

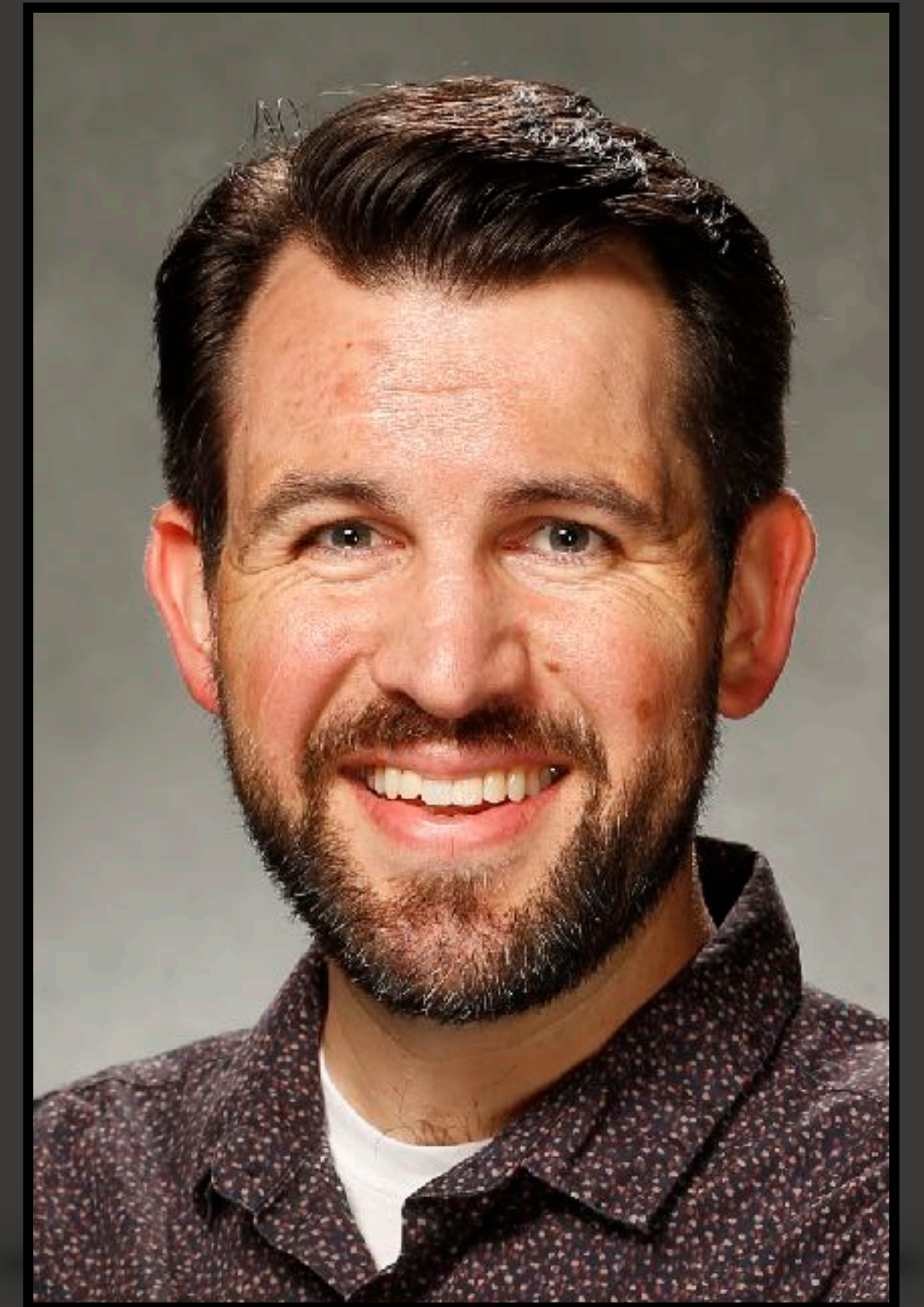
ITS-LOG!



**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

ITS-LOG — I: THE PROBLEM

An emergency arises...



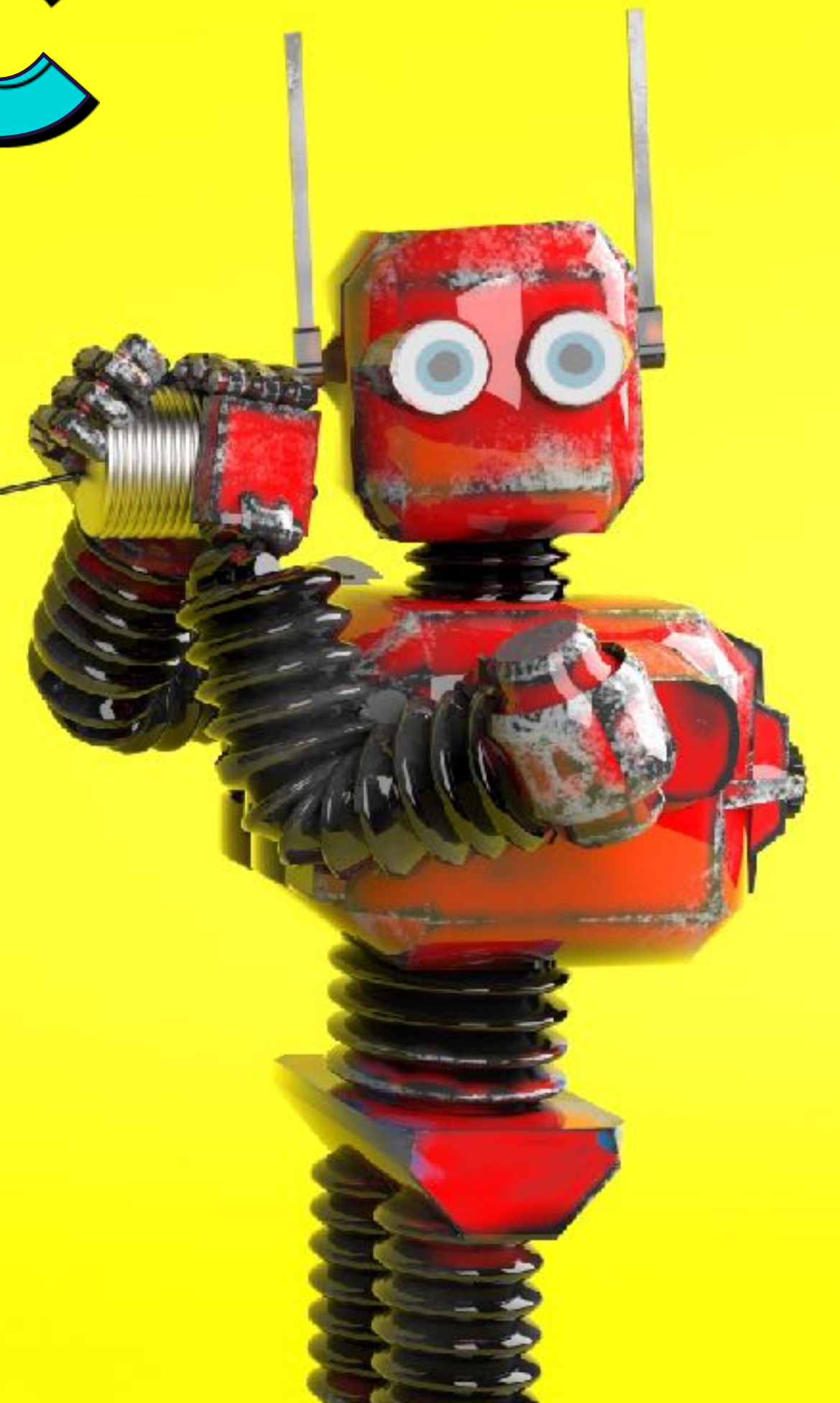
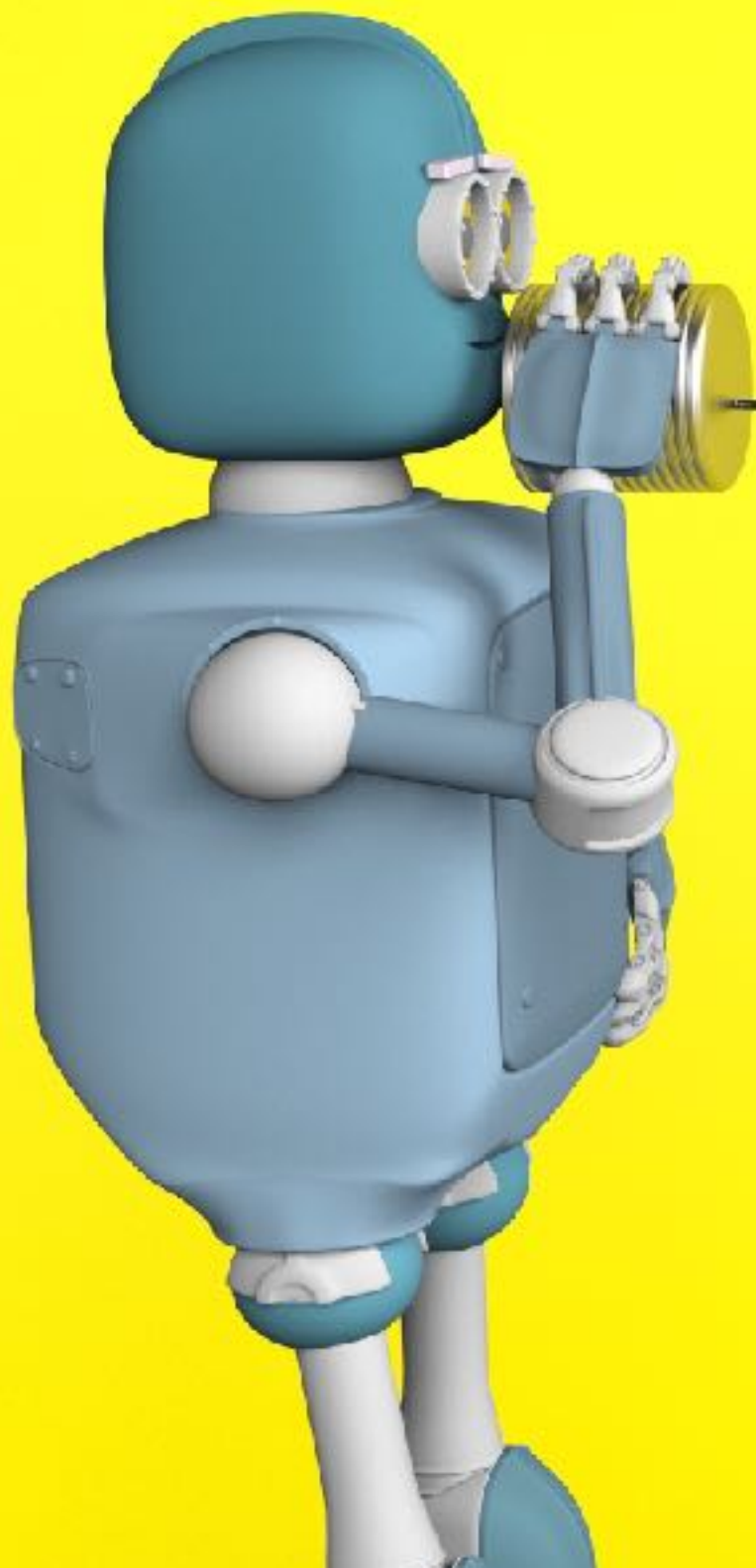
An emergency arises...

