Prerequisites

- **You need to use your own AWS account with administrator access**
- This is an advanced security workshop that assumes knowledge of fundamental AWS services
- If you do not have an account, you are welcome to attend – we will be walking through the labs live
- All workshop material is public; you will be able to do these labs offline – https://tinyurl.com/mlmpworkshop
- $25 AWS credits will be provided to each participate to compensate for the labs
- You will not be writing code in this workshop – you'll simply execute it

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

MKT301

Build secure and compliant ML and data-backed applications

Lauren Mullennex
Solutions Architect
AWS

Om Patri
Customer Delivery Architect
AWS

Kanchan Waikar
Senior Solutions Architect
AWS

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

Agenda

- Workshop overview
- Setting up secure infrastructure for hosting your ML model
- Establishing governance and access control
- Self-service enablement at scale

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

Why did we create this workshop?

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

Asks:

- I want my customers to only deploy **specific** third-party ML models
- I want my customers to export **specific third-party datasets** only
- Datasets should be exported into team-specific S3 buckets
- I want my customers to only create Amazon SageMaker notebook instances within their own VPC
- I don’t want my customers to have access to other user’s notebook instances
- I want my customers to only use specific IAM roles when working with data
- My customers should access only their team-specific S3 buckets via Amazon SageMaker IAM role

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

Accelerate time to market

Remove undifferentiated heavy lifting

Automate and standardize security guardrails

Control user access and customize product procurement

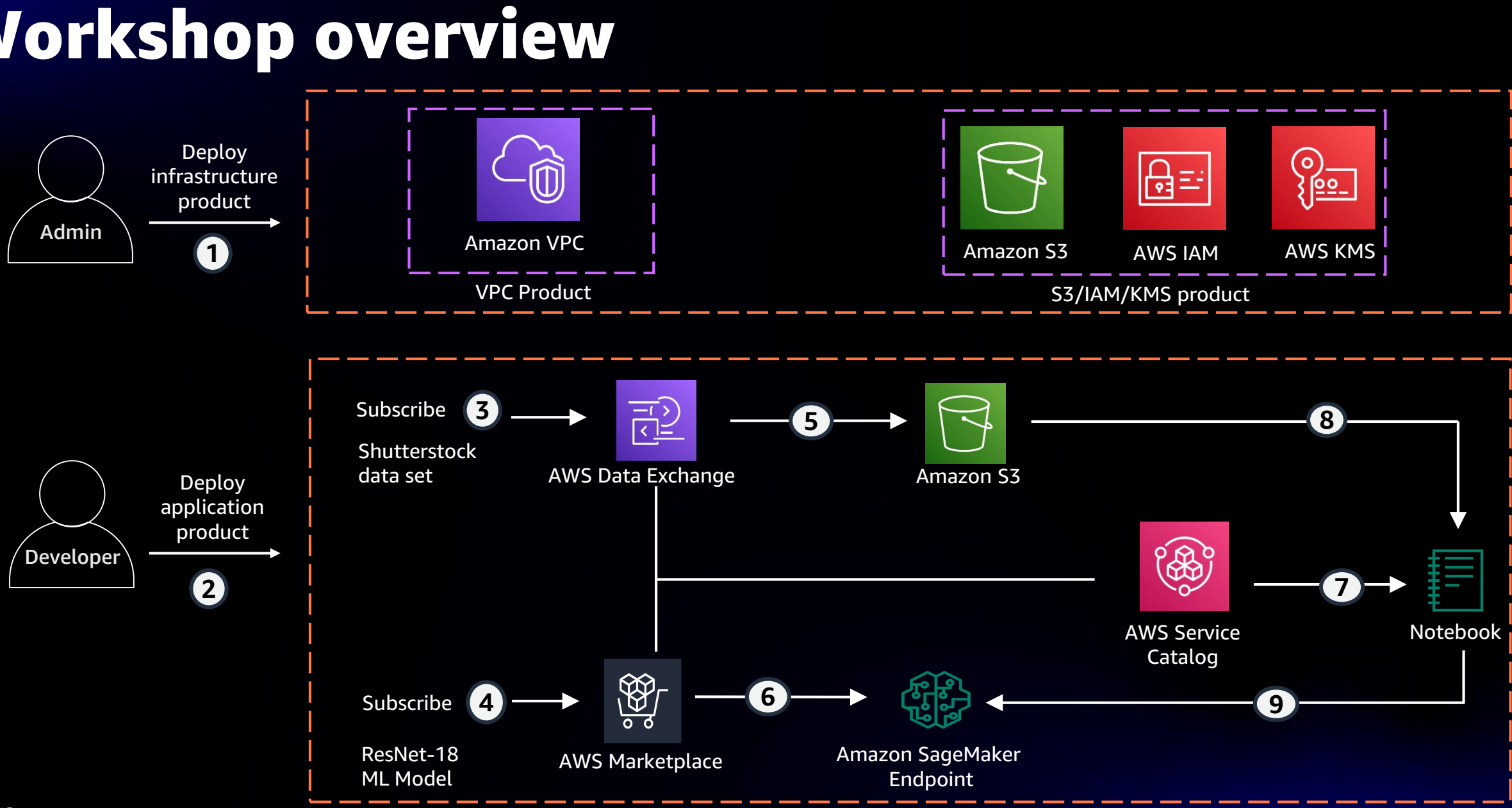
Spend more time achieving your business outcomes

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

Workshop overview

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

Workshop overview



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

Lab 1 – Subscribe to dataset and pre-trained ML model on AWS Marketplace

https://tinyurl.com/mlmpworkshop

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

> Pre-trained ML Models

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

> AWS Data Exchange overview

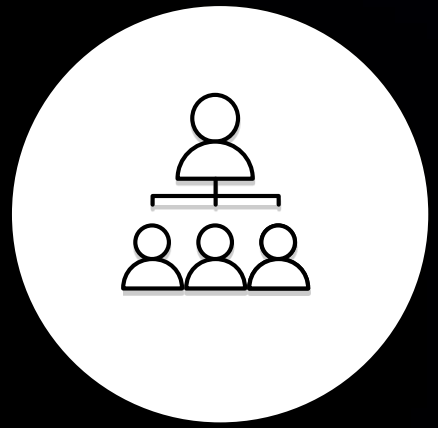
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lab 2 – Set up workshop environment

