
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

CON307

Protecting production with Amazon ECS security features

Spiros Tsitsonis

Sr. PMT-External Services,
Amazon Elastic Container Services

Sharanya Devaraj

Sr. Software Development Engineer,
Amazon Elastic Container Services

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Topics

A Fundamental Enterprise Pillar

The ECS Security Model - Isolation & Segregation by Design

ECS Security Features

Security Feature Administration Use Cases

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A Fundamental Enterprise Pillar

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

"Enterprises have compliance teams and tight regulatory requirements, and they can't purchase a tool like ours if we don't meet their expectations. Being on AWS gives us credibility in the enterprise space by enabling us to check every box and answer our users' security questions confidently."

John Eitel

Global Vice President of Sales and Success, Canva

aws © 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Access, Workflow and Data Security

A Fundamental Enterprise Pillar

Canva for Enterprise pillars

- Reliability
- Scalability
- Security

Amazon ECS (Image Processing)

Amazon IAM (Authentication & Authorization)
Amazon Key Management Service (Encryption)
Amazon S3 (Data Storage)
Amazon SageMaker (Machine Learning)
Amazon Personalize (the User Experience)
Amazon Inspector (Security Assessments)



“AWS has always provided scalability, enhanced security, and high availability,” says Jim Tyrrell, head of Infrastructure at Canva.

https://aws.amazon.com/solutions/case-studies/canva-case-study/

aws © 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud Security Areas

Authentication (Identity) & Authorization (Access)



AWS Identity and Access Management (IAM)

Intelligent Threat Detection & Protection



Amazon GuardDuty

Data Protection & Secrets Management



AWS Certificate Manager (ACM)



AWS Secrets Manager



AWS Key Management Service (AWS KMS)

Network & Application Protection



AWS Firewall Manager



AWS WAF (Web Application Firewall)

Vulnerability Management



Amazon Inspector

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud Security Areas - Observability

Log Ingestion & Retrieval



Amazon CloudWatch



Amazon Kinesis Data Firehose

Metrics Monitoring & Analytics (Dashboarding)



CloudWatch Insights



AWS Distro for OpenTelemetry



Amazon OpenSearch



Amazon Managed Service for Prometheus



Amazon Managed Grafana

Troubleshoot Tracing



AWS CloudTrail



AWS X-Ray



APN Partner Services



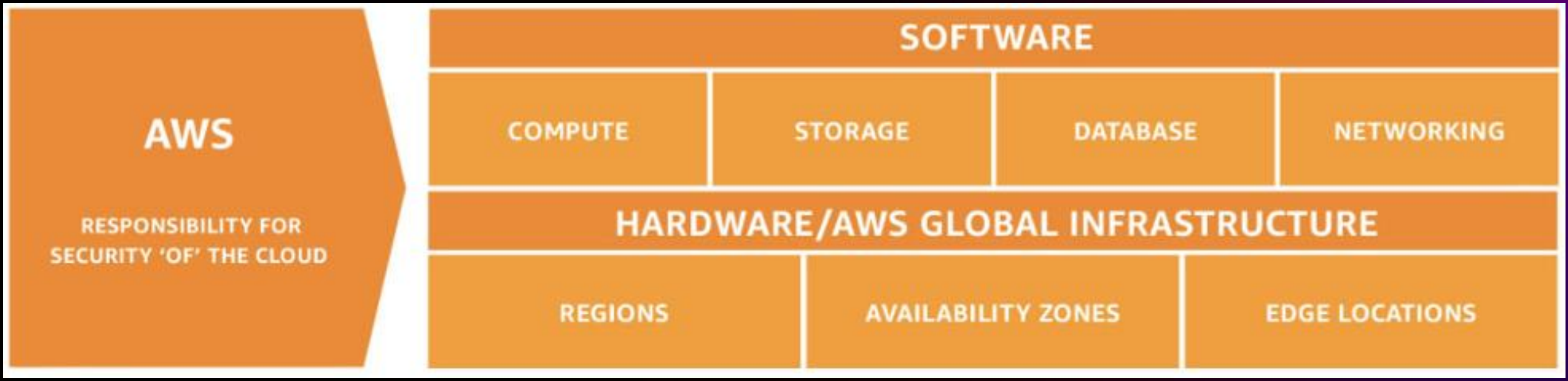
APN Partner Services



APN Partner Services

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

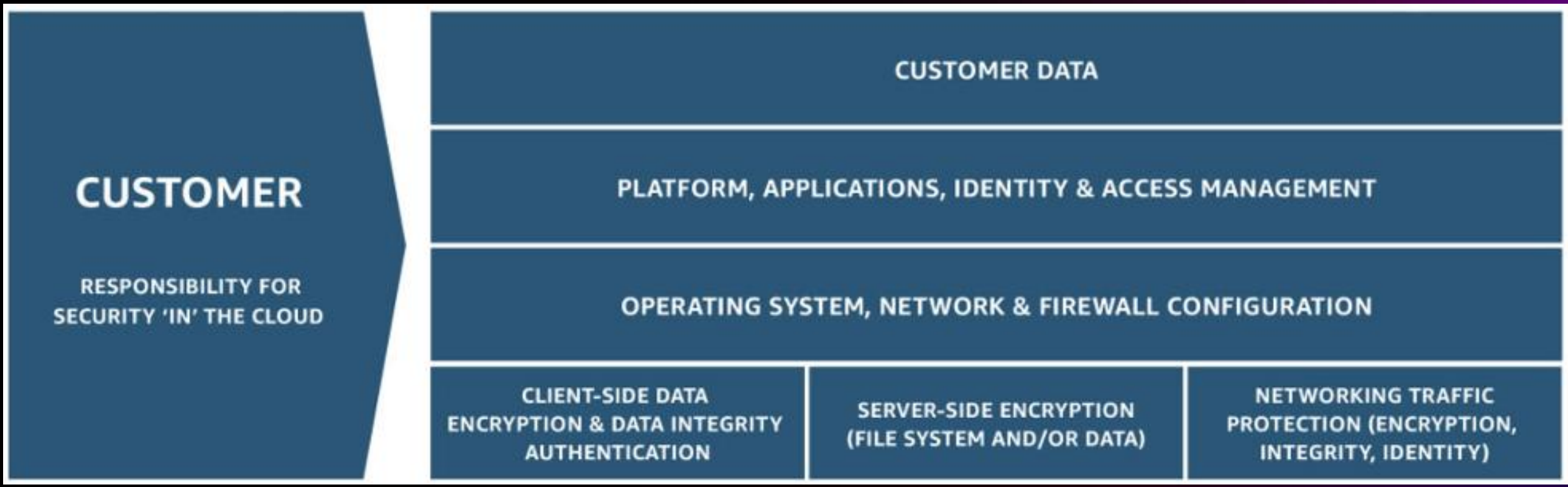
AWS Shared Responsibility Model for Security



- Amazon ECS
- Ancillary AWS Services Infrastructure
- AWS Security Services

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Shared Responsibility Model for Security



- Customer Data
- Applications
- Access Policies & Enforcement

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon ECS – Unprecedented scale



Over 2.25 billion

Tasks launched every week

Tens of thousands

API requests served per second

27 AWS Regions, 6 continents

Global presence

65% of all new AWS containers customers

Use Amazon ECS

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Compliance

ECS is certified on:

PCI, HIPAA, SOC, ISO/CSA STAR, ISMAP, MTCS, C5, HITRUST CSF, FINMA, PiTuKri, FEDRAMP, DoD CC, IRAP, K-ISMS, ENS-High, OSPAR, GSMA, CCCS

