AWS
Black Belt
Online Seminar

【AWS Black Belt Online Seminar】

re:Invent Recap: Compute, Container and Network

アマゾン ウェブ サービス ジャパン株式会社
ソリューションアーキテクト
西谷　圭介
ソリューションアーキテクト　ネットワークスペシャリスト
菊池　之裕

2018.01.17

内容についての注意点

- 本資料では2018年1月17日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(http://aws.amazon.com)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっています。日本居住者のお客様が東京リージョンを使用する場合、別途消費税をご請求させていただきます。
- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Who am I ?

Keisuke Nishitani

Specialist Solutions Architect, Serverless

Amazon Web Service Japan

@Keisuke69

Keisuke69

Keisuke69x

Keisuke69

Keisuke69

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

新しい本を出します

※カバー画像はイメージです

サーバーレスアプリケーションの開発についてアプリの実装を通して解説します

紹介予定のサービス

- API Gateway, Lambda, Cognito, S3, Kinesis, DynamoDB, Rekognition etc…

2018年2月末発売予定

Amazonで予約受付中
http://amzn.asia/0QzrGYh

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

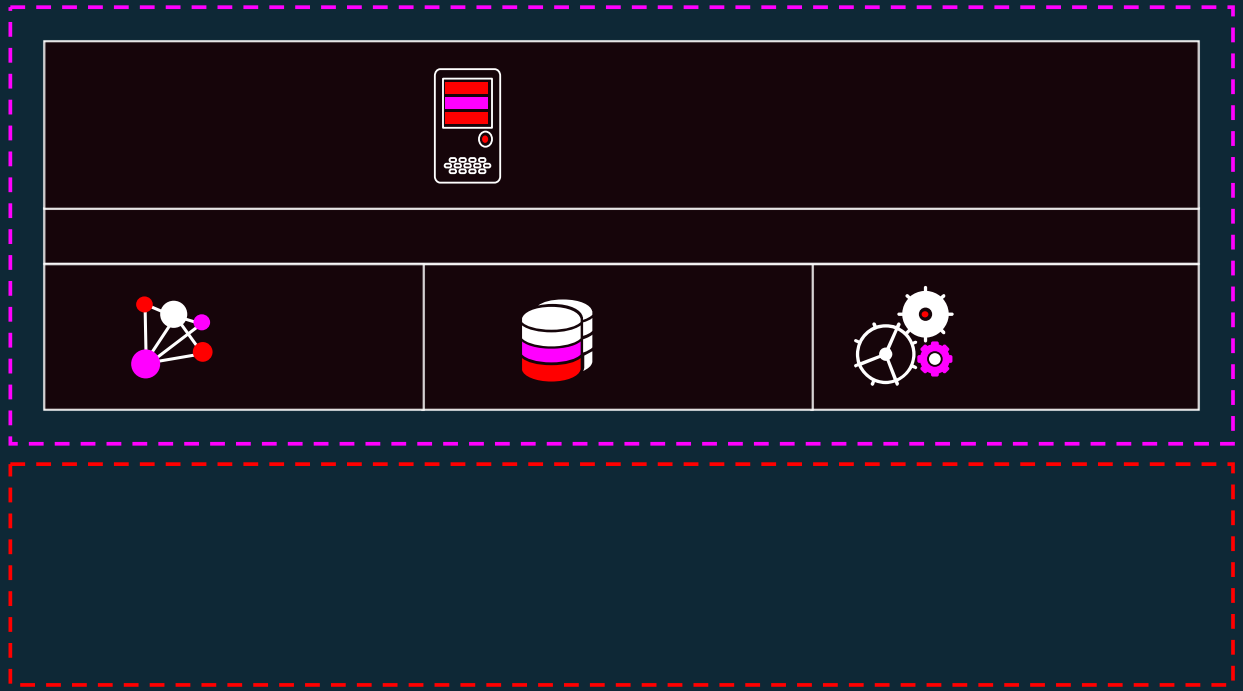
Compute update

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AMAZON EC2 HOST オリジナルアーキテクチャ