https://tinyurl.com/mlmpworkshop

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

Self-service provisioning via AWS Service Catalog



Organizations

Security

Curation

Compliance

Standardization

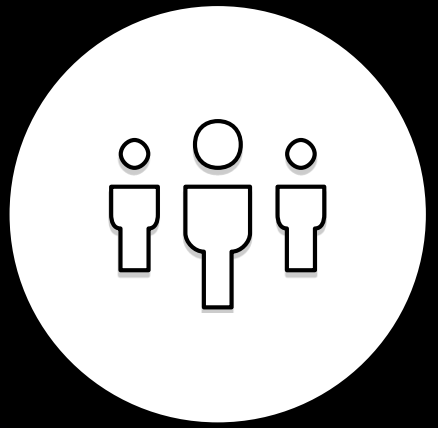


Speed

Agility

Self-service

Time to market



End users

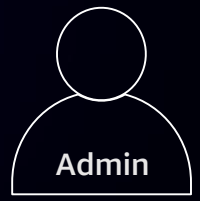
Service catalogs enable organizations to deploy and manage infrastructure and applications that reflect the organization's security and operational policies

aws

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



AWS services



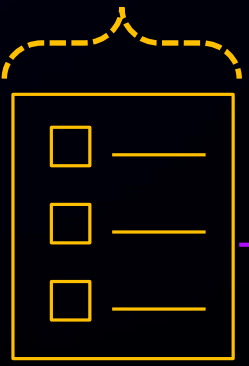
Defines standardized AWS products and curates compliant catalogs for teams



