
AWS
re:Invent

NFX301

Untangling multi-account management with ConsoleMe

Curtis Castrapel
Sr. Security Software Engineer
Netflix

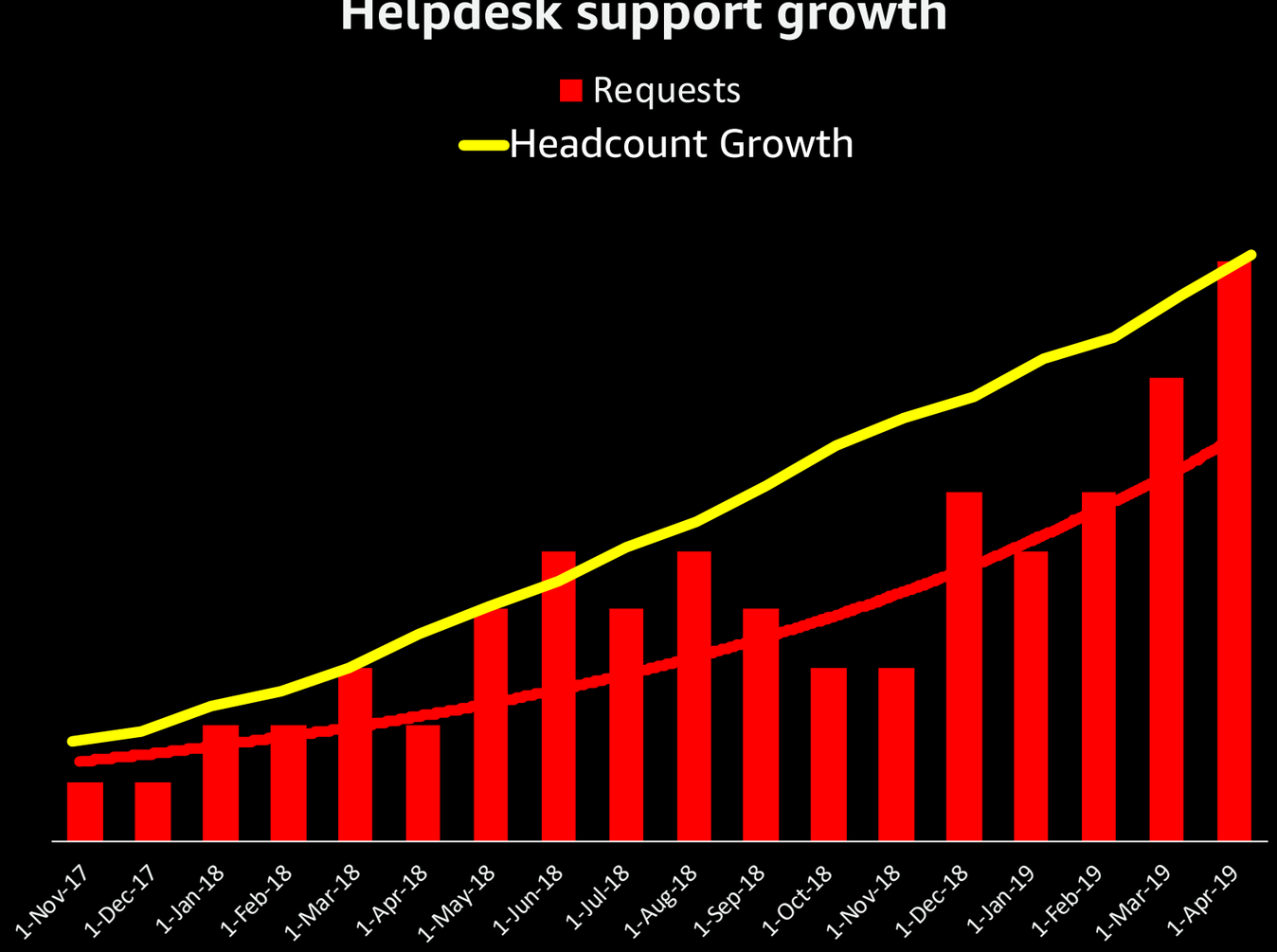
AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.





