AWS re:Invent

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

SEC201-R2

Manage and customize service control policies at scale

Cassia Martin
Security Solutions Architect
Amazon Web Services

Matt Luttrell
Solutions Architect, Identity Solutions
Amazon Web Services

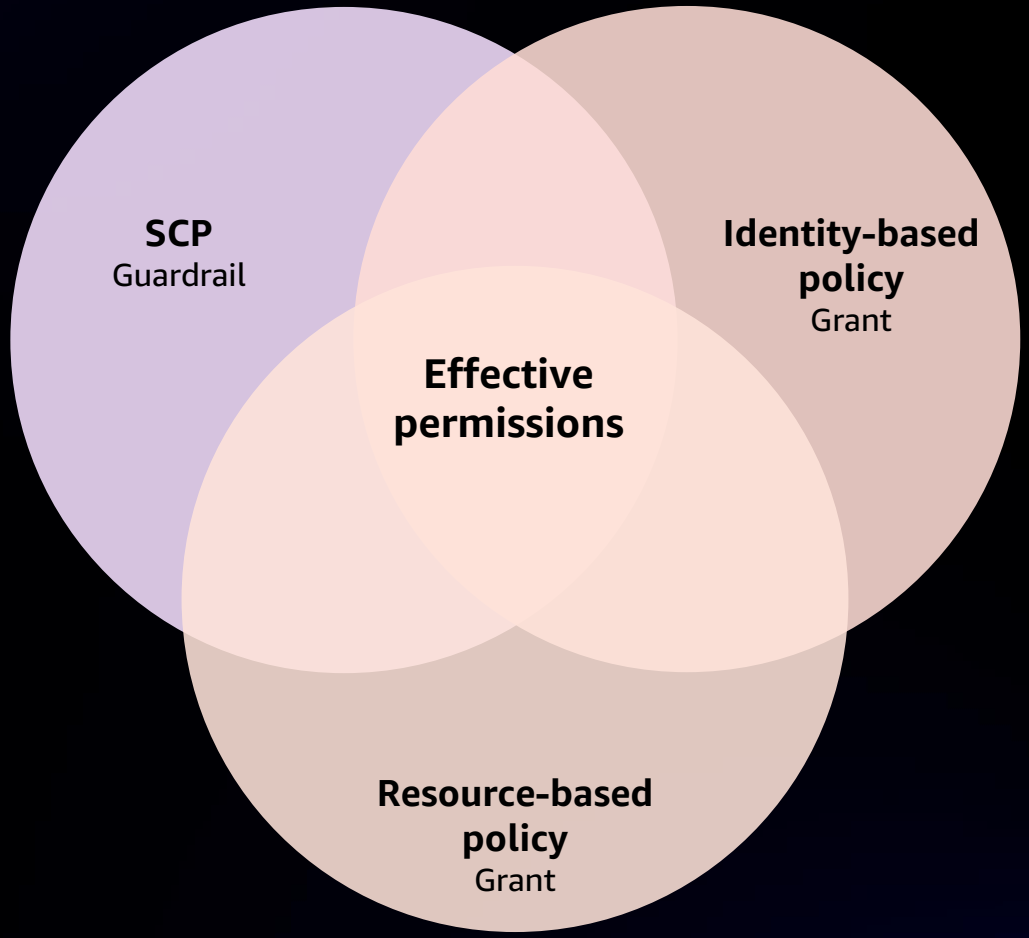
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What are we going to talk about?

- Overview of service control policies (SCPs)
- SCPs and AWS Organizations
- Deploying and testing your SCPs
- Sample SCP exception processes
- Examples of common SCPs

