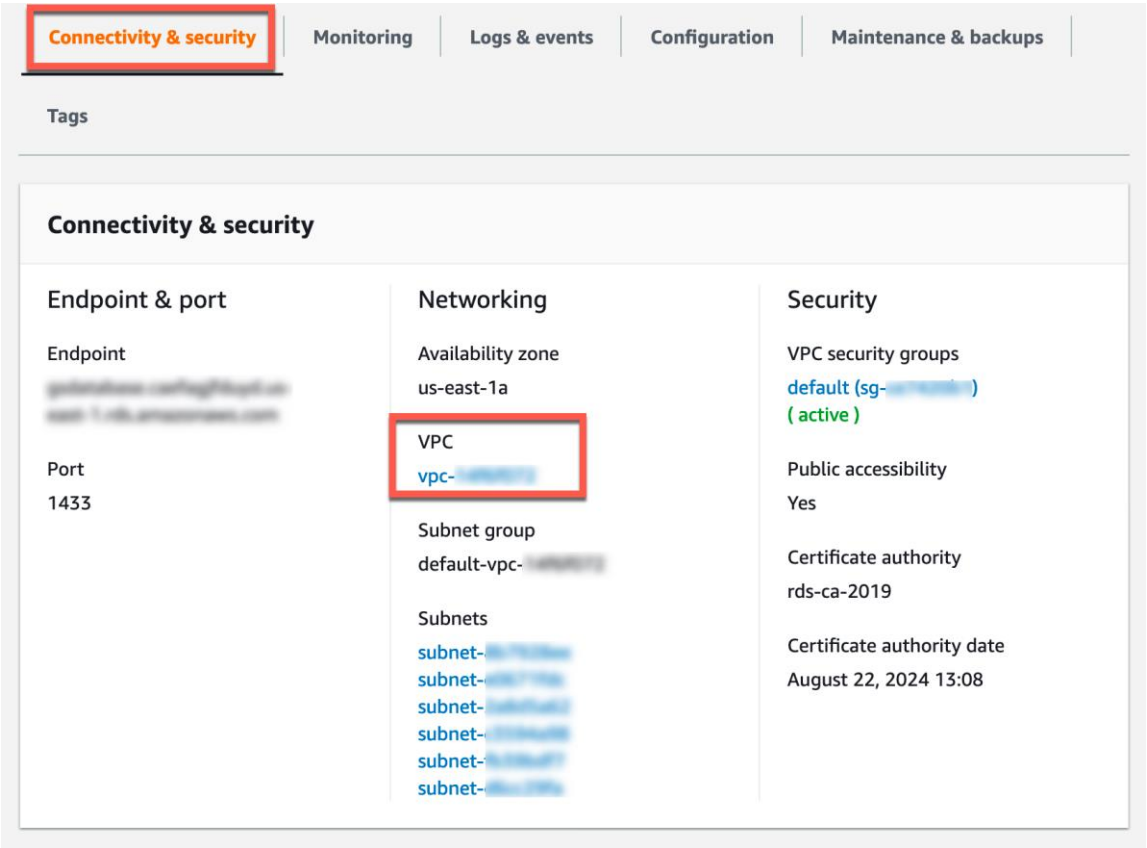
---

a. Open the Amazon RDS console, in the left-hand navigation, choose Databases. Then, choose the qsdatabase.

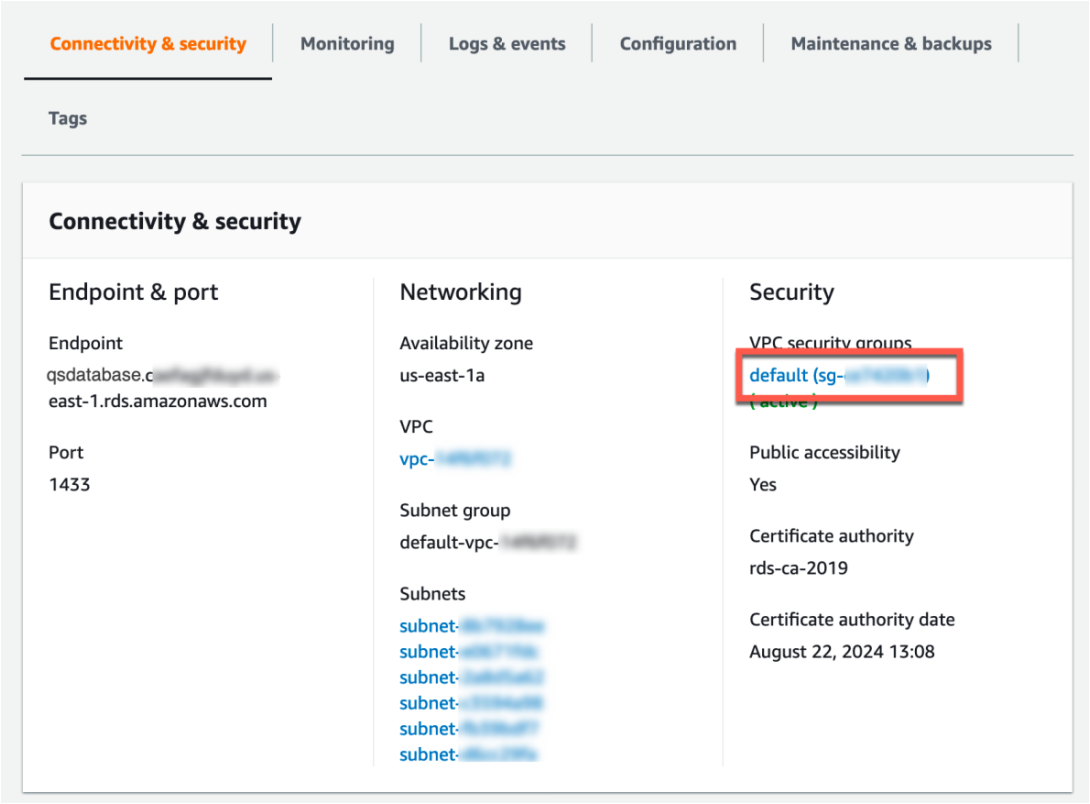


---

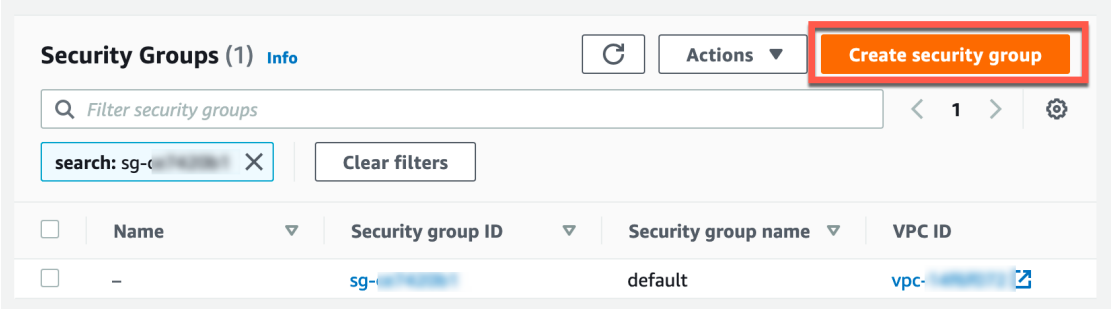
b. On the qsdatabase page, in the Connectivity & security section, copy the VPC id.



c. Under Security, choose the VPC security groups link.



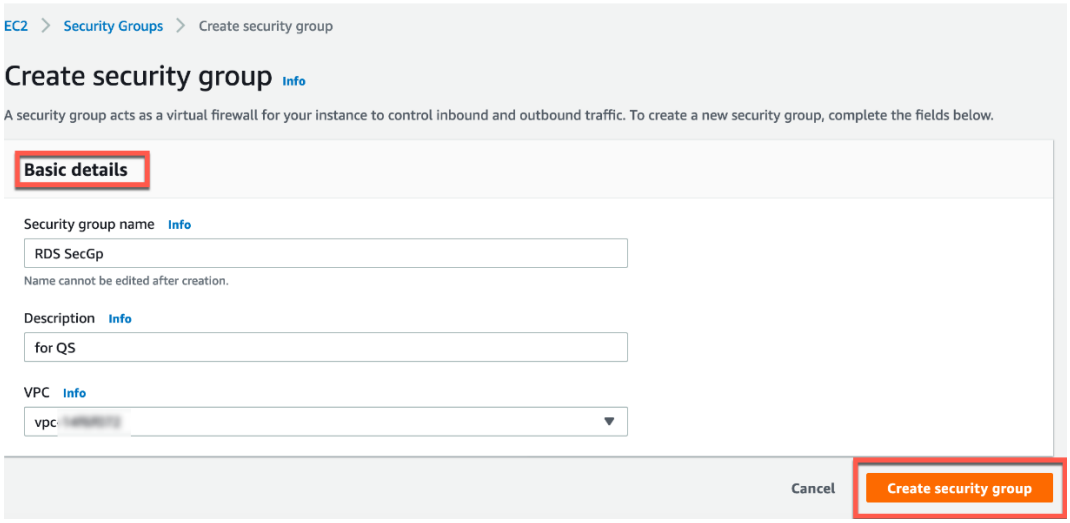
d. On the Security Groups page, choose Create security group.



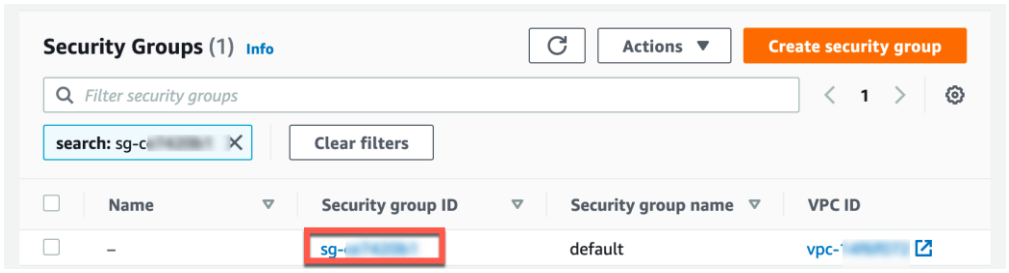
e. On the Create security group page, in the Basic details section, enter the following details.

- For Name, type RDS SecGP
- For Description, type for QS
- For VPC, choose the VPC id for your RDS instance.

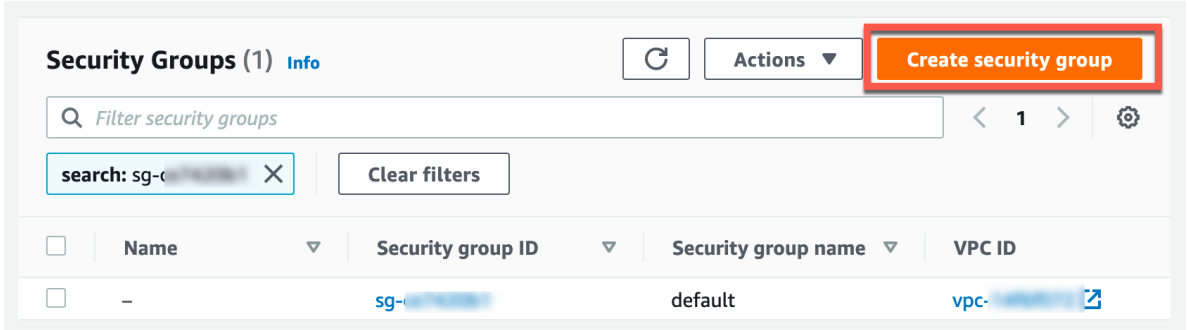
f. Then, choose Create security group.



g. On the Security Groups page, copy the Security group ID.



h. On the Security Groups page, choose Create security group.



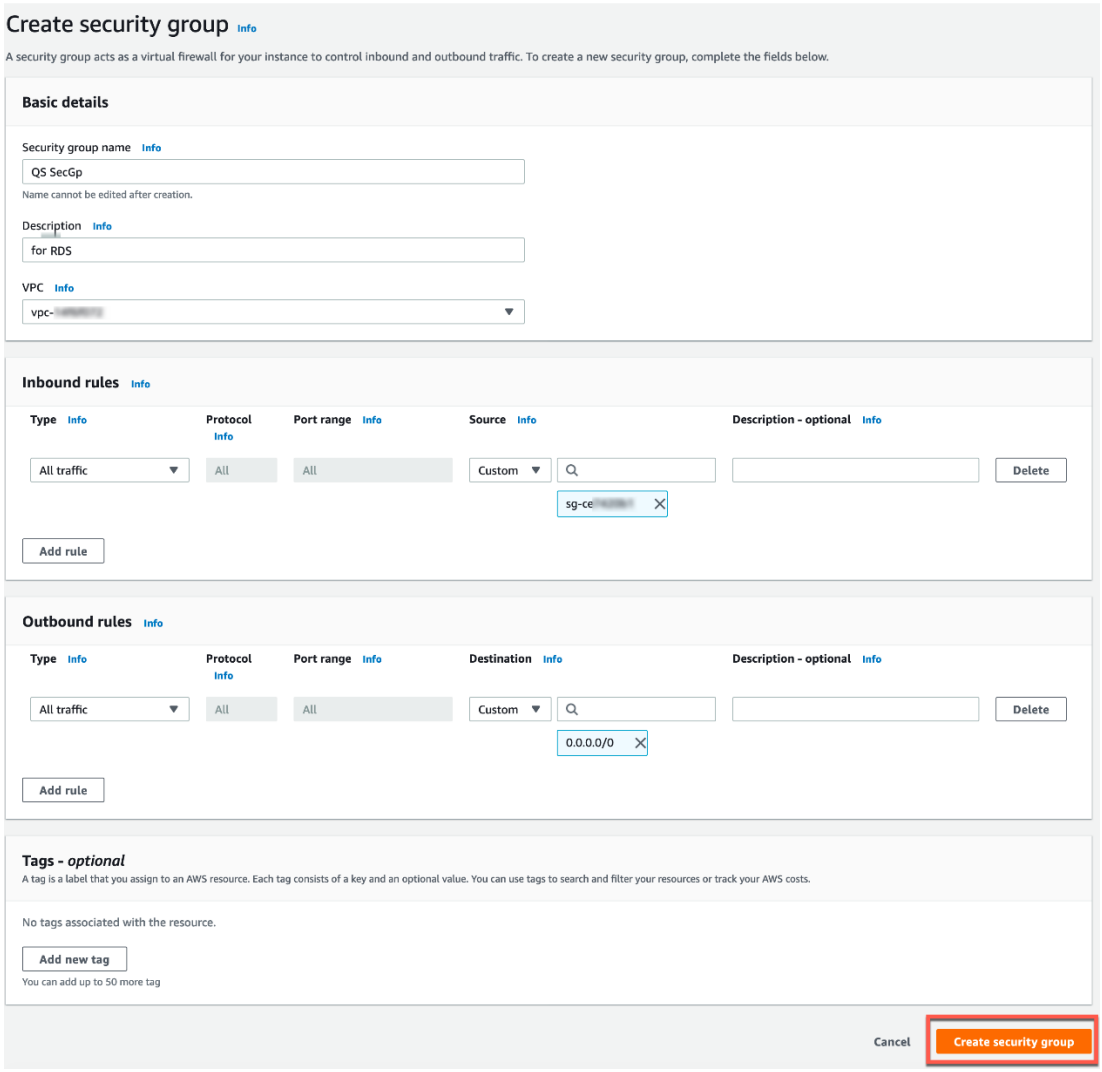
i. On the Create security group page, in the Basic details section, enter the following details.

- For Name, type QS SecGP
- For Description, type for RDS
- For VPC, choose the VPC id for your RDS instance.

