Deploying AWS Infrastructure using Ansible and CloudFormation

Justin Menga
FULL STACK TECHNOLOGIST

@jmenga pseudo.co.de

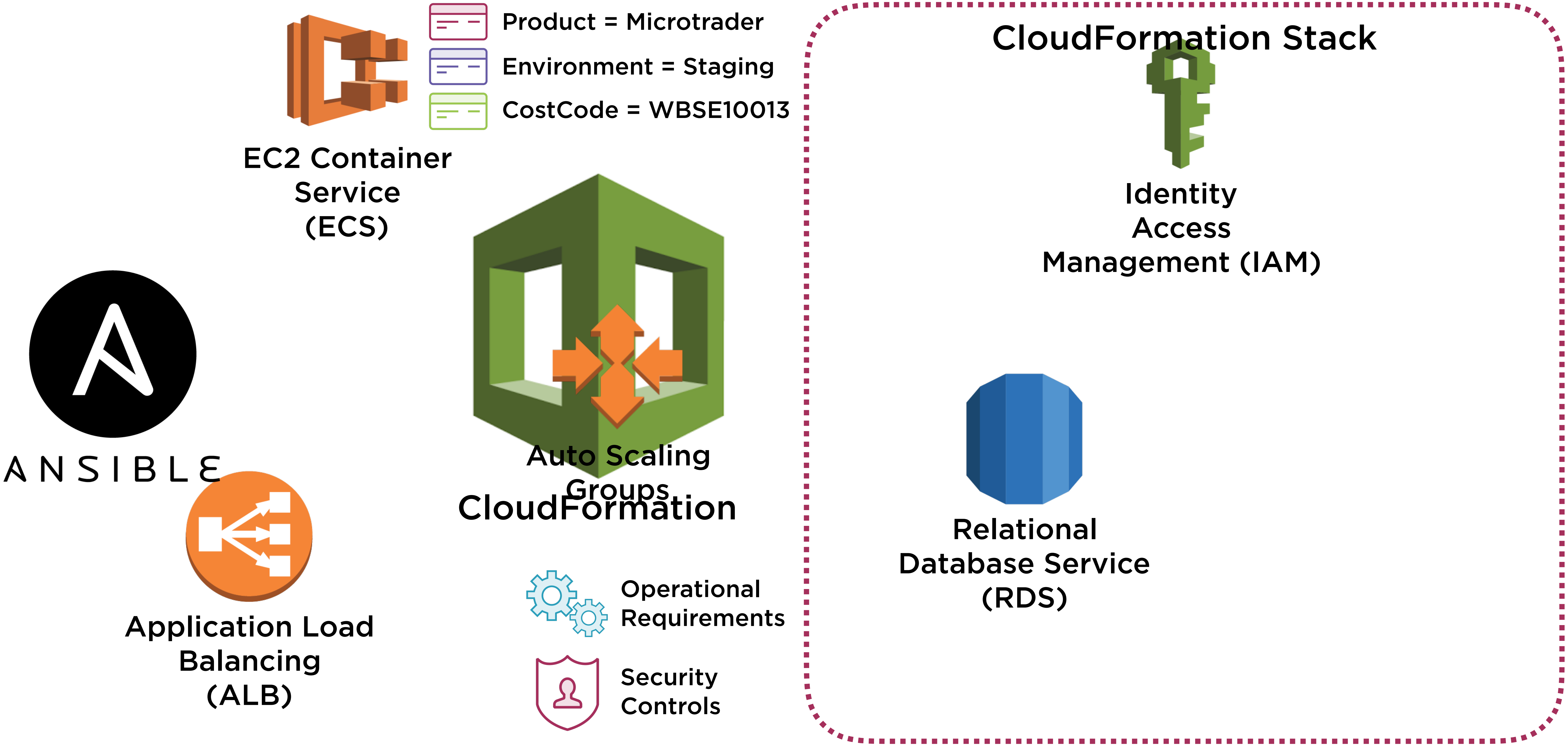
Introduction

Deploying AWS Infrastructure

- AWS Deployment Strategy
  - Supporting resources
  - Infrastructure as code
- Shared Infrastructure
  - Ansible and CloudFormation
  - Network infrastructure
  - CloudFormation/Lambda/KMS
  - ECR repositories
  - HTTP proxy stack

AWS Deployment Strategy

Key Deployment Technologies



Product = Microtrader

Environment = Staging

CostCode = WBSE10013

EC2 Container Service (ECS)

ANSIBLE

Application Load Balancing (ALB)

Auto Scaling Groups

CloudFormation

Operational Requirements

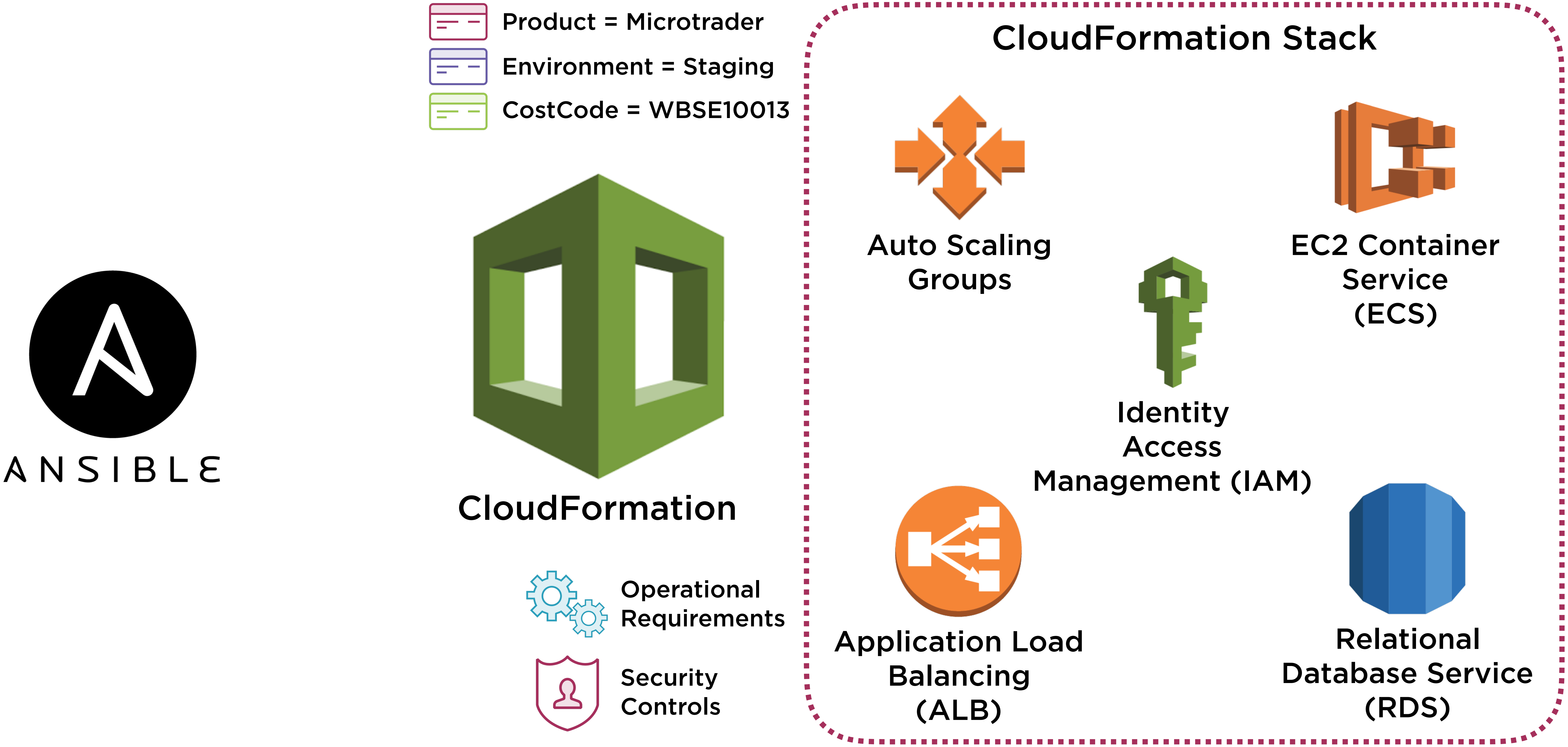
Security Controls

CloudFormation Stack

Identity Access Management (IAM)

Relational Database Service (RDS)

Key Deployment Technologies



ANSIBLE

Product = Microtrader

Environment = Staging

CostCode = WBSE10013

CloudFormation

Operational Requirements

Security Controls

CloudFormation Stack

Auto Scaling Groups

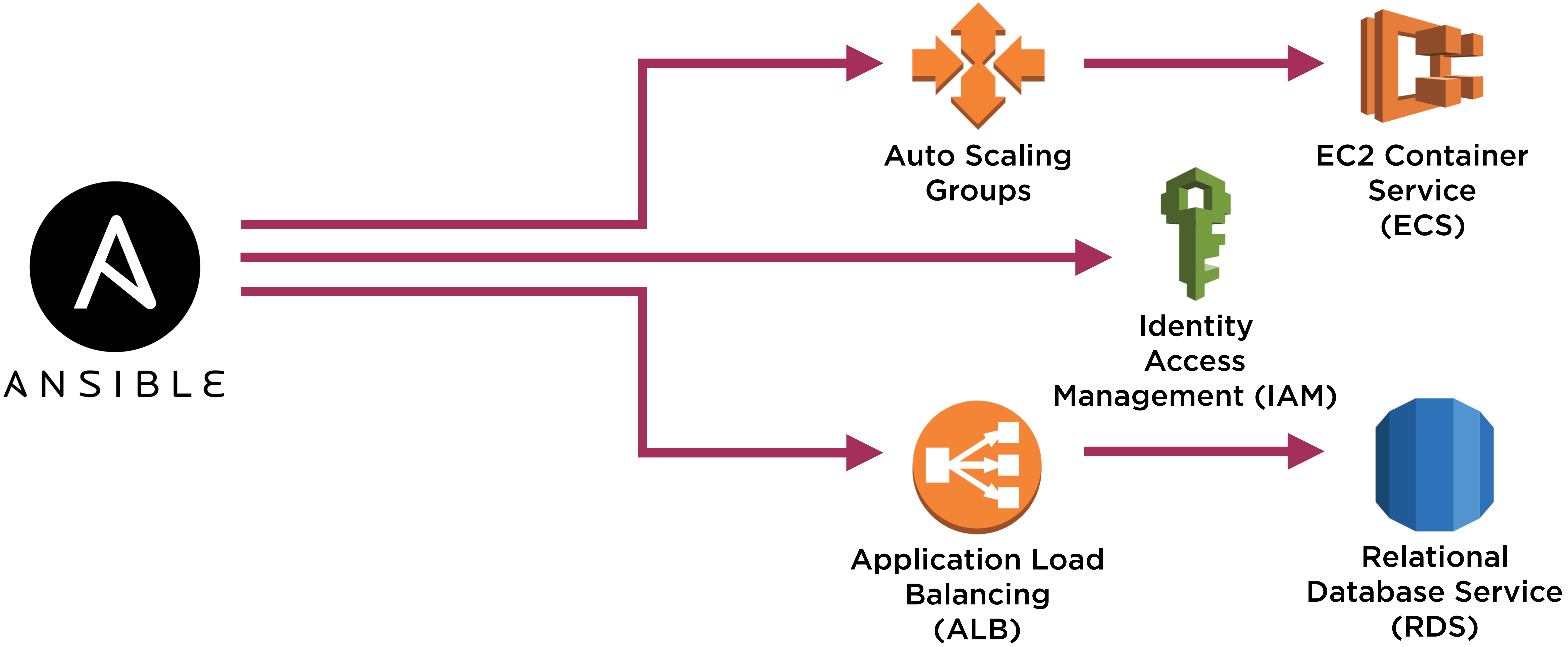
EC2 Container Service (ECS)