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

NITRO SYSTEM アーキテクチャ



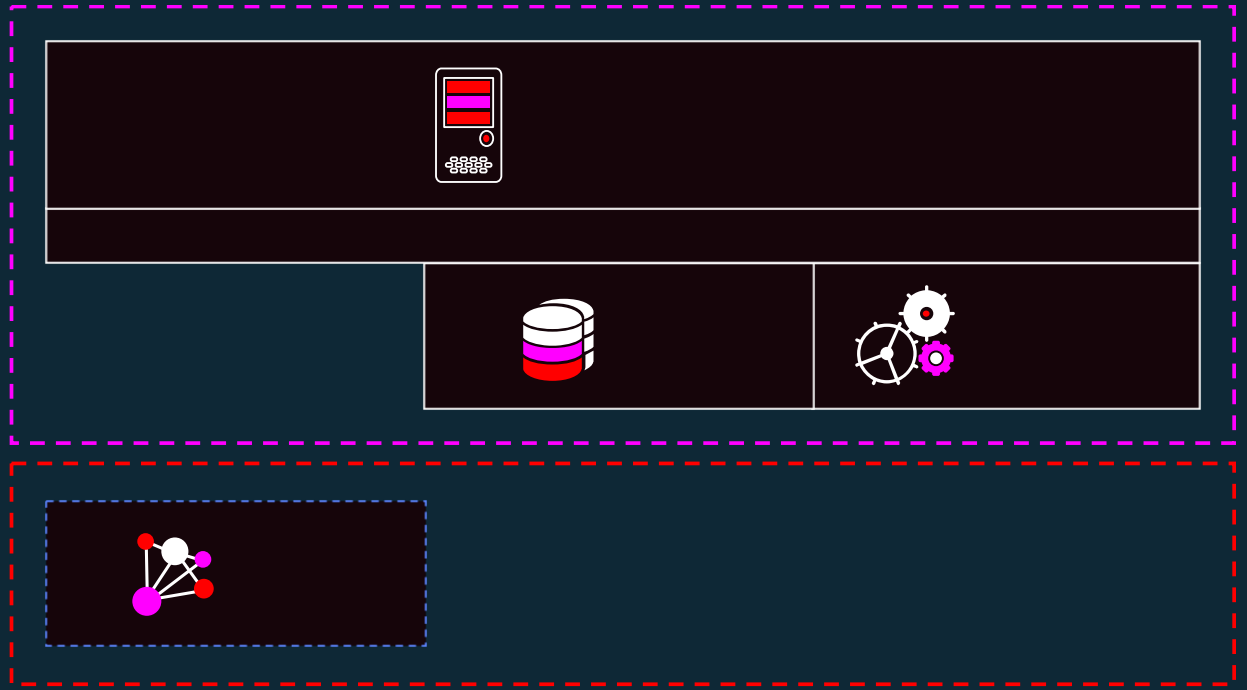
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AMAZON EC2 C3 インスタンス

ネットワークパケット処理にはかなりの CPU 時間が必要

C3 ではネットワーク処理 をオフロード

re:Invent 2013 にてローンチ



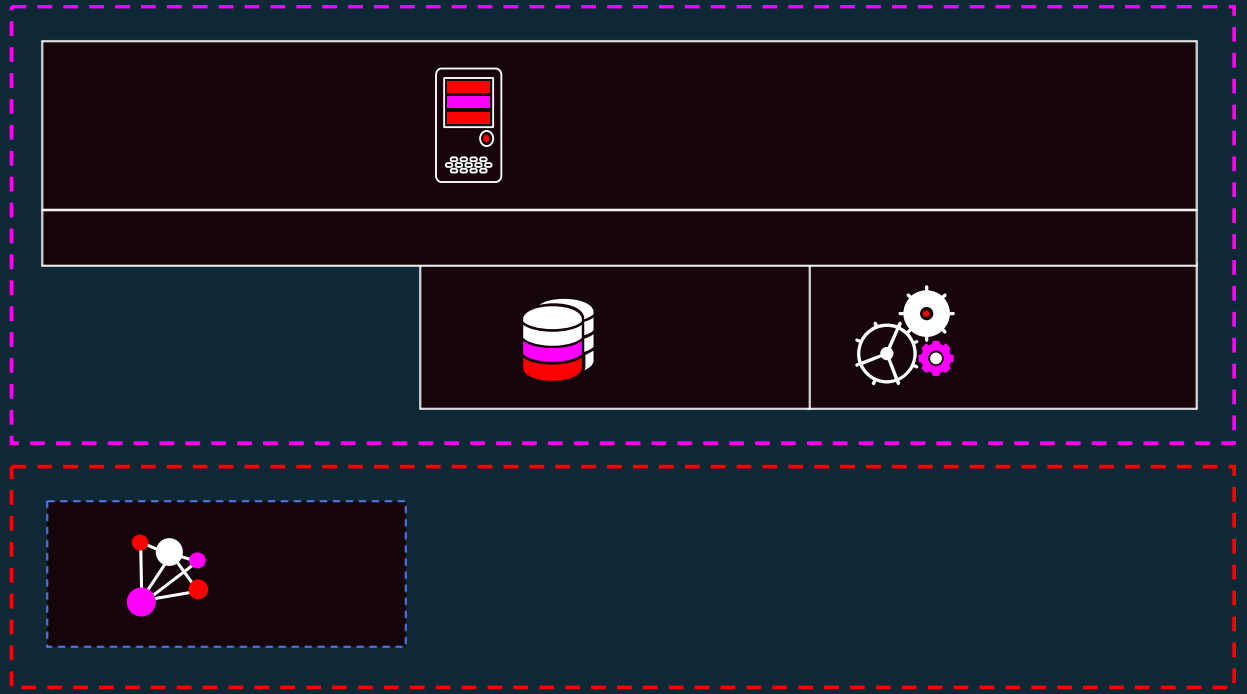
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AMAZON EC2 C4 インスタンス