- ★ 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:



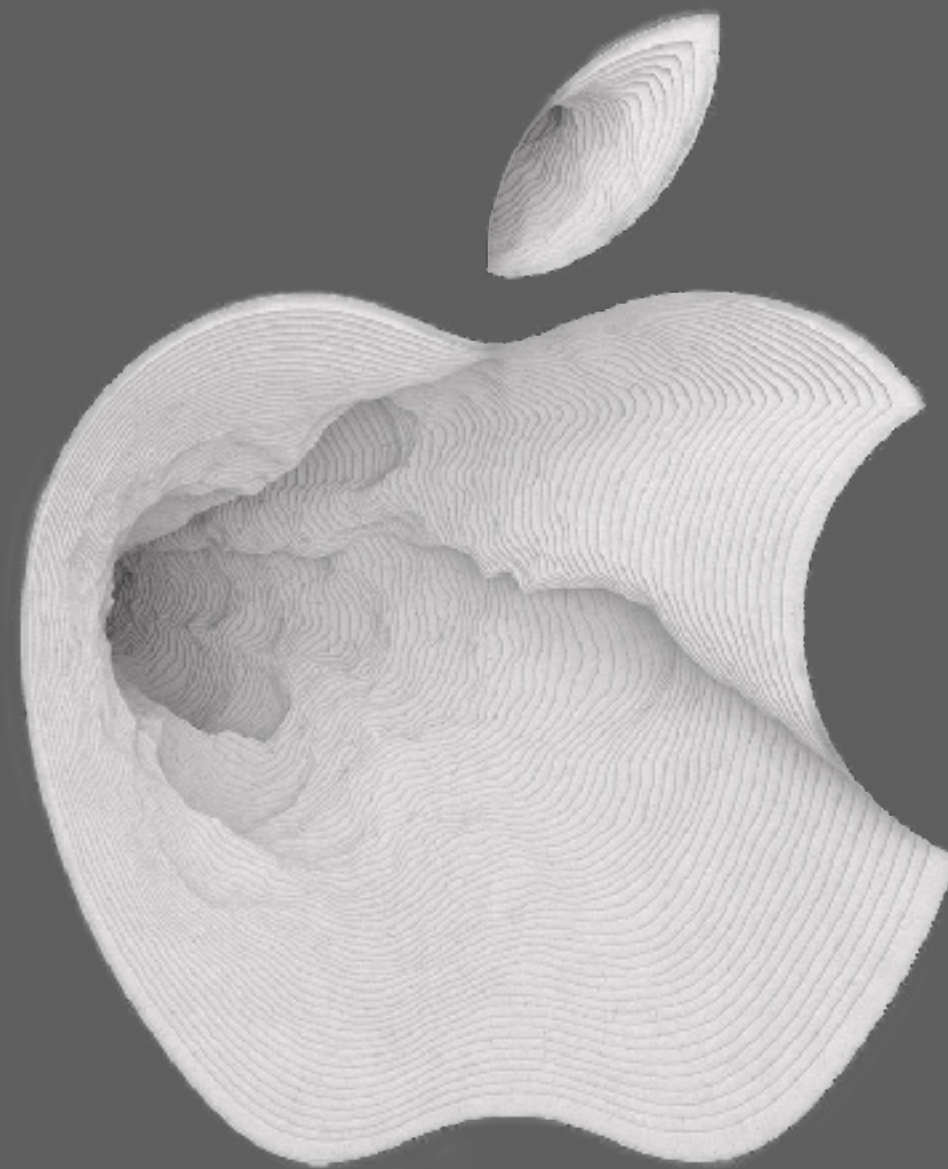
“Users are getting locked out of their Macs randomly.”

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!

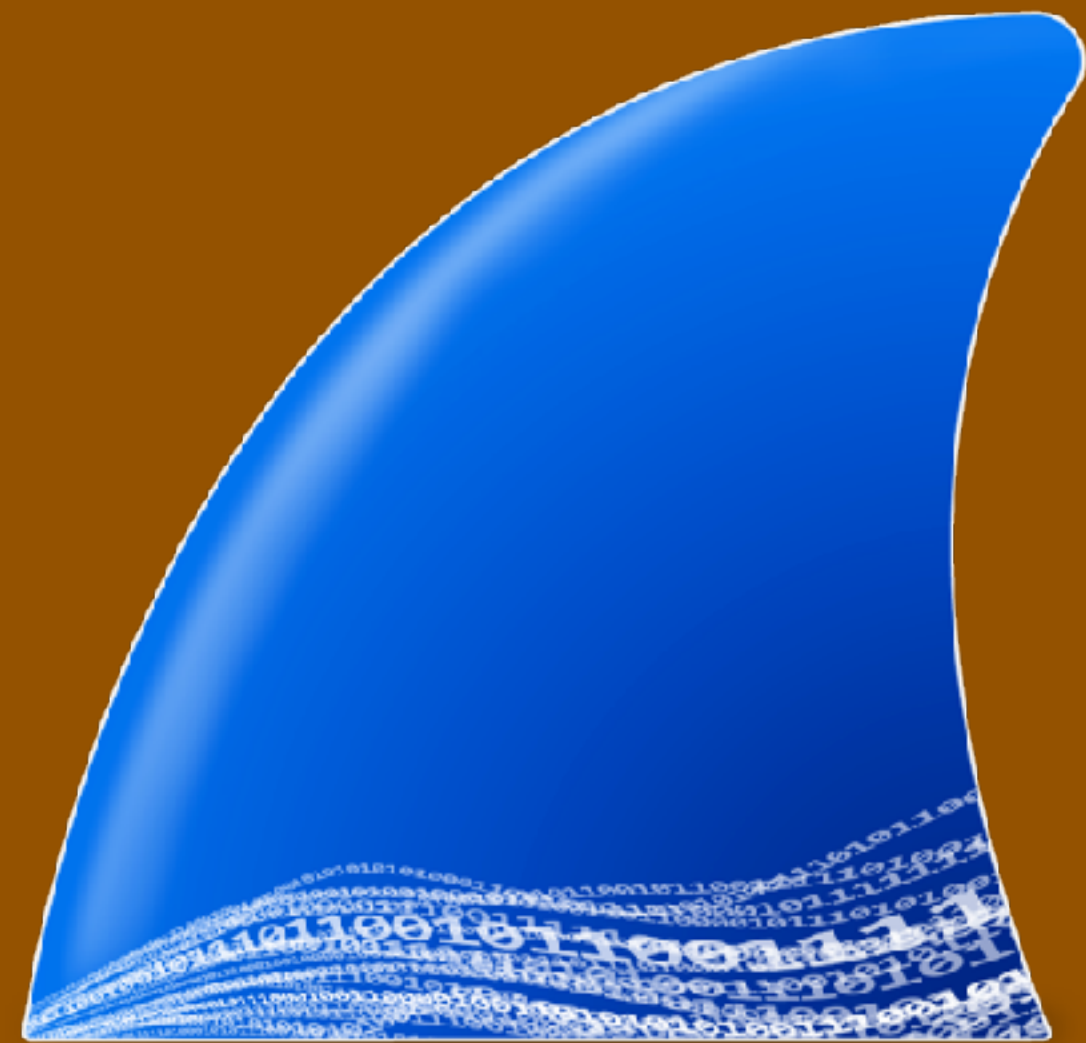
Root Cause Analysis:



"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 Solution

ITS-LOG!

