Audrey Long

JHU WebSec Cloud Computing & Security Assignment

03/16/2021

Introduction

In this module you have learned a bit about virtualization and how a" cloud" is an abstraction of a typical data center that aggregates resources and then carefully distributes them based on demand.

For this assignment you get the chance to for some hands-on security experience using AWS, a popular cloud service provider. From semester-to-semester the freely available resources change, so this semester we will be exploring Amazon's S3 and Key Management Services (KMS).

DELIVERABLES

Submit a Word or PDF doc with annotated screenshots and address the 17 questions.

Part 1: AWS CloudTrail

Building on what we learned about server-side security, look at Amazon's CloudTrail service. Amazon relies heavily on the use of REST API's to interact with its services and CloudTrail is a great way to monitor API usage.

QUESTIONS

1. At a high-level, what is CloudTrail used for?

According to the Amazon web docs CloudTrail can be used for compliance aid to ensure internal policies and regulations are met. Data detection and exfiltration features are a feature of CloudTrial which can be utilized by collecting data from lambda functions and monitoring upon with cloud watch events. Security analysis can be used in this service to also provide insights into behavior patterns by analysing log data.

2. What role does CloudTrail play in the security and/or compliance realm of an organization?

The role that this tool plays is incident analysis along with compliance and risk analysis. This tool can be utilized to enable governance, compliance and lower risk by auditing AWS accounts. This tool can also be utilized for discovery and security analysis to collect data from amazon services to best lock down and protect important data based on the trends and log analysis.

3. How can CloudTrail be used to notify you of a potential security incident?

CloudTrail can be used to notify you of a potential security incident by setting up the tool to gather event logs from all services and then integrate these logs with tools such as cloudwatch to monitor and receive alerts on malicious events being tripped.

4. Provide 2 examples of alerts that may be useful to configure.

There are many alerts that would be excellent to configure with CloudTrail one of those would be to configure cloud trial to set an alarm if admin privileges get granted this way adversaries cannot achieve privilege escalation to overtake and concur your infrastructure and applications. Alerting on modifications to security groups would be another great example of what we would not want to happen if an adversary went into our environments. If these alerts are set then we can quickly investigate and mitigate the problems to ensure that information cannot be leaked, the system is locked down, and the adversary removed.

5. Provide 2 threats that exist against cloud computing?

In general two threats against cloud computing can come in the form of DDoS attacks which can potentially bring down your services and data breaches against the data we are trying to use and protect in the cloud environment.

6. How would you recommend defending against those threats using the data generated by CloudTrail? Would you use CloudWatch too?

With CloudTrail and CloudWatch we can gather log events from all of our services, which also include the capturing of packet information off the write to ensure that the people and machines connecting to our instance are clean and clear of adversaries. CloudTrail can capture many log events throughout the system to better understand events that are happening with the data to better protect and safeguard it from potential leakage by using a fine tooth comb to fully understand and analyze our infrastructure. Also DDoS protection can be enabled within cloudwatch to ensure our services always persist and have preventative measures against DDoS attacks by creating dashboards and alerts on.

Part 2: AWS Simple Storage Service (S3)

AWS S3 is a simplified service for highly durable data storage; it is cheap too! As with all data storage, there are security concerns, especially when it is being stored on the web: controlling access to the data, maintaining data integrity and confidentiality, and logging data access.

HANDS-ON

Let's step through a hands-on example for how to create a bucket and configure access within S3:

A. Start by registering for a free account at: qwiklabs.com

B. At the top, search for: “Introduction to Amazon Simple Storage Service (S3)”

C. Click on the lab and press” Start Lab”. You will have an hour to complete a lab that is projected to take 30.

D. Please take screenshots of the” important” steps. Things like successful outputs, and key configuration items are” important” while things like clicking ’Finish’ are not.

