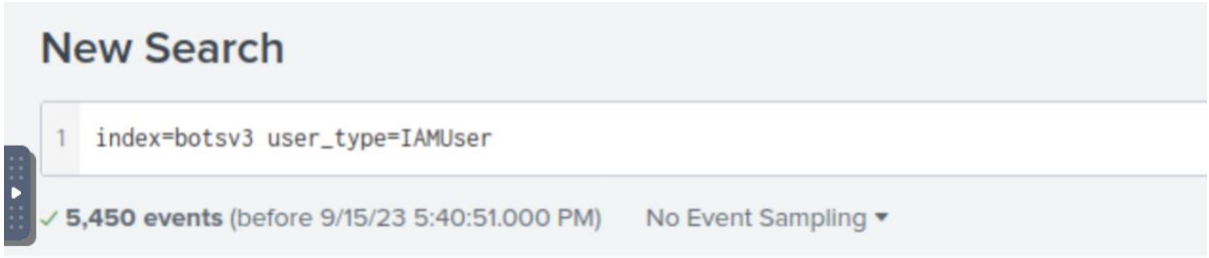
Splunk 3 – AWS Cloudtrail

In this task, you'll focus on AWS-related events with some questions focusing on endpoint-related events. The questions below are from the 200 series of the BOTSv3 dataset.

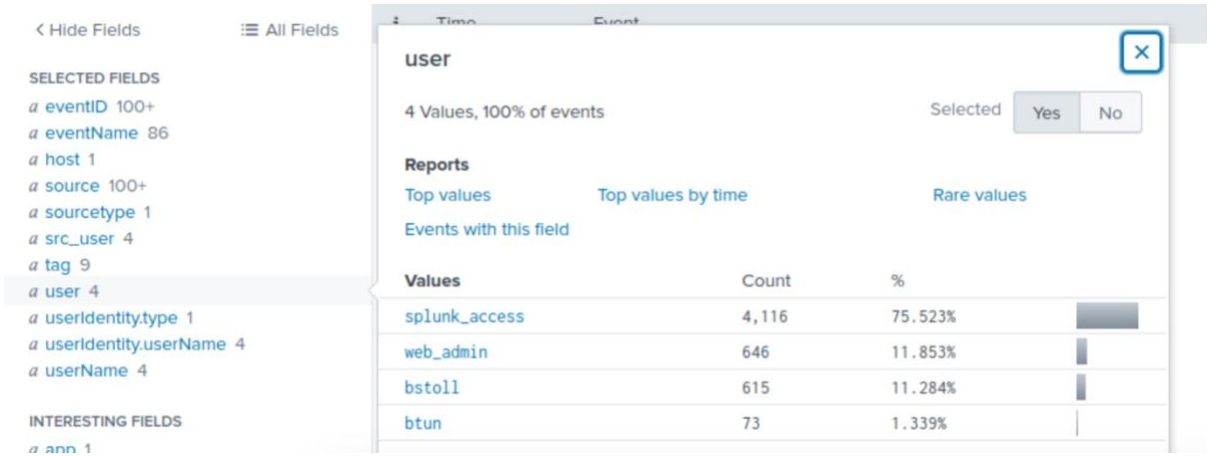
Question 1:
You're tasked to find the IAM (Identity & Access Management) users that accessed an AWS service in Frothly's AWS environment.
List out the IAM users that accessed an AWS service (successfully or unsuccessfully) in Frothly's AWS environment? Answer guidance: Comma separated without spaces, in alphabetical order. (Example: ajackson,mjones,tmiller)

Answer: bstoll,btun,splunk_access,web_admin

I first used the query `index=botsv3 *IAM*` from this I was able to find the "IAMUser" type and field name "user-type"
I then used the following query below



