
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SPACE SECURITY PRIVACY ASSURANCE CORPORATE ENGINEERING | NETFLIX

NFX305

Reimagining multi-account deployments for security and speed

Joseph Kjar (he/him)
Sr. Security Software Engineer
Netflix

Patrick Sanders (he/him)
Sr. Security Software Engineer
Netflix

Prateek Sharma (he/him)
Sr. Solutions Architect
AWS

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

A brief history of AWS at Netflix

Revisiting multi-account

A neat idea

Making it real

The outcomes

Looking forward

Q&A

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A brief history of AWS at Netflix

We've been around since the dinosaurs roamed the untamed wilds of Amazon EC2 classic

Our early growth happened in a single account

We tried a massively multi-account approach . . . and learned a lot

We spearheaded efforts to make least privilege possible in large accounts





aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why multi-account?

Operational risks

Security risks

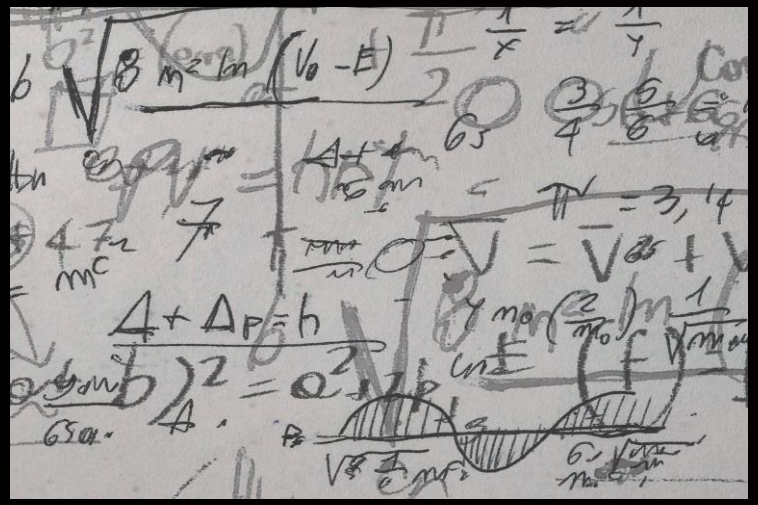
Developer experience

Best practices

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Revisiting multi-account

Understand the challenges







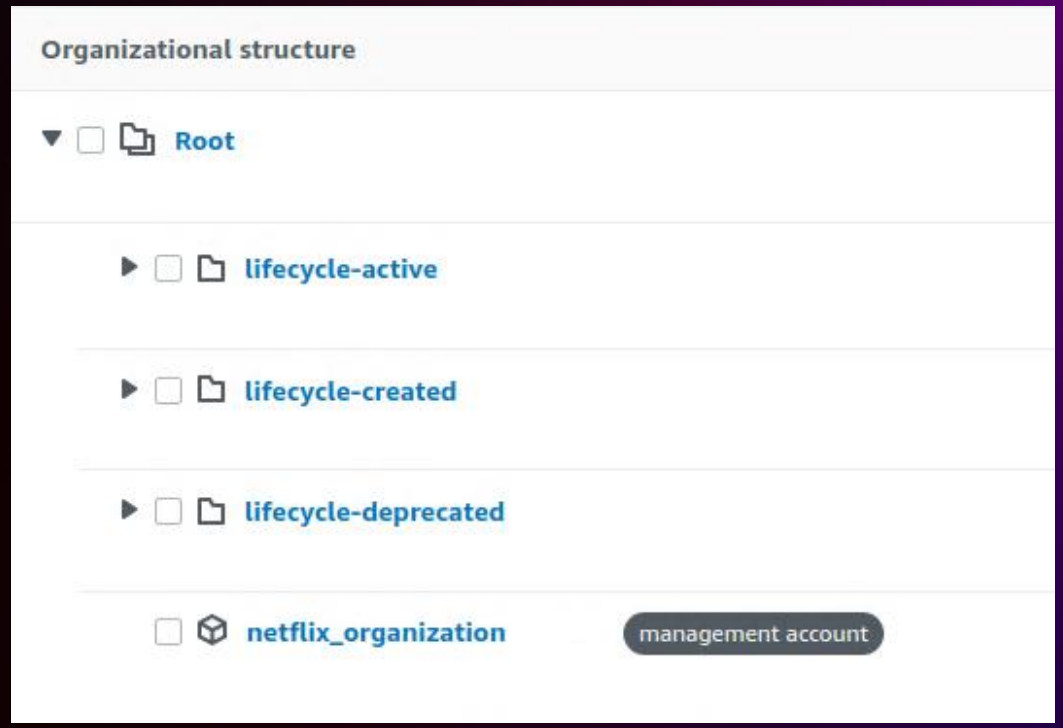
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Revisiting multi-account