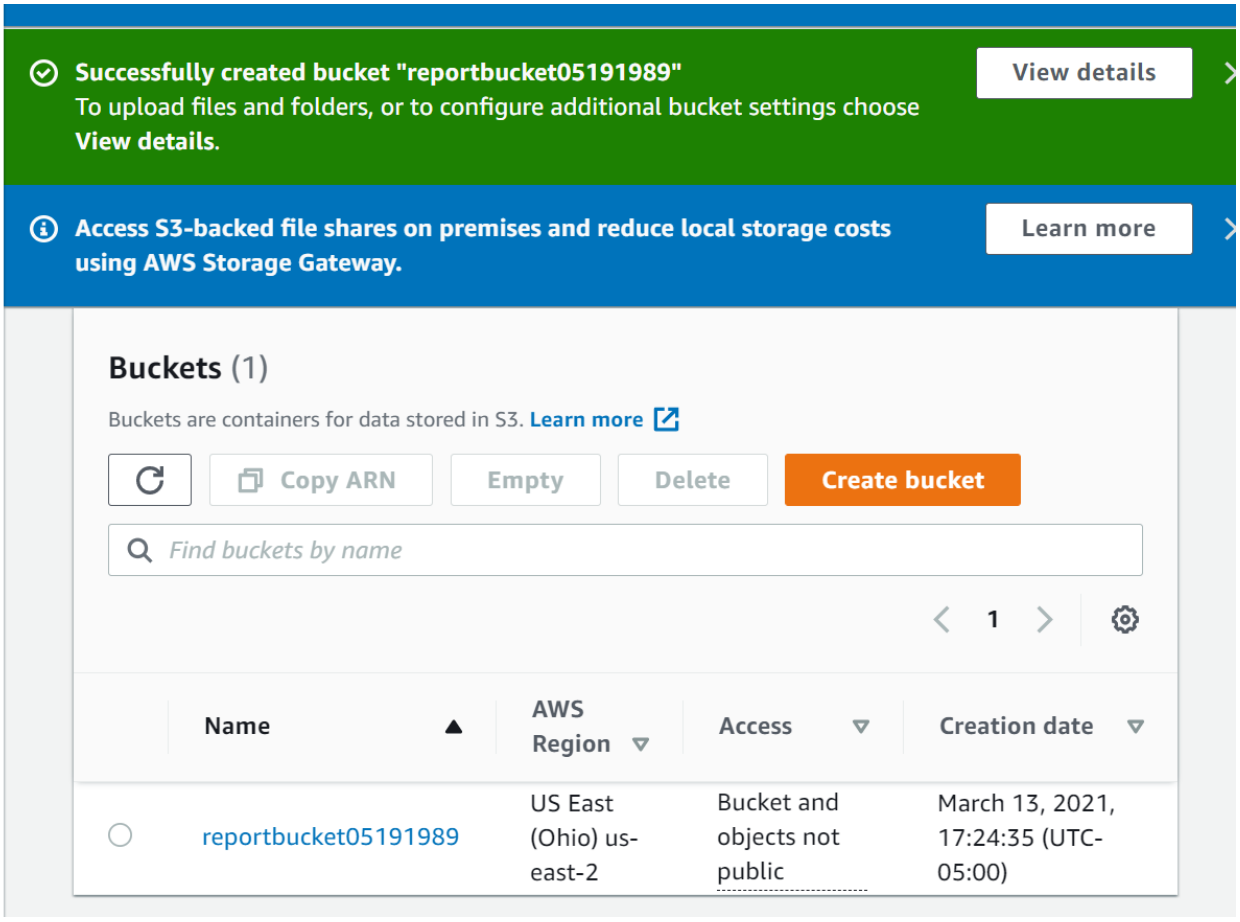

Figure 1: Task 1 - bucket creation

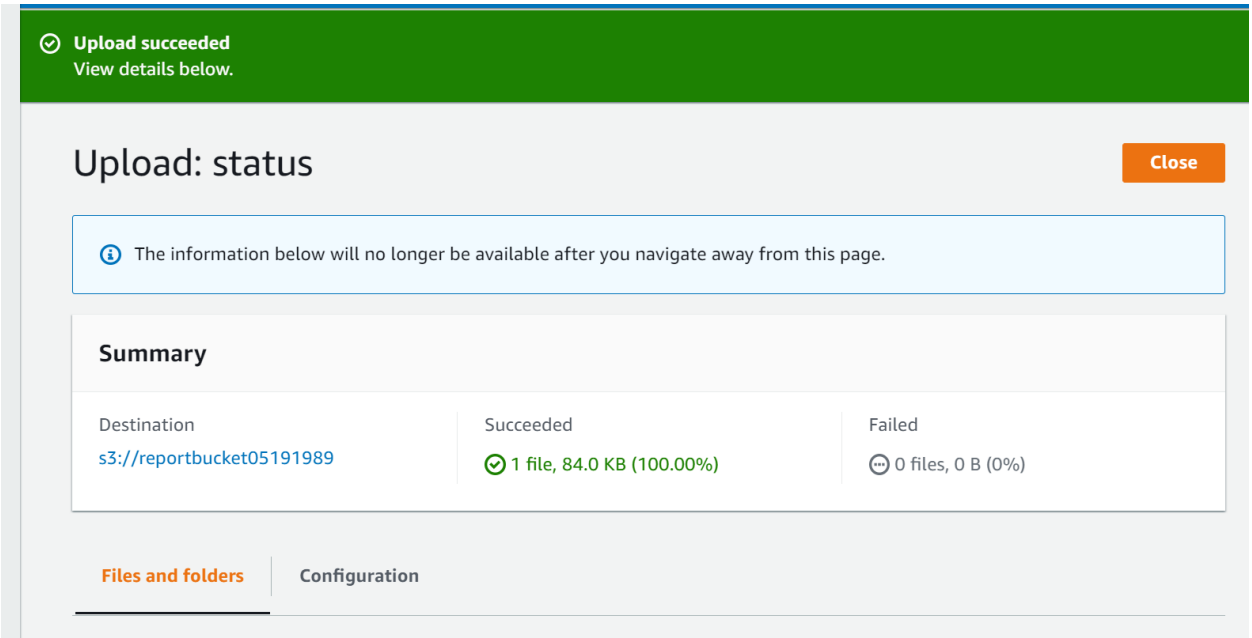

Figure 2: Task 2 - uploading image to new bucket

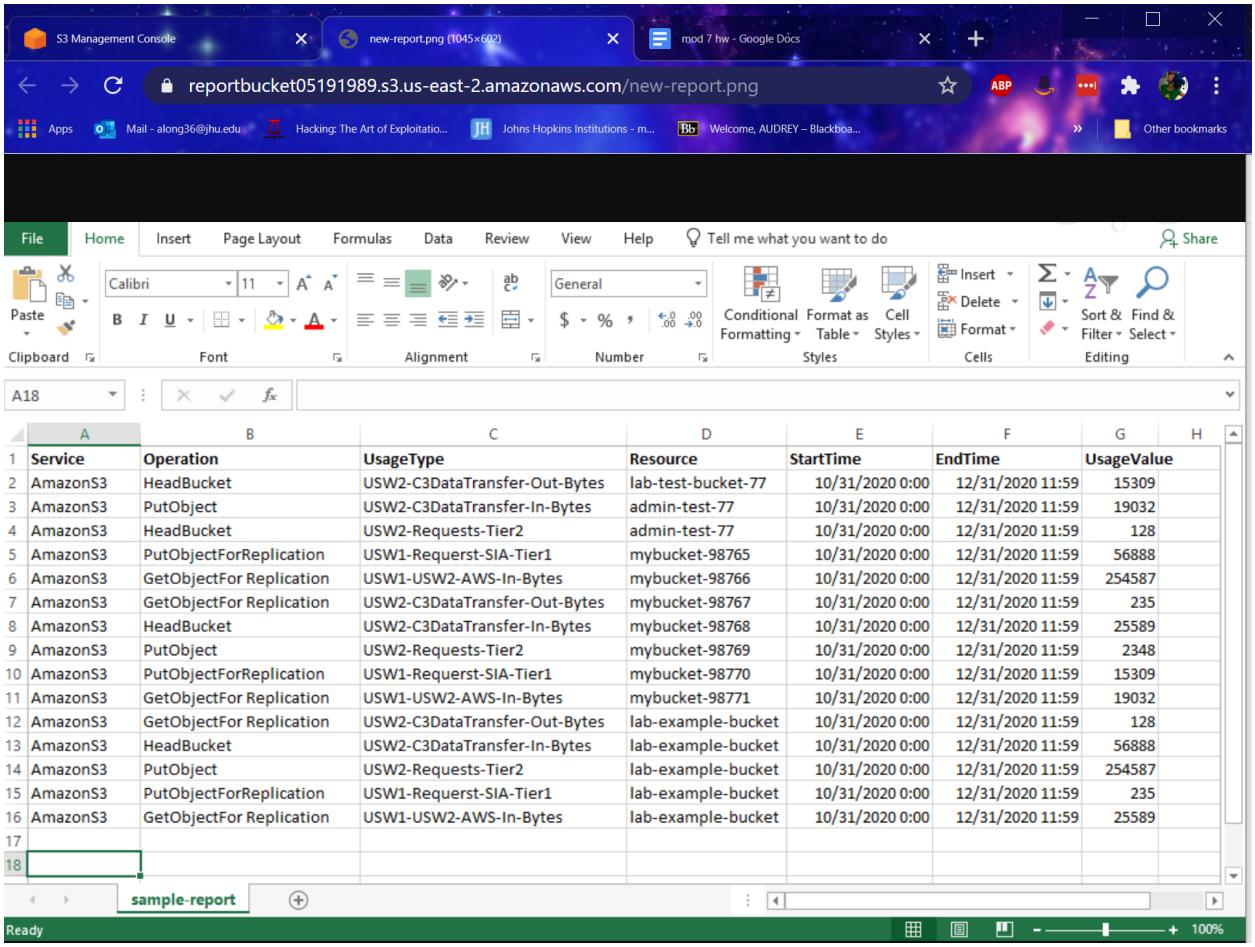

Figure 3: Task 3 - public bucket permissions

```
sh-4.2$ cd reports/
sh-4.2$ ls
dolphins.jpg  files.zip  report-test1.txt  report-test2.txt  report-test3.txt  whale.jpg
sh-4.2$ aws s3 cp report-test1.txt s3://bucket05191989
upload failed: ./report-test1.txt to s3://bucket05191989/report-test1.txt An error occurred (AccessDenie
d) when calling the PutObject operation: Access Denied
sh-4.2$
```

Figure 4: Task 4 - connectivity for ec2 instance

```
An error occurred (NoSuchBucket) when calling the ListObjectsV2 operation: The specified bucket does not
 exist
sh-4.2$ aws s3 ls s3://bucket05191989
2021-03-13 22:56:09      86065 new-report.png
sh-4.2$ cd reports/
sh-4.2$ ls
dolphins.jpg  files.zip  report-test1.txt  report-test2.txt  report-test3.txt  whale.jpg
sh-4.2$ aws s3 cp report-test1.txt s3://bucket05191989
