aws SUMMIT

WASHINGTON, DC | JUNE 7–8, 2023

DEV203

Cloud-grade network segmentation using AWS Transit Gateway & Terraform

William Collins

Principal Cloud Architect

Alkira

Agenda

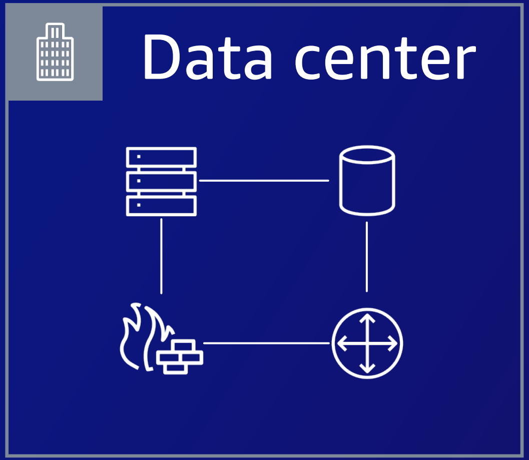
- *How* did we get here?
- Benefits of *segmentation*
- Thinking through the *workflow*
- Let’s *demo*!

How did we get here?

Enterprise

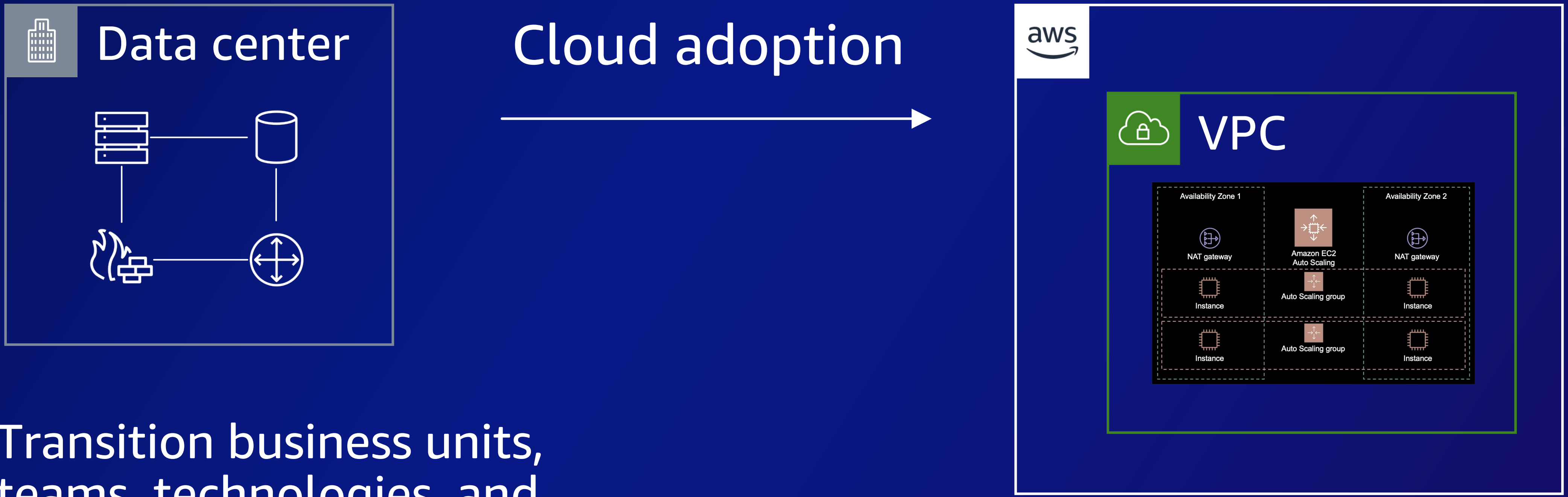
(15K or more employees)

100–2,000 applications



Data center

How did we get here?