Identity Access Management (IAM)

Application Load Balancing (ALB)

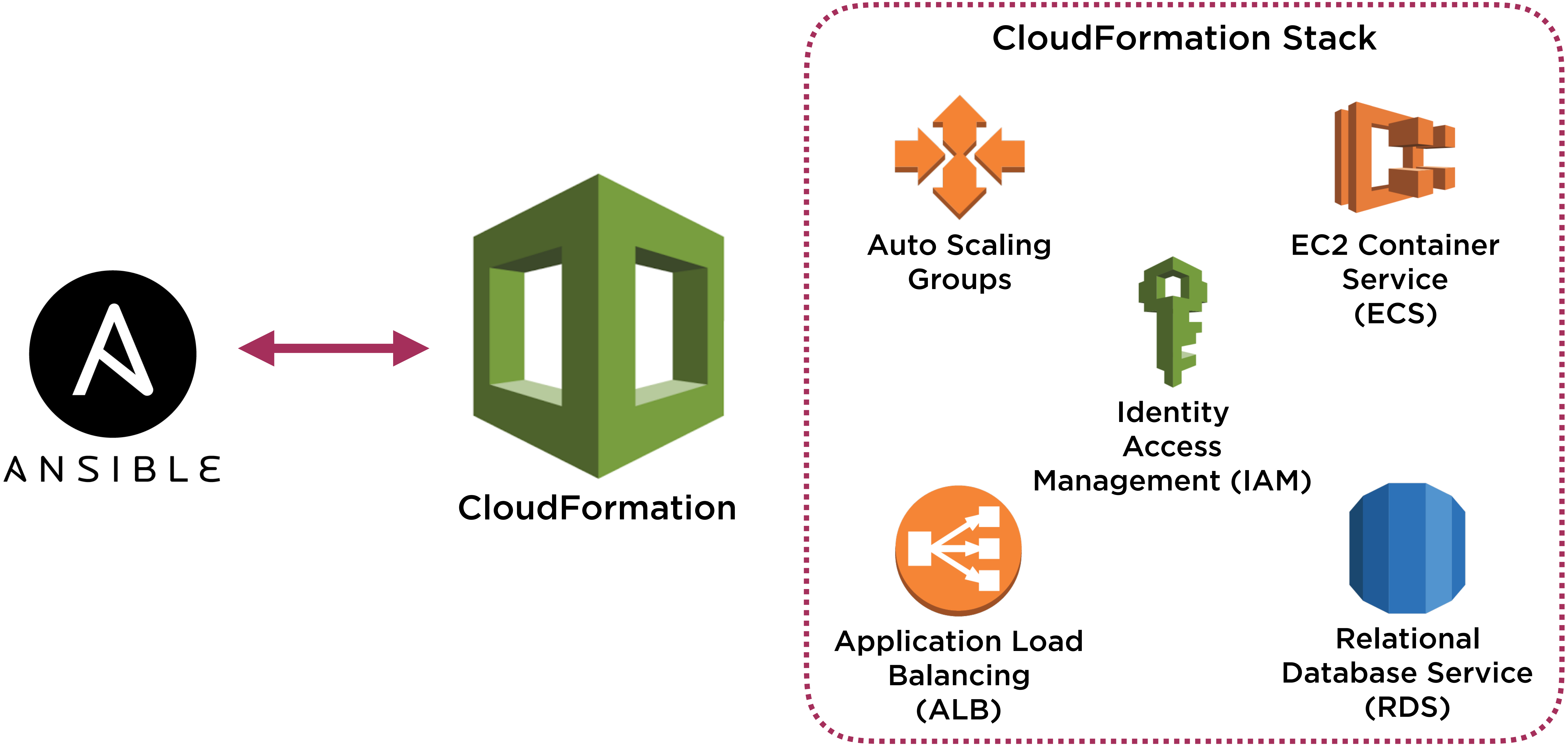
Relational Database Service (RDS)

Key Deployment Technologies



ANSIBLE
Auto Scaling Groups
EC2 Container Service (ECS)
Identity Access Management (IAM)
Application Load Balancing (ALB)
Relational Database Service (RDS)

Key Deployment Technologies



ANSIBLE

CloudFormation

CloudFormation Stack

Auto Scaling Groups

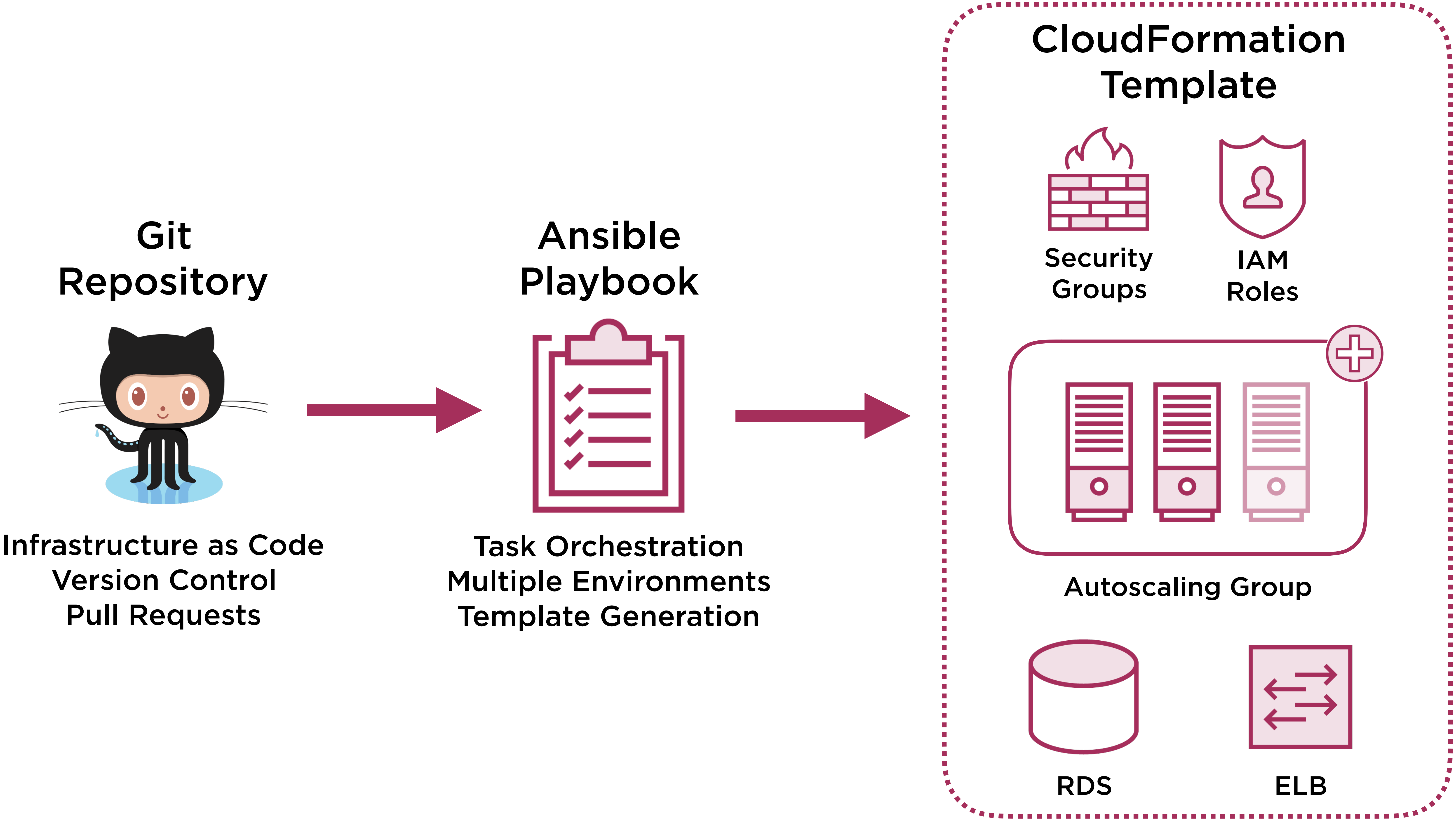
EC2 Container Service (ECS)

Identity Access Management (IAM)

Application Load Balancing (ALB)

Relational Database Service (RDS)