upload failed: ./report-test1.txt to s3://bucket05191989/report-test1.txt An error occurred (AccessDenie
d) when calling the PutObject operation: Access Denied
sh-4.2$
sh-4.2$
sh-4.2$ pwd
/home/ssm-user/reports
sh-4.2$ aws s3 ls s3://bucket05191989
2021-03-13 22:56:09      86065 new-report.png
2021-03-13 23:05:12        113 sample-file.txt
sh-4.2$ ls
dolphins.jpg  files.zip  report-test1.txt  report-test2.txt  report-test3.txt  whale.jpg
sh-4.2$ aws s3 cp report-test1.txt s3://bucket05191989
upload: ./report-test1.txt to s3://bucket05191989/report-test1.txt
sh-4.2$ aws s3 ls s3://bucket05191989
2021-03-13 22:56:09      86065 new-report.png
2021-03-13 23:14:35         31 report-test1.txt
2021-03-13 23:05:12        113 sample-file.txt
sh-4.2$ aws s3 cp s3://bucket05191989/sample-file.txt sample-file.txt
download: s3://bucket05191989/sample-file.txt to ./sample-file.txt
sh-4.2$ ls
dolphins.jpg  files.zip  report-test1.txt  report-test2.txt  report-test3.txt  sample-file.txt  whale.jpg
sh-4.2$
```

