Managing Organization Policies

Brian Eiler
CLOUD ARCHITECT

www.thecoursewaregroup.com

Overview

Service Control Policies (SCPs)

- Policy Inheritance across Hierarchy
- SCPs vs. IAM Policies
- Policy Structure

Policy Strategy

- Policy Evaluation
- Whitelisting and Blacklisting

Service Control Policies

Service Control Policies: Overview

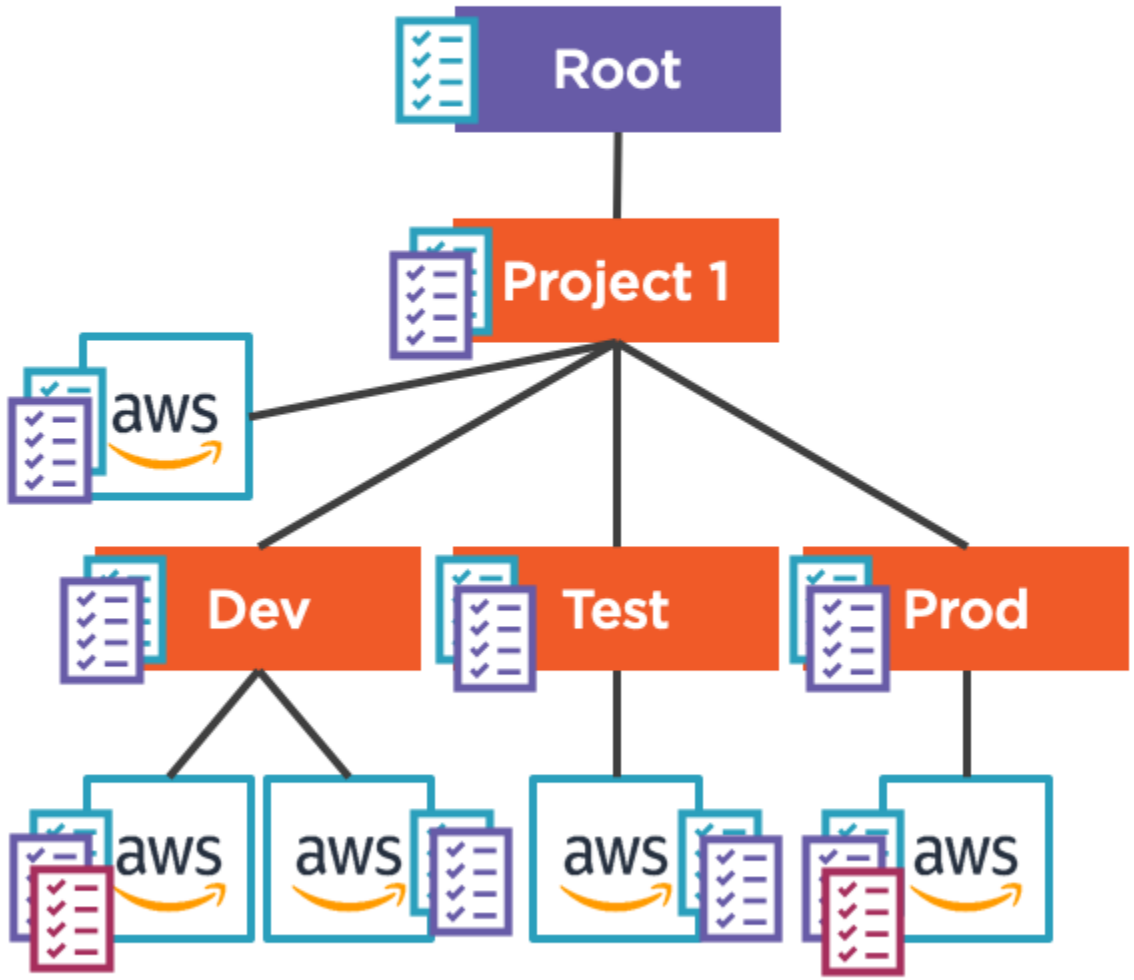
AWS Organizations enable access control at the account level using Service Control Policy (SCP)

These policies are available to an organization with "all features" enabled

Service control policy is the only supported policy type in AWS Organizations

Service Control Policies: Application Levels

Service Control Policies: Inheritance Diagram



Policy applied to a root applies to all entities (OUs and accounts)

Policy applied to an OU applies to all accounts and any child OUs

Policy can be applied directly to a single account

Service Control Policies: Capabilities

Service control policies (SCPs) restrict services and actions for users, groups and roles in the member accounts within an organization

GLOBOMANTICS

"We will certainly use SCPs on OUs and certain accounts directly; but, how do these SCPs compare and integrate with IAM policies?"