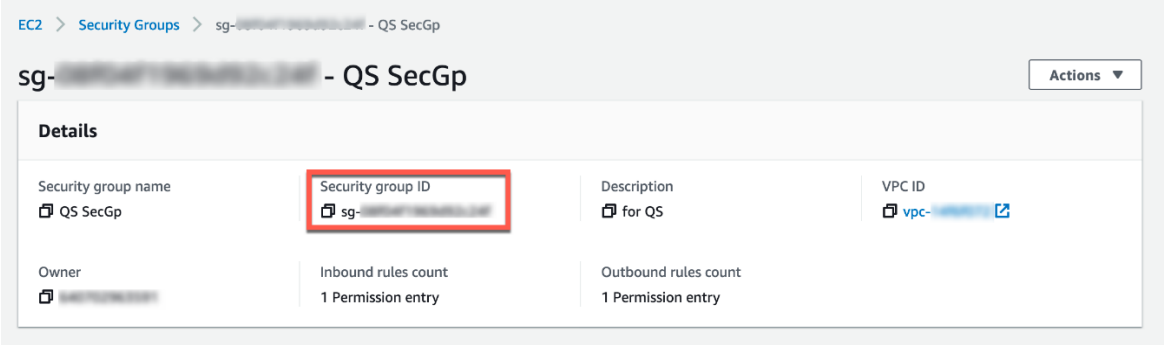
j. In the Inbound rules section, choose Add rule.

- For Type, choose All traffic
- For Source, choose Custom
- In the search box, paste the security group id you copied in step 6.g.

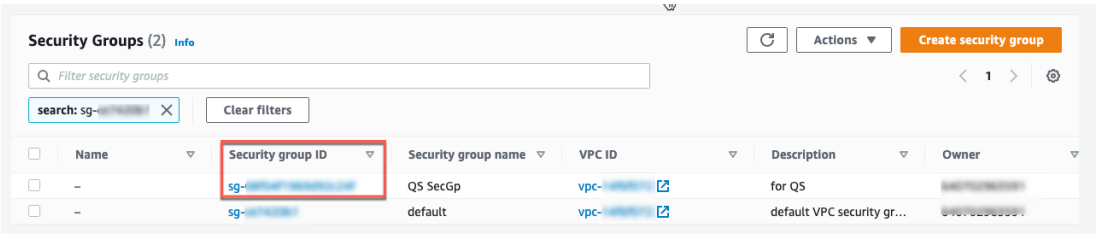
k. Choose Create security group.



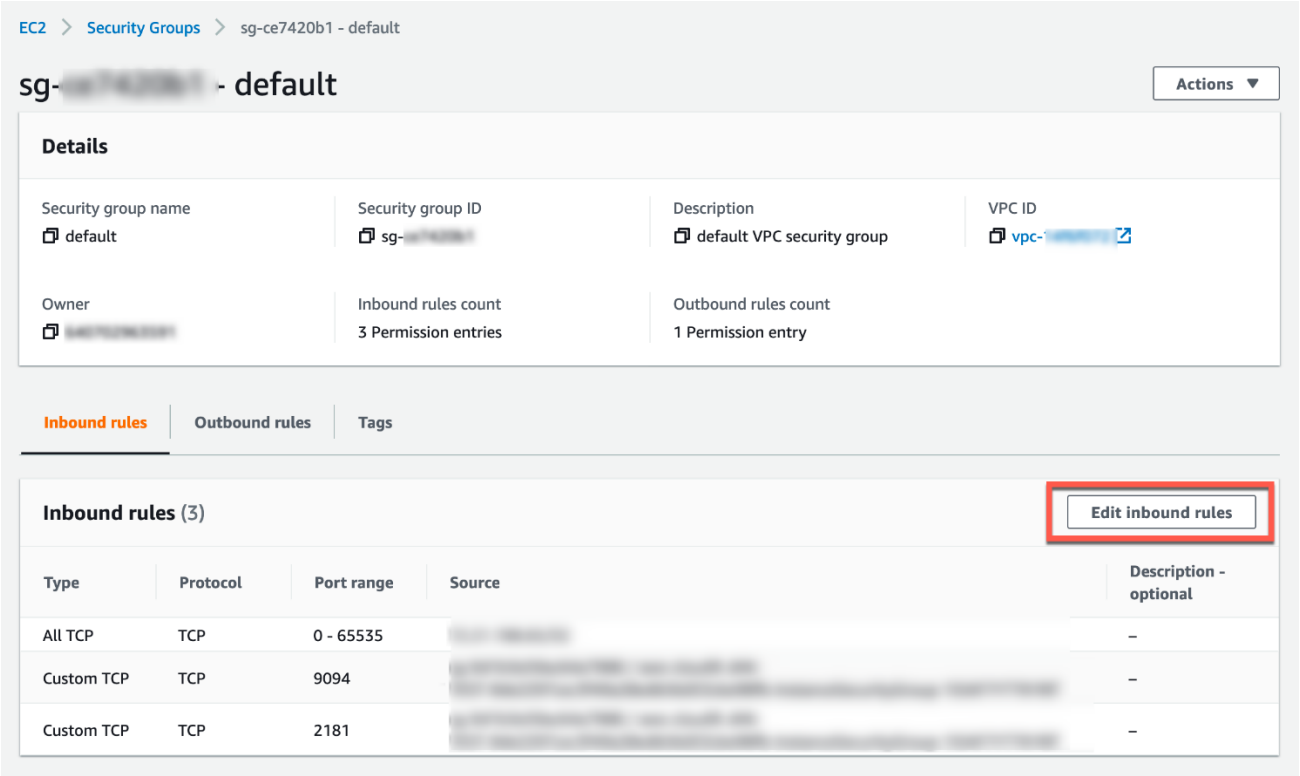
l. On the sg-QS SecGp page, copy the security group id. This security group is needed for Amazon QuickSight to connect to Amazon RDS.



m. On the Security Groups page, choose the security group you created in step 6.g.



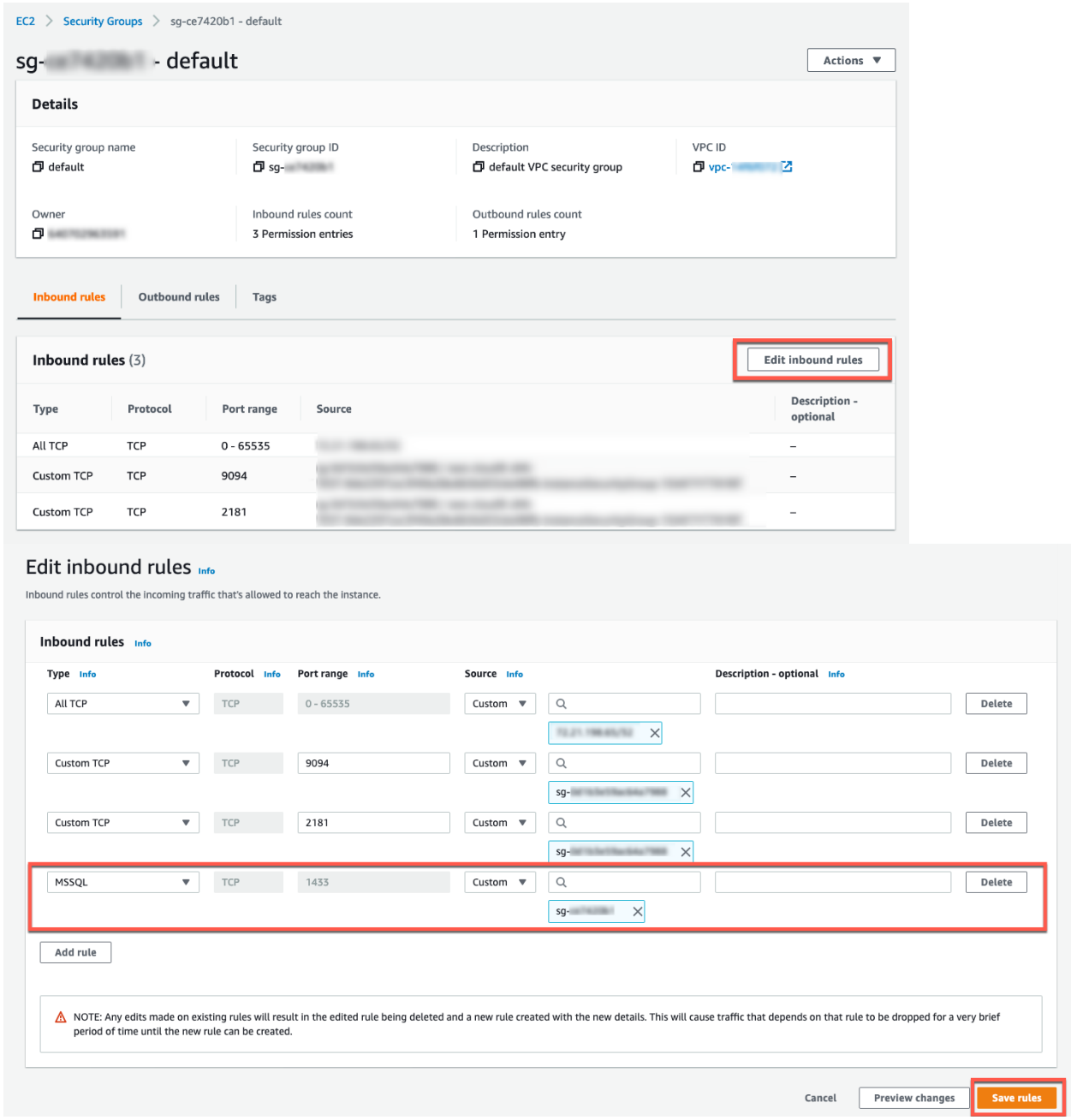
n. In the Inbound rules section, choose Edit inbound rules.



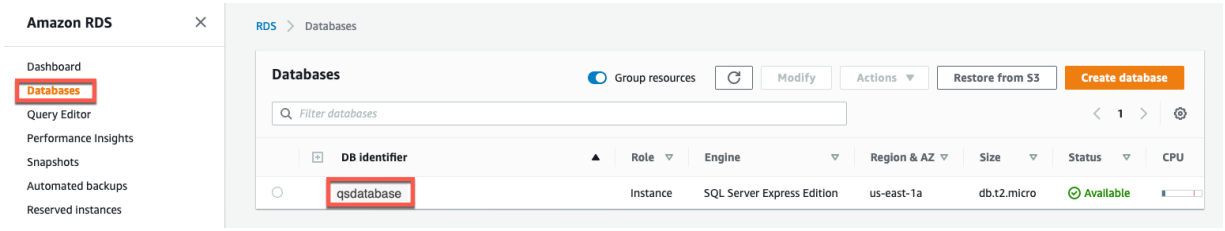
o. On the Edit inbound rules page, in the Inbound rules section, choose Add rule. Then, enter the following details.

- For Type, choose MSSQL
- For Source, choose Custom
- In the search box, paste the security group id you copied in Step 6.l

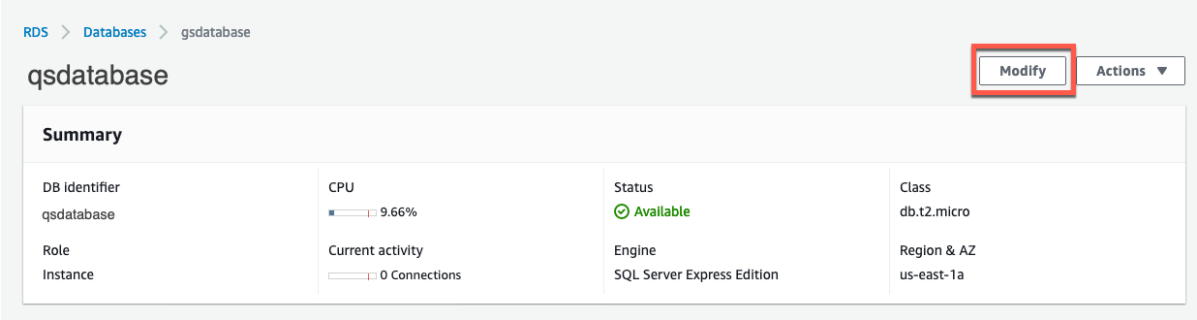
p. Choose Save rules. This security group is needed for Amazon RDS to connect Amazon QuickSight.



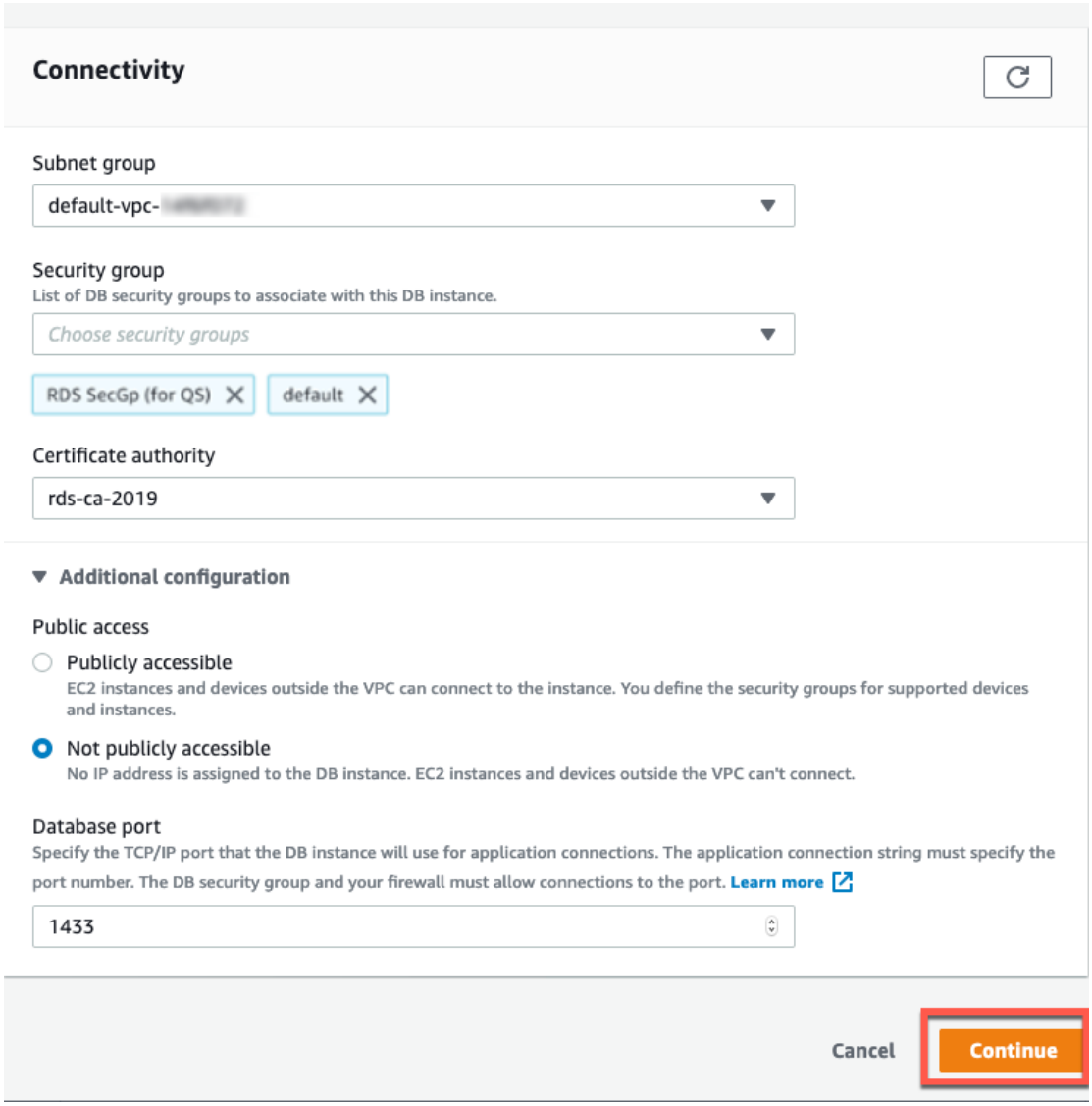
q. Open the Amazon RDS console, in the left-hand navigation, choose Databases. Then, choose the qsdatabase.