Customer-created AWS-based solution



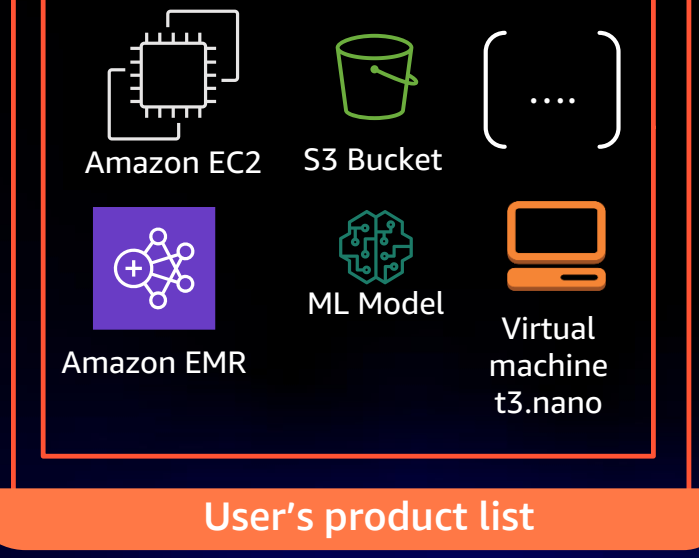
AWS Marketplace third-party products



JSON or YAML



AWS Service Catalog





User

Deploys AWS resources

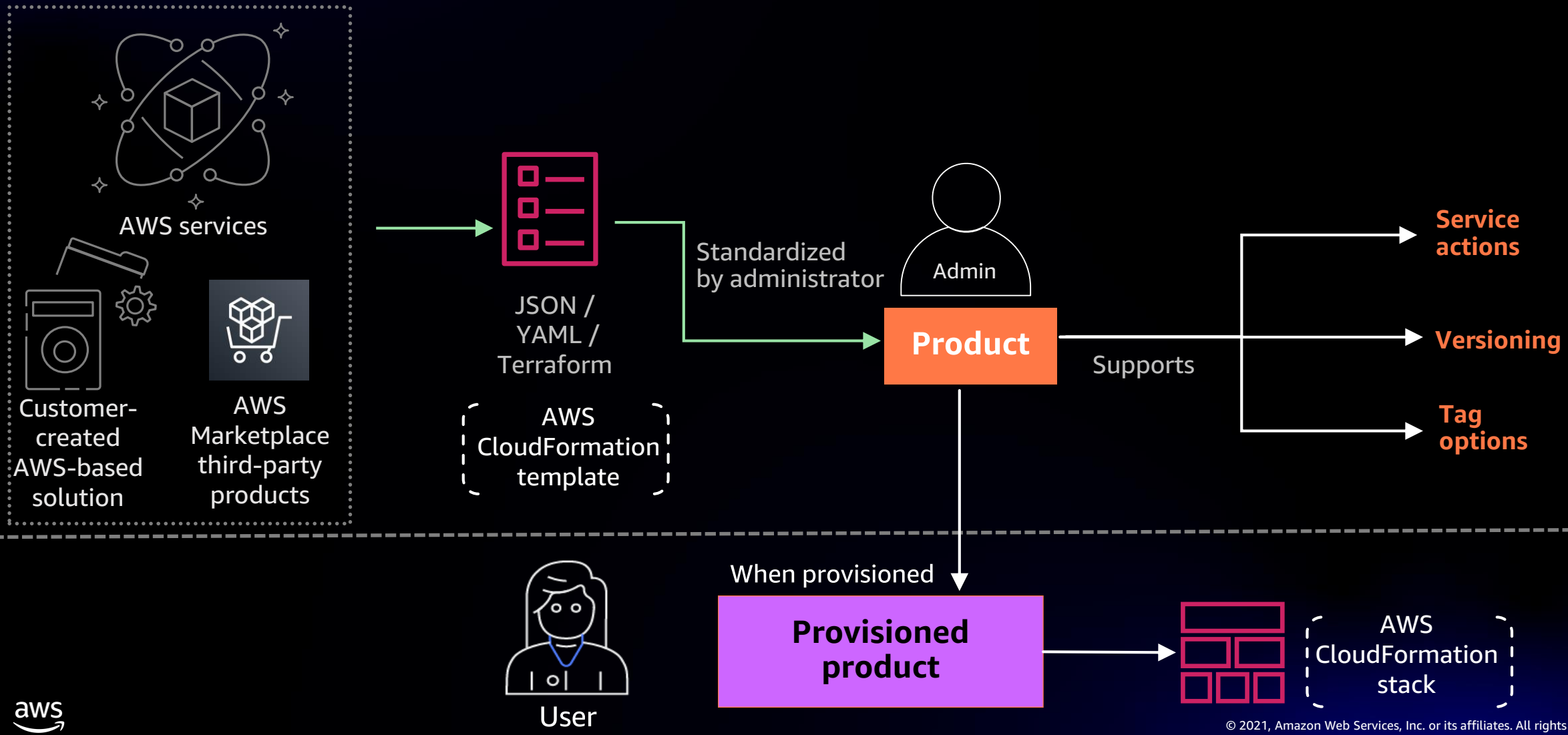


- ✓ Compliant with polices
- ✓ Correctly tagged
- ✓ Within budget

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

Products

CONTROL HOW A COMPLIANT AWS RESOURCE GETS CREATED



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

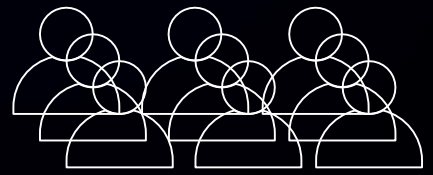
Portfolios

A COLLECTION OF PRODUCTS, TOGETHER WITH CONFIGURATION INFORMATION

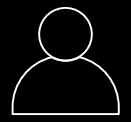
Portfolio

Control who should deploy which product

Generic



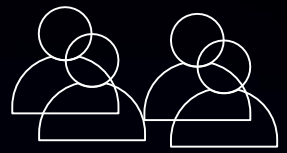
Individual



Team specific



Role based



Generic portfolio

- EC2 instance

Line of business administrator portfolio

- VPC connected to transit VPC
- An AWS account
- A Bastion host

Developer portfolio for team A

- An EC2 instance
- An RDS database

Developer portfolio for team B

- Amazon SageMaker notebook Instance
- Fargate cluster

Data scientist portfolio

- Amazon SageMaker Studio notebook instance backed by EMR cluster
- An EMR cluster