We needed to address the **growing** support burden around IAM




NETFLIX
TIDYING UP
WITH MARIE KONDO

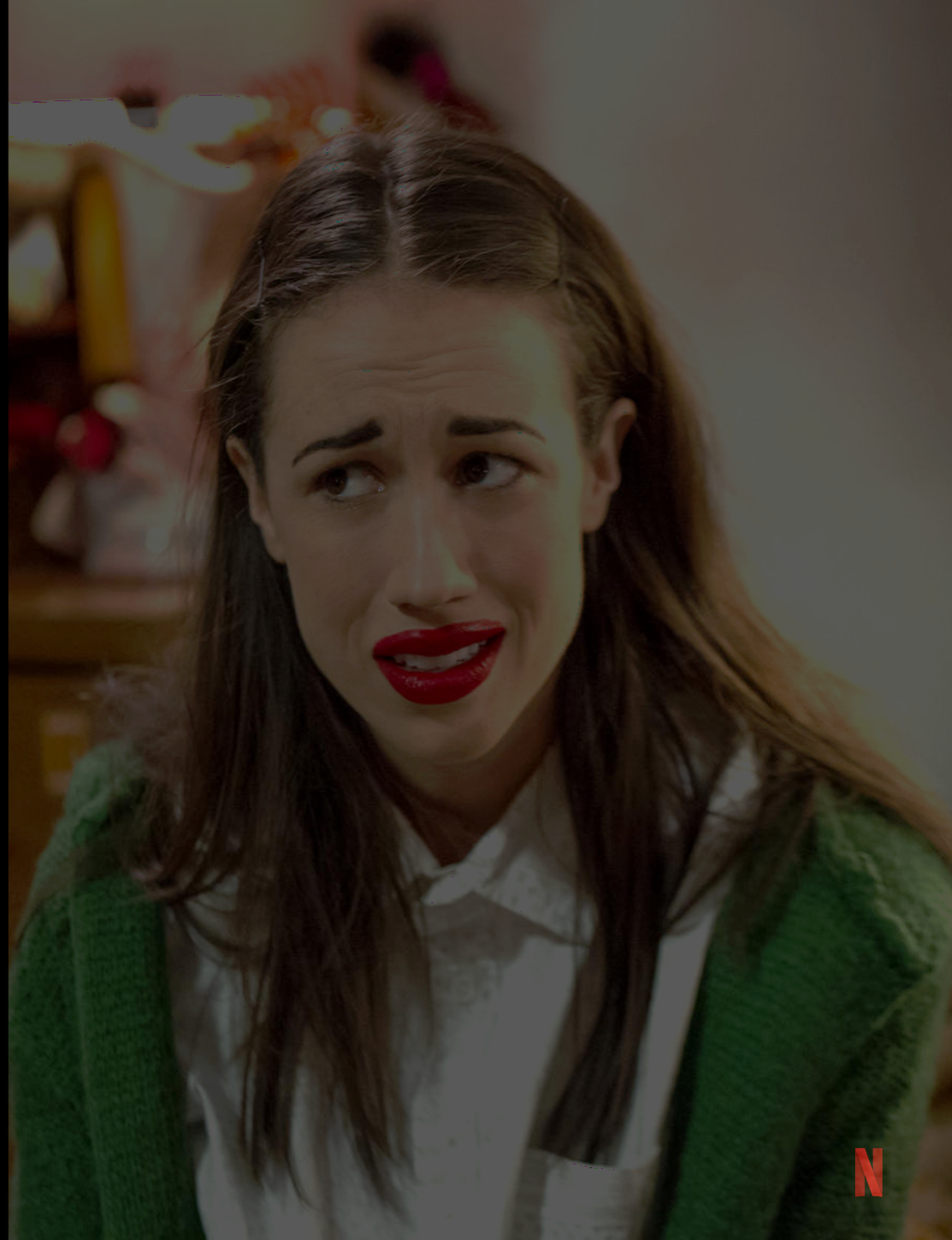
Our goal:

Your **entire** IAM workflow in a single place



Wave 1:

Multiple insecure ways to get IAM credentials

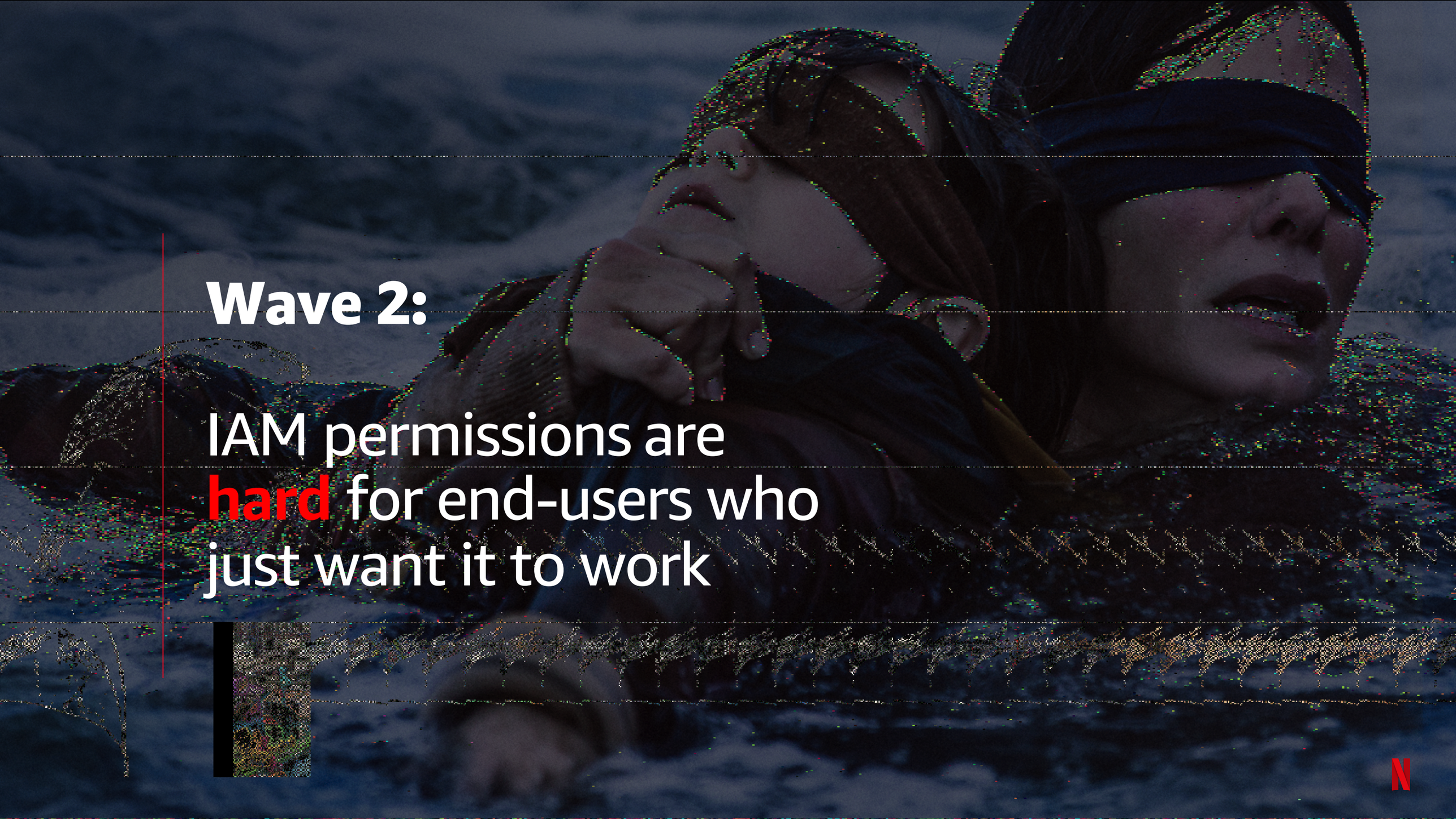


Flexible console access to fit every personality



Weep is a local instance metadata service for your developers that **automatically** refreshes your IAM credentials





Wave 2:

IAM permissions are **hard** for end-users who just want it to work

Self-service IAM Wizard makes it **easier** for your users to express their intentions **clearly**



Step 1.
Search and Select Resource

Step 2.
Provide Permission Details

Step 3.
Review and Submit

Select a Role

Please search for your role where you want to attach new permissions.

For Help, please visit go/selfserviceiamtldr

Search Your Application Roles *

Selected Role Information

No Role is selected for display.