Establish a robust account lifecycle

- Account provisioning
- Account vending
- Complementary systems: IAC, account inventory, AWS Organizations

Optimize for long-term security and manageability



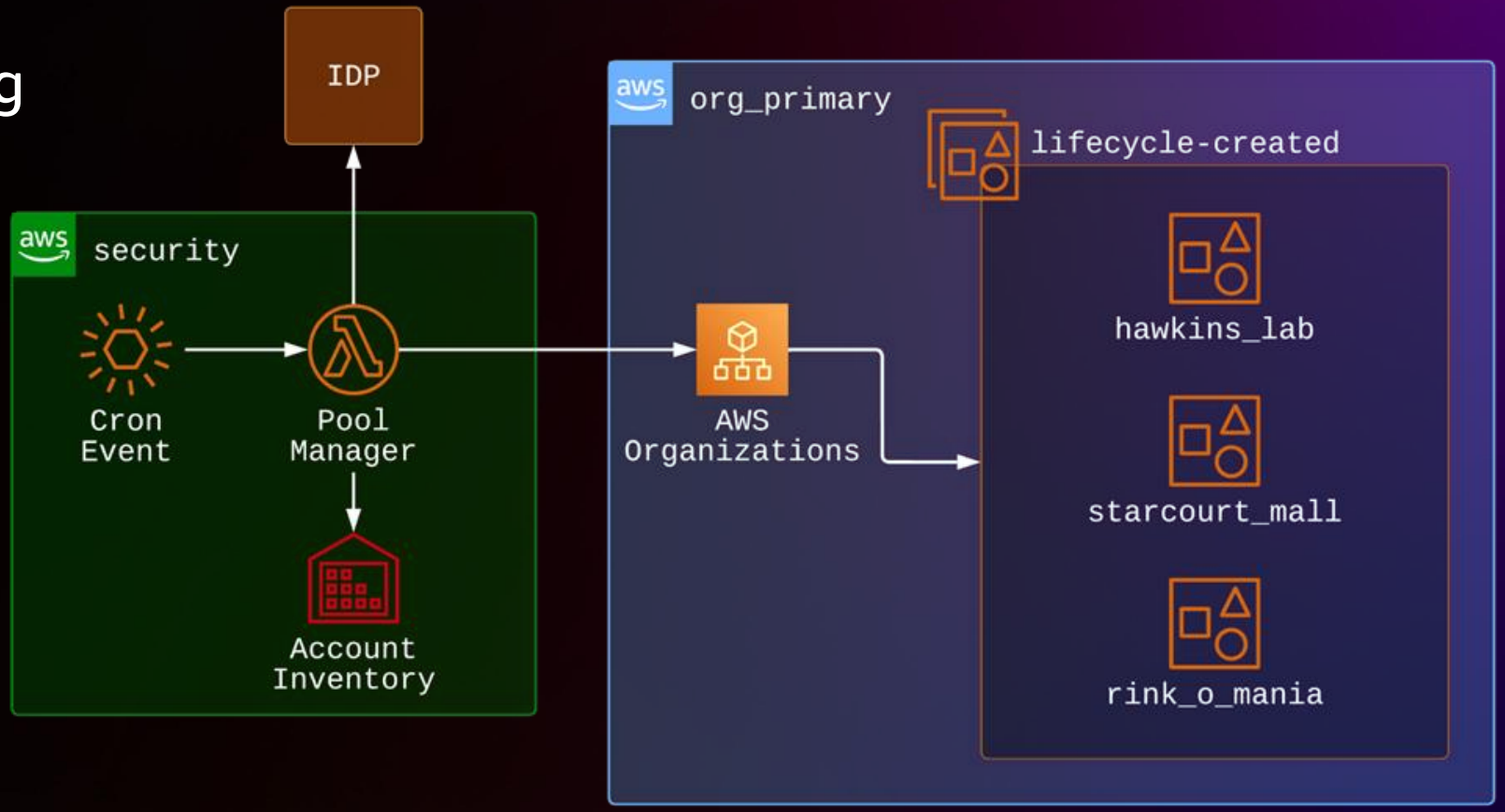
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Account provisioning

