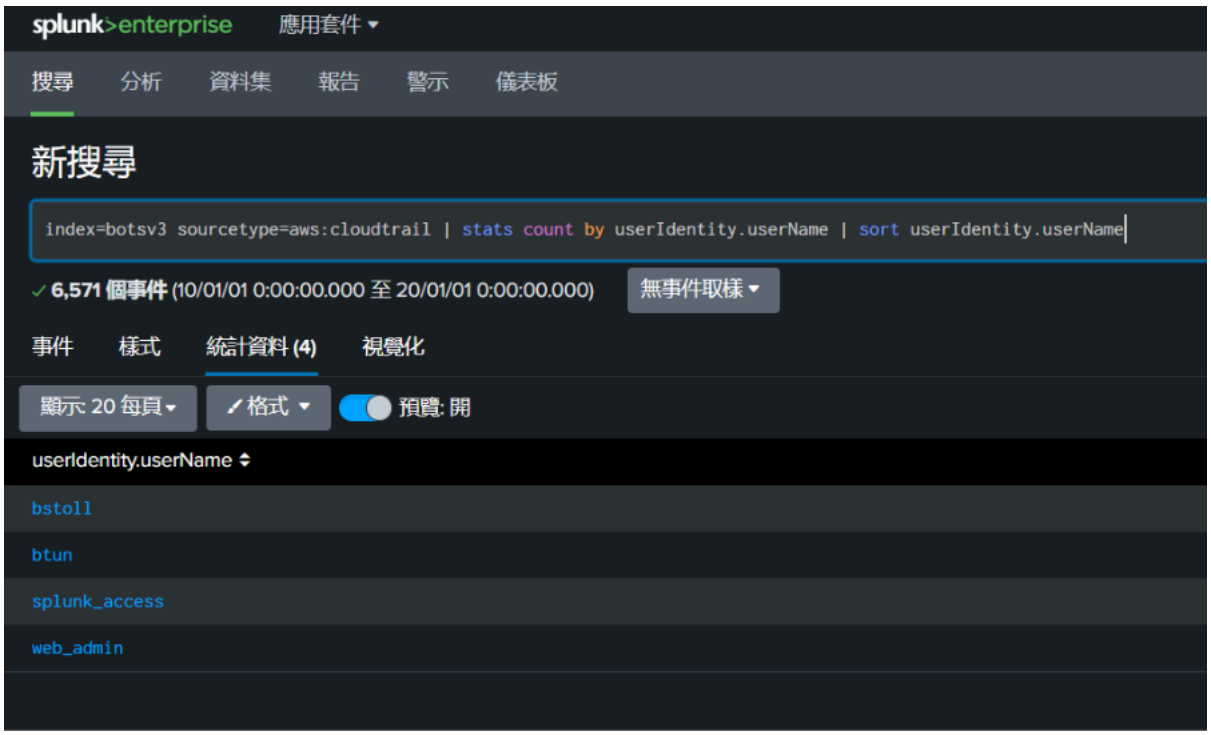
Answers to the 200-level Questions

Question 1: Which IAM users used AWS services?

Answer: bstoll,btun,splunk_access,web_admin

Search used: `index=botsv3 sourcetype=aws:cloudtrail | stats count by userIdentity.userName | sort userIdentity.userName`

