

2023
MACADMINS
CONFERENCE

ITS-LOG!



**The one-click collector of diagnostic logs
and user feedback for busy Mac Admins!**

Bradley Chapman

Mac Systems Engineer



ITS-LOG!

- I The Problem
- II Case Studies
- III The Solution
- IIII Let's Build It
- V Remarks



The Problem

An emergency arises...



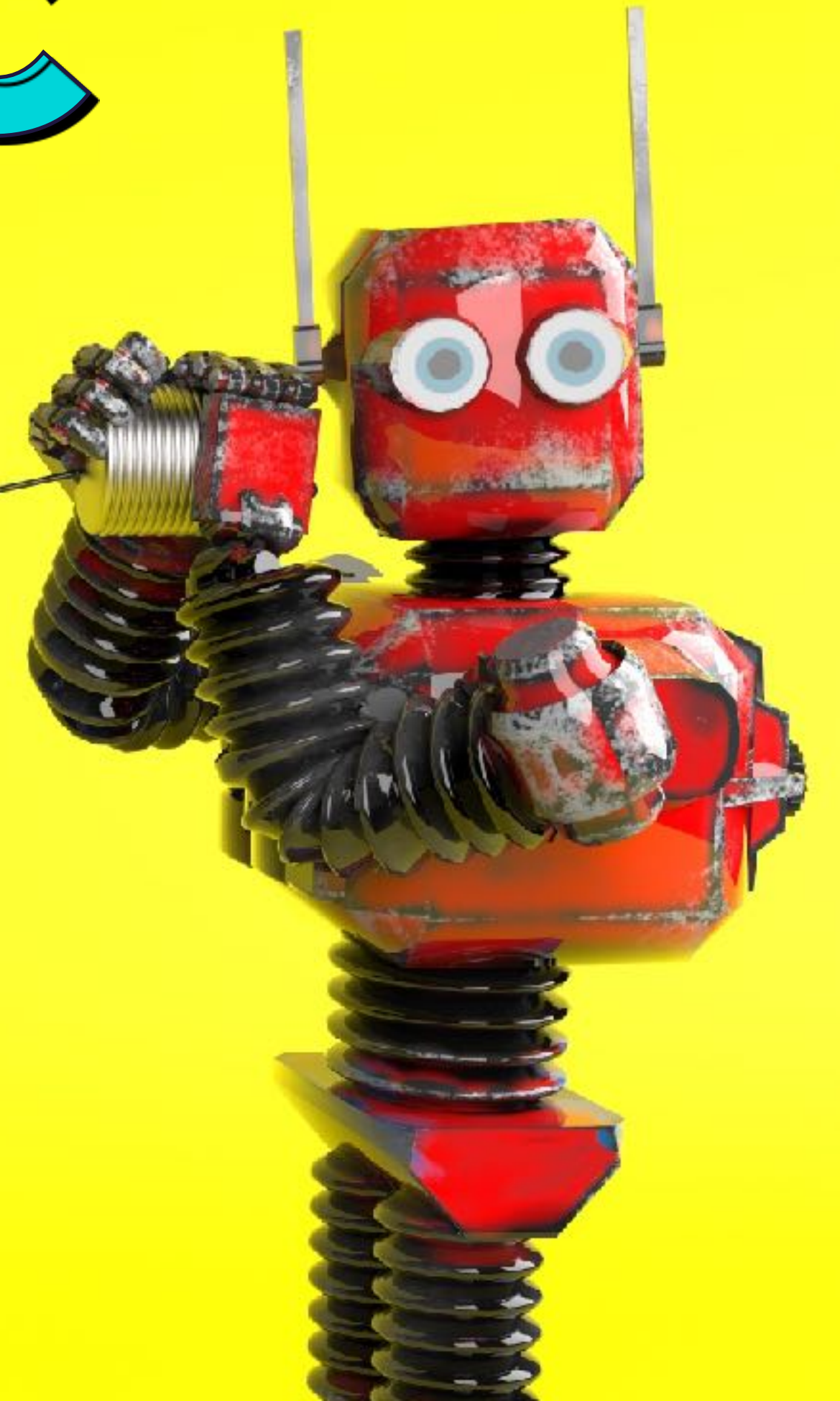
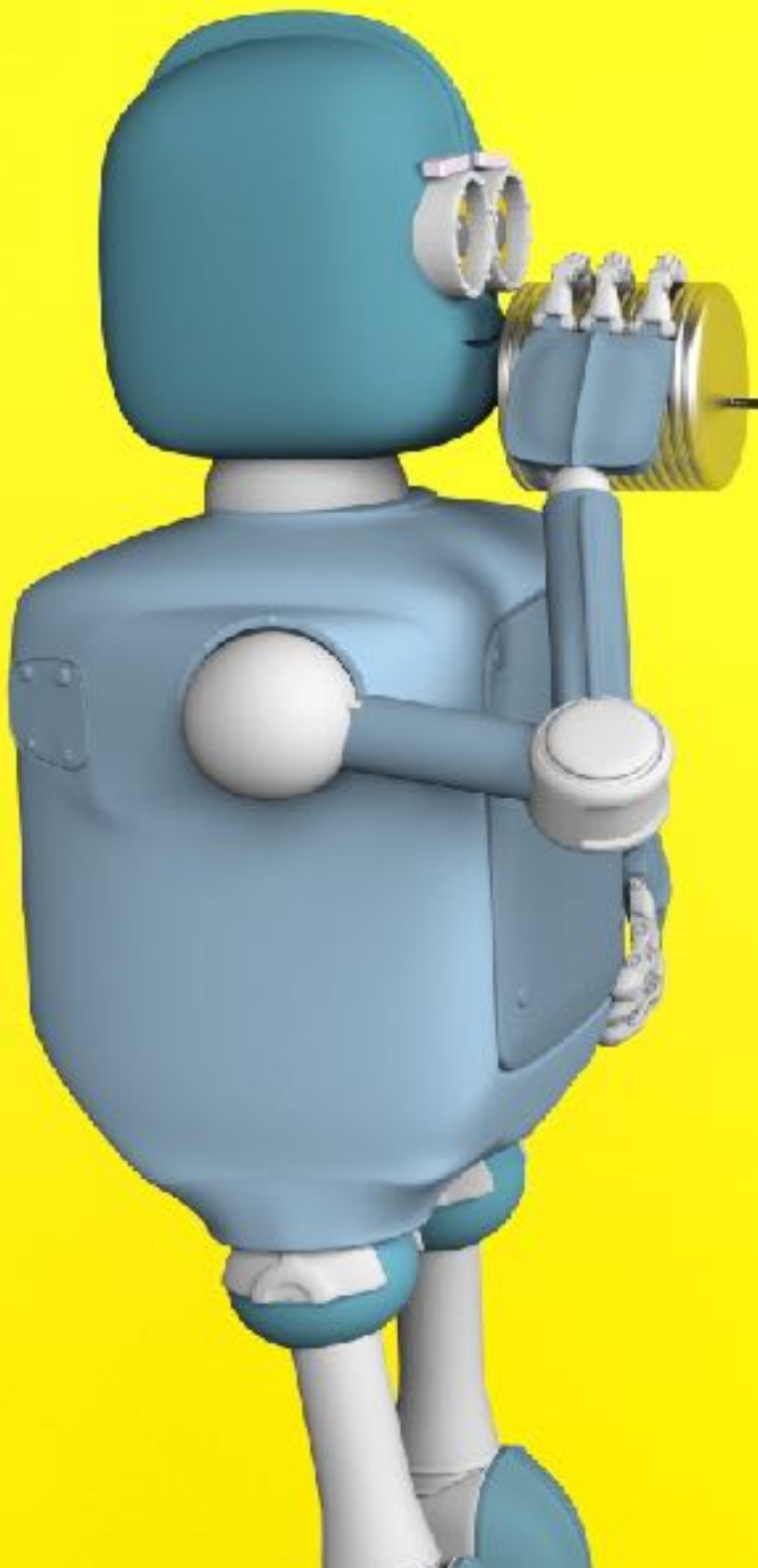
An emergency arises...

- ★ User has a hard crash
- ★ Opens a ticket and escalates urgently
- ★ Help Desk reaches out to admins
- ★ Some symptoms not understood, or overlooked
- ★ Additional details required from Mac
- ★ End user not always available for timely follow-up
- ★ We try to collect logs anyway (cross fingers)
- ★ Critical story details may already be lost

THE LIFE TELEPHONIC

WITH STEVE SAYS-WHO

a film by
WES ANDERSON





Case Studies

Three Examples In the Wild



STORY #1

The local support team told us:



“Users are getting locked out of their Macs randomly.”

What the user actually said:



“My screen was black this morning when I turned it on. I could see the mouse, but couldn’t enter my password anywhere, so I restarted. This happens every month or so. Also, my coworker had it happen to her Mac around the same time. We both have docking stations and external monitors.”

Root Cause Analysis:



A rare issue with the loginwindow process and screen savers, which resulted in a black screen on multi-monitor setups after the Mac was awakened from sleep.

A case was opened with Apple. Problem first seen on Catalina. Went away in Big Sur.

Story #2

The local support team told us:



“Edit bays are freezing under heavy workloads. How do we uninstall Crowdstrike?”

What the user actually said:



“Our team works on Avid remotely. The connection dies randomly. When it comes back, the Mac looks like it rebooted. We use Adobe applications and PathFinder. Our files are on Xsan volumes. Sometimes we see high CPU activity for Crowdstrike. Oh yeah, and these crashes have been happening randomly for about a year now.”

Root Cause Analysis:



Certain kinds of Xsan requests were crashing macOS. This issue was resolved in macOS Ventura 13.3.

(Issue fixed by Apple)

A third Tale of Misery and Woe

The local support team told us:



“We need to roll
back to Mojave,
A.S.A.P.”

What the user actually said:



Worldwide licensing upgraded half the Macs to Big Sur as required, but now when we copy files to the server, they randomly lock us out. Other people on our team can see them just fine. We have to reconnect to the server to copy more files. This didn't happen on Mojave. We need help!

Root Cause Analysis:



"Finder increases parallel processing in Big Sur. When starved for SMB2 credits, file server operations may stall or behave unexpectedly. Credit limit should be raised from 128 to 256. Windows Server 2012R2 and later offer 256 credits."

(NBCU Storage team addressed the issue)

Root Cause Analysis:



Wireshark

Deep network analysis tool

Hundreds of protocols

Linux, Windows, Mac (Universal)

Free & Open Source

The NBCUniversal logo is positioned on the left side of the slide. It consists of two grey vertical bars followed by three orange vertical bars, all of equal height and width, spaced evenly.

The Solution

ITS-LOG!

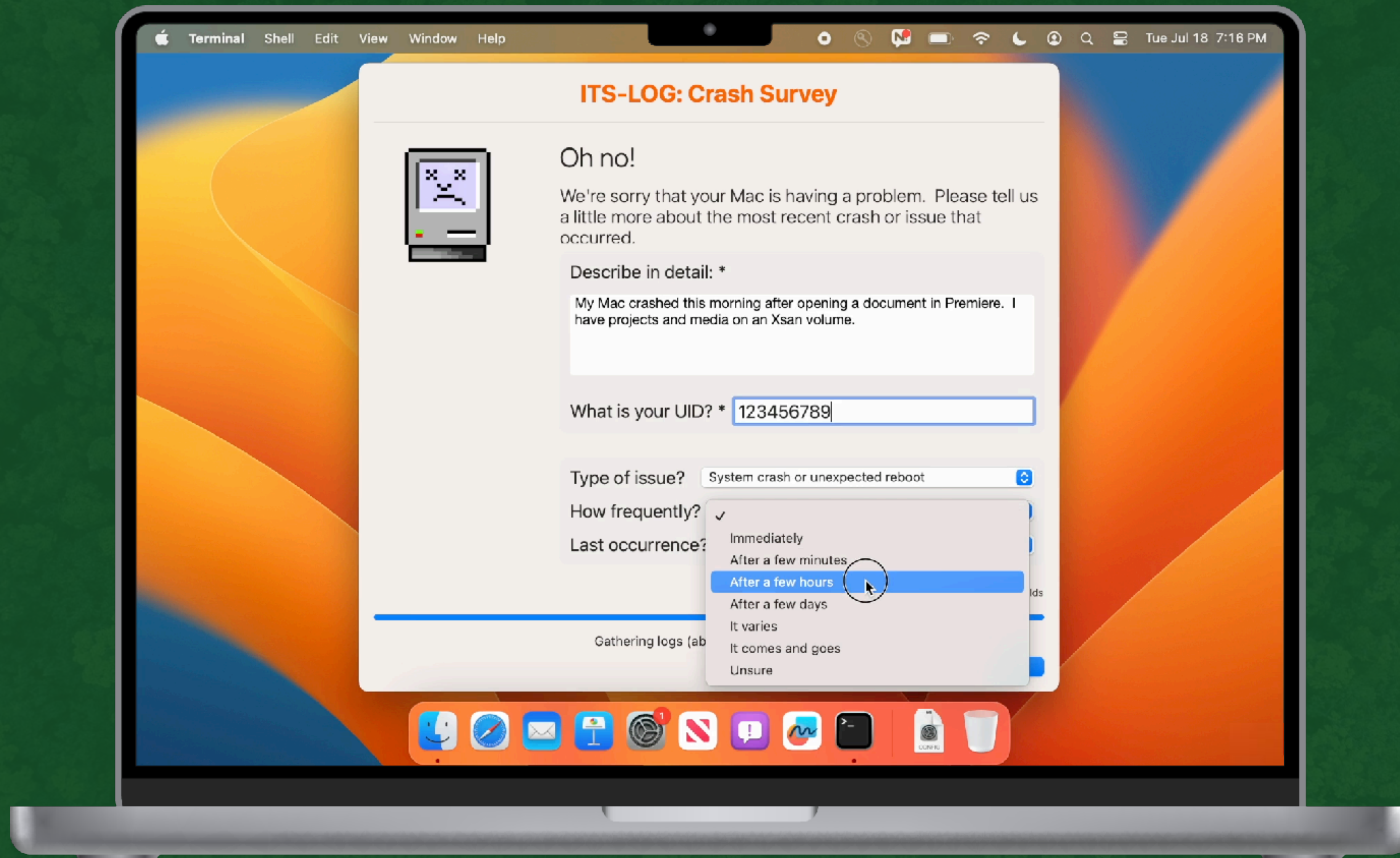
ALL ADMINS
LOVE LOGS!