次のオフロードのターゲットはストレージ

ストレージのリクエストを検証、暗号化、およびルーティングするための EC2 のホストソフトウェアが必要であった

re:Invent 2014 にてローンチ



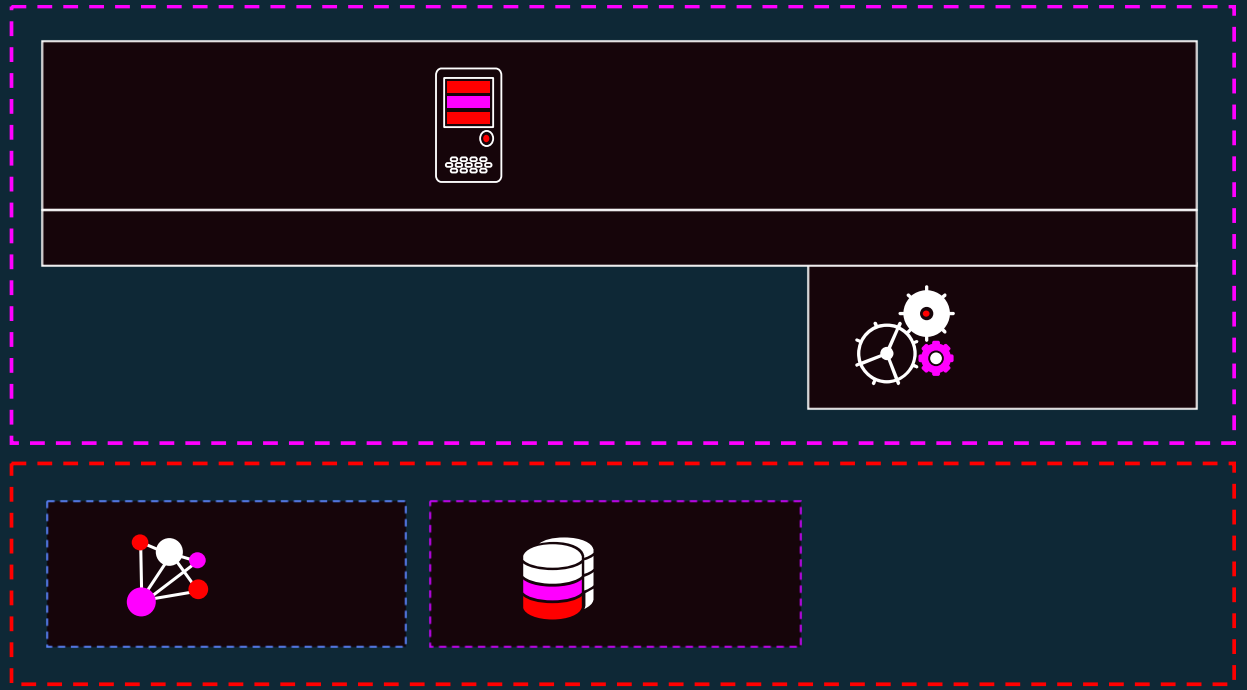
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AMAZON EC2 C4 インスタンス