AWS Account Infrastructure Architecture



Git Repository

Infrastructure as Code
Version Control
Pull Requests

Ansible Playbook

Task Orchestration
Multiple Environments
Template Generation

CloudFormation Template

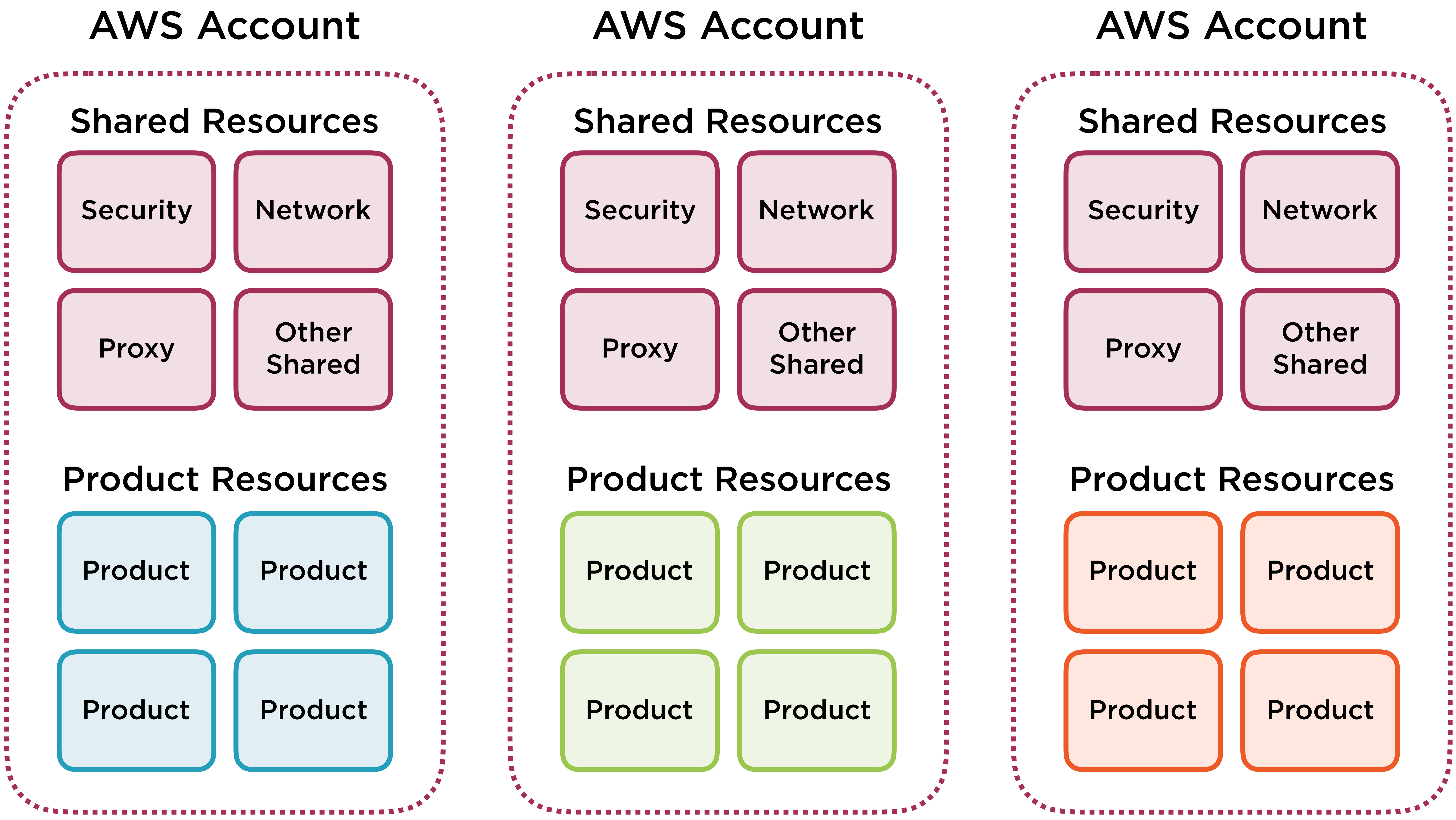
Security Groups

IAM Roles

Autoscaling Group

RDS

ELB



AWS Account

Shared Resources

Security

Network

Proxy

Other Shared

Product Resources

Product

Product

Product

Product

AWS Account

Shared Resources

Security

Network

Proxy

Other Shared

Product Resources

Product

Product

Product

Product

AWS Account

Shared Resources

Security

Network

Proxy

Other Shared

Product Resources

Product

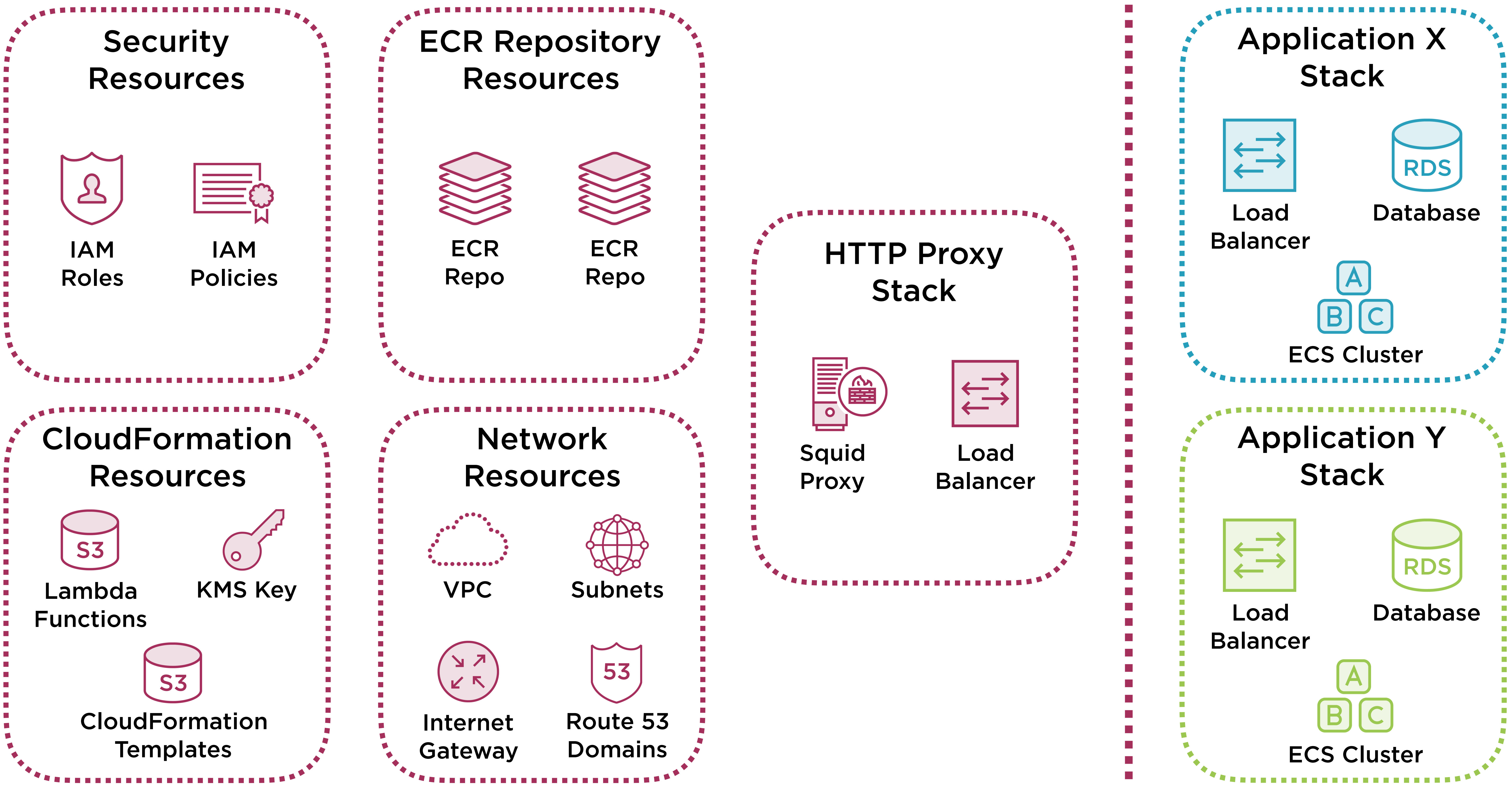
Product

Product

Product

Shared Resources

Product Teams



Security Resources

IAM Roles

IAM Policies

ECR Repository Resources

ECR Repo

ECR Repo

CloudFormation Resources

Lambda Functions

KMS Key

CloudFormation Templates

Network Resources

VPC

Subnets

Internet Gateway

Route 53 Domains