IT'S BETTER
THAN BASH.
IT'S GOOD!

Use only as directed. Each sold separately. Batteries not included. Not responsible for back injuries.

PREVIEW



some sequences have been shortened

ITS-LOG!

- ★ Designed for end users
- ★ Collects diagnostic logs in background
- ★ Requests additional info about incident
- ★ Uploads system logs to cloud storage
- ★ Sends you a notification when done
- ★ Contains responses, download link to logs
- ★ Intented for serious crashes, repeatable bugs
- ★ Set appropriate expectations for use



ITS-LOG — III: THE SOLUTION

SYSDIAGNOSE

'sɪs,dɪəg'nɒʊs

What's a sysdiagnose?

- ★ A compressed archive
- ★ Collection of logs from most Mac services
- ★ Includes realtime performance snapshot
- ★ Historical power and performance data
- ★ Copy of MacOS unified log archive
- ★ Copy of System Profiler report
- ★ Much much more...

What's in a sysdiagnose?

<ul style="list-style-type: none">> Accessibility<ul style="list-style-type: none">acdiagnose-503.txtairport_info.txtapfs_stats.txtapplessdstats.txtapsd-status.txt> ASPSnapshots<ul style="list-style-type: none">bc_stats.txtbless_info.txtBluetoothTraceFile.pklgbootstamps.txtbputil.txt> brctl<ul style="list-style-type: none">ckksctl_status.txtcodectl.txtcom.apple.windowserver.displays.plist> crashes_and_spins<ul style="list-style-type: none">csrutil-status.txtDiskMountConditioner.jsondisks.txtdiskutil_apfs_listUsers.txtdiskutil_apfs.txtdiskutil_cs.txtdiskutil_info.txtdiskutil_list.txtdiskutil_listClients.txtdiskutil_listSnapshot.txtdisplay_diagnose.txtefi-dump-logs.txterror_log.txt> errors<ul style="list-style-type: none">filecoordination.txtfileproviderctl_check.logfileproviderctl_dump.logfileproviderctl.logfind-system-migration-history.txtfootprint.txtgpt.txthdiutil-pmap.txthidutil.plist	<ul style="list-style-type: none">hpmDiagnose.txtiogdiagnose.txt> ioreg<ul style="list-style-type: none">kextstat.txtkmutil-diagnose.txtlaunchctl-dumpstate.txtlaunchctl-list-0.txtlaunchctl-list-503.txtlaunchctl-print-gui-503.txtlaunchctl-print-system.txtlaunchctl-print-user-503.txtlaunchctl-procinfo-7195-Self Service.txt> libtrace✓ logs<ul style="list-style-type: none">> asl> BatteryBDC> BatteryHealth> BatteryUIPlist> CalendarPreferencescom.apple.SocialLayer.plist> DCP> DiagnosticMessages> EndpointSecurity> FDR> fsckinstall.logInstallHistory.plist> IntlDataCacheionodecache.json> iSCPreboot> launchd> loginwindow> MemoryExceptions> MobileActivation> MobileInstallation> MobileSoftwareUpdate> olddsc> parsecd> powerlogs> psm	<ul style="list-style-type: none">SFRRestoreVersion.plist> SiriAnalytics> Splat> suggest_toolsystem.logsystem.log.0.gz> SystemExp✓ systemstats<ul style="list-style-type: none">✓ db<ul style="list-style-type: none">...many files> SystemVersion> UserManagementlsappinfo.txtlsregister-0.csstoredumplsregister-503.csstoredump> mddiagnose.mdsdiagnostic> microstackshotsmount.txtnclist.txt> network-infonfsstat.txtnight-shift.lognvram.txtodutil.txtoslog_archive_error.logotctl_status.txtpcsstatus.txt> Personalizationpluginkit-503.txtpmset_everything.txtpowermetrics.txt> Preferencesps_thread.txtps.txtREADME.txtremotectl_dumpstate.txtresolv.conf> RunningBoardsample-389-highcpu.txtsample-662-highcpu.txt	<ul style="list-style-type: none">sample-1443-highcpu.txtsample-7195.txtsecurebootvariables.txtsecurity-sysdiagnose.txtsfltool.LSSharedFileList.FavoriteItems.txtsfltool.LSSharedFileList.FavoriteVolumes.txtsfltool.LSSharedFileList.iCloudItems.txtsmcDiagnose.txtspindump.txtstackshot.kcdata> summariessw_vers.txtswcutil_show.txtsysctl.txtsysdiagnose.logsystem_logs.logarchive> SystemConfigurationsystemextensionsctl_diagnose.txt> SystemProfilertailspin-info.txttailspin-trace.tailspintalagent-503.txttaskinfo.txttaskSummary.csvtbtDiagnose.txtthermal.txt> TimezoneDBtop.txttransparency.loguptime.txtvar_run_resolv.confvm_stat.txt✓ WiFi<ul style="list-style-type: none">> CoreCapture> WiFiWindowServer.external.winfo.plistxartutil.txtzprint.txt
--	---	---	---

"Apple needs some information..."

Sysdiagnoses can be generated:

- ★ with a keyboard combo
- ★ `/usr/bin/sysdiagnose`
- ★ via Feedback Assistant
- ★ via Enterprise Data Collector (EDC)
(used mostly by AppleCare)



(screen flashes briefly...)

Critical Information

- Who: About the affected Mac and the user
- What: Description of crash or issue, including steps
- When: Issue timestamp; frequency; reproducibility
- Where: The range of affected users and devices
- Why: Describe the impact this is having

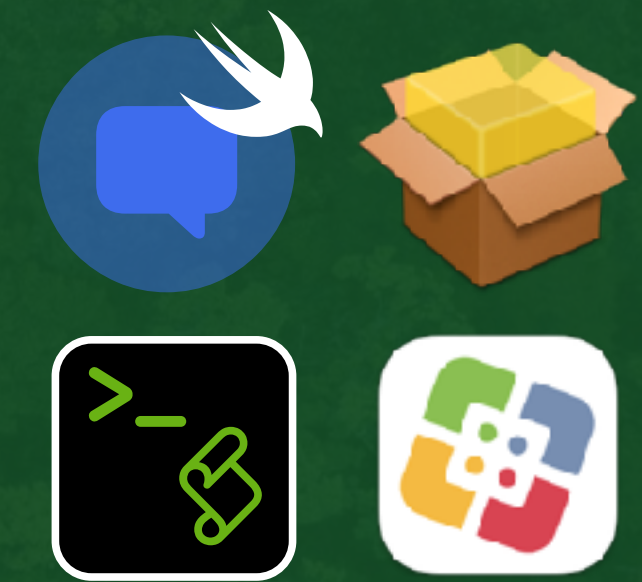
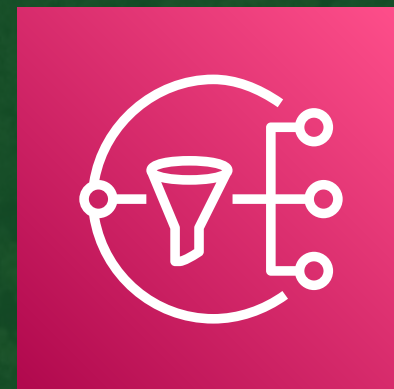
Big file. Bigger problem.

- ★ Time to compile: ~5 minutes
- ★ Average file size = **400 MB**
- ★ How do end-users transmit a very large file reliably?
- ★ How do you capture the user's story in the moment?

The NBCUniversal logo is positioned on the left side of the slide. It consists of a grey vertical bar followed by four orange vertical bars of equal height, all set against a dark grey background with a hexagonal pattern.

Let's Build it

ITS-LOG Components & Build Order:



1. Email
2. SNS
3. S3 Bucket
4. Lambda (λ) function

5. IAM policy
6. IAM user & access keys
7. swiftDialog
8. Mac script & assets

Flow: Mac to AWS



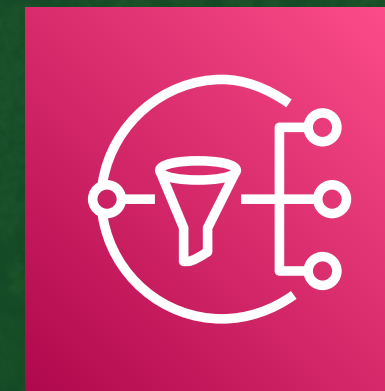
Flow: AWS to You



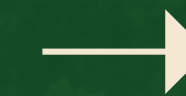
S3



Lambda



SNS

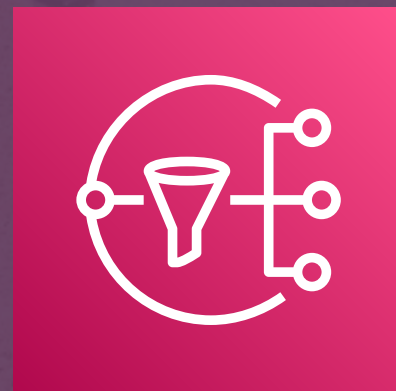


Email






Email

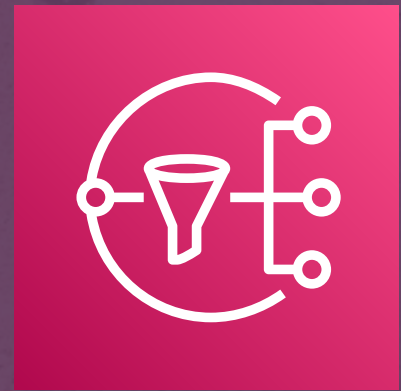
- ★ Any email address will do
- ★ One-time confirmation required to use SNS
- ★ Allow sender: **@sns.amazonaws.com**



SNS

- ★ Simple Notification Service
- ★ Publish-Subscribe (pub/sub) messaging
- ★ Messages are published to topics in SNS
- ★ SNS sends the messages to Subscribers
- ★ Topic cannot be renamed once created
- ★ SNS is region-specific. Check first!

[Option+S]					Oregon ▲
US East (N. Virginia)		us-east-1			
US East (Ohio)		us-east-2			
US West (N. California)		us-west-1			
US West (Oregon)		us-west-2			



SNS

- ★ Type: **Standard**
- ★ Name: As you wish.
- ★ Description: optional; however...
- ★ Email will use this as the “From” display name.

● Standard

- Best-effort message ordering
- At-least once message delivery
- Highest throughput in publishes/second
- Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints



SNS

- ★ Encryption: none (optional)
- ★ Access policy: **Basic**
 - ★ Publishers: topic owner
 - ★ Subscribers: topic owner
- ★ Use defaults for other settings
- ★ **Create Topic.**

▼ Access policy - *optional*

This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic. [Info](#)

Choose method

☒ **Basic**

Use simple criteria to define a basic access policy

☐ **Advanced**

Use a JSON object to define an advanced access policy.