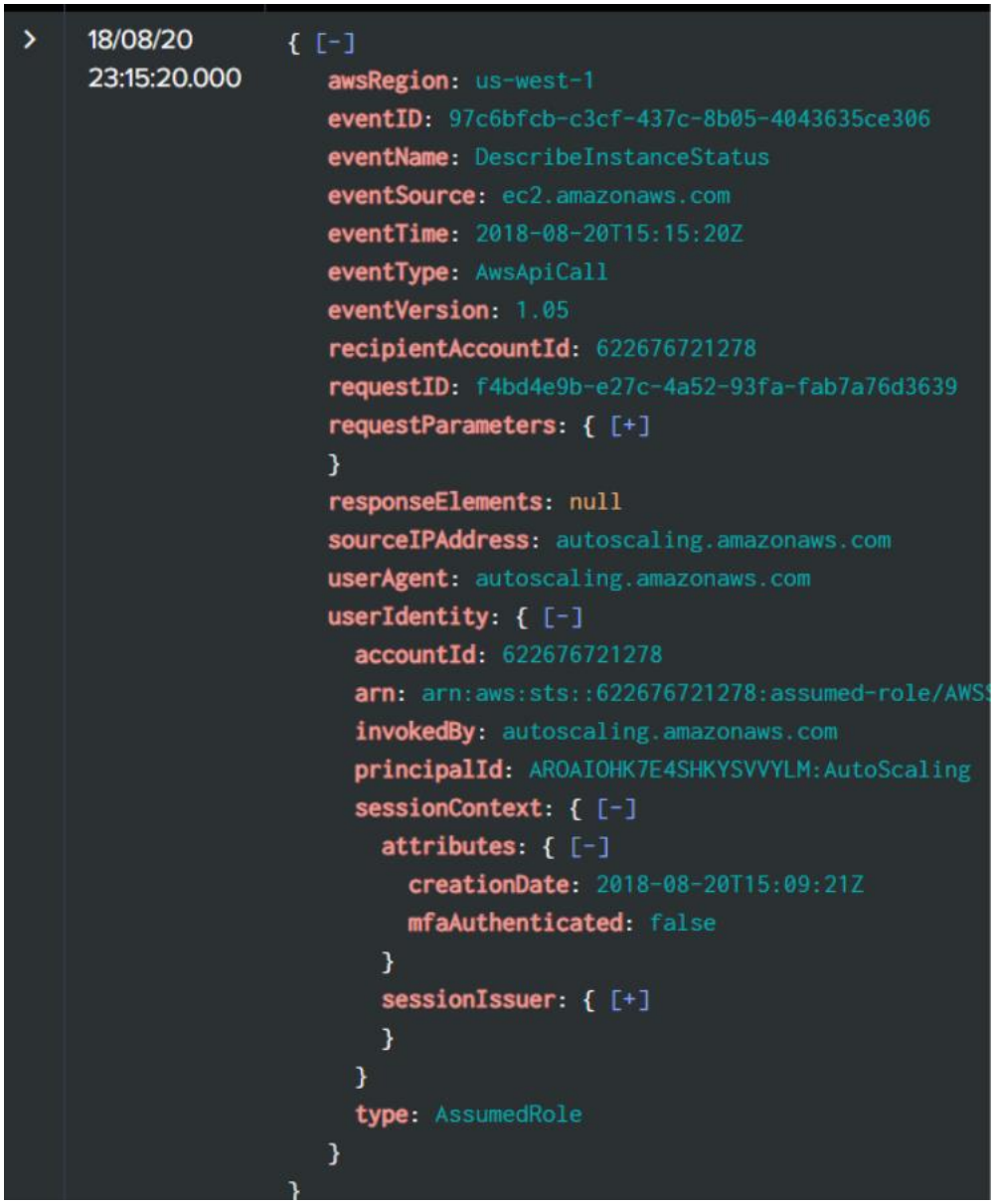
Pay attention to userName



Why it matters: In a real company, SOC must watch who is using cloud accounts. Strange users or too many actions can be signs of hacking.

Question 2: Which field shows if someone did NOT use MFA?

Answer: userIdentity.sessionContext.attributes.mfaAuthenticated



Pay attention at mfaAuthenticated

MfaAuthentication: false

Why it matters: Without MFA, stolen passwords are very dangerous. SOC should make an alert for any important action done without MFA.

Question 3: What CPU model is on the web servers?

Answer: E5-2676

Why it matters: Knowing normal hardware helps SOC notice strange things, for example if CPU usage suddenly goes very high because of malware.

Question 4: What is the Event ID that made the S3 bucket public?