FINMA	Swiss Financial Market Supervisory Authority
GSMA	Global System for Mobile Communications Association
PiTuKri	Criteria for Assessing the Information Security of Cloud Services
CCCS	Canadian Centre for Cyber Security

https://aws.amazon.com/compliance/services-in-scope/

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon ECS: Isolation & Segregation by Design

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

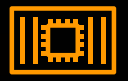
Self hosted container infrastructure

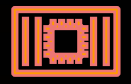


Amazon Elastic Container Service (ECS)

AZ – 3

EC2 instance





Availability Zone (AZ) – 1

EC2 instance





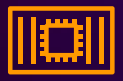
EC2 instance

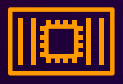




AZ – 2

EC2 instance



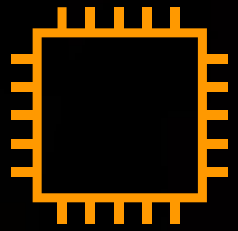


aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ECS Security Model

EC2 Launch Type: Inherent Security at the compute instance level



Hardware virtualization

isolated compute



Network isolation*

dedicated ENIs



Storage isolation

dedicated storage



Credentials isolation*

Isolated long-term credentials



Hands-off patching

Infrastructure always patched

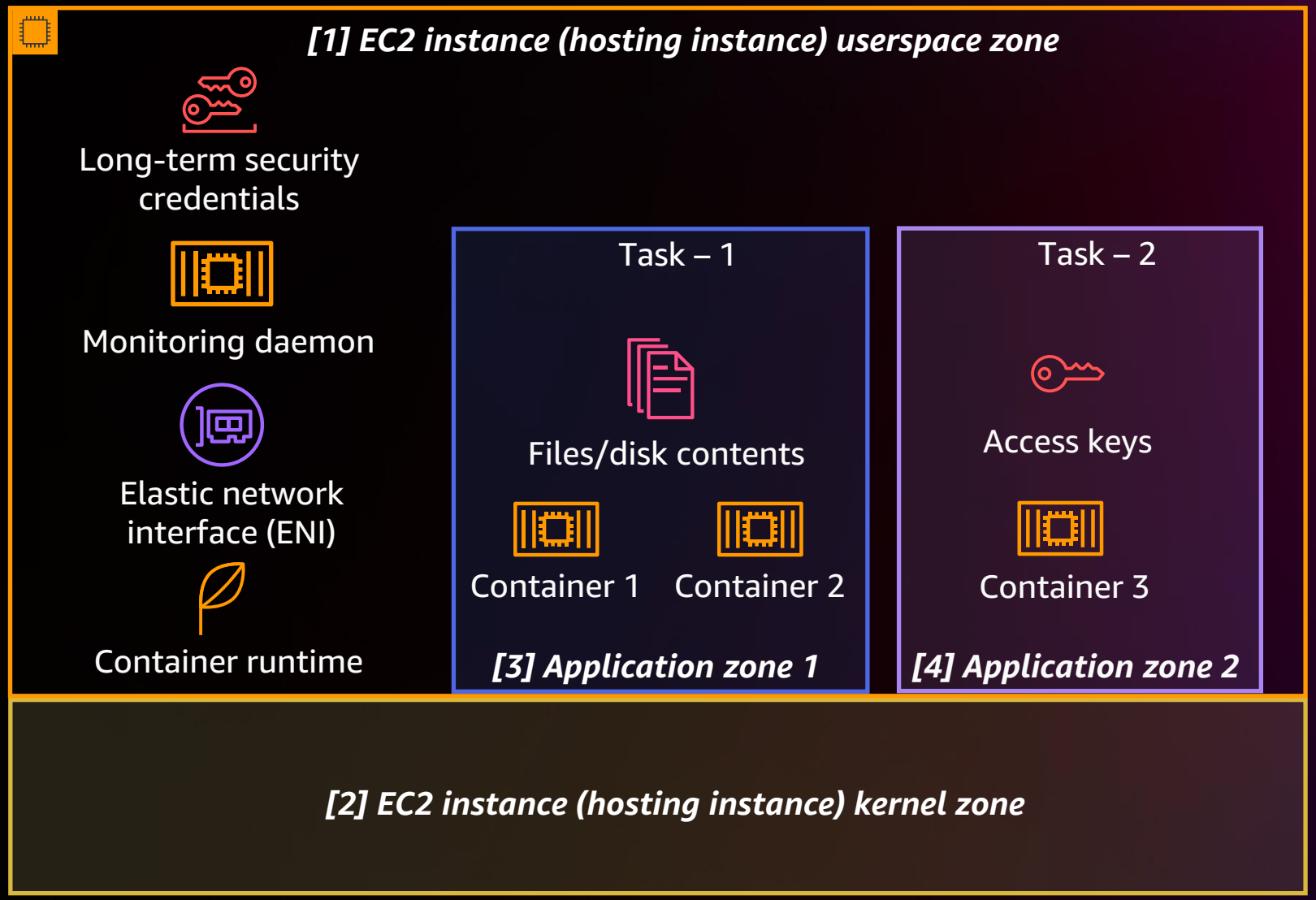
*ECS can further isolate ENI, Credentials into the Task levels