Web developer portfolio

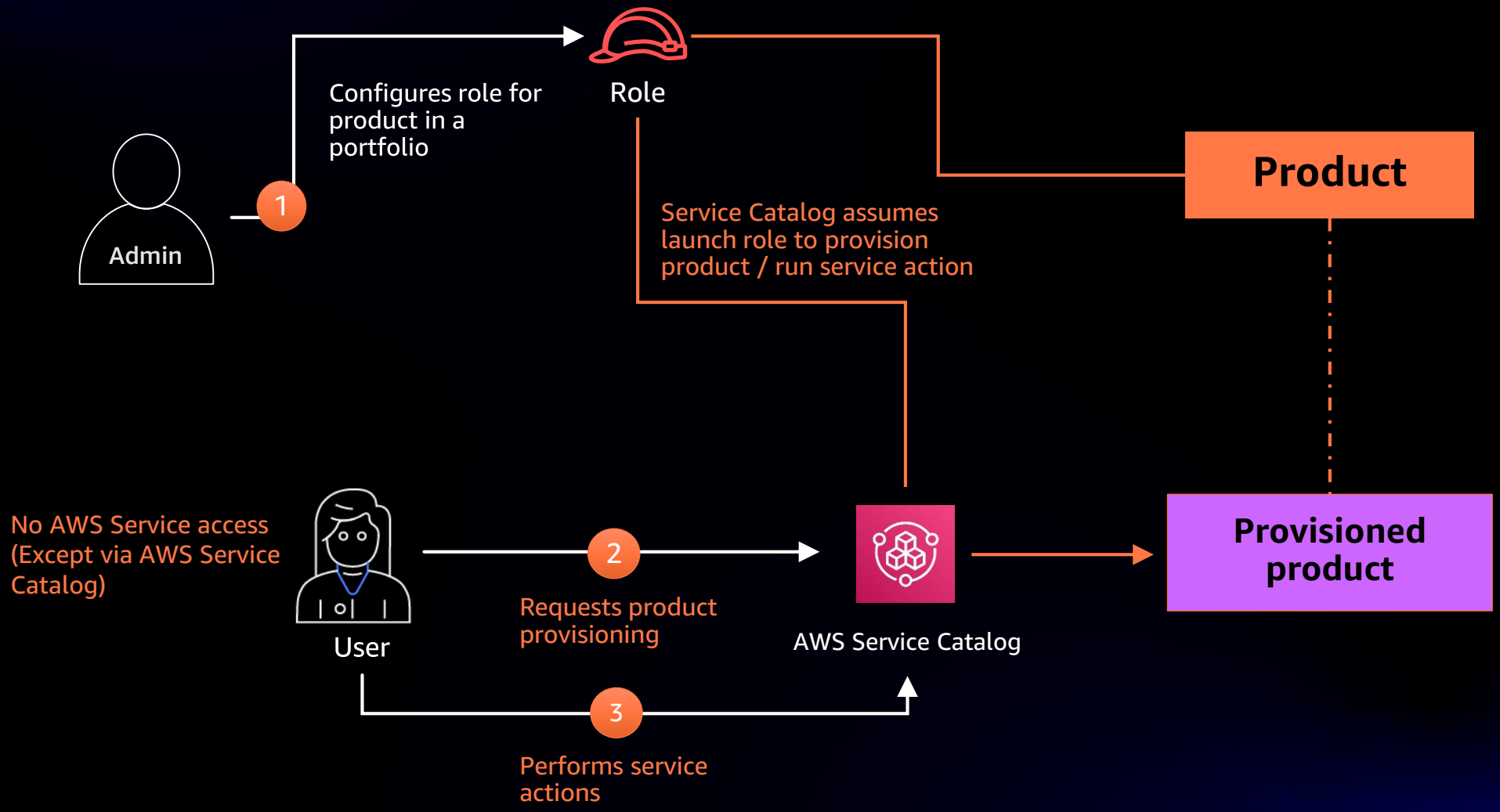
- Amazon Workspaces desktop

https://github.com/aws-samples/aws-service-catalog-reference-architectures

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

Launch constraints

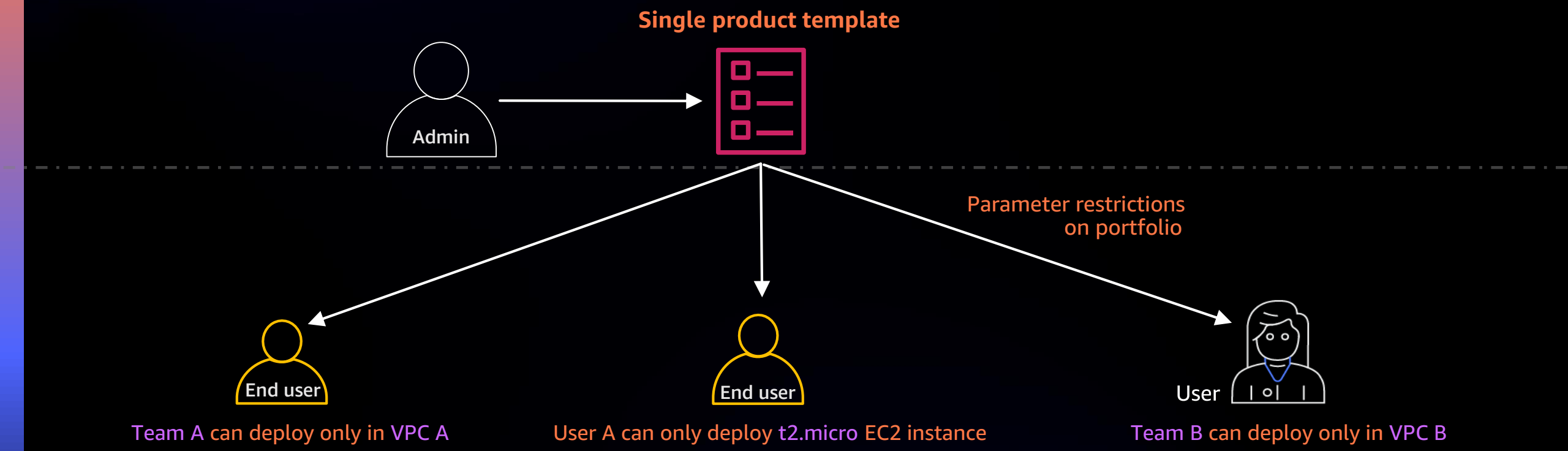
LIMIT USER'S PERMISSIONS WHILE ENABLING THEM TO DEPLOY PRODUCTS



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

Template constraints

ADD PORTFOLIO-PRODUCT SPECIFIC CONFIGURATION CONSTRAINTS



https://aws.amazon.com/blogs/mt/how-to-dynamically-constrain-parameter-options-in-aws-service-catalog-based-on-specific-tag-values

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

Catalog structure



Lead/admin user

Infrastructure portfolio

Team portfolio



Team user

Infrastructure product

Application product

VPC product

S3/IAM roles/KMS product

Data exchange product

ML model product

SageMaker notebook instance product

VPC product launch constraint

S3/IAM roles/KMS product launch constraint

Data exchange product launch constraint

ML model product launch constraint

SageMaker notebook instance product launch constraint

Notebook instance template constraint

ML model product template constraint

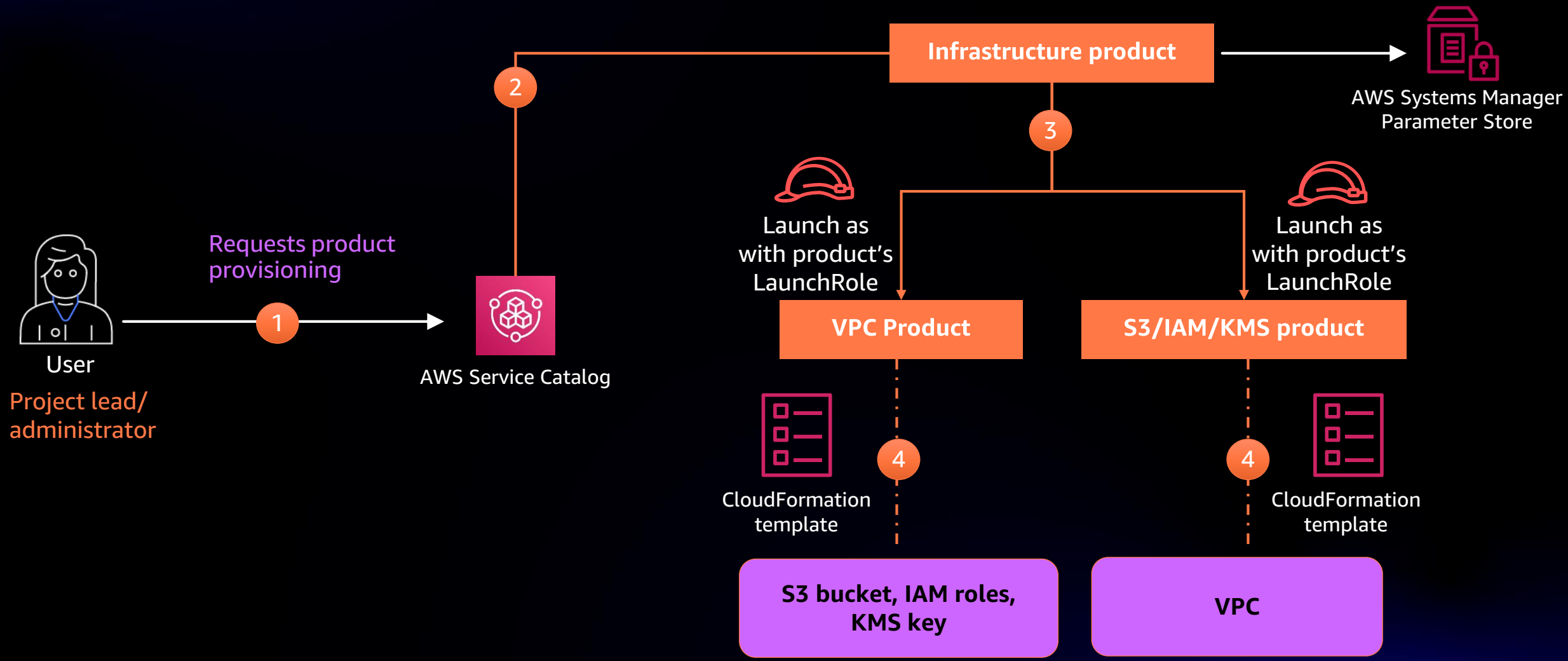
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lab 3 – Deploy the Infrastructure product