Figure 5: Task 5 - create bucket policy

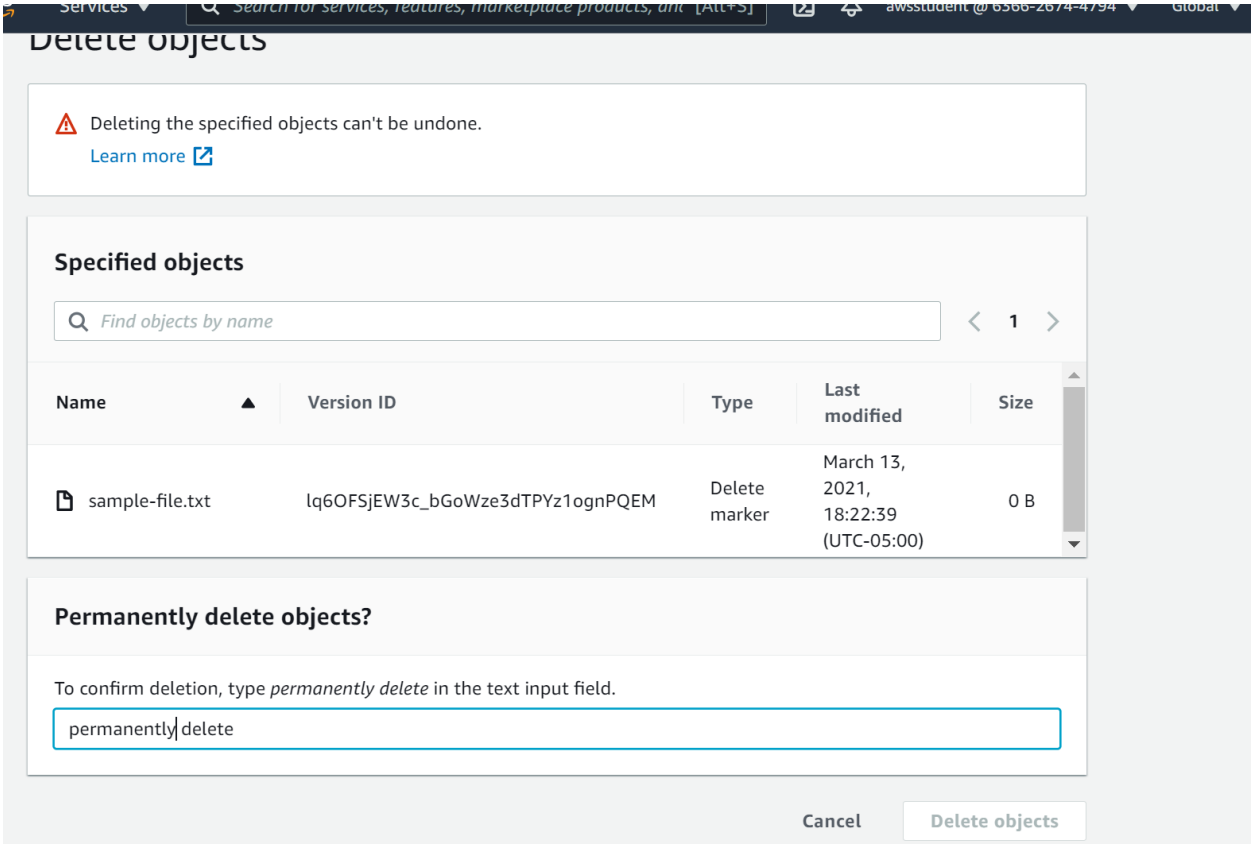

Figure 6: Task 6 - explore versioning

QUESTIONS

Please answer the following questions to get a better feel for not only how S3 stores data, but how it protects it.

7. S3 touts its data ”durability”. How ”durable” is the data (# of 9’s)?

According to the Amazon docs S3 is Designed to provide 99.999999999% durability and 99.99% availability of objects over a given year.

8. How much downtime does the S3 SLA claim? How much does that equate to annually?

For EC2 (and associated services) the available credits are as follows:

Monthly Uptime Percentage	Service Credit Percentage	Downtime Per Month
Less than 99.99% but equal to or greater than 99.0%	10%	4.38 minutes to 7.31 hours
Less than 99.0% but equal to or greater than 95.0%	30%	7.31 hours to 36.53 hours
Less than 95.0%	100%	More than 36.53 hours

Figure 7: SLA Downtime chart [4]

According to the chart above the worst case would be 7.31 hours a month which would equate to 87.72 hours a year.

9. Of the security fundamentals in CI4A, which can S3 provide?

Amazon S3 provides data integrity with any object being stored in this service because each object is tied with an entity tag which is a hash of the object which could be an MD5 depending on how the object was created and encrypted. Since the tag sometimes is not an MD5 hash it can be used to ensure the object entering storage is the same exiting by comparing the hash values.

10. Explain how data in S3 can be protected using server-side encryption.

Server side encryption in S3 protects data at rest and amazon ensures that each object entering s3 contains a unique key and also encrypts the key itself with a master key which is tied into a key rotation plan. Amazon also uses the strongest block ciphers to encrypt the data with NIST standard encryption.

11. Which encryption algorithm does S3 use? Explain any concerns you may have.

S3 uses 256-bit AES encryption standards. I don't have any concerns with this encryption practice in today's world. It's a worldwide standard right now and is very safe, especially with key rotation being utilized. The only concern will be when quantum computing comes around and breaks all of the encryption.

12. What impact does the GDPR have on how companies store data in S3?

As long as the customer consents to storing their data in amazon there should be any issues with GDPR in this scenario. The data is being encrypted in transit with web protocols and being encrypted at rest with the encryption mentioned above,

13. Describe the various access policies/permissions options available and how they can help enforce “least privilege access.”

One of amazon’s best practices for all services is to implement the practice of least privilege within their services. Basically this means that you grant user permissions based on how much privilege escalation they need in order to execute their tasks, and with this mindset we can ensure that every specific user can only have the permissions they need- no higher. Some features in Amazon we can utilize to practice this principal would be to utilize IAM roles and group users, developers, testers, auditors in their own specific categories to then group wide push their identity and access policies.

Part 3: Securing S3 using KMS

HANDS-ON

Now, we’ll step through a hands-on example for how to secure data in S3 using AWS’ KMS service:

A. Login to your Qwiklabs account and search for:” Introduction to AWS Key Management Service”

B. Click on the lab and press” Start Lab”. You will have 50 minutes to complete a lab that is projected to take 30.

C. Please take screenshots of the” important” steps. Things like successful outputs, and key configuration items

are” important” while things like clicking ’Finish’ are not.