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

SCPs define maximum allowable permissions



* SCPs only affect principals within your organization

aws

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

Structure and contents of an SCP

Element	Purpose	Supported effects
`Effect`	Defines whether the SCP statement allows or denies access to principals in an account	Allow, Deny
`Action`	Specifies AWS service and actions that the SCP allows or denies	Allow, Deny
`NotAction`	Specifies AWS service and actions that are **exempt** from the SCP; used instead of the `Action` element	Deny
`Resource`	Specifies the AWS resource that the SCP applies to	Deny
`Condition`	Specifies conditions for when the statement is in effect	Deny

aws

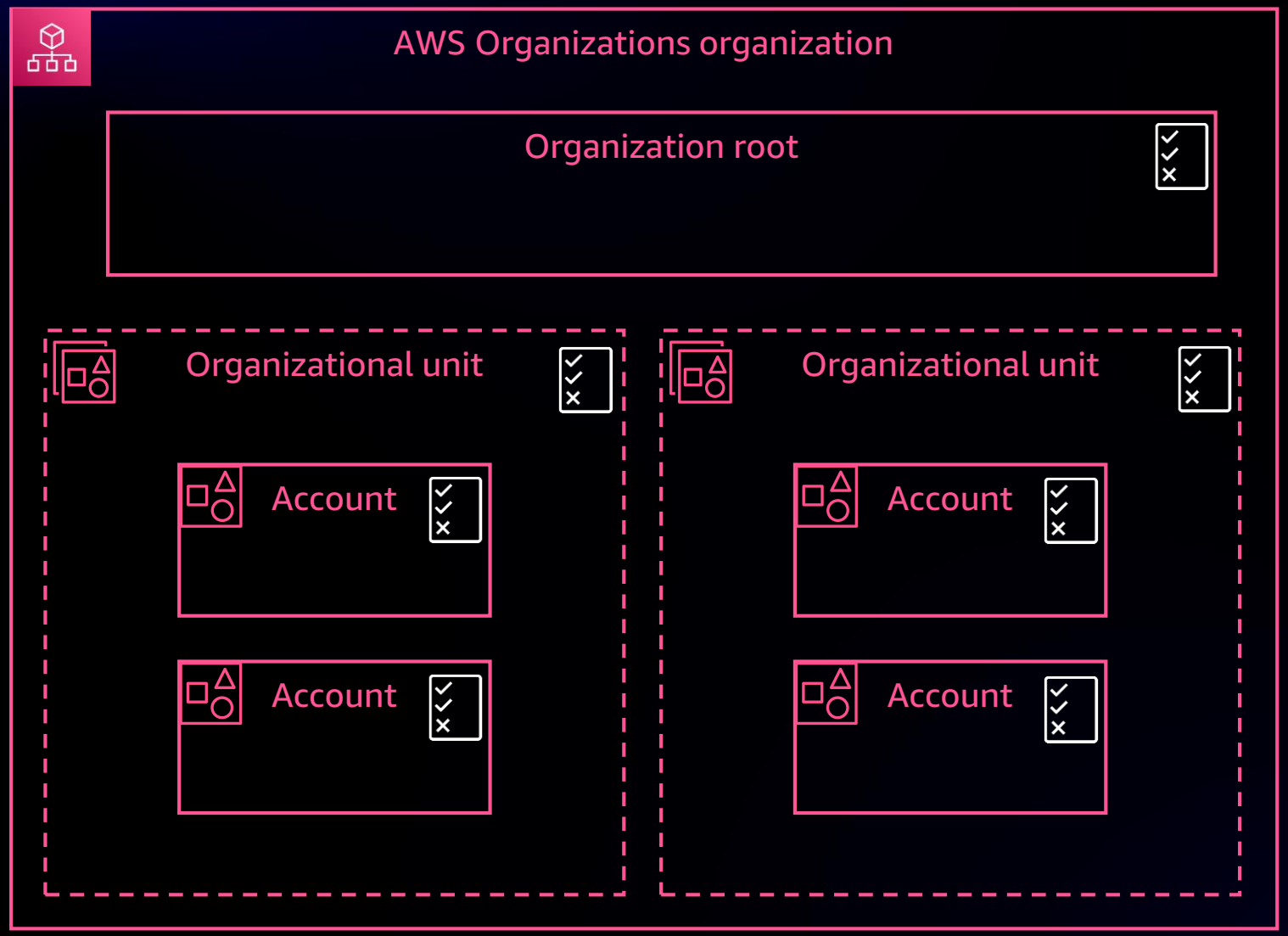
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Example SCP

```
{
    "Effect": "Deny",
    "Action": "cloudtrail:*",
    "Resource": “*”
    "Condition": {
        "ArnNotLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/administrator"
            ]
        }
     }
}
```