Define who can publish messages to the topic

☒ **Only the topic owner**

Only the owner of the topic can publish to the topic

☐ **Everyone**

Anybody can publish

☐ **Only the specified AWS accounts**

Only the specified AWS account IDs can publish to the topic

Define who can subscribe to this topic

☒ **Only the topic owner**

Only the owner of the topic can subscribe to the topic

☐ **Everyone**

Any AWS account can subscribe to the topic

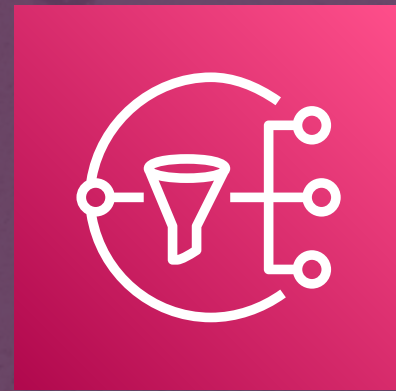
☐ **Only the specified AWS accounts**

Only the specified AWS account IDs can subscribe to the topic

☐ **Only requesters with certain endpoints**

JSON preview

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid":
        "__default_statement_ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "SNS:Publish",
        "SNS:RemovePermission",
        "SNS:SetTopicAttributes",
        "SNS>DeleteTopic",
```

SNS

- ★ Encryption: none (optional)
- ★ Access policy: **Basic**
 - ★ Publishers: topic owner
 - ★ Subscribers: topic owner
- ★ Use defaults for other settings
- ★ **Create Topic.**

▼ Access policy - optional

► Data protection policy - optional [Info](#)
This policy defines which sensitive data to monitor and to prevent from being exchanged via your topic.

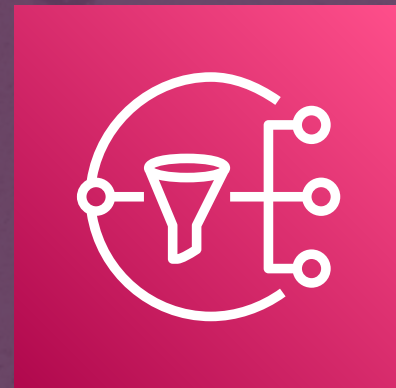
► Delivery policy (HTTP/S) - optional [Info](#)
The policy defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. To modify the default settings, expand this section.

► Delivery status logging - optional [Info](#)
These settings configure the logging of message delivery status to CloudWatch Logs.

► Tags - optional
A tag is a metadata label that you can assign to an Amazon SNS topic. Each tag consists of a key and an optional value. You can use tags to search and filter your topics and track your costs. [Learn more](#) [🔗](#)

► Active tracing - optional [Info](#)
Use AWS X-Ray active tracing for this topic to view its traces and service map in Amazon CloudWatch. Additional costs apply.

Cancel [Create topic](#)



SNS

★ Click “Create Subscription”

Amazon SNS > Topics > sysdiag-alerts

sysdiag-alerts

[Edit](#)[Delete](#)[Publish message](#)

Details

Name

sysdiag-alerts

Display name

-

ARN

arn:aws:sns:us-east-1:607456343589:sysdiag-alerts

Topic owner

607456343589

Type

Standard



Subscriptions

[Access policy](#)

[Data protection policy](#)

[Delivery policy \(HTTP/S\)](#)

[Delivery](#)



Subscriptions (2)

[Edit](#)[Delete](#)[Request confirmation](#)[Confirm subscription](#)[Create subscription](#)

Search

< 1 >



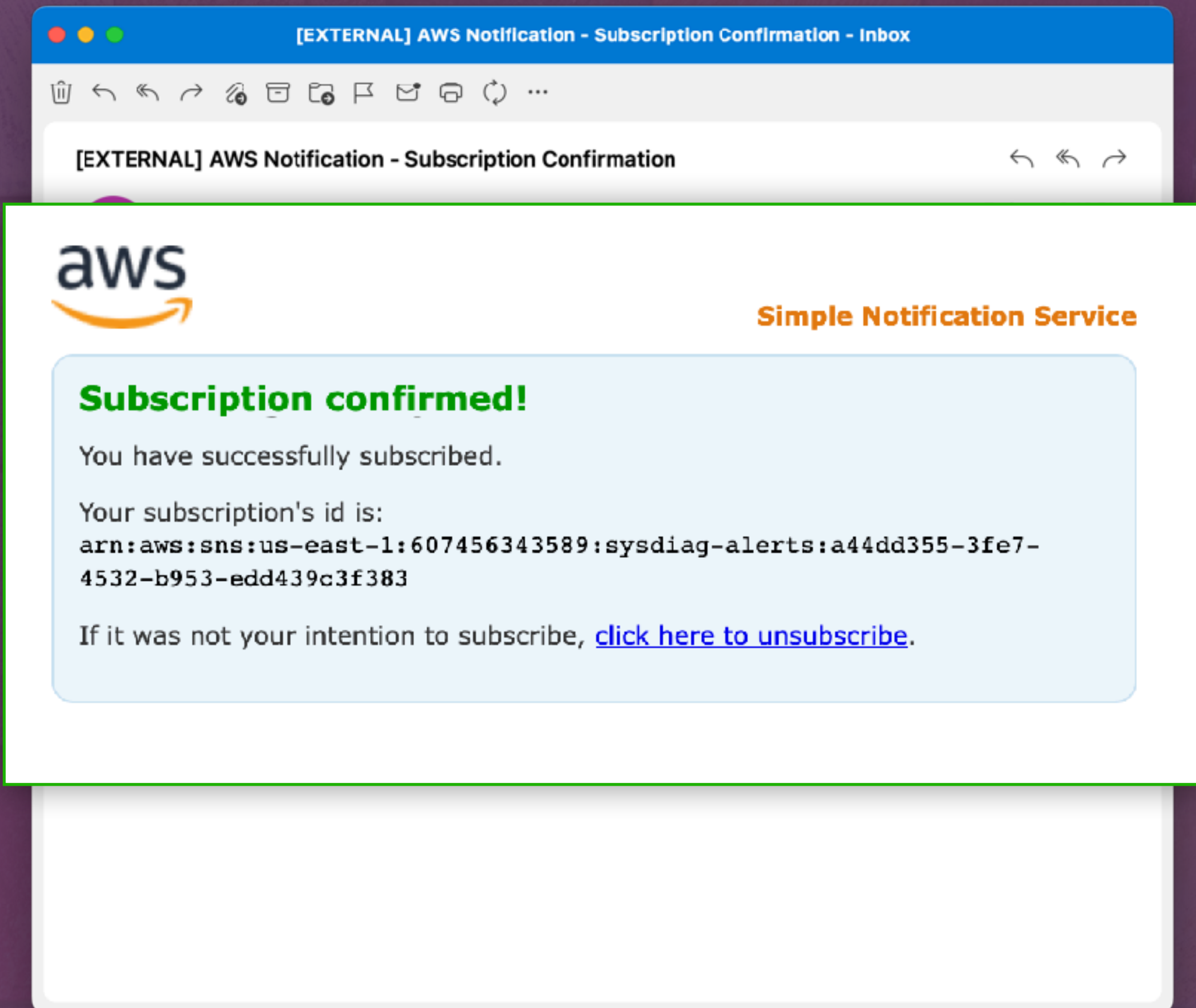
	ID ▲	Endpoint ▼	Status ▼	Protocol ▼
<input type="radio"/>	7987a328-924c-4...	[REDACTED]	✔ Confirmed	EMAIL
<input type="radio"/>	a44dd355-3fe7-45...	Johnny.appleseed...	✔ Confirmed	EMAIL

< 1 >



SNS

- ★ Enter Topic ARN (auto-populates)
- ★ Protocol: Email
- ★ Enter your email address
- ★ Create Subscription
- ★ Go check your inbox
- ★ **Check your spam folders!**





S3: Bucket

- ★ Choose globally unique bucket name (*it's always DNS*)
- ★ Choose region (check costs)
- ★ Ownership: ACLs disabled
- ★ Block all public access (default)
- ★ No Versioning, Tags
- ★ Default encryption

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

myawsbucket

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

AWS Region

US East (N. Virginia) us-east-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket



S3: Bucket

- ★ Choose globally unique bucket name (*it's always DNS*)
- ★ Choose region (check costs)
- ★ Ownership: ACLs disabled
- ★ Block all public access (default)
- ★ No Versioning, Tags
- ★ Default encryption

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

itslog-blammo-002 [Info](#)

Objects

Properties

Permissions

Metrics

Management

Bucket overview

AWS Region

US East (Ohio) us-east-2

Amazon Resource Name (ARN)

 arn:aws:s3:::itslog-blammo-002

Only the bucket settings in the following configuration are copied.

Choose bucket



S3: Lifecycle Rules

- ★ Find bucket tab: **Management**
- ★ Create Lifecycle Rule
- ★ Limit scope using filters
- ★ Filter Type: Prefix
 - ★ Rule: **itslog/***

itslog-delete-logs-7days

Lifecycle rule configuration

Lifecycle rule name	Prefix
itslog-delete-logs-7days	itslog/logs/
Status	Object tags
✔ Enabled	-
Scope	
Filtered	



S3: Lifecycle Rules

- ★ Find bucket tab: **Management**
- ★ Create Lifecycle Rule
- ★ Limit scope using filters
- ★ Filter Type: Prefix
 - ★ Rule: **itslog/***

itslog-delete-logs-7days

Choose a rule scope

- ☒ Limit the scope of this rule using one or more filters
- ☐ Apply to all objects in the bucket

Filter type

You can filter objects by prefix, object tags, or object metadata.

Prefix

Add filter to limit the scope of this rule to a single prefix.

itslog/logs/*

Don't include the bucket name in the prefix. Using protocols. [Learn more](#)



S3: Lifecycle Rules

- ★ Actions to apply:
 - ★ Expire current versions
 - ★ Permanently delete noncurrent
- ★ Expire objects after **7** days
- ★ Permanently delete **1** day later

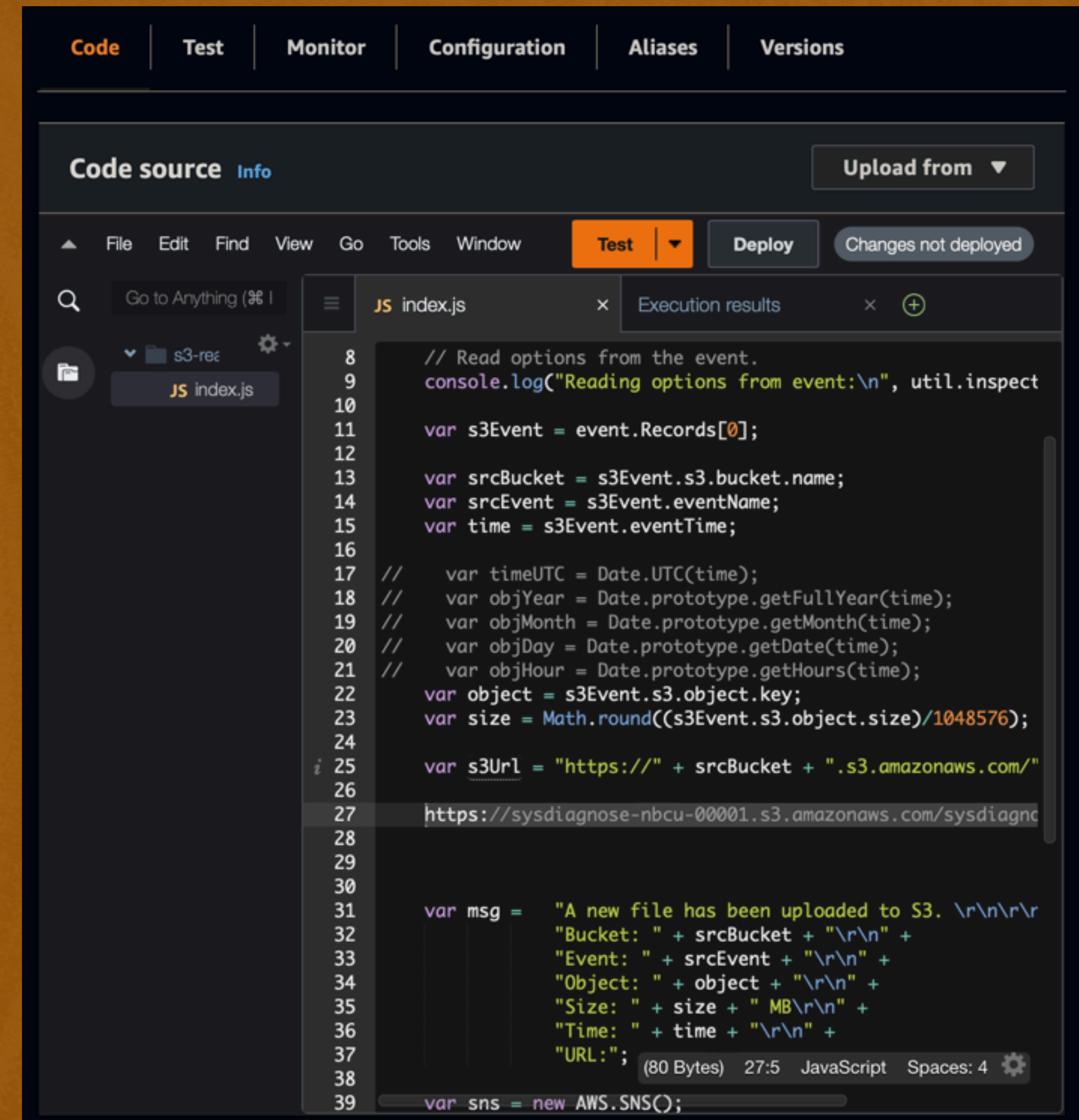
Lifecycle rule actions

Choose the actions you want this rule to perform. For more information, see [Lifecycle rule actions](#).

- ☐ Move current versions of objects between buckets
 - ☐ Move noncurrent versions of objects between buckets
 - ☒ Expire current versions of objects
 - ☒ Permanently delete noncurrent versions of objects
 - ☐ Delete expired object delete markers or noncurrent versions
- These actions are not supported when filtering on object size.



- ★ Serverless microcode
- ★ S3 events sent as raw JSON
- ★ This λ processes a text file
- ★ Sends email via SNS API
- ★ Basic code repository organizer

A screenshot of the AWS Lambda console's 'Code source' tab. The interface shows a file explorer on the left with a folder 's3-rec' containing a file 'index.js'. The main area displays the JavaScript code for 'index.js'. The code reads options from an event, extracts S3 event details (bucket, event name, time), calculates the file size in MB, and constructs an S3 URL. It then formats a message string with these details and initializes the AWS SNS client. The console includes tabs for 'Code', 'Test', 'Monitor', 'Configuration', 'Aliases', and 'Versions'. A 'Test' button is highlighted, and a 'Deploy' button is visible. The status bar at the bottom indicates '(80 Bytes) 27:5 JavaScript Spaces: 4'.



Function: Read Surveys

- ★ Create Function
- ★ “Author From Scratch”
- ★ Name: as you wish
- ★ Runtime/Arch: **Node.js 16.x**, x86_64
- ★ Create role from policy templates:
 - ★ S3 object read-only permissions
 - ★ SNS publish policy
- ★ **Note: role creation takes ~30 sec.**

Lambda > Functions > Create function

Create function [Info](#)

Choose one of the following options to create your function.

Author from scratch



Start with a simple Hello World example.

Use a blueprint



Build a Lambda application from sample code and configuration presets for common use cases.



Function: Read Surveys

- ★ Create Function
- ★ “Author From Scratch”
- ★ Name: as you wish
- ★ Runtime/Arch: **Node.js 16.x**, x86_64
- ★ Create role from policy templates:
 - ★ S3 object read-only permissions
 - ★ SNS publish policy
- ★ **Note: role creation takes ~30 sec.**

Basic information

Function name

Enter a name that describes the purpose of your function

itslog-read-logs

Use only letters, numbers, hyphens, or underscores

Runtime [Info](#)

Choose the language to use to write your function

Node.js 16.x

Architecture [Info](#)

Choose the instruction set architecture you want

☒ x86_64

☐ arm64



Function: Read Surveys

- ★ Create Function
- ★ “Author From Scratch”
- ★ Name: as you wish
- ★ Runtime/Arch: **Node.js 16.x**, x86_64
- ★ Create role from policy templates:
 - ★ S3 object read-only permissions
 - ★ SNS publish policy
- ★ **Note: role creation takes ~30 sec.**

Basic information

▼ Change default execution role

Execution role

Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).

- ☐ Create a new role with basic Lambda permissions
- ☐ Use an existing role
- ☒ Create a new role from AWS policy templates

i Role creation might take a few minutes.
Please do not delete the role or edit the trust or permissions policies in this role.

Role name

Enter a name for your new role.

itslog-lambda-s3-readonly

☐ arm64



Function: Read Surveys

- ★ Create Function
- ★ “Author From Scratch”
- ★ Name: as you wish
- ★ Runtime/Arch: **Node.js 16.x**, x86_64
- ★ Create role from policy templates:
 - ★ S3 object read-only permissions
 - ★ SNS publish policy
- ★ **Note: role creation takes ~30 sec.**

A screenshot of the AWS IAM console showing the 'Basic information' tab for a new role. The 'Policy templates - optional' section is active, displaying a list of policy templates. Two templates are selected: 'Amazon S3 object read-only permissions' and 'Amazon SNS publish policy'. A 'Refresh' button is visible below the list. The 'arm64' architecture option is selected at the bottom.

Basic information

Policy templates - *optional* [Info](#)
Choose one or more policy templates.

Amazon S3 object read-only permissions X
S3

Amazon SNS publish policy X
SNS

☒ arm64



Function: Read Surveys

★ Add Trigger...

itslog-get-surveys

▼ Function overview [Info](#)



itslog-get-surveys



Layers

(0)


+ Add trigger



Function: Read Surveys

- ★ Service: **S3**; select bucket
- ★ Event: all object create events
- ★ Prefix: **itslog/surveys/**
- ★ Suffix: **.txt**
- ★ **Recursion warning...**
- ★ Lambda will auto-add necessary permissions for S3 -> Lambda

Trigger configuration [Info](#)

 **S3**
aws storage

Bucket

Please select the S3 bucket that serves as the event source. The bucket must exist in the same region as the Lambda function.

Bucket region: us-east-1

Event types

Select the events that you want to have trigger the Lambda function. However, for each bucket, individual events cannot have multiple configurations that match the same object key.

All object create events



Function: Read Surveys

- ★ Service: **S3**; select bucket
- ★ Event: all object create events
- ★ Prefix: **itslog/surveys/**
- ★ Suffix: **.txt**
- ★ **Recursion warning...**
- ★ Lambda will auto-add necessary permissions for S3 -> Lambda

Trigger configuration [Info](#)

Event types

Select the events that you want to have trigger the Lambda function. However, for each bucket, individual events cannot have multiple event types that match the same object key.

All object create events ✕

Prefix - *optional*

Enter a single optional prefix to limit the notifications to objects with the specified prefix.

Suffix - *optional*

Enter a single optional suffix to limit the notifications to objects with the specified suffix.



Function: Read Surveys

- ★ Service: **S3**; select bucket
- ★ Event: all object create events
- ★ Prefix: **itslog/surveys/**
- ★ Suffix: **.txt**
- ★ **Recursion warning...**
- ★ Lambda will auto-add necessary permissions for S3 -> Lambda

Trigger configuration [Info](#)

Event types

Recursive invocation

If your function writes objects to an S3 bucket, ensure that you are not using the same bucket for both the function and the bucket. Using the same bucket increases the risk of creating a recursive invocation, which can cause your function to call itself repeatedly.

- ☒ I acknowledge that using the same S3 bucket for both the function and the bucket is not recommended and that this configuration can cause recursive invocation, which can cause Lambda usage, and increased costs.

Lambda will add the necessary permissions for AWS S3 to the function's execution role. For more information about the Lambda permissions model, see [AWS Lambda permissions model](#).

Enter a single optional suffix to limit the notifications to objects with the specified suffix.

.txt



Function: Read Surveys

- ★ Replace “hello world”
- ★ Insert arn: from SNS
- ★ Edit email body
- ★ Edit email subject
- ★ Lambda publishes directly to SNS via internal API call