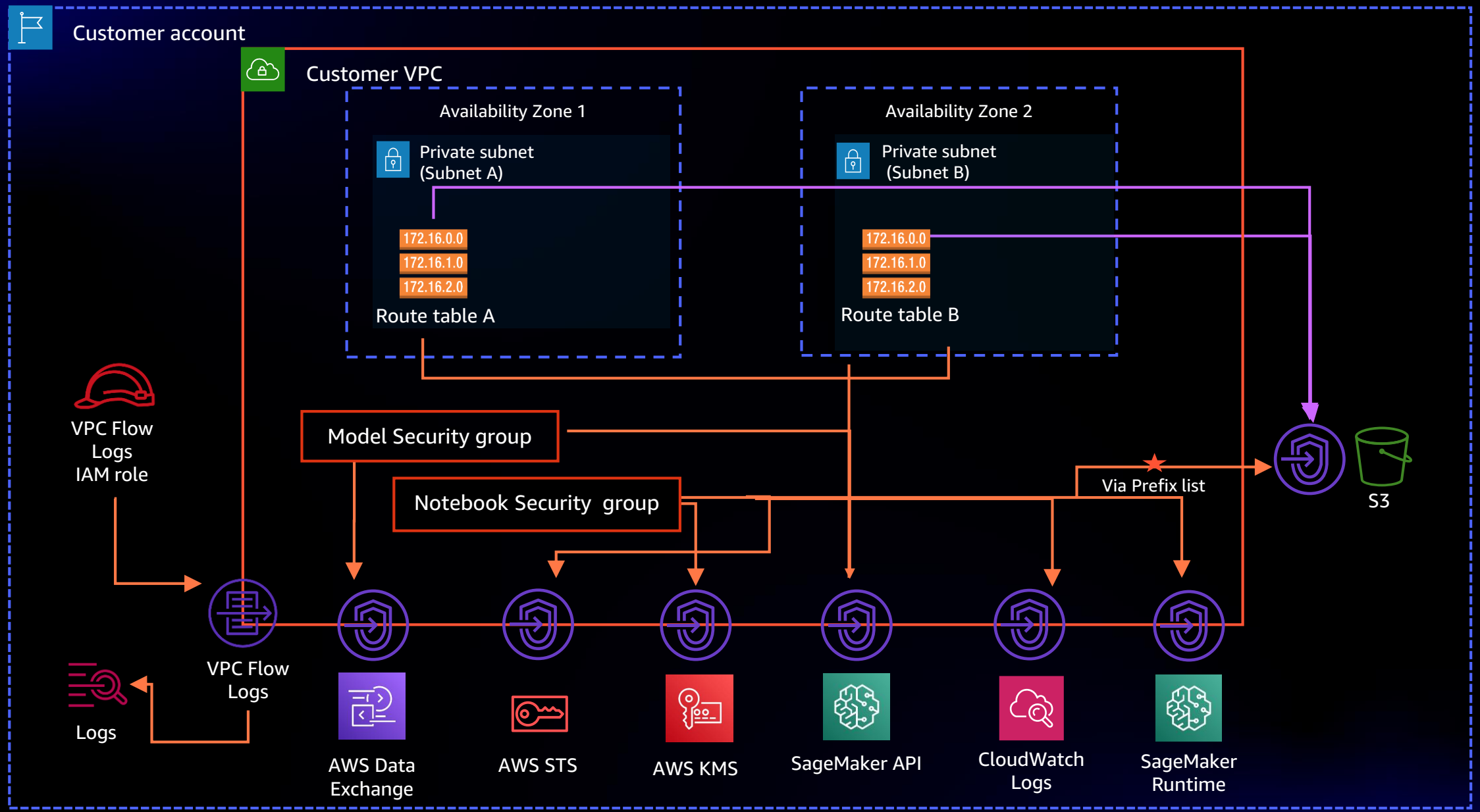
https://tinyurl.com/mlmpworkshop

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

Lab 3: Vending infrastructure

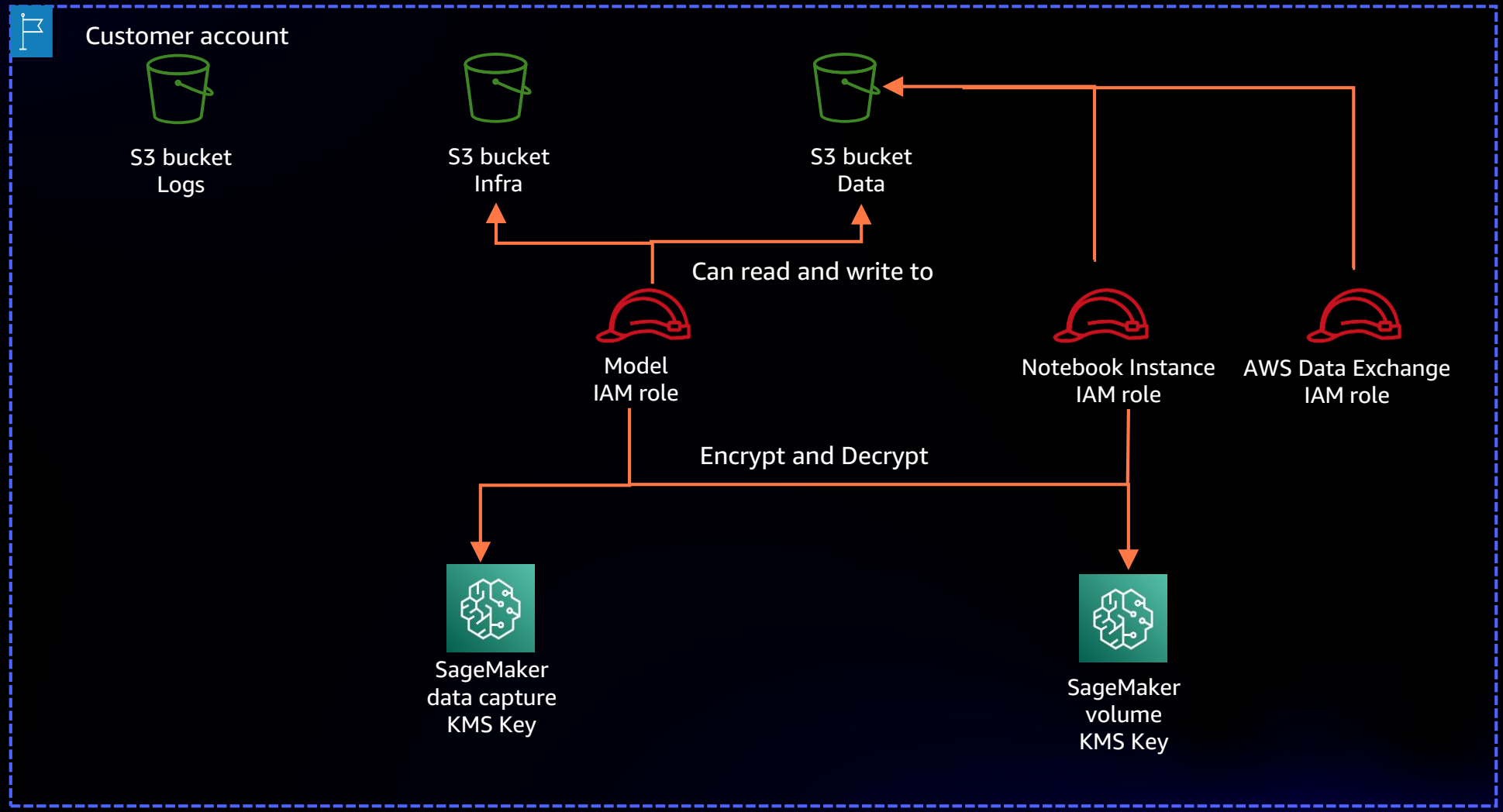


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



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

