**AWS – Amazon Web Service**

Contents

[ **Bastion Server** 2](#_Toc516259242)

1. [Our Bastion IP 2](#_Toc516259243)

[ **CIT - Server details** 2](#_Toc516259244)

1. [Bastion IP 2](#_Toc516259245)

[ **UAT - Server details** 3](#_Toc516259246)

1. [Bastion IP 3](#_Toc516259247)

[ **To run any Scripts:** 3](#_Toc516259248)

[ **To run any Jar file:** 4](#_Toc516259249)

[ **To know the permission of any files:** 4](#_Toc516259250)

[ **To give permission to any file** 4](#_Toc516259251)

[ **To Debug the file** 5](#_Toc516259252)

[ **To go to tomcat folder** 5](#_Toc516259253)

[ **To do Sudo su** 5](#_Toc516259254)

[ **To Exit** 5](#_Toc516259255)

[ **To Kill the Port:** 5](#_Toc516259256)

[ **To move one folder** 6](#_Toc516259257)

[ **To run the mock service in QA sever:** 6](#_Toc516259258)

[ **To list the Databases:** 6](#_Toc516259259)

[ **To make the schema as default schema:** 6](#_Toc516259260)

[ **To list the Tables:** 6](#_Toc516259261)

[ **To list the Stored Procedure:** 6](#_Toc516259262)

[ **To View stored procedure/function:** 6](#_Toc516259263)

[ **To Execute the Stored Procedure:** 7](#_Toc516259264)

[ **To insert new Stored procedure in the MYSQL:** 7](#_Toc516259265)

[ **To copy & paste the entire line:** 8](#_Toc516259266)

[ **To know the current date/time of the server:** 8](#_Toc516259267)

[ **SQL QUERIES** 8](#_Toc516259268)

[ **Secure Shell** (SSH) 9](#_Toc516259269)

[ **Secure copy Protocol or SCP** 10](#_Toc516259270)

[ **How to create id\_rsa file for any one?** 10](#_Toc516259271)

[ **Tomcat start/stop/restart** 11](#_Toc516259272)

[ What is WinSCP? 12](#_Toc516259273)

[ Open VPN IP: 12](#_Toc516259274)

[Connection Refuse: 12](#_Toc516259275)

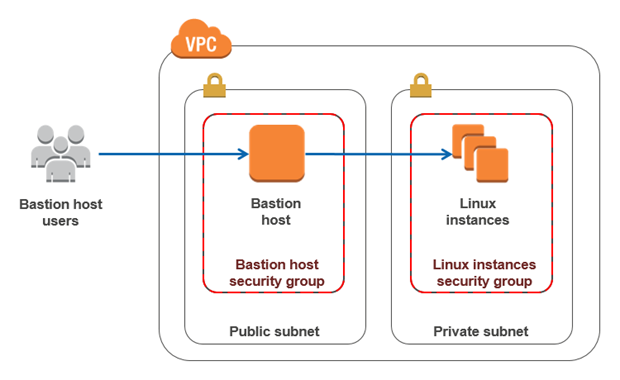
[ Quickly Create a Text File: 12](#_Toc516259276)

[ Service based Authentication credentials for AWS: 12](#_Toc516259277)

* **Bastion Server** (Landing server)

Bastion hosts are instances that sit within your public subnet and are typically accessed using SSH or RDP. Once remote connectivity has been established with the bastion host, it then acts as a **‘jump’ server,** allowing you to use SSH or RDP to log in to other instances (within private subnets) deeper within your VPC. When properly configured through the use of security groups and Network ACLs (NACLs), the bastion essentially acts as a bridge to your private instances via the internet.

Our Bastion IP= 13.228.127.243



Expansions:

SSH - *Secure Shell*

RDP - Remote Desktop *Protocol*

VPC - Virtual Private Cloud (Amazon VPC)

ACL - Access control list

NACL - Network ACL

# **CIT - Server details**

Bastion IP= 13.228.127.243

Login

Username: balamurugan.m

Passphrase: bgfdhg46dfs464/>jgbf2jkdfb

Application server URL:

ssh balamurugan.m@cit-ap-app-01.sg.bimamobile.internal

Db server URL:

ssh balamurugan.m@cit-ap-app-01.sg.bimamobile.internal

mysql -h cit-ap-rds-01.sg.bimamobile.internal -P 3306 -u mipadmin -pTG47g7NyeabzzyXnXDAw