```
1 // Sources:
2 // https://stackoverflow.com/questions/30651502/how-to-get-contents-of-a-text-file
3 // https://stackoverflow.com/questions/38831829/nodejs-aws-sdk-s3-generate-presign
4 // The trigger for this function is the S3 bucket
5 // Event type: s3:ObjectCreated:*
6 // Prefix: itslog/surveys/
7
8 var snsTopicARN = "arn:aws:sns:us-west-2:095367[REDACTED]:nbcu-itslog-sns";
9 var util = require('util')
10 var AWS = require('aws-sdk');
11 var s3 = new AWS.S3();
12
13 exports.handler = function(event, context, callback) {
14
15     // Use the event passed from S3 to Lambda to retrieve
16     // the parameters necessary to run this function.
17
18     var s3Event = event.Records[0];
19     var srcBucket = s3Event.s3.bucket.name;
20     var srcRegion = s3Event.s3.bucket.awsRegion;
21     var srcEvent = s3Event.eventName;
22     var srcTime = s3Event.eventTime;
23     var srcKey = s3Event.s3.object.key;
24
25     // Obtain the key for the sysdiagnose file using the survey file key.
26     // NOTE: filenames differ by their prefix (path) and suffix (extension).
27     // Modify at your own risk.
28
29     var sysdiagnoseObject = srcKey.replace("surveys", "logs");
30     var sysdiagnoseObject = sysdiagnoseObject.replace(".txt", ".tar.gz");
31     var signedUrlValidSeconds = 86400*7;
32     var signedUrlValidDays = Math.round(signedUrlValidSeconds / 86400);
```




Function: Read Surveys

- ★ Replace “hello world”
- ★ Insert arn: from SNS
- ★ Edit email body
- ★ Edit email subject
- ★ Lambda publishes directly to SNS via internal API call

```
1 // Sources:
2
3 // Event type: s3:ObjectCreated:*
4 // Prefix: itslog/surveys/
5
6
7
8 var snsTopicARN = "arn:aws:sns:us-west-2:123456789012:itslog-sns";
9 var util = require('util');
10 var AWS = require('aws-sdk');
11 var s3 = new AWS.S3();
12
13 exports.handler = function(event, context, callback) {
14
15
16
17     var s3Event = event.Records[0];
18     var srcBucket = s3Event.s3.bucket.name;
19     var srcRegion = s3Event.s3.bucket.awsRegion;
20     var srcEvent = s3Event.eventName;
21     var srcTime = s3Event.eventTime;
22     var srcKey = s3Event.s3.object.key;
23
24
25     // Obtain the key for the sysdiagnose file using the survey file key.
26     // NOTE: filenames differ by their prefix (path) and suffix (extension).
27     // Modify at your own risk.
28
29     var sysdiagnoseObject = srcKey.replace("surveys", "logs");
30     var sysdiagnoseObject = sysdiagnoseObject.replace(".txt", ".tar.gz");
31     var signedUrlValidSeconds = 86400*7;
32     var signedUrlValidDays = Math.round(signedUrlValidSeconds / 86400);
```




Function: Read Surveys

- ★ Replace “hello world”
- ★ Insert arn: from SNS
- ★ Edit email body
- ★ Edit email subject
- ★ Lambda publishes directly to SNS via internal API call

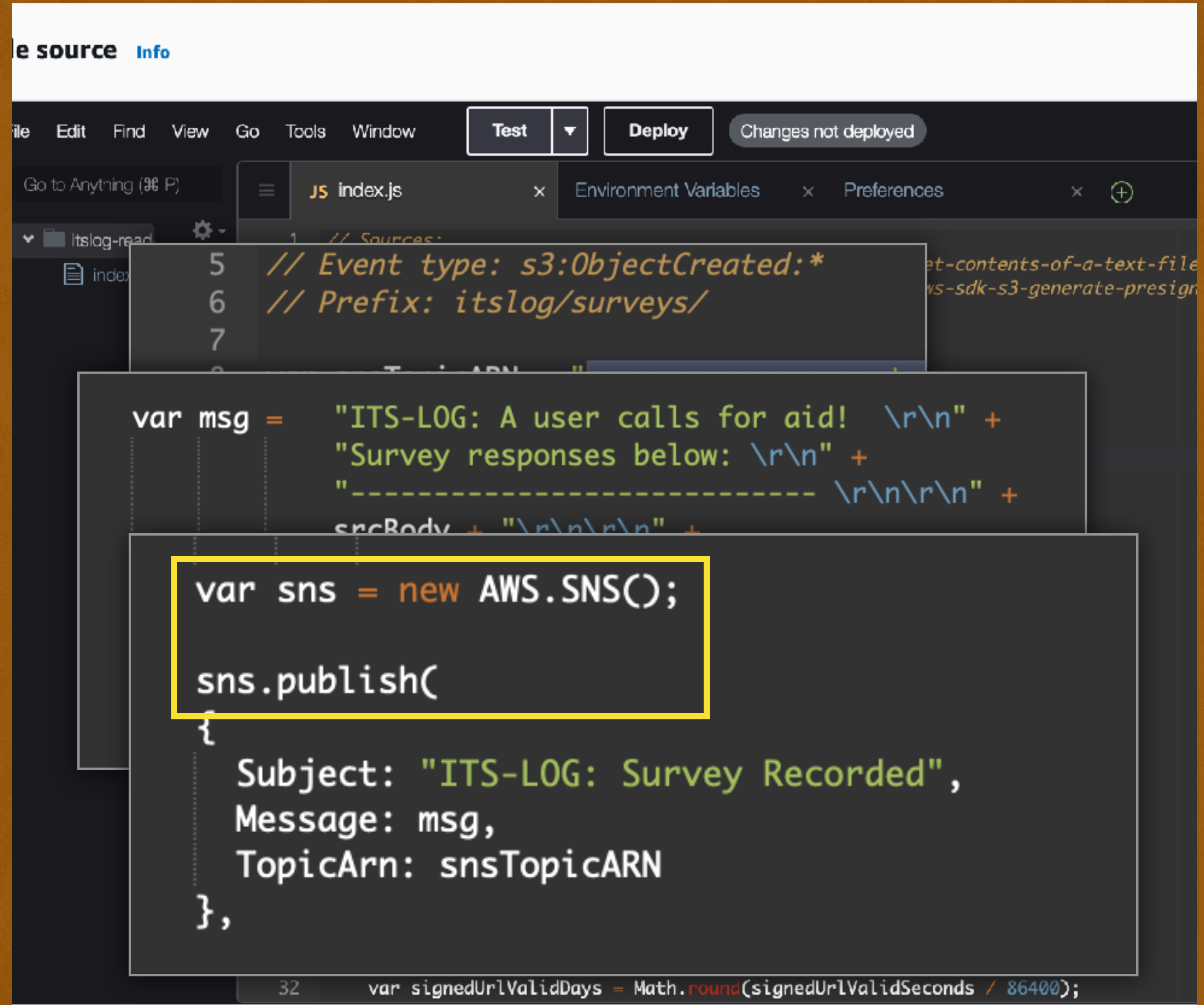
```
1 // Sources:
2
3 // Event type: s3:ObjectCreated:*
4 // Prefix: itslog/surveys/
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23 var msg = "ITS-LOG: A user calls for aid! \r\n" +
24           "Survey responses below: \r\n" +
25           "----- \r\n\r\n" +
26           srcBody + "\r\n\r\n" +
27           "DOWNLOAD SYSDIAGNOSE FILE NOW. Link expires " +
28           signedUrlValidDays + " day(s) after time sent " +
29           signedUrl + "\r\n\r\n" +
30           "S3 Bucket : " + srcBucket + "\r\n" +
31           "File (key): " + srcKey + "\r\n";
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612

```




Function: Read Surveys

- ★ Replace “hello world”
- ★ Insert arn: from SNS
- ★ Edit email body
- ★ Edit email subject
- ★ Lambda publishes directly to SNS via internal API call



```
1 // Sources:
2 // Event type: s3:ObjectCreated:*
3 // Prefix: itslog/surveys/
4
5 // ...
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612
2613
2614
2615
2616
2617
2618
2619
2620
2621
2622
2623
2624
2625
2626
2627
262
```




Function: Read Surveys

- ★ File > Save your code.
- ★ **NOTE:** function is not live until you click **Deploy**!