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

SCPs and AWS Organizations



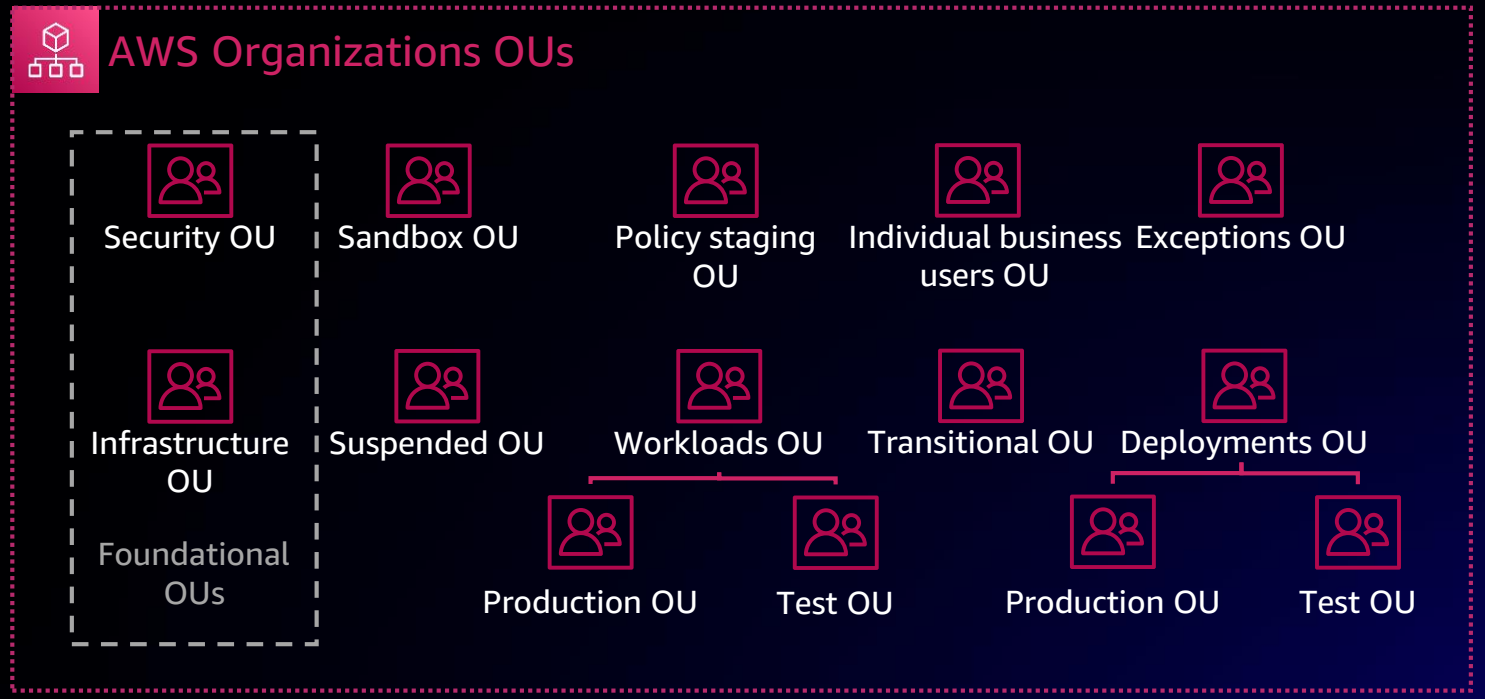
SCPs

- Are used to enforce security invariants
- Act as preventive guardrails for principals in your organization (including root user)

= SCP

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

Recommended organizational unit (OU) structure



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

Discussion

Q: How are you deploying and testing SCPs?