次のオフロードのターゲットはストレージ

ストレージのリクエストを検証、暗号化、およびルーティングするための EC2 のホストソフトウェアが必要であった

re:Invent 2014 にてローンチ



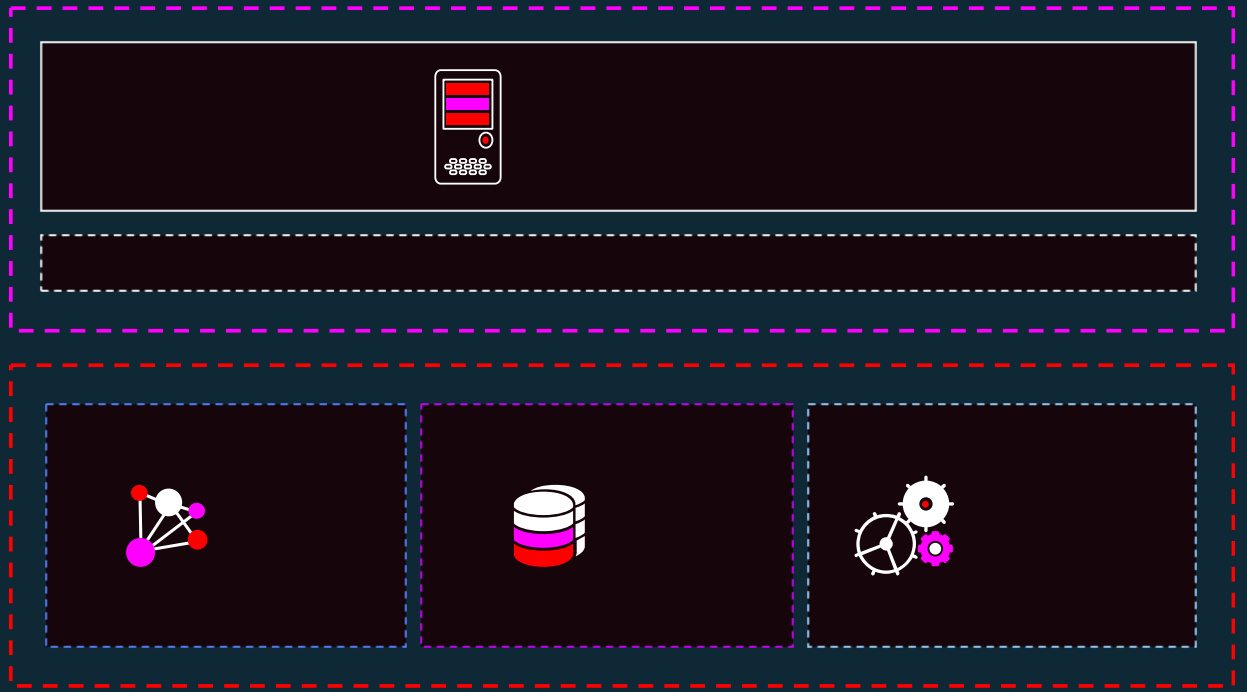
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AMAZON EC2 C5 インスタンス

C5は、EC2ソフトウェアスタック全体をオフロードする最初のインスタンス

Annapurna と AWSが開発した最初のシリコンを使用

最適化されたバージョンの Linux KVM をベースにした完全に新しいEC2ハイパーバイザ



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AMAZON EC2 C5 インスタンス

新世代のコンピューティング最適化インスタンス、高クロックのCPUを搭載し分散並列処理やビデオエンコーディング、HPCなどの分野に最適

SkylakeコアのXeon Platinum 8000シリーズプロセッサ搭載。3.0GHzのベースクロックで、Turbo Boostにより最大3.5GHzで動作、AVX-512命令セットに対応