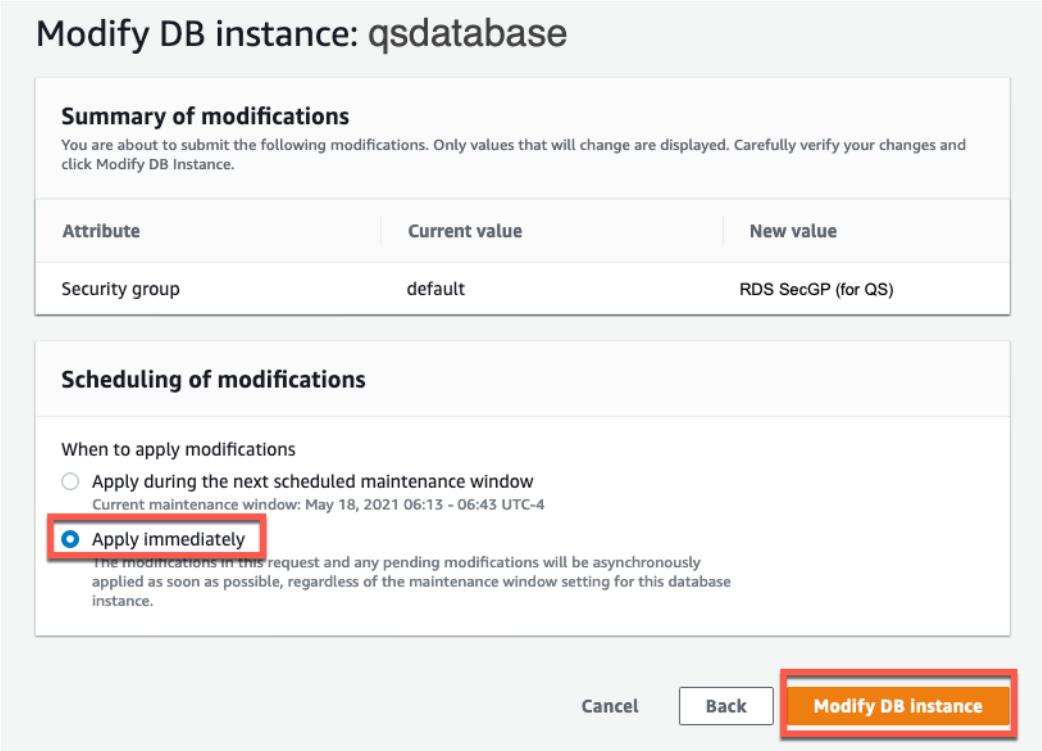
r. On the qsdatabase page, choose Modify.



s. On the Modify DB instance: qsdatabase page, in the Connectivity section, for Security group, choose RDS SecGP (for QS). Then, choose Continue.



t. On the Modify DB instance: qsdatabase page, in the Scheduling of modifications section, choose Apply immediately. Then, choose Modify DB instance.

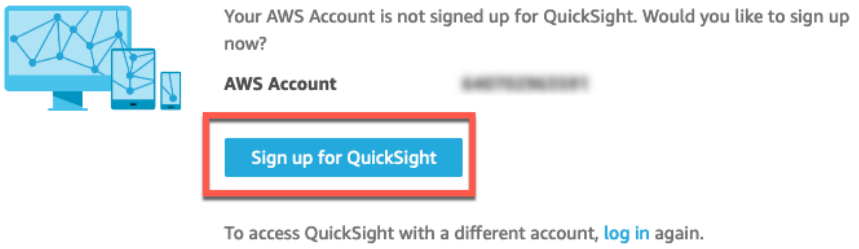


Step 7. Create your Amazon QuickSight account
Complete the following steps to create your Amazon QuickSight account.

Note: For more information, see Setting up Amazon QuickSight in the Amazon QuickSight documentation.

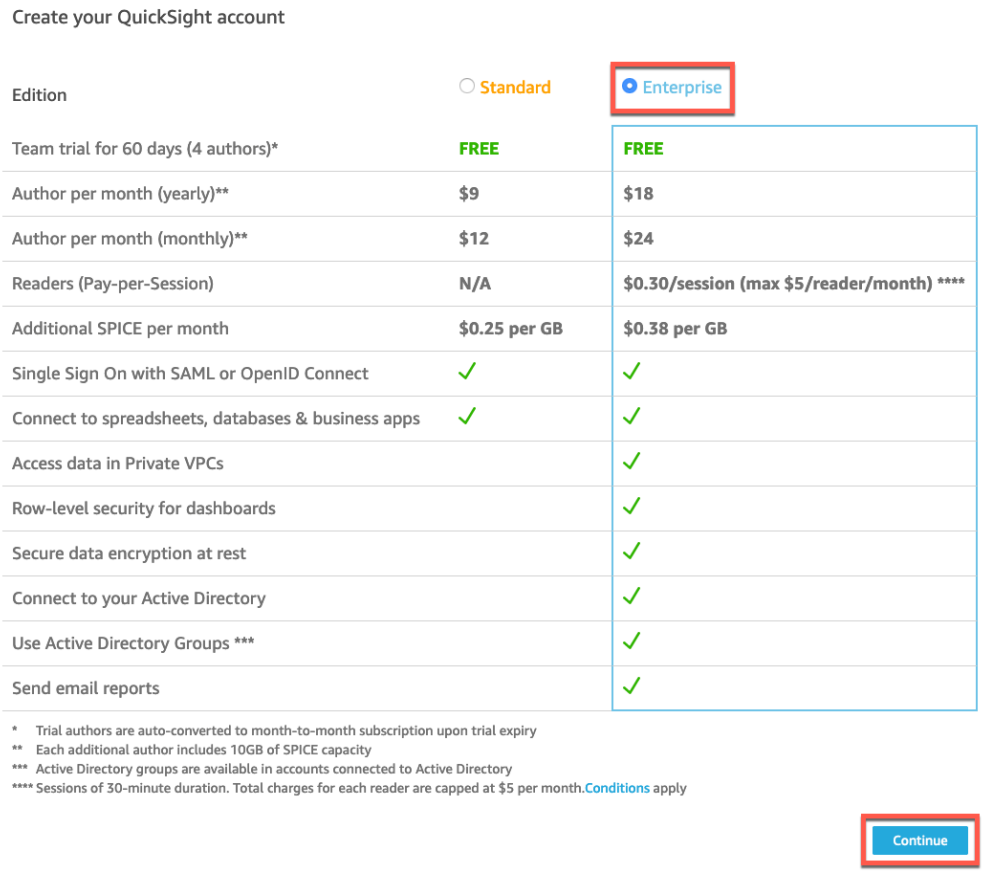
---

a. Open the Amazon QuickSight landing page, and choose Sign up for QuickSight.



---

b. On the Create you QuickSight account page, for Edition, choose Enterprise, and choose Continue.



Create your QuickSight account

Edition	Standard	Enterprise
Team trial for 60 days (4 authors)*	FREE	FREE
Author per month (yearly)**	$9	$18
Author per month (monthly)**	$12	$24
Readers (Pay-per-Session)	N/A	$0.30/session (max $5/reader/month) ****
Additional SPICE per month	$0.25 per GB	$0.38 per GB
Single Sign On with SAML or OpenID Connect	✓	✓
Connect to spreadsheets, databases & business apps	✓	✓
Access data in Private VPCs		✓
Row-level security for dashboards		✓
Secure data encryption at rest		✓
Connect to your Active Directory		✓
Use Active Directory Groups ***		✓
Send email reports		✓

* Trial authors are auto-converted to month-to-month subscription upon trial expiry
** Each additional author includes 10GB of SPICE capacity
*** Active Directory groups are available in accounts connected to Active Directory
**** Sessions of 30-minute duration. Total charges for each reader are capped at $5 per month.Conditions apply

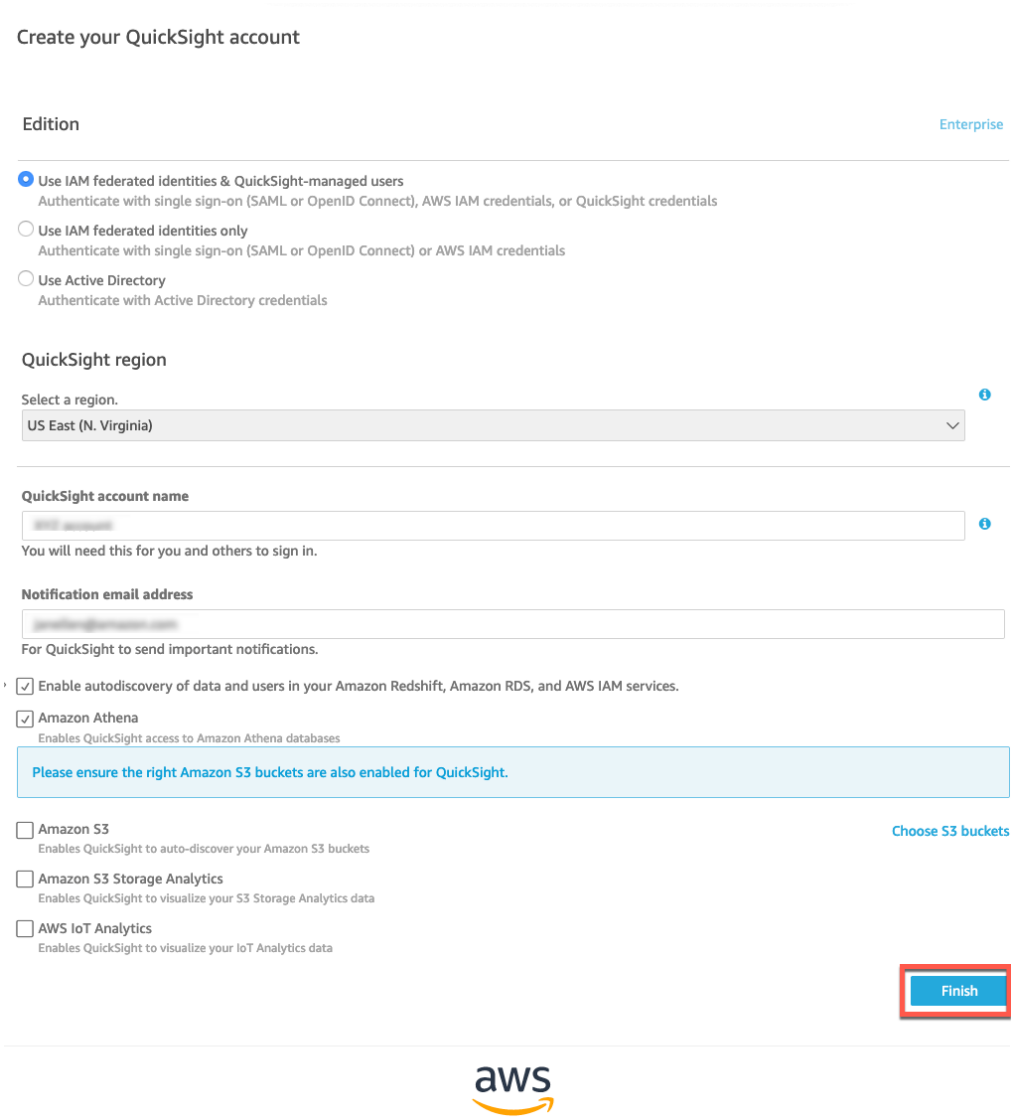
Continue

c. On the Create your QuickSight account page, in the Edition section, choose Use IAM federated identities and QuickSight-managed users.

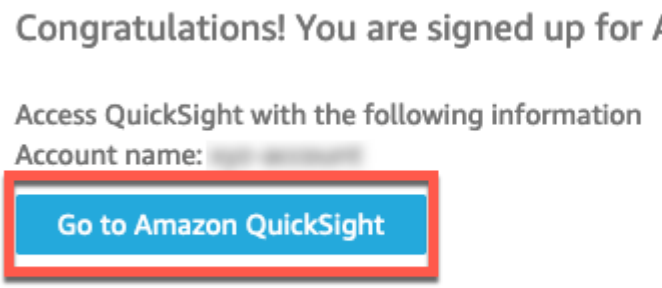
d. In the QuickSight region section, enter the following details.

- Select a region from the drop-down list.
- For QuickSight account name, type a unique account name.
- For Notification email address, type an email address where you will receive notifications.

e. Then, choose Finish.



f. Choose Go to Amazon QuickSight, to open the Amazon QuickSight console.

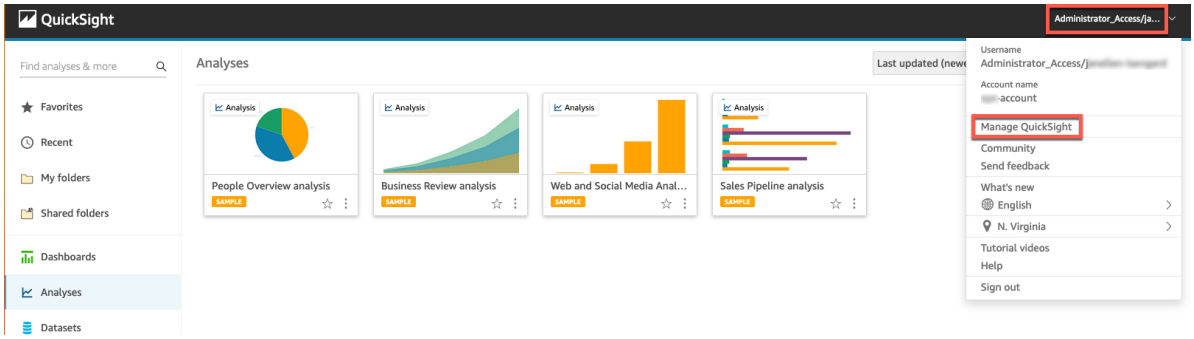


Step 8. Enable Amazon QuickSight to connect to Amazon RDS and create a dataset for visualization Complete the following steps to create a secure private connection to an Amazon VPC, and visualize the Amazon RDS data.

Note: For more information, see Configuring the VPC Connection in the QuickSight Console in the Amazon QuickSight documentation.

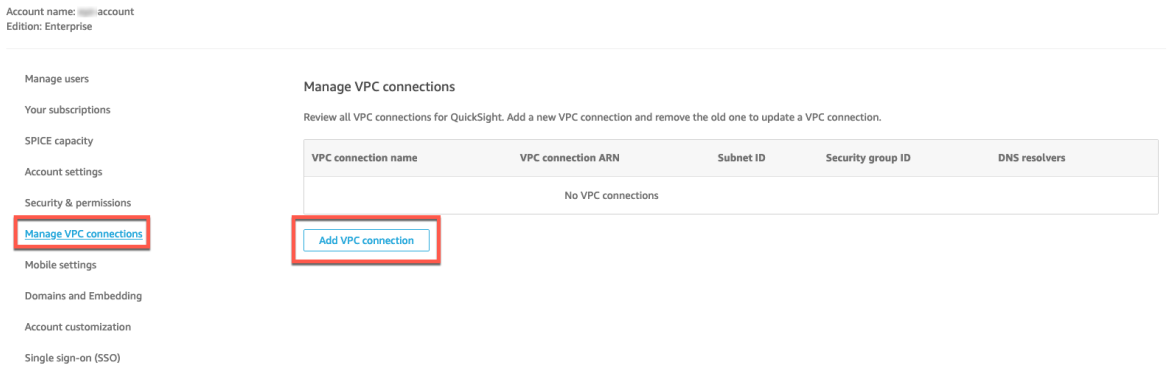
---

a. On the Analyses page, in the top right corner of the screen, and choose your username. Then, from the drop-down list, choose Manage QuickSight.