SCPs vs. IAM Policies

Service Control Policies	IAM Policies
One single type	Multiple types
Never grants permissions	Grants permissions
Affects users, groups and roles	Affects users, groups and roles
Affects root user in an account*	Does not affect root user in an account

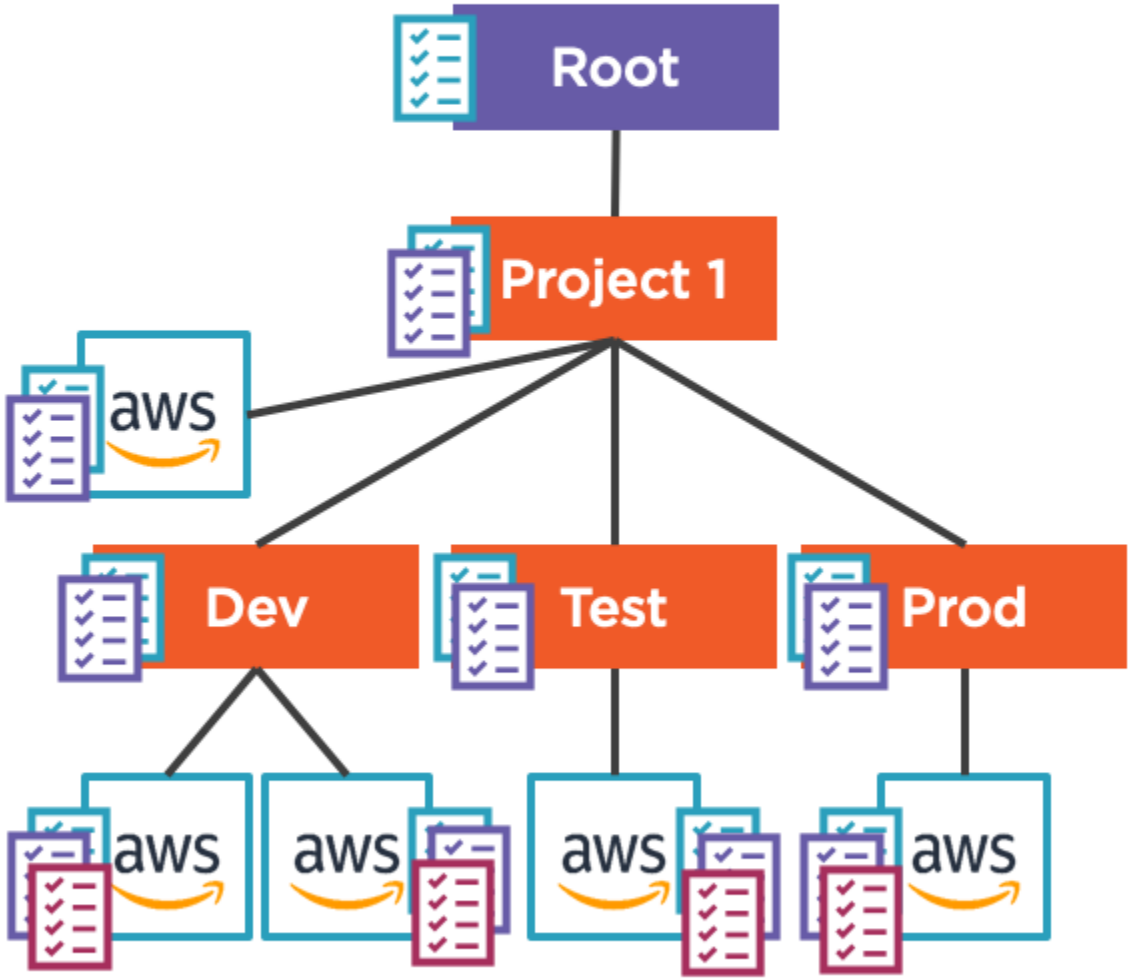
Service Control Policies: Inheritance

SCPs acts as a filter rather than granting permissions

At each level of hierarchy, OUs or accounts inherit permissions or restrictions from its parent

If a permission is blocked at the any level above the account, a user or role in that account cannot use that permission

Service Control Policies: Scenario



S3 Bucket Access	List	Read	Write
	✓	✓	
	✓	✓	
	✓		✓
	?	?	?

