AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

SEC316-R2

Managing temporary elevated access to your AWS environment

Kevin Higgins
Principal Cloud Architect,
Professional Services
AWS

Bikash Behera
Principal Solutions Architect,
Global Financial Services
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

What is the problem we are trying to solve?

What is temporary elevated access?

Why use temporary elevated access?

Guidance for using temporary elevated access

Implementing temporary elevated access

A minimal reference implementation

Demo

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is the problem we are trying to solve?

- Access is granted once and reviewed periodically
- Persistent access/standing access/always-on access
- May provide high-risk access
- High-risk access is not justified, reviewed, and audited

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is temporary elevated access?

- The goal is to ensure that each time a user invokes high-risk access, there is an appropriate business reason for doing so
- Access is only granted if the business reason is appropriate
- The scope and duration of access granted is aligned to the business reason

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why use temporary elevated access?

- High-risk access is granted only if there is a valid business reason
- Increases visibility to reviewers and auditors
- A reminder to be vigilant
- Reporting, analytics, and continuous improvement

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Guidance for using temporary elevated access

- You can use temporary elevated access to mitigate risks related to human user access that your organization considers high risk
- While this can reduce risk, the preferred approach is to automate your way out of needing human access in the first place
- Use temporary elevated access only for infrequent activities that cannot yet be automated

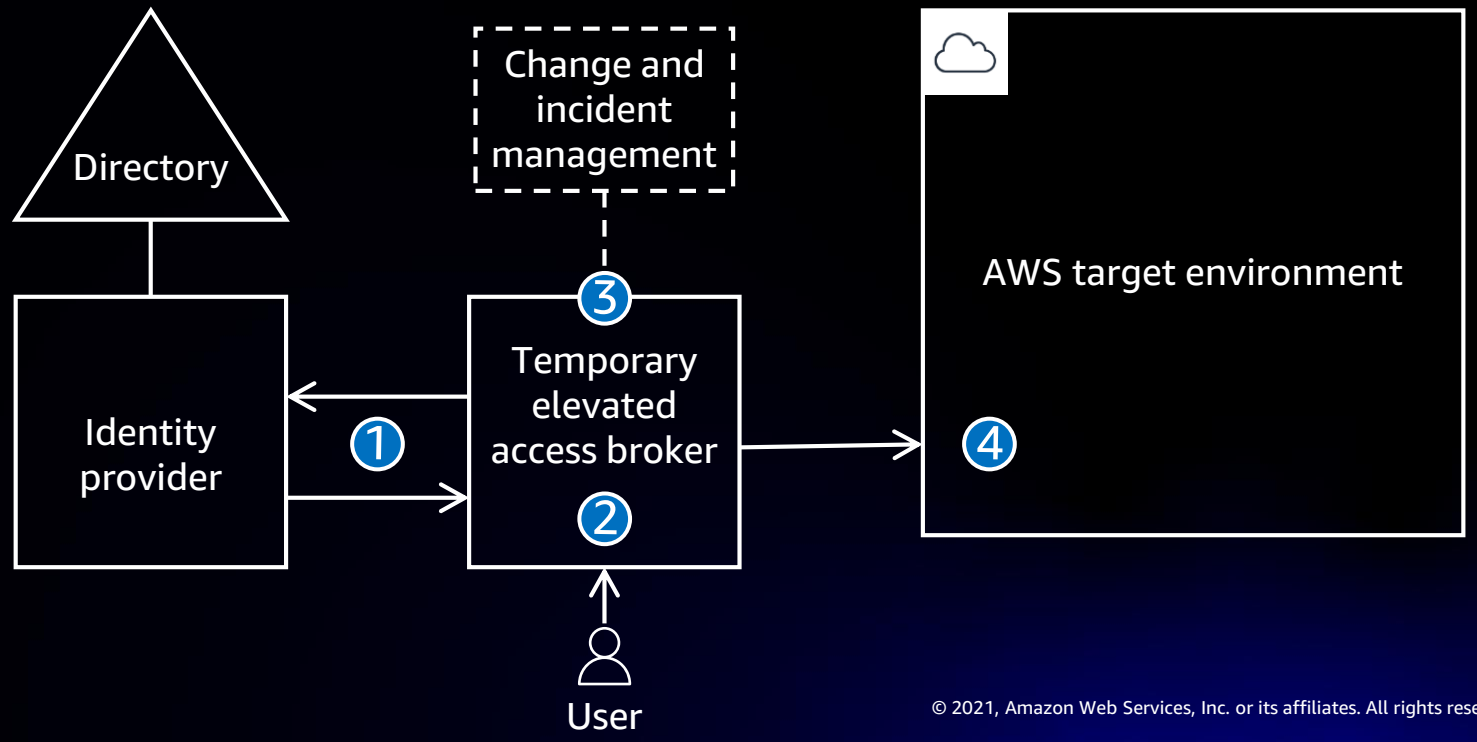
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Implementing temporary elevated access