Maintain a pool of pre-provisioned accounts

Minimal resource provisioning

- Admin roles
- AWS CloudTrail
- AWS Config
- Event forwarding
- Amazon security services



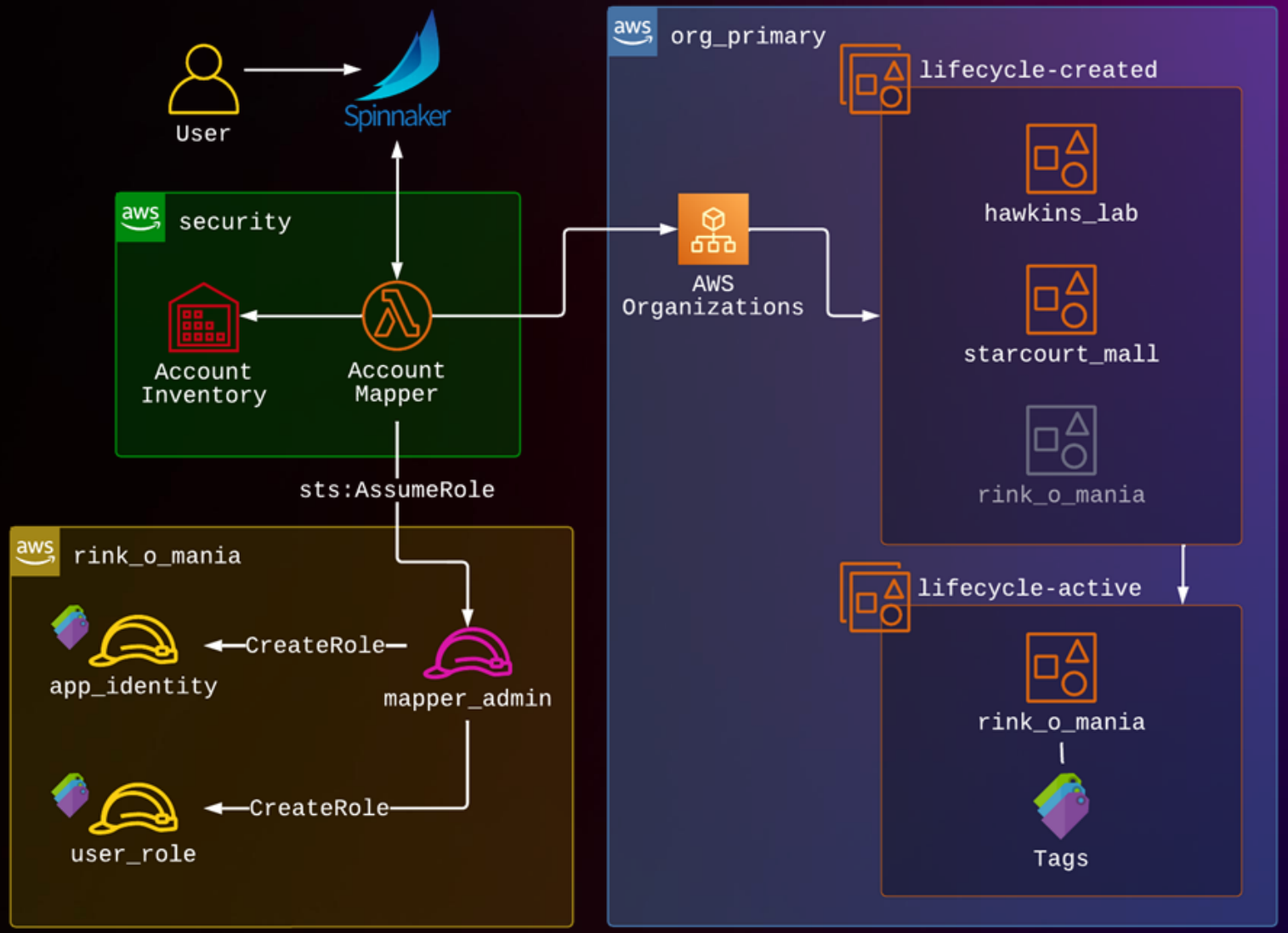
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Account vending

We use an AWS Lambda function to vend accounts to customers on demand

Two critical duties:

1. Assign an account
2. Provision roles for the app and owner



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Options, options

VPC peering to extend our flat network

Transit gateways

VPC sharing

Security lockdown

Sandbox model

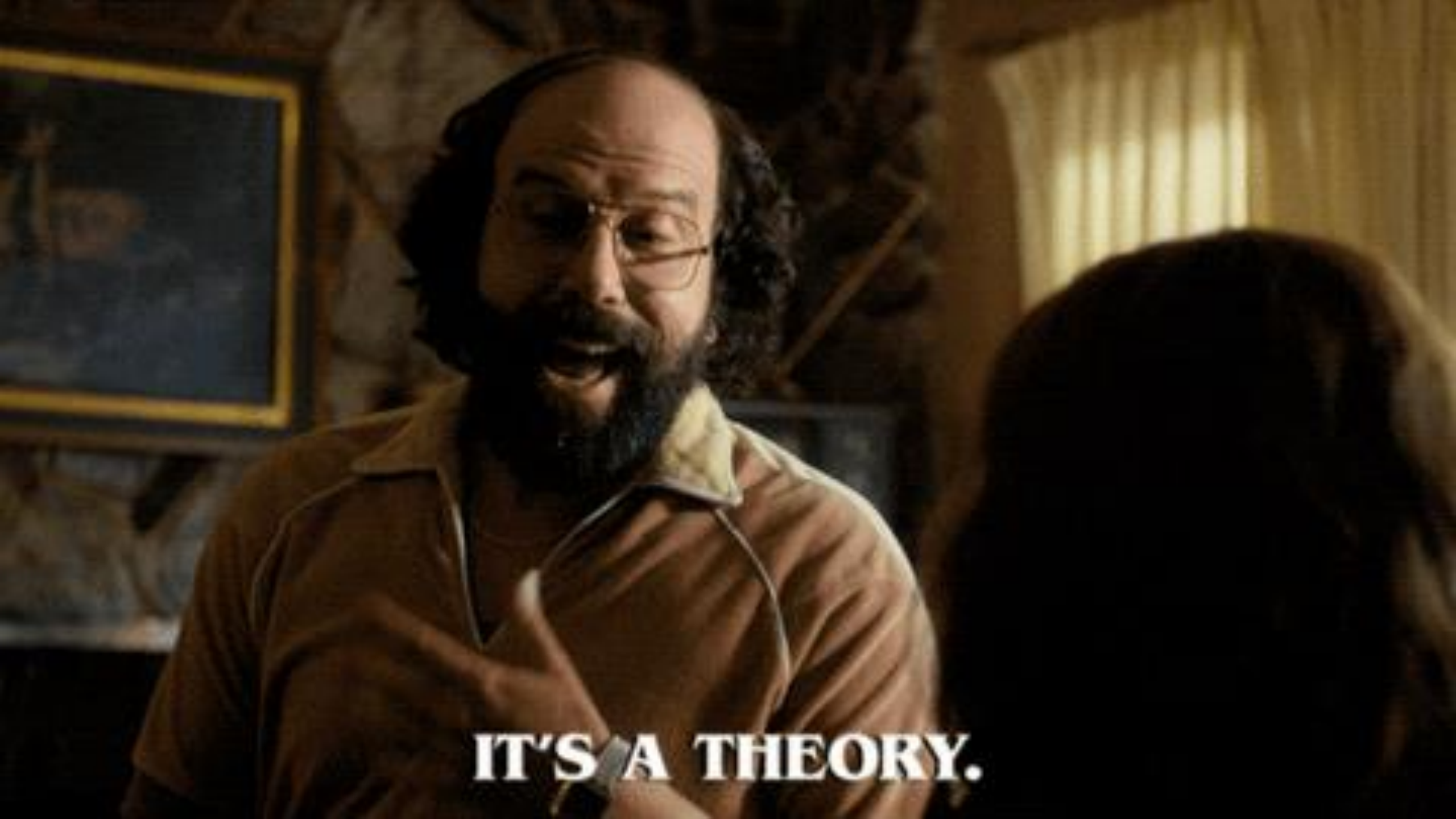
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.


NETFLIX
Everybody start thinking outside the box.

Why does an application's IAM role have to be bound to the underlying cloud infrastructure?

. . . Because it's always been that way

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.


IT'S A THEORY.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

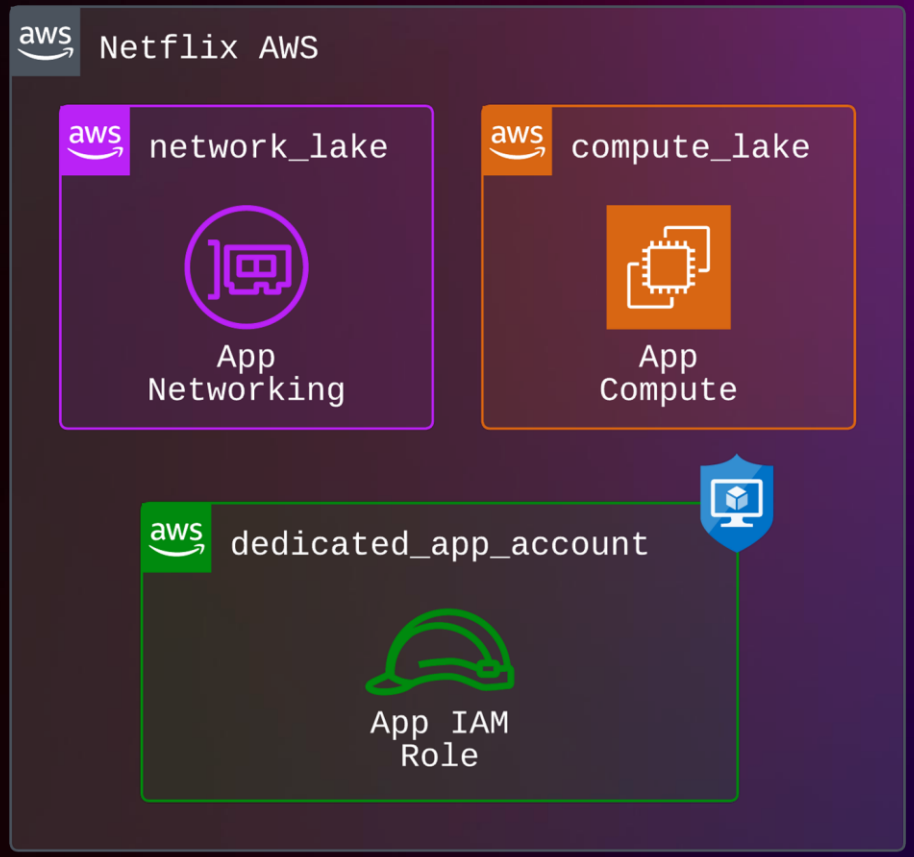


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A neat idea

Our dream: Decouple each application's cloud identity (IAM role) from its network, compute, and other platform resources

A workload's identity becomes its sandbox



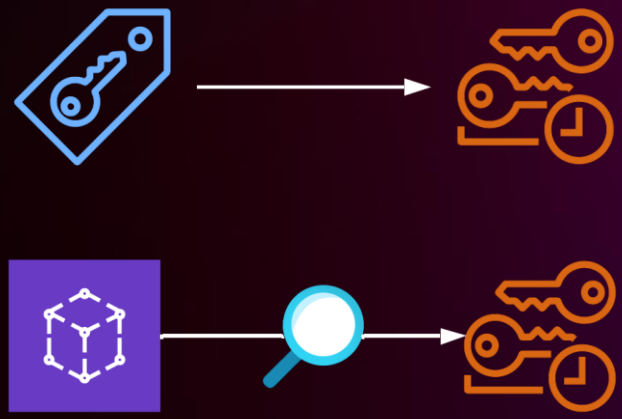
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A neat idea

Two big obstacles

1. Credential exchange

2. Credential delivery



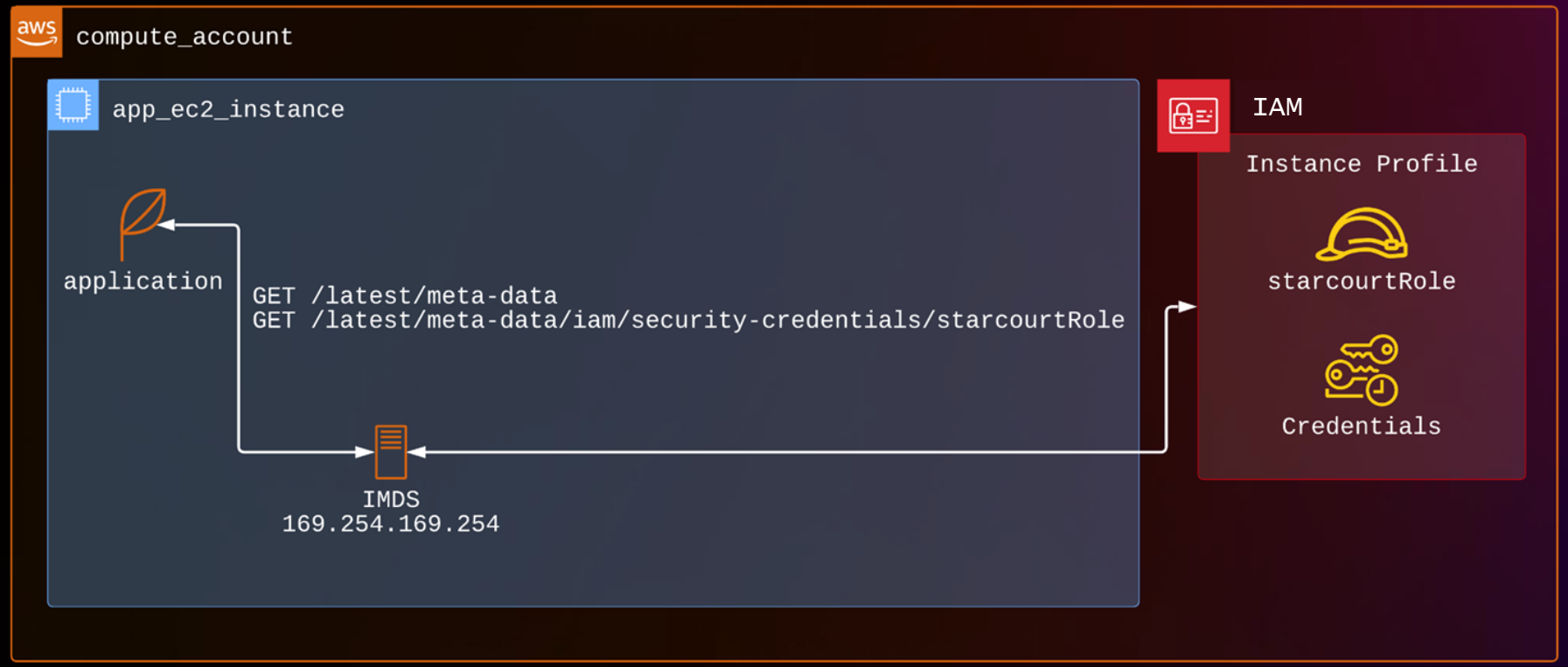
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Credential exchange

How compute services and IAM work in AWS today

The Instance Metadata Service (IMDS)



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

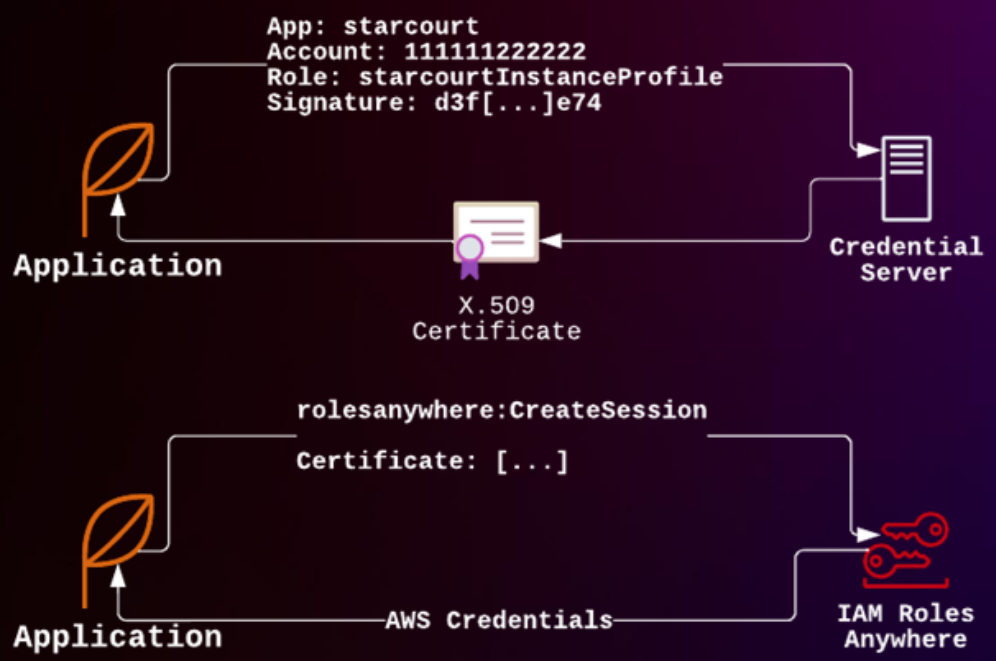
Credential exchange

Exchanging workload identity for AWS IAM credentials

OIDC



IAM Roles Anywhere



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Credential delivery

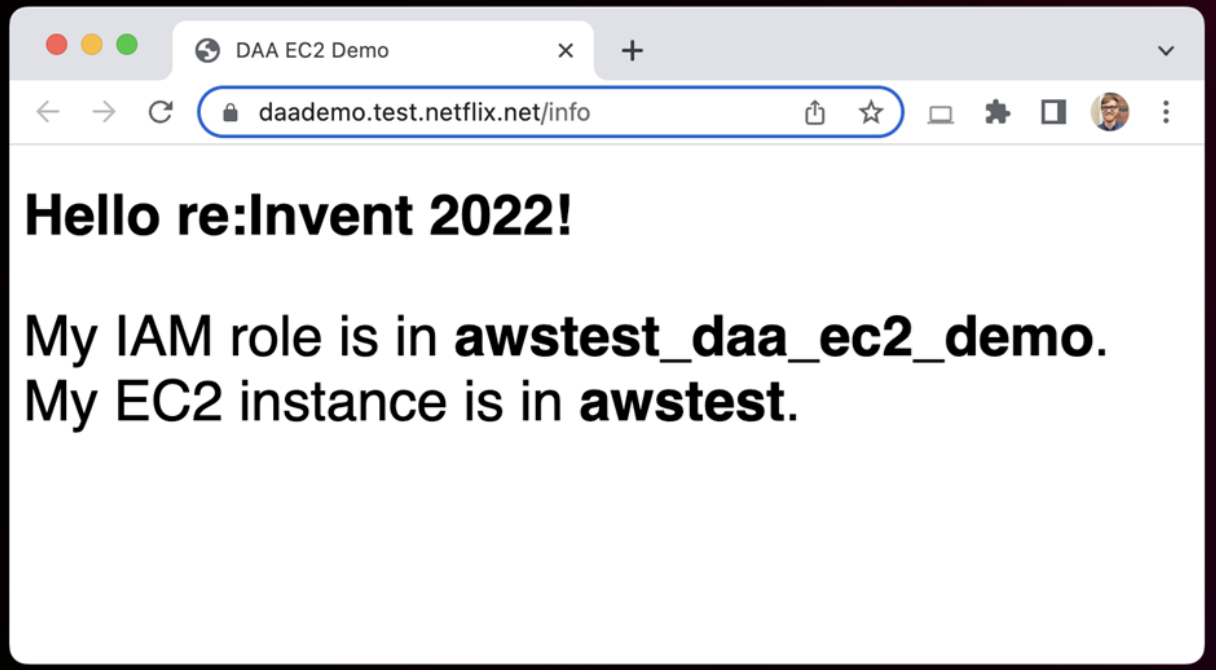
Facilitating credential discovery with an IMDS proxy



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Making it real

Putting it all together



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The outcomes

Robust security isolation and reduction of scope of impact

Maximum flexibility for other architectures

Relief from a variety of rate limits and service quotas

Scalable, simplified permissions management

Improved developer productivity

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What this does not do

Prevent network-based lateral movement

Prevent abuse of shared cloud resources

Prevent abuse of your app accounts

Protect against events on centralized control planes (e.g., container escapes)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Looking forward

Migration strategy

Check out recording of NFX302!

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Special thanks

Steven Reiling

AWS Account Team

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Joseph Kjar

linkedin.com/in/joseph-kjar
@josephkjar@infosec.exchange
jkjar@netflix.com

Patrick Sanders

@patricksanders@infosec.exchange
psanders@netflix.com

Prateek Sharma

prshaz@amazon.com



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.