Next

Approve
safe requests
automatically
with Zelkova



Auto-approval probes can be **selectively** applied

```
- Action:
    - sqs:GetQueueAttributes
    - sqs:GetQueueUrl
    - sqs:SendMessage
  Effect: Allow
  Resource: 'arn:aws:sqs:*:*:metrics'
```

Request Review for: arn:aws:iam::985081345396:role/happy-crawfish

User	Curtis Castrapel - curtis@example.com
Request Time	10/19/2020, 2:24:44 PM
Title	AWS Architect
Manager	Head Honcho - salaryraiser@example.com
User Justification	Just testing
Status	pending
ARN	arn:aws:iam::985081345396:role/happy-crawfish
Last Updated	10/19/2020, 2:25:01 PM
Cross-Account	True

Reviewer Instructions

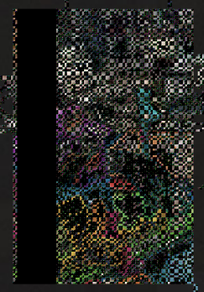
Please review each change in this request carefully. Reviewers can selectively apply, modify, cancel individual changes, or reject the entire request. Requesters can modify, cancel individual changes, or cancel their entire request. This page does not provide a button for reviewers to approve all changes in a request because each individual change should be carefully reviewed.

Inline Policy Change - cm_ccastrapel_1603142684_kywt - New Policy

Current Policy

Proposed Policy

A policy editor for **all** of your IAM roles, SQS queues, SNS topics, and S3 buckets



Edit Policy for arn:aws:iam::844240725092:role/consolemetarget

Delete

Account	consoleme-oss-1 (844240725092)
Amazon Resource Name	arn:aws:iam::844240725092:role/consolemetarget
Resource type	IAMROLE
Resource name	consolemetarget
CloudTrail Events	Link
S3 Access Log	Link
Config Timeline	Link
Created on	09/24/2020, 07:50:00 AM
Last updated	10/10/2020, 11:48:38 PM
Templated	False

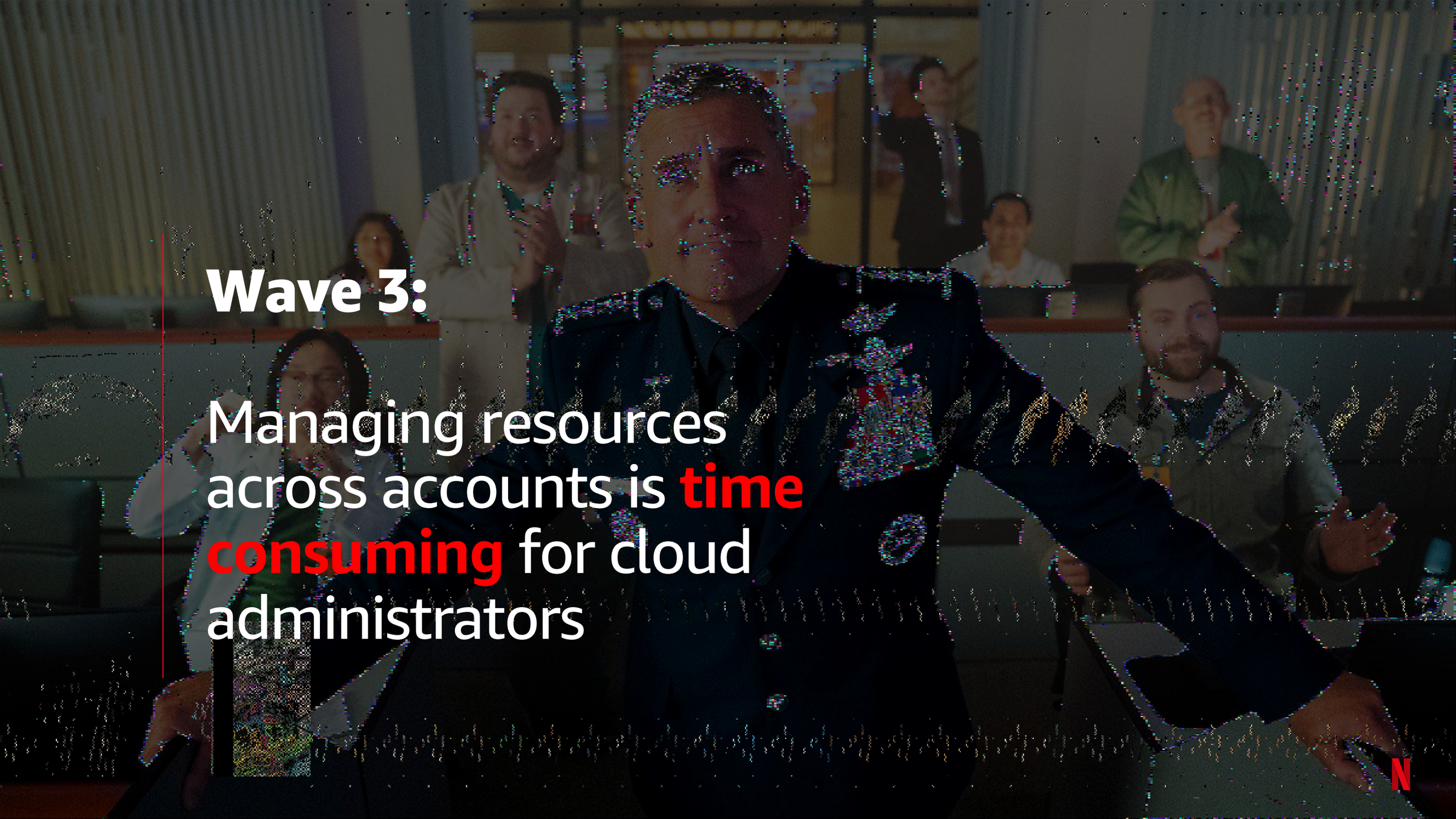
Inline Policy 1 | Assume Role Policy | Managed Policy | Tags | Issues 1