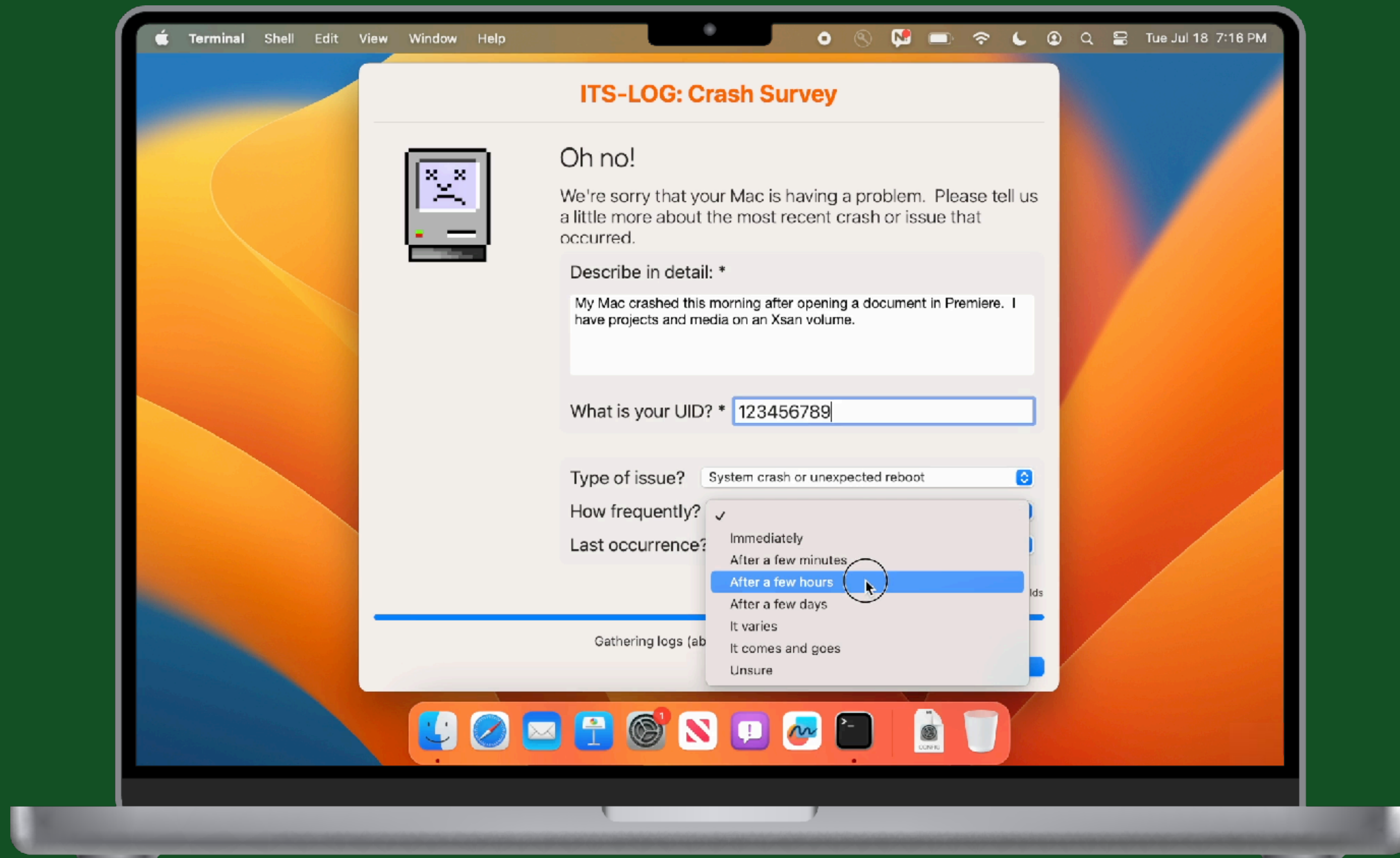
ALL ADMINS
LOVE LOGS!



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,daɪəg'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?

> Accessibility

- acdiagnose-503.txt
- airport_info.txt
- apfs_stats.txt
- applessdstats.txt
- apsd-status.txt
- > **ASPSnapshots**
- bc_stats.txt
- bless_info.txt
- BluetoothTraceFile.pklg
- bootstamps.txt
- bputil.txt
- > **brctl**
- ckksctl_status.txt
- codectl.txt
- com.apple.windowserver.displays.plist

> crashes_and_spins

- csrutil-status.txt
- DiskMountConditioner.json
- disks.txt
- diskutil_apfs_listUsers.txt
- diskutil_apfs.txt
- diskutil_cs.txt
- diskutil_info.txt
- diskutil_list.txt
- diskutil_listClients.txt
- diskutil_listSnapshot.txt
- display_diagnose.txt
- efi-dump-logs.txt
- error_log.txt

> errors

- filecoordination.txt
- fileproviderctl_check.log
- fileproviderctl_dump.log
- fileproviderctl.log
- find-system-migration-history.txt
- footprint.txt
- gpt.txt
- hdiutil-pmap.txt
- hidutil.plist

- hpmDiagnose.txt
- iogdiagnose.txt
- > **ioreg**
- kextstat.txt
- kmutil-diagnose.txt
- launchctl-dumpstate.txt
- launchctl-list-0.txt
- launchctl-list-503.txt
- launchctl-print-gui-503.txt
- launchctl-print-system.txt
- launchctl-print-user-503.txt
- launchctl-procinform-7195-Self Service.txt

> libtrace

✓ logs

- > **asl**
- > **BatteryBDC**
- > **BatteryHealth**
- > **BatteryUIplist**
- > **CalendarPreferences**
- com.apple.SocialLayer.plist
- > **DCP**
- > **DiagnosticMessages**
- > **EndpointSecurity**
- > **FDR**
- > **fsck**
- install.log
- InstallHistory.plist
- > **IntlDataCache**
- ionodecache.json
- > **iSCPreboot**
- > **launchd**
- > **loginwindow**
- > **MemoryExceptions**
- > **MobileActivation**
- > **MobileInstallation**
- > **MobileSoftwareUpdate**
- > **olddsc**
- > **parsecd**
- > **powerlogs**
- > **psm**

- SFRRestoreVersion.plist

> SiriAnalytics

> Splat

> suggest_tool

- system.log

- system.log.0.gz

> SystemExp

✓ systemstats

✓ db

- ...many files

> SystemVersion

> UserManagement

- lsappinfo.txt
- lsregister-0.csstoredump
- lsregister-503.csstoredump
- > **mddiagnose.mdsdiagnostic**
- > **microstackshots**
- mount.txt
- nclist.txt
- > **network-info**
- nfsstat.txt
- night-shift.log
- nvram.txt
- odutil.txt
- oslog_archive_error.log
- otctl_status.txt
- pcstatus.txt
- > **Personalization**
- pluginkit-503.txt
- pmset_everything.txt
- powermetrics.txt
- > **Preferences**
- ps_thread.txt
- ps.txt
- README.txt
- remotectl_dumpstate.txt
- resolv.conf
- > **RunningBoard**
- sample-389-highcpu.txt
- sample-662-highcpu.txt

- sample-1443-highcpu.txt
- sample-7195.txt
- securebootvariables.txt
- security-sysdiagnose.txt
- sfltool.LSSharedFileList.FavoriteItems.txt
- sfltool.LSSharedFileList.FavoriteVolumes.txt
- sfltool.LSSharedFileList.iCloudItems.txt
- smcDiagnose.txt
- spindump.txt
- stackshot.kcdata

> summaries

- sw_vers.txt
- swutil_show.txt
- sysctl.txt
- sysdiagnose.log
- system_logs.logarchive
- > **SystemConfiguration**
- systemextensionsctl_diagnose.txt
- > **SystemProfiler**
- tailspin-info.txt
- tailspin-trace.tailspin
- talagent-503.txt
- taskinfo.txt
- taskSummary.csv
- tbtDiagnose.txt
- thermal.txt

> TimezoneDB

- top.txt
- transparency.log
- uptime.txt
- var_run_resolv.conf
- vm_stat.txt

✓ WiFi

> CoreCapture

> WiFi

- WindowServer.external.winfo.plist
- xartutil.txt
- zprint.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

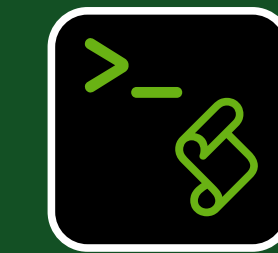
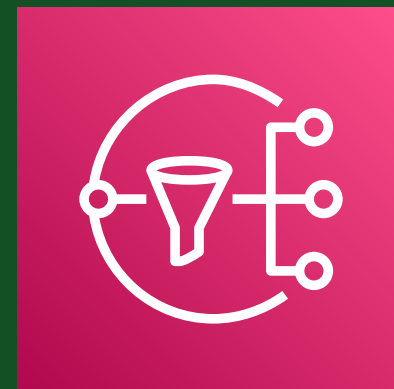
Big file. Bigger problem.

- ★ 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?