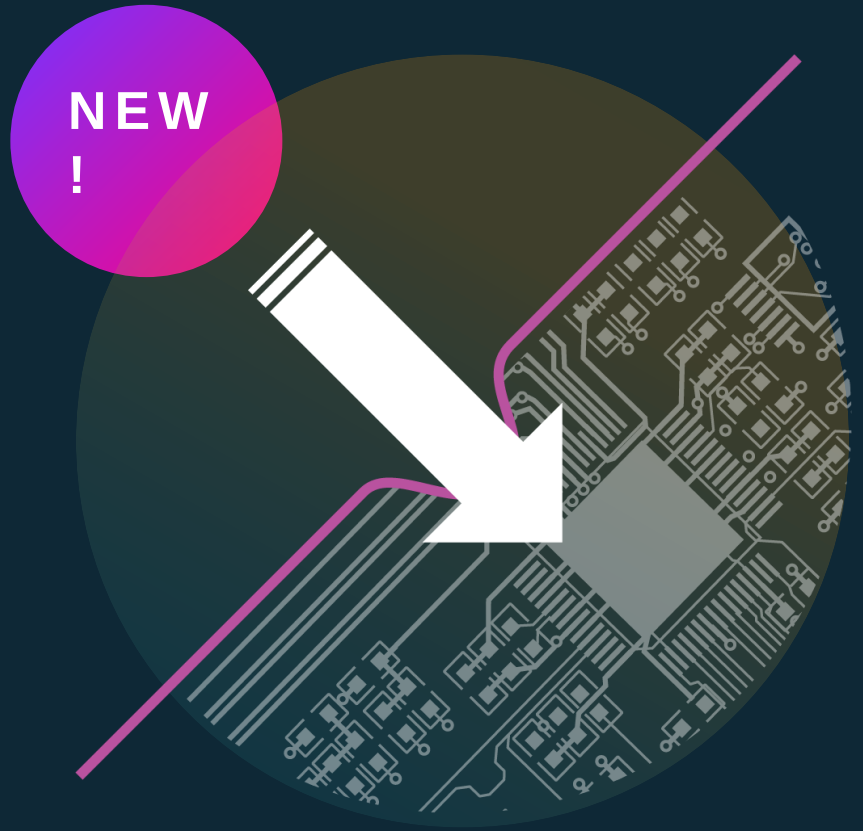
前世代(C4)インスタンスに対して25%の価格/性能

新世代NITROハイパーバイザーによりCPU、ネットワーク、ストレージ性能を引き出す設計

Elastic Network Adaptor(ENA)をサポートし、最大25Gbpsの通信帯域をサポート

バージニア、オレゴン、アイルランドの3リージョンで利用可能

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Bare Metal Instances

AWS のすべての弾力性、セキュリティ、スケーラビリティ

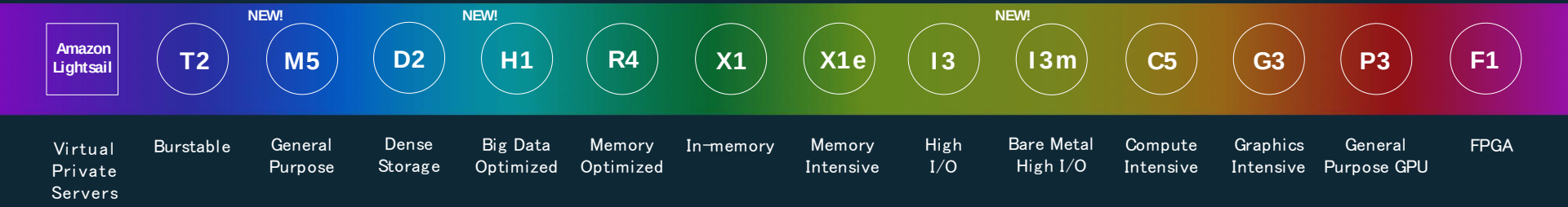
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Bare Metal Instances

- ハードウェアへのダイレクトアクセスを提供
- AWSの各種サービスとの連携が可能で、AWSクラウドのメリットを失うことなく、OSが直接下層のハードウェアにアクセス可能
- Bare Metalインスタンスとしてi3.metalインスタンスのプレビューを開始
  - CPU:Intel Xeon E5-2686v4 2Processers(2.3Ghz), 36core(HTで72core)
  - メモリ:512GiB
  - ストレージ:ローカルストレージとして15.2TB、SSDベースのNVMeストレージ
  - ネットワーク:25Gbps (ENAベースの拡張ネットワーキング)

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

コンピュートインスタンスの選択肢



EC2 Elastic GPUs

Graphics acceleration for EC2 instances

EC2 Spot Instances

NEW!

- Hibernation
- No Bid Pricing

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon EC2 H1インスタンス

- ビッグデータアプリケーション向けの新たなストレージ最適化インスタンス
- D2よりもローカルストレージ容量あたりのCPU・メモリが多い
- ビッグデータ処理向けに設計されており、シーケンシャルI/Oに最適化された磁気ストレージを搭載。CPUはIntel Xeon E5-2686 v4を採用
- バージニア、オレゴン、オハイオ、アイルランドで利用可能

タイプ	vCPU	メモリ	ローカルストレージ	NW帯域幅
h1.2xlarge	8	32GiB	2TB	最大10Gbps
h1.4xlarge	16	64GiB	4TB	最大10Gbps
h1.8xlarge	32	128GiB	8TB	10Gbps
h1.16xlarge	64	256GiB	16TB	25Gbps

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon EC2 M5インスタンス

- 最新世代の汎用インスタンス
- 2.5GHz Xeon Platinum 8000シリーズSkylakeプロセッサーを搭載、M4インスタンスに比べ、およそ14%の性能向上
- 新世代NITROハイパーバイザーで稼働
- 小規模なインスタンスにおけるネットワークとEBSの性能の改善
- Intel-AVX512のサポート
- 対応リージョン：バージニア、オレゴン、アイルランド

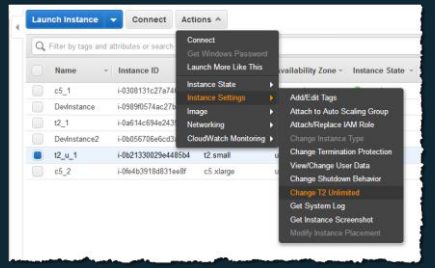
New Hypervisor!

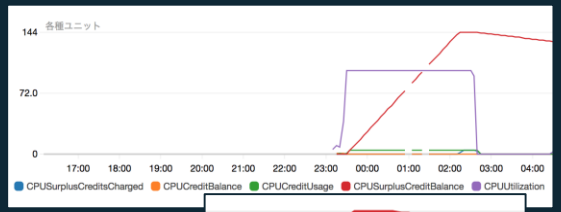
タイプ	vCPU	メモリ	EBS帯域幅	NW帯域幅
m5.large	2	8GiB	最大2,120Mbps	最大10Gbps
m5.xlarge	4	16GiB	最大2,120Mbps	最大10Gbps
m5.2xlarge	8	32GiB	最大2,120Mbps	最大10Gbps
m5.4xlarge	16	64GiB	2,120Mbps	最大10Gbps
m5.12xlarge	48	192GiB	5,000Mbps	10Gbps
m5.24xlarge	96	384GiB	10,000Mbps	25Gbps