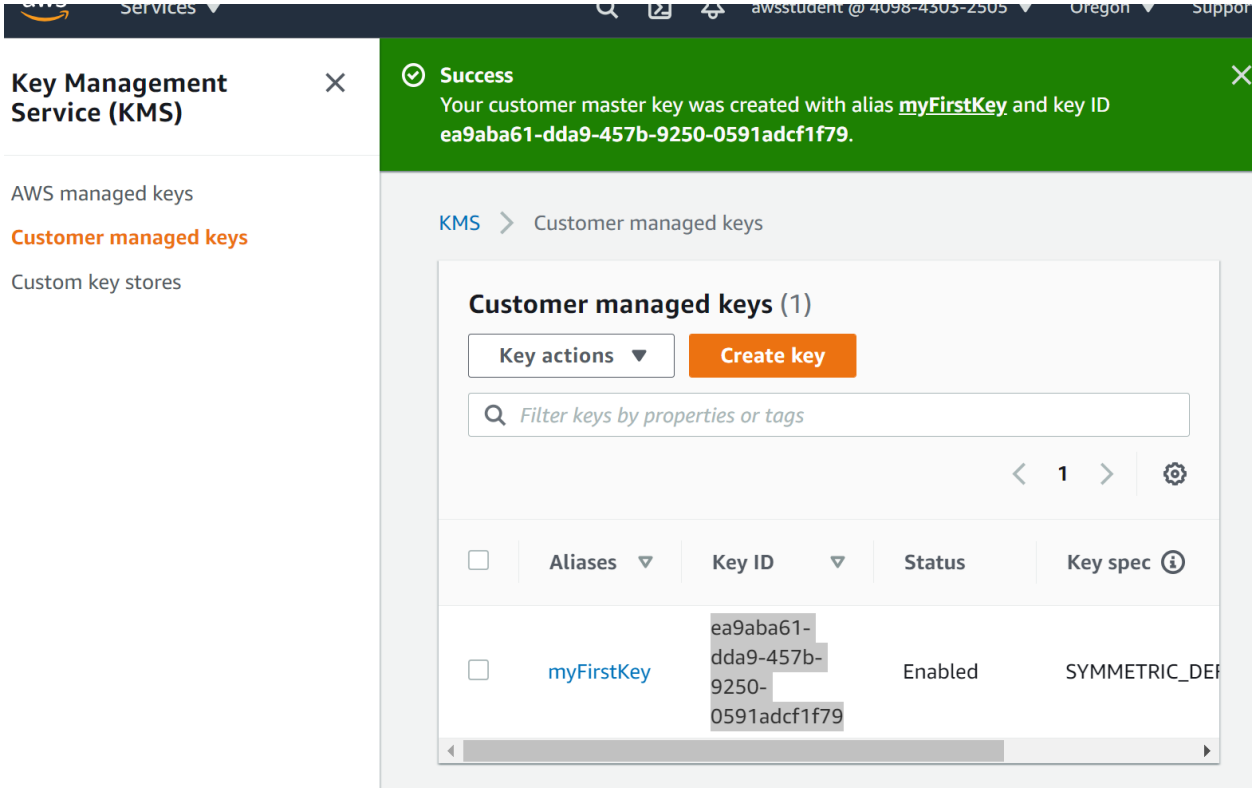

Figure 8: Task 1 Create KMS Master Key

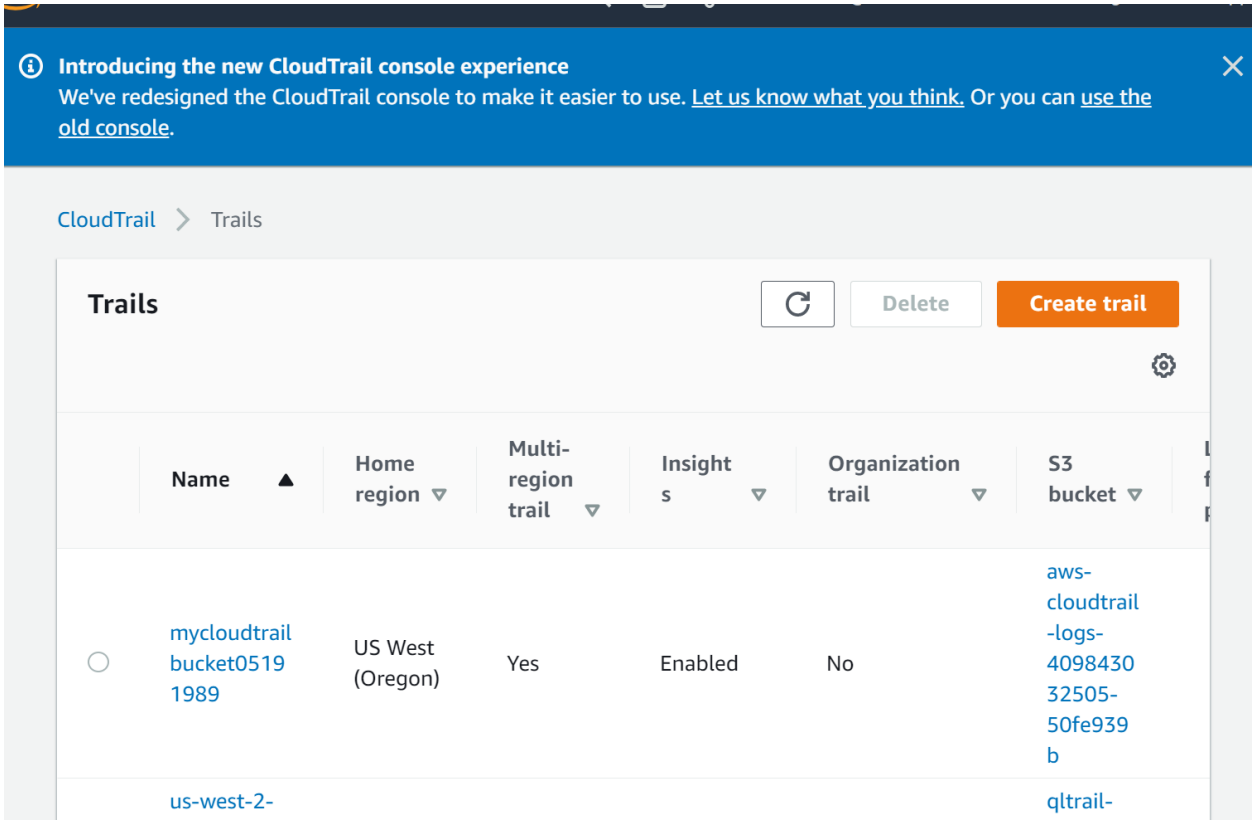

Figure 9: Task 2 Configure cloudtrail to store s3 bucket logs

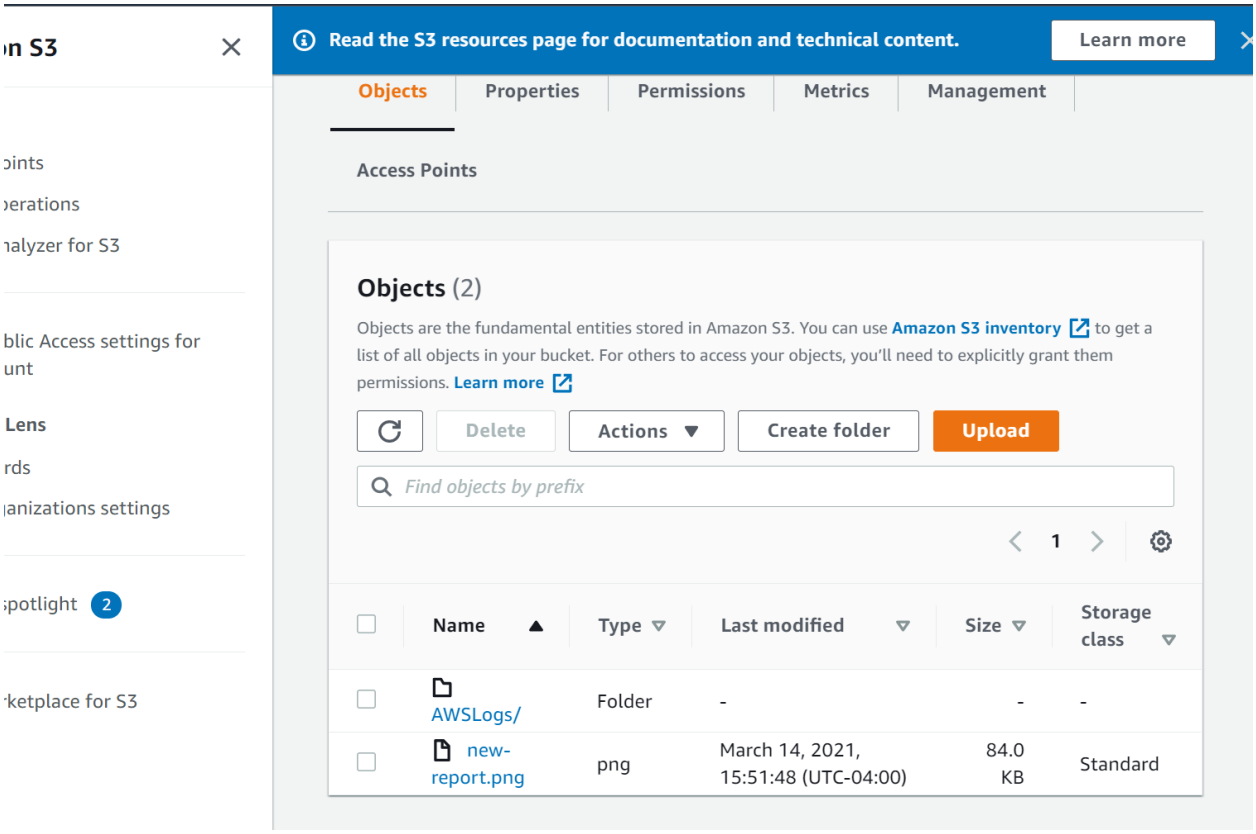

Figure 10: Task 3 Upload image to s3 bucket and encrypt

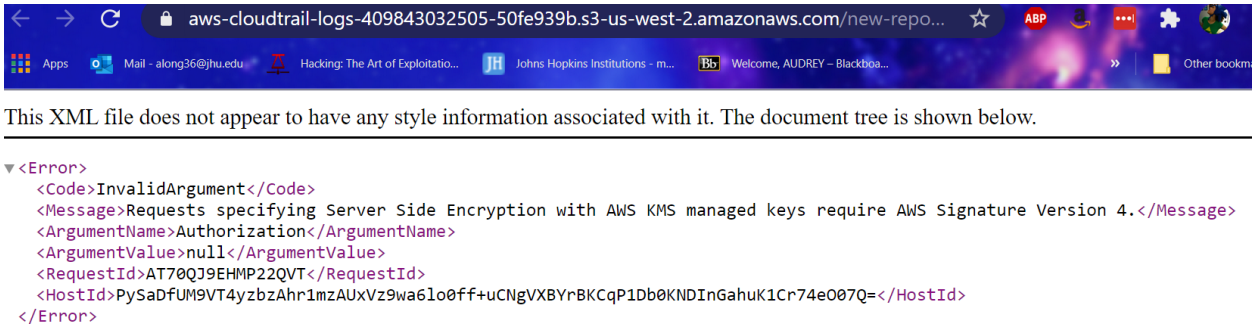

Figure 11: Task 4 access the encrypted image

{"Records":[{"eventVersion":"1.08","userIdentity":
{"type":"FederatedUser","principalId":"409843032505:awsstudent","arn":"arn:aws:sts::409843032505:federated-
user/awsstudent","accountId":"409843032505","accessKeyId":"ASIAV63EMMG4XMHDJVGI","sessionContext":{"sessionIssuer":
{"type":"IAMUser","principalId":"AIDAJ7KXOFGD43BRMLHCS","arn":"arn:aws:iam::409843032505:user/awsstudent","accountId":"409843032505","userName":"awsstuder
t"},"webIdFederationData":{},"attributes":{"mfaAuthenticated":"false","creationDate":"2021-03-14T19:37:52Z"}}},"eventTime":"2021-03-
14T19:45:00Z","eventSource":"kms.amazonaws.com","eventName":"CreateAlias","awsRegion":"us-west-2","sourceIPAddress":"73.83.17.187","userAgent":"aws-
internal/3 aws-sdk-java/1.11.970 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.282-b08 java/1.8.0_282
vendor/Oracle_Corporation","requestParameters":{"aliasName":"alias/myFirstKey","targetKeyId":"ea9aba61-dda9-457b-9250-
0591adcf1f79"},"responseElements":null,"requestID":"cb8eb179-fec9-4044-b03d-c10bce488114","eventID":"9dbc831f-ef67-4057-9db3-
ef5e58a53fff","readOnly":false,"resources":[{"accountId":"409843032505","type":"AWS::KMS::Key","ARN":"arn:aws:kms:us-west-2:409843032505:key/ea9aba61-
dda9-457b-9250-0591adcf1f79"},{"accountId":"409843032505","type":"AWS::KMS::Key","ARN":"arn:aws:kms:us-west-