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



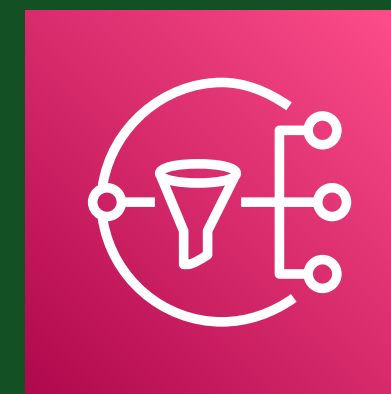
Flow: AWS to You



S3



Lambda



SNS

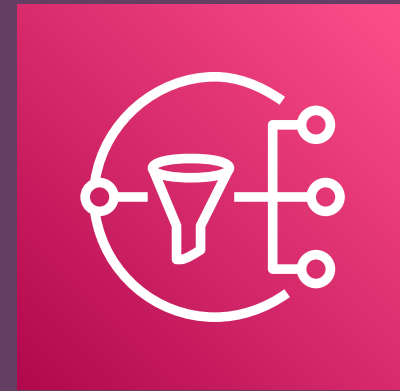


Email



Email

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

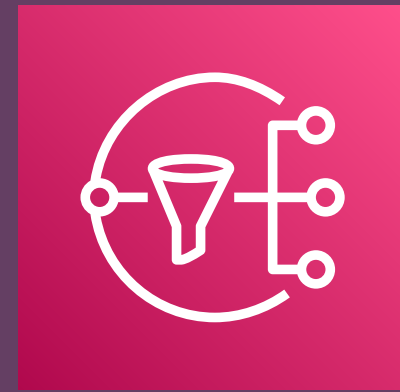


SNS

- ★ 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!

A screenshot of the AWS IAM console region dropdown menu. The menu is open, showing a list of regions. The current region is 'Oregon'. The dropdown menu is dark-themed with white text. The 'Oregon' region is highlighted in orange. The list of regions is as follows:

Region Name	Region Code
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

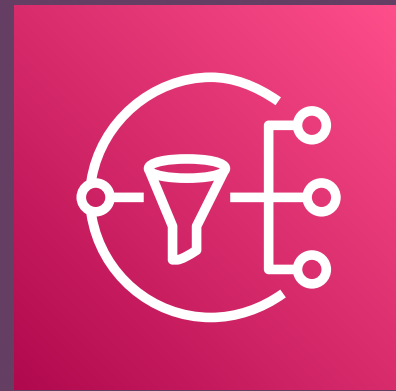


SNS

- ★ 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

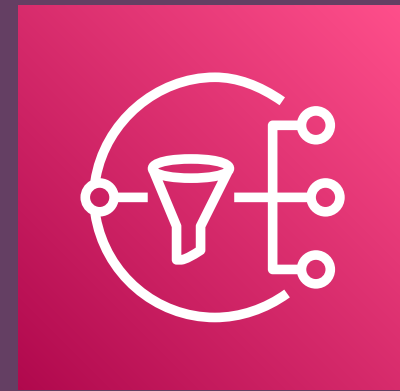
Everyone
Any AWS account can subscribe to the topic

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",
```

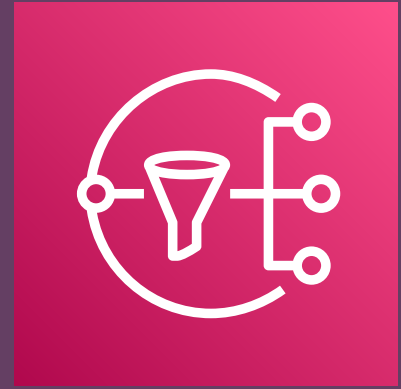
SNS

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

The screenshot shows the 'Create Topic' dialog box in the AWS console. It features several expandable sections for optional settings:

- Access policy - optional** (collapsed)
- 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.

At the bottom right, there are two buttons: 'Cancel' and '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 >

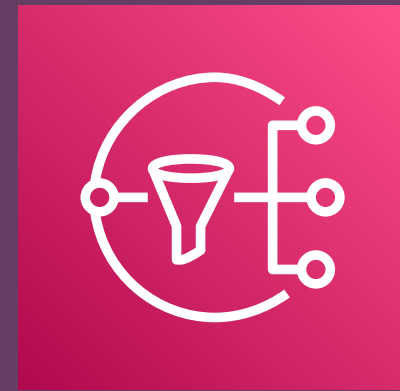
Subscriptions (2)

Edit Delete Request confirmation Confirm subscription Create subscription

Q Search < 1 > ⚙

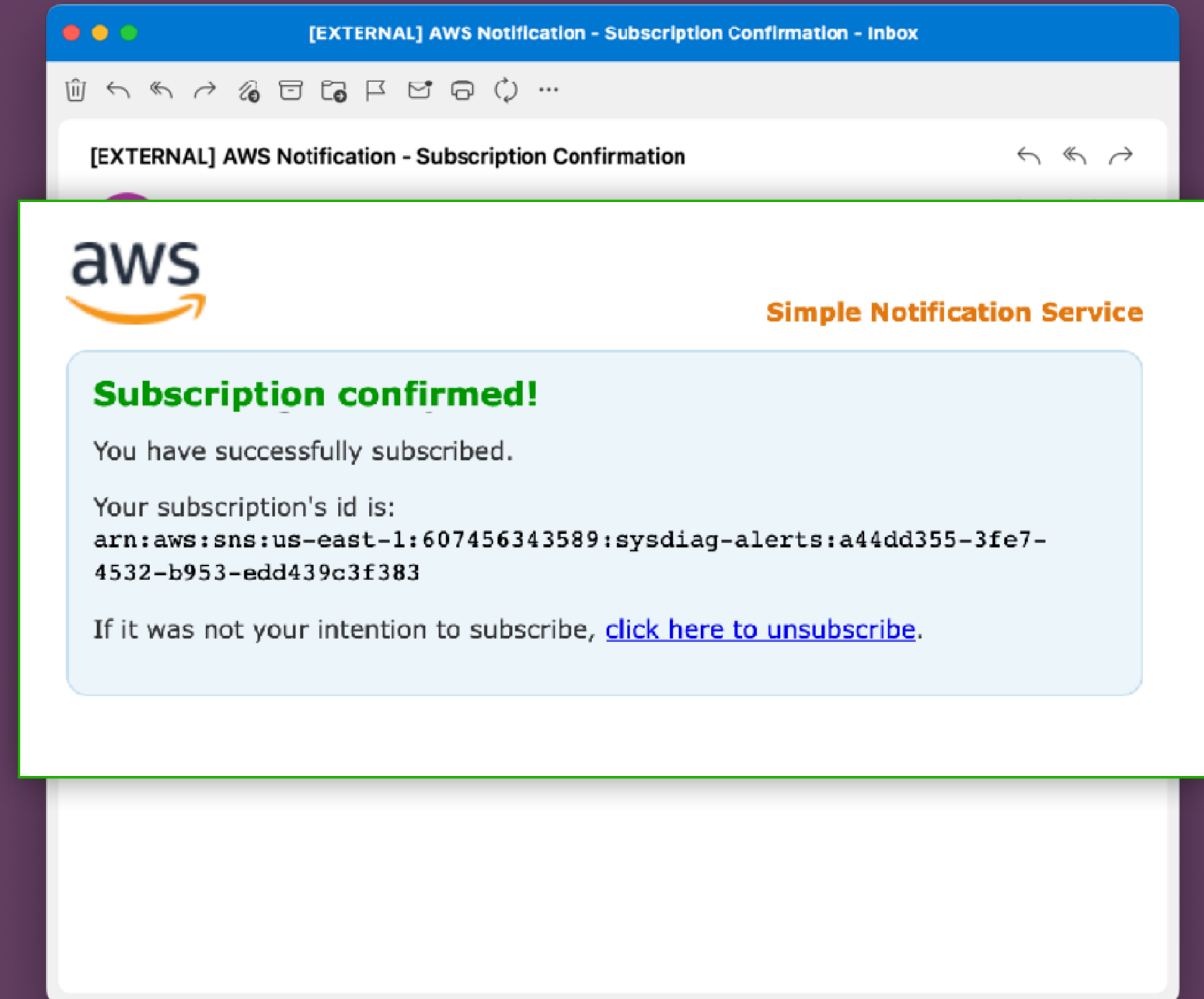
ID	Endpoint	Status	Protocol
7987a328-924c-4...	[REDACTED]	✔ Confirmed	EMAIL
a44dd355-3fe7-45...	Johnny.appleseed...	✔ Confirmed	EMAIL

< 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 of the following filter types
- 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 of objects
- These actions are not supported when filtering by 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 interface. The top navigation bar includes tabs for Code, Test, Monitor, Configuration, Aliases, and Versions. The main content area is titled "Code source" and includes an "Upload from" dropdown menu. Below this is a menu bar with File, Edit, Find, View, Go, Tools, and Window. The "Test" tab is active, showing a code editor for "index.js" and an "Execution results" panel. The code in the editor is JavaScript that processes S3 event records, extracts metadata like bucket name, event name, and time, and constructs a message for an SNS notification. The execution results panel shows the output of the code, including the constructed message and the URL of the source file.