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ECS Trust boundaries

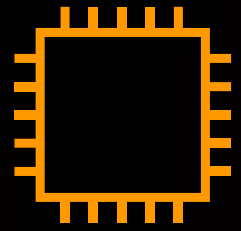
EC2 launch type



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ECS Security Model

Fargate Launch Type: Inherent Security at the task instance level



Hardware virtualization

isolated compute



Network isolation

dedicated ENIs



Storage isolation

dedicated storage



Credentials isolation

credentials scoped to applications



Hands-off patching

Infrastructure always patched

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ECS Trust boundaries

Fargate launch type

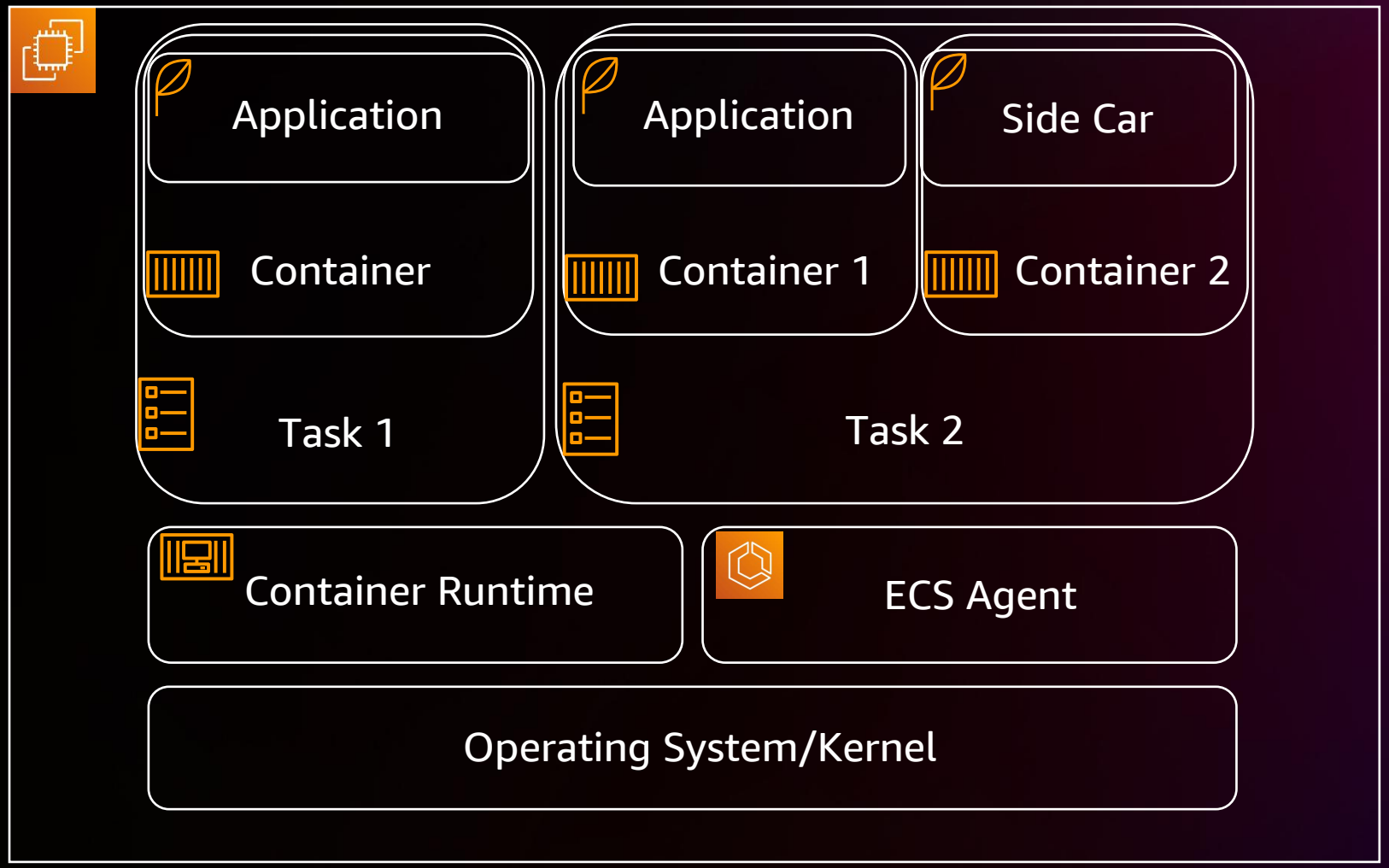


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon ECS Security Features

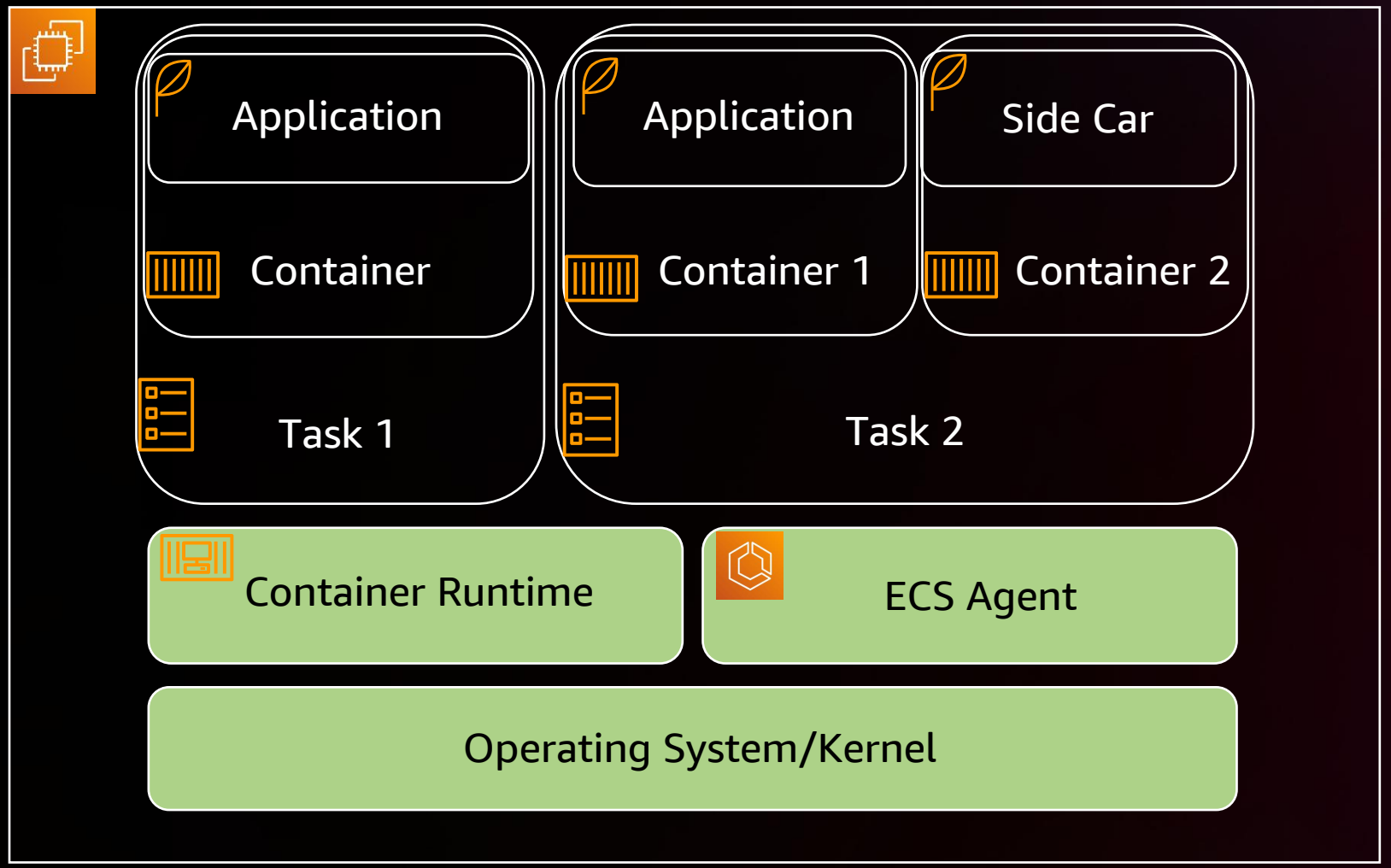
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon ECS Architecture