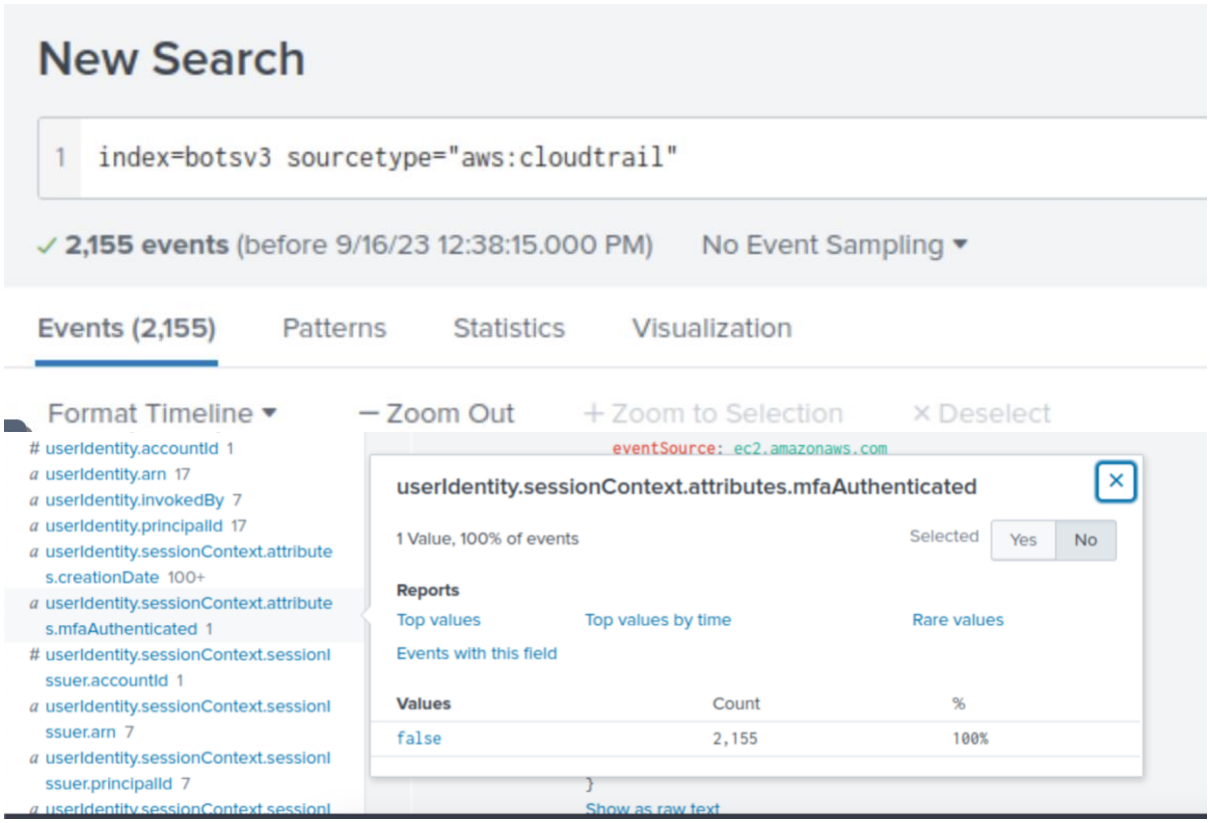
From there I searched the selected fields and found the answer, all 4 users as shown below in the "user" field.



Question 2:
Make sure you exclude events related to console logins.
It might be a good idea to do a keyword search query on this one. Don't forget to surround the keyword with asterisks.
What field would you use to alert that AWS API activity has occurred without MFA (multi-factor authentication)? Answer guidance: Provide the full JSON path. (Example: iceCream.flavors.traditional)

