# Aws ASSESMENT

Contents

[Aws 1](#_Toc141994916)

[1. Create an AWS account 3](#_Toc141994917)

[2. Create a billing alarm [1$] 3](#_Toc141994918)

[3. Identity and Access Management [IAM] 4](#_Toc141994919)

[3.1 Create 3 user groups: HCS-Admins, HCS-Developers, HCS-DevOps 4](#_Toc141994920)

[3.2 Create 6 IAM users: 4](#_Toc141994921)

[3.3 Assign users to groups: 5](#_Toc141994922)

[3.4 Add a tag to all users: HCS-Foundation-Program 5](#_Toc141994923)

[3.5 Add MFA for users: <Your\_name> and Horatiu 5](#_Toc141994924)

[4. Amazon S3 6](#_Toc141994925)

[4.1 Create a S3 bucket 6](#_Toc141994926)

[4.2. Download a picture 7](#_Toc141994927)

[4.3. Upload apple.png file into your bucket. 7](#_Toc141994928)

[4.4. Try to open the object’s URL. 7](#_Toc141994929)

[4.5. Enable Versioning for <yourfullname>-hcs-foundation-program 9](#_Toc141994930)

[4.6. Download another picture with the APPLE logo 9](#_Toc141994931)

[4.7. Upload the new apple.png file into your bucket. 10](#_Toc141994932)

[4.8. List all the apple.png versions 10](#_Toc141994933)

[4.9. Delete apple.png object (the new object) 10](#_Toc141994934)

[4.10. Expend Versions 11](#_Toc141994935)

[4.11. Restore the old apple.png image 12](#_Toc141994936)

[4.12. Permanently delete all objects 13](#_Toc141994937)

[4.13. Enable replication 13](#_Toc141994938)

[4.14. Download a picture with the IBM logo 14](#_Toc141994939)

[4.15. Upload ibm.png file 14](#_Toc141994940)

[4.16. Create a life cycle policy 14](#_Toc141994941)

[6. Amazon EC2 16](#_Toc141994942)

[6.1 Create three EC2s: 16](#_Toc141994943)

[6.2 Are servers reachable? Why? 18](#_Toc141994944)

[From your WorkStation ping Bastion-Server - SUCCESS 18](#_Toc141994945)

[From your WorkStation ping Web-Server - SUCCESS 20](#_Toc141994946)

[From your WorkStation ping DB-Server -FAIL? 21](#_Toc141994947)

[6.3 Are servers accessible? Why? 22](#_Toc141994948)

[Connect to Bastion-Server -SUCCESS 22](#_Toc141994949)

[Connect to Web-Server - SUCCESS 27](#_Toc141994950)

[Connect to DB-Server from Web-Server – SUCCESS 30](#_Toc141994951)

[6.4 Reconfigure the SGs : 34](#_Toc141994952)

[For bastion-server 34](#_Toc141994953)

[For Web-server 35](#_Toc141994954)

[For DB-Server: 36](#_Toc141994955)

[6.5 Retry all the PINGs and Connections: 37](#_Toc141994956)

[From Bastion-Server ping Web-Server - SUCCESS 37](#_Toc141994957)

[From Bastion-Server ping DB-Server – FAIL? 37](#_Toc141994958)

[From Web-Server ping Bastion-Server -SUCCESS 38](#_Toc141994959)

[From Web-Server ping DB-Server – FAIL? 39](#_Toc141994960)

[From DB-Server ping Web-Server FAIL 39](#_Toc141994961)

[From DB-Server ping Bastion-Server FAIL 39](#_Toc141994962)

[Ping www. google.com from Bastion-Server – SUCCESS 39](#_Toc141994963)

[Ping www.google.com from Web-Server - SUCCESS 40](#_Toc141994964)

[Ping www.google.com from DB-Server - FAIL 40](#_Toc141994965)

[7. Cloud Watch 40](#_Toc141994966)

[7.1. Create a CloudWatch Alarm for Bastion-Server 40](#_Toc141994967)

[7.2. Generate some traffic in order to trigger the alarm. 41](#_Toc141994968)

# Create an AWS account

A screenshot of a computer

Description automatically generated

# Create a billing alarm [1$]

A screenshot of a computer

Description automatically generated

# Identity and Access Management [IAM]

## 3.1 Create 3 user groups: HCS-Admins, HCS-Developers, HCS-DevOps

* I added no policies because it was not specified

A screenshot of a computer

Description automatically generated

3.2 Create 6 IAM users: David, <Your\_name>, Horatiu, Laurentiu, Olivia, Adrian.Note: The users need to have AWS Management Console access and a new password needs to berequested at the next sign-in.