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

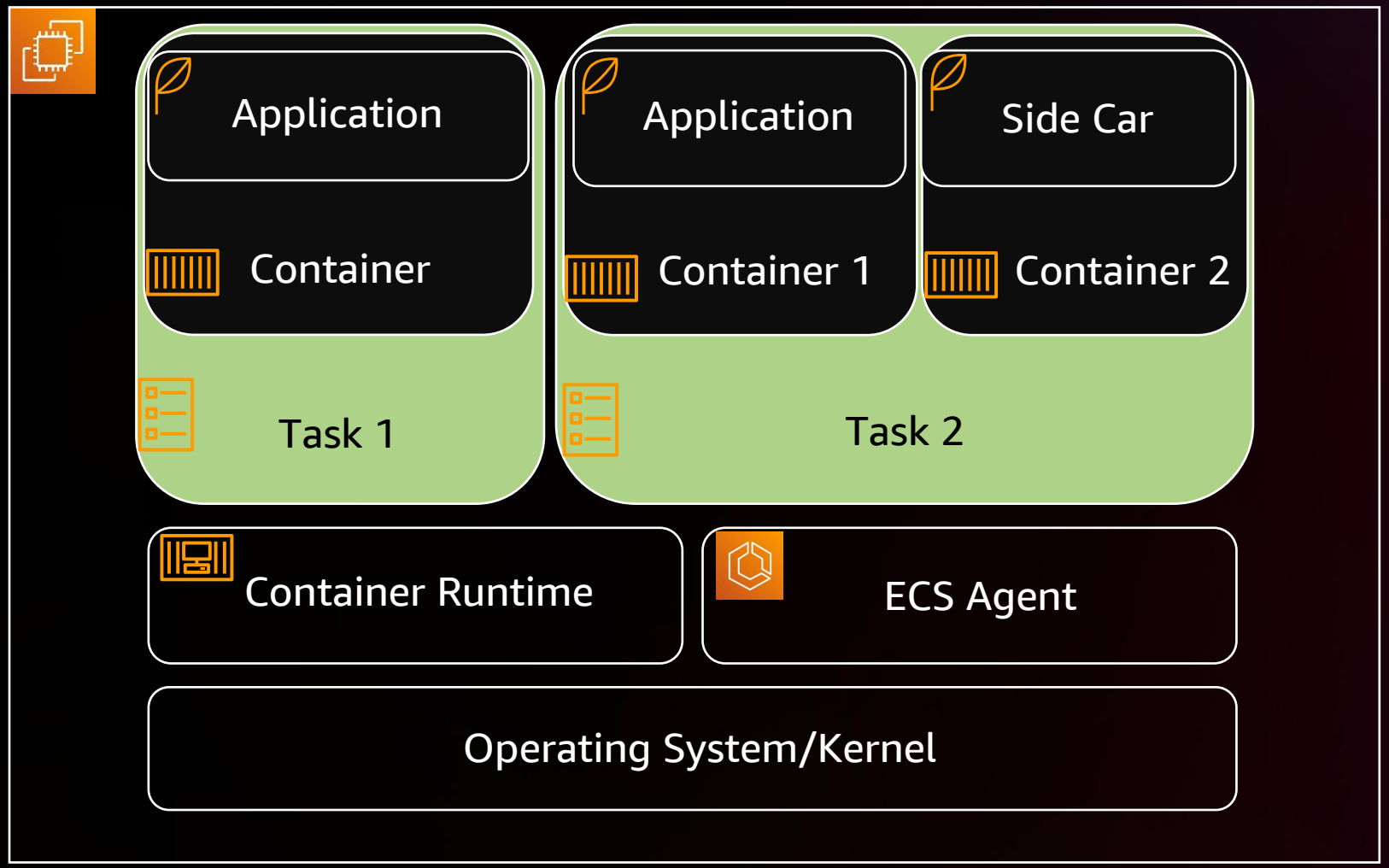
Compute/Infrastructure Security



- Compute Segregation
- Infrastructure Patching
- Security Groups, Network ACLs, IAM Role for Container Instances
- AWS PrivateLink

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

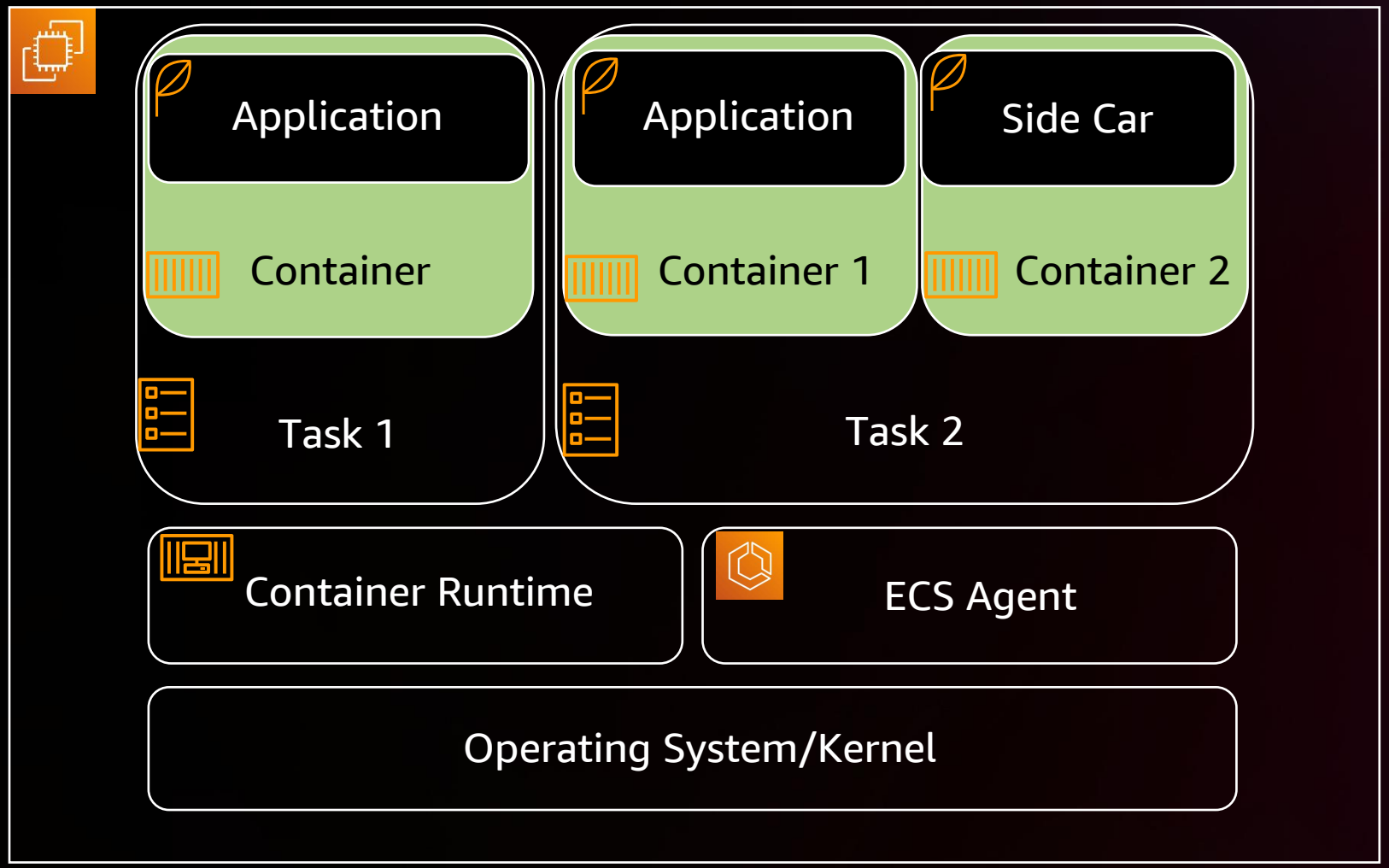
Task Security



- IAM Role for Tasks
- Task Execution Role
- Dedicated ENI for Tasks
- Storage Isolation
  - Ephemeral storage
  - Amazon EFS volume