Inline Policies

You can add/edit/delete inline policies for this role from here. Please create a new policy by using the buttons on the right.

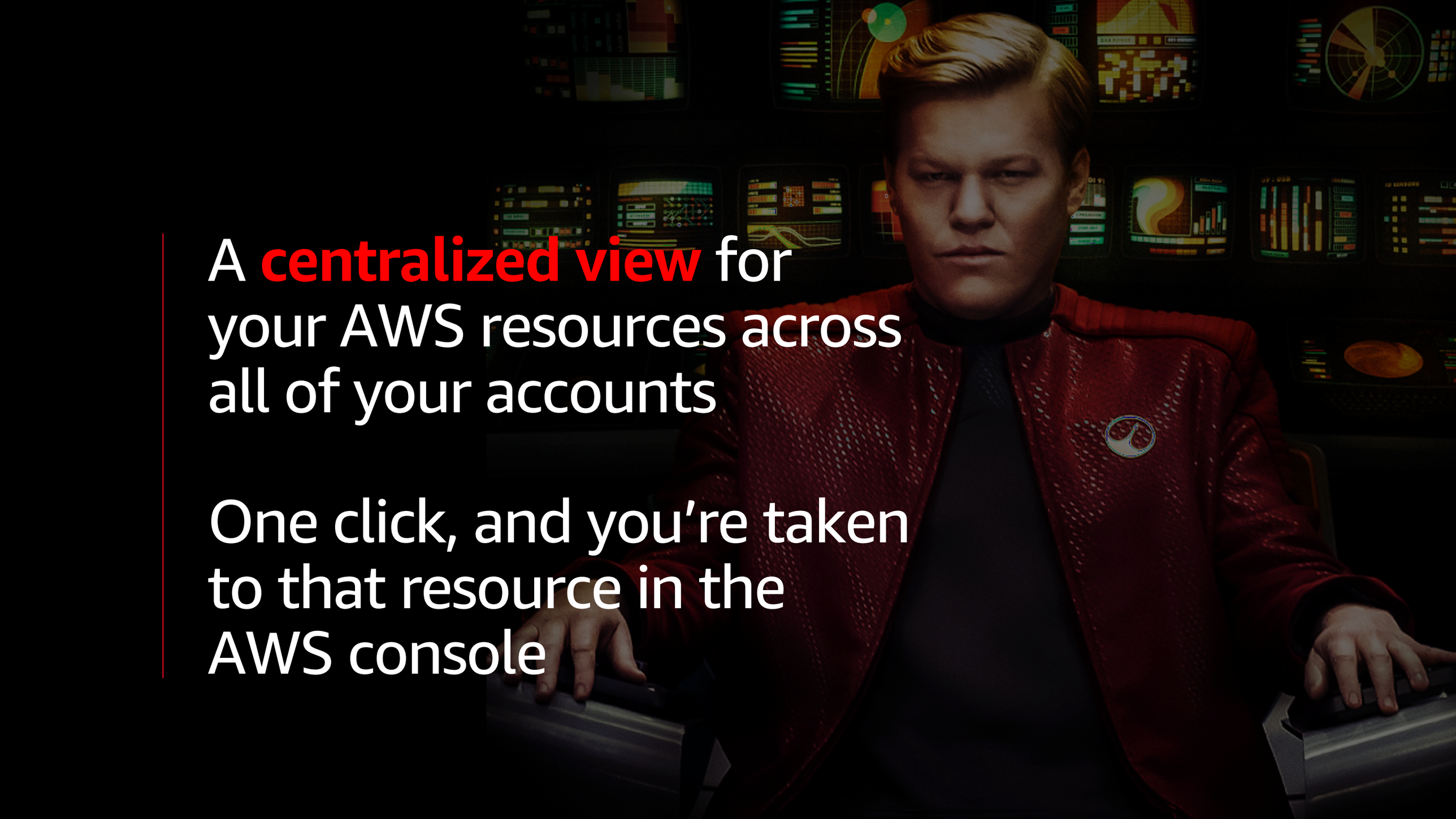
Create New Inline Policy or Policy Wizard