Example for David + tag HCS-Foundation-Program

A screenshot of a computer

Description automatically generated

3.3 Assign users to groups:HCS-DevOps group: Laurentiu, OliviaHCS-Developers group: David, <Your\_name>, HoratiuHCS-Admins group: Horatiu, Laurentiu

A screenshot of a computer

Description automatically generated

## 3.4 Add a tag to all users: HCS-Foundation-Program

* See example at 3.2 for David

## 3.5 Add MFA for users: <Your\_name> and Horatiu

* For Dana I used Autenticator app ( from Microsoft)
* For Horatiu I used IBM Verify

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

# Amazon S3

* 1. Create a S3 bucket, named <yourfullname>-hcs-foundation-program in us-east-2.Eg: horatiustaicovici-hcs-foundation-program

Note: Bucket – Private, Versioning – Disable, Tag: HCS-Foundation-Program

A screenshot of a computer

Description automatically generated

4.2. Download a picture with the APPLE logo (black and white) and name it apple.png

## 4.3. Upload apple.png file into your bucket.

A screenshot of a computer

Description automatically generated

## 4.4. Try to open the object’s URL.

- Accessing this <https://danabalasic-hcs-foundation-program.s3.us-east-2.amazonaws.com/apple.png>

Does not work, even if I am removing the HTTPS

A screenshot of a computer

Description automatically generated

But opening directly works

**A screenshot of a computer

Description automatically generated**

A black and white apple logo

Description automatically generated

Access for the bucket is blocked, must edit the policies to give access if I want.

## 4.5. Enable Versioning for <yourfullname>-hcs-foundation-program

A screenshot of a computer

Description automatically generated

4.6. Download another picture with the APPLE logo (color) and name it apple.png.

## 4.7. Upload the new apple.png file into your bucket.

A colorful logo with a green leaf

Description automatically generated

## 4.8. List all the apple.png versions

A screenshot of a computer

Description automatically generated

## 4.9. Delete apple.png object (the new object)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

4.10. Expend Versions in order to see if the image has been deleted or not

A screenshot of a computer

Description automatically generated

4.11. Restore the old apple.png image (black and white) without re-uploading the image.

A black and white apple logo

Description automatically generated

## 4.12. Permanently delete all objects

A screenshot of a computer

Description automatically generated

4.13. Enable replication for <yourfullname>-hcs-foundation-program into a new bucket<yourfullname>-hcs-foundation-program-replica

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

4.14. Download a picture with the IBM logo and name it ibm.png

4.15. Upload ibm.png file into <yourfullname>-hcs-foundation-program and check the replication.

* It appeared after a while

A screenshot of a computer

Description automatically generated

4.16. Create a life cycle policy to move data from Standard Class IA after 30 days, IA to the Glacier after90 days, and expire after 360 days.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

# Amazon EC2

## 6.1 Create three EC2s:

Bastion-Server -> Windows VM [in HCS-Public]

Web-Server -> Linux VM [in HCS-Public]

DB-Server -> Linux VM [in HCS-Private]

So first I should create subnets in my default VPC (10.0.0.0/20)– it doesn’t work because the default VPC is public, I cannot make a subnet private, so I must create a new VPC.

HCS-Public 10.0.1.0/24

HCS-Private 10.0.2.0/24

Created the VPC-Dana in OHIO – us-east-2

https://assistanz.com/creating-vpc-public-private-subnets/index.html

The EC2 instance needs an public IP – an Elastic IP attached available in the zone BUT – I need to enable ICMP as well in SG

<https://stackoverflow.com/questions/21981796/cannot-ping-aws-ec2-instance>

The VPCs:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The EC2 Instances:

* Bastion-Server

A screenshot of a computer

Description automatically generated

* Web-Server

A screenshot of a computer

Description automatically generated

* DB-Server

A screenshot of a computer

Description automatically generated

* 1. Are servers reachable? Why? NO, need to modify security group to add an inbound rule to permit echo request ICMP on IPv4

### From your WorkStation ping Bastion-Server - SUCCESS

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

Eventually I did managed to get it to work, but I made some modification in the windows firewall of the ec2 instance to allow all inbound and outbound ICMP for IP4 traffic.