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

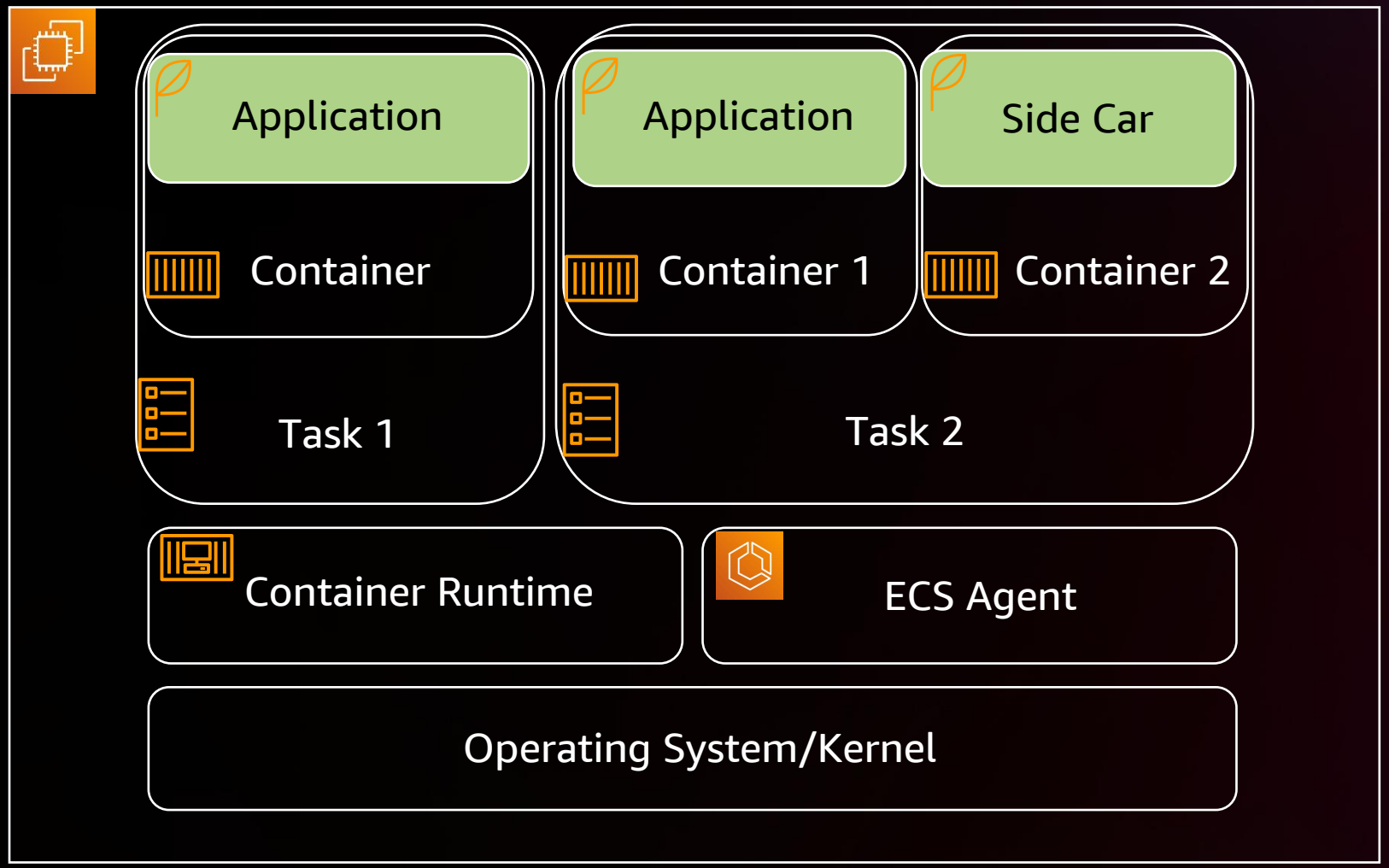
Container Security



- Container Secrets
- Linux Kernel capabilities
- Ulimits
- User Options
- Image Scanning
- Image Pruning

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Application Security



- Transport Layer Security (TLS) – AWS App Mesh
- Tag-based Access Control
- Log Routing
- Metrics Reporting
- Audit & Tracing
- Execute Command for Debugging

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Feature Administration Use Cases

6 Use Cases

3 Personas

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use case #1: Security vulnerability found in an OS level package. How do I patch it?

Persona: DevOps

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compute/Infrastructure Security

ECS on Fargate

- Hands-off patching
    - Fargate Platform Version (PV)
    - Operating system, Kernel, Container runtime updates
    - Automatic PV upgrades
    - Task Termination Notifications

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compute/Infrastructure Security

ECS on EC2

- ECS performs AMI Patching
- Infrastructure operators update ECS AMIs
  - Leverage SSM parameters for AMI updates

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/recommended
```

  - In-place instance updates
    - `yum update` using SSM agent
  - ECS Auto Scaling/Capacity Providers

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compute/Infrastructure Security Recap

Use case: Security vulnerability patching for infrastructure

Persona: DevOps

Security feature:

Launch type	Support
ECS on Fargate	Hands-off patching
ECS on EC2	AMI ID using SSM parameters, In-place updates, ECS Capacity Providers
ECS on External	Customer does the patching

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use case #2:
I want to provide fine grained permissions to my different services such as AuthService, OrderService etc. and have a way to audit their access.

Persona: Application Developer

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Task Security

IAM Role for Tasks

- Credential isolation
- Scoped permissions to ECS tasks to call AWS APIs
- Authorization
- Auditability
  - AWS CloudTrail logs using task ARN or task ID



Amazon Elastic Container Service (Amazon ECS)

+

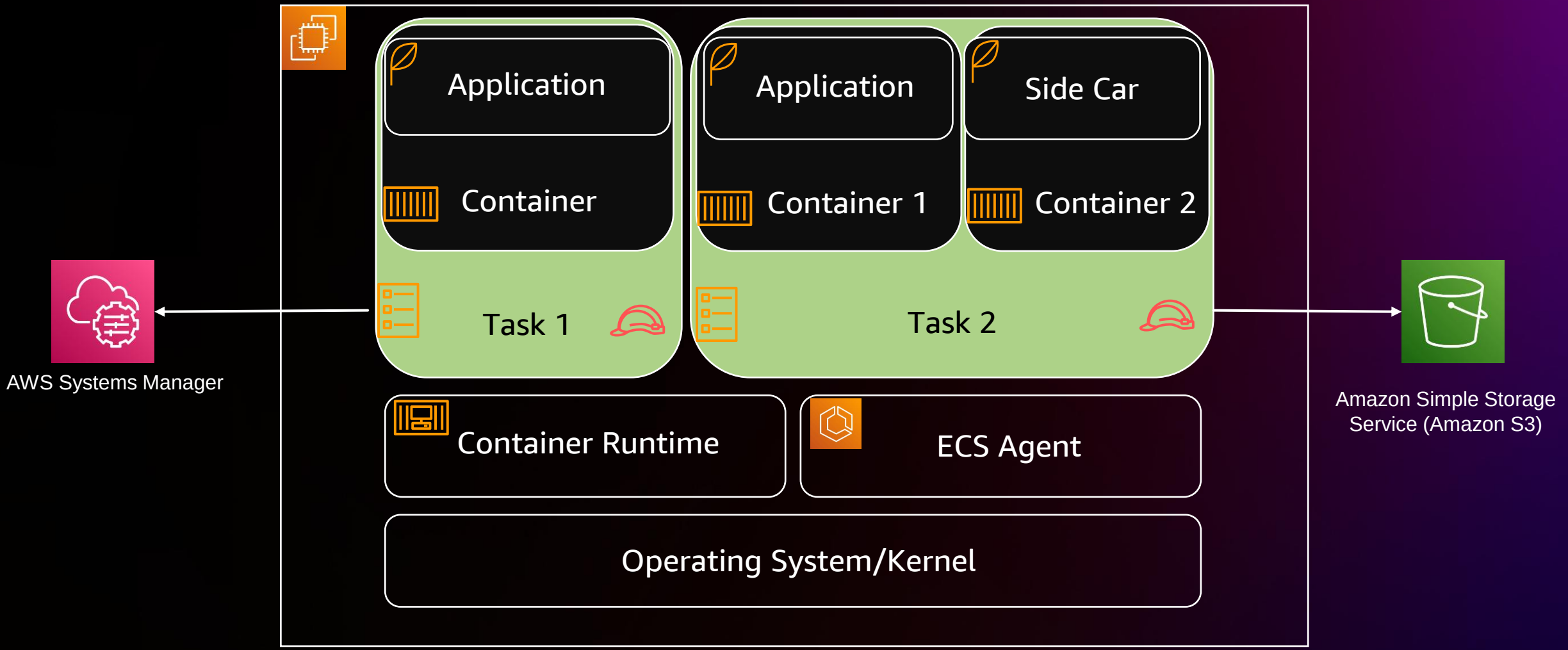


AWS Identity and Access Management (IAM)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Task Security

IAM Role for Tasks



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Task Security

- Setting up Task IAM roles

Task 1's IAM Role policy