ESB Server URL:

ssh balamurugan.m@cit-ap-esb-01.sg.bimamobile.internal

QA server URL:

ssh balamurugan.m@ap-qa-01.sg.bimamobile.internal

```````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````

* **UAT - Server details:**

Bastion IP: 13.228.127.243

Login

Username: balamurugan.m

Passphrase: xxxxxxxxxx

Application server

ssh balamurugan.m@uat-ap-app-01.sg.bimamobile.internal

Db server

ssh balamurugan.m@uat-ap-app-01.sg.bimamobile.internal

mysql -h uat-ap-rds-01.sg.bimamobile.internal -P 3306 -u mipadmin -pTG47g7NyeabzzyXnXDAw

ESB Server

ssh balamurugan.m@uat-ap-esb-01.sg.bimamobile.internal

````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````

# **To run any Scripts:**

* login to ESB server
* type command “**sudo su – bimaapp**” (bimaapp is the user which has more access permission)
* The Scripts will be present in the below mentioned path:

cd /opt/scripts

* Command to run the Scripts:

**./<shell script.sh>**

* **Example:**

**````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

# **To run any Jar file:**

:/opt/apps

Java –jar <jarfile.jar>

Example:

To run the smsqueue jar file:

Java –jar smsinqueue.jar

**````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

# **To know the permission of any files:**

* Command**= ls -l**

**````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

# **To give permission to any file**

* Command**:**

**chmod 750 <filename>.sh**

*(Note: Login to bimaapp user before giving permission)*

* 4 read (r)
* 2 write (w)
* 1 execute (x)

7 = 4+2+1 (read/write/execute)

6 = 4+2 (read/write)

5 = 4+1 (read/execute)

4 = 4 (read)

3 = 2+1 (write/execute)

2 = 2 (write)

1 = 1 (execute)

**````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

# **To Debug the file**

* Command

**sh -x <scriptname>.sh**

**````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

# **To go to tomcat folder**

* Command

**/var/lib/tomcat6/webapps**

**````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

# **To do Sudo su**

Steps:

* Login to specific server with your credentials
* Type "**sudo su - bimaapp**"
* (Now u will login to bimaapp login , not your login)
* Now execute what u want, with more access permissions

Example:

balamurugan.m@fiji-esb-01:~$ **sudo su - bimaapp**

**bimaapp@fiji-esb-01:~$**cd /opt/scripts

bimaapp@fiji-esb-01:/opt/scripts$ xxxxxxxxxxxxx

**````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

# **To Exit**

* Command**:**

**Ctrl + C**

**````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

# **To View the port running in ur credentials:**

* Command

**lsof -i:(portnumber)**

Example

lsof -i:8088

You will get the information of the port:

Example:

balamurugan.m@ap-qa-01:/opt/SoapUI/bin$ lsof -i:8088

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

java **13546** balamurugan.m 113u IPv6 2157916 0t0 TCP \*:omniorb (LISTEN)

Note: This command will show only the ports running in ur credentials not others

````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````

# **To Kill the Port:**

Now we need to kill the PID

* Command

**Kill (PID)**

Example:

Kill 13546

**````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

# **To View the port running in the instance: (all the users)**

* Command

**netstat –listen**

**````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

# **To move one folder**

* Command

**mv <file name><folder name>**

Example:

Filename = id\_rsa

Folder name = .ssh

Command: **mv id\_rsa .ssh**

**````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

# **To run the mock service in QA sever:**

Steps:

Go to the folder where **mockservicerunner** application was deployed

*Here the mockservicerunner is deployed in QA server in the path “* ***/opt/SoapUI/bin****”*

Command**:./mockservicerunner.sh (path where your mock service is present)**

Example

./mockservicerunner.sh /home/balamurugan.m/Soap\_project/FJ\_WIN\_BACK\_CR/FIJI-prepost0-chargingGateway-soapui-project.xml

**````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

**Data Base AWS Information**

# **To list the Databases:**

show databases;

# **To make the schema as defaultschema:**

Use<databases>

# **To list the Tables:**

Show Tables;

# **To list the Stored Procedure:**

SHOW PROCEDURE STATUS;

# **To View stored procedure/function:**

SHOW CREATE PROCEDURE <name>

# **To Execute the Stored Procedure:**

Step 1: Edit the stored procedure given by dev team.

*Add*

DELIMITER $$

DROP PROCEDURE IF EXISTS <your procedure name>$$

*Remove DEFINER=`mipadmin`@`localhost`from the content (proceedure content)*

***Example:***

*It should be “CREATE PROCEDURE `ADD\_ROLE\_MENU\_ACCESS\_DETAILS”*

END$$

(Note: already END statement will be there just add $$ at the end)

Step2: Transfer to cit\_ap\_app (Using WInscp)

Check in the term server whether the the file is there or not by logging in the term server and type “ls” command

Step 3: Run the below command in Landing server to move the file to CIt serevr

scp ASSIGN\_OFFER.sql balamurugan.m@cit-ap-app-01.sg.bimamobile.internal:/home/bimaapp/SQL\_Files/

Step 4 : Run the below command in the CIT server

mysql -h cit-ap-rds-01.sg.bimamobile.internal -P 3306 -u mipadmin -pTG47g7NyeabzzyXnXDAw Your Schema name< /home/bimaapp/Automatoin\_Test/Your stored procedure.sql

*Example:*

mysql -h cit-ap-rds-01.sg.bimamobile.internal -P 3306 -u mipadmin -pTG47g7NyeabzzyXnXDAw mipfj < /home/bimaapp/Automatoin\_Test/ASSIGN\_OFFER.sql