- A typical implementation involves placing an additional component between your identity provider and the AWS environment your users need to access
- We refer to this as a temporary elevated access broker

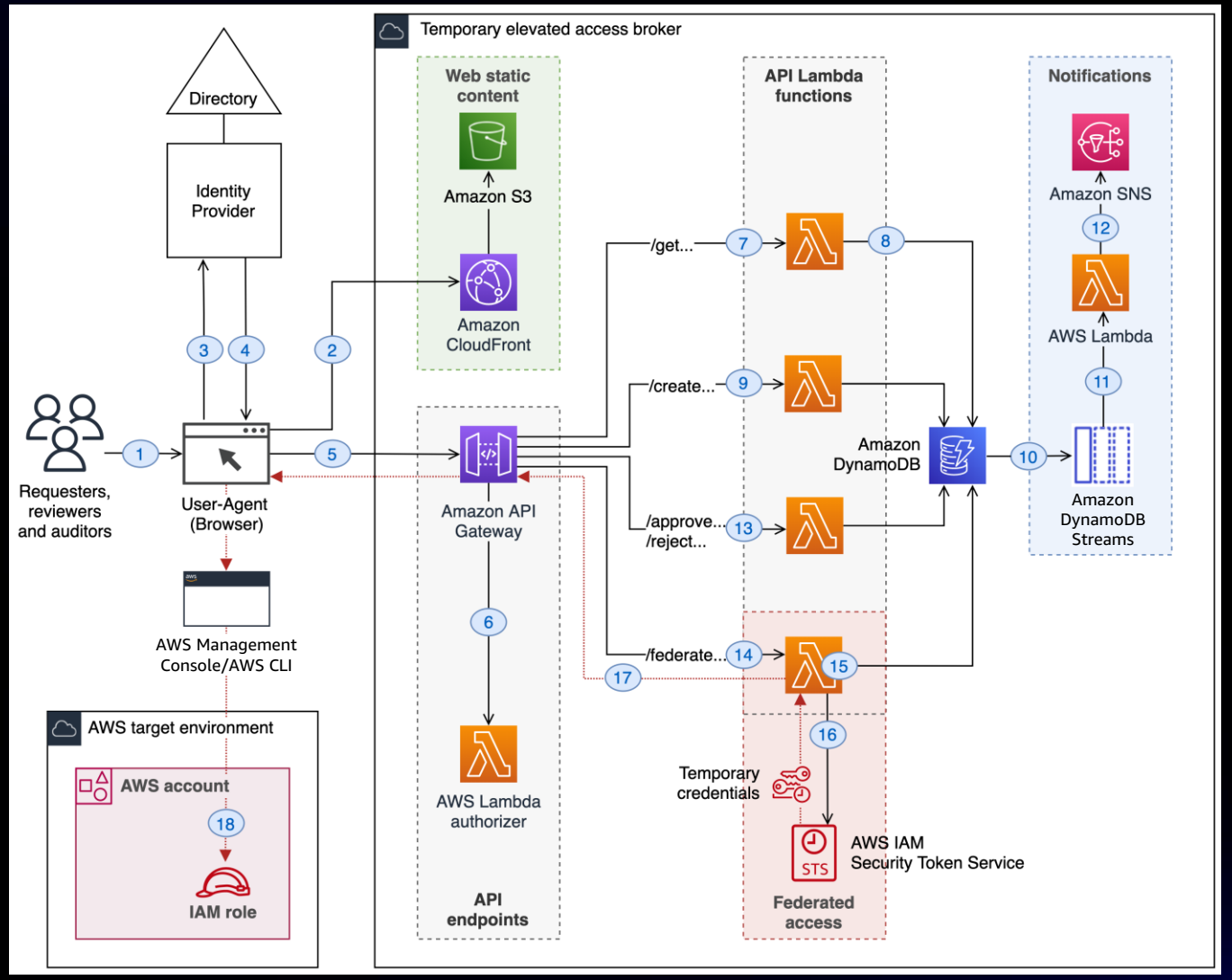
High-level process flow

1. Authenticate user and determine eligibility
2. Initiate request for access
3. Establish a valid business reason for invoking access
4. Grant time-bound access to your AWS environment



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A minimal reference implementation



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Kevin Higgins
kevhiggi@amazon.com

Bikash Behera
behebika@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.