HTTP Proxy Stack

Squid Proxy

Load Balancer

Application X Stack

Load Balancer

Database

ECS Cluster

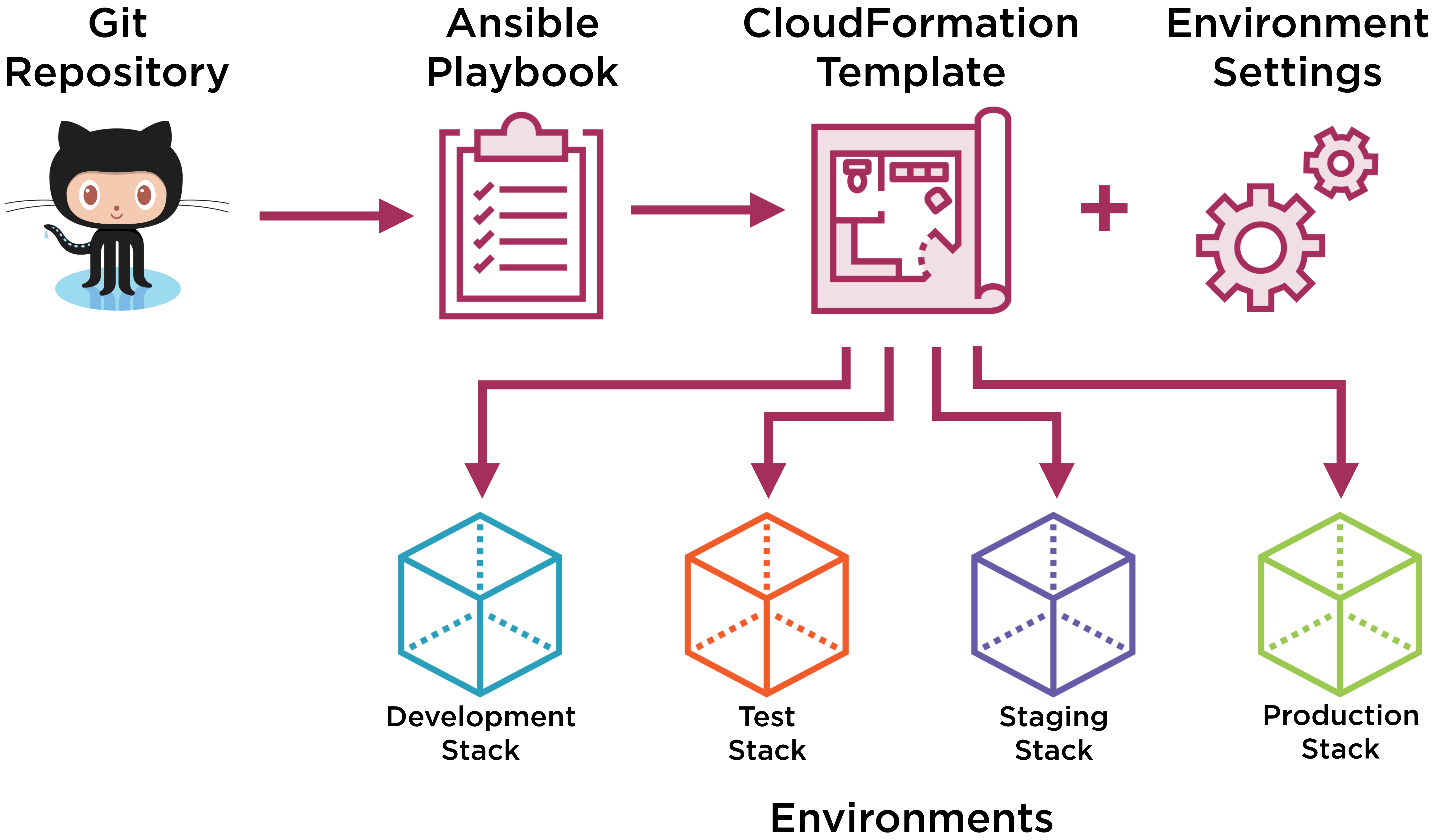
Application Y Stack

Load Balancer

Database

ECS Cluster

Ansible Playbooks



Git Repository

Ansible Playbook

CloudFormation Template

Environment Settings

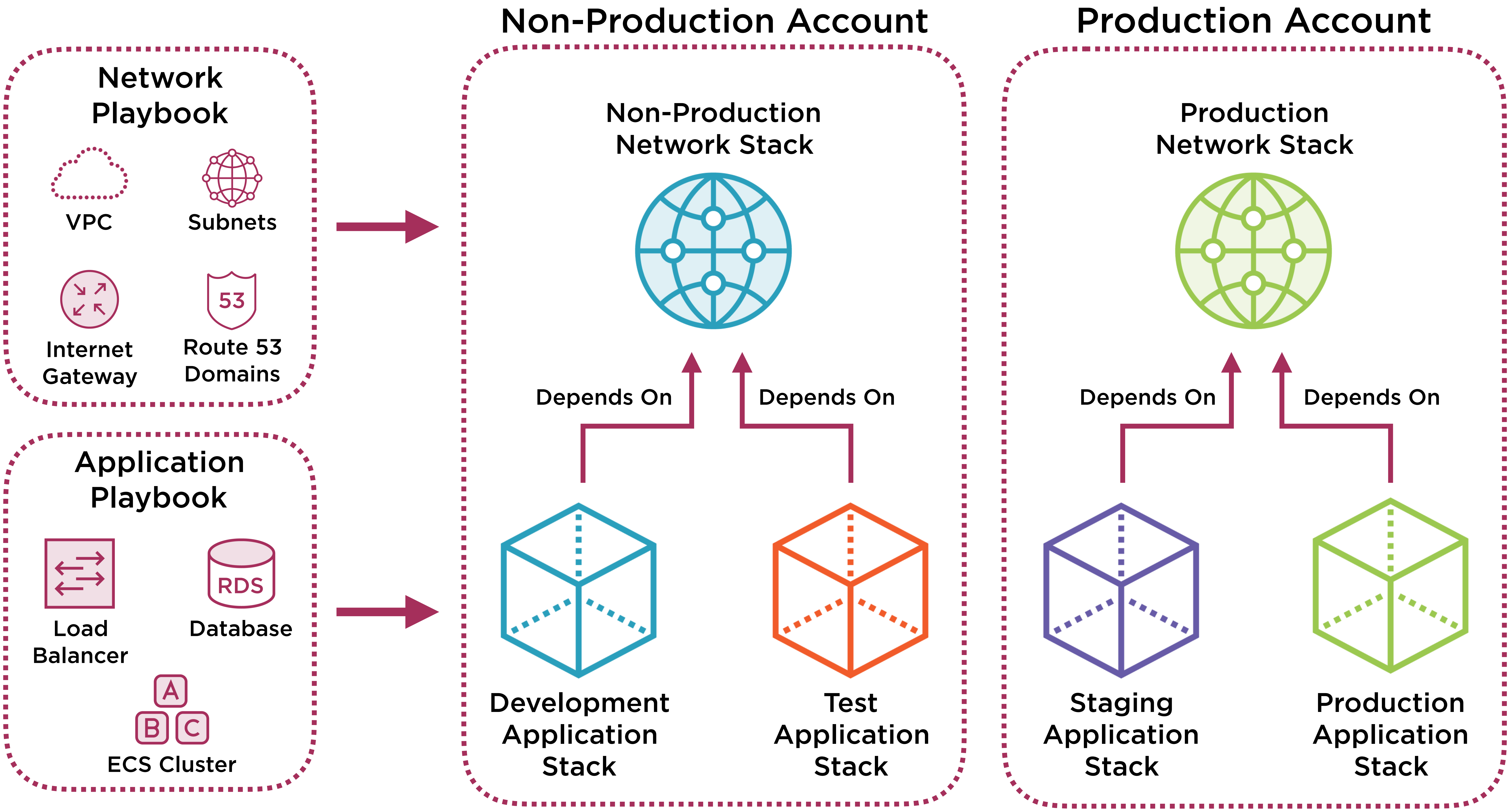
Development Stack

Test Stack

Staging Stack

Production Stack

Environments



Non-Production Account

Production Account

Network Playbook

VPC

Subnets

Internet Gateway

Route 53 Domains

Application Playbook

Load Balancer

Database

ECS Cluster

Non-Production Network Stack

Depends On

Depends On

Development Application Stack

Test Application Stack

Production Network Stack

Depends On

Depends On

Staging Application Stack

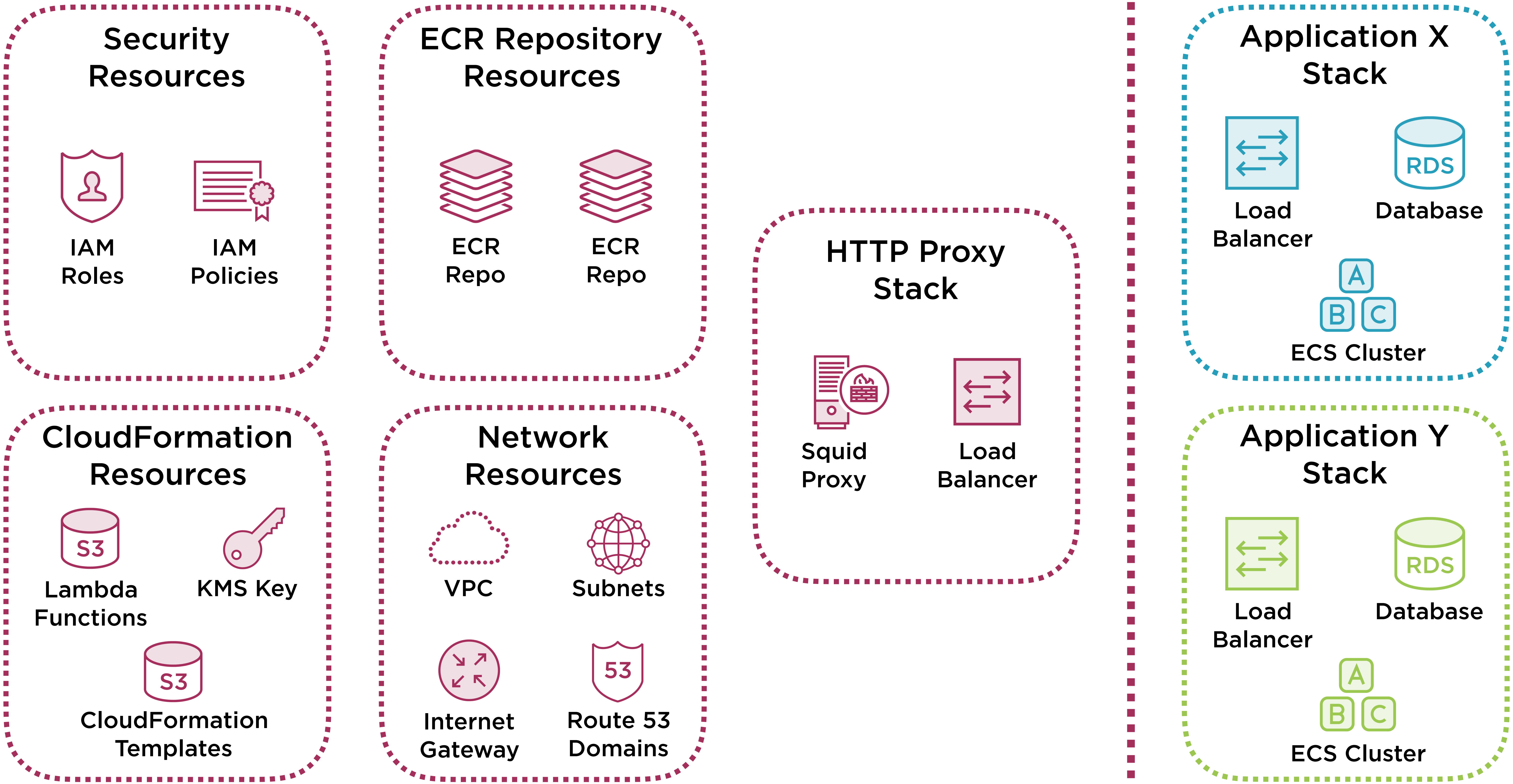
Production Application Stack

Ansible Playbook Structure

Creating an Ansible Playbook

Shared Resources

Product Teams



Security Resources

IAM Roles

IAM Policies