Product – S3/IAM roles/KMS keys



SageMaker API

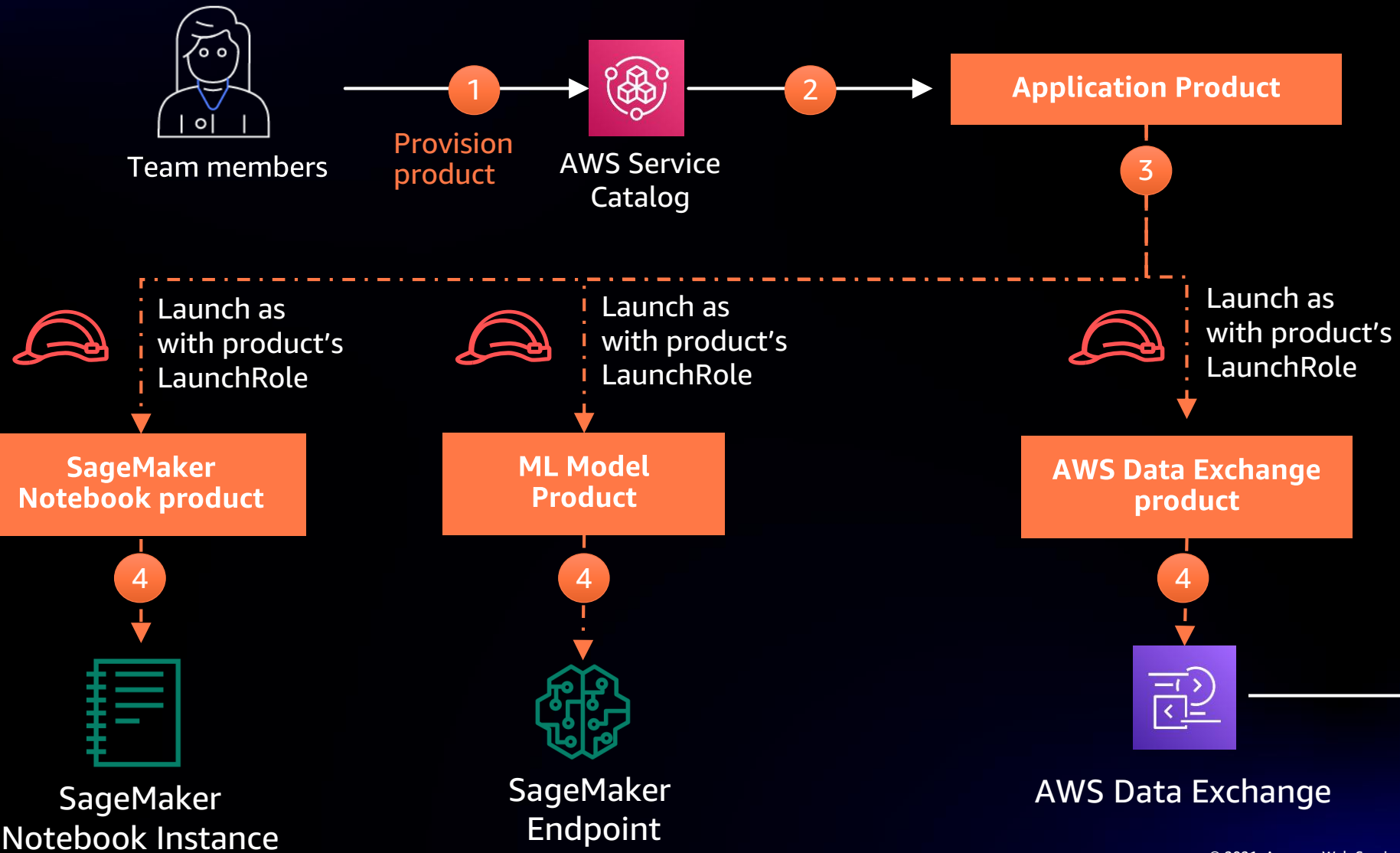
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lab 4 – Deploy the Application product

https://tinyurl.com/mlmpworkshop

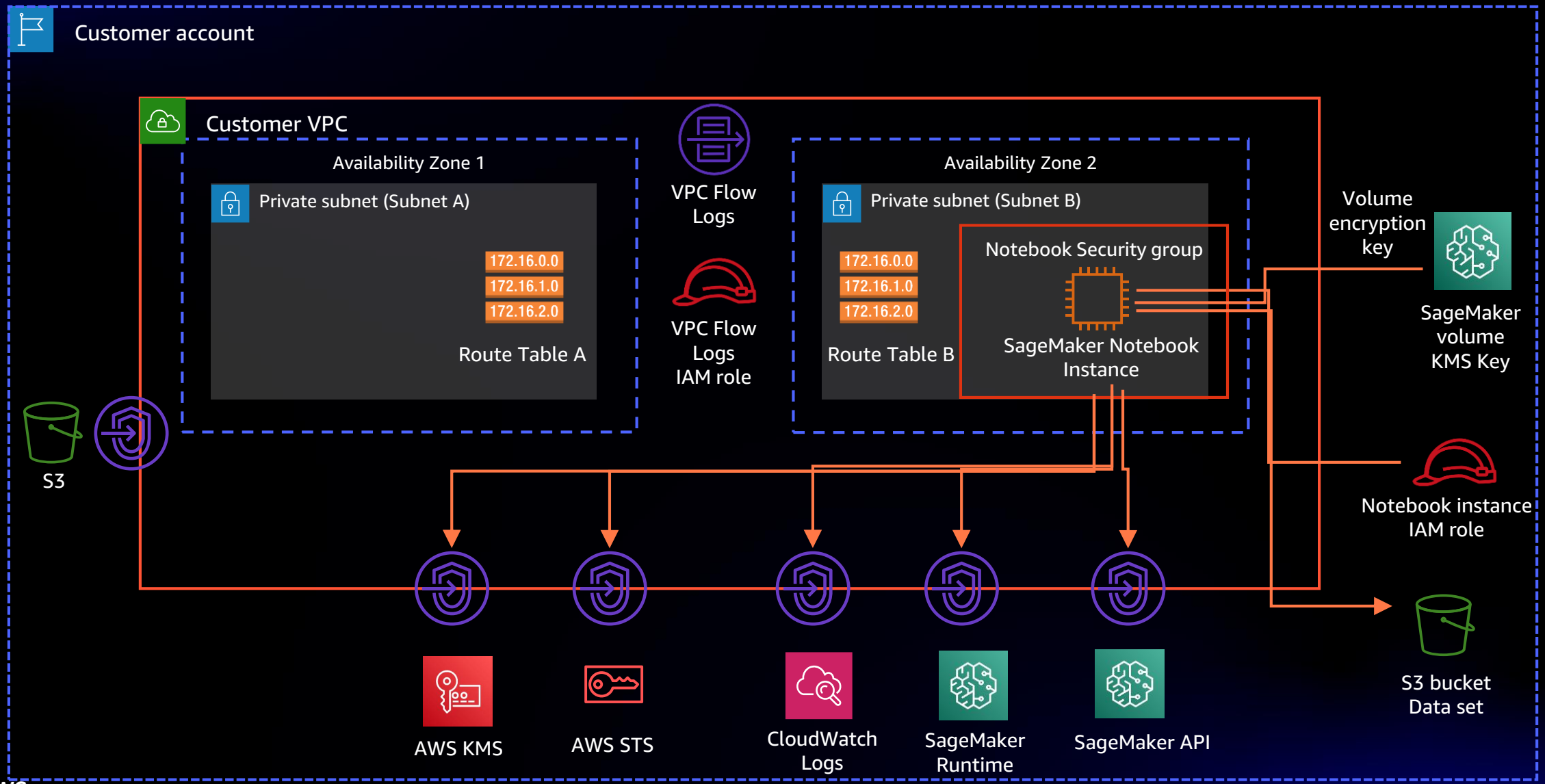
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lab 4: Vending application