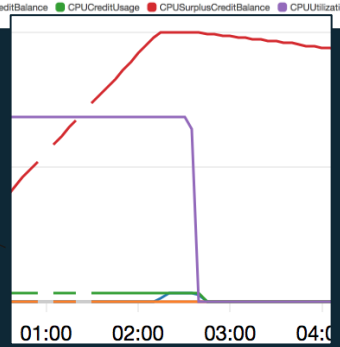
© 2018, Amazon Web Services, Inc. or its Af

T2 Unlimited インスタンス

- CPUのバーストクレジットが枯渇しても、継続してCPUリソースを使い続けられるオプション
- 向こう24時間に付与されるクレジットを前借りしてバーストを継続、それも使い切った場合は有償でバーストを継続できる
  - 状況はCloudwatchメトリクスで確認可能
- 1vCPUあたりLinuxで$0.05、Windowsで$0.096の時間毎課金となる
- 東京を含む各リージョンで利用可能







赤：前借り残高
青：有償調達クレジット

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Nitro Hypervisor(C5&M5)注意事項

C5 M5

使用するOSの前提として、ENAドライバサポート＋NVMeサポートが必須です。またACPIサポートがないとOSの停止が失敗します。対応するOSは下記になります。(参照 https://aws.amazon.com/jp/ec2/faqs/)

- Amazon Linux 2014.03 or newer
- SUSE Linux Enterprise Server 12 or newer
- CentOS 7 or newer
- Windows Server 2012 R2
- Ubuntu 14.04 or newer
- Red Hat Enterprise Linux 7.4 or newer
- FreeBSD 11.1-RELEASE
- Windows Server 2016

その他現時点で分かっていること

＜Amazon Linux AMI＞

- 古いAMIをベースにした環境からインスタンスタイプを変更する場合、acpidを明示的にインストールしてください(yum install acpid)。しないとインスタンスのstopが正常に機能しません。

＜CentOS＞

- CentOS 6: ENAドライバがコンパイルできない可能性が高く利用困難。
- CentOS 7: Marketplace AMIがM5に未対応。(C5は最近対応された模様)

＜SLES 12＞

- 古いAMIはNVMeドライバがinitramfsに含まれていないため起動できません。initramfsを更新してからインスタンスタイプを変更することで回避できます。もしくは最新AMIを使ってください。

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

Container update

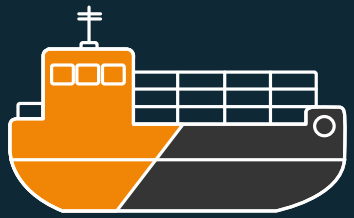
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

DAY ONE!

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

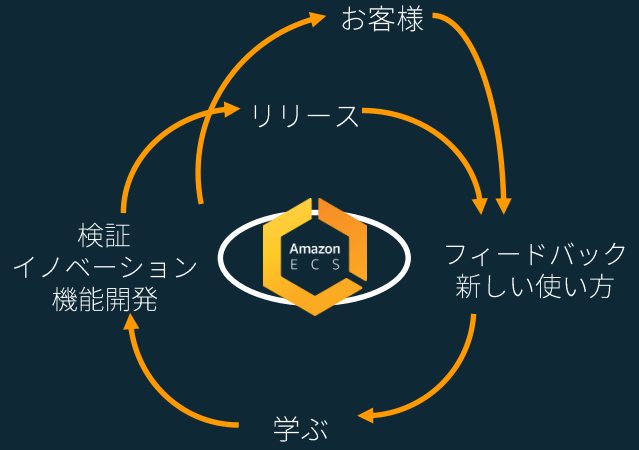
Amazon ECS

450+%
年間アクティブユーザの成長
(2016年と比較)