ECR Repository Resources

ECR Repo

ECR Repo

CloudFormation Resources

Lambda Functions

KMS Key

CloudFormation Templates

Network Resources

VPC

Subnets

Internet Gateway

Route 53 Domains

HTTP Proxy Stack

Squid Proxy

Load Balancer

Application X Stack

Load Balancer

Database

ECS Cluster

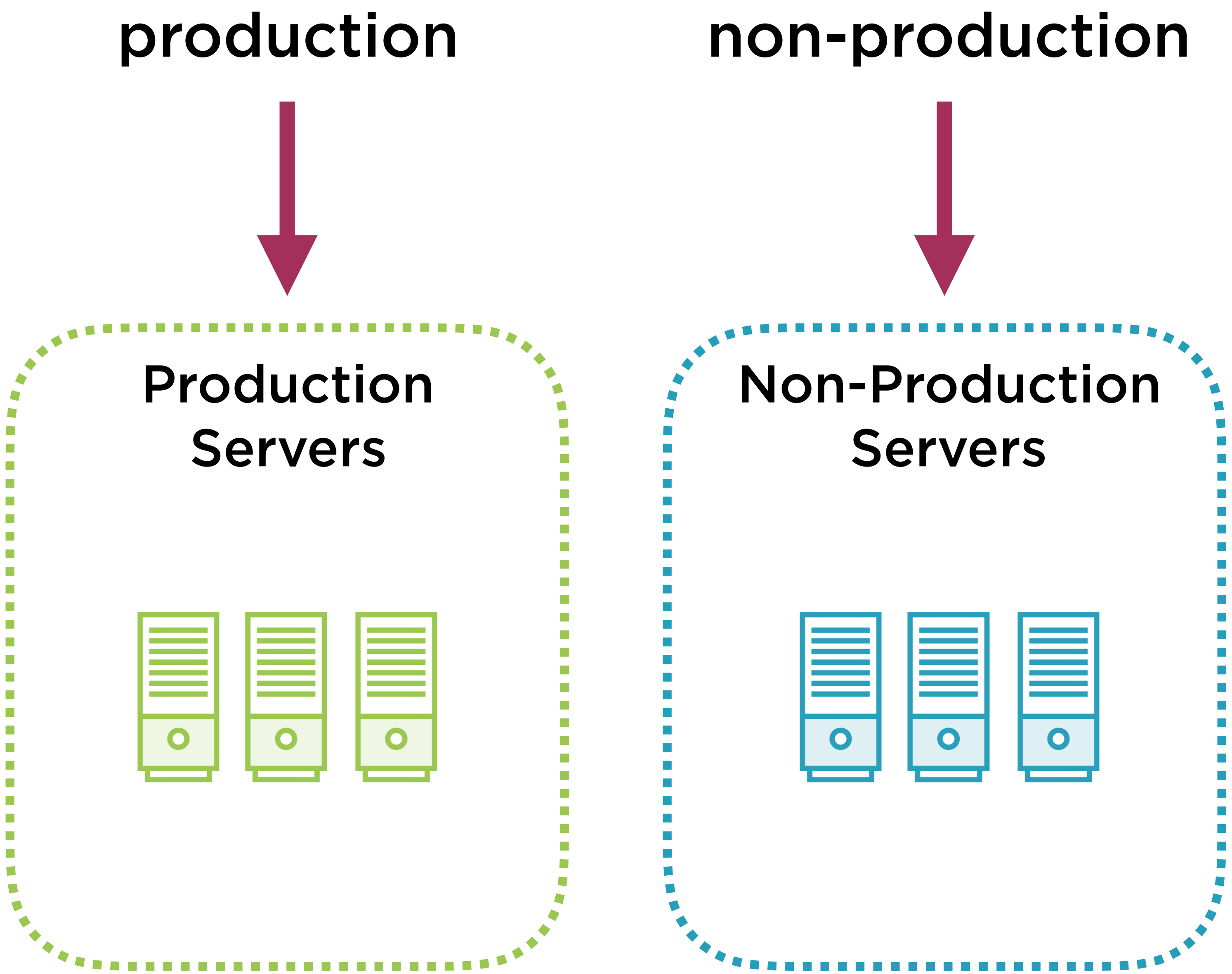
Application Y Stack

Load Balancer

Database

ECS Cluster

Traditional Ansible



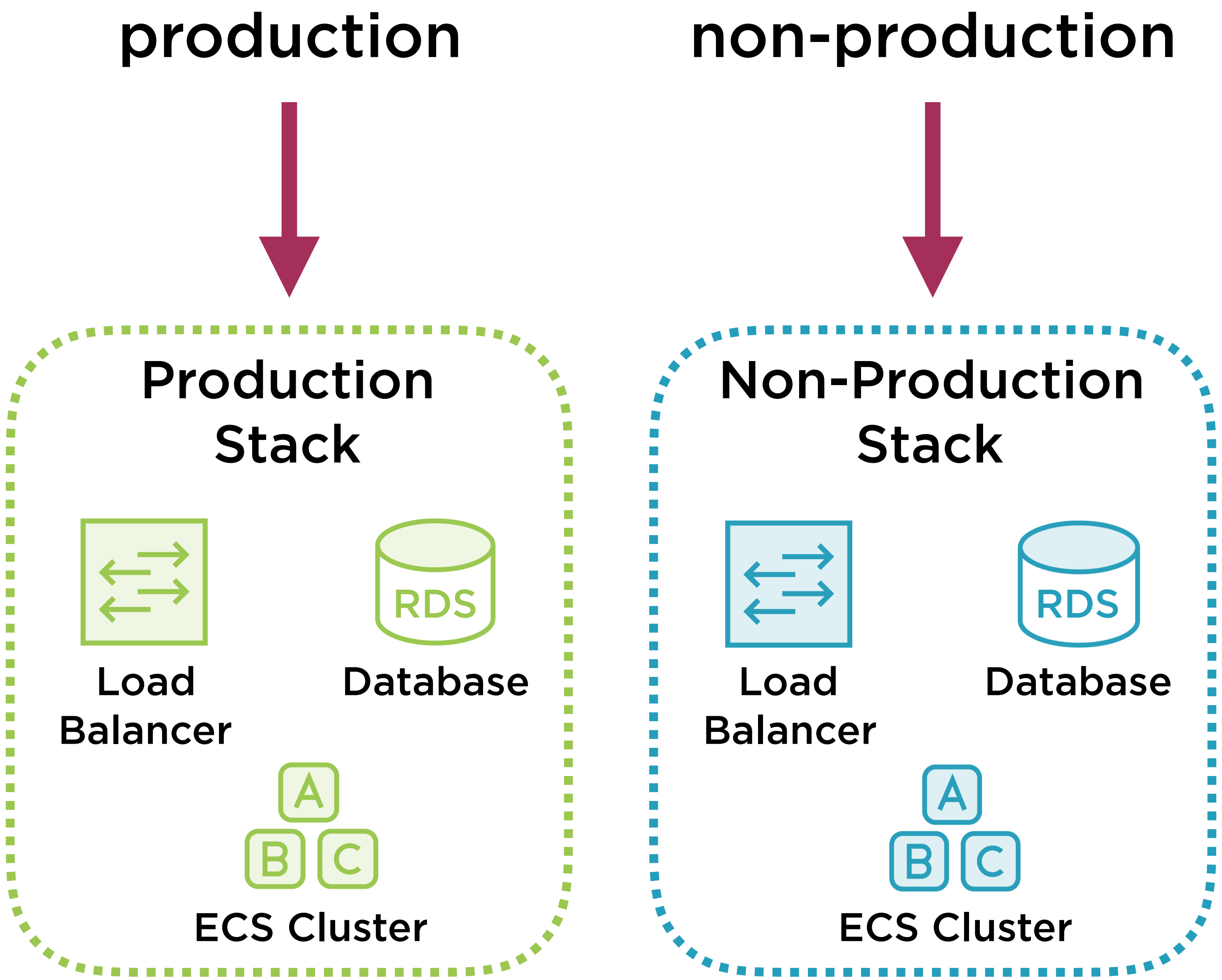
production

non-production

Production Servers

Non-Production Servers

This Course



production

non-production

Production Stack

Load Balancer

Database

ECS Cluster

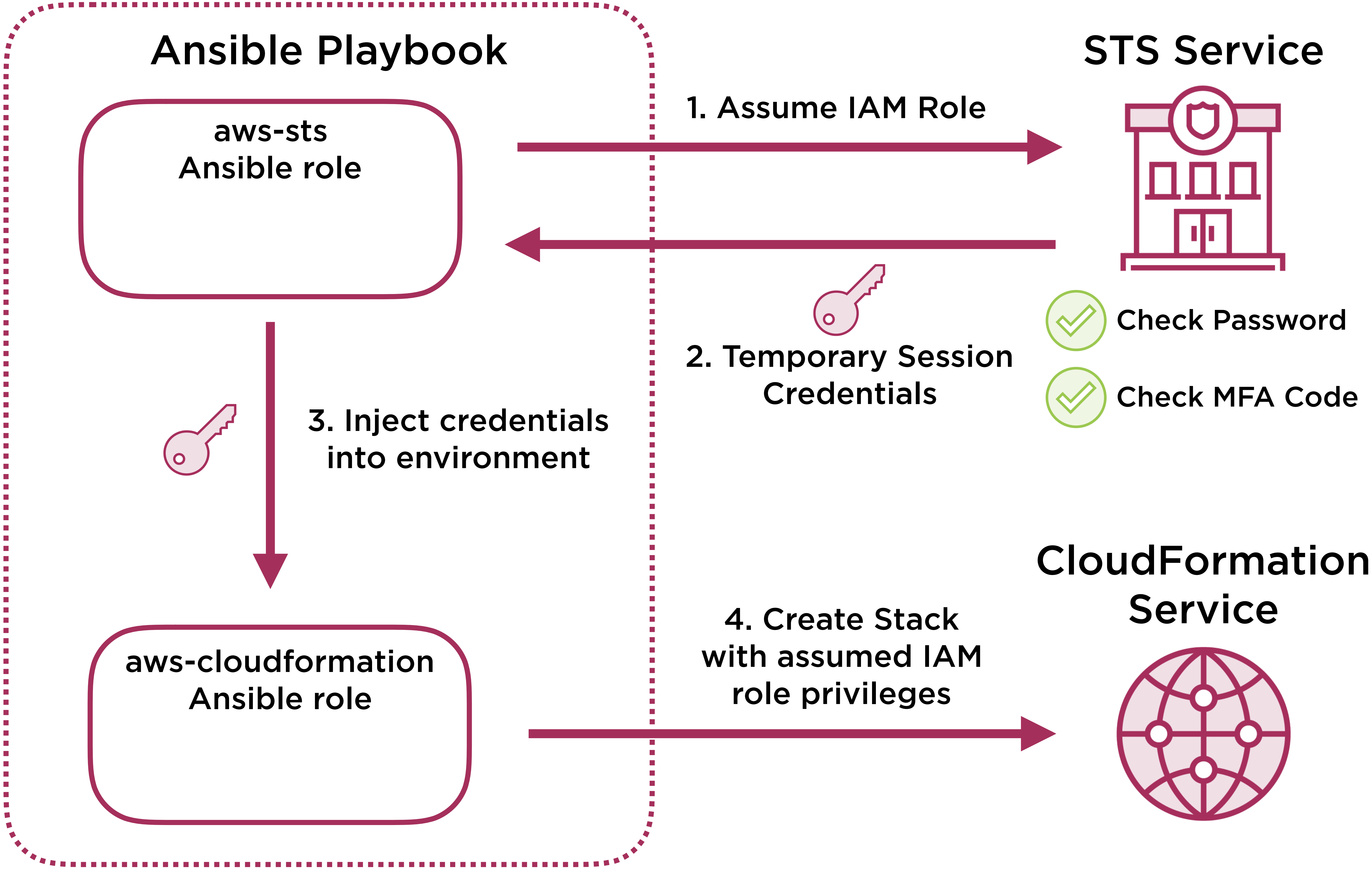
Non-Production Stack

Load Balancer

Database

ECS Cluster

Configuring the AWS STS Role



Ansible Playbook

aws-sts
Ansible role

aws-cloudformation
Ansible role

3. Inject credentials
into environment

STS Service

1. Assume IAM Role

2. Temporary Session
Credentials

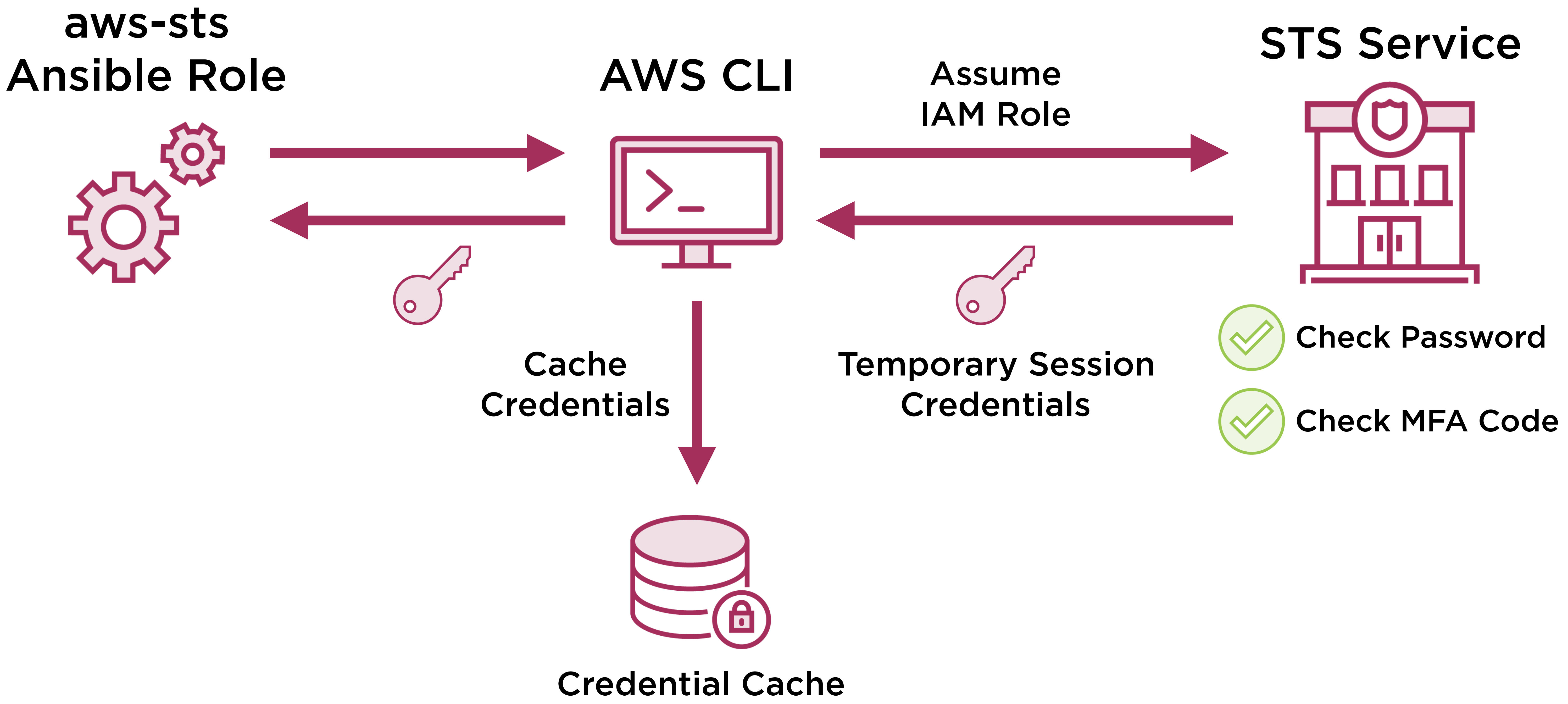
✓ Check Password

✓ Check MFA Code