▼ ConsoleMeTargetPolicy



Wave 3:

Managing resources across accounts is **time consuming** for cloud administrators

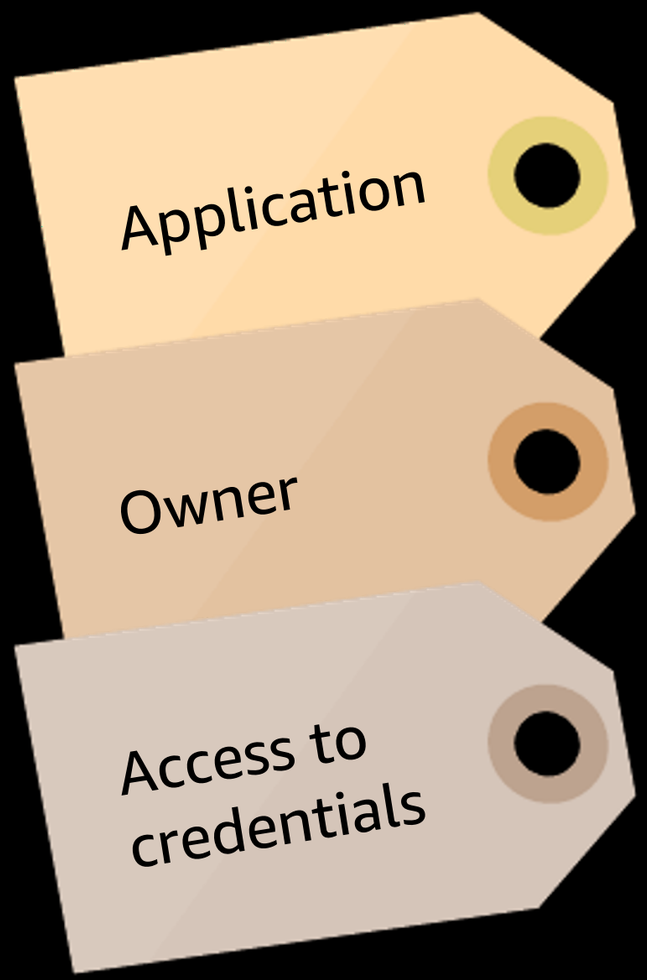

A centralized view for your AWS resources across all of your accounts
One click, and you're taken to that resource in the AWS console