数億コンテナ
が毎週起動

数百万もの
インスタンス上で



50+
2015年のGA以来
リリースした機能の数

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

アプリケーションの開発に集中したい

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Fargate

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

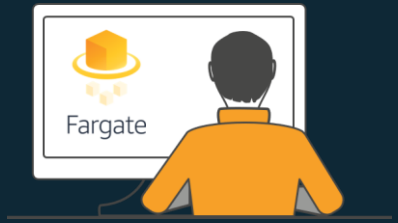
計算リソースの使い方を根本的に変える

インスタンス
管理不要

タスク
ネイティブAPI

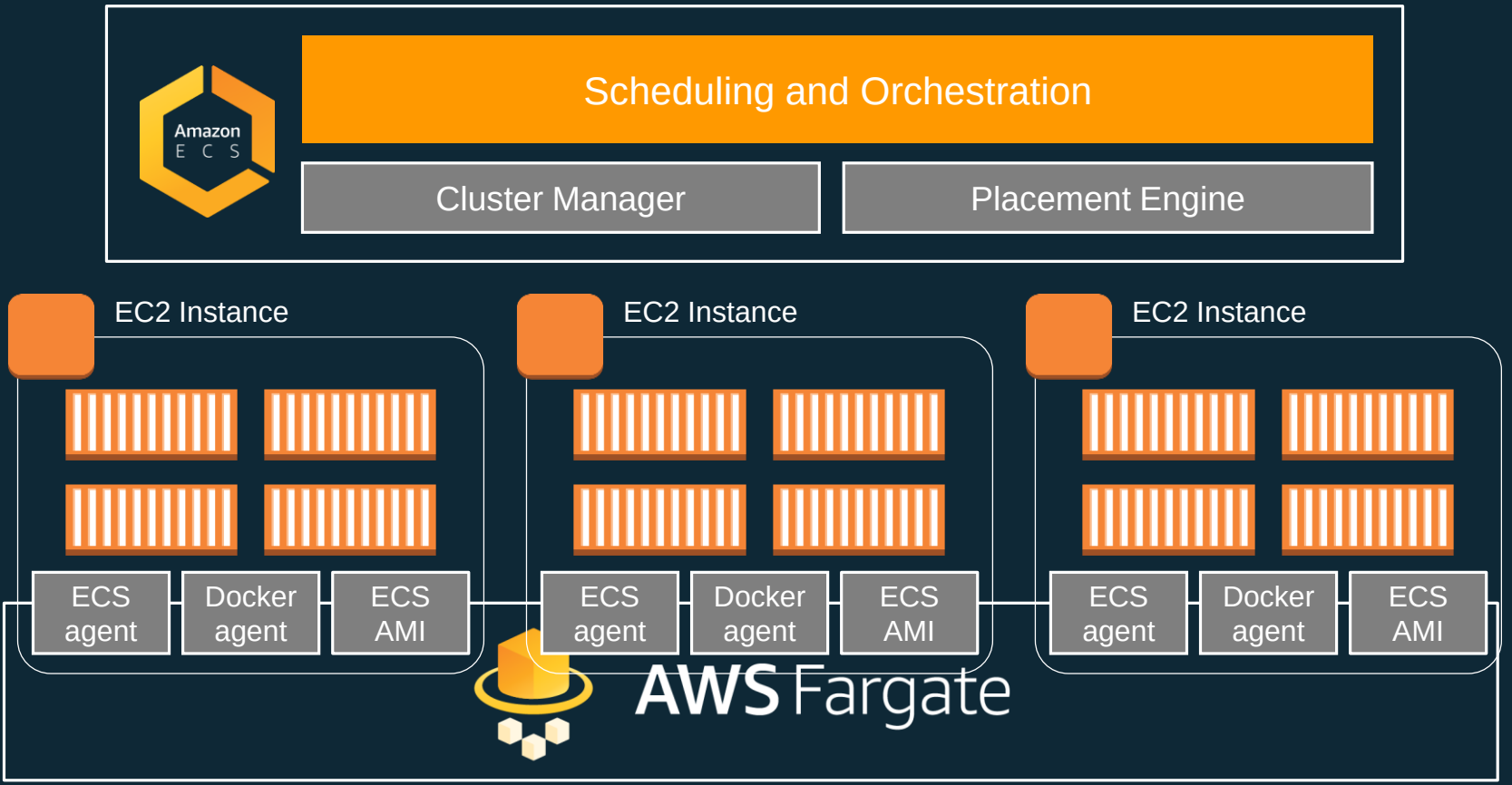
リソース
ベースの価格

=



簡素で、使いやすく、
強力な
新しいリソース消費モデル

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWSで本番環境利用可能

AWS VPCネットワークモード

タスク配置

他のAWSサービスとの深い連携

ECS CLI

グローバル展開 (2018年)

強力なスケジューラ

オートスケーリング

CloudWatch メトリクス

ロードバランサ

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

料金

課金基準: CPUとメモリ

秒単位 で課金

タスク リソースに対する課金

- CPUとメモリはそれぞれの範囲内で独立に指定

```
{
”cpu": “1 vCPU”,
”memory": “2 gb”,
"networkMode": ”AWSVPC",
"compatibilities": [”FARGATE",
”EC2"],
"placementConstraints": [],
  "containerDefinitions": [
    {

<snip>…...
```

Task Level Resources

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

タスクに割り当てるCPUとメモリの設定

柔軟な設定の選択肢
– 50 のCPU/メモリ設定から

CPU	Memory
256 (.25 vCPU)	512MB, 1GB, 2GB
512 (.5 vCPU)	1GB to 4GB (1GB 刻み)
1024 (1 vCPU)	2GB to 8GB (1GB 刻み)
2048 (2 vCPU)	4GB to 16GB (1GB 刻み)
4096 (4 vCPU)	8GB to 30GB (1GB 刻み)