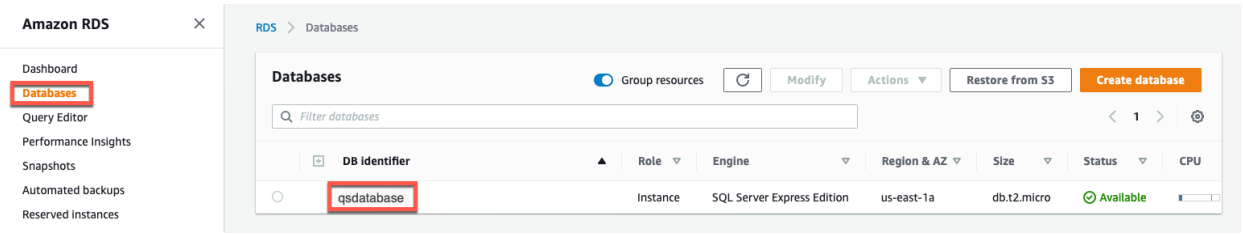


---

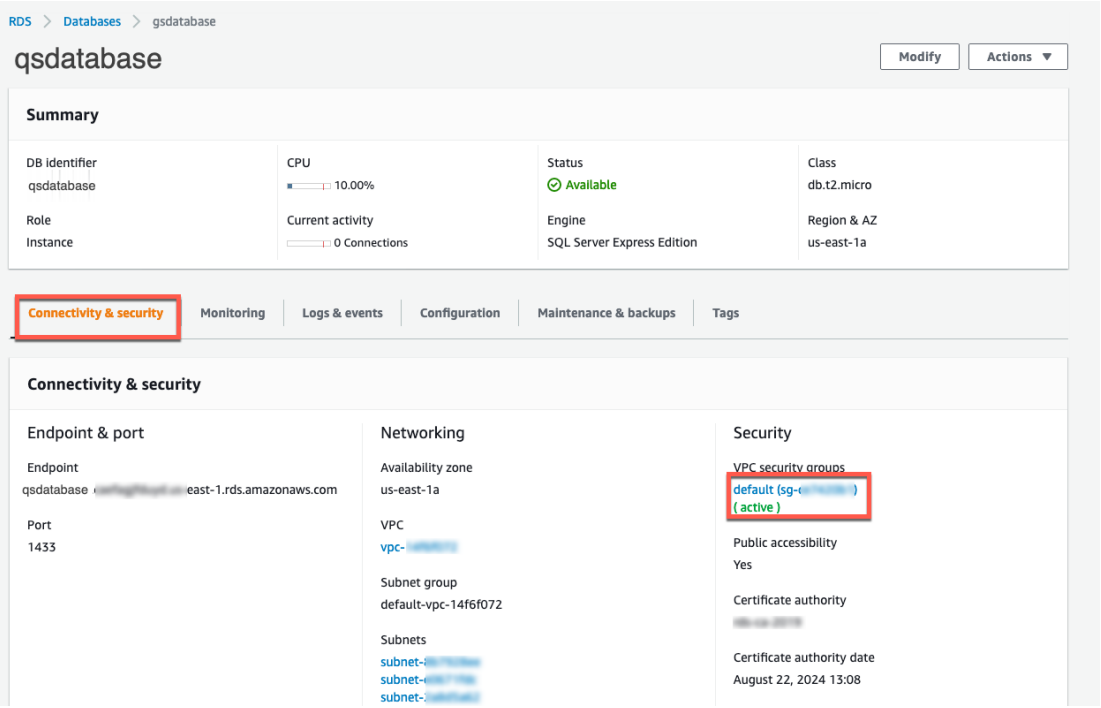
b. On the left navigation pane, choose Manage VPC connections. Then, choose Add VPC connection.



c. In your web browser, open a new tab. Then, open the Amazon RDS console, in the left-hand navigation, choose Databases. Then, choose the qsdatabase.



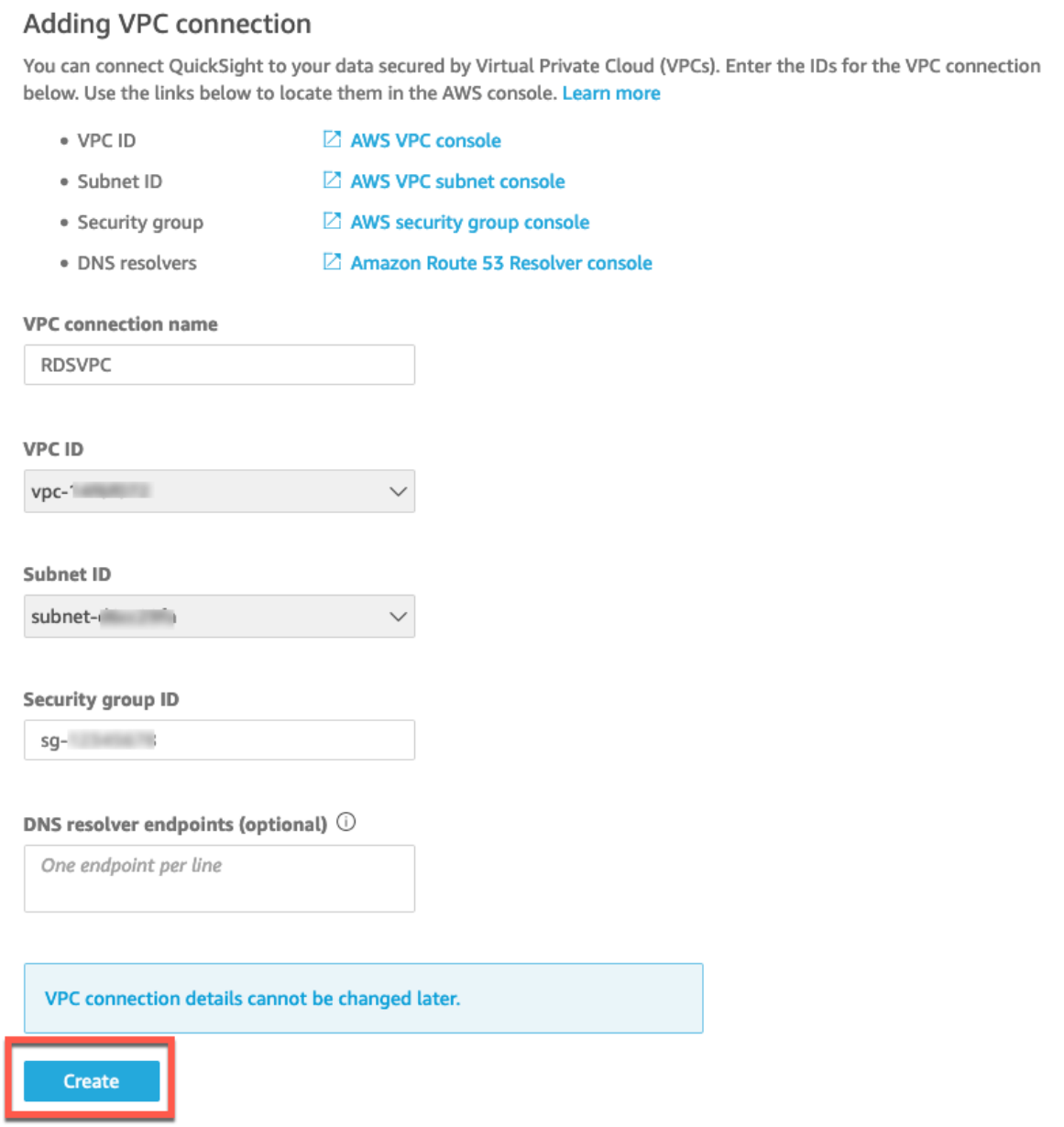
d. On the qsdatabase page, in the Connectivity & security section, under VPC, copy the id. Then, under Subnets, copy one of the ids.



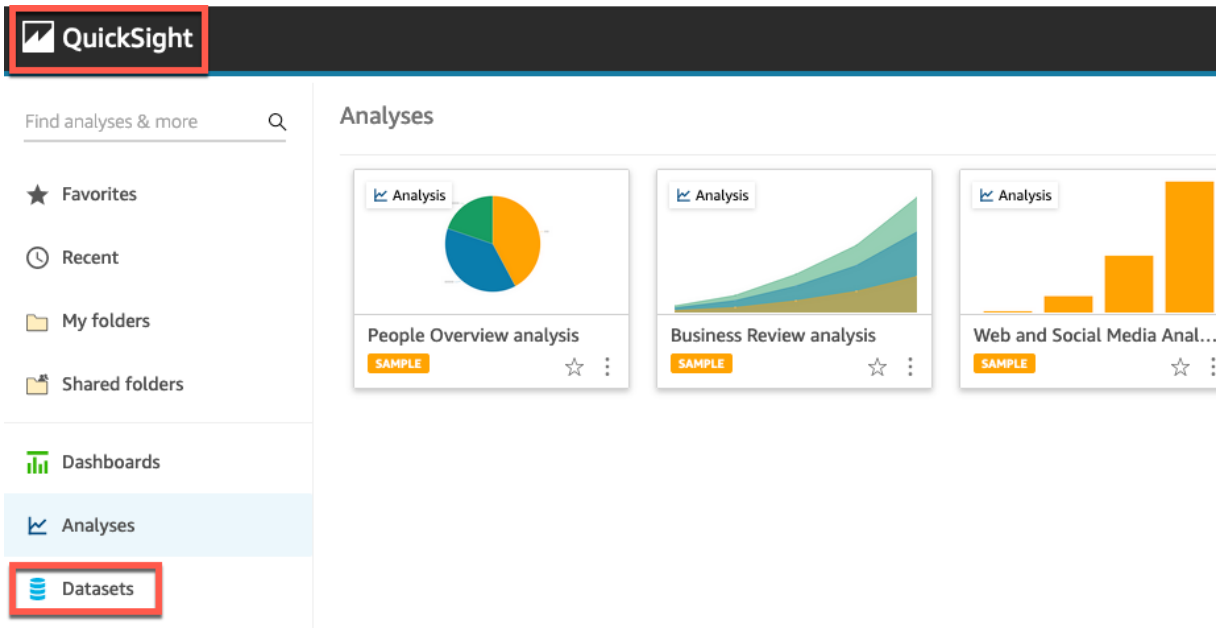
d. Navigate back to the Adding VPC connection page, and enter the following details.

- For VPC connection name, type RDSVPC
- For VPC ID, choose the id you copied in Step 8.e
- For Subnet ID, paste the id you copied in Step 8.e
- For Security group ID, paste the id you copied in Step 6.g

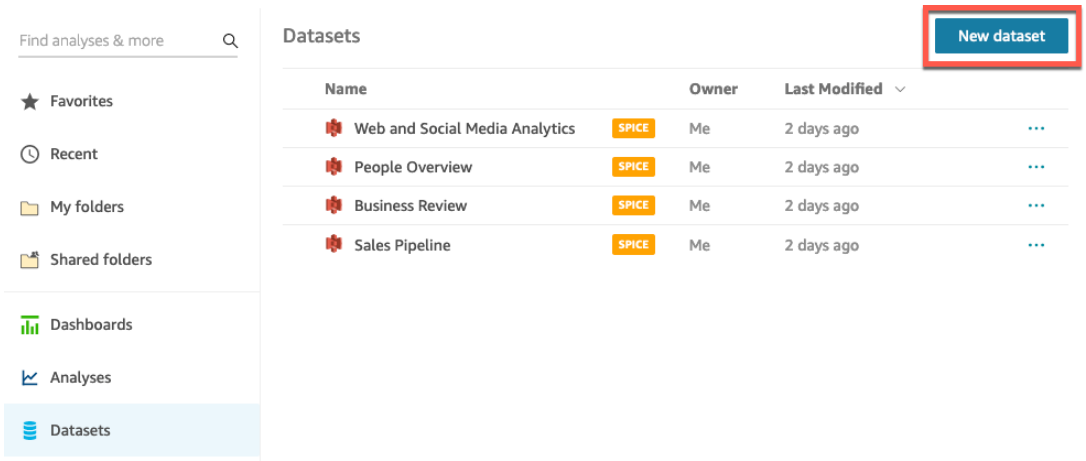
e. Then, choose Create.



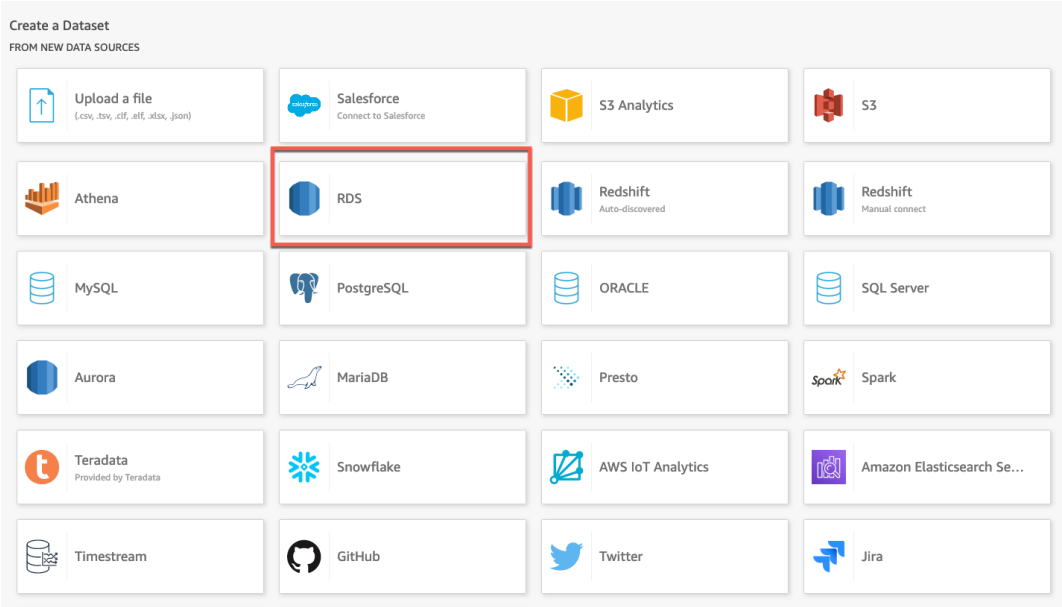
f. On the top left corner of your screen, choose the QuickSight icon. Then, in the left navigation, choose Datasets.



g. On the Datasets page, choose New dataset.



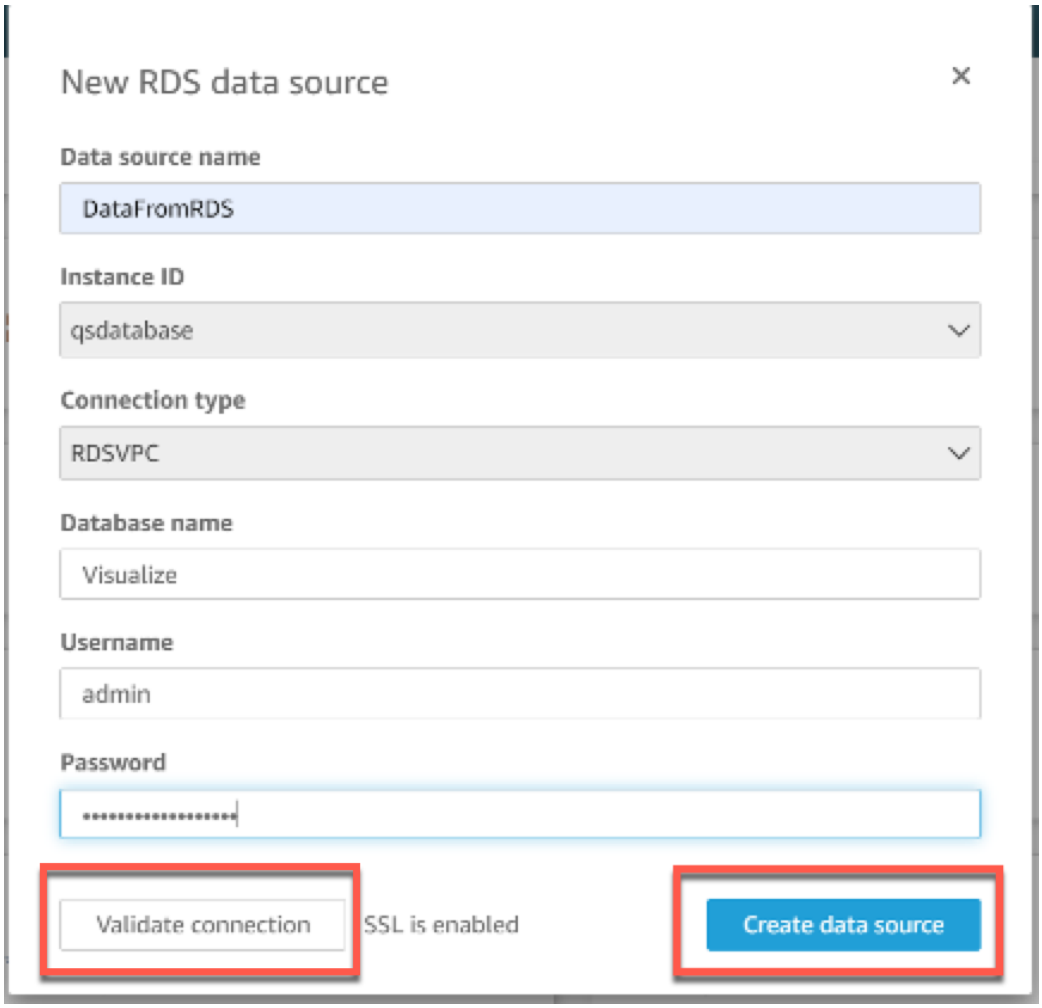
h. On the Create a Datasets page, choose RDS.



i. On the New RDS data source page, enter the following details.