Service Control Policies: Interaction with IAM Policies

- **SCPs use the same syntax as IAM policies**
- **Again, SCPs never grant permissions**
- **SCPs set restrictions on what services and actions can be performed by IAM users, groups and roles**
- **IAM policies still need to be assigned to identities to actually perform actions**

Service Control Policies: JSON Structure

```
{   "Version": "2012-10-17",
    "Statement": [
        {   "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*" ],
            "Resource": "*"          }]}
```

GLOBOMANTICS

"Restricting access to the root users in member accounts improves security posture; however, we will have to tightly secure our master account's root user."

Demo

Working with Organization Policies

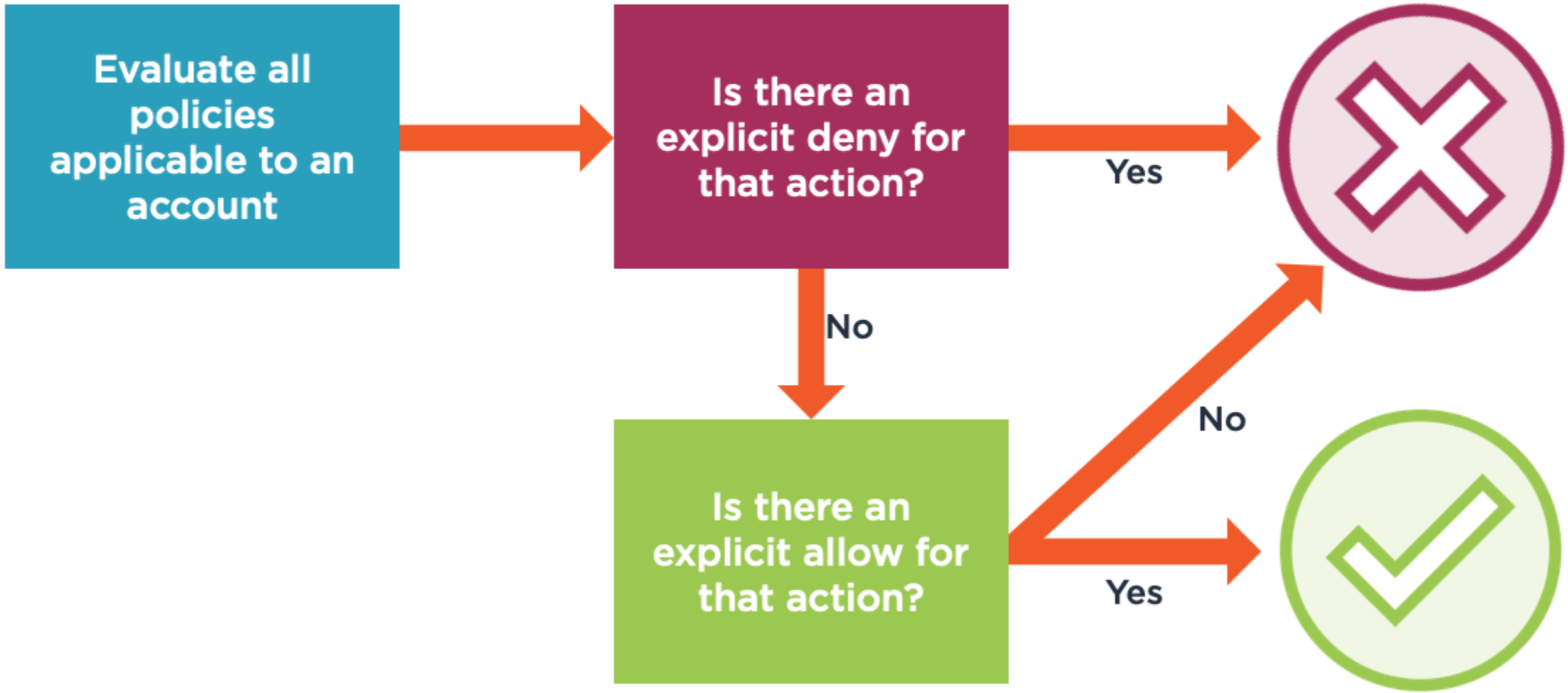
- Create a Service Control Policy (SCP)
- Attach and Detach SCP to the Root, Organization Unit and Account
- Verify the Access Control at Different Levels of Hierarchy

GLOBOMANTICS

"Managing these overlapping SCPs along with IAM policies seems quite complicated. How do we approach this?"