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

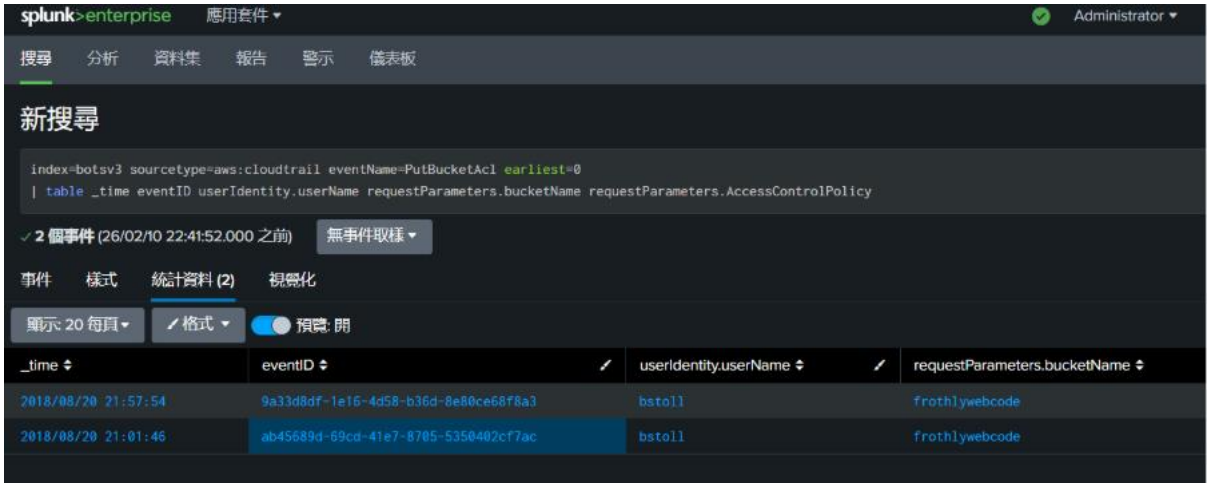
```
{ [-]
  Grantee: { [-]
    URI: http://acs.amazonaws.com/groups/global/AllUsers
    xmlns:xsi: http://www.w3.org/2001/XMLSchema-instance
    xsi:type: Group
  }
  Permission: READ
}
{ [-]
  Grantee: { [-]
    URI: http://acs.amazonaws.com/groups/global/AllUsers
    xmlns:xsi: http://www.w3.org/2001/XMLSchema-instance
    xsi:type: Group
  }
  Permission: WRITE
}
]
}
```


Pay attention at /AllUsers

Why it matters: This ID proves exactly when and how the security mistake happened.

Question 5: What is Bud’ s username?

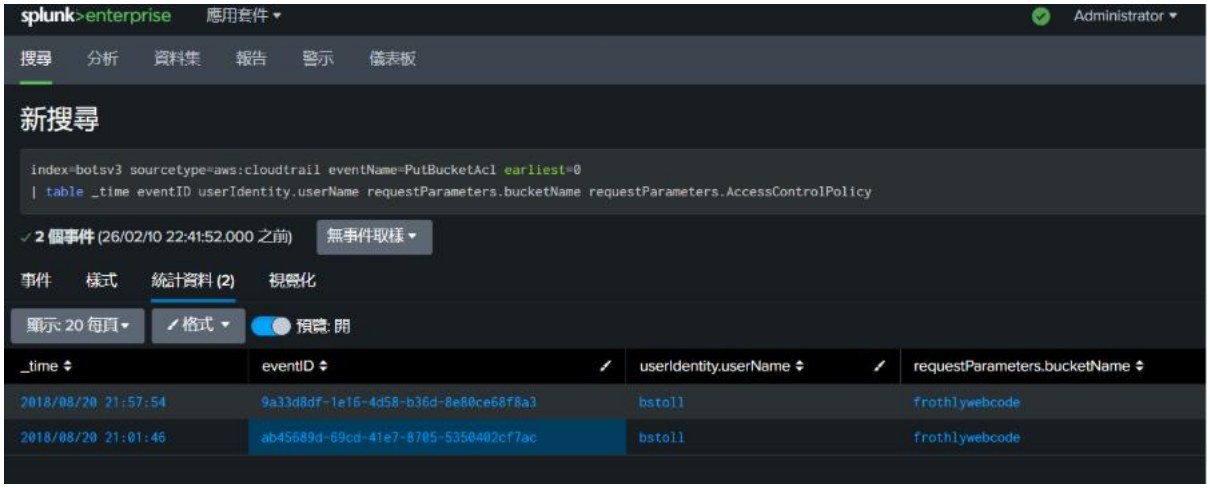
Answer: bstoll



Why it matters: We can see it was probably an accident by an employee, not an outside hacker.

Question 6: What is the name of the public S3 bucket?