```
Go Tools Window Test Deploy Changes not deployed
JS index.js Environment Variables Preferences
1 // Sources:
2 // https://stackoverflow.com/questions/30651502/how-to-get-contents-of-a-te
3 // https://stackoverflow.com/questions/38831829/nodejs-aws-sdk-s3-generate-
4 // The trigger for this function is the S3 bucket
5 // Event type: s3:ObjectCreated:*
6 // Prefix: itslog/surveys/
7
8 var snsTopicARN = "arn:aws:sns:us-west-2:095367123456:nbcu-itslog-sns";
9 var util = require('util')
10 var AWS = require('aws-sdk');
11 var s3 = new AWS.S3();
12
13 exports.handler = function(event, context, callback) {
14
15     // Use the event passed from S3 to Lambda to retrieve
16     // the parameters necessary to run this function.
17
18     var s3Event = event.Records[0];
19     var srcBucket = s3Event.s3.bucket.name;
20     var srcRegion = s3Event.s3.bucket.awsRegion;
21     var srcEvent = s3Event.eventName;
22     var srcTime = s3Event.eventTime;
23     var srcKey = s3Event.s3.object.key;
24
```



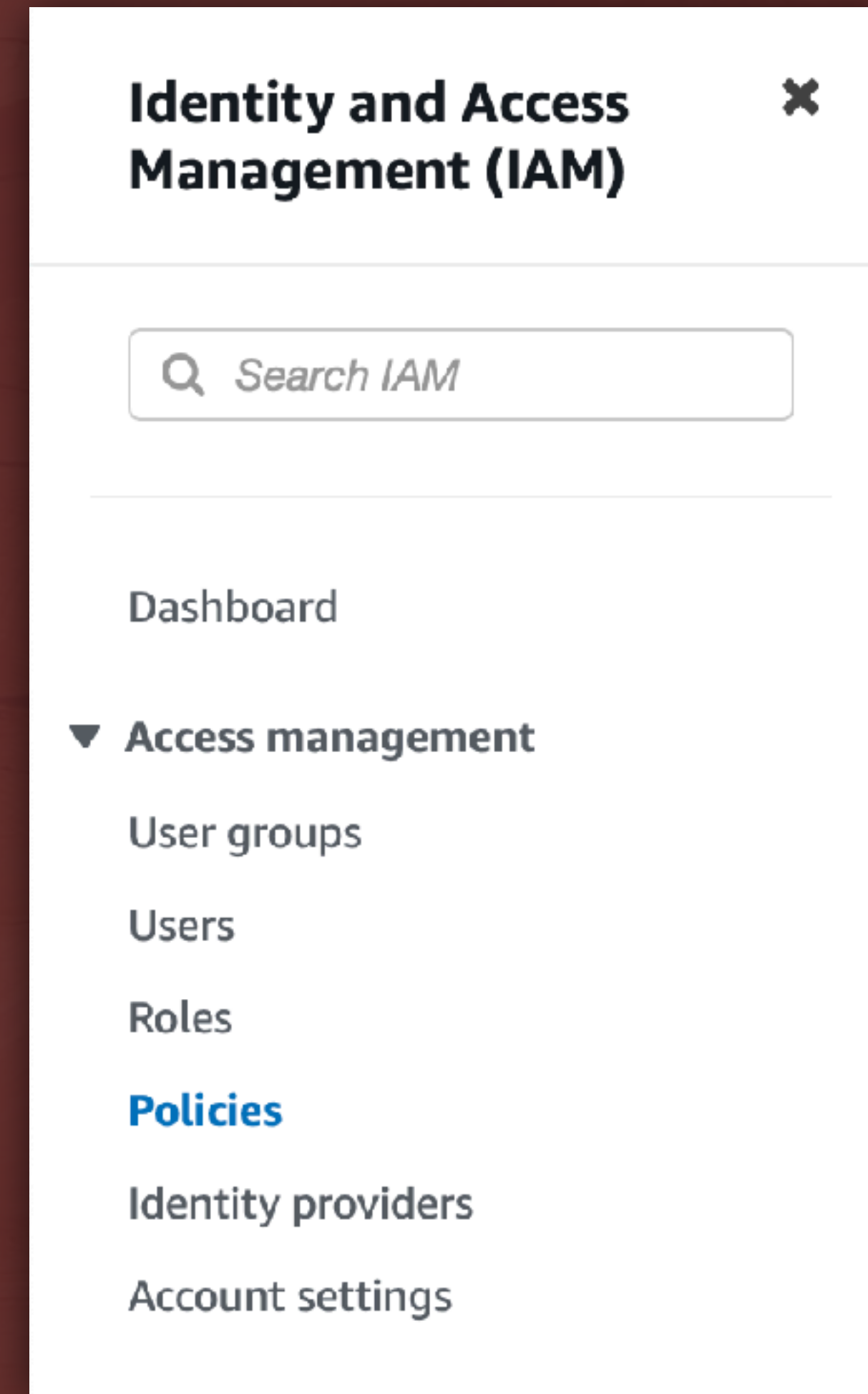

IAM Policy

- ★ Policies define user access rights to services
- ★ Managed vs. Inline policies
 - ★ AWS Managed: predefined by Amazon
 - ★ Customer Managed: attachable to many users
 - ★ Customer Inline: applies to only one user.



IAM Policy

- ★ **Customer Managed Policy:**
- ★ IAM dashboard > “Policies”
- ★ Create Policy
- ★ Use the Visual Editor
- ★ Search for “S3”
- ★ Click “S3”





IAM Policy

- ★ Customer Managed Policy:
- ★ IAM dashboard > “Policies”
- ★ Create Policy
- ★ Use the Visual Editor
- ★ Search for “S3”
- ★ Click “S3”

Identity and Access Management (IAM) ✕

Policy editor

VisualJSONActions ▼

▼ Select a service
Specify what actions can be performed on specific resources in a service.

Q s3 ✕

Popular services

Glacier ⓘ

S3 ⓘ

S3 Object Lambda ⓘ

S3 Outposts ⓘ

+ Add more permissions


CancelNext

Identity providers

Account settings



IAM Policy

- ★ Actions Allowed:
- ★ Search for “PutObject”
- ★  Write: PutObject

Policy editor

VisualJSONActions

▼ S3

Allow0 Actions

Specify what actions can be performed on specific resources in S3.

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Switch to deny permissions

Manual actions | Add actions

☐ All S3 actions (s3:*)

Access level

Expand all | Collapse all

► List (10)

► Read (53)

► Write (42)

► Permissions management (15)

► Tagging (10)

► Resources

Specify resource ARNs for these actions.

► Request conditions - optional

Actions on resources are allowed or denied only when these conditions are met.

+ Add more permissions

CancelNext

NBCUniversal

2023 MACADMINS
CONFERENCE



IAM Policy

- ★ Resource: specific, add ARN
 - ★ Bucket name: **bucket/prefix**
 - ★ Object name: *****
- ★ Click **Add ARNs**.
- ★ Click **Next**.

Specify ARNs

Visual

Resource bucket name

☐ Any bucket name

itslog-blammo-002/itslog

Resource object name

☒ Any object name

*

ARN

☐ Any resource

itslog-blammo-002/itslog/*

arn:aws:s3:::itslog-blammo-002/itslog/*

Cancel

Add ARNs



IAM Policy

- ★ Enter policy name and description.
- ★ Review defined permissions.
- ★ Click **Create Policy**.

Policy details

Policy name

Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and '+=,.,@-_' characters.

Description - *optional*

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=,.,@-_' characters.

[Cancel](#)

[Previous](#)

[Create policy](#)



IAM Policy

Raw Policy Statement

- ★ Effect: **Allow**
- ★ Actions:
 - ★ **s3:PutObject**
- ★ Resource:
 - ★ **arn:aws:s3:::bucket/prefix/***

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::itslog-blammo-002/itslog/*"
    }
  ]
}
```




IAM User

- ★ IAM Dashboard > Users
- ★ Click **[Add User]**.
- ★ Enter a user name.
- ★ **NO** access to AWS console
- ★ Click **[Next]**

User details

User name

itslog-s3-writeonly

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

- ☐ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

i If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user.
[Learn more](#)

Cancel

Next



IAM User

- ★ Attach policies directly
- ★ Search for IAM policy (itslog...)
- ★ No boundary (unless req'd)

- **Attach policies directly**
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1122)

Choose one or more policies to attach to your new user.



Create policy [↗](#)

itslog



Filter by Type

All types ▼

1 match

< 1 >



Policy name [↗](#)



Type ▼

Atta... ▼



itslog-s3-writeonly

Customer mana...

0



IAM User

- ★ Select newly-minted user
- ★ ‘Security Credentials’ tab.
- ★ **Create** access key.
- ★ *Review Amazon’s Access Key “Best Practices & Alternatives”*
- ★ **App running outside AWS**
- ★ Click Next.

Access keys (1)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

Create access key

AKIAY23ZYG

Actions ▼

Description

Upload-only account for writing an object to the S3 bucket.

Status

✓ Active

Last used

9 hours ago

Created

16 days ago

Last used region

us-east-1

Last used service

s3



IAM User

- ★ Select newly-minted user
- ★ ‘Security Credentials’ tab.
- ★ **Create** access key.
- ★ *Review Amazon’s Access Key “Best Practices & Alternatives”*
- ★ **App running outside AWS**
- ★ Click Next.

☐ Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

☒ Application running outside AWS
You plan to use this access key to enable an application running on an on-premises host, or to use a local AWS client or third-party AWS plugin.

☐ Other
Your use case is not listed here.

It's okay to use an access key for this use case, but follow the best practices:

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access keys when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [Best practices for managing AWS access keys](#).

Cancel **Next**



IAM User

- ★ Secret key is only shown **once!**
- ★ No, seriously...
- ★ ...you won't see it again.
- ★ Save the credentials in a .CSV

✓ Success!

You successfully created the users shown below.
You can view and download user security credentials...

This is the last time these credentials will be available to download. However, you can create new credentials at any time.




IAM User

- ★ Secret key is only shown **once!**
- ★ No, seriously...
- ★ ...you won't see it again.
- ★ Save the credentials in a .CSV

✓ **Success!**

You successfully created the users shown below.

Access key ID	Secret access key
AKIA23ZYGYSEMUKQSI 	***** Show



Download .csv



IAM User

- ★ Secret key is only shown **once!**
- ★ No, seriously...
- ★ ...you won't see it again.
- ★ Save the credentials in a .CSV
- ★ **“Keep it secret. Keep it safe.”**





IAM User

- ★ Even with write-only permissions...
- ★ Please at least minimally encode your access keys.
- ★ Avoids being flagged by DLP and basic security audits
- ★ The script expects **base64**.
- ★ Modify if additional security is required.
- ★ Encoding: `echo "AKIA..." | base64`
- ★ Decoding: `echo "QUtJ..." | base64 -D`



IAM User

- ★ Access keys do not expire.
- ★ They are not a username and password.
- ★ If you lose either half, you must create a new pair.
- ★ Maximum two (2) access keys per IAM user.



IAM User

- ★ Destroying access/secret keys:
 - ★ Deactivate key
 - ★ Enter AK to confirm
 - ★ Delete key

Delete AKIARMNCSYN ×

Delete access key **AKIARMNCSYN**? You can't use an inactive key to make AWS API calls but you can activate it again later.

Access key last used
9 hours ago

IAM user
sysdiagnose-collector-writeonly

Account
[REDACTED]

You must deactivate the access key before you can delete it. We recommend analyzing the impact of deactivating the access key before permanently deleting it.

Deactivate

To confirm deletion, enter the access key ID in the text input field.

AKIARMNCSYN [REDACTED]

Cancel **Delete**



IAM User

- ★ We need one more thing...
- ★ Go to IAM Dashboard > Users
- ★ Select the IAM User
- ★ Copy the ARN
- ★ Return to the S3 bucket

IAM > Users > itslog-s3-writeonly

itslog-s3-writeonly [Info](#)

Delete

Summary

ARN

 `arn:aws:iam::328271117716:user/itslog-s3-writeonly`

Console access

Disabled

Access key 1

AKIAUY3T3XWKJFKJODEF - Active

 Used 5 hours ago. Yesterday old.