Policy Strategies

Service Control Policies: Evaluation



Service Control Policies: Default SCP

- The root, all OUs, and accounts are attached with a default SCP, FullAWSAccess that allows all actions and services
- FullAWSAccess is an AWS-managed policy; it cannot be modified or deleted
- It can be attached or detached
- SCPs must be added or modified to restrict access

Service Control Policies: Strategies

Blacklist

Actions are allowed by default

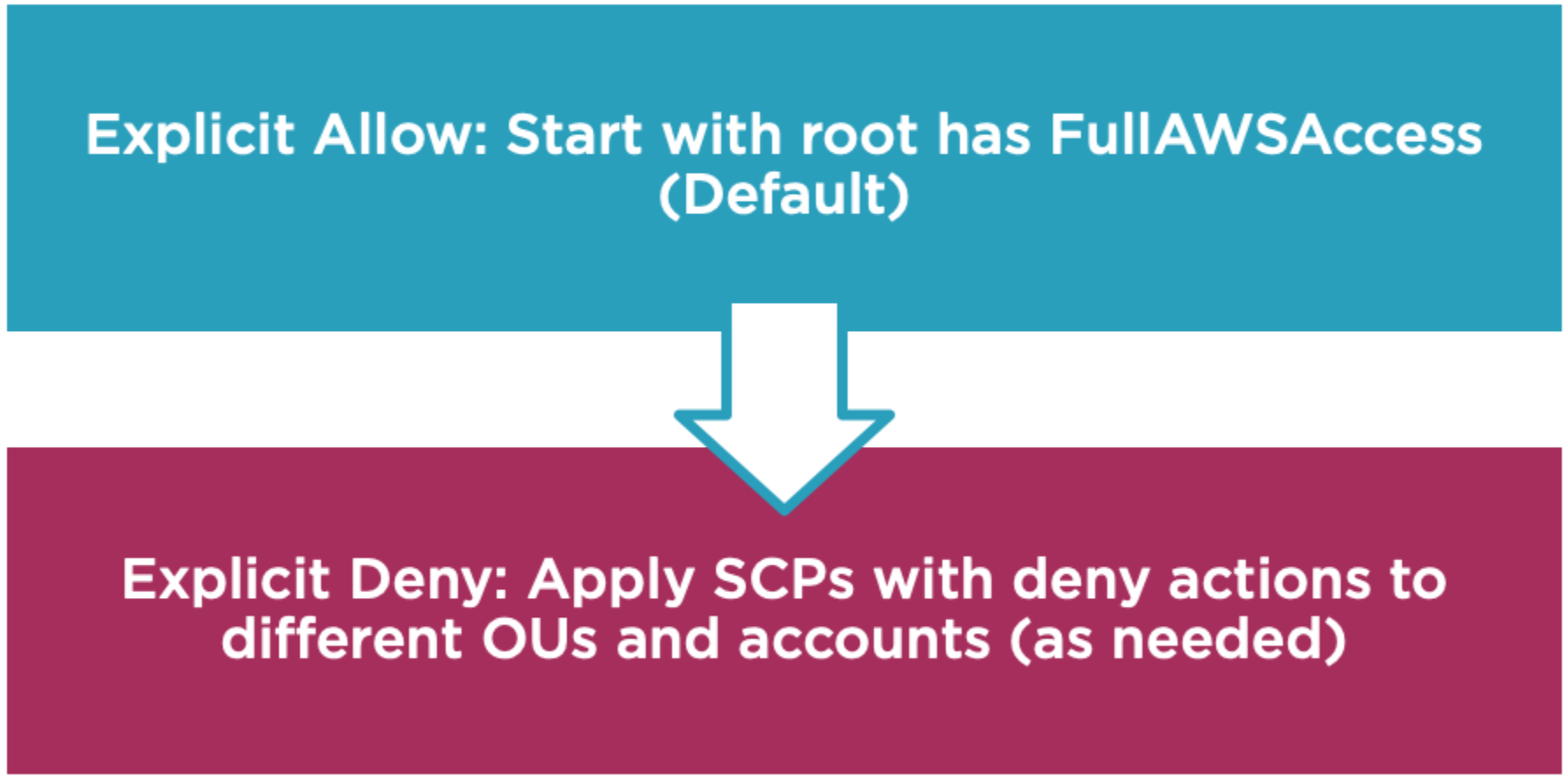
Specify what services and actions are denied