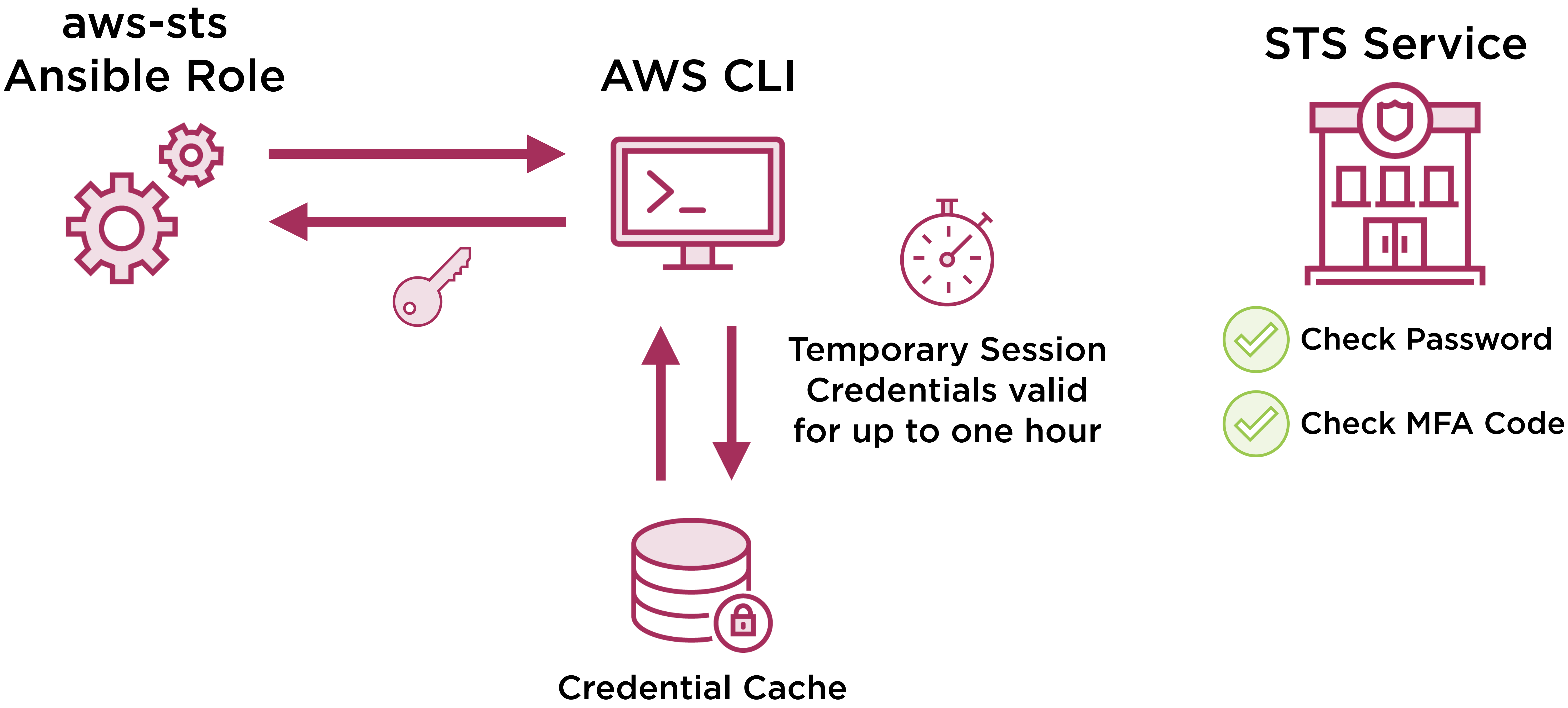
CloudFormation
Service

4. Create Stack
with assumed IAM
role privileges

AWS CLI Credential Caching



AWS CLI Credential Caching



aws-sts
Ansible Role

AWS CLI

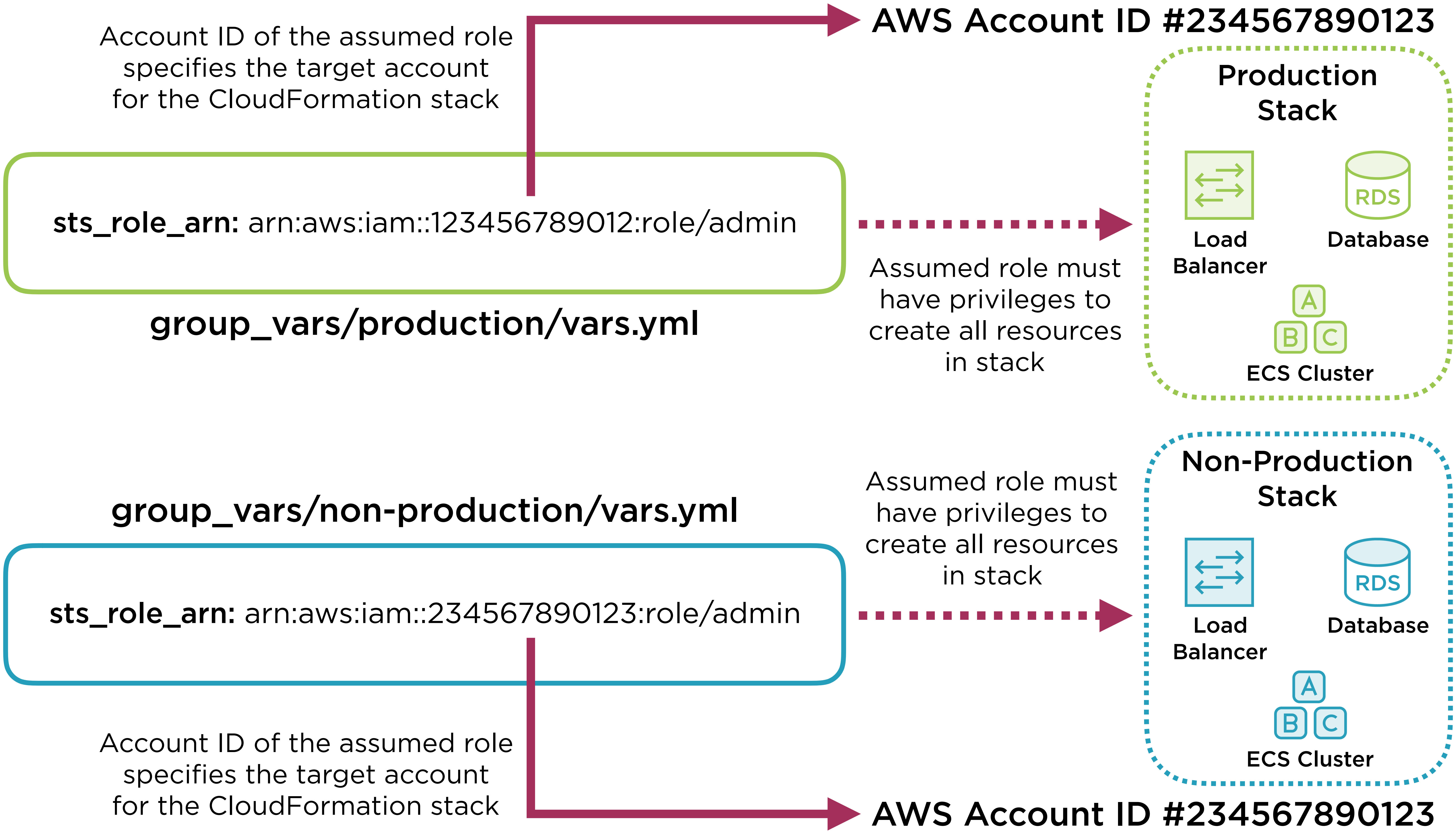
STS Service

Temporary Session
Credentials valid
for up to one hour

✓ Check Password

✓ Check MFA Code

Credential Cache



AWS Account ID #234567890123

Account ID of the assumed role specifies the target account for the CloudFormation stack

sts_role_arn: arn:aws:iam::123456789012:role/admin

group_vars/production/vars.yml

Assumed role must have privileges to create all resources in stack

Production Stack

Load Balancer

Database

ECS Cluster

group_vars/non-production/vars.yml

sts_role_arn: arn:aws:iam::234567890123:role/admin

Assumed role must have privileges to create all resources in stack

Non-Production Stack

Load Balancer

Database

ECS Cluster

Account ID of the assumed role specifies the target account for the CloudFormation stack