2:409843032505:alias/myFirstKey"}],"eventType":"AwsApiCall","managementEvent":true,"eventCategory":"Management","recipientAccountId":"409843032505"},
{"eventVersion":"1.08","userIdentity":{"type":"FederatedUser","principalId":"409843032505:awsstudent","arn":"arn:aws:sts::409843032505:federated-
user/awsstudent","accountId":"409843032505","accessKeyId":"ASIAV63EMMG4XMHDJVGI","sessionContext":{"sessionIssuer":
{"type":"IAMUser","principalId":"AIDAJ7KXOFGD43BRMLHCS","arn":"arn:aws:iam::409843032505:user/awsstudent","accountId":"409843032505","userName":"awsstuder
t"},"webIdFederationData":{},"attributes":{"mfaAuthenticated":"false","creationDate":"2021-03-14T19:37:52Z"}}},"eventTime":"2021-03-
14T19:45:00Z","eventSource":"kms.amazonaws.com","eventName":"ListAliases","awsRegion":"us-west-2","sourceIPAddress":"73.83.17.187","userAgent":"aws-
internal/3 aws-sdk-java/1.11.970 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.282-b08 java/1.8.0_282
vendor/Oracle_Corporation","requestParameters":{"limit":100},"responseElements":null,"requestID":"2a74c382-25f3-4c74-8710-
1af5f429de54","eventID":"18b36879-4b35-4b6e-9aa5-
aa42d2e0cd9a","readOnly":true,"eventType":"AwsApiCall","managementEvent":true,"eventCategory":"Management","recipientAccountId":"409843032505"},
{"eventVersion":"1.08","userIdentity":{"type":"FederatedUser","principalId":"409843032505:awsstudent","arn":"arn:aws:sts::409843032505:federated-
user/awsstudent","accountId":"409843032505","accessKeyId":"ASIAV63EMMG4XMHDJVGI","sessionContext":{"sessionIssuer":
{"type":"IAMUser","principalId":"AIDAJ7KXOFGD43BRMLHCS","arn":"arn:aws:iam::409843032505:user/awsstudent","accountId":"409843032505","userName":"awsstuder
t"},"webIdFederationData":{},"attributes":{"mfaAuthenticated":"false","creationDate":"2021-03-14T19:37:52Z"}}},"eventTime":"2021-03-