Answer: userIdentity.sessionContext.attributes.mfaAuthenticated

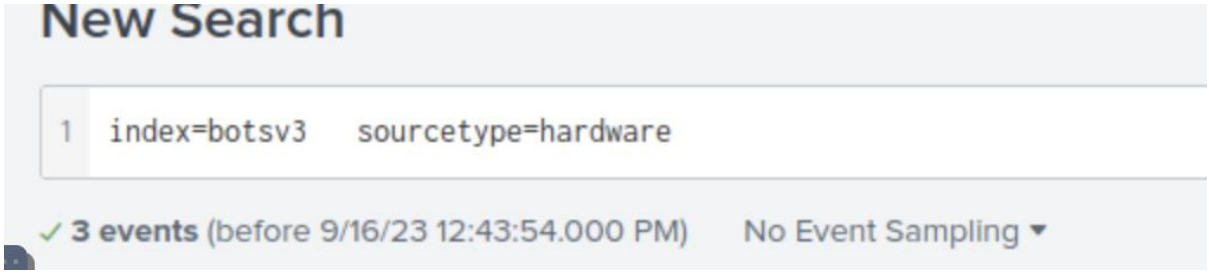
My focus here is fields, so I used the query below with the sourcetype aws:cloudtrail" and then hunted subfields within the "userIdentity" field and came across the answer below.



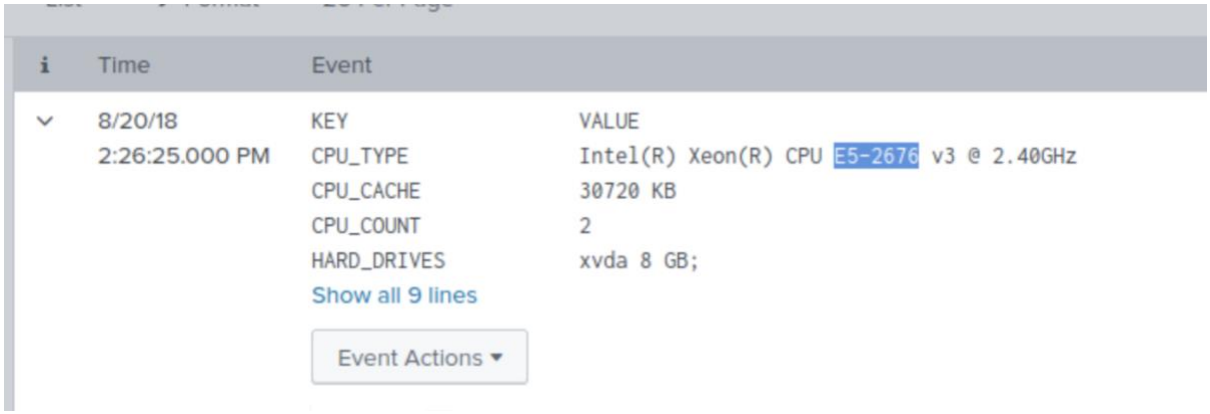
Question 3:
What is the processor number used on the web servers? Answer guidance: Include any special characters/punctuation. (Example: The processor number for Intel Core i7-8650U is i7-8650U.)

Answer: E5-2676

I first used "index=botsv3 *Intel*" however it produced too many search results. I then used the table function to go through all the potential sourcetypes whereby I found "hardware" and finally came up with the query below which produced 3 results.



Then after investigating I found the processor number highlighted below under the event