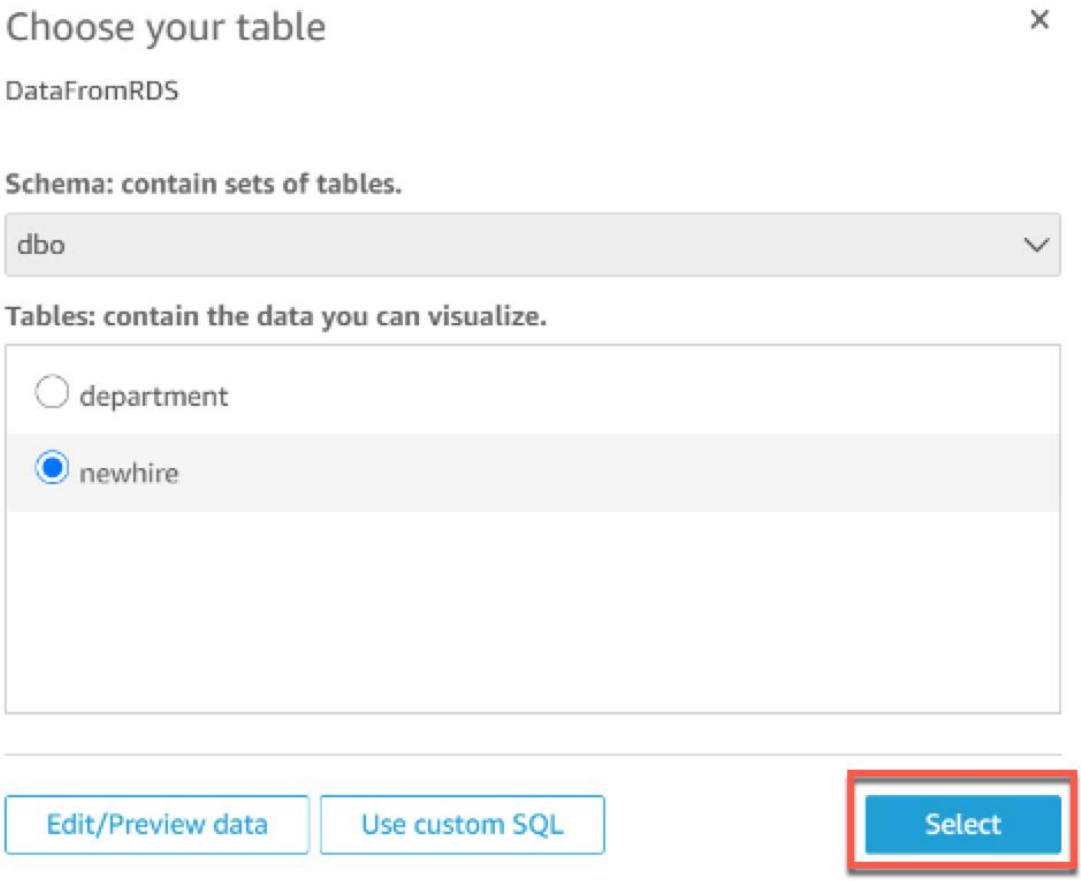
- For Data source name, type DataFromRDS
- For Instance ID, choose qsdatabase
- For Connection type, choose RDSVPC
- For Database name, type Visualize
- For Username, type the username you entered when creating the Visualize database
- For Password, type the password you entered when creating the Visualize database

j. Then, choose Validate connection. If the connection was successful, choose Create data source.

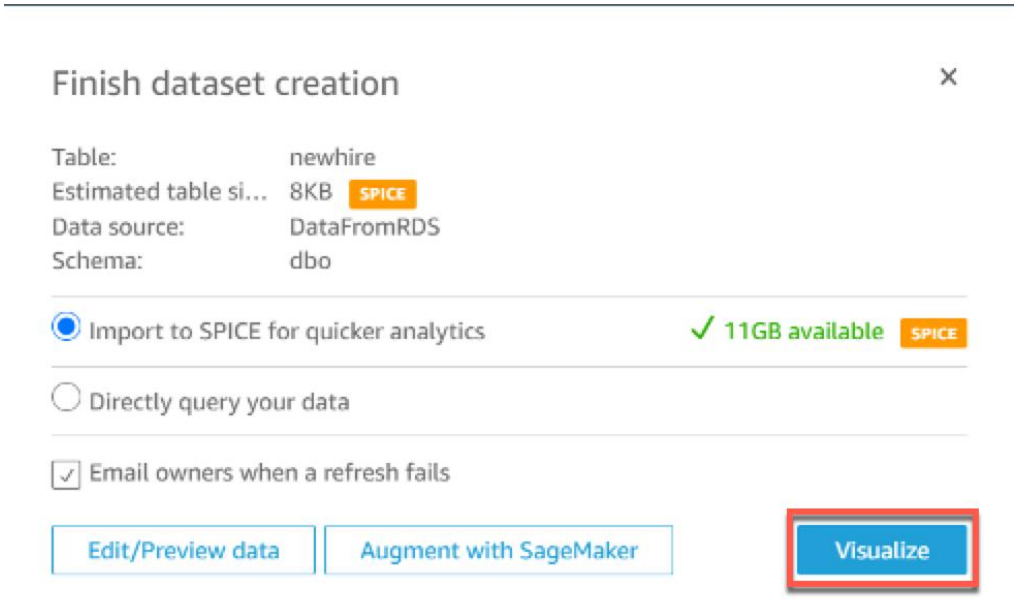


k. On the Choose your table page, in the Schema section, choose dbo.

l. In the Tables section, choose newhire. Then, choose Select.



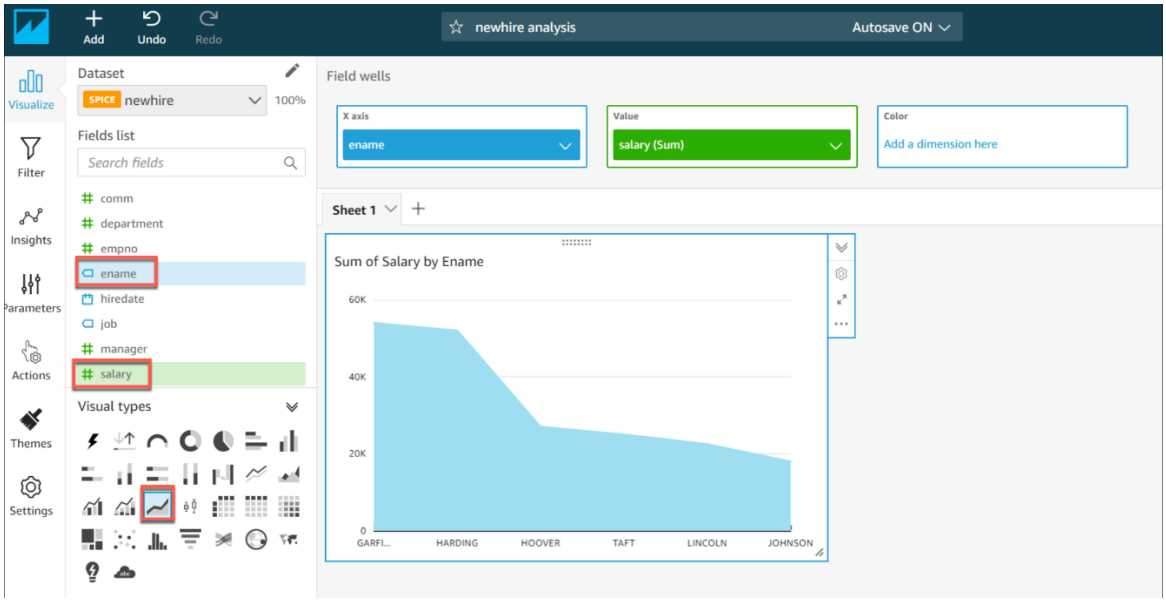
m. On the Finish dataset creation page, leave the default selections, and choose Visualize.



n. On the Visualize page, in the Visual types section, choose the Stacked Area Line Chart.

o. In the Fields list section, drag and drop ename and salary to the Field Wells section.

Note: For more information, see Working with Visuals in the Amazon QuickSight documentation.



Step 11. Clean up
In this step, you delete the resources you used in this lab.

Lab Assignment No.	**11**
Title	Setup, Create and connect your Word Press site to an object storage bucket using Lightsail service.
Roll No.	
Class	TE
Date of Completion	
Subject	Mini Project(Cyber Security)
Assessment Marks	
Assessor's Sign	

ASSIGNMENT No: 11

Title: Setup, Create and connect your Word Press site to an object storage bucket using Lightsail service.

Problem Statement: Setup, Create and connect your Word Press site to an object storage bucket using Lightsail service.

Prerequisite:

Basic of Cloud

Software Requirements:

AWS

Hardware Requirement:

2GB RAM, 500 GB HDD

Learning Objectives:

Learning AWS Environment

Outcomes:

After completion of this assignment students are able to how to create IAM user to use in the account setup the AWS CLI

Theory:

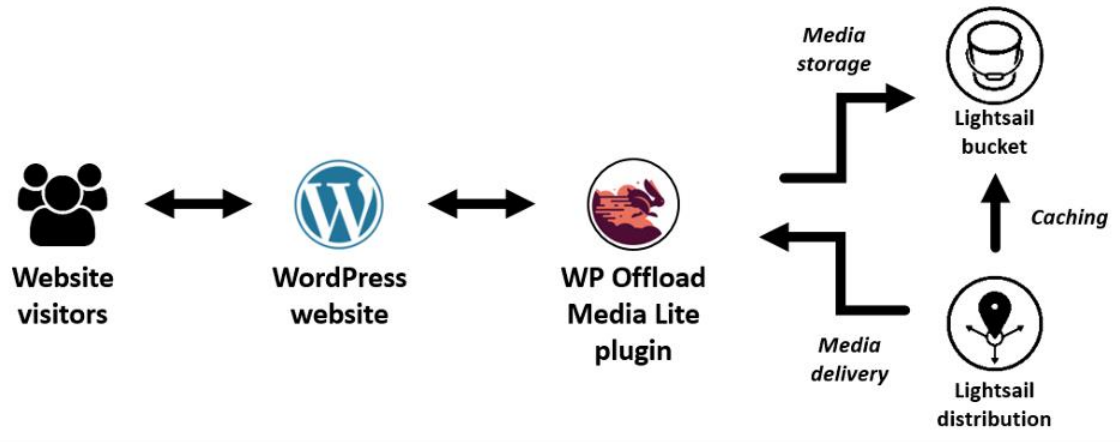
Amazon Lightsail is the easiest way to get started with AWS. It offers virtual servers, storage, databases, networking, and now containers, plus a cost-effective, monthly plan.

Lightsail now offers object storage describes the steps required to configure your Lightsail bucket as the origin of a Lightsail content delivery network (CDN) distribution. It also describes the steps required to configure your WordPress website to upload and store media (images, movies files, etc.) on your bucket, and deliver it from your distribution.

You do this by installing and configuring the WP Offload Media Lite plugin on your WordPress website. The following diagram illustrates this configuration.

Storing website media in a Lightsail bucket takes the load off your instance from having to store and serve those files. Caching and serving media from a Lightsail distribution speeds up the delivery of those files to your website visitors, and can improve overall website performance.

Get started with Amazon Lightsail for free.



Step 1: Prerequisites

Complete the following prerequisites if you haven't already:
1.1 — Create a Lightsail account.
Sign up for AWS

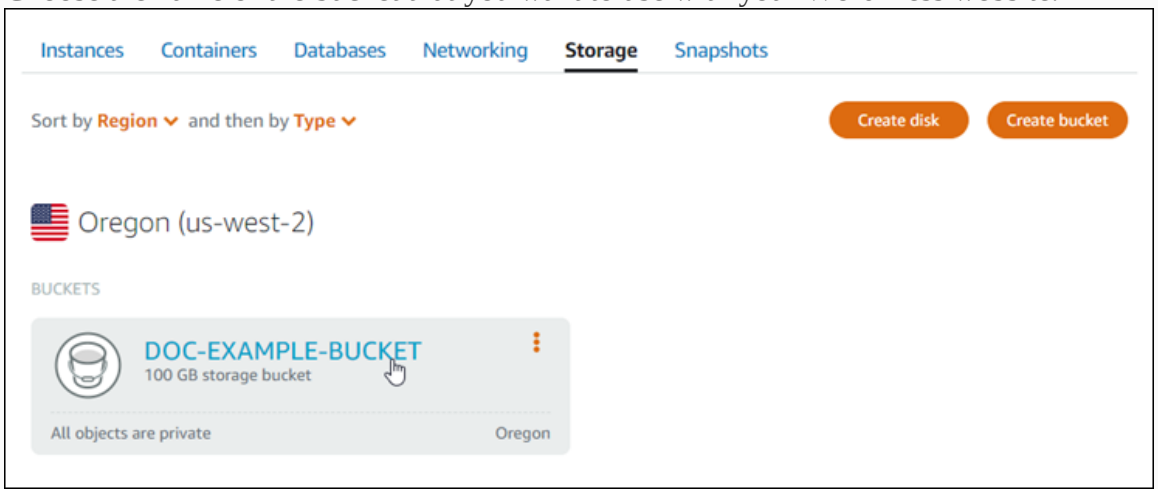
Already have an account? Log in to your account

1.2 — Create and configure a WordPress instance in Lightsail, and get the password to sign in to the administration dashboard.
1.3 — Create a bucket in the Lightsail object storage service.