AWS Account ID #234567890123

Playbook Variable Naming Conventions

Ansible Role Variables

aws-sts role: sts_xxx_xxxx

- e.g. sts_role_arn, sts_disable

aws-cloudformation role: cf_xxx_xxxx

- e.g. cf_stack_name, cf_stack_template

Environment Settings

All variables prefixed with config_

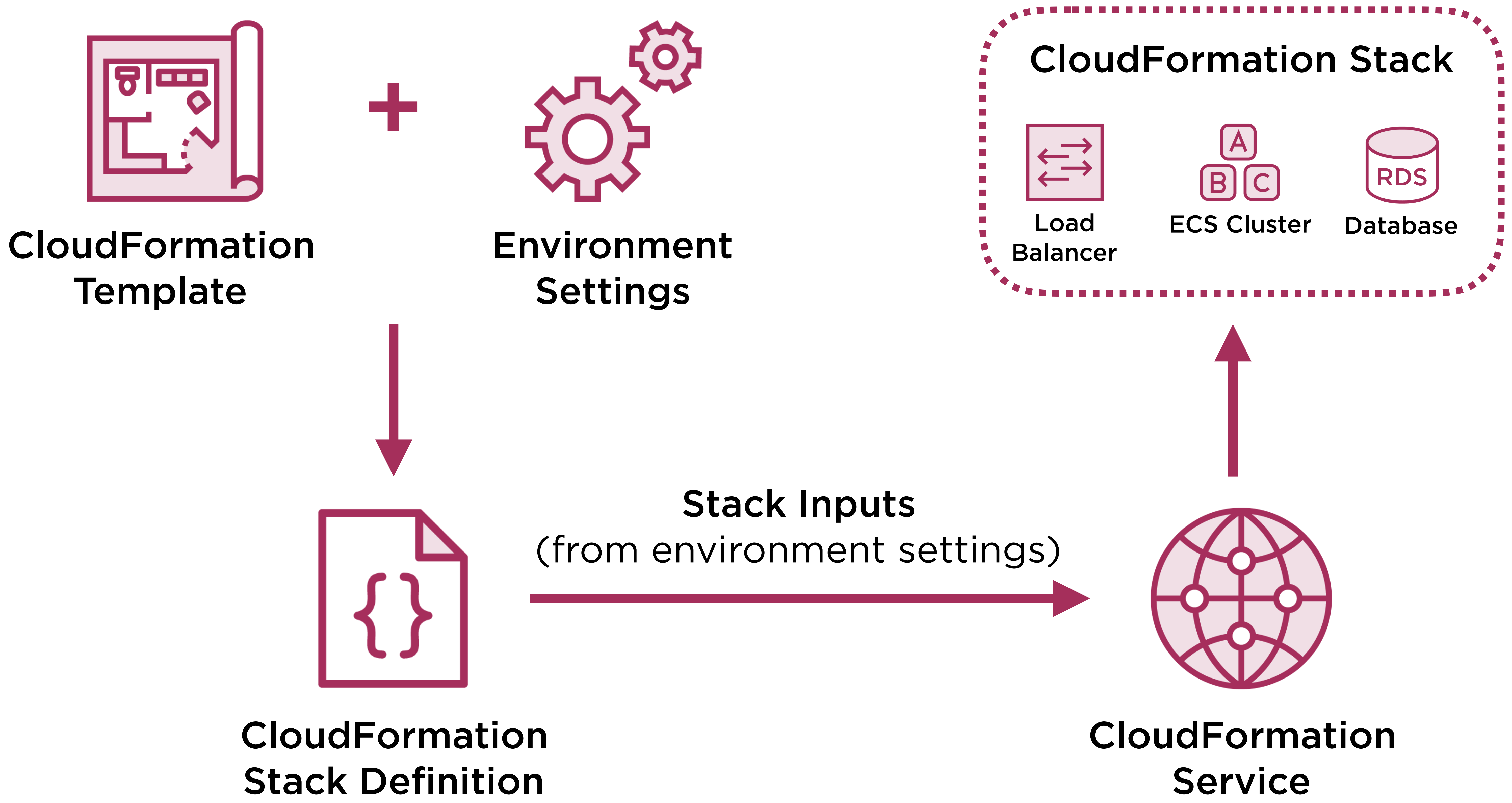
- e.g. config_application_ami
- e.g. config_db_username

Configuring the AWS CloudFormation Role

Understanding the AWS CloudFormation Role

Template Generation Phase

Deployment Phase



CloudFormation Template

+

Environment Settings

CloudFormation Stack Definition

Stack Inputs
(from environment settings)