A screenshot of a computer

Description automatically generated

My guess is that by modifying the ‘File and Printer Sharing’ inbound rule, it got fixed.

A screenshot of a computer program

Description automatically generated

### From your WorkStation ping Web-Server - SUCCESS

A computer screen with white text

Description automatically generated

I finally got it working, I tried to modify the firewall in Amazon Linux 2023 – but it has none… eventually I edited the inbound rule to receive all traffic on ICMP:

A screenshot of a computer

Description automatically generated

### From your WorkStation ping DB-Server -FAIL?

A computer screen with white text

Description automatically generated

I do not expect it to be pingable from my workstation, because I moved it in a private subnet, I couldn’t connect to it through putty. As for security rules it uses the same as Web-Server: launch-wizard-2.

* 1. Are servers accessible? Why? No – they need security group rule to permit ssh for linux and rdp for windows

### Connect to Bastion-Server -SUCCESS

A screenshot of a computer

Description automatically generated

A screenshot of a computer security

Description automatically generated

A screenshot of a computer screen

Description automatically generated

I do not know why it adds ‘@ibm.com’ at the end of Administrator; connection through AWS System Manager works

UPDATE!!!!!!!!!

Managed to make it work with the user \Administrator; the blank in front is because the machine is missing hostname.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

On ipconfig it has only the private address:

A screenshot of a computer

Description automatically generated

The security rules on this ec2 instance:

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

### Connect to Web-Server - SUCCESS

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Also works through putty:

A screen shot of a computer

Description automatically generated

### Connect to DB-Server from Web-Server – SUCCESS

* I Used AWS System Manager quick setup to connect, but unfortunantely, after a week or so stopped working – I do not know why, I reconfigured it, but still doesn’t work… my guess is that I have to wait a while.

A computer screen shot of a computer program

Description automatically generated

* I don’t know how to add a key in EC2 Instance Connect for Web-Server if I cannot connect from my own workstation to it, I cannot scp/sftp the key to connect to DB-Server, I could have used winscp as well

SO I will use putty agent on my workstation

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Copied the key to AWS EC2 Web-Server in home path:

A screenshot of a computer

Description automatically generated

It didn’t work, unfortunately. I guess I could also create ssh keys and put them in know-host but I’ll stop for now

A computer screen shot of a black screen

Description automatically generated

## 6.4 Reconfigure the SGs :

Allow SSH for Linux VMs,

Allow RDP for Windows VM and

Allow ICMP – IPv4 from Anywhere [Linux and Windows VMs]

Inbound rules are for incoming traffic

Outbound rules are for outgoing traffic

### For bastion-server

* + Incoming: rdp, icmp
  + Out: icmp, rdp

A screenshot of a computer

Description automatically generated

Connection through RDP works now!

### For Web-server

* + In: ssh, icmp
  + Out: ssh – so I can access db-server, icmp

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

### For DB-Server:

* + In: ssh, icmp
  + Out: ssh, icmp
* Used launch-wizard-2 here as well; connection to it directly doesn’t work, but that should be ok because is on a private VPC

## 6.5 Retry all the PINGs and Connections:

### From Bastion-Server ping Web-Server - SUCCESS

A computer screen shot of a black and white screen

Description automatically generated

### From Bastion-Server ping DB-Server – FAIL?

I don’t expect it to work

A computer screen with white text

Description automatically generated

### From Web-Server ping Bastion-Server -SUCCESS

A computer screen shot of a computer program

Description automatically generated

### From Web-Server ping DB-Server – FAIL?

I do not expect it to work

A screenshot of a computer

Description automatically generated

### From DB-Server ping Web-Server FAIL

* Cannot connect to db-server using SSManager

### From DB-Server ping Bastion-Server FAIL

* Cannot connect to db-server usting SSManager

### Ping www. google.com from Bastion-Server – SUCCESS

A computer screen shot of a black screen

Description automatically generated

### Ping www.google.com from Web-Server - SUCCESS

A screenshot of a computer

Description automatically generated

### Ping www.google.com from DB-Server - FAIL

I cannot connect.

# 7. Cloud Watch

7.1. Create a CloudWatch Alarm for Bastion-Server, in order to generate an alarm (email) for Network Packets IN > 100.

A screenshot of a computer

Description automatically generated

A screenshot of a computer error

Description automatically generated

## 7.2. Generate some traffic in order to trigger the alarm.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

It stopped

A screenshot of a computer

Description automatically generated