```
8 // Read options from the event.
9 console.log("Reading options from event:\n", util.inspect
10
11 var s3Event = event.Records[0];
12
13 var srcBucket = s3Event.s3.bucket.name;
14 var srcEvent = s3Event.eventName;
15 var time = s3Event.eventTime;
16
17 // var timeUTC = Date.UTC(time);
18 // var objYear = Date.prototype.getFullYear(time);
19 // var objMonth = Date.prototype.getMonth(time);
20 // var objDay = Date.prototype.getDate(time);
21 // var objHour = Date.prototype.getHours(time);
22 var object = s3Event.s3.object.key;
23 var size = Math.round((s3Event.s3.object.size)/1048576);
24
25 var s3Url = "https://" + srcBucket + ".s3.amazonaws.com/"
26
27 https://sysdiagnose-nbcu-00001.s3.amazonaws.com/sysdiagn
28
29
30
31 var msg = "A new file has been uploaded to S3. \r\n\r\n
32           "Bucket: " + srcBucket + "\r\n" +
33           "Event: " + srcEvent + "\r\n" +
34           "Object: " + object + "\r\n" +
35           "Size: " + size + " MB\r\n" +
36           "Time: " + time + "\r\n" +
37           "URL: ";
38
39 var sns = new AWS.SNS();
```



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 to use.

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.

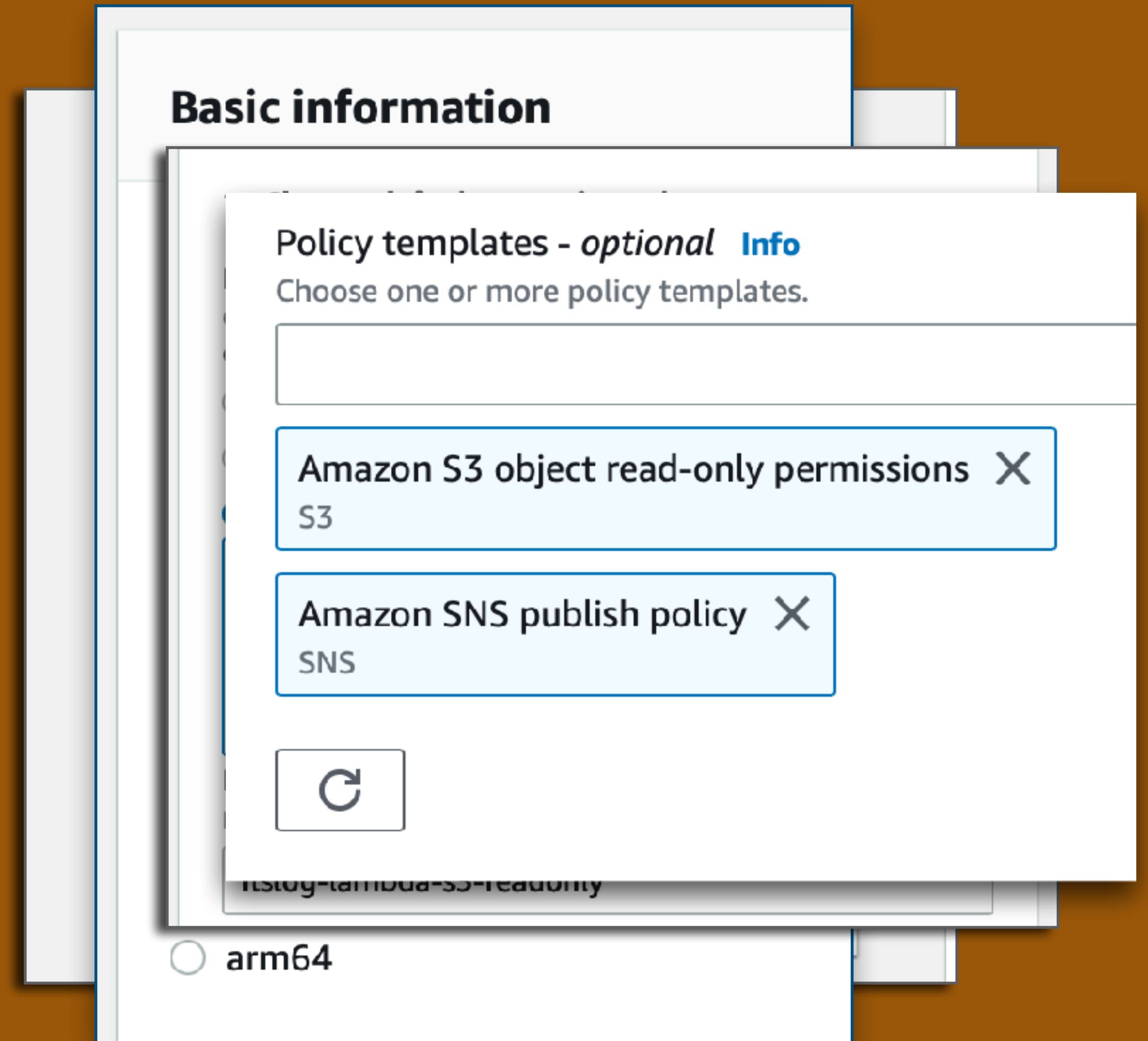
itslog-lambda-s3-readonly

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.**





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 be 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 filters 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 source and destination. Using the same bucket increases the risk of creating a recursive invocation, which can cause your function to run indefinitely.

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

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

Enter a single optional suffix to limit the notifications to objects with the following suffix:



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

```
file Edit Find View Go Tools Window Test Deploy Changes not deployed
Go to Anything (36 P)
itslog-read
  index.js
JS index.js
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

```
file Edit Find View Go Tools Window Test Deploy Changes not deployed
Go to Anything (⌘ P) JS index.js Environment Variables Preferences
// Sources:
5 // Event type: s3:ObjectCreated:*
6 // Prefix: itslog/surveys/
7
8 var snsTopicARN = "arn:aws:sns:us-west-
9 var util = require('util')
10 var AWS = require('aws-sdk');
11 var s3 = new AWS.S3();
12
13 exports.handler = function(event, conte
14
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

```
file Edit Find View Go Tools Window Test Deploy Changes not deployed
Go to Anything (36 P) JS index.js Environment Variables Preferences
// Sources:
5 // Event type: s3:ObjectCreated:*
6 // Prefix: itslog/surveys/
7
var msg = "ITS-LOG: A user calls for aid! \r\n" +
"Survey responses below: \r\n" +
"----- \r\n\r\n" +
srcBody + "\r\n\r\n" +
"DOWNLOAD SYSDIAGNOSE FILE NOW. Link expires
signedUrlValidDays + " day(s) after time sent
signedUrl + "\r\n\r\n" +
"S3 Bucket : " + srcBucket + "\r\n" +
"File (key): " + srcKey + "\r\n";
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

```
file Edit Find View Go Tools Window Test Deploy Changes not deployed
Go to Anything (36 P) JS index.js Environment Variables Preferences
// Sources:
5 // Event type: s3:ObjectCreated:*
6 // Prefix: itslog/surveys/
7
var msg = "ITS-LOG: A user calls for aid! \r\n" +
"Survey responses below: \r\n" +
"----- \r\n\r\n" +
srcBody + "\r\n\r\n" +
var sns = new AWS.SNS();
sns.publish(
{
  Subject: "ITS-LOG: Survey Recorded",
  Message: msg,
  TopicArn: snsTopicARN
},
32 var signedUrlValidDays = Math.round(signedUrlValidSeconds / 86400);
```