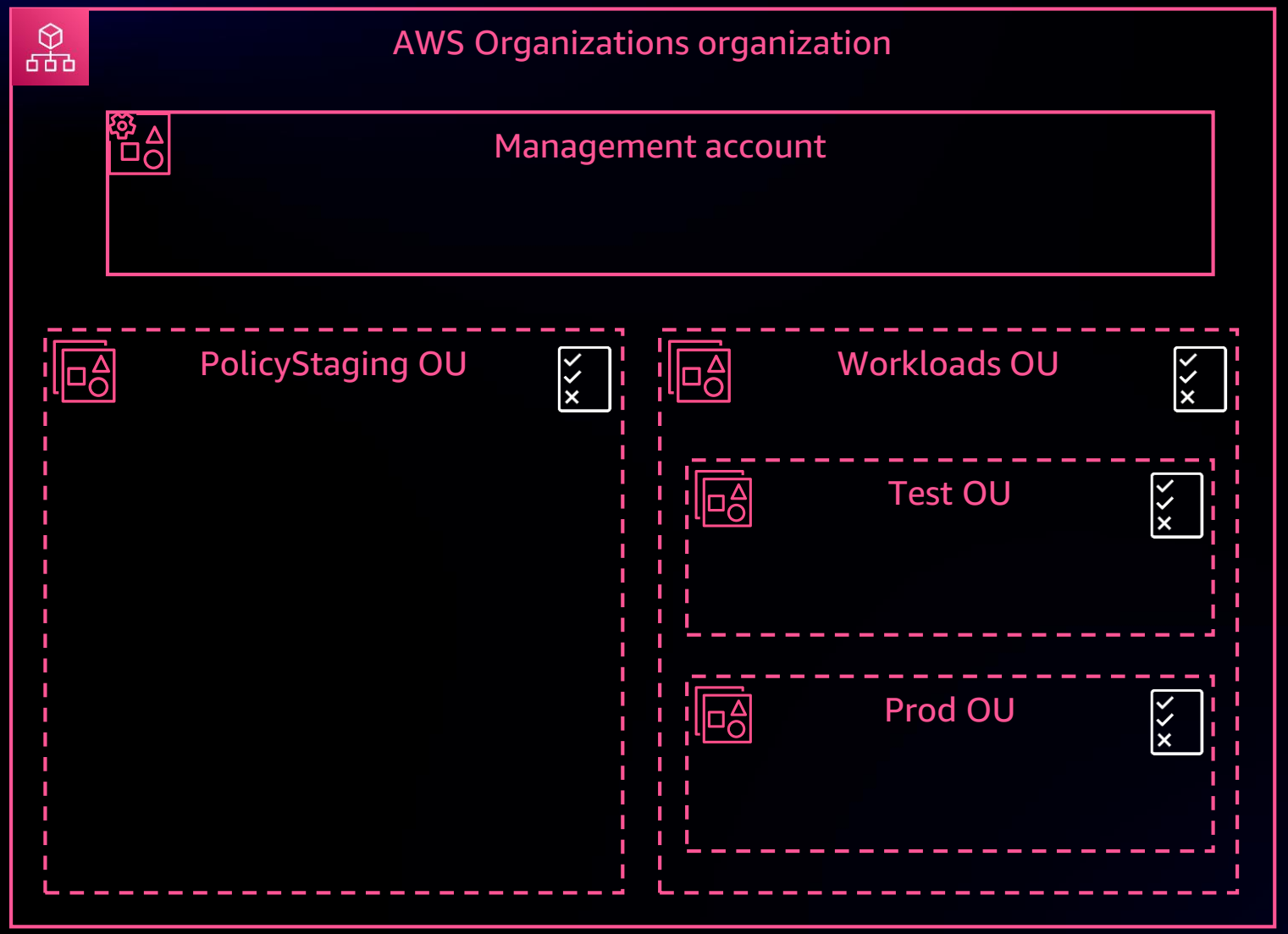
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Some options for deploying SCPs

- AWS Console
- Custom AWS CloudFormation resources
- Scripting with the AWS CLI or SDK
- Customizations for AWS Control Tower

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

Testing your SCPs



Testing lifecycle:

- Attach SCP to `PolicyStaging` OU to validate SCP functionality
- Use a rolling deployment to `Test` OU and `Prod` OU to identity impact on other workloads
- Attach tested policy to the `Workloads` OU and remove policies from `Test` OU and `Prod` OU