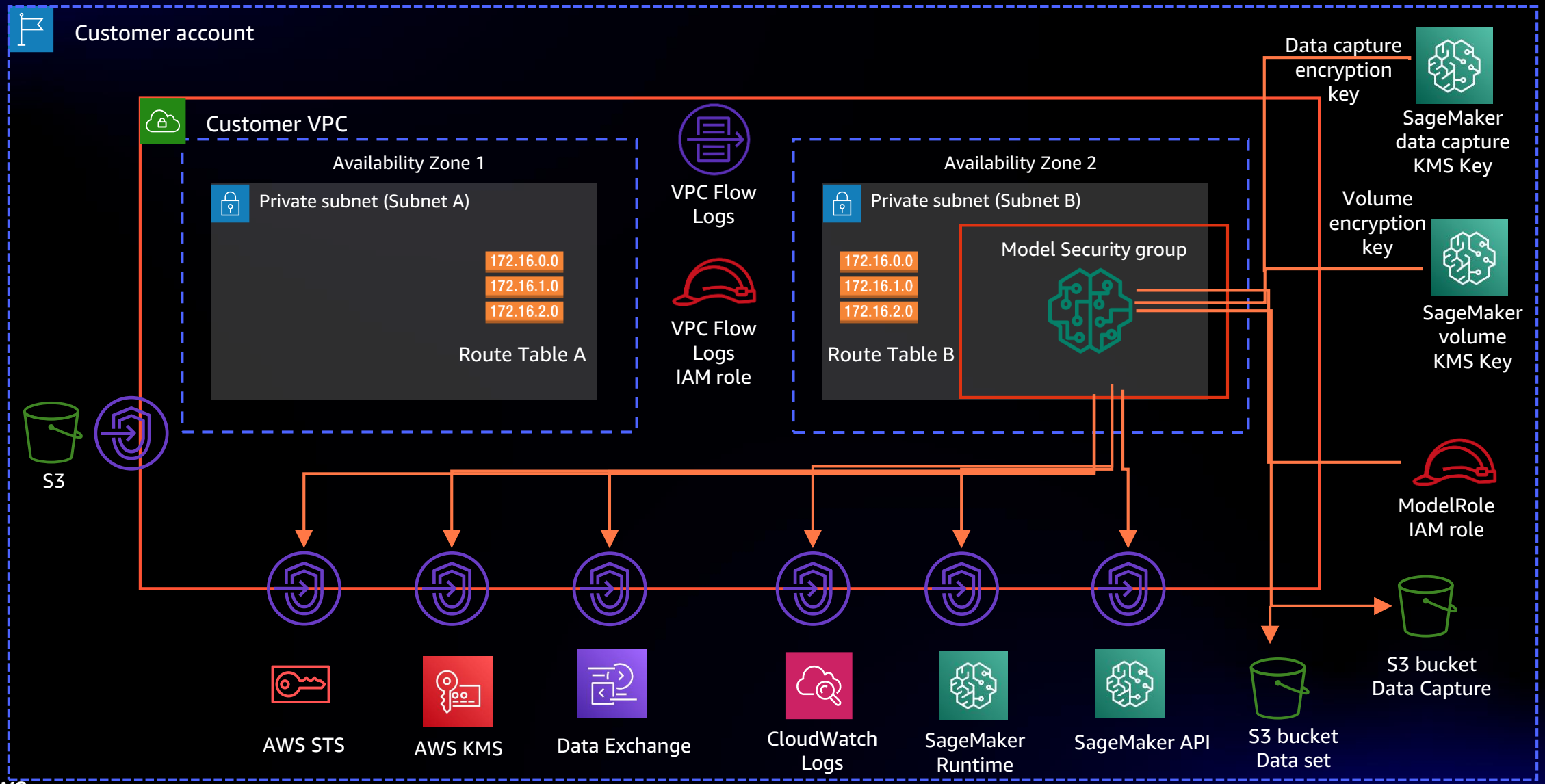
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lab 4: Notebook product