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
```



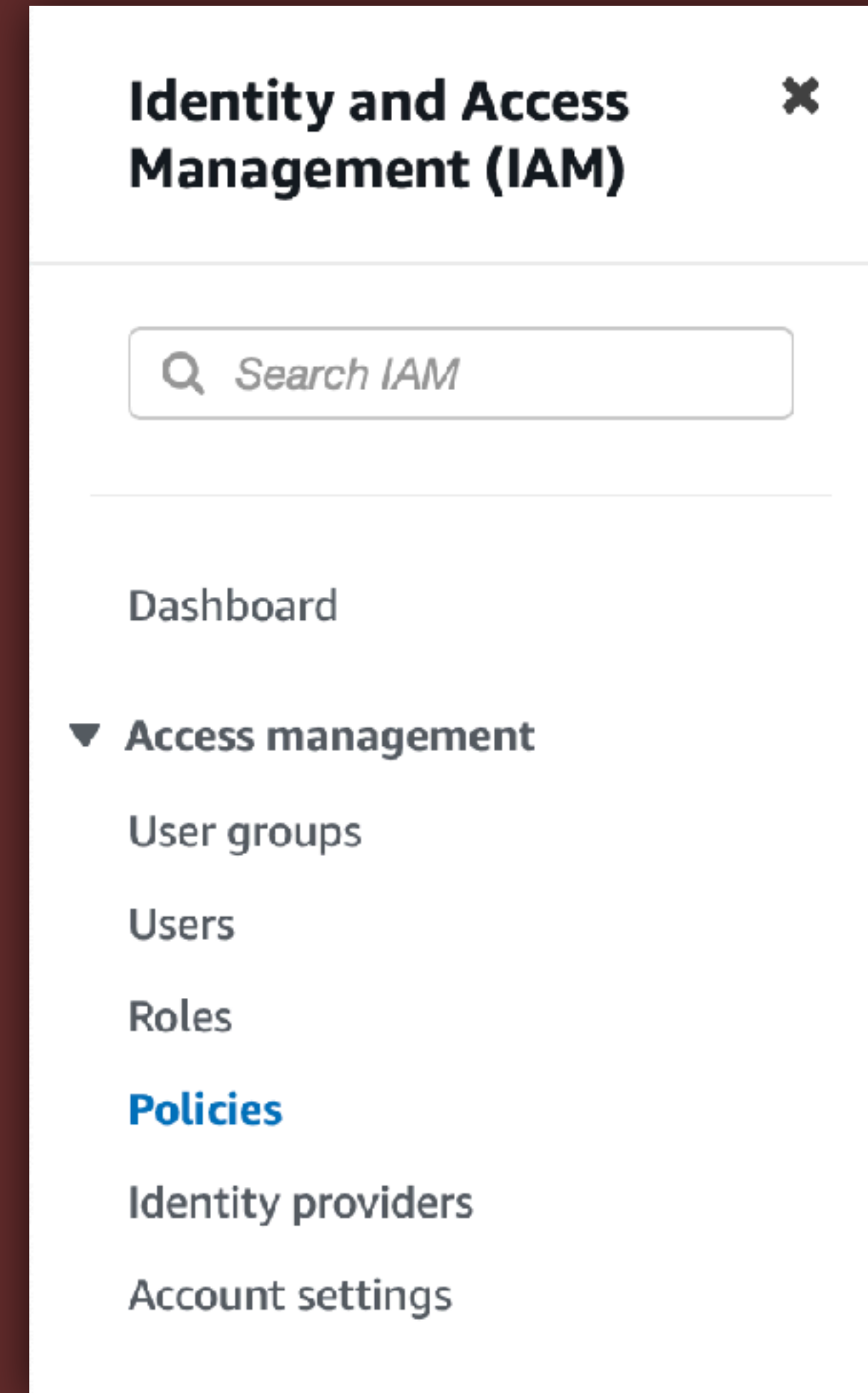

IAM Policy

- ★ 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

Visual JSON Actions

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

Q s3 x Popular services

Glacier ⓘ S3 ⓘ S3 Object Lambda ⓘ S3 Outposts ⓘ


+ Add more permissions

Cancel Next

Identity providers
Account settings



IAM Policy

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

Policy editor Visual JSON Actions ▼

▼ S3 Allow 0 Actions + -

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

▼ Actions allowed
Specify actions from the service to be allowed.

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

Cancel Next



IAM Policy

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

The screenshot shows the 'Specify ARNs' dialog box in the AWS IAM console. It has a title bar with a close button (X). The dialog is divided into several sections:

- Visual**: A dropdown menu showing 'Visual'.
- Resource bucket name**: A checkbox for 'Any bucket name' is unchecked. Below it is a text input field containing 'itslog-blammo-002/itslog'.
- Resource object name**: A checkbox for 'Any object name' is checked. Below it is a text input field containing '*'.
- ARN**: A checkbox for 'Any resource' is unchecked. Below it is a text input field containing 'itslog-blammo-002/itslog/*'. At the bottom of this section is a text input field containing the full ARN: 'arn:aws:s3:::itslog-blammo-002/itslog/*'.

At the bottom right of the dialog are two buttons: 'Cancel' and '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

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.

Filter by Type

1 match

< 1 >

<input checked="" type="checkbox"/>	Policy name	Type	Atta...
<input checked="" type="checkbox"/>	<input type="button" value="+"/> 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](#)

AKIAIY23ZYG	Actions ▼
Description	Status
Upload-only account for writing an object to the S3 bucket.	✔ Active
Last used	Created
9 hours ago	16 days ago
Last used region	Last used service
us-east-1	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
AKIAY23ZYGYSSEMUKQSI 	***** 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 [REDACTED] ✕

Delete access key AKIARMNCSYN [REDACTED]? 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

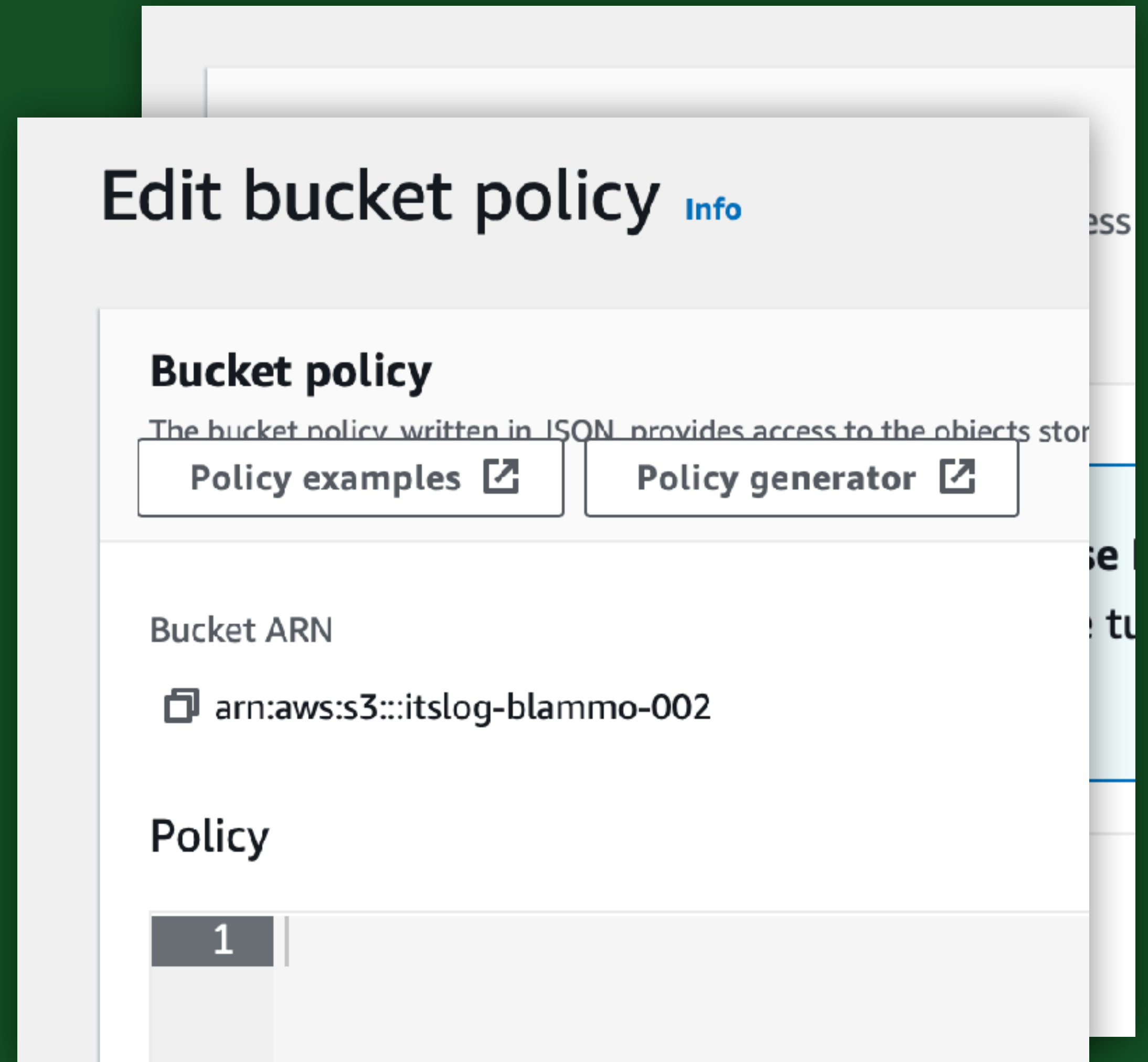
- ★ Go to Permissions tab
- ★ Under Bucket Policy, click Edit.
- ★ Click [Policy Generator].
- ★ Prepare for a time warp to **2010...**

The screenshot shows the AWS S3 console interface for managing a bucket's policy. At the top, the heading "Bucket policy" is followed by a sub-heading "The bucket policy, written in JSON, provides access". Below this, there are two buttons: "Edit" and "Delete". The "Edit" button is highlighted with a red rectangular border. Below the buttons is a light blue information box with a circular icon containing an 'i'. The text in the box reads "Public access is blocked because" followed by "To determine which settings are tu" and a link labeled "Access" with an external link icon. At the bottom of the screenshot, there is a greyed-out area with the text "No policy to display."



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](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of 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

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 Allow Deny

Principal
Use a comma to separate multiple values

Service
Use multiple statements to add permissions

Actions

ARN
ARN should follow the following format:
Use a comma to separate multiple values

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



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.”

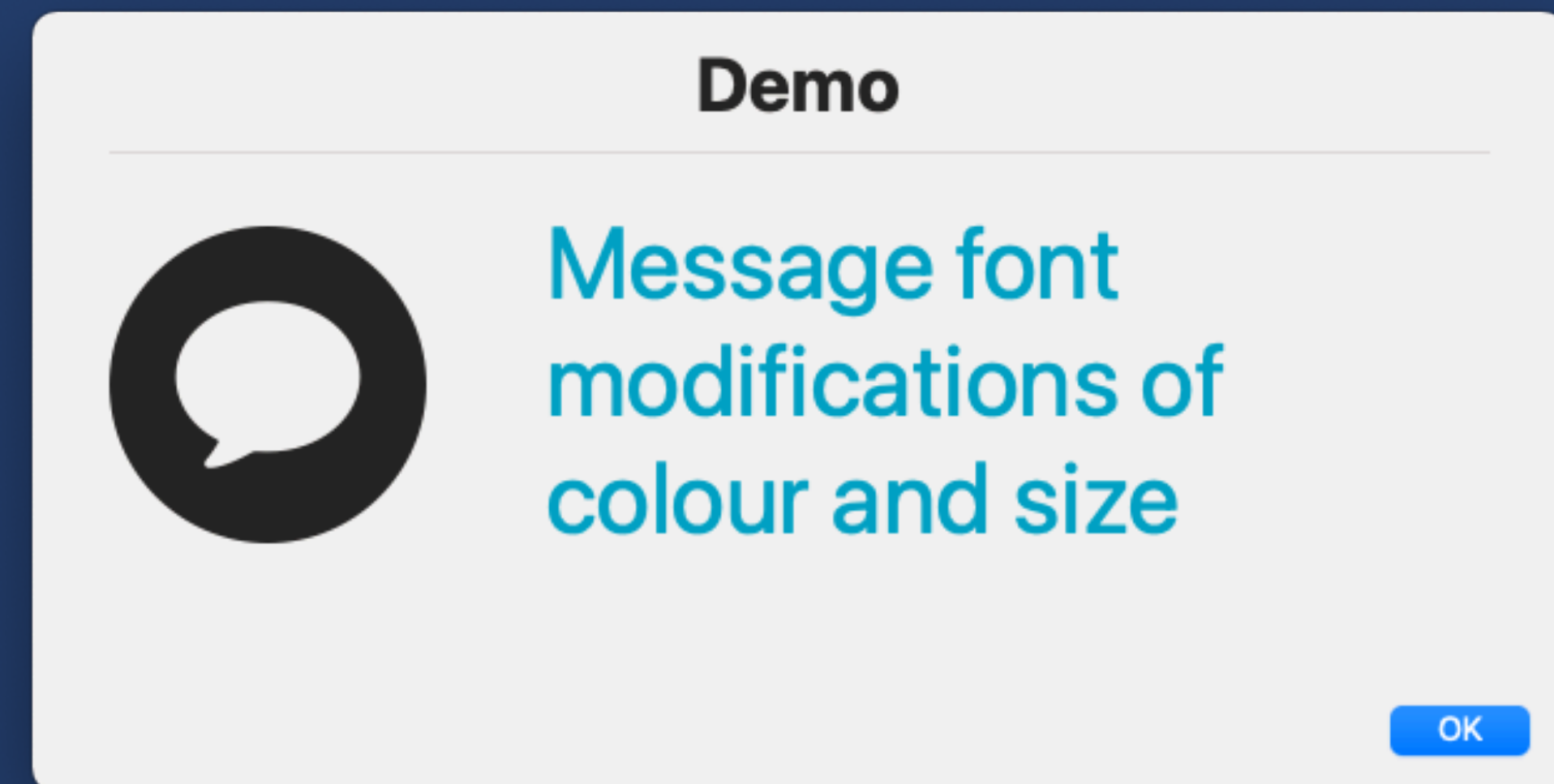
```
Policy
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Principal": {
7          "AWS": "arn:aws:iam::328271117716:user
           /itslog-s3-writeonly"
8        },
9        "Action": "s3:PutObject",
10       "Resource": "arn:aws:s3:::itslog-blammo-002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

```
Shell Script
Language Run Stop Run Settings... Back/Forward View
itslog-crash-survey.sh itslog-master-script.sh
184
185
186 #
187 ##### STAGE 2: SYSDBGNOSE COLLECTION
188 #
189
190 generateSysdiagnose() {
191
192     /usr/bin/sysdiagnose -b -n -u -Q -P -G -f /var/tmp -A "$sysDiagArchive" | cat &
193
194     swd_echo "progresstext: Gathering logs (about 3-5 minutes) ..."
195
196     sleep 1
197
198     while [[ -n $(pgrep "sysdiagnose_helper") ]]
199     do
200         # Keep checking until the sysdiagnose utility has finished. "Sysdiagnose is still
201         # running..."
202
203         # If user finishes the survey before curl or sysdiagnose are completed...
204         # Launch the mini window to keep them informed.
205
206         if [[ -z $(ps -ax $swd_survey_PID | tail +2) && $mini_window_launched == false ]]
207         then
208             launch_mini_window
209             swd_echo "progresstext: Gathering logs (about 3-5 minutes) ..."
210         fi
211
212         sleep 1
213
214     done
215
216     /usr/bin/tar -czf "$sysDiagTarball" "$sysDiagArchive/" &
217     tarPID=$!
218
219     echo "PID of tar is $tarPID"
220
221     swd_echo "progresstext: Compressing logs and preparing to upload."
222
223     sleep 1
224
225     while [[ -n $(ps -ax $tarPID | tail +2) ]]
226     do
227         # echo "tar is still balling..."
228
229         # If user finishes the survey before curl or sysdiagnose are completed...
230         # Launch the mini window to keep them informed.
231
232         if [[ -z $(ps -ax $swd_survey_PID | tail +2) && $mini_window_launched == false ]]
233         then
234             launch_mini_window
235             swd_echo "progresstext: Compressing logs and preparing to upload."
236         fi
237
238         sleep 1
239     done
240 }
241
242 launchSurveyWindow
243
244 Run Succeeded Time 0:00:41 Peak Memory 55.4M launchSurveyWindow Tabs: 4 Line 138, Column 1
```