Step 2: Modify your bucket permissions

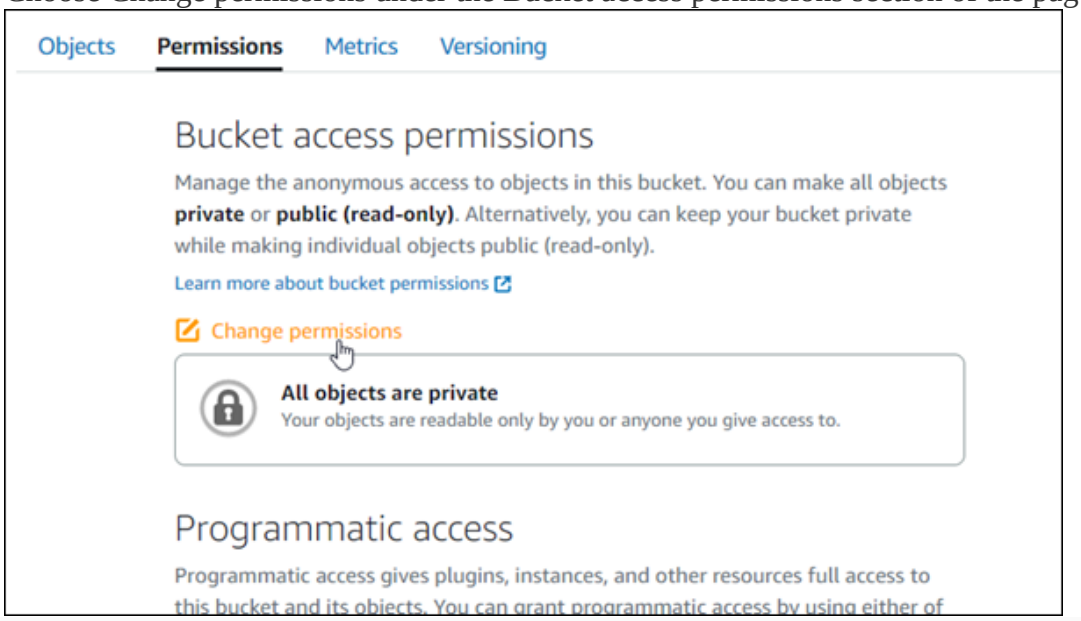
Complete the following procedure to give your WordPress instance and the WP Offload Media Lite plugin access to your bucket. The permissions of your bucket must be set to Individual objects can be made public (read only). You must also attach your WordPress instance to your bucket.
2.1 — Sign into the Lightsail console.
2.2 —On the Lightsail home page, choose the Storage tab.

Choose the name of the bucket that you want to use with your WordPress website.



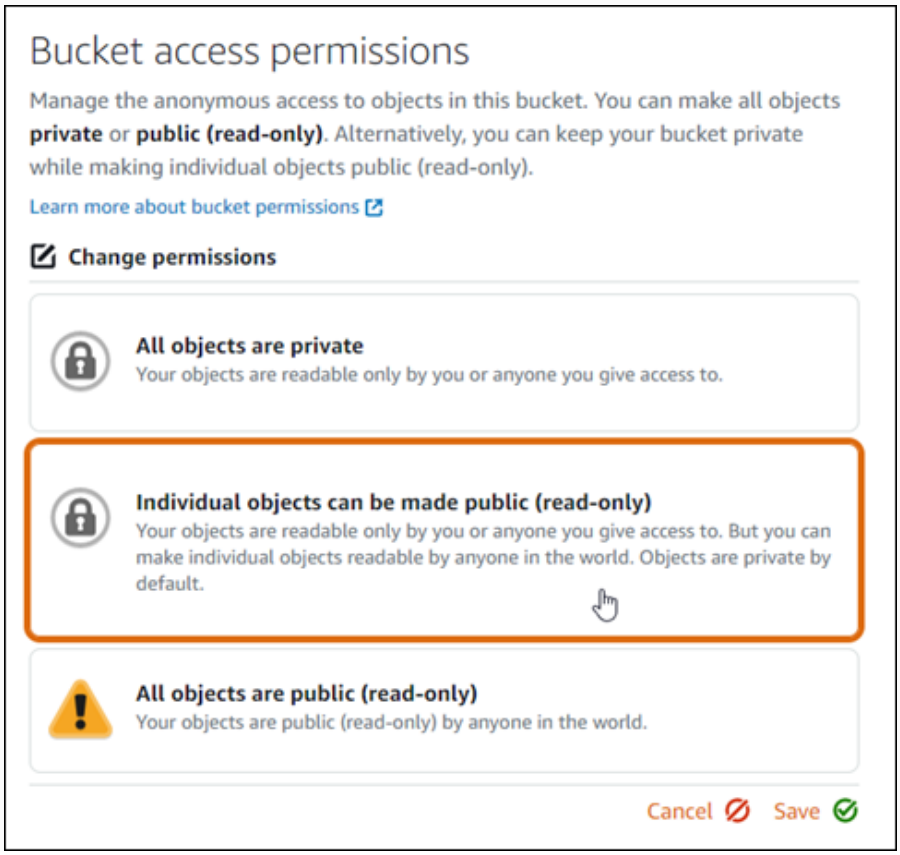
2.3 — Choose the Permissions tab on the Bucket management page.

Choose Change permissions under the Bucket access permissions section of the page.



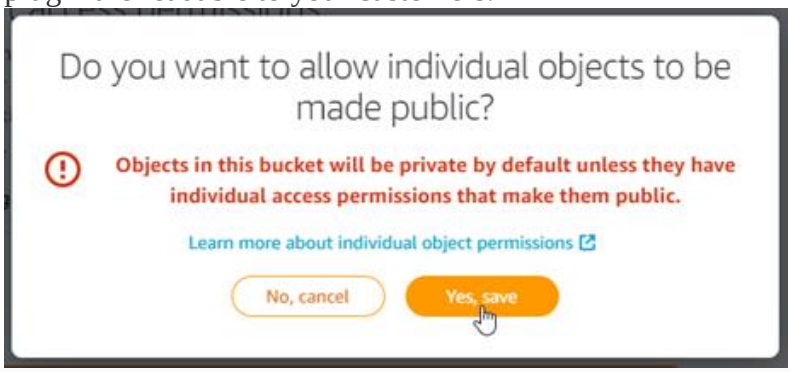
2.6 — Choose Individual objects can be made public (read-only).

Choose Save.

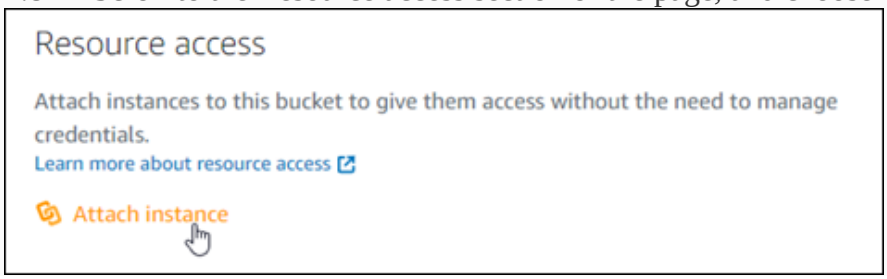


2.7 — Choose Yes, Save in the confirmation prompts that appear.

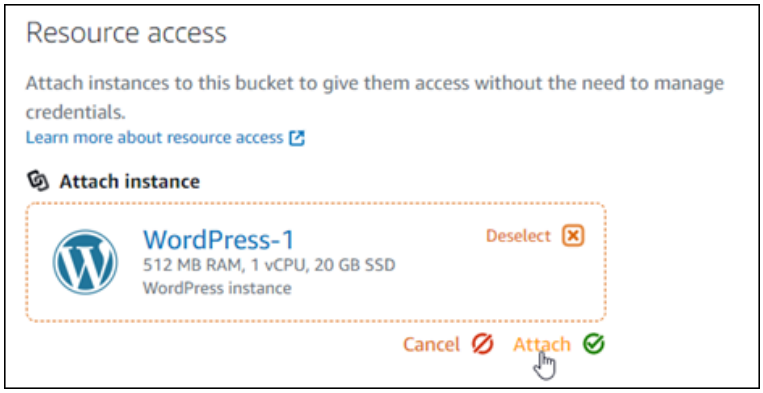
After a few moments, your bucket will be configured to allow for individual object access. This ensures that objects uploaded to your bucket from your WordPress website using the WP Offload Media Lite plugin are readable to your customers.



2.8 — Scroll to the Resource access section of the page, and choose Attach instance.



2.9 — Choose the name of your WordPress instance in the dropdown menu that appears. Choose Attach.



After a few moments, your WordPress instance is attached to your bucket. This gives your WordPress instance access to manage your bucket and its objects.

Step 3: Create a distribution with a bucket as the origin

Complete the following procedure to create a Lightsail distribution and choose your Lightsail bucket as the origin.

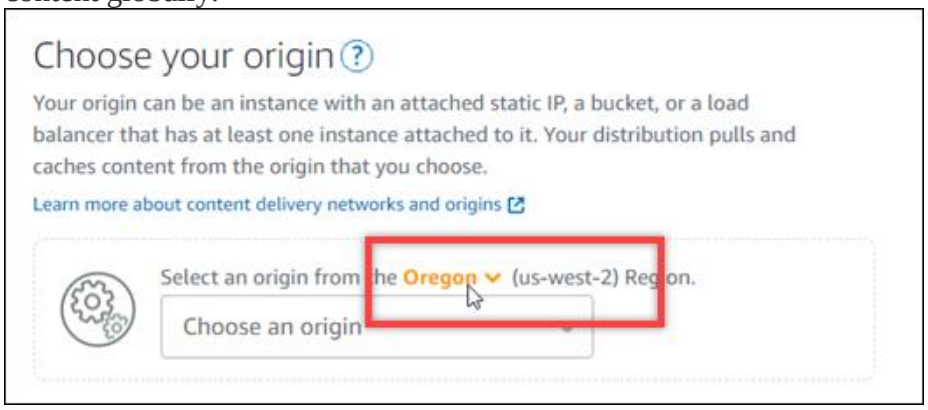
3.1 — Choose Home on the top navigation menu of the Lightsail console.

3.2 — On the Lightsail home page, choose the Networking tab.

Choose Create Distribution.

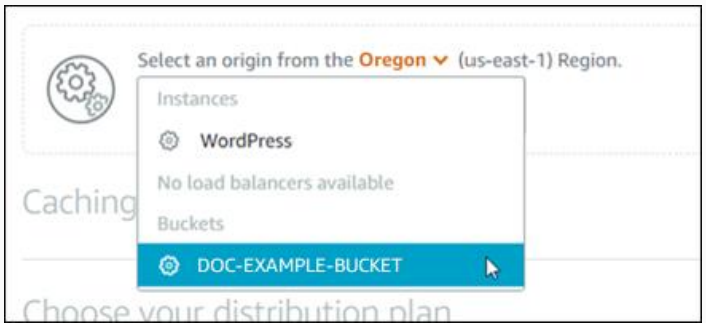
3.3 — In the Choose your origin section of the page, choose the AWS Region in which you created your bucket.

Distributions are global resources. They can reference a bucket in any AWS Region, and distribute its content globally.



3.4 — Choose your bucket as the origin.

Note: When you choose a bucket as the origin of a distribution, the options to specify the origin protocol policy, caching behavior, default behavior, and directory and file overrides become unavailable and cannot be edited. The origin protocol policy defaults to HTTP only for buckets, and the caching behavior defaults to Cache everything. However, you can change the advanced cache settings of the distribution after it's created.



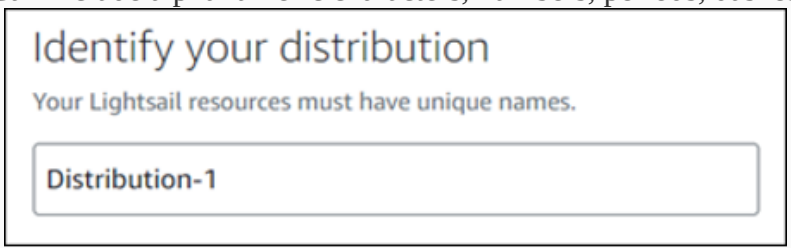
3.5 — Choose your distribution plan.

3.6 — Enter a name for your distribution.

Resource names:

- Must be unique within each AWS Region in your Lightsail account.
- Must contain 2 to 255 characters.

- Must start and end with an alphanumeric character or number.
- Can include alphanumeric characters, numbers, periods, dashes, and underscores.



3.9 — Choose Create distribution.

Your distribution is created after a few moments. When your new distribution reaches an Enabled state, it is ready to serve and cache objects that are in your bucket.

Step 4: Enable a custom subdomain for your distribution

When you create your distribution, it is configured with a default domain that is similar to 123abc.cloudfront.net. You can specify that default domain as the source of your media files when you configure the WP Offload Media Lite plugin.

But we highly recommend that you enable a custom domain for your distribution. The custom domain that you enable for your distribution should be a subdomain of the domain that you're using with your WordPress website. For example, if you're using mycustomdomain.com with your WordPress website, then you might choose to use the custom domain media.mycustomdomain.com with your distribution. Using the same domain and subdomain combination between your WordPress website and your distribution helps improve the search engine optimization score of your website.

Complete the following steps to configure a custom domain for your distribution:
4.1 — Create a Lightsail SSL/TLS certificate for your domain to use it with your distribution. Lightsail distributions require HTTPS, so you must request an SSL/TLS certificate for your domain before you can use it with your distribution

4.2 — Enable custom domains for your distribution to use your domain with your distribution. Enabling custom domains requires that you specify the Lightsail SSL/TLS certificate that you created for your domain. This adds your domain to your distribution and enables HTTPS

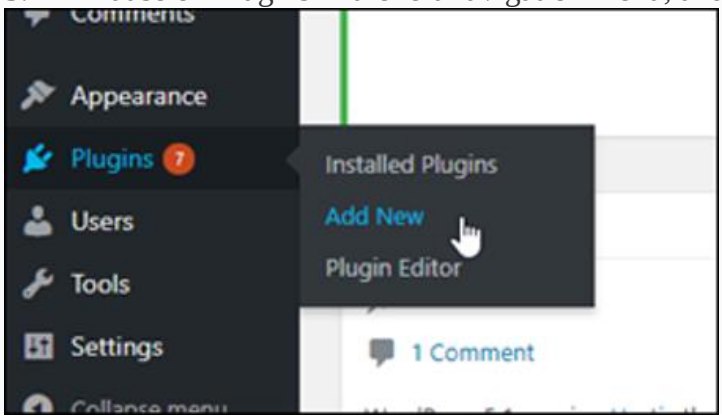
4.3 — Add an alias record to your domain's DNS to begin routing traffic for your domain to your distribution. After you add the alias record, users who visit your domain are routed through your distribution.

Step 5: Install the WP Offload Media Lite plugin on your WordPress website

Complete the following procedure to install the WP Offload Media Lite plugin on your WordPress website. This plugin automatically copies images, videos, documents, and any other media added through WordPress' media uploader to your Lightsail bucket. It can also be configured to serve media from your bucket through your Lightsail distribution.

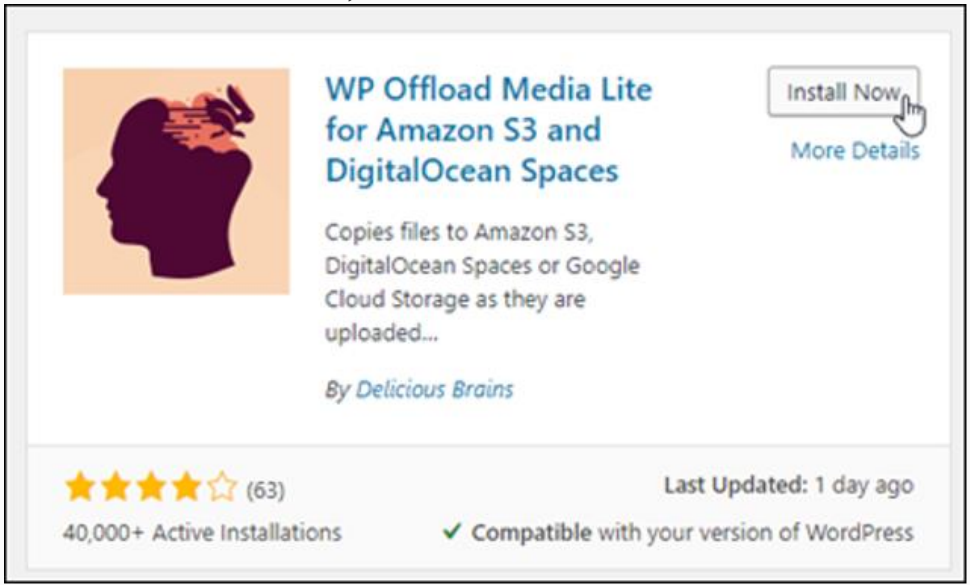
5.1 — Sign in to the dashboard of your WordPress website as an administrator.