Transition business units, teams, technologies, and processes to leverage AWS

Benefits of segmentation

Reduce attack surface

Compliance enforcement

Environment isolation

Optimize performance

Thinking through the workflow

VPCs

Acceleration in AWS adoption for large enterprises leads to an increase in VPCs over time

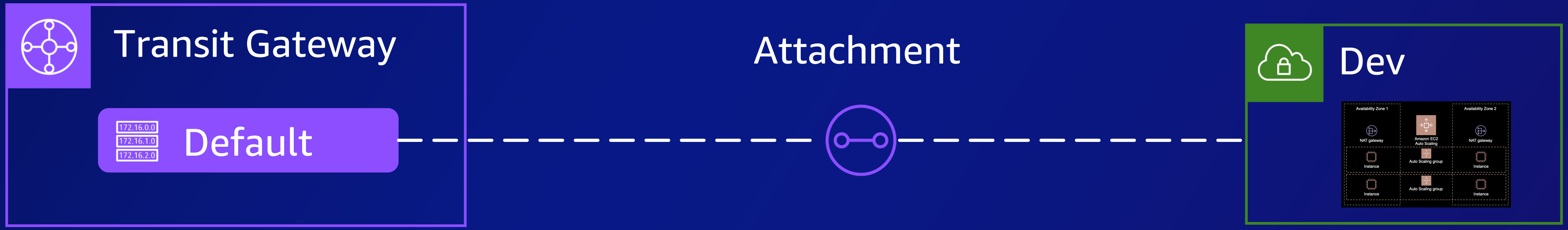
AWS Transit Gateway

Simplifies connectivity at scale for VPCs and on-premises networking

Terraform

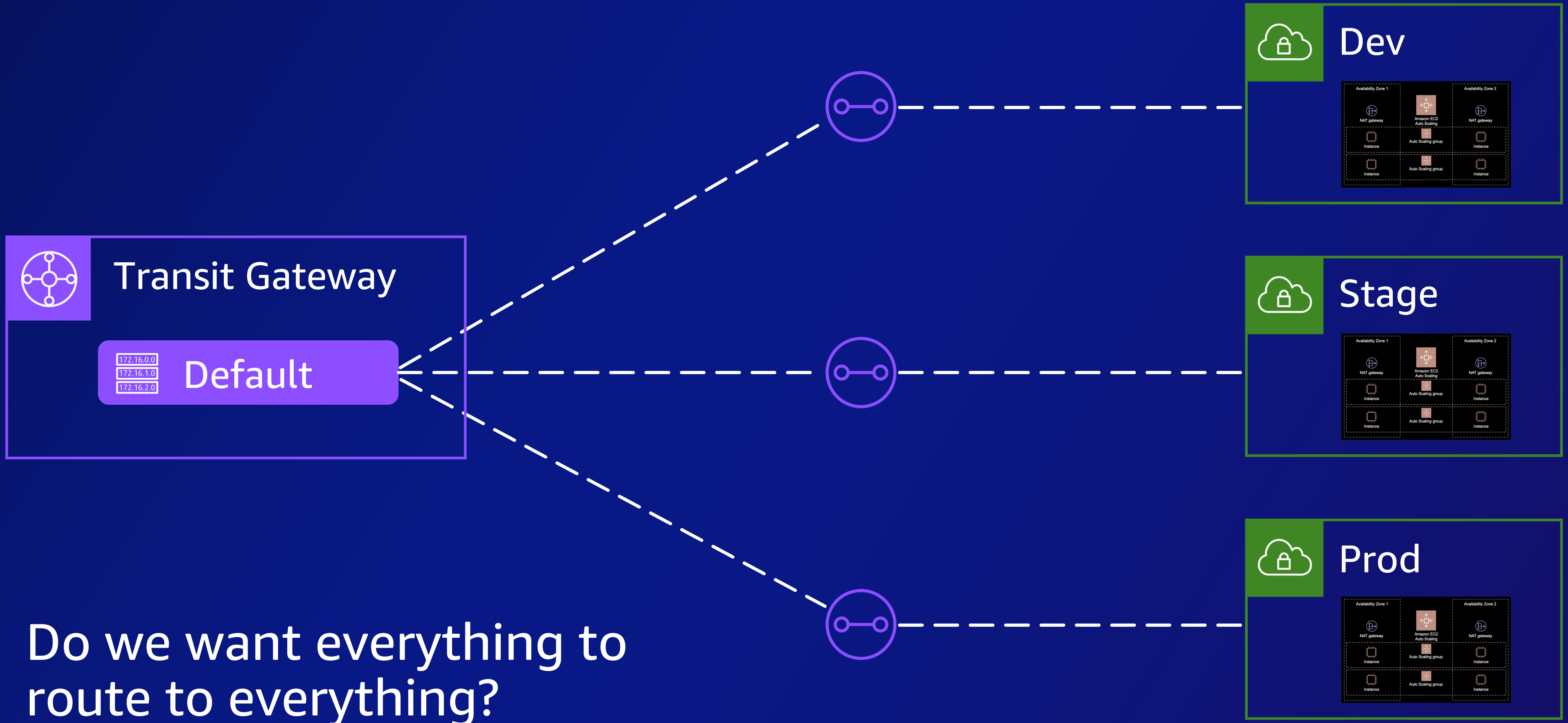
Infrastructure as code tool that uses a declarative approach for managing cloud resources