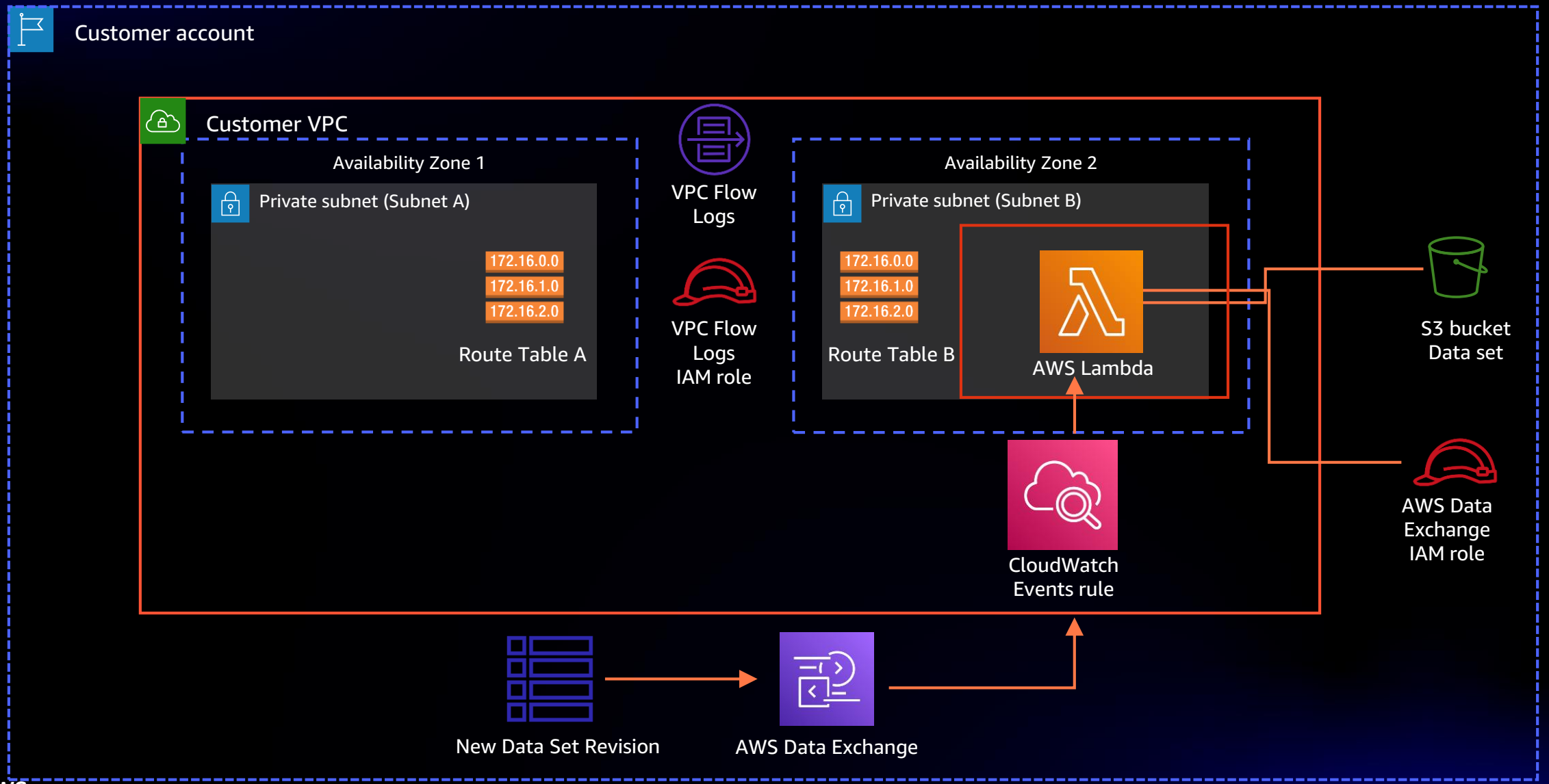
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lab 4: ML model product



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

Lab 4: AWS Data Exchange product



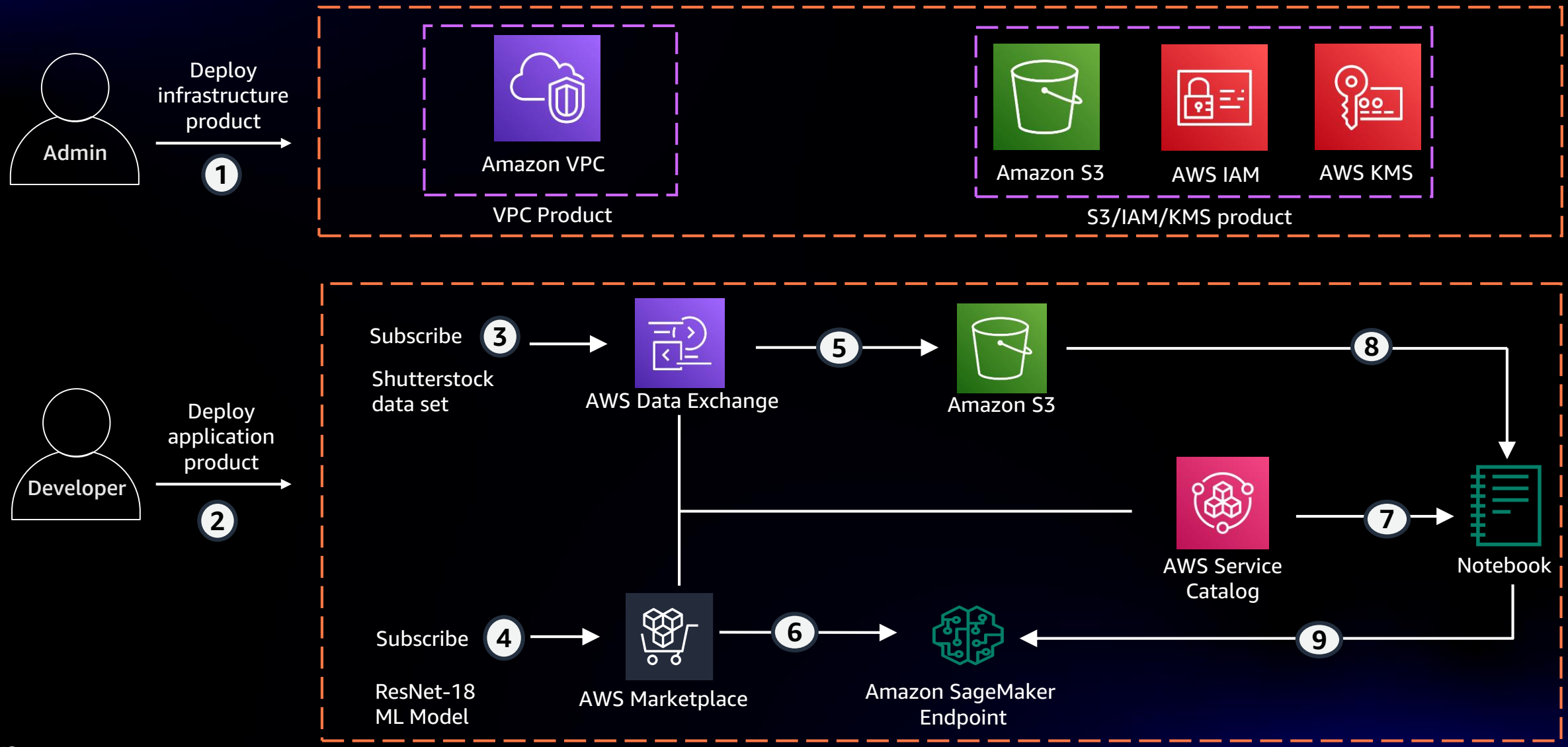
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lab 5 – Machine learning lab (optional)

https://tinyurl.com/mlmpworkshop

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

Workshop summary



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

Call to action

The workshop is available at https://tinyurl.com/mlmpworkshop

All code is available in the GitHub repo

Please clean up all AWS CloudFormation resources and S3 buckets

Need custom ML model that fits your use case?
Contact awsmp-ml-seller-inquiry@amazon.com

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

Thank you!

Lauren Mullennex
lemull@amazon.com

Om Patri
ompatri@amazon.com

Kanchan Waikar
kwwaikar@amazon.com

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