CloudFormation Service

CloudFormation Stack

Load Balancer

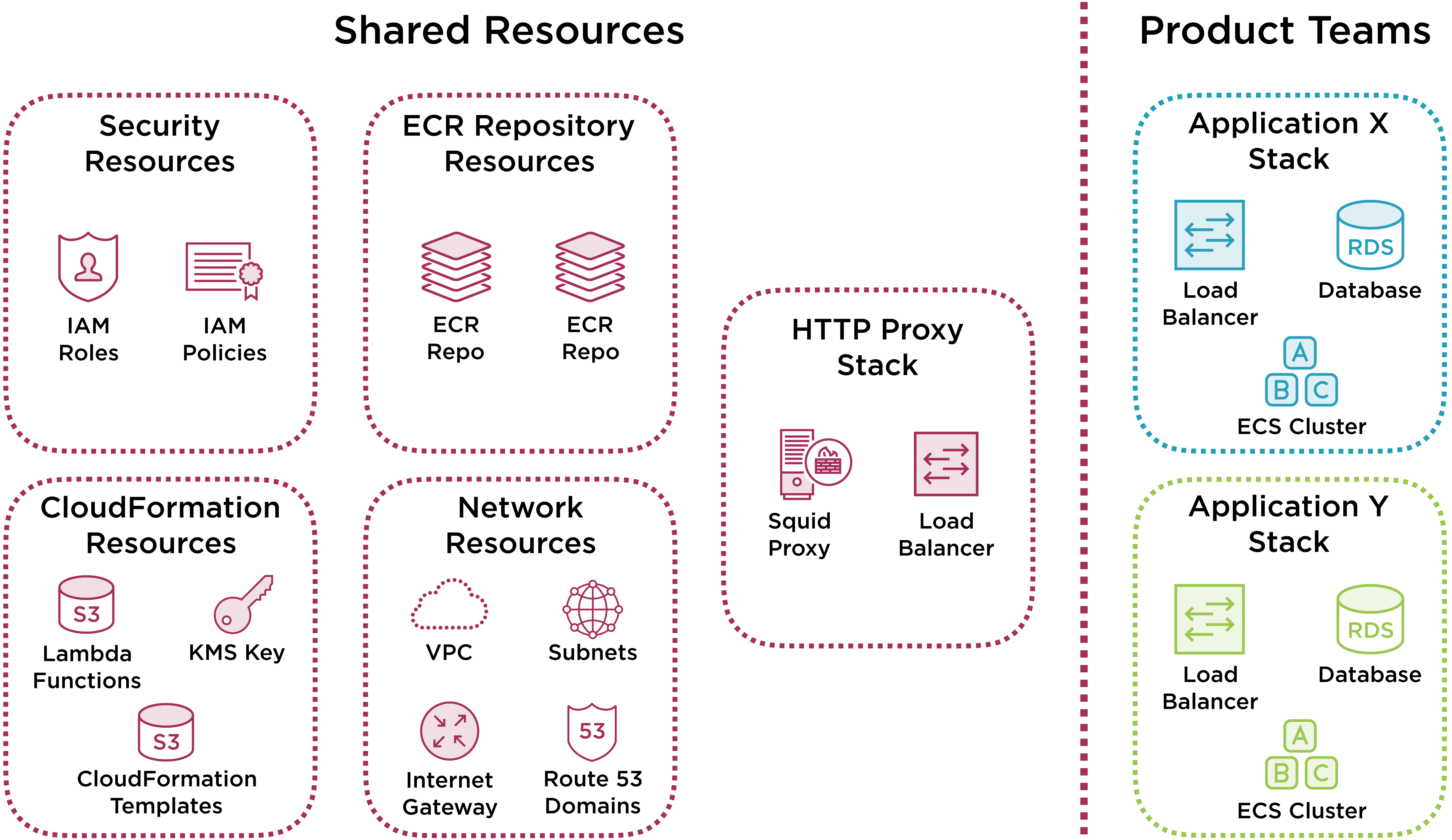
ECS Cluster

Database

Using AWS CloudFormation Role Templates

Creating the CloudFormation Resources Stack

Creating the EC2 Container Registry Stack



Shared Resources

Security Resources

IAM Roles

IAM Policies

ECR Repository Resources

ECR Repo

ECR Repo

CloudFormation Resources

Lambda Functions

KMS Key

CloudFormation Templates

Network Resources

VPC

Subnets

Internet Gateway

Route 53 Domains

HTTP Proxy Stack

Squid Proxy

Load Balancer

Product Teams

Application X Stack

Load Balancer

Database

ECS Cluster

Application Y Stack

Load Balancer

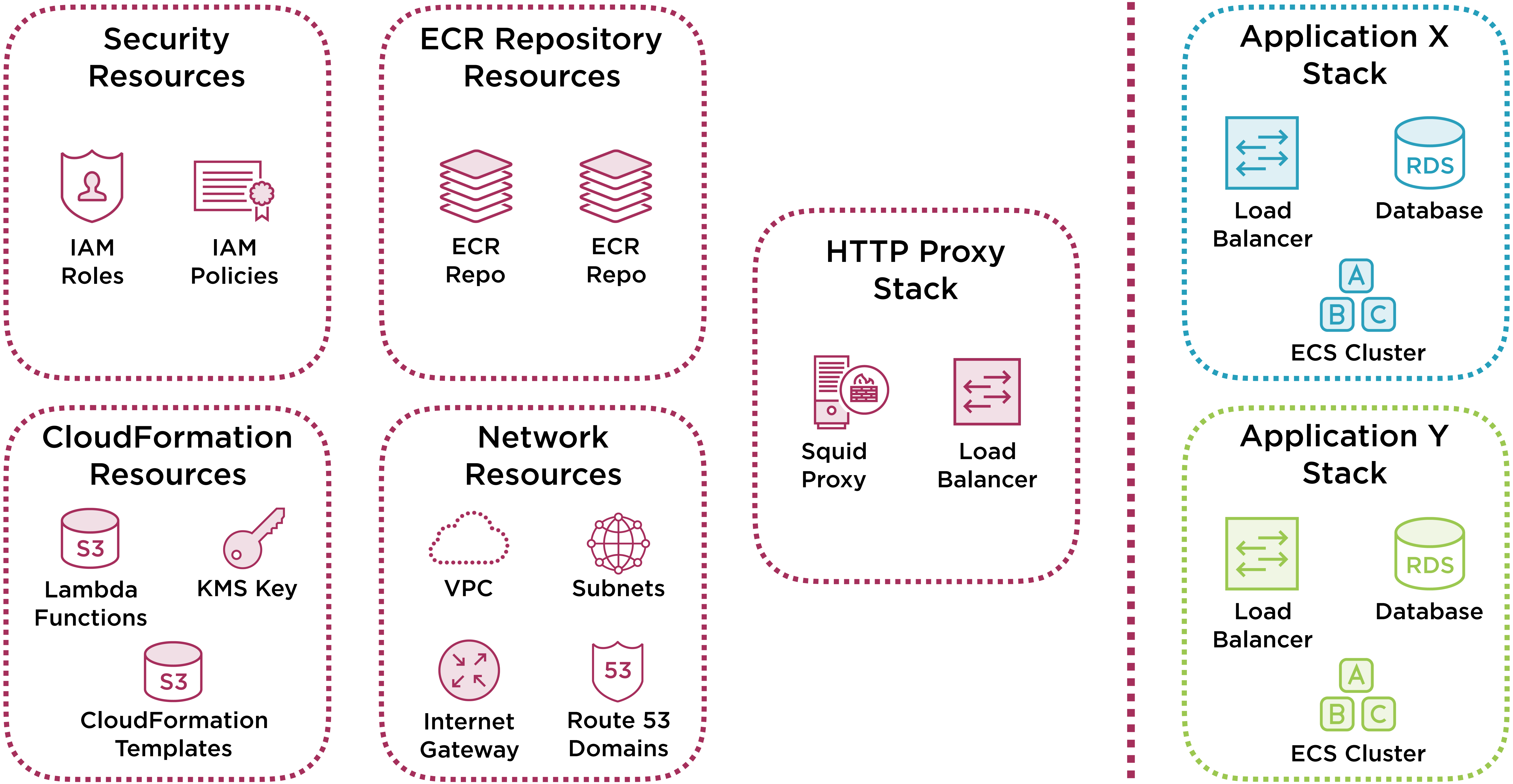
Database

ECS Cluster

Creating the Network Stack

Shared Resources

Product Teams



Security Resources

IAM Roles

IAM Policies

ECR Repository Resources

ECR Repo

ECR Repo

CloudFormation Resources

Lambda Functions

KMS Key

CloudFormation Templates

Network Resources

VPC

Subnets

Internet Gateway

Route 53 Domains

HTTP Proxy Stack

Squid Proxy

Load Balancer

Application X Stack

Load Balancer

Database

ECS Cluster

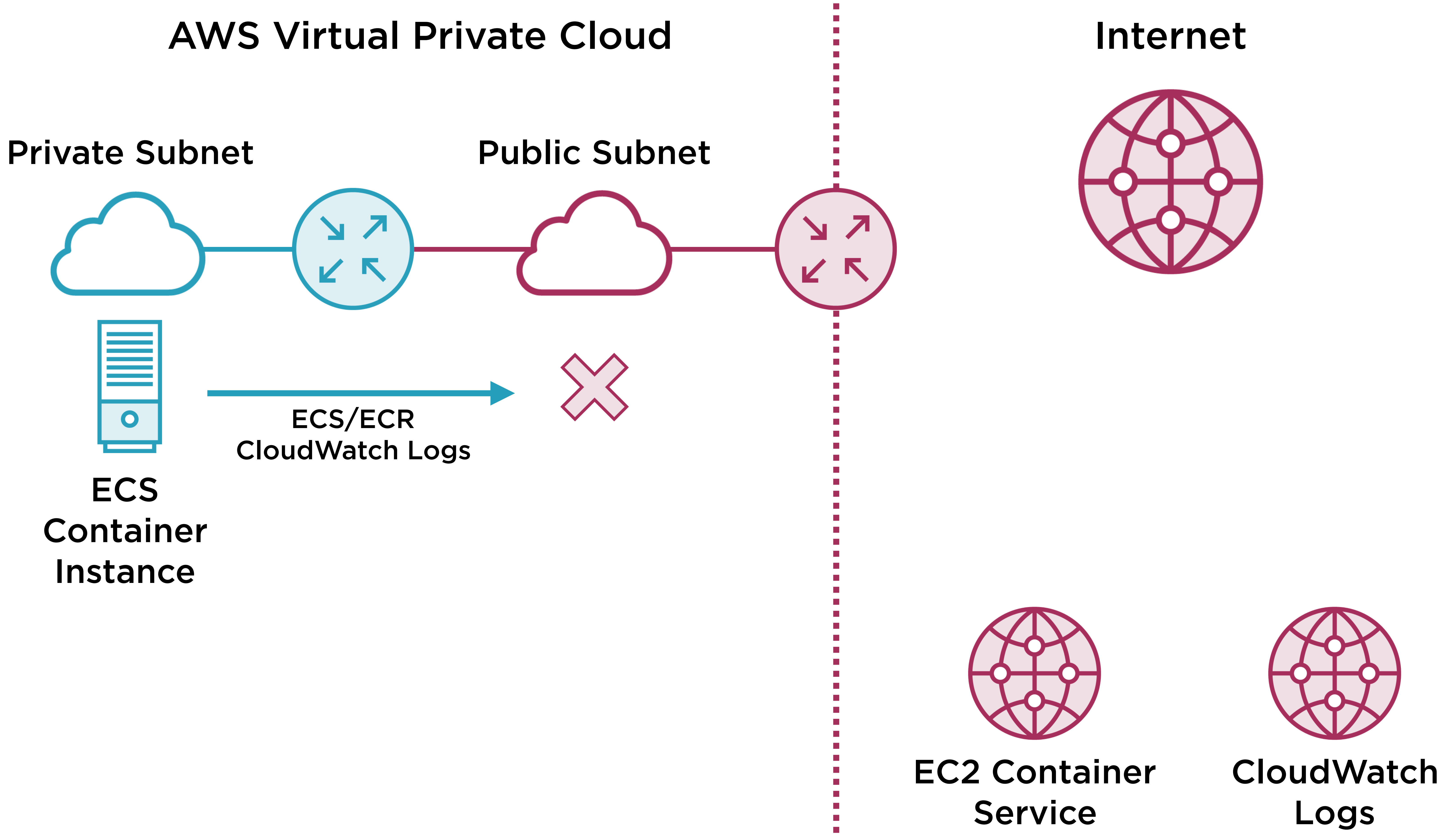
Application Y Stack

Load Balancer

Database

ECS Cluster

Publishing the Docker Squid Image



AWS Virtual Private Cloud

Internet

Private Subnet

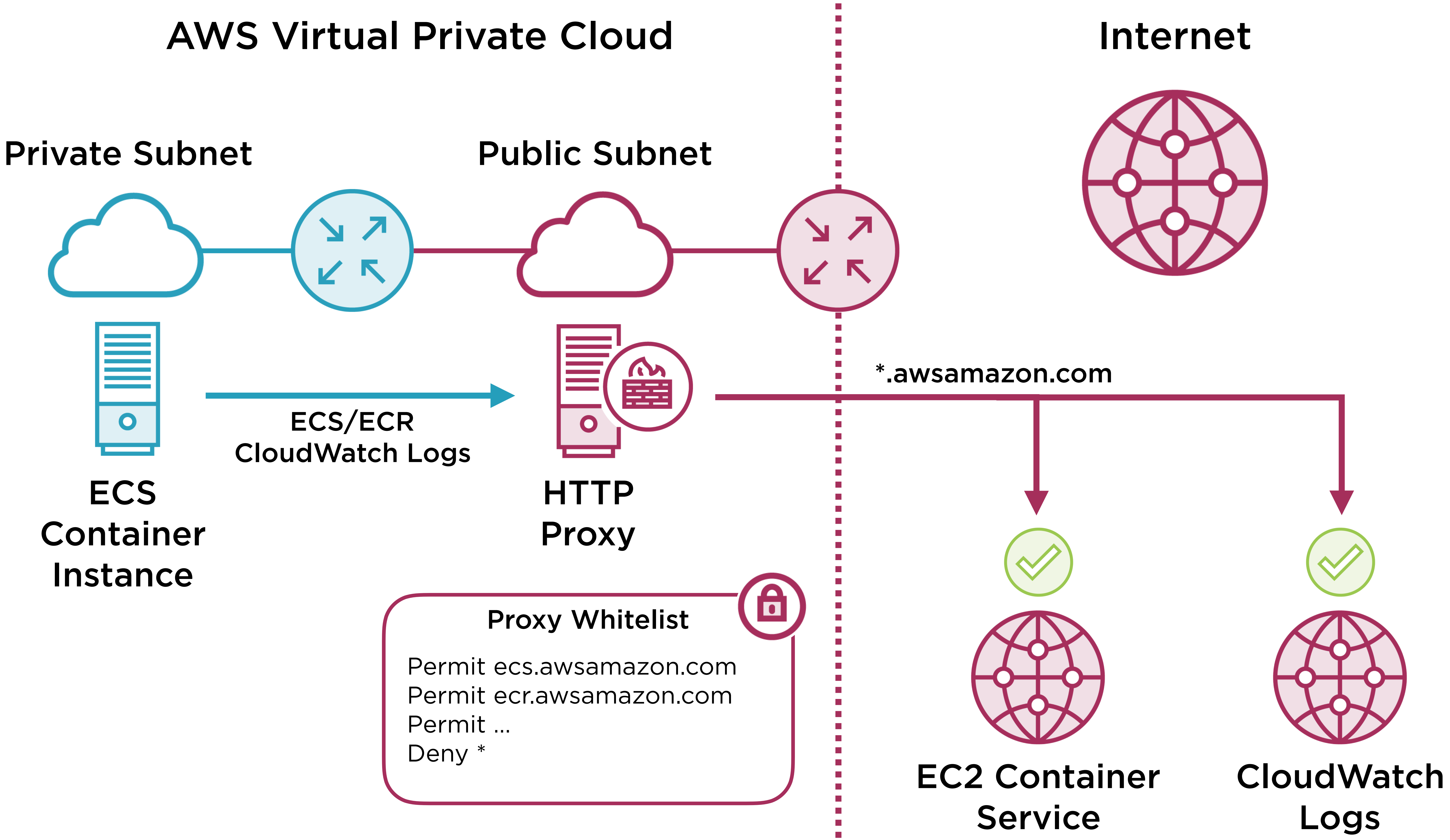
Public Subnet

ECS/ECR
CloudWatch Logs

ECS
Container
Instance

EC2 Container
Service

CloudWatch
Logs



Proxy Whitelist

Permit ecs.awsamazon.com
Permit ecr.awsamazon.com
Permit ...
Deny *

Creating the HTTP Proxy Stack

Deploying the HTTP Proxy Stack

Summary

Deploying AWS Infrastructure using Ansible and CloudFormation

- Shared resources
- Multiple environments
- Multiple accounts
- Complete environments
- Ansible roles
- Jinja templating
- Fully automated
- Infrastructure as Code