Thinking through the workflow



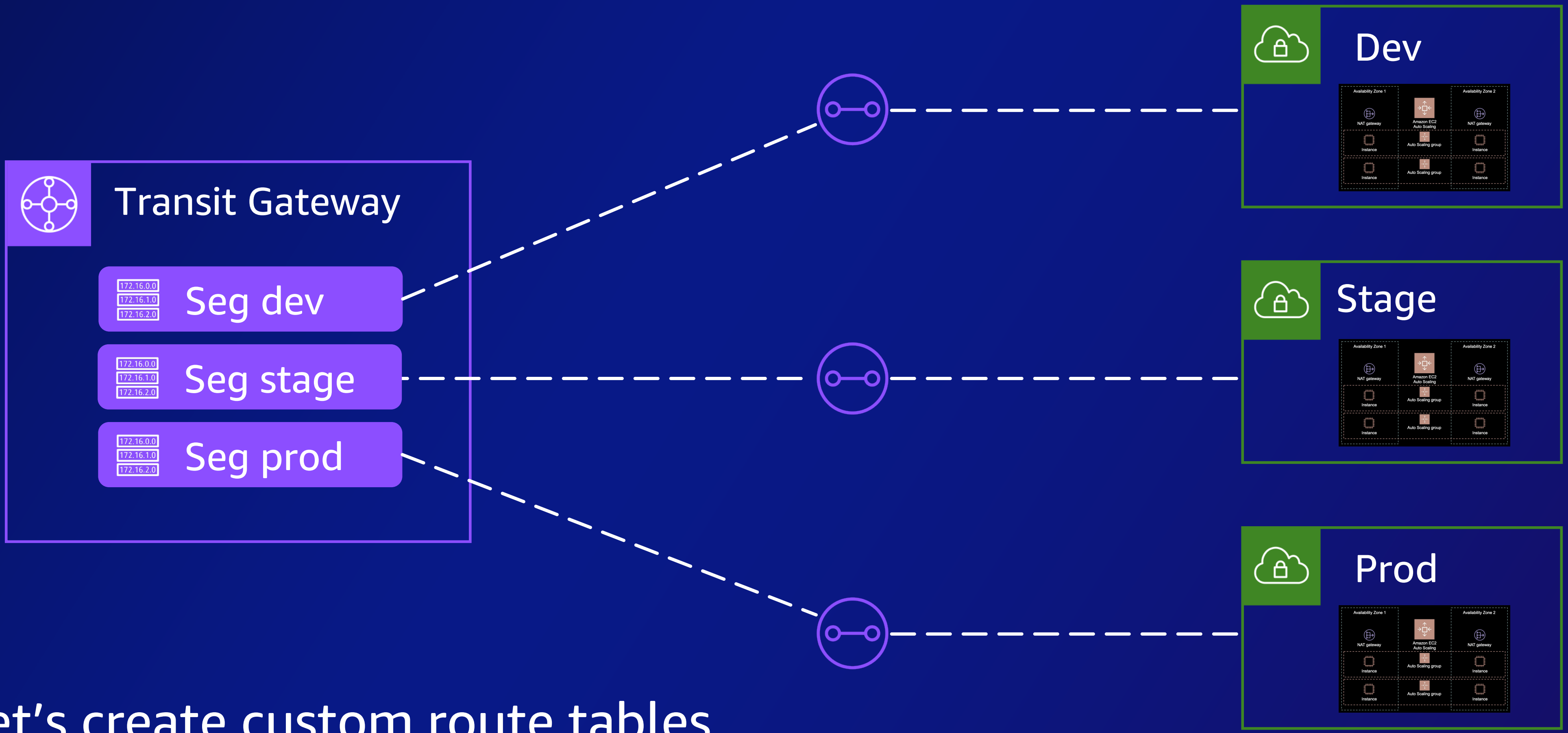
Default provider behavior will associate attachments with Transit Gateway’s default route table and propagate routes