```
…
{
   "Sid":"SystemsManagerAccess",
   "Effect": "Allow",
   "Action": [
       "ssm:DescribeParameters"
       "ssm:GetParameters"
   ],
  "Resource": "arn:aws:ssm:us-east-
2:123456789012:parameter/auth-*"
},
…
```

Task 2's IAM Role Policy

```
…
{
   "Sid":"S3Access",
   "Effect": "Allow",
   "Action": [
       "s3:GetObject",
       "s3:PutObject",
       "s3:DeleteObject",
       "s3:ListBucket"
   ],
   "Resource":["arn:aws:s3:::order/*"]"
},
…
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Task Security

IAM Role for Tasks

- Trust relationship only for ECS Tasks

Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "ecs-tasks.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

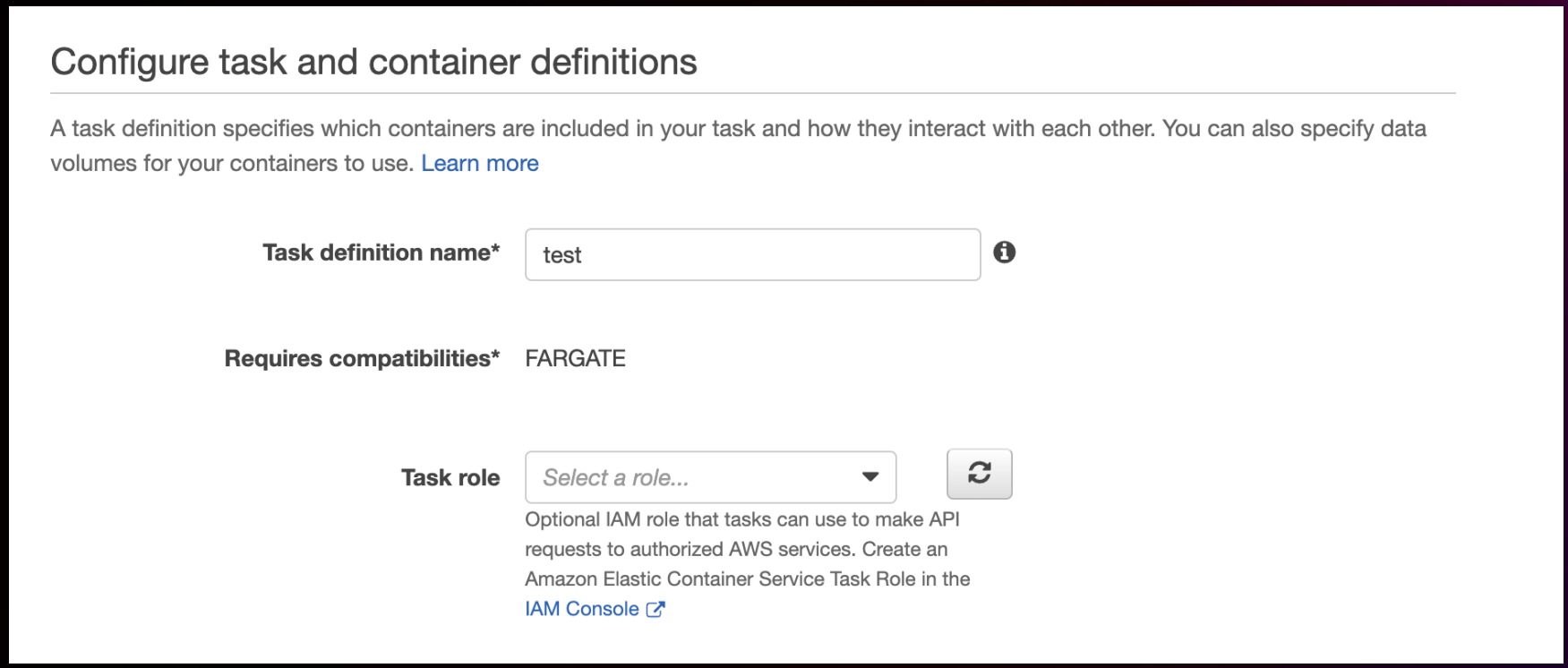
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Task Security

IAM Role for Tasks

- Configuration in the Task definition



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Task Security – Task IAM role recap

Use case: Credentials Isolation for applications

Persona: Application Developer

Security feature:

Launch type	Support
All launch types	• Credentials isolation using fine-grained IAM role permissions for ECS tasks/services • TaskRole Field in ECS task definition

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

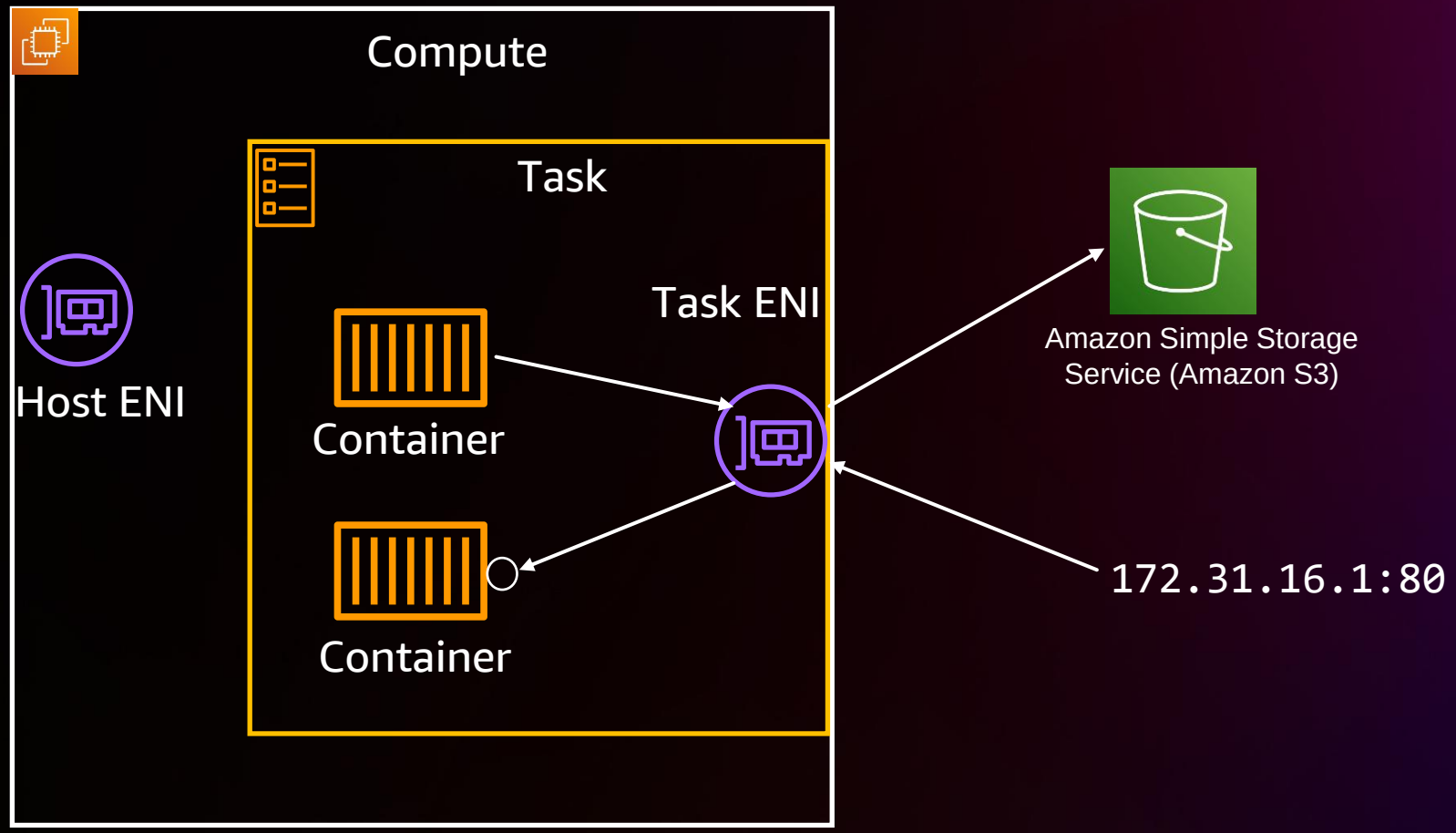
Use case #3:
Better network security for services, separate services' traffic from one another and have traffic monitoring capability.