````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````

# **To insert new stored procedure in the MYSQL:**

Step 1: Paste the stored procedure in the app server in any place

Step 2: The place where the file is there, open the Mysql by giving that URL

Step 3: check whether the stored procedure is exist or not.. by using the command

***SHOW PROCEDURE STATUS WHERE Db = DATABASE() AND Type = 'PROCEDURE' ;***

Step 4: Create the stored procedure by using the command

***source <sql file name>;***

**Example:**

source topup.sql;

````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````

# **To copy & paste the entire line:**

**Cltrl + U** = to copy the particular line from beginning to end

**Cltrl + Y** = to paste what had copied.

````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````

# **To know the current date/time of the server:**

To know the Date and Time:

**SELECT NOW();**

To know the Date:

**SELECT CURDATE();**

````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````

# **SQL QUERIES**

select \* from customer\_details order by cust\_id desc limit 5;

select \* from customer\_details where cust\_id = 78820;

select \* from customer\_details where msisdn = 7077777;

select \* from offer\_subscription order by offer\_sn\_id desc limit 5;

select \* from offer\_subscription where cust\_id = 78820;

Update offer\_subscription set is\_confirmed = 1, confirmation\_channel\_id = 2, confirmed\_date = '2018-01-23 12:28:36' where offer\_sn\_id =156370;

Update offer\_subscription set is\_confirmed = 1, confirmation\_channel\_id = 2, confirmed\_date = '2018-01-23 12:28:36' where cust\_id = 78820;

Update offer\_subscription setdeducted\_offer\_amount = 10 where cust\_id = 78804;

Update offer\_subscription setoffer\_cover = 100, hospital\_cover = 100, offer\_charges =1000, is\_deduction\_completed = 1, is\_prev\_deduction\_successful = 1, next\_deduction\_amount = 2, amount\_deducted\_today = 10, cycle\_id = 2018012578804, is\_prior\_month\_purchase\_successful = 1, rolled\_out\_amount = 5, pooled\_date = '2018-01-23 12:28:36' where cust\_id = 78804;

select \* from insured\_relative\_details order by ins\_id desc limit 5;

select \* from insured\_relative\_details where cust\_id = 78820;

select \* from sms\_in\_queue order by sms\_queue\_id desc limit 5;

select \* from sms\_in\_queue where sms\_msisdn = 7077777;

select \* from bima\_cancellations order by bc\_id desc limit 5;

select \* from bima\_cancellations where cust\_id = 78820;

select \* from offer\_cancellations order by oc\_id desc limit 5;

select \* from offer\_cancellations where cust\_id = 78820;

`````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````

# [**Secure Shell**](https://en.wikipedia.org/wiki/Secure_Shell) (SSH)

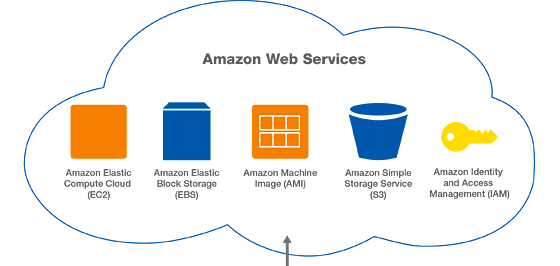
SSH, also known as Secure Socket Shell, is a network protocol that provides administrators with a secure way to access a remote computer.

SSH also refers to the suite of utilities that implement the protocol. Secure Shell provides strong authentication and secure encrypted data communications between two computers connecting over an insecure network such as the Internet.

SSH is widely used by network administrators for managing systems and applications remotely, allowing them to log in to another computer over a network, execute commands and move files from one computer to another.