Thinking through the workflow



Do we want everything to route to everything?

Thinking through the workflow



Transit Gateway

Seg dev

Seg stage

Seg prod

Dev

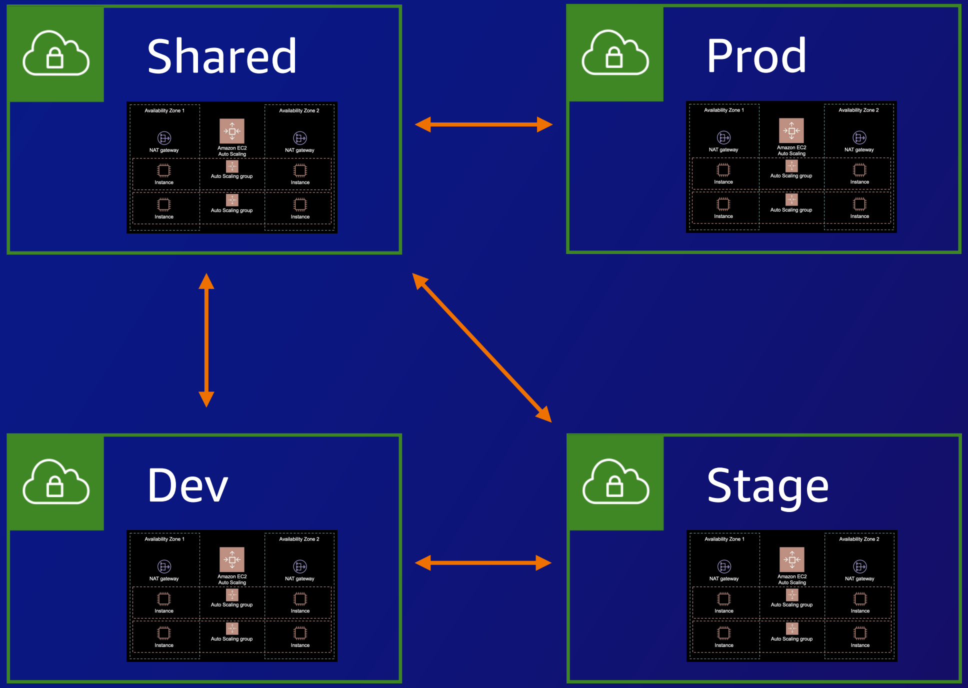
Stage

Prod

Let’s create custom route tables
for *network segmentation*!

Demo!

- **“Shared”** can reach all VPCs
- “**Dev**” and “**Stage**” have reachability to each other but not to “**Prod**”



Thank you!

William Collins

@wcollins502

linkedin.com/in/william-collins

wcollins.io

Please complete the session survey in the mobile app

No mobile app?
Use this code