14T19:44:59Z","eventSource":"kms.amazonaws.com","eventName":"CreateKey","awsRegion":"us-west-2","sourceIPAddress":"73.83.17.187","userAgent":"aws-
internal/3 aws-sdk-java/1.11.970 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.282-b08 java/1.8.0_282
vendor/Oracle_Corporation","requestParameters":{"description":"KMS Key for S3 data","policy":"{\n   \"Id\": \"key-consolepolicy-3\",\n   \"Version\":
\"2012-10-17\",\n   \"Statement\": [\n   {\n   \"Sid\": \"Enable IAM User Permissions\",\n   \"Effect\": \"Allow\",\n
\"Principal\": {\n   \"AWS\": \"arn:aws:iam::409843032505:root\"\n   },\n   \"Action\": \"kms:*\",\n
\"Resource\": \"*\"\n   },\n   {\n   \"Sid\": \"Allow access for Key Administrators\",\n   \"Effect\": \"Allow\",\n
\"Principal\": {\n   \"AWS\": \"arn:aws:iam::409843032505:user/awsstudent\"\n   },\n   \"Action\": [\n
\"kms:Create*\",\n   \"kms:Describe*\",\n   \"kms:Enable*\",\n   \"kms:List*\",\n   \"kms:Put*\",\n
\"kms:Update*\",\n   \"kms:Revoke*\",\n   \"kms:Disable*\",\n   \"kms:Get*\",\n   \"kms:Delete*\",\n
\"kms:TagResource\",\n   \"kms:UntagResource\",\n   \"kms:ScheduleKeyDeletion\",\n   \"kms:CancelKeyDeletion\"\n
],\n   \"Resource\": \"*\"\n   },\n   {\n   \"Sid\": \"Allow use of the key\",\n   \"Effect\": \"Allow\",\n
\"Principal\": {\n   \"AWS\": \"arn:aws:iam::409843032505:user/awsstudent\"\n   },\n   \"Action\": [\n
\"kms:Encrypt\",\n   \"kms:Decrypt\",\n   \"kms:ReEncrypt*\",\n   \"kms:GenerateDataKey*\",\n
\"kms:DescribeKey\"\n   ],\n   \"Resource\": \"*\"\n   },\n   {\n   \"Sid\": \"Allow attachment of persistent
resources\",\n   \"Effect\": \"Allow\",\n   \"Principal\": {\n   \"AWS\": \"arn:aws:iam::409843032505:user/awsstudent\"\n