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 $5}' | head -1`],
63 {"content-md5": "5md5" },
64 {"x-amz-date": "$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
83
84
85
86
87
88 # If user finishes the survey before curl or sysdiagnose are completed...
89 # Launch the mini window to keep them informed.
90
91 if [[ -z $(ps -ax $swd_survey_PID | tail +2) && $mini_window_launched == false ]]
92 then
93     launch_mini_window
94     swd_echo "progress.txt: Compressing logs and preparing to upload."
95 fi
96
97 sleep 1
98
99 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 >/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": "$date" },
65   {"x-amz-credential": "$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
83
84
85
86
87
88 # If user finishes the survey before curl or sysdiagnose are completed...
89 # Launch the mini window to keep them informed.
90
91 if [[ -z $(ps -ax $swd_survey_PID | tail +2) && $mini_window_launched == false ]]
92 then
93     launch_mini_window
94     swd_echo "progress.txt: Compressing logs and preparing to upload."
95 fi
96
97
98 sleep 1
99
100 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

.v

A hiker with a red backpack and a brown beanie stands at a fork in a dirt path in a forest. The sun is shining brightly from the right, creating a warm, golden glow and long shadows on the path. The trees are tall and thin, with some green foliage visible. The hiker is looking towards the right path.

*“ 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

The screenshot shows the Jamf Pro console interface for configuring a policy. The breadcrumb trail is 'Computers : Policies' followed by 'ITS-LOG! Collector'. The 'Options' tab is selected, showing a sidebar with categories: General (selected), Packages (0 Packages), Software Updates (Not Configured), Scripts (1 Script), and Printers (0 Printers). The main configuration area includes: 'General' section with 'Display Name' set to 'ITS-LOG! Collector'; 'Enabled' checkbox checked; 'Site' dropdown set to 'None'; 'Category' dropdown set to 'Self Help'; and 'Trigger' field.



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:

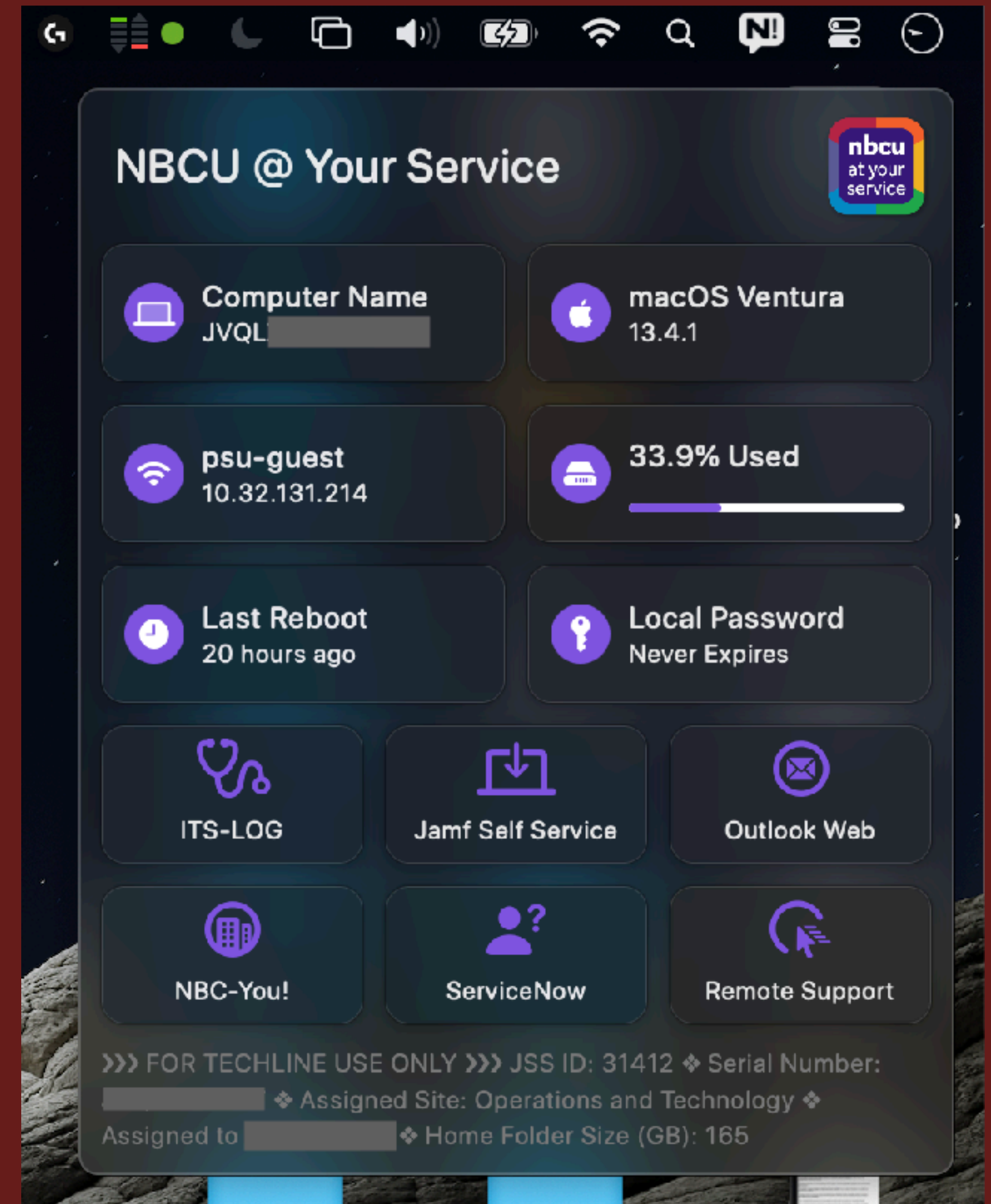
- ★ No software catalog app
- ★ MDM can't run arbitrary scripts
- ★ Boutique MSP deployments
- ★ Menu bar support tools