Created

July 17, 2023, 21:25 (UTC-04:00)

Last console sign-in

-

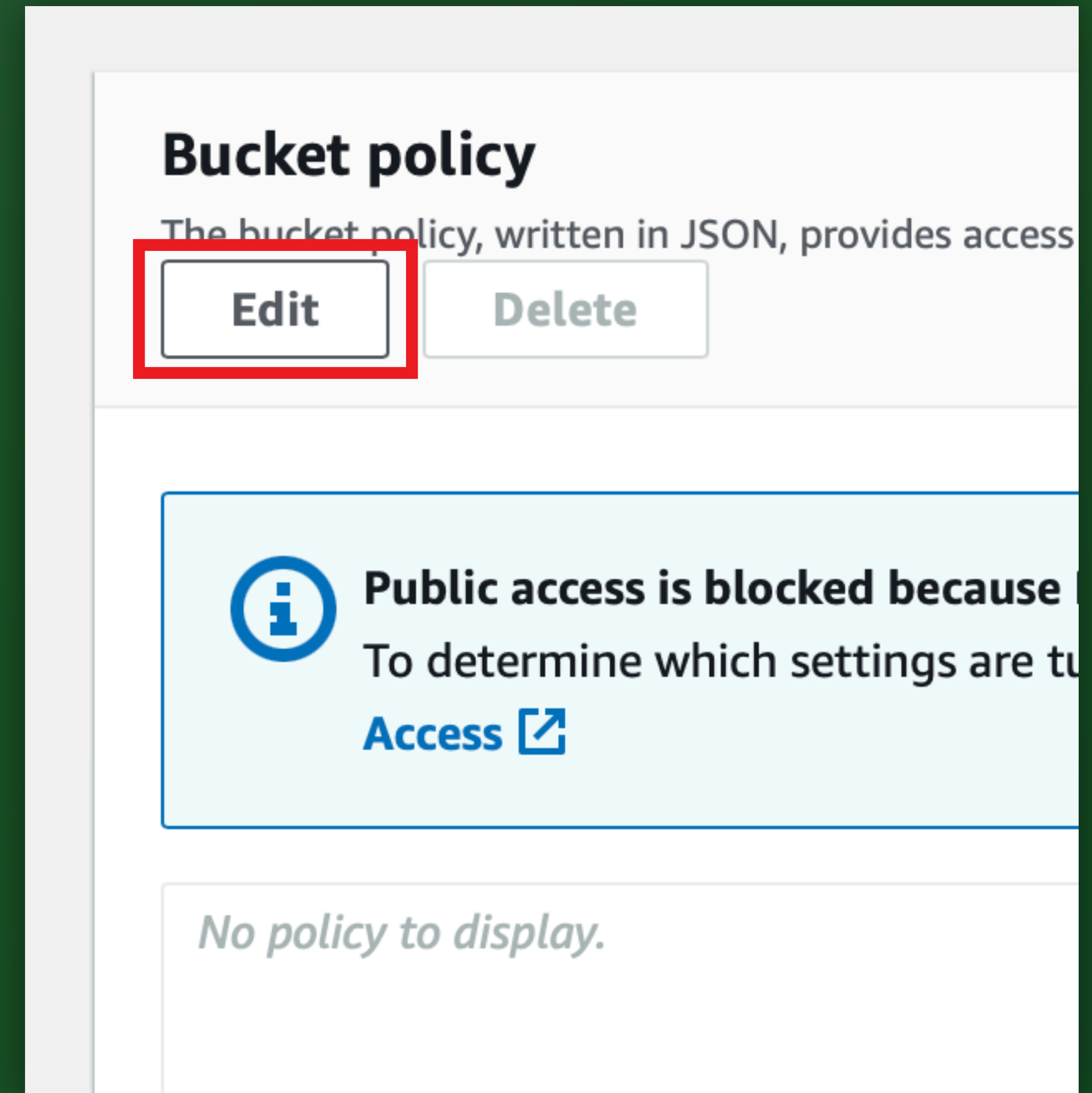
Access key 2

Not enabled



S3: Bucket Policy

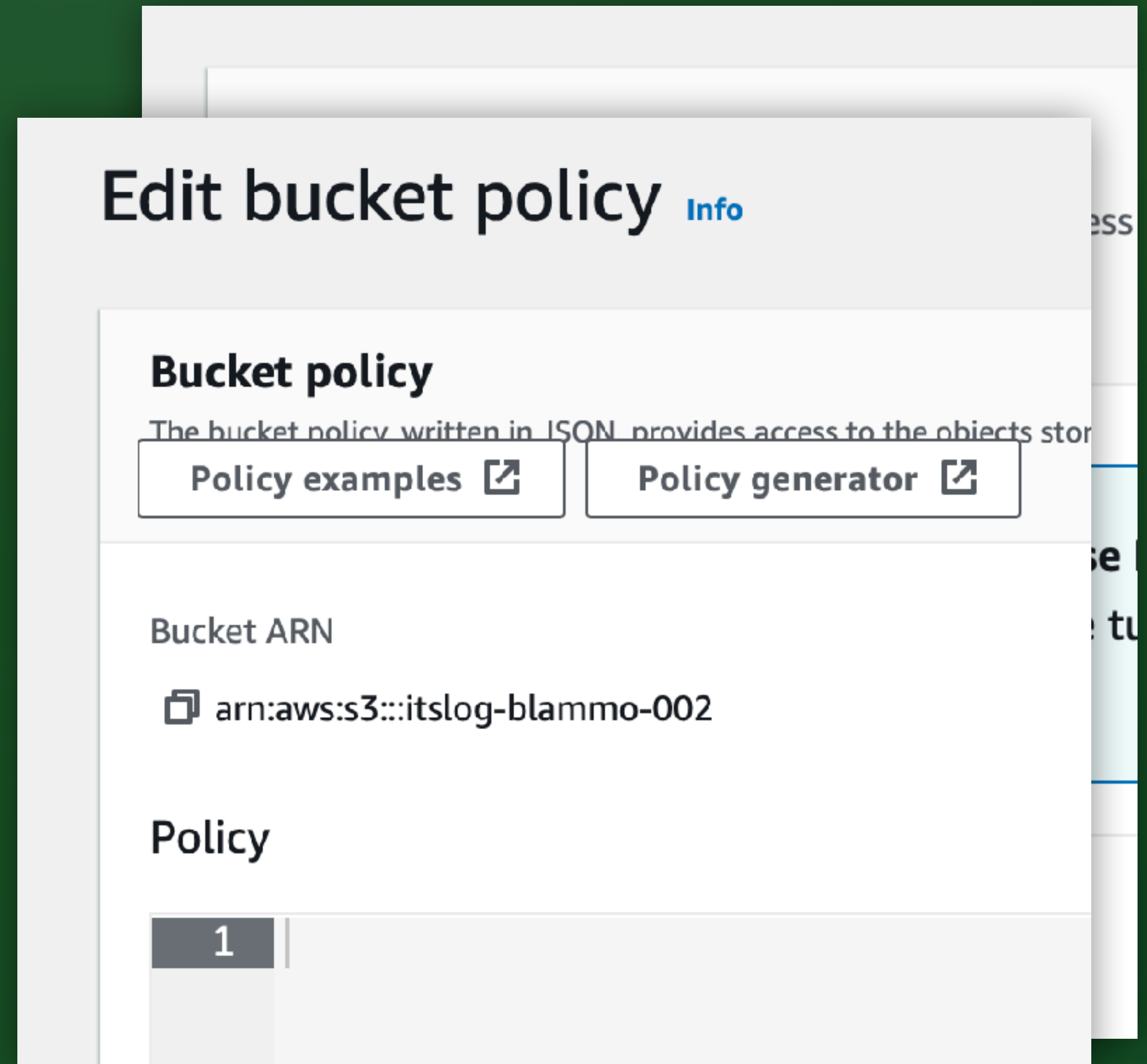
- ★ Go to Permissions tab
- ★ Under Bucket Policy, click Edit.
- ★ Click [Policy Generator].
- ★ Prepare for a time warp to **2010...**





S3: Bucket Policy

- ★ Go to Permissions tab
- ★ Under Bucket Policy, click Edit.
- ★ Click [Policy Generator].
- ★ Prepare for a time warp to **2010...**



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to [Amazon Web Services \(AWS\)](#) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), an [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

Effect ☒ Allow ☐ Deny

Principal

Use a comma to separate multiple values.

AWS Service Amazon S3

Use multiple statements to add permissions for more than one service.

☐ All Services





S3: Policy Generator

Effect ☒ Allow ☐ Deny

Principal

Use a comma to separate multiple values.

AWS Service

☐ All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions

☐ All Actions ('*')

Amazon Resource Name (ARN)

ARN should follow the following format: `arn:aws:s3:::${BucketName}/${KeyName}`.
Use a comma to separate multiple values.

[Add Conditions \(Optional\)](#)

Add Statement



S3: Policy Generator

- ★ Step 1: **S3 Bucket Policy**
- ★ Step 2: Statement...
- ★ Effect: Allow
- ★ Principal: **IAM User ARN**
- ★ Actions: PutObject
- ★ ARN: **arn:aws:s3:::
\${BucketName}/
\${KeyName}**
- ★ Click "Add Statement."

Effect	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Principal	<input type="text" value="arn:aws:iam::328271117"/> <small>Use a comma to separate multiple values</small>
Service	<input type="text" value="Amazon S3"/> <small>Use multiple statements to add permissions</small>
Actions	<input type="text" value="1 Action(s) Selected"/>
ARN	<input type="text" value="arn:aws:s3:::itslog-blam"/> <small>ARN should follow the following format Use a comma to separate multiple values</small>
Add Conditions (Optional)	
<input type="button" value="Add Statement"/>	



S3: Policy Generator

- ★ Policy summary appears.
- ★ Click "Generate Policy."
- ★ Policy JSON document appears.
- ★ Copy this to a text editor.
- ★ Return to 2023...

You added the following statements. Click the button below to Generate a policy

Principal(s)	Effect	Action
<ul style="list-style-type: none">arn:aws:iam::328271117716:user/itslog-s3-writeonly	Allow	<ul style="list-style-type: none">s3

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a cor

Generate Policy

Start Over



S3: Policy Generator

- ★ Policy summary appears.
- ★ Click "Generate Policy."
- ★ Policy JSON document appears.
- ★ Copy this to a text editor.
- ★ Return to 2023...

Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected** in the policy generator

```
{
  "Id": "Policy1689651133904",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1689650510201",
      "Action": [
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::itslog-blammo-002"
```




S3: Bucket Policy

- ★ Back in the bucket policy...
- ★ Paste JSON from Generator
- ★ Click “Save Changes.”

Policy

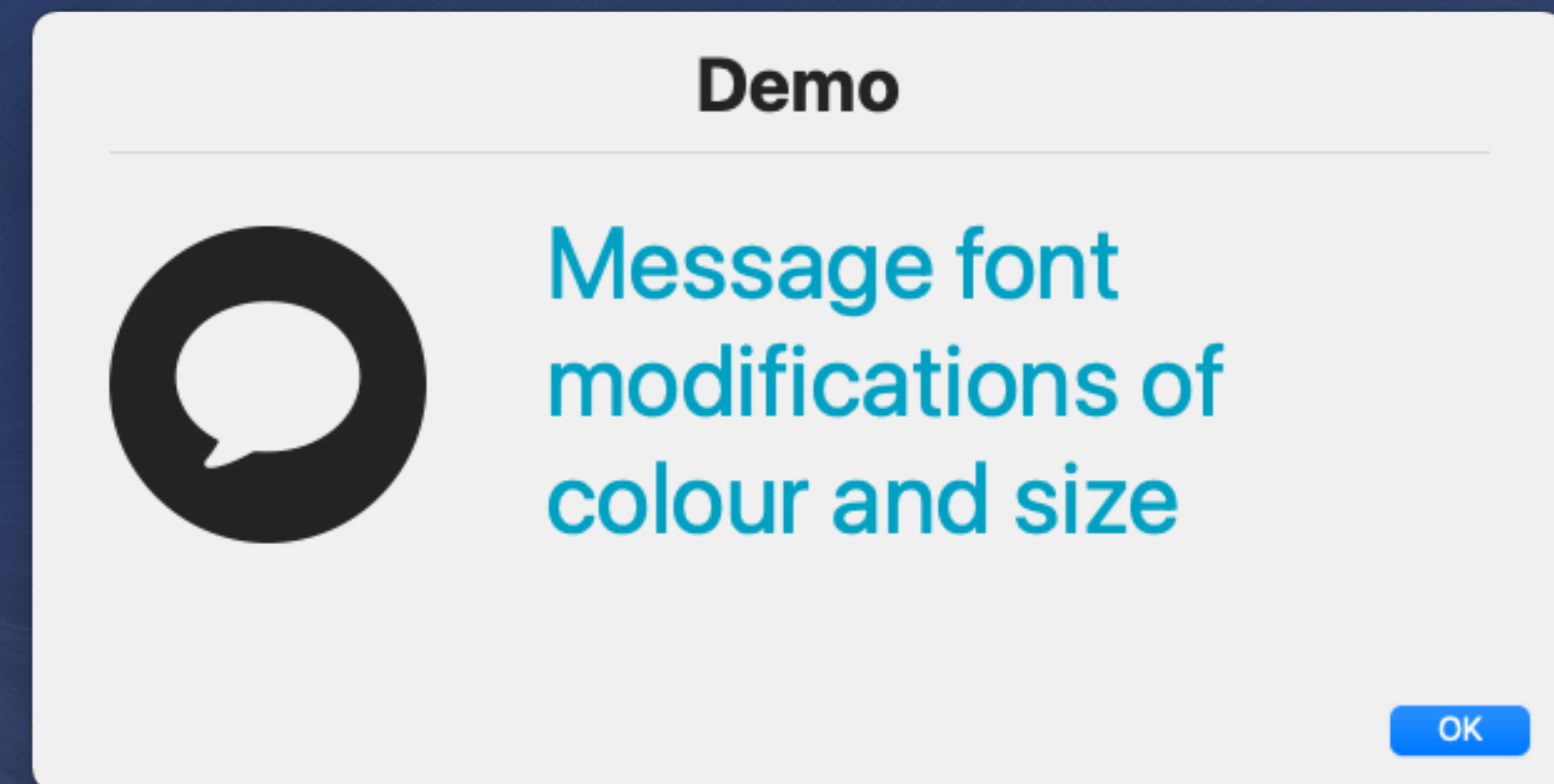
```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Principal": {
7          "AWS": "arn:aws:iam::328271117716:user/itslog-s3-writeonly"
8        },
9        "Action": "s3:PutObject",
10       "Resource": "arn:aws:s3:::itslog-blammo-002/*"
11      }
12    ]
13  }
```