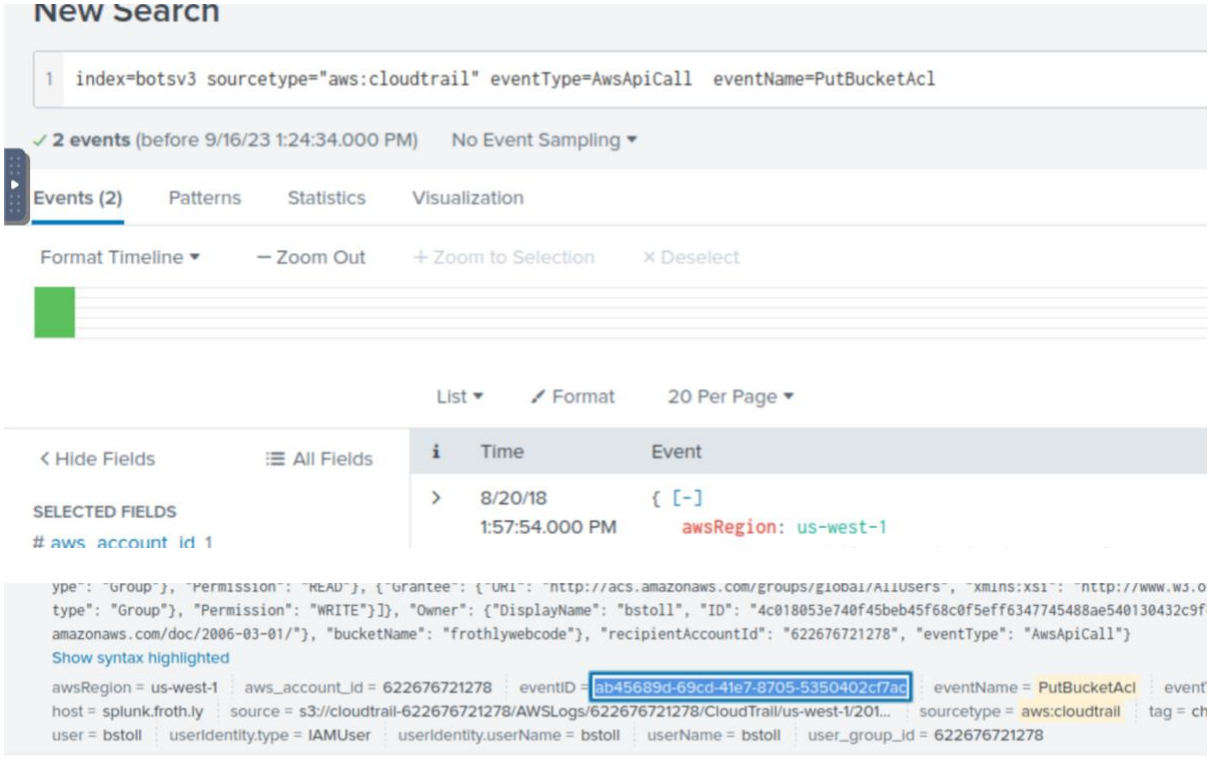
Question 4:
Bud accidentally makes an S3 bucket publicly accessible. What is the event ID of the API call that enabled public access? Answer guidance: Include any special characters/punctuation.

Answer: ab45689d-69cd-41e7-8705-5350402cf7ac

This was quite difficult and took sometime. I initially tried to find an error code as the question suggested the incident was an accident however with no luck. I then went further using the query below but it didn't produce the policy or rule I was looking for.

```
iam-password-policy
iam-user-group-membership-check
iam-user-no-policies-check
lambda-function-public-access-prohibited
rds-multi-az-support
rds-storage-encrypted
restricted-ssh
root-account-mfa-enabled
s3-bucket-logging-enabled
s3-bucket-public-read-prohibited
s3-bucket-public-write-prohibited
```

I then done some research into event names in relation to modifying/updating buckets or permissions and came up with “PutBucketAcl”. I then added the following into the query below which produced 2 events. After analysing the events I was able to decipher the event ID as highlighted below.



Question 5:
What is Bud's username?

Answer: bstoll

After finding the event in the previous question I was simply able to go through the fields and find the user as stated below. “bstoll”

Question 6:
What is the name of the S3 bucket that was made publicly accessible?

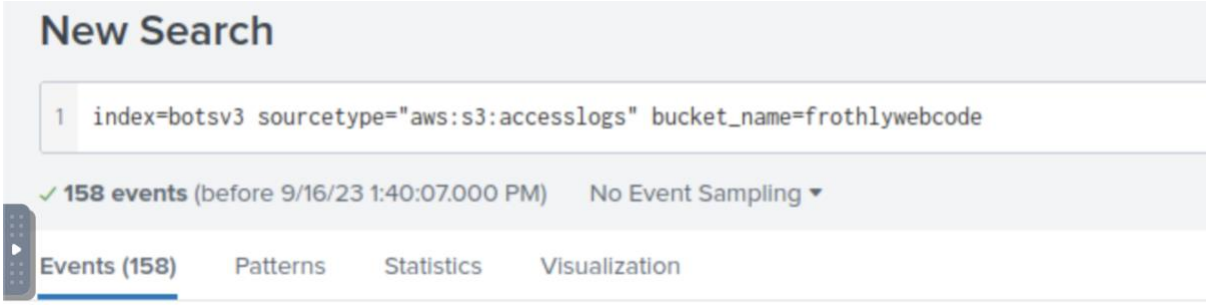
Answer: frothlywebcode

This was also surprisingly difficult, after some research I found the standard field name given for S3 buckets is usually “Bucket” or “bucketname”. I used both in the query and was able to find the answer in the event below