5.2 — Pause on Plugins in the left navigation menu, and choose Add New.

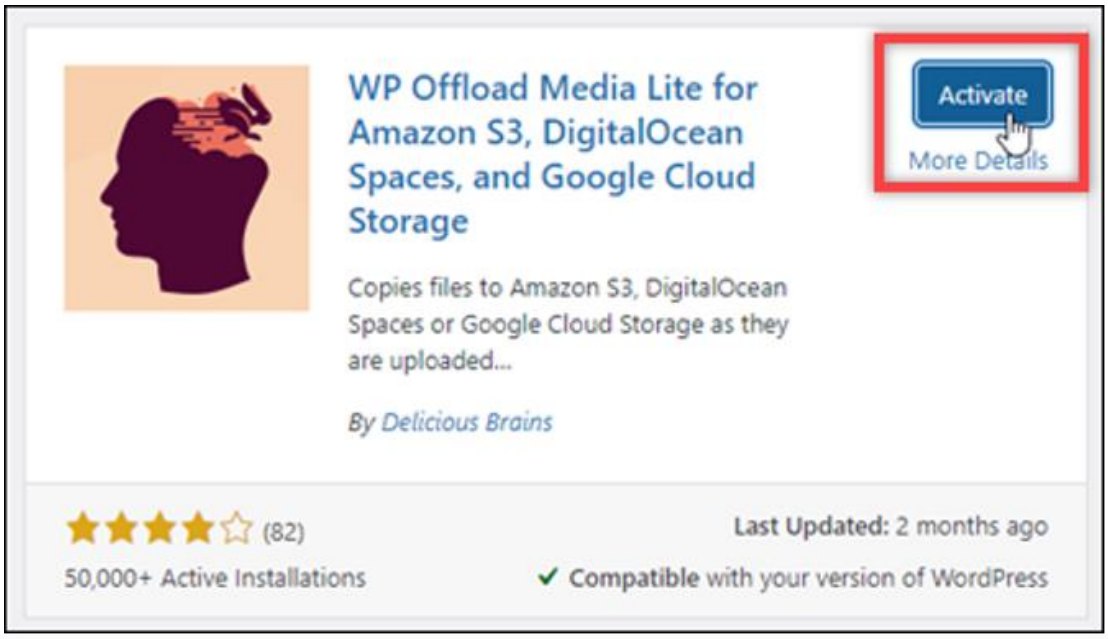


5.3 — Search for WP Offload Media Lite.

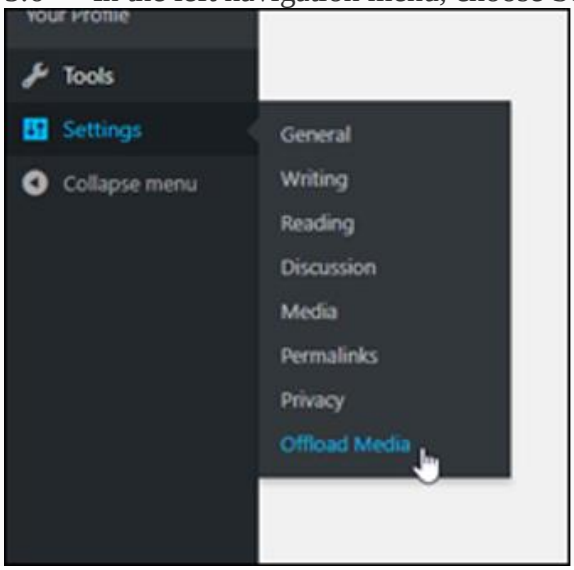
5.4 — In the search results, choose Install Now next to the WP Offload Media Lite plugin.



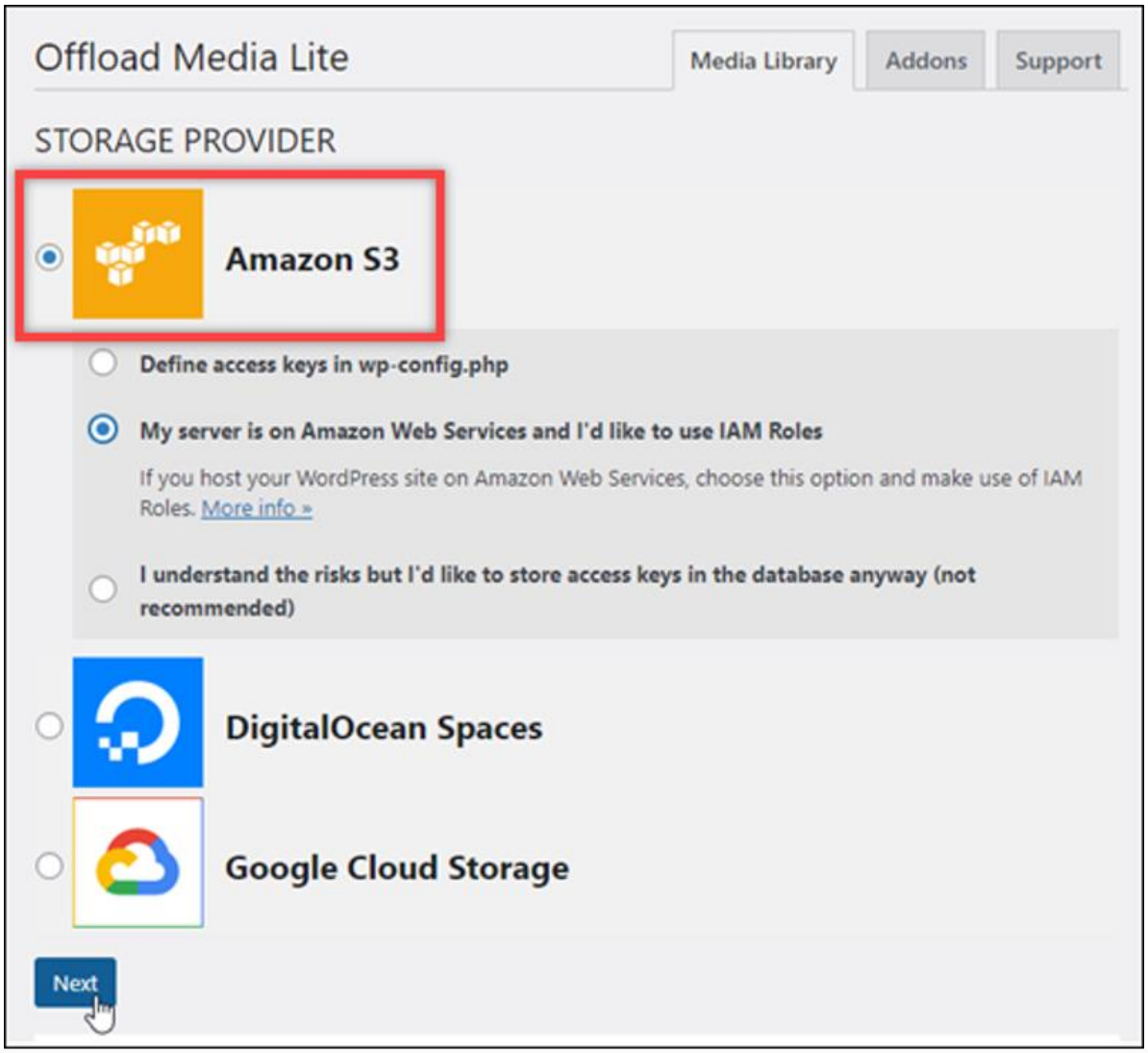
5.5 — Choose Activate after the plugin is done installing.



5.6 — In the left navigation menu, choose Settings, then choose Offload Media.

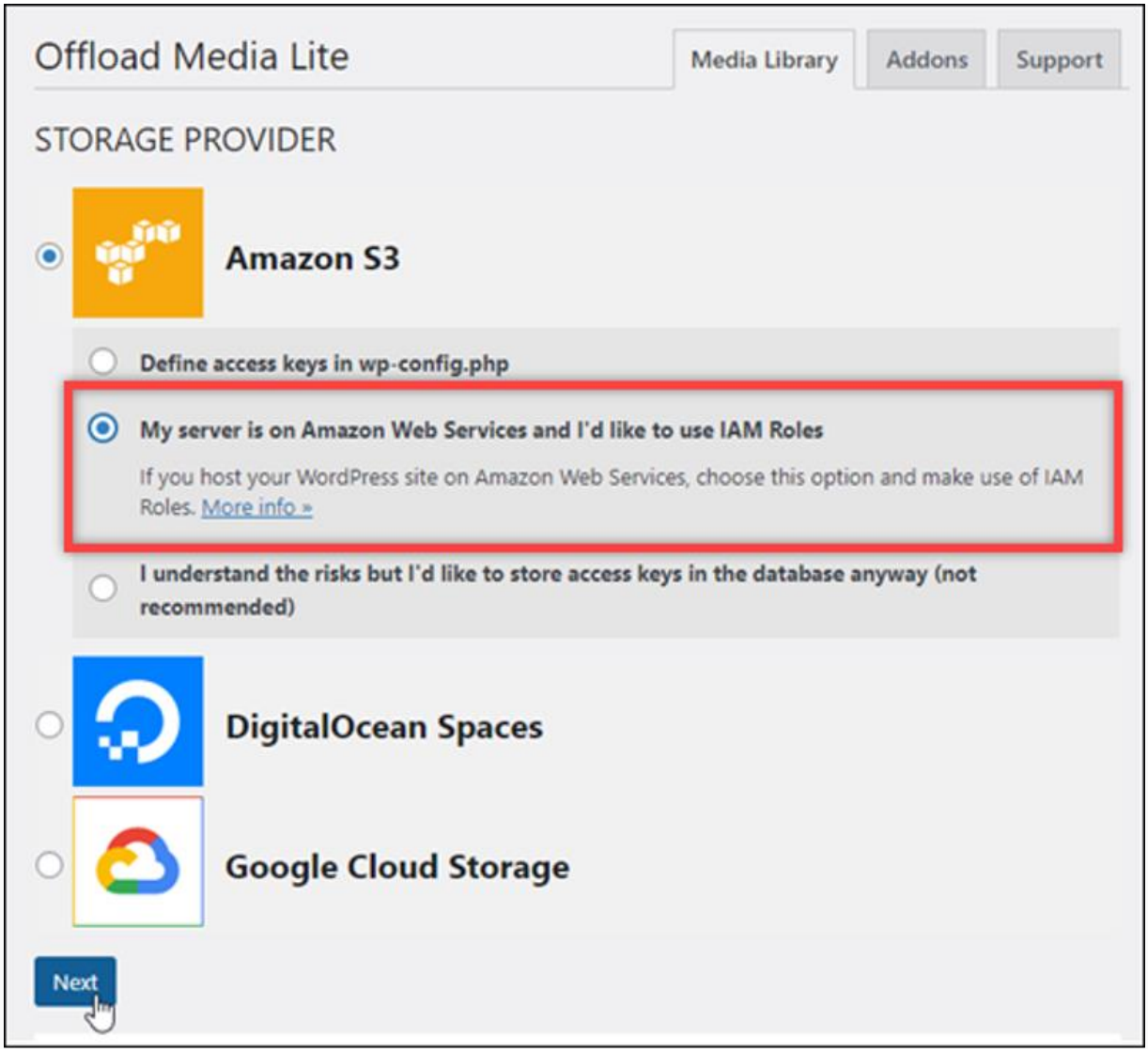


5.7 — In the Offload Media Lite page, choose Amazon S3 as the storage provider.

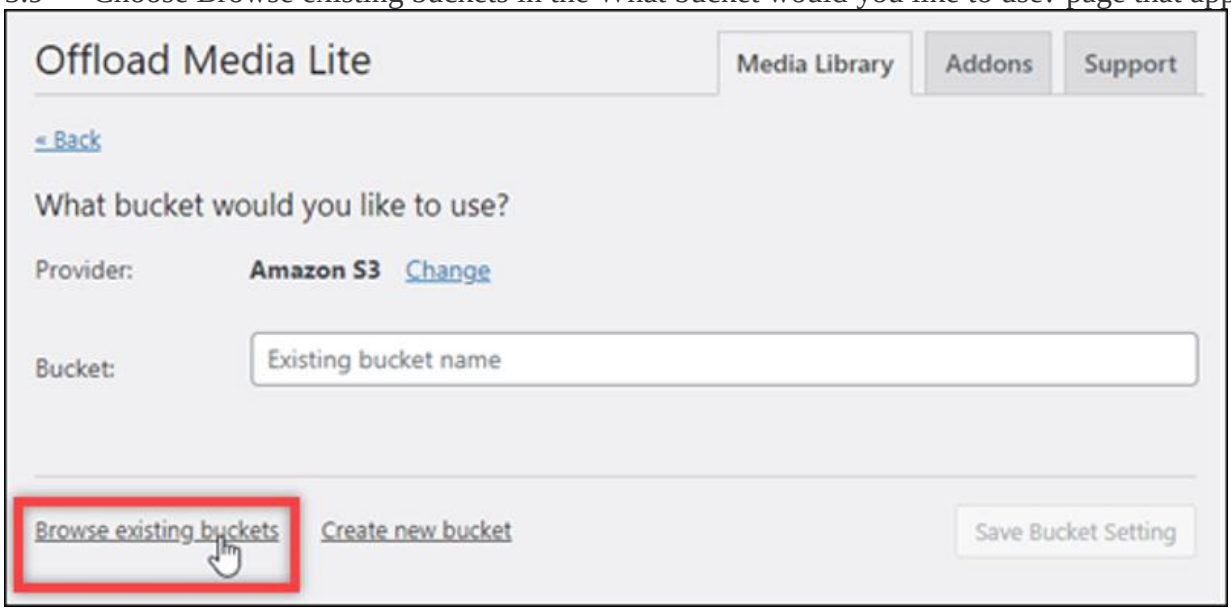


5.8 — Choose My server is on Amazon Web Services and I'd like to use IAM Roles.

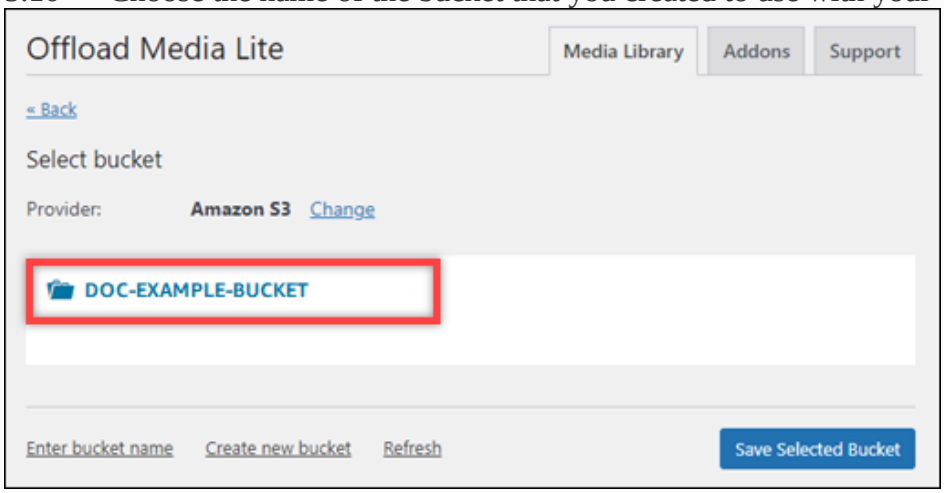
Then choose Next.



5.9 — Choose Browse existing buckets in the What bucket would you like to use? page that appears.