Cancel Save changes



swiftDialog

- ★ A new app for end-user interactions
- ★ Update window live while running
- ★ Capture form outputs in shell script
- ★ Can replace cocoaDialog, Pashua, jamfHelper, many others...
- ★ **100% Swift (macOS 11+)**
- ★ github.com/bartreardon/
- ★ Extensive wiki & community projects





Script

- ★ Only bash, curl, and built-ins
- ★ no aws-cli or python
- ★ AWS v4 security policy

```
154  
155  
156 #  
157 ##### STAGE 2: SYSDBGNOSE COLLECTION  
158 #  
159  
160 generateSysdiagnose() {  
161  
162     /usr/bin/sysdiagnose -b -n -u -Q -P -G -f /var/tmp -A "$sysDiagArchive" | cat &  
163  
164     swd_echo "progress: Gathering logs (about 3-5 minutes) ..."  
165  
166     sleep 1  
167  
168     while [[ -n $(pgrep "sysdiagnose_helper") ]]  
169     do  
170         # Keep checking until the sysdiagnose utility has finished. "Sysdiagnose is still  
171         # running..."  
172  
173         # If user finishes the survey before curl or sysdiagnose are completed...  
174         # Launch the mini window to keep them informed.  
175  
176         if [[ -z $(ps -ax $swd_survey_PID | tail +2) && $mini_window_launched == false ]]  
177         then  
178             launch_mini_window  
179             swd_echo "progress: Gathering logs (about 3-5 minutes) ..."  
180         fi  
181  
182         sleep 1  
183     done  
184  
185     /usr/bin/tar -czf "$sysDiagTarball" "$sysDiagArchive/" &  
186     tarPID=$!  
187  
188     echo "PID of tar is $tarPID"  
189  
190     swd_echo "progress: Compressing logs and preparing to upload."  
191  
192     sleep 1  
193  
194     while [[ -n $(ps -ax $tarPID | tail +2) ]]  
195     do  
196         # echo "tar is still balling..."  
197  
198         # If user finishes the survey before curl or sysdiagnose are completed...  
199         # Launch the mini window to keep them informed.  
200  
201         if [[ -z $(ps -ax $swd_survey_PID | tail +2) && $mini_window_launched == false ]]  
202         then  
203             launch_mini_window  
204             swd_echo "progress: Compressing logs and preparing to upload."  
205         fi  
206  
207         sleep 1  
208     done  
209 }
```




Script

- ★ Only bash, curl, and built-ins
- ★ no aws-cli or python
- ★ AWS v4 security policy

```

43
44 # Create signature if not public upload.
45 key_and_sig_args=""
46 if [ "$aws_ak" != "" ] && [ "$aws_sk" != "" ]; then
47
48     # Need current and file upload expiration date. Handle GNU and BSD date command style to get tomorrow's date.
49     date='date -u +%Y-%m-%dT%H%M%S'
50     expdate='if ! date -v+1d +%Y-%m-%d 2>/dev/null; then date -d tomorrow +%Y-%m-%d; fi'
51     expdate_s=$(printf $expdate | sed s/-//g) # without dashes, as we need both formats below
52     service='s3'
53
54     # Generate policy and sign with secret key following AWS Signature version 4, below
55     p=$(cat <<POLICY | openssl base64
56 { "expiration": "${expdate}T12:00:00.000Z",
57   "conditions": [
58     { "acl": "$acl" },
59     { "bucket": "$bucket" },
60     [ "starts-with", "\$key", "" ],
61     [ "starts-with", "\$content-type", "" ],
62     [ "content-length-range", 1, $(ls -l -H "$srcfile" | awk '{print $5}' | head -1) ],
63     { "content-md5": "$md5" },
64     { "x-amz-date": "$date" },
65     { "x-amz-credential": "$aws_ak/$expdate_s/$region/$service/aws4_request" },
66     { "x-amz-algorithm": "AWS4-HMAC-SHA256" }
67   ]
68 }
69 POLICY
70 )
71
72 # AWS4-HMAC-SHA256 signature
73 s=$(printf "$expdate_s" | openssl sha256 -hmac "AWS4$aws_sk" -hex | sed 's/(stdin)= //'
74 s=$(printf "$region" | openssl sha256 -mac HMAC -macopt hexkey:"$s" -hex | sed 's/(stdin)= //'
75 s=$(printf "$service" | openssl sha256 -mac HMAC -macopt hexkey:"$s" -hex | sed 's/(stdin)= //'
76 s=$(printf "aws4_request" | openssl sha256 -mac HMAC -macopt hexkey:"$s" -hex | sed 's/(stdin)= //'
77 s=$(printf "$p" | openssl sha256 -mac HMAC -macopt hexkey:"$s" -hex | sed 's/(stdin)= //'
78
79 key_and_sig_args="-F X-Amz-Credential=$aws_ak/$expdate_s/$region/$service/aws4_request -F X-Amz-Algorithm=AWS4-
80 fi
81
82
198 # If user finishes the survey before curl or sysdiagnose are completed...
199 # Launch the mini window to keep them informed.
200
201 if [[ -z $(ps -ax $swd_survey_PID | tail +2) && $mini_window_launched == false ]]
202 then
203     launch_mini_window
204     swd_echo "progress.txt: Compressing logs and preparing to upload."
205 fi
206
207 sleep 1

```

Run Succeeded | Time 0:00:41 | Peak Memory 55.4M | launchSurveyWindow | Tabs: 4 | Line 138, Column 1



Script

- ★ Script takes six arguments:
- ★ \$1 \$2 \$3 = dummy values
- ★ \$4 = Access Key
- ★ \$5 = Secret Key
- ★ \$6 = bucket@region
- ★ Buckets may require this URL:
- ★ [https://\\${bucket}.s3.\\${region}.amazonaws.com/](https://${bucket}.s3.${region}.amazonaws.com/)

```

43
44 # Create signature if not public upload.
45 key_and_sig_args=""
46 if [ "$saws_ak" != "" ] && [ "$saws_sk" != "" ]; then
47
48     # Need current and file upload expiration date. Handle GNU and BSD date command style to get tomorrow's date.
49     date='date -u +%Y-%m-%dT%H%M%S'
50     expdate='if ! date -v+1d +%Y-%m-%d 2>/dev/null; then date -d tomorrow +%Y-%m-%d; fi'
51     expdate_s=$(printf $expdate | sed s/-//g) # without dashes, as we need both formats below
52     service='s3'
53
54     # Generate policy and sign with secret key following AWS Signature version 4, below
55     p=$(cat <<POLICY | openssl base64
56 { "expiration": "${expdate_s}T12:00:00.000Z",
57   "conditions": [
58     { "acl": "$acl" },
59     { "bucket": "$bucket" },
60     [ "starts-with", "\$key", "" ],
61     [ "starts-with", "\$content-type", "" ],
62     [ "content-length-range", 1, $(ls -l -H "$srcfile" | awk '{print $5}' | head -1) ],
63     { "content-md5": "$md5" },
64     { "x-amz-date": "$date" },
65     { "x-amz-credential": "$saws_ak/$expdate_s/$region/$service/aws4_request" },
66     { "x-amz-algorithm": "AWS4-HMAC-SHA256" }
67   ]
68 }
69 POLICY
70 )
71
72 # AWS4-HMAC-SHA256 signature
73 s=$(printf "$expdate_s" | openssl sha256 -hmac "AWS4$saws_sk" -hex | sed 's/(stdin)= //' )
74 s=$(printf "$region" | openssl sha256 -mac HMAC -macopt hexkey:"$s" -hex | sed 's/(stdin)= //' )
75 s=$(printf "$service" | openssl sha256 -mac HMAC -macopt hexkey:"$s" -hex | sed 's/(stdin)= //' )
76 s=$(printf "aws4_request" | openssl sha256 -mac HMAC -macopt hexkey:"$s" -hex | sed 's/(stdin)= //' )
77 s=$(printf "$p" | openssl sha256 -mac HMAC -macopt hexkey:"$s" -hex | sed 's/(stdin)= //' )
78
79 key_and_sig_args="-F X-Amz-Credential=$saws_ak/$expdate_s/$region/$service/aws4_request -F X-Amz-Algorithm=AWS4-
80 fi
81
82
198 # If user finishes the survey before curl or sysdiagnose are completed...
199 # Launch the mini window to keep them informed.
200
201 if [[ -z $(ps -ax $swd_survey_PID | tail +2) && $mini_window_launched == false ]]
202 then
203     launch_mini_window
204     swd_echo "progress.txt: Compressing logs and preparing to upload."
205 fi
206
207 sleep 1
208
Run Succeeded | Time 0:00:41 | Peak Memory 55.4M | launchSurveyWindow | Tabs: 4 | Line 138, Column 1

```




Script

- ★ Monitors progress of sysdiagnose, curl
- ★ Contains settings for swiftDialog
- ★ Insert additional logs into archive before sending
- ★ Displays a mini-window until finished uploading.



Assets

- ★ Application icon for ITS-LOG
- ★ Custom branding for swiftDialog
- ★ Optional sound effects :-)



Decision Tree



“ *Two roads diverged
in a yellow wood... ”*

—Robert Frost

“ *Two roads diverged
in a yellow wood...* ”

—Robert Frost



**Jamf
Self Service**



**Open Source
Tools**



Jamf Policy

General

- ★ Execution: Ongoing
- ★ Custom Trigger optional
- ★ **Self Service**
- ★ Upload an icon
- ★ Set relevant category

Computers : Policies

← ITS-LOG! Collector

Options Scope Self Service User Interaction

General

Display Name Display name for the policy

ITS-LOG! Collector

☒ Enabled

Site Site to add the policy to

None

Category Category to add the policy to

Self Help

Trigger Event(s) to use to initiate the policy

Packages 0 Packages

Software Updates Not Configured

Scripts 1 Script

Printers 0 Printers



Jamf Policy

General


- ★ Execution: Ongoing
- ★ Custom Trigger optional
- ★ **Self Service**
- ★ Upload an icon
- ★ Set relevant category

Computers : Policies

← ITS-LOG! Collector

Options Scope **Self Service** User Interaction

Icon Icon to display for the policy. It is recommended that you use a file with the GIF or PNG format.



log-button.png

Upload Icon

Select Existing Icon

Categories Categories in which to display or feature the policy in Self Service

☒ Include the policy in the Featured category



Jamf Policy

Script

- ★ \$4 : Access Key (base64)
- ★ \$5 : Secret Key (base64)
- ★ \$6 : bucket@region
- ★ \$7 : customer (optional)
- ★ Add script to policy

Settings : Computer management > Scripts

← itslog-collector.sh

General

Script

Options

Limitations

accesskey_base64

Parameter 5

secretkey_base64

Parameter 6

bucket@region

Parameter 7

customer



Open Source

Use when you have:

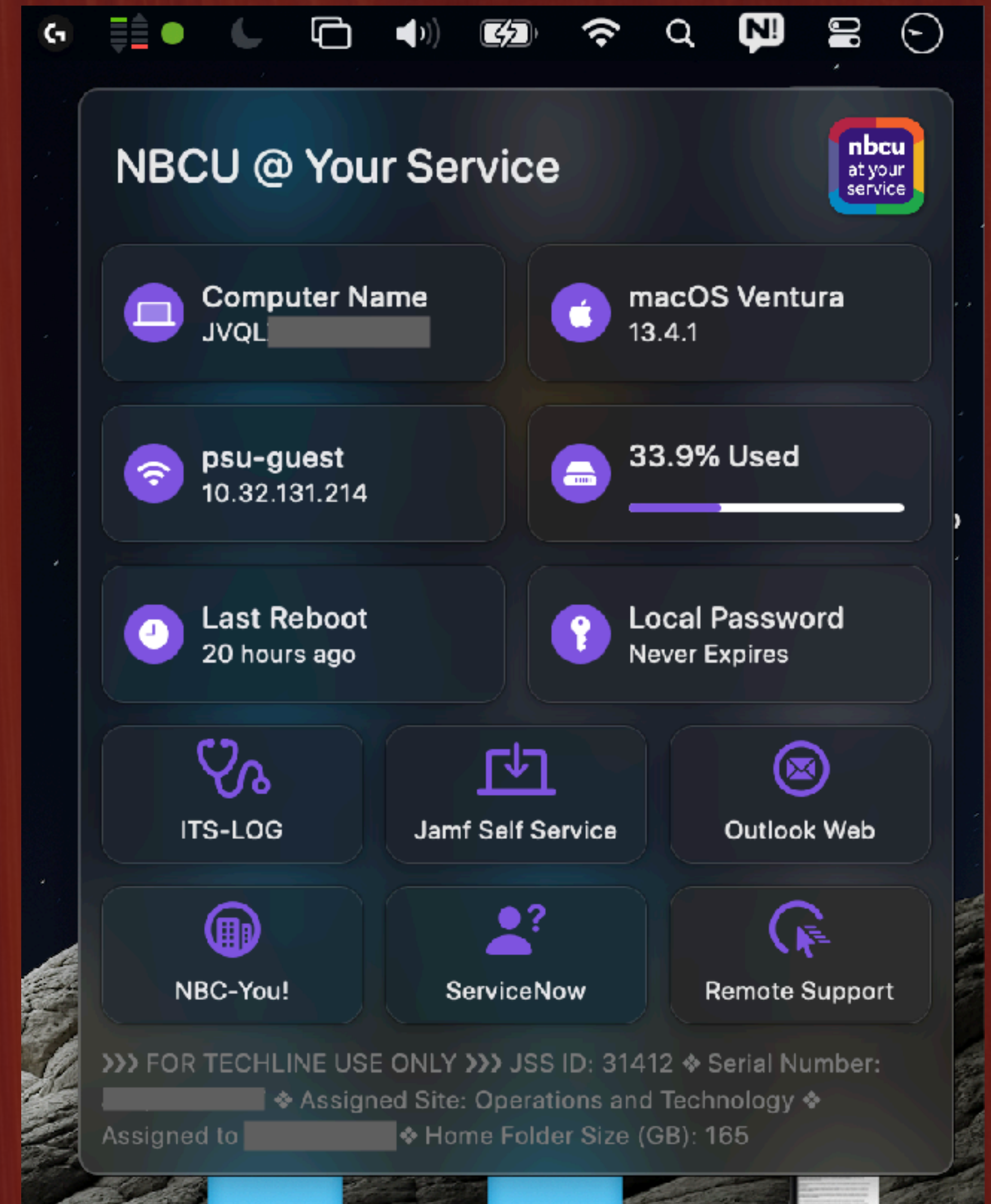
- ★ No software catalog app
- ★ MDM can't run arbitrary scripts
- ★ Boutique MSP deployments
- ★ Menu bar support tools





SupportApp

- ★ Menu bar support tool for end users
- ★ Loads of information at a glance
- ★ Buttons launch settings, websites, apps, scripts
- ★ SwiftUI, SF Symbols, custom branding
- ★ Settings deployed via configuration profile
- ★ Opt. Jamf custom schema, profile variables
- ★ **SupportHelper = elevated privileges**
- ★ Free @ github.com/root3nl



Root3 B.V., Hartweg, The Netherlands



Final Thoughts

ITS-LOG is flexible!

- ★ Customize and brand the user input form
- ★ Set custom filenames for sysdiagnose
- ★ Collect additional logs and add to archive
- ★ Add a 'customer' field to further organize logs

AppleCare for Enterprise

- ★ **ITS-LOG clears the escalation bottleneck**
- ★ Timely collection of user stories & data
- ★ Technical Contacts can open support cases
- ★ Access to Level 3 support engineers
- ★ Faster case turnaround

Learning from experience

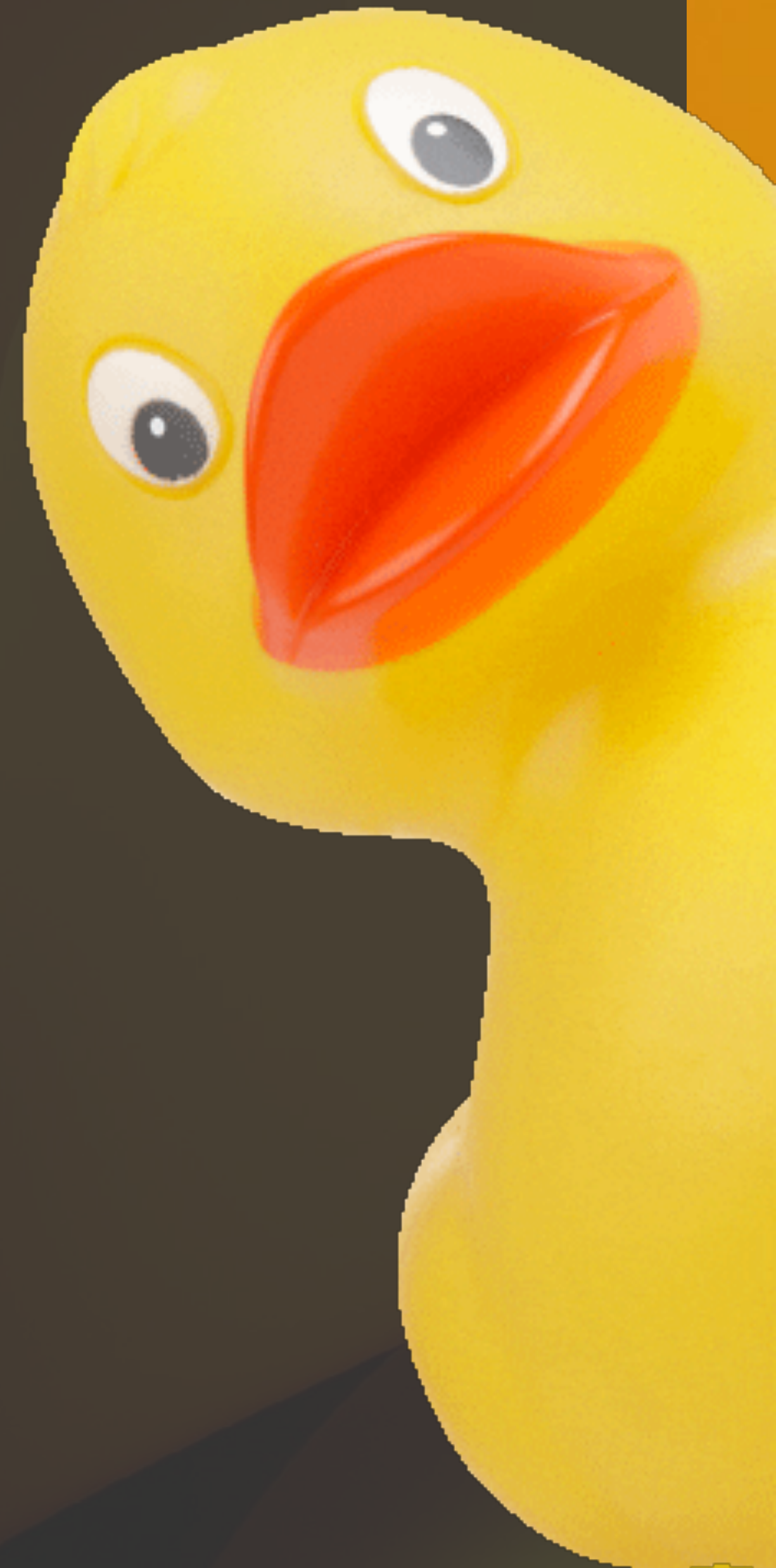
- ★ JNUC 2022 @ San Diego
- ★ Rehearsal went great...
- ★ Live build done with time to spare
- ★ The app failed to run properly.
- ★ Couldn't figure out what was wrong.
- ★ Played the safety pre-record instead.

Learning from experience

- ★ IAM policy incomplete, missing S3 bucket policy
- ★ Reviewed code, made improvements
- ★ Encountered a **fatal** issue with curl
- ★ Enabled **set -x** in script
- ★ “Talked” through problem (on Slack)
- ★ After many hours, I had a “Eureka!” moment
- ★ Stream of consciousness on Slack

Learning from experience

- ★ IAM policy incomplete, missing S3 bucket policy
- ★ Reviewed code, made improvements
- ★ Encountered a **fatal** issue with curl
- ★ Enabled **set -x** in script
- ★ “Talked” through problem (on Slack)
- ★ After many hours, I had a “Eureka!” moment
- ★ Stream of consciousness on Slack



Learning

- ★ IAM policy
- ★ Reviewed c
- ★ Encountere
- ★ Enabled **sc**
- ★ “Talked” th
- ★ After many
- ★ Start typing



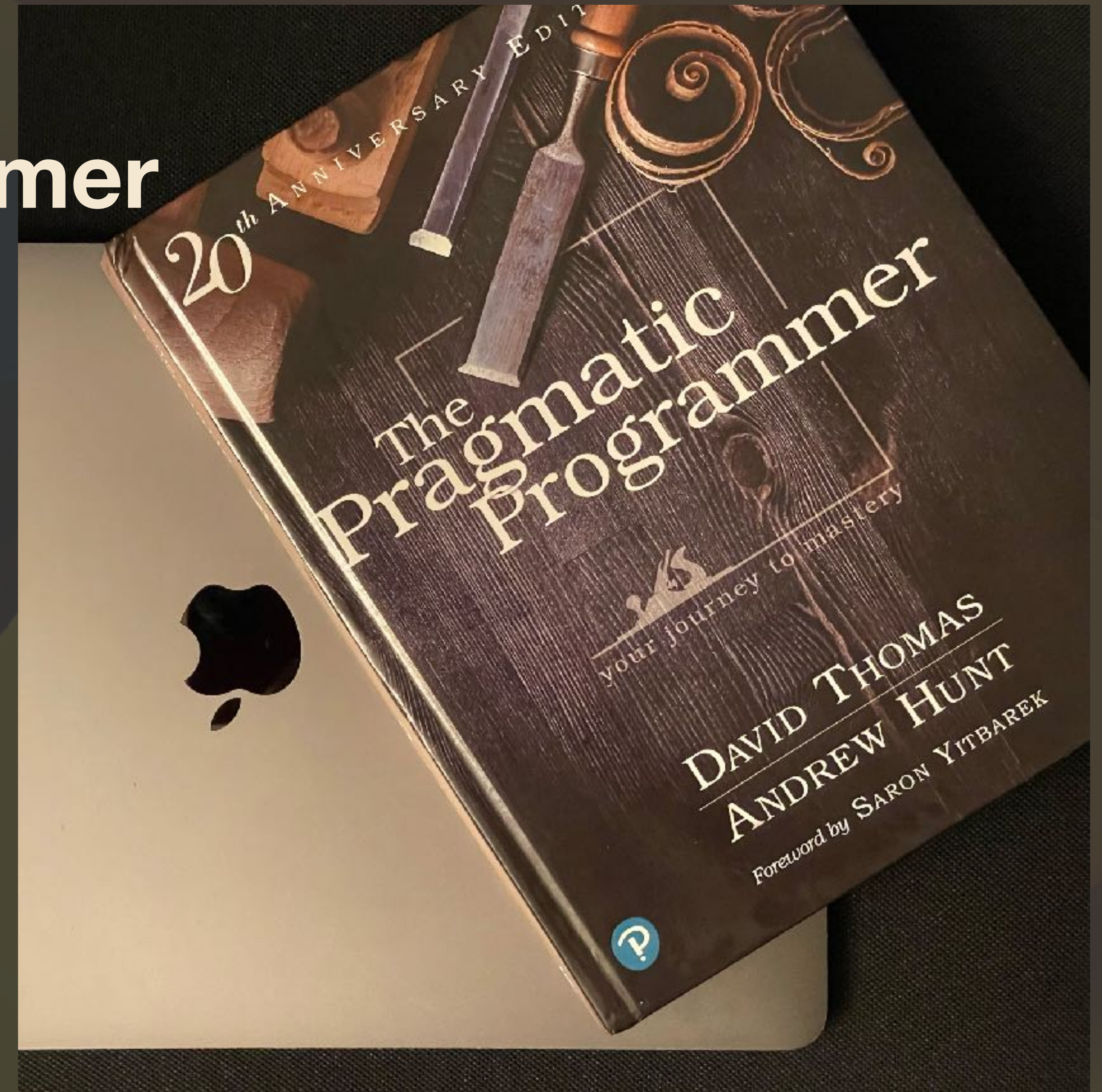
“Rubber Duck” Debugging

- ★ Explain your code to someone.
- ★ Rubber ducks are excellent listeners
- ★ The solutions often reveals itself
- ★ Improves critical analysis and problem-solving and deepens understanding



The Pragmatic Programmer

- ★ A collection of short topics, concepts, pro-tips, and anecdotes
- ★ Not specific to any programming language, framework, or SDK
- ★ Sound, practical advice for casual and serious programmers alike
- ★ “Rubber-duck” debugging (p.94)



ITS-LOG — V: FINAL THOUGHTS

Go Duck Yourself!

- ★ Please take a rubber ducky with you!



Resources

- ★ <https://derflounder.wordpress.com/2020/10/16/remotely-gathering-sysdiagnose-files-and-uploading-them-to-s3/>
- ★ swiftDialog: github.com/bartreardon/swiftDialog
- ★ SupportApp: github.com/root3nl/SupportApp
- ★ This session: github.com/bradtchapman/psumac2023

Special Thanks

- ★ Many helpful people on MacAdmins Slack
- ★ Bryson Terrell, Dave Siederer, Scott Blake
- ★ Milly ❤️
- ★ Pumpkin (cat)

THANK YOU!



github.com/bradtchapman/psumac2023
Static QR code. No tracking. No redirection.