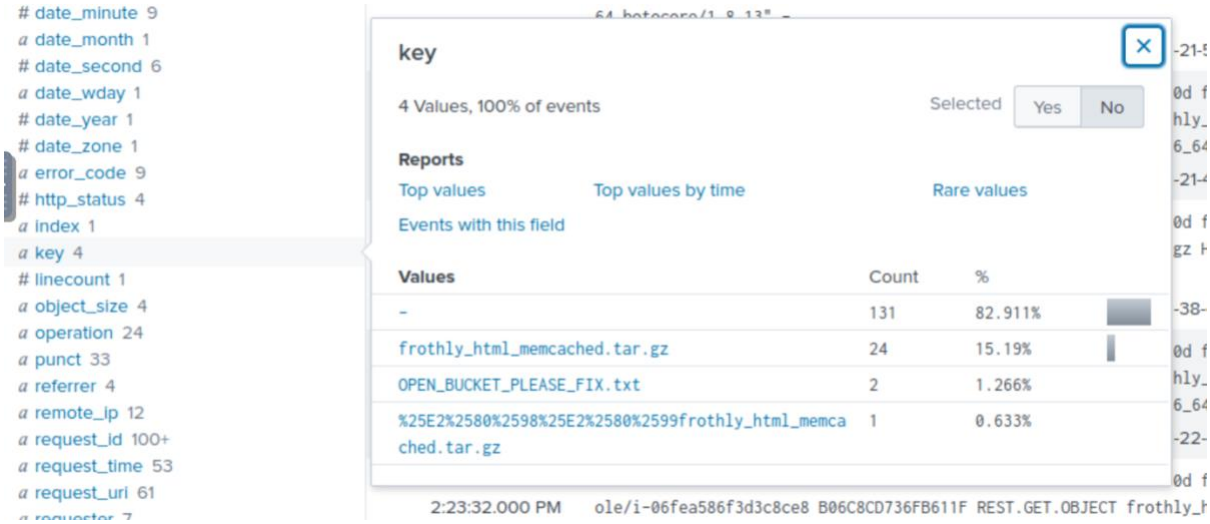
Question 7:
What is the name of the text file that was successfully uploaded into the S3 bucket while it was publicly accessible? Answer guidance: Provide just the file name and extension, not the full path. (Example: filename.docx instead of /mylogs/web/filename.docx)

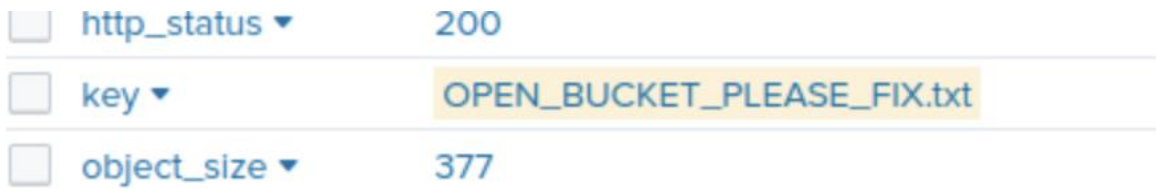
Answer: OPEN_BUCKET_PLEASE_FIX.txt

I used the bucketName:”frothlywebcode” from the previous question combined with the sourcetype “aws:s3:accesslogs”. This produced 158 events from which I investigated the field names.