Persona: DevOps

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Task Security

Amazon ECS Task Networking Feature

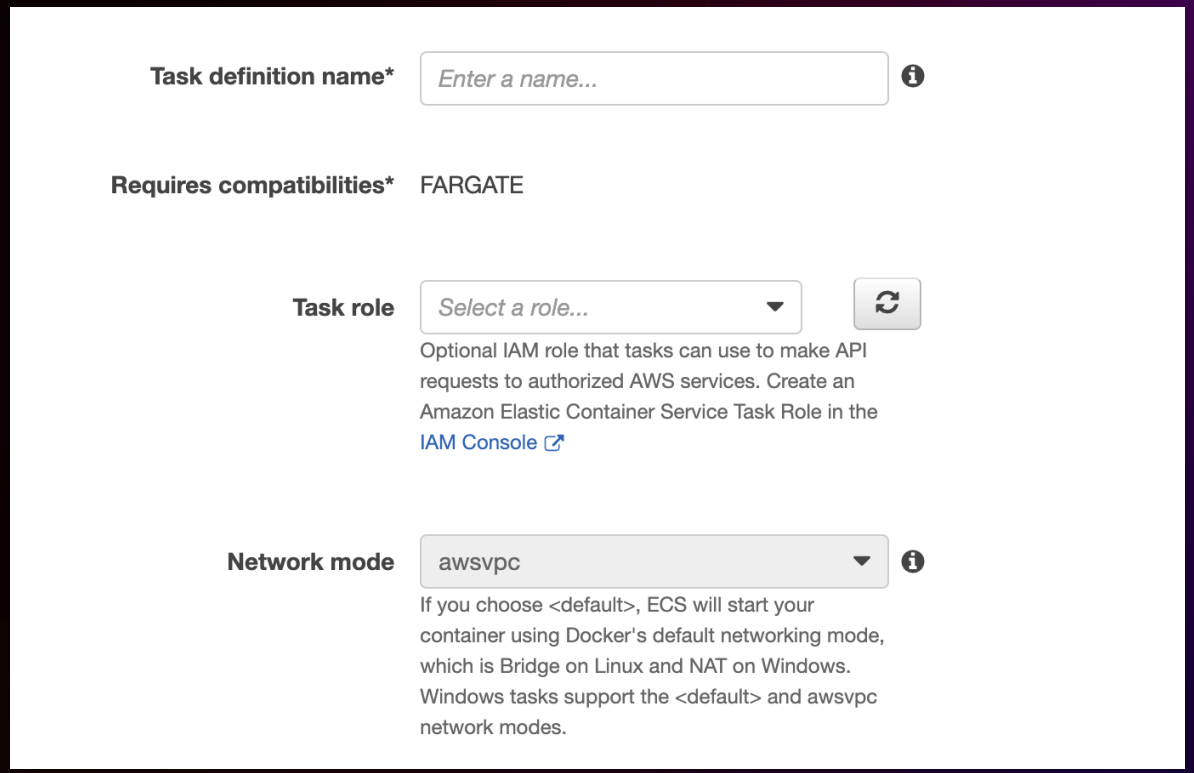


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Task Security

Dedicated Elastic Network Interface for each task

- Securely pull Container Images, Secrets, Logs and Traffic
- awsvpc network mode
  - Configured in Task definition



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Task Security

- Dedicated Elastic Network Interface for each task
  - Security groups, Network ACLs for ENIs
    - VPC configuration

Security Group Service 1 sg-3678

	Source	Protocol	Port Range	Type
Inbound	0.0.0.0/0	TCP	80	HTTP
Outbound	0.0.0.0/0	All	All	All traffic

Security Group Service 2

	Source	Protocol	Port Range	Type
Inbound	sg-3678	TCP	3306	Custom TCP
Outbound	0.0.0.0/0	All	All	All traffic

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Task Security

- Dedicated Elastic Network Interface for each task
  - Provide Subnets, Security groups configuration in RunTask or CreateService API

```
aws ecs create-service --cluster test-cluster \
--service-name test-service \
--task-definition test-app:1 \
--desired-count 1 \
--network-configuration \
"awsvpcConfiguration={subnets=[subnet-abcd1234,subnet-abcd5678],securityGroups=[sg-abcd1234]}"
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Task Security

- Trunk ENIs
  - High density ENI tasks
  - c5.large instance – 2 vs. 10 tasks
  - Avoid IP address exhaustion
  - Enabled through ECS account level setting

- VPC Flow Logs for Audit
  - Enables capturing traffic information to and from the network interface
  - Enable VPC Flow Logs using AWS config rules and Lambda
  - Example:

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 172.31.16.21 20641 22 6 20 4249
1418530010 1418530070 REJECT OK
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Task Security – Task Networking recap

Use case: Inbound and Outbound traffic control for applications

Persona: DevOps

Security feature:

Launch type	Support
ECS on Fargate ECS on EC2	• Task networking feature – awsvpc network mode • Network Configuration in RunTask or CreateService ECS APIs • Security groups for ENIs • ENI Trunking (only EC2 launch type) • VPC Flow Flogs

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use case #4:
How do I securely provide access to sensitive data like database password to my container?

Persona: Application Developer

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Container Security

Container Secrets

- Inject sensitive data into containers
- Use AWS Secrets Manager or AWS Systems Manager Parameter Store
- Two ways to inject
  - Environment Variables
  - Part of log configuration

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Container Security

Container Secrets

1. Create Secret in AWS Secrets Manager

```
aws secretsmanager create-secret
--name admin
--secret-string "{\"user\":\"admin\",\"password\":\"test-password\"}"
```

2. Secrets Permissions in ECS Task Execution Role

```
{ "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "secretsmanager:GetSecretValue" ],
      "Resource": ["arn:aws:secretsmanager:us-east-1:0567812876:secret:admin*"]
    }
  ]
}
```

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Container Security

Container Secrets

3. Container's Environment Variable

```
{
  "containerDefinitions": [{
    "secrets": [{
      "name": "LOGIN_PASSWORD",
      "valueFrom": "arn:aws:secretsmanager:us-east-1:0567812876:secret:admin:password::"
    }]
  }]
}
```

4. Log configuration secret options

```
"logConfiguration": [{
  "logDriver": "splunk",
  "secretOptions": [{
    "name": "splunk-token",
    "valueFrom": "arn:aws:secretsmanager:us-east-1:0567812876:secret:admin:password::"
  }]
}]
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Container Security – Secrets recap

Use case: Supply confidential information to applications

Persona: Application Developer

Security feature:

Launch type	Support
All launch types	• Container secrets from AWS Secrets Manager or AWS Systems Manager • Container environment variables – secrets option in task definition • Container log configuration – secret options in log configuration of task definition

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use case #5:
Without using privileged mode for containers, how do I provide them specific permissions to perform privileged kernel operations?