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

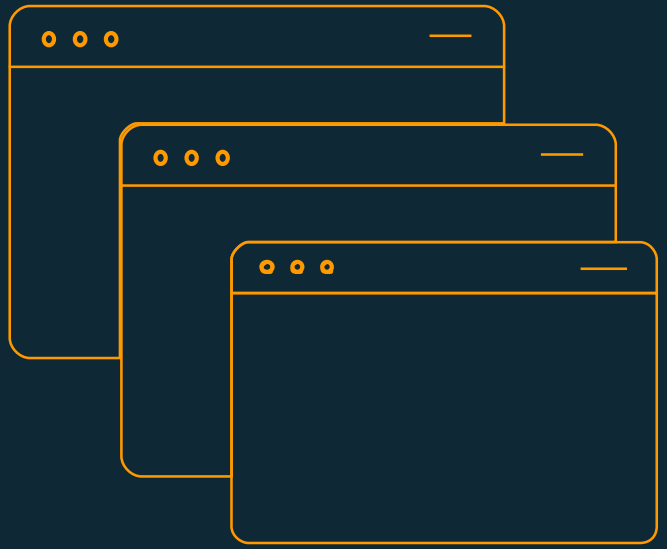
FARGATE: UNDER THE HOOD

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

マイクロサービス

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

バッチジョブ



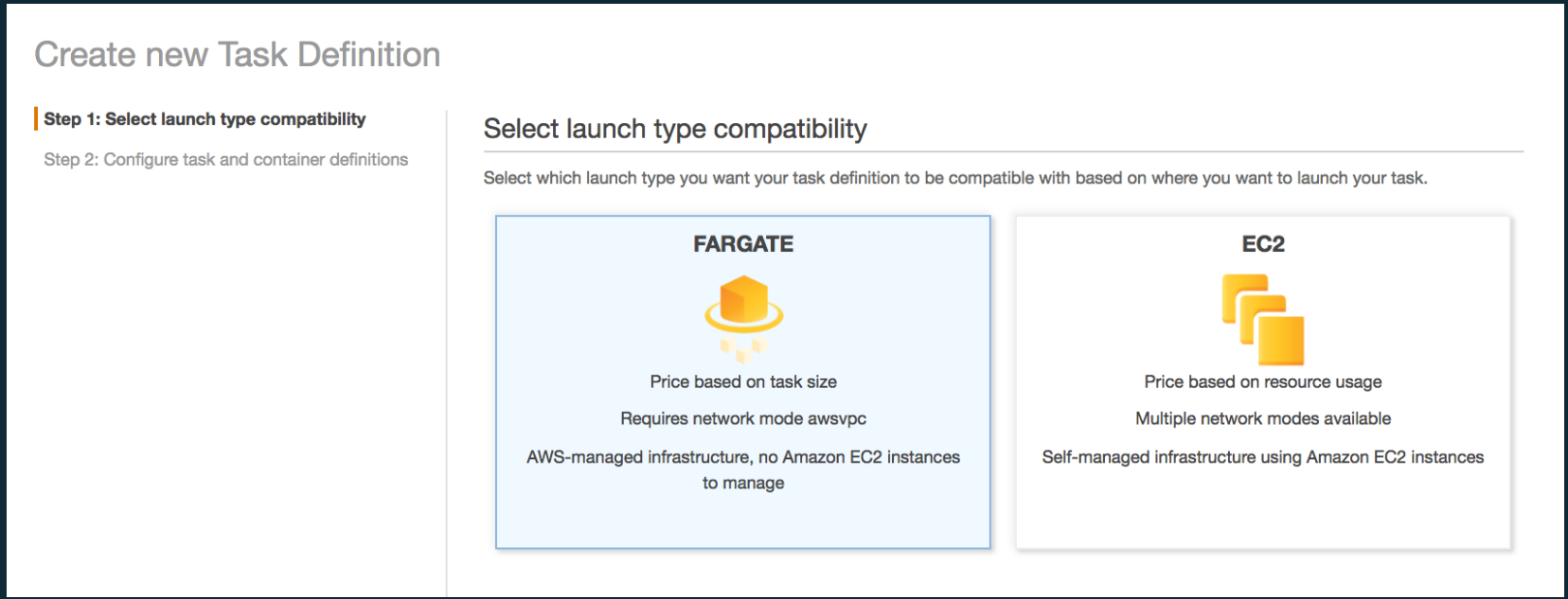
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

クラウドへの移行

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

HOW DO I RUN
CONTAINERS
ON FARGATE?

Fargateでのコンテナ実行



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

ECS CONSTRUCTS

register

Task Definition

Define application containers: Image URL, CPU & Memory requirements, etc.

run

Task

- A running instantiation of a task definition
- Use FARGATE launch