Figure 12: Task 5

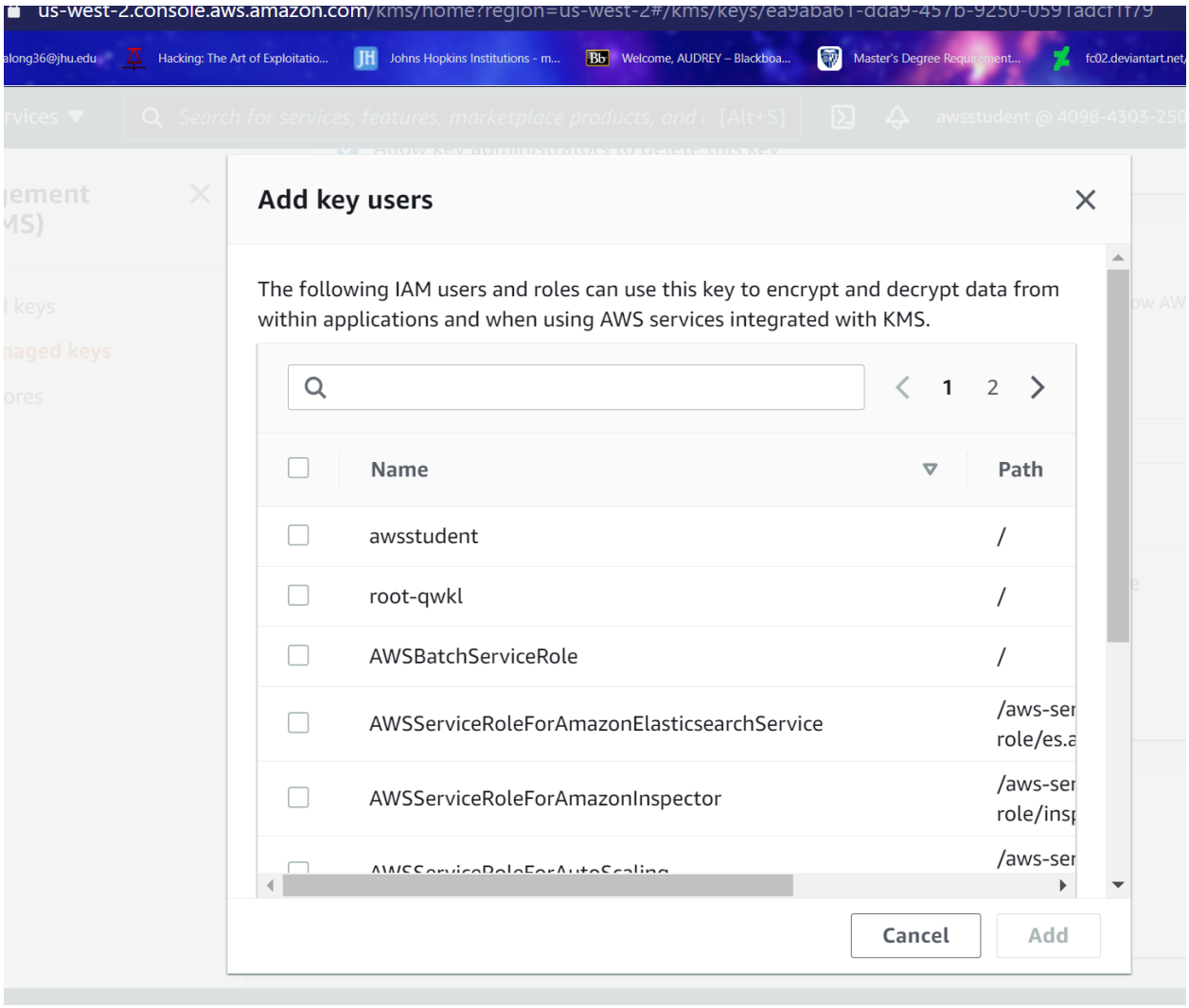

Figure 13: Task 6

QUESTIONS

14. How easy or difficult did AWS make it to implement encryption inside of S3?

AWS made the implementation of encryption inside of the S3 very easy, the guidelines we not too hard to follow.

15. Given this, how more or less likely are folks to exercise good security practices and encrypt their data?

I think the only way a developer is going to utilize this functionality is if a security engineer told them/encrypted the data settings for them, or if they were a requirement in the backlog to configure all of the security settings.

16. Explain the different methods AWS provides for key management and how each one works.

With the key management tab a user can add and customer role based encryption on data sets with unique keys. Customers can also store their own key materials in the key management page. This is a nice and centralized location to configure user and customer keys as well as access control policies to those key materials. With the AWS key management tool you can encrypt all of your applications and digitally sign everything, as well as manage all encryption of aws services.

17. Which one would you recommend to the CIO of your company and why?

If i were to recommend to the CIO a feature of these services in aws i would recommend setting up the data encryption and role based access to key materials so that only the keys land in the correct hands, i would also advise them to use the service to audit the key materials and settings often as well as implement key rotation strategies in order to safeguard the data from any adversaries and to ensure the system is not bogged down with cryptographic information on all services that do not need to be encrypted.

References

https://us-east-2.console.aws.amazon.com/cloudtrail/home?region=us-east-2#/ [1]
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html [2]
https://docs.aws.amazon.com/AmazonS3/latest/userguide/DataDurability.html [3]
https://www.logicata.com/blog/aws-service-level-agreement/ [4]
https://aws.amazon.com/premiumsupport/knowledge-center/data-integrity-s3/ [5]
https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingServerSideEncryption.html [6]