Persona: Application Developer

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Container Security

ECS Linux Capabilities

- Privileged mode
- Add and drop Kernel Capabilities
  - AWS Fargate only supports adding `SYS_PTRACE` kernel capability
  - Tracing system calls of container processes - compliance

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Container Security

Linux Capabilities Configuration

```
{
  "containerDefinitions": [{
    "linuxParameters": [{
      "capabilities": {
        "add": ["SYS_PTRACE"]
      }
    }]
  }]
}
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Container Security – Linux Capability recap

Use case: Fine-grained elevated privileges to applications

Persona: Application Developer

Security feature:

Launch type	Support
ECS on Fargate	Add SYS_PTRACE Linux capability through linuxParameters option in task definition
ECS on EC2 ECS on External	Add/Drop available Linux Capabilities through linuxParameters option in task definition

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use case #6:
Provide access control to DevOps, Application developers to access different Amazon ECS resources.

Persona: Cloud Architect

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Across Amazon ECS Resources

- Control access to ECS resources using Tagging
- Tag contains key, value
- IAM condition keys using Tags

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Across Amazon ECS Resources

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "clusterCreation",
      "Effect": "Allow",
      "Action": [
        "ecs:createCluster"
      ],
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "dev-test"
          ]
        }
      }
    },
    {
      "Sid": "clusterDeletion",
      "Effect": "Allow",
      "Action": [
        "ecs:deleteCluster"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "ecs:ResourceTag/dev-test": "false"
        }
      }
    }
  ]
}
```

How this translates..

```
% aws ecs create-cluster --cluster-name test-app \
--tags "key=dev-test,value=true" | jq '.cluster.status'

"ACTIVE"
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Across Amazon ECS Resources

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "clusterCreation",
      "Effect": "Allow",
      "Action": [
        "ecs:createCluster"
      ],
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "dev-test"
          ]
        }
      }
    },
    {
      "Sid": "clusterDeletion",
      "Effect": "Allow",
      "Action": [
        "ecs:deleteCluster"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "ecs:ResourceTag/dev-test": "false"
        }
      }
    }
  ]
}
```

How this translates..

```
% aws ecs create-cluster --cluster-name test-app \
--tags "key=prod,value=true"

An error occurred (AccessDeniedException) when calling the CreateCluster operation:
User: arn:aws:iam::012345678912:user/dev-tester is not authorized to perform:
ecs:CreateCluster on resource: * because no identity-based policy allows
the ecs:CreateCluster action
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Across Amazon ECS Resources

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "clusterCreation",
      "Effect": "Allow",
      "Action": [
        "ecs:createCluster"
      ],
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "dev-test"
          ]
        }
      }
    },
    {
      "Sid": "clusterDeletion",
      "Effect": "Allow",
      "Action": [
        "ecs:deleteCluster"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "ecs:ResourceTag/dev-test": "false"
        }
      }
    }
  ]
}
```

How this translates..

```
% aws ecs delete-cluster --cluster test-app \
| jq '.cluster.status'

"INACTIVE"
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Across Amazon ECS Resources

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "clusterCreation",
      "Effect": "Allow",
      "Action": [
        "ecs:createCluster"
      ],
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "dev-test"
          ]
        }
      }
    },
    {
      "Sid": "clusterDeletion",
      "Effect": "Allow",
      "Action": [
        "ecs:deleteCluster"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "ecs:ResourceTag/dev-test": "false"
        }
      }
    }
  ]
}
```

How this translates..

```
% aws ecs delete-cluster --cluster prod-app

An error occurred (AccessDeniedException) when calling the DeleteCluster operation:
User: arn:aws:iam::012345678912:user/dev-tester is not authorized to perform:
ecs:DeleteCluster on resource: arn:aws:ecs:us-west-2:012345678912:cluster/prod-app
because no identity-based policy allows the ecs:DeleteCluster action
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Across Amazon ECS Resources

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "tasksDescribe",
      "Effect": "Allow",
      "Action": [
        "ecs:describeTasks"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "ecs:ResourceTag/dev-test": "false"
        }
      }
    }
  ]
}
```

How this translates..

```
% aws ecs describe-tasks --tasks e908f250f15d4e359a3b72fa87b1c9ed \
--cluster  test-app \
--include TAGS | jq '.tasks[].tags'
[
  {
    "key": "dev-test",
    "value": "true"
  }
]
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Across Amazon ECS Resources

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "tasksDescribe",
      "Effect": "Allow",
      "Action": [
        "ecs:describeTasks"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "ecs:ResourceTag/dev-test": "false"
        }
      }
    }
  ]
}
```

How this translates..

```
% aws ecs describe-tasks --tasks b1786250f15d4e359a3b72fa87bkl765 \
--cluster prod-app \
--include TAGS | jq '.tasks[].tags'

An error occurred (AccessDeniedException) when calling the DescribeTasks operation:
User: arn:aws:iam::074626758757:user/dev-tester is not authorized to perform:
ecs:DescribeTasks on resource:
arn:aws:ecs:us-west-2:012345678912:task/prod-app/b1786250f15d4e359a3b72fa87bkl765
because no identity-based policy allows the ecs:DescribeTasks action
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Across Amazon ECS Resources – Recap

Use case: Access Control for Amazon ECS resources

Persona: Cloud Architect

Security feature:

Launch type	Support
All launch types	• AWS Tagging for ECS resources • Tags in IAM Condition Keys • Protect production resources

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ECS Security Features Deep Dive

- Compute Segregation
- Infrastructure Patching
- Security Groups, Network ACLs, IAM Role for Container Instances
- AWS PrivateLink

- IAM Role for Tasks
- Task Execution Role
- Dedicated ENI for Tasks
- Storage Isolation
  - Ephemeral storage
  - Amazon EFS volume

- Container Secrets
- Linux Kernel capabilities
- Ulimits
- User Options
- Image Scanning
- Image Pruning

- Transport Layer Security (TLS) – AWS App Mesh
- Tag-based Access Control
- Log Routing
- Metrics Reporting
- Audit & Tracing
- Execute Command for Debugging

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Conclusion – Security on ECS

- Security is top priority for customers, AWS and ECS
- Widely deployed, with seamless integration for all AWS Security Services
- Security functions built-in across all architecture levels
- Rich security feature set and interfaces to facilitate the customer experience

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

To learn more...

- AWS Fargate Security Whitepaper: https://d1.awsstatic.com/whitepapers/AWS_Fargate_Security_Overview_Whitepaper.pdf
- Rolling AMI updates with Capacity Providers: https://aws.amazon.com/blogs/containers/rolling-ec2-ami-updates-with-capacity-providers-in-amazon-ecs/
- Enable VPC Flow Logs using AWS Config rules: https://aws.amazon.com/blogs/mt/how-to-enable-vpc-flow-logs-automatically-using-aws-config-rules/
- IAM Roles for Tasks: https://aws.amazon.com/about-aws/whats-new/2016/07/amazon-ec2-container-service-now-supports-iam-roles-for-tasks/
- ECS Tags-based Authorization: https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ecs-using-tags.html
- ECS Task Configuration Security Controls: https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task_definition_parameters.html#container_definition_security
- AWS Trusted Advisor: https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor.html
- Amazon Services Compliance Scope: https://aws.amazon.com/compliance/services-in-scope/

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Spiros Tsitsonis
spirosts@amazon.com

Sharanya Devaraj
sharanyd@amazon.com



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.