Whitelist

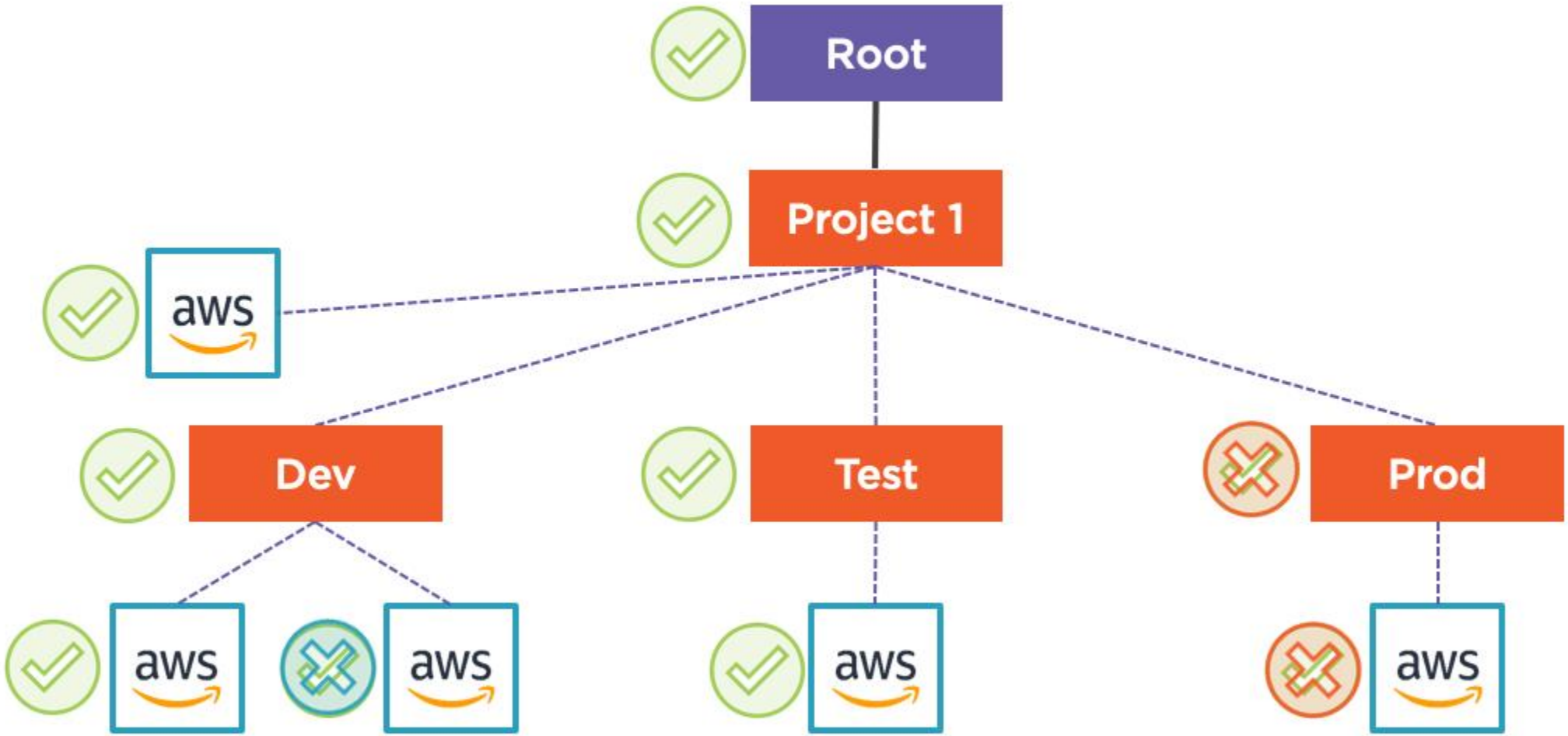
Actions are denied by default

Specify what services and actions are allowed

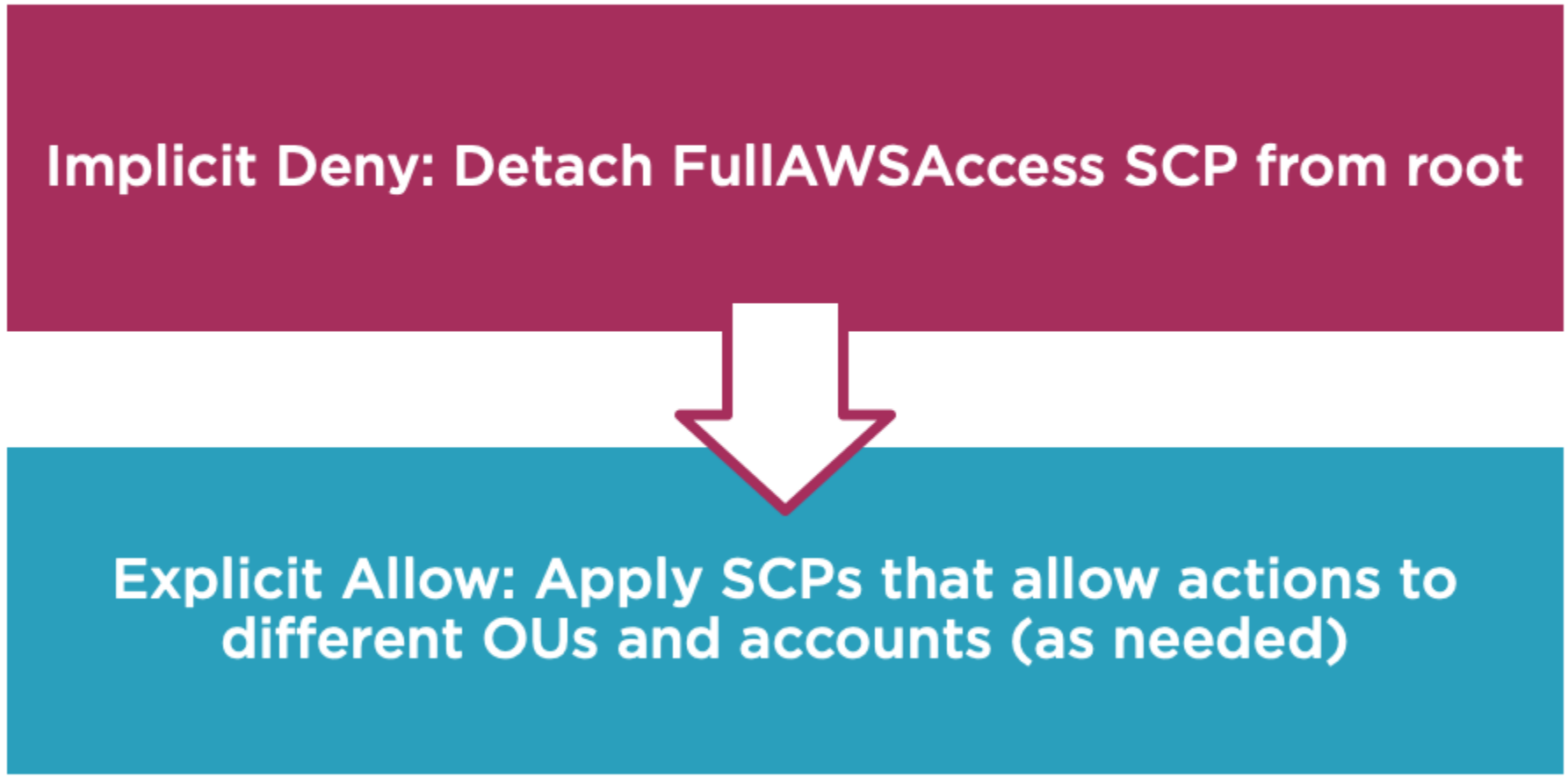
Service Control Policies: Blacklist



Service Control Policies: Blacklist Example



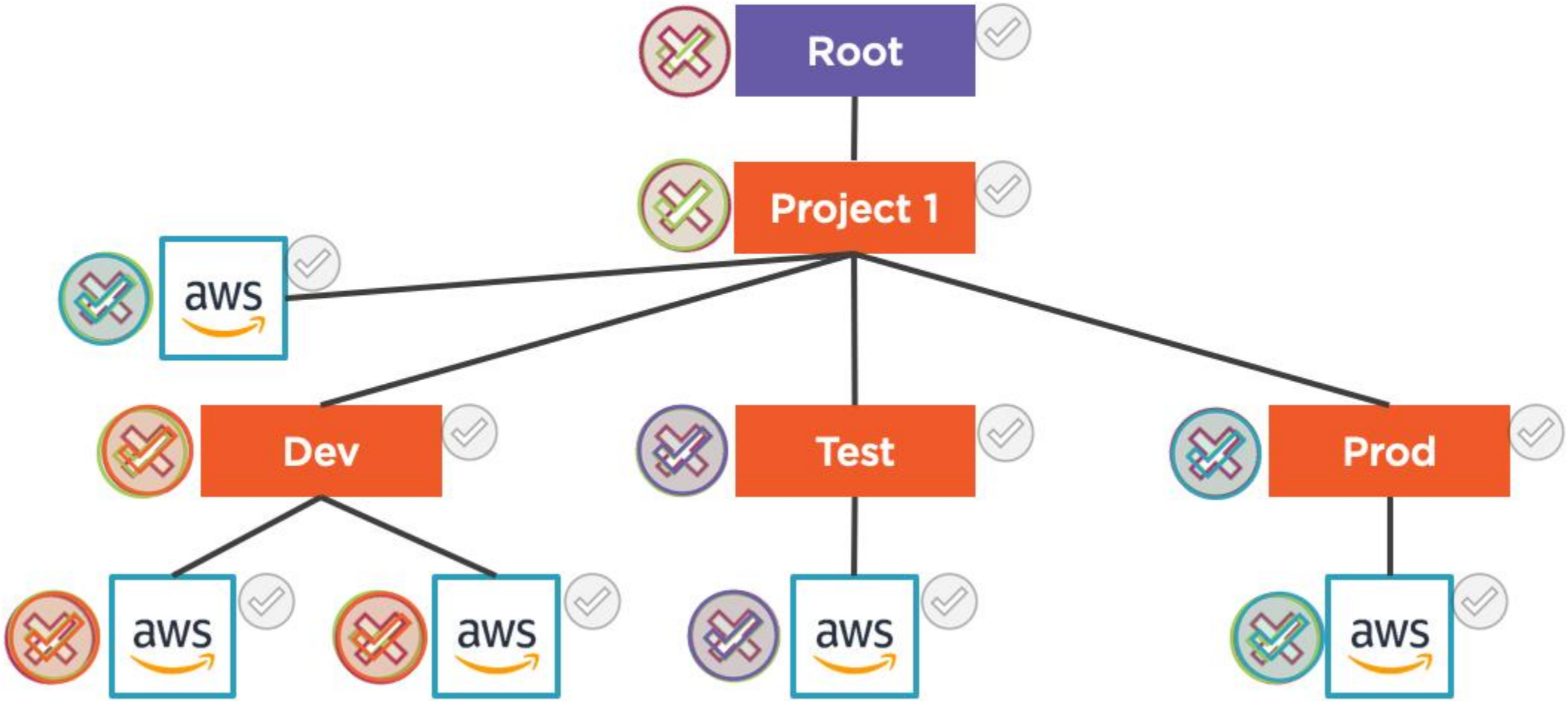
Service Control Policies: Whitelist



There must at least one attached policy to the root.

To detach FullAWSAccess SCP, you must create and attach another SCP that has at least minimal access.

Service Control Policies: Whitelist Example



Service Control Policies and the Master Account

The master account cannot be restricted

The master account can be placed anywhere in the hierarchy

SCPs will not affect the master account

Service Control Policies and Service-linked Roles

SCPs do not affect service-linked roles in a member account

Service-linked roles allow or deny permissions to AWS services

Service Control Policies: Limitations

SCPs affect only principals in an account

Users or roles from outside the account cannot be restricted

Example: Using a bucket policy, a user from a standalone account can access S3 bucket in a member account

Service Control Policies and the Root User

Root User

SCP affects the root user in a member account

Exceptions:

- Managing root credentials (example: changing root user's password)
- Registering for Enterprise support plan
- Changing the AWS support level

GLOBOMANTICS

"Restricting access to the root users in member accounts improves security posture; however, we will have to tightly secure our master account's root user."

Summary

Service Control Policies (SCPs)

- Policy Inheritance across Hierarchy
- SCPs vs. IAM Policies
- Policy Structure

Policy Strategy

- Policy Evaluation
- Whitelisting and Blacklisting