Policies

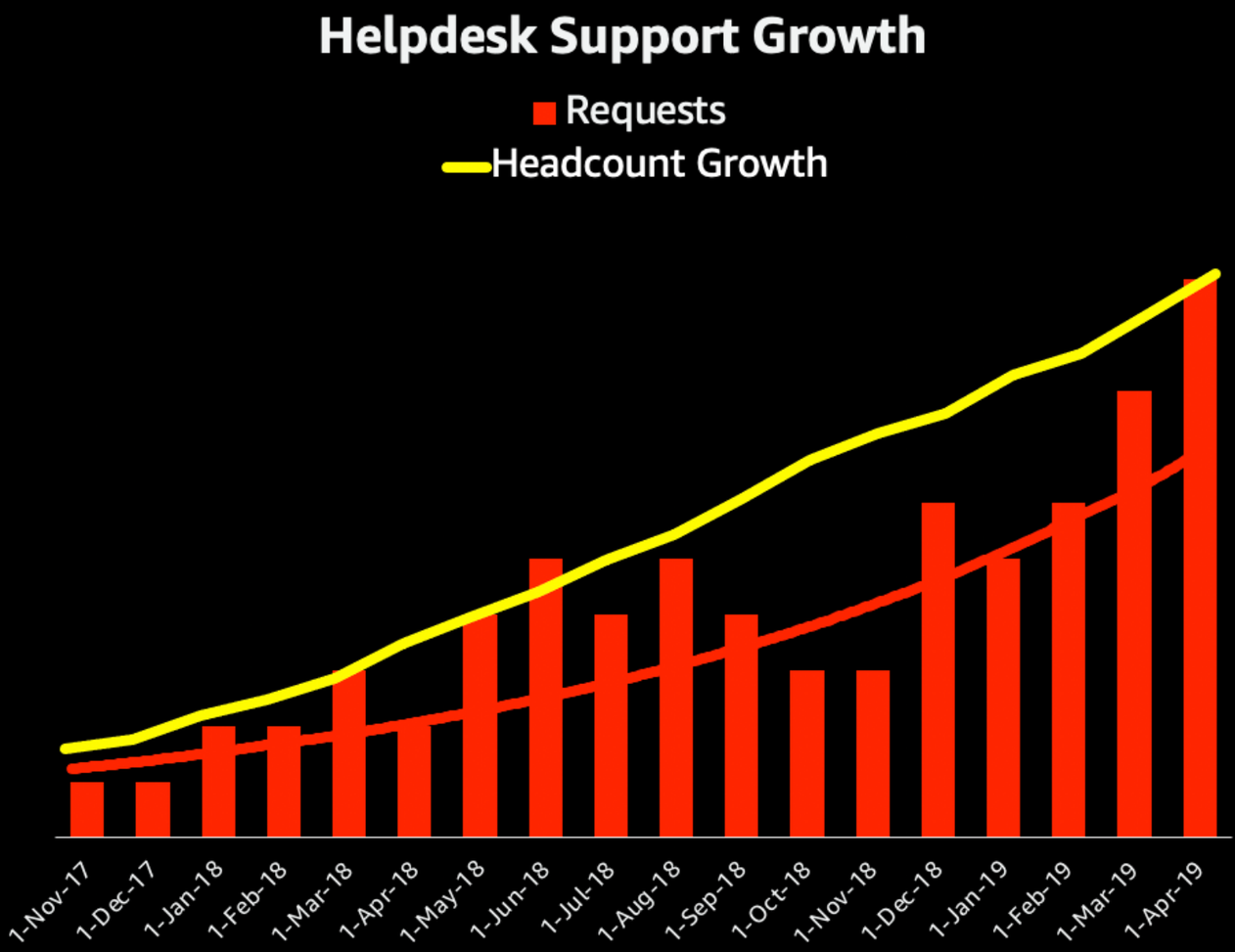
View all of the AWS Resources we know about.