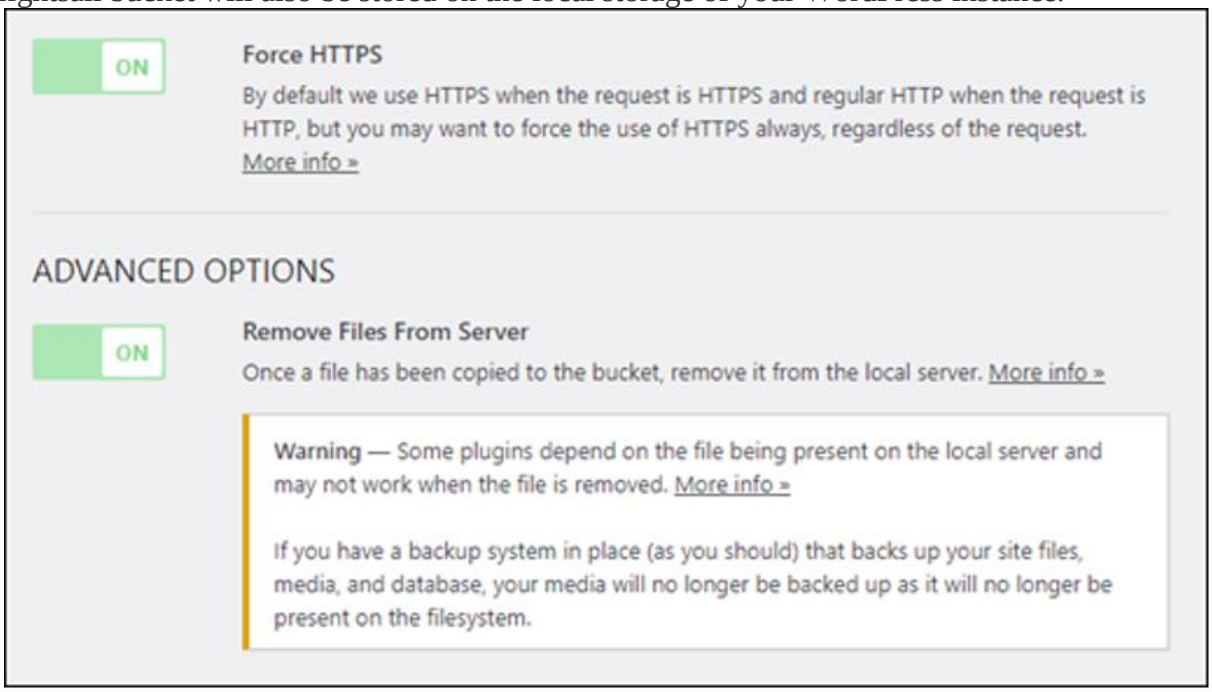


5.10 — Choose the name of the bucket that you created to use with your WordPress instance.

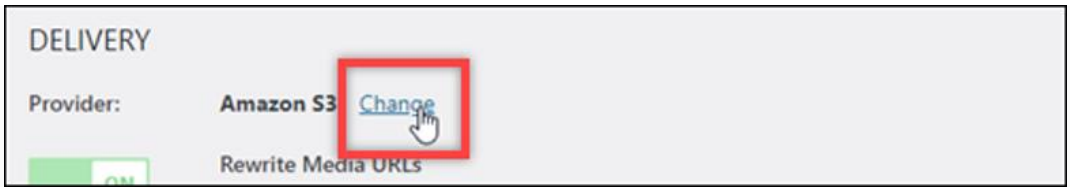


5.11 — In the Offload Media Lite Settings page that appears, enable Force HTTPS and Remove Files From Server.

- The Force HTTPS setting must be enabled because Lightsail buckets use HTTPS by default to serve media files. If you don't enable this feature, media files that are uploaded to your Lightsail bucket from your WordPress website will not be be served correctly to your customers when they visit your website.
- The Remove Files From Server setting ensures that media that is uploaded to your Lightsail bucket isn't also stored on your instance's disk. If you don't enable this feature, media files that are uploaded to your Lightsail bucket will also be stored on the local storage of your WordPress instance.

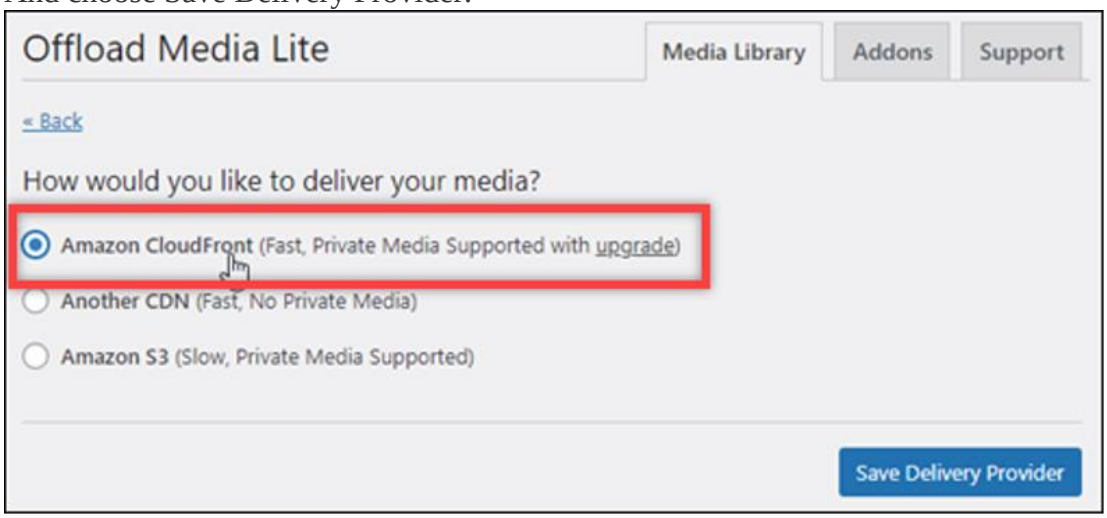


5.12 — Under the Delivery section of the page, choose Change next to the Amazon S3 label.

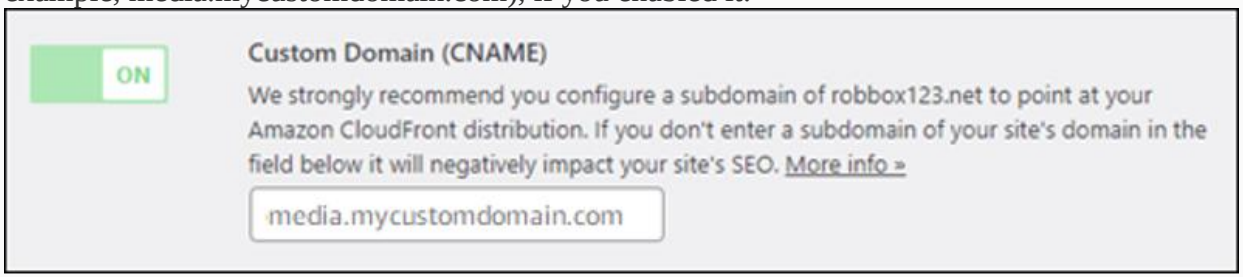


5.13 — In the How would you like to deliver your media? page that appears, choose Amazon Cloudfront.

And choose Save Delivery Provider.



5.14 — In the Offload Media Lite Settings page that appears, enable Custom Domain (CNAME) and then enter the domain of your Lightsail distribution into the text box. This could be the default domain of your distribution (for example, 123abc.cloudfront.net) or the custom domain for your distribution (for example, media.mycustomdomain.com), if you enabled it.



5.15 — Choose Save Changes.

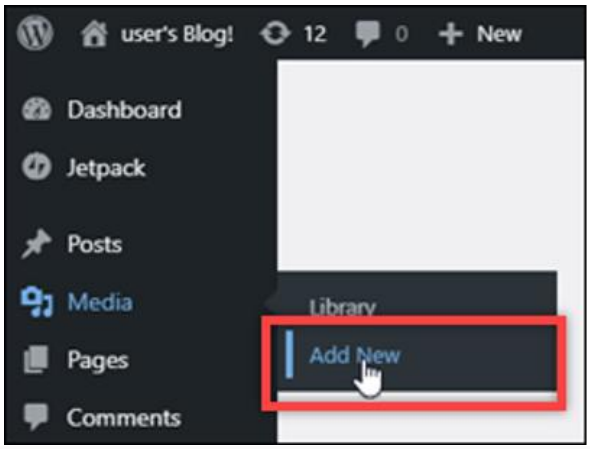
Note: To return to the Offload Media Lite Settings page later, hover over Settings in the left navigation menu, and choose Offload Media.

Your WordPress website is now configured to use the Media Lite Plugin. The next time you upload a media file through WordPress, that file is automatically uploaded to your Lightsail bucket, and is served by the distribution. Continue to the next section of this tutorial to test the configuration.

Step 6: Test the connection between your WordPress website and your Lightsail bucket and distribution

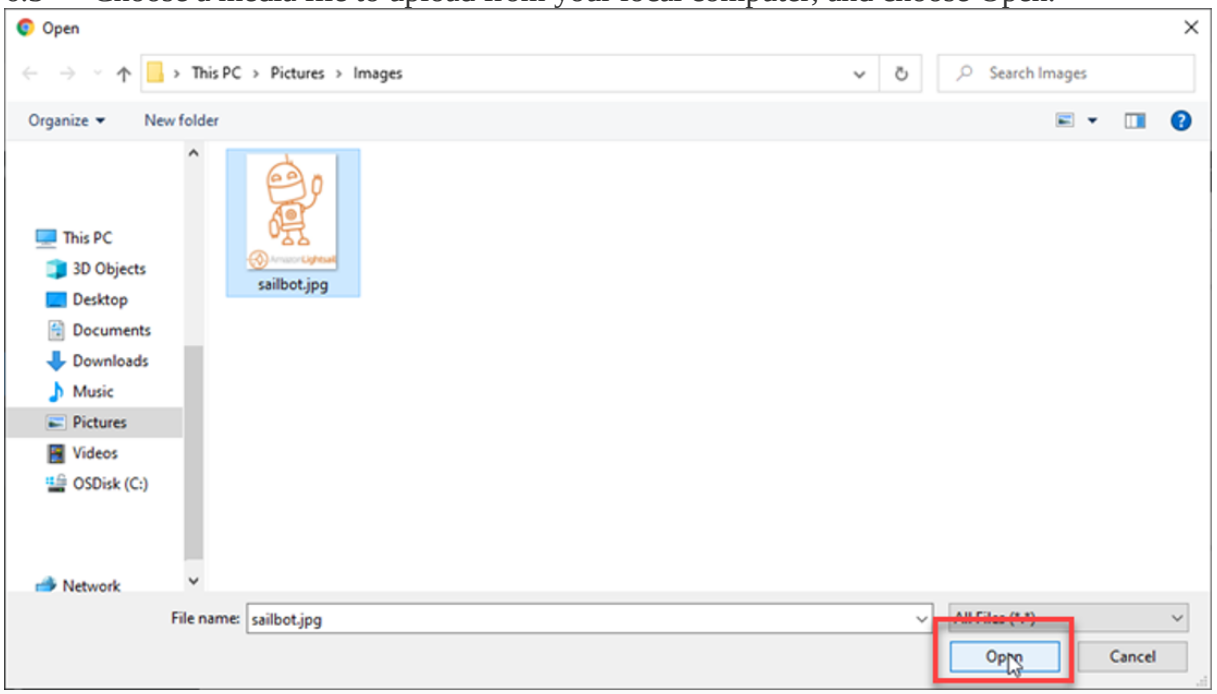
Complete the following procedure to upload a media file to your WordPress instance and confirm that it is uploaded to your Lightsail bucket and is served from your distribution.

6.1 —Pause on Media in the left navigation menu of the WordPress dashboard, and choose Add New.

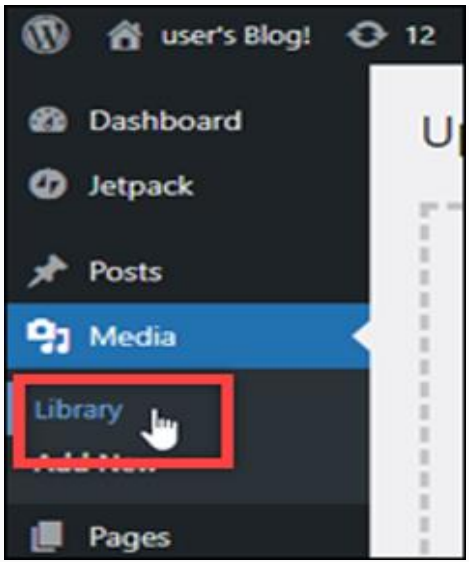


6.2 —Choose Select Files on the Upload New Media page that appears.

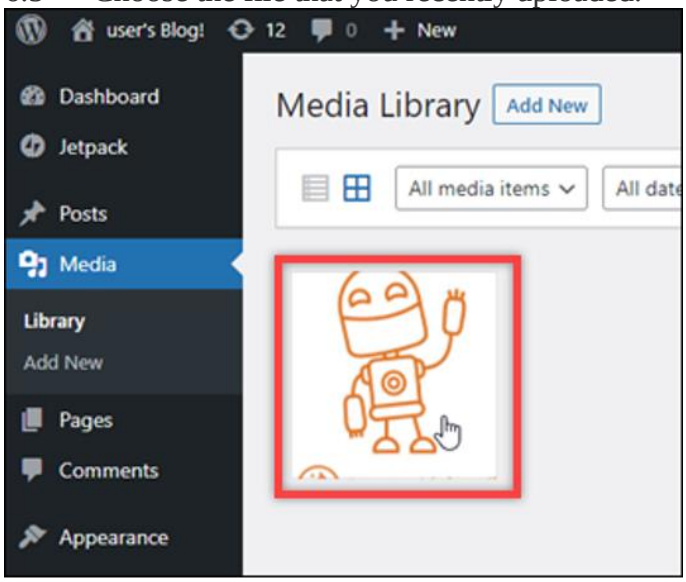
6.3 — Choose a media file to upload from your local computer, and choose Open.



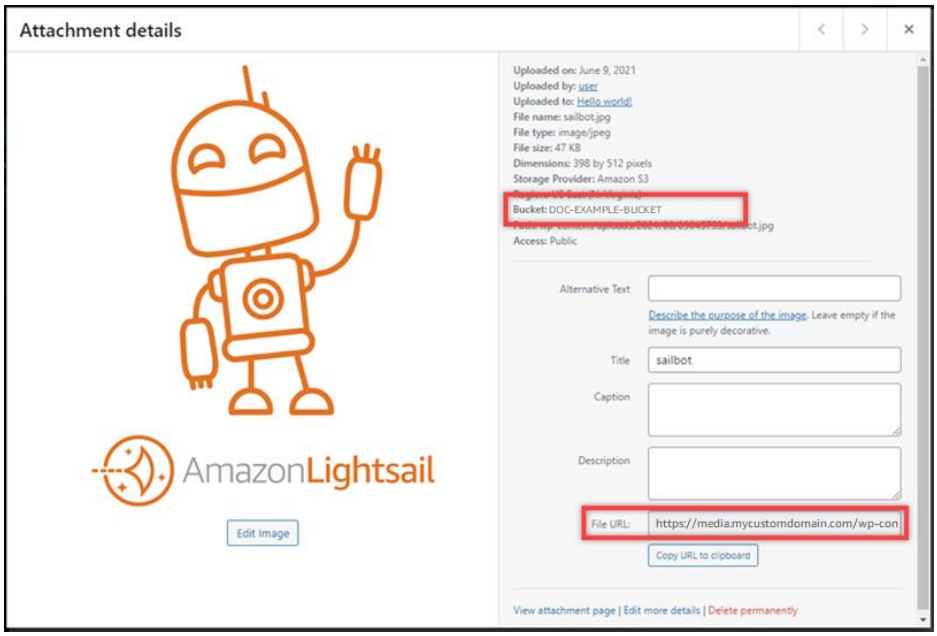
6.4 — When the file is done uploading, choose Library under Media in the left navigation menu.



6.5 — Choose the file that you recently uploaded.



6.6 — In the details panel of the file, you should see the name of your bucket in the Bucket field, and the URL of your distribution in the File URL field.



6.7 — If you go to the Objects tab of the Lightsail bucket management page, you should see a wp-content folder. This folder is created by the Offload Media Lite plugin, and will be used to store your uploaded media files.