Using the “key” field you can see the 4 files below. As im after a .txt file I queried “OPEN_BUCKET_PLEASE_FIX.txt” value and confirmed that it was in fact the answer



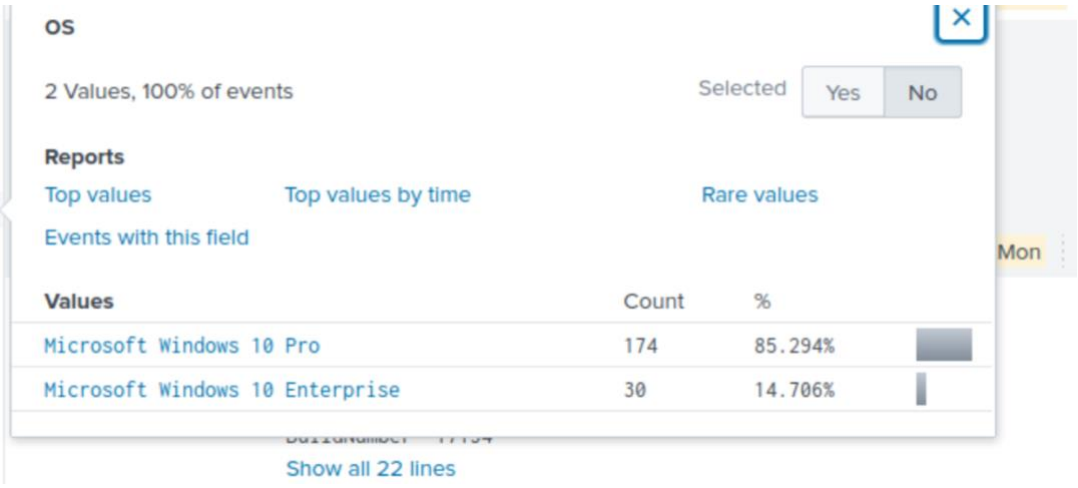


Question 8:

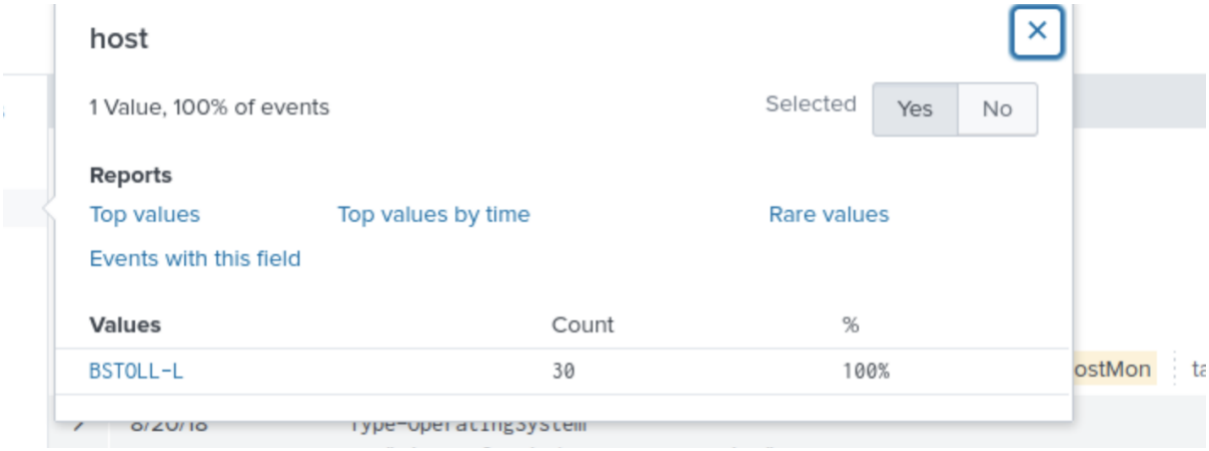
What is the FQDN of the endpoint that is running a different Windows operating system edition than the others?

Answer: BSTOLL-L.froth.ly

I used the OS field within the “wineventlog” which came up with the following values. I was able to then find that the different windows operating system edition was in fact “Microsoft Windows 10 Enterprise”



From there I could find the host of that windows operating system.



However the question was asking for the FQDN (fully qualified domain name) and so I used the host value from above in the query below to then find the answer under the “ComputerName” subfield below as shown.