Reference: <http://searchsecurity.techtarget.com/definition/Secure-Shell>

**`````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**



**```````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

**Amazon VPC:**

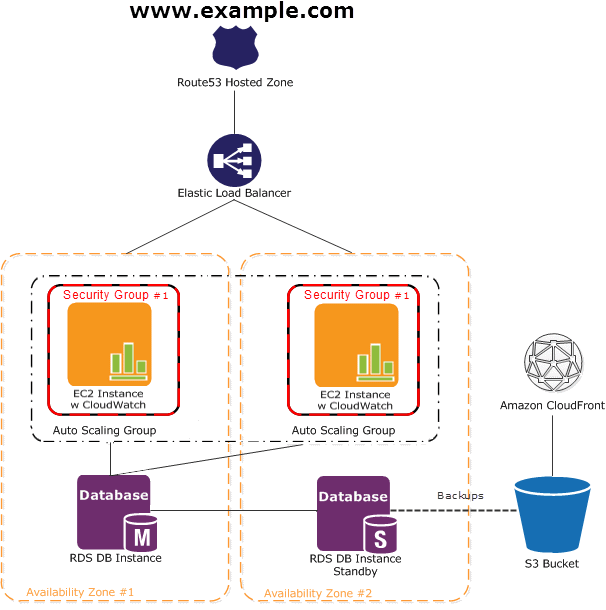
<https://www.youtube.com/watch?v=HgBADK-0oF4>

**````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

**AWS Route 53:**

<https://www.youtube.com/watch?v=JAYNGI3H6Ak>

**````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**



**```````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````**

# **Secure copy Protocol or SCP**

is a means of securely transferring [computer files](https://en.wikipedia.org/wiki/Computer_file) between a local host and a remote [host](https://en.wikipedia.org/wiki/Server_(computing)) or between two remote hosts. It is based on the [Secure Shell](https://en.wikipedia.org/wiki/Secure_Shell) (SSH) protocol.

"SCP" commonly refers to both the Secure Copy Protocol and the program itself

`````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````

# **How to create id\_rsa file for any one?**

If this file is not kept in the .ssh folder in landing server (term) of each person, then he/she can’t able to move from term server to app/DB/ESB server.

Steps:

Step 1: click on "PUTTYGEN.EXE" file.

Step 2: Select "Load" button

Step 3: Select the already created and save Private Key of the user whom we want to create the id\_rsa file.

Step 4: Enter the Passphrase of the user, in the popup.

Step 5: Select "conversions" menu, which is present in the top.

Step 6: Select "Export OpenSSH key".( second option in the drop down)

Step 7: Save the file with the name "id\_rsa" (the file name should be only **id\_rsa** )

Thats is you have successfully created the id\_rsa file...

Now we have to put this id\_rsa file in to the ".ssh" folder in our landing server.

we can do this with the help of "Winscp" software.

Once you logged in with the Winscp , you will be landing into the root folder.

Move the "id\_rsa" file from your desktop/anyfolder to the root folder(simply drag from left to right).

Now login to landing server(term) and do "ls - l" command.. you could see your id\_rsa file over there.

Now we need to move this file to the ".ssh" folder.

Use the command "mv id\_rsa .ssh" this will move the file to the ".ssh" folder.

Next, we have to give only Read permission to this file.

Go to the .ssh folder and give permission

So, for that use the command "chmod 400 id\_rsa".

So now the "id\_rsa" file is successfully moved to the .ssh folder, also the read permission is also given.

Check the file by giving "cd .ssh" command.. you could see the file now in .ssh folder..

````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````

# Tomcat start/stop/restart

sudo /etc/init.d/tomcat7 stop

sudo /etc/init.d/tomcat7 start

sudo /etc/init.d/tomcat7 restart

Note: execute the above commands as **bimaapp user**

````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````

# What is WinSCP?

WinSCP is a free and open-source SFTP, FTP, WebDAV, S3 and SCP client for Microsoft Windows. Its main function is secure file transfer between a local and a remote computer.

<https://winscp.net/eng/docs/start>

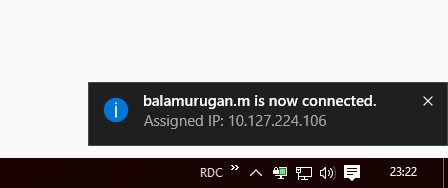
```````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````

LS : command:

<https://www.tecmint.com/15-basic-ls-command-examples-in-linux/>

`````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````

# Open VPN IP:



``````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````

# Connection Refuse:

If received connection refused means there is nothing running on the port that you are trying to connect

# Quickly Create a Text File:

cat > sample.txt

touch sample.txt

> sample.txt

# Service based Authentication credentials for AWS:

bimatestuser: jKtNTwqczw7jHnvvMzrM8UnkBz4RnA2AvNb2

**Credentials:**

Username: bimatestuser

Password: jKtNTwqczw7jHnvvMzrM8UnkBz4RnA2AvNb2

```````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````````