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

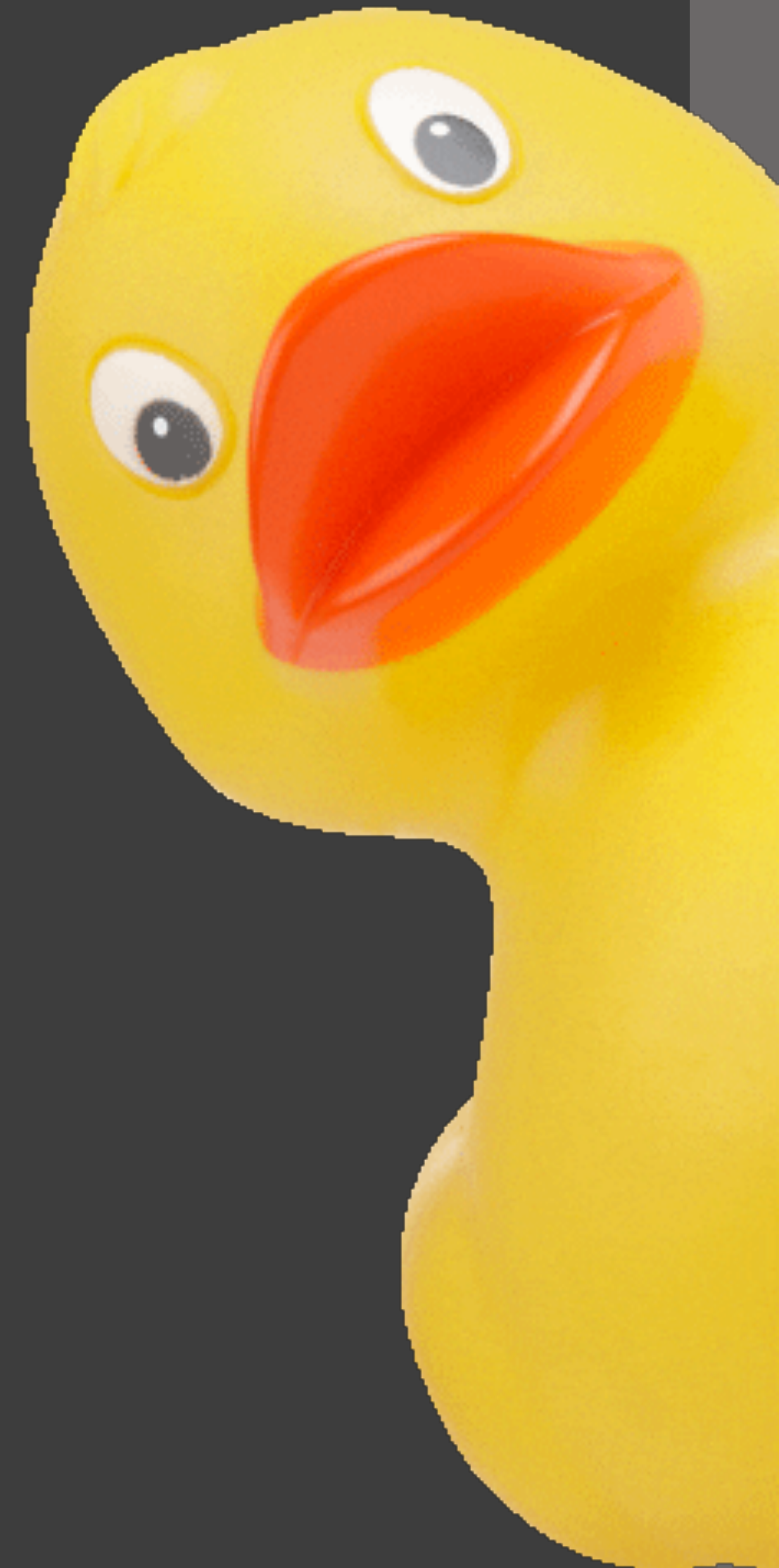
- ★ JNUC 2022 @ San Diego
- ★ Rehearsal went great...
- ★ Live build done with time to spare
- ★ The app failed to run properly.
- ★ Couldn't figure out what was wrong.
- ★ Played the safety pre-record instead.

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 **s**
- ★ “Talked” th
- ★ After many
- ★ Start typing



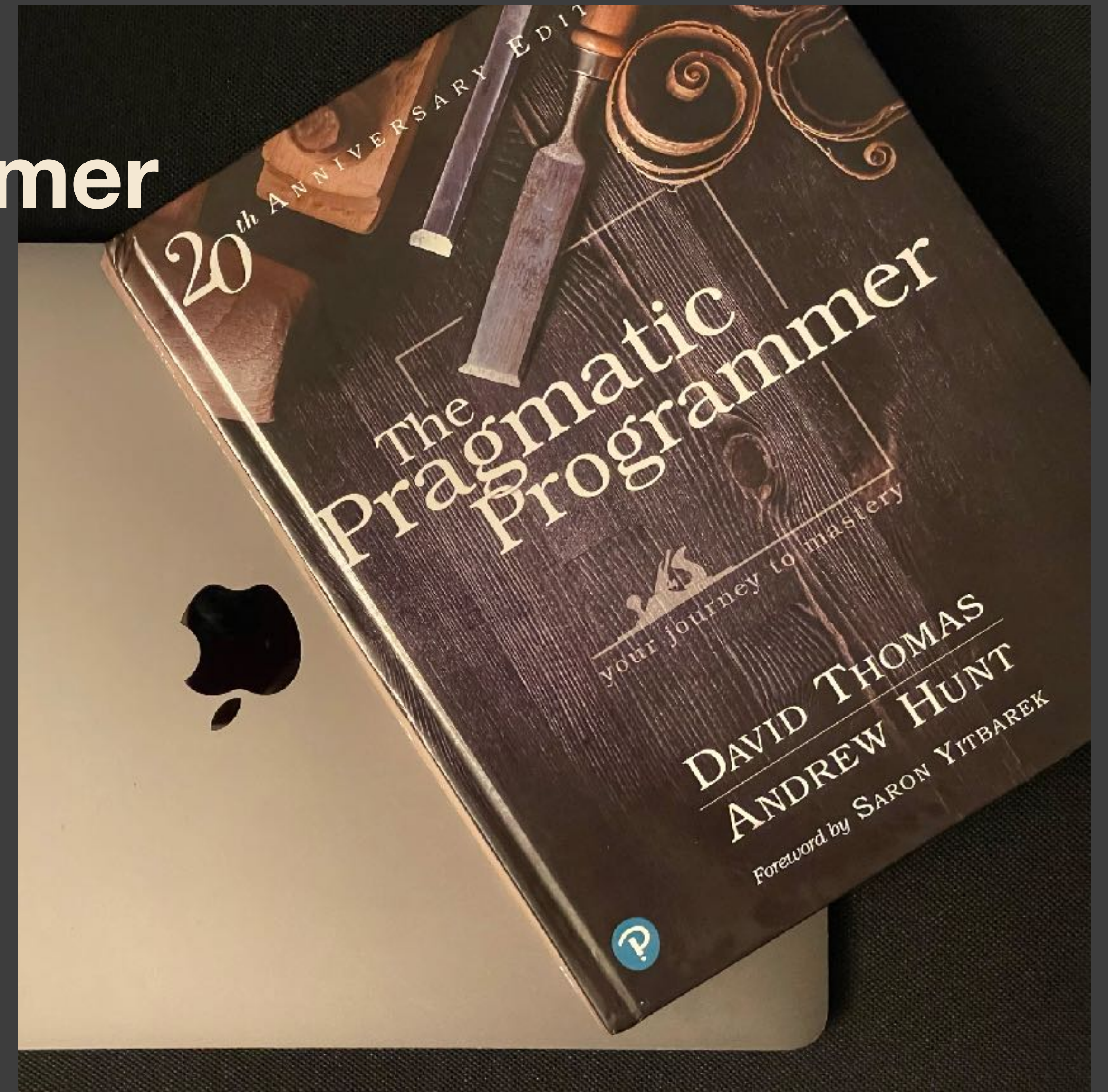
“Rubber Duck” Debugging

- ★ 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)**



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!



Static QR code. No tracking. No redirection.