Answer: frothlywebcode

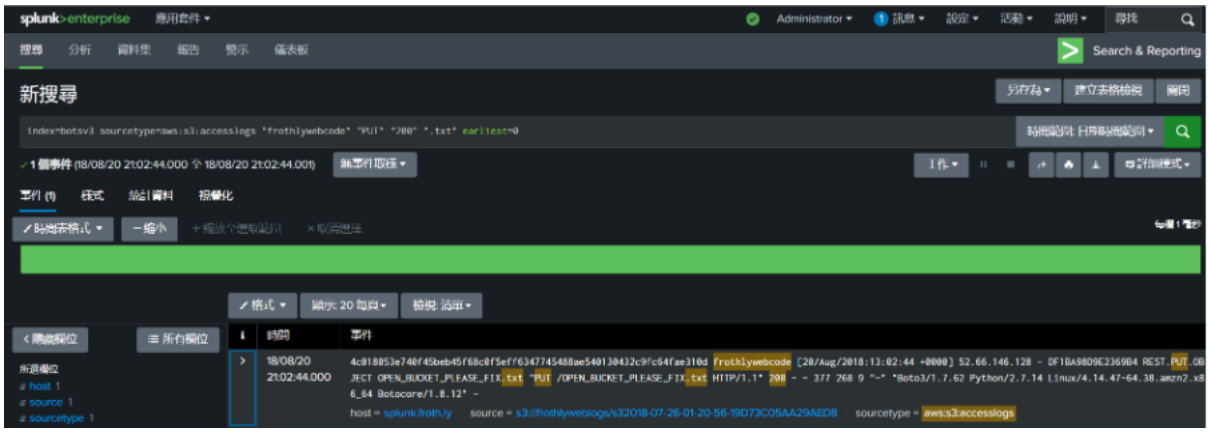


Pay attention at bucketName

Why it matters: Knowing the exact bucket name helps understand how much data was at risk.

Question 7: What text file was uploaded when the bucket was public?