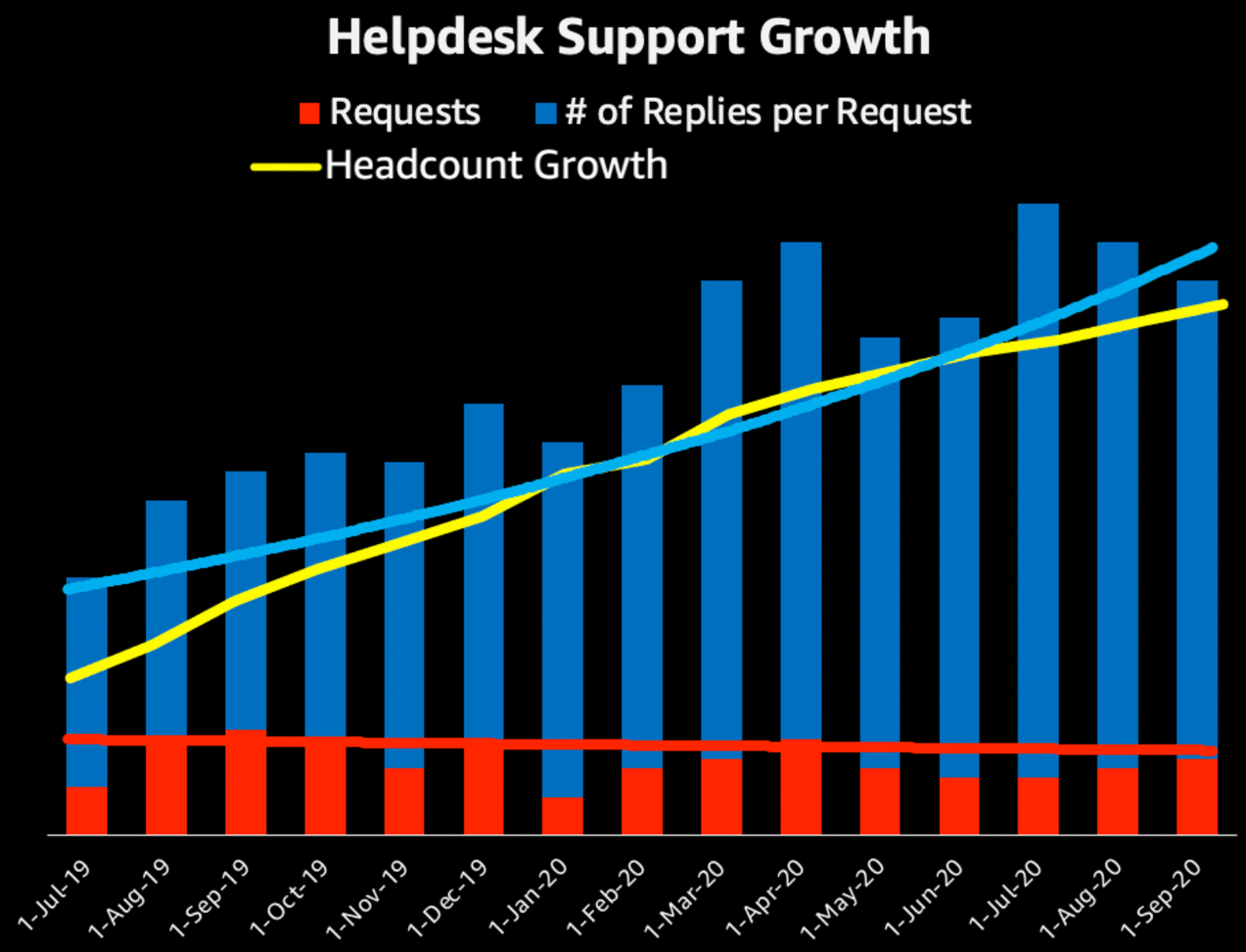
Account ID	Account	Resource	Tech	Template	Errors
985081345396	consoleme_oss_2_test	arn:aws:iam::985081345396:role/genuine-bluebird	iam	N/A	0
985081345396	consoleme_oss_2_test	arn:aws:iam::985081345396:role/consoleme_oss_2_test_admin	iam	N/A	0
844240725092	consoleme_oss_1_test	arn:aws:iam::844240725092:role/stable-cheetah	iam	N/A	0
985081345396	consoleme_oss_2_test	arn:aws:iam::985081345396:role/fond-longhorn	iam	N/A	0
844240725092	consoleme_oss_1_test	arn:aws:iam::844240725092:role/powerful-anteater	iam	N/A	0
844240725092	consoleme_oss_1_test	arn:aws:iam::844240725092:role/causal-finch	iam	N/A	0
985081345396	consoleme_oss_2_test	arn:aws:iam::985081345396:role/emerging-hedgehog	iam	N/A	0
844240725092	consoleme_oss_1_test	arn:aws:iam::844240725092:role/prime-quagga	iam	N/A	0
985081345396	consoleme_oss_2_test	arn:aws:iam::985081345396:role/aws-service-role/support.amazonaws.com/AWSServiceRoleForSupport	iam	N/A	0
985081345396	consoleme_oss_2_test	arn:aws:iam::985081345396:role/pleasing-peacock	iam	N/A	0
844240725092	consoleme_oss_1_test	arn:aws:iam::844240725092:role/neutral-chimp	iam	N/A	0
985081345396	consoleme_oss_2_test	arn:aws:iam::985081345396:role/proven-herring	iam	N/A	0
985081345396	consoleme_oss_2_test	arn:aws:iam::985081345396:role/modern-grubworm	iam	N/A	0
844240725092	consoleme_oss_1_test	arn:aws:iam::844240725092:role/suitable-lemming	iam	N/A	0
985081345396	consoleme_oss_2_test	arn:aws:iam::985081345396:role/adjusted-mammoth	iam	N/A	0

Resource tags make authorization decisions **easy** to reason about



Now it’s time to focus on more **complex** requests






Now open source!
github.com/Netflix/consoleme
github.com/Netflix/weep

Thank you!



Special thanks to: Hee Won Kim, Patrick Sanders, Srinath Kuruvadi, Jay Dhulia, Kinnaird McQuade, Cloud Infrastructure Security Team at Netflix, InfoSec at Netflix, and our AWS partners

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.


RATED TV-MA
language, smoking, animal harm



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.