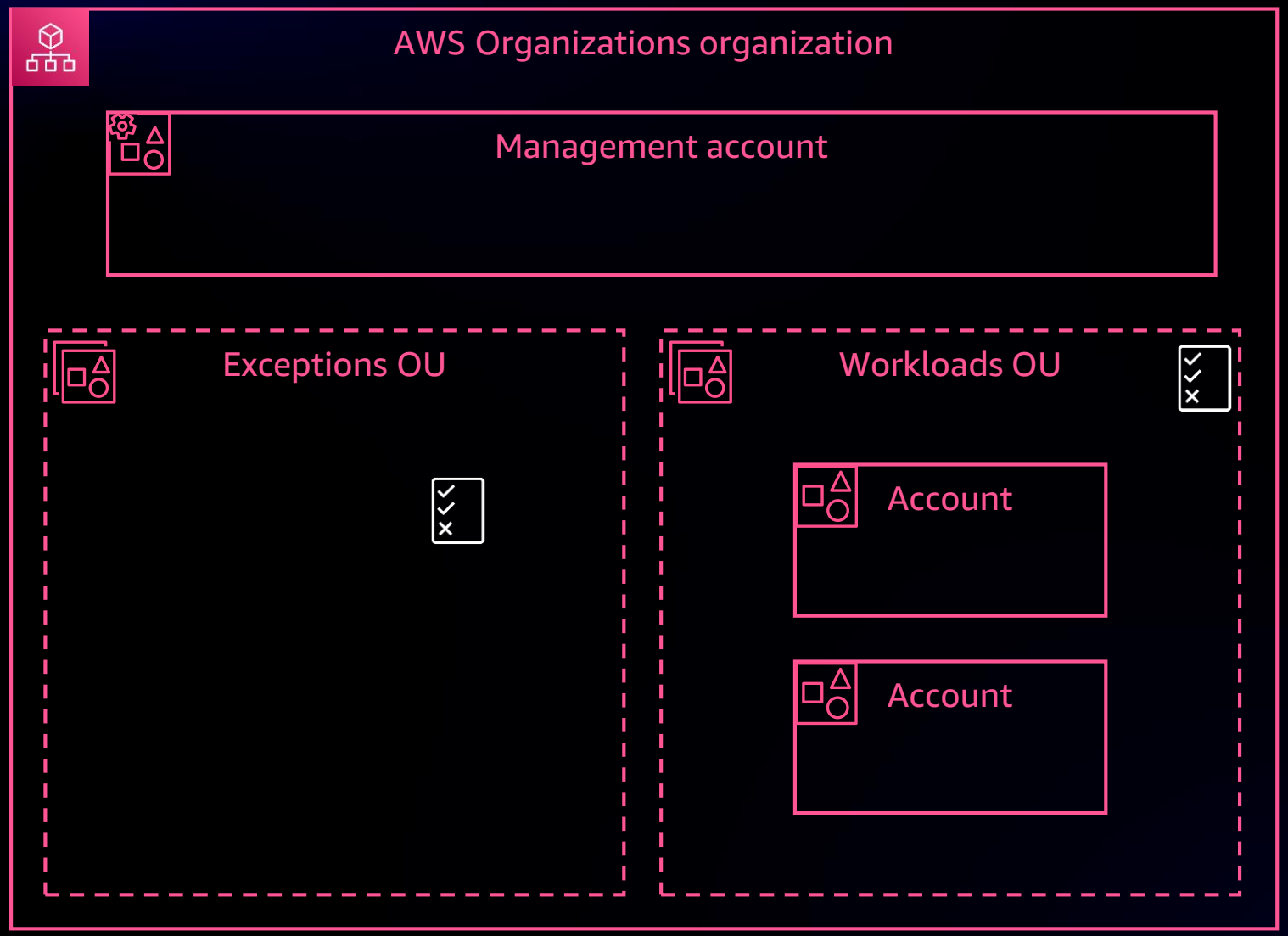
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Discussion

Q: How are you managing SCP exceptions?

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

Managing exceptions



Exceptions OU

- Accounts that require exceptions
- Minimal accounts, if any
- SCPs attached directly to accounts

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

Apply the concepts.

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

Learn more and contribute!

Learn more about SCPs and IAM condition keys

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html

Contribute to open-source repository of permission guardrails

https://aws-samples.github.io/aws-iam-permissions-guardrails/guardrails/scp-guardrails.html

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

Wrap-up

- Reviewed fundamentals of SCPs
- Discussed patterns for testing and deploying SCPs
- Proposed ways to handle exceptions in your SCPs
- Applied learnings through examples

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

Thank you!

Cassia Martin
ccsm@amazon.com

Matt Luttrell
matluttr@amazon.com

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