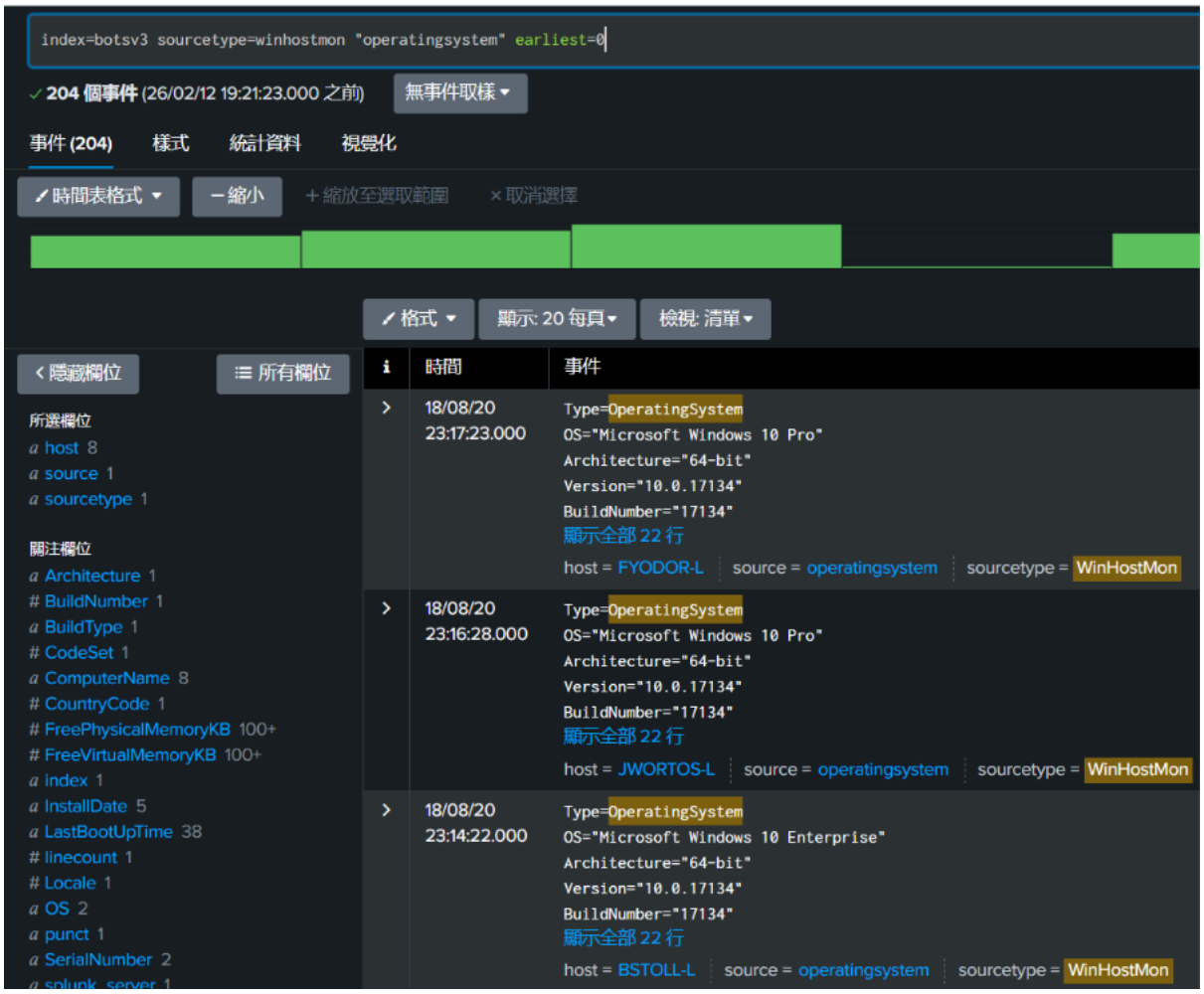
Answer: OPEN_BUCKET_PLEASE_FIX.txt



Why it matters: This shows attackers (or curious people) could download secret files very easily after the mistake.

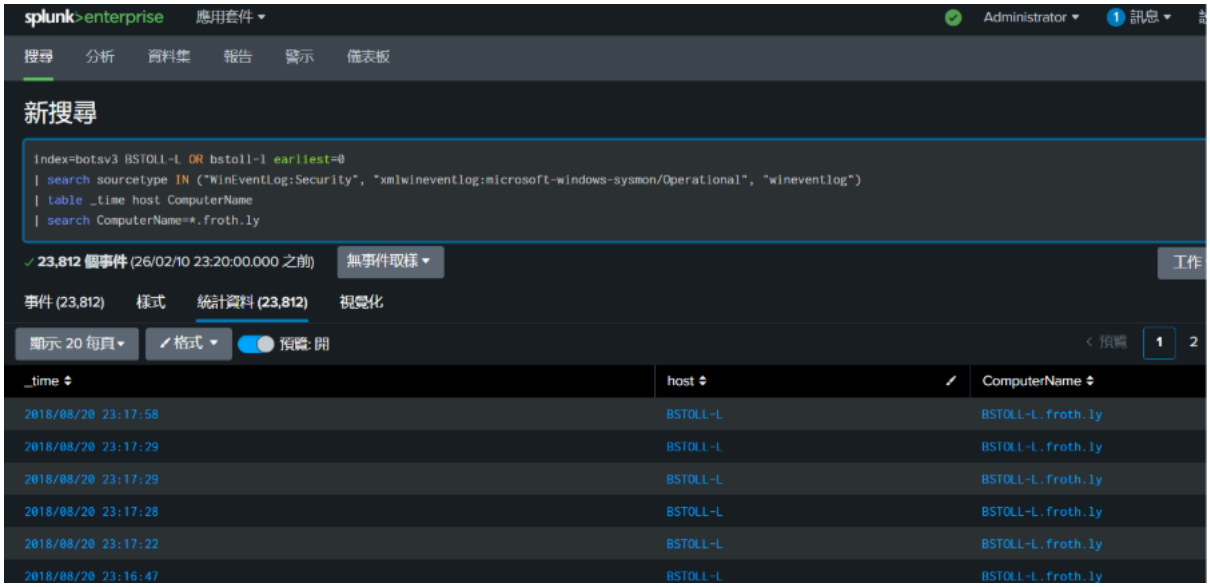
Question 8: Which computer has a different Windows version?

Answer: bstoll-l.froth.ly



Pay attention at OS=” Microsoft Windows 10 Enterprise”

Other hosts using Microsoft Windows 10 Pro, but host: BSTOLL-L is uniquely using Microsoft Windows 10 Enterprise version.



Why it matters: Different versions can be a sign of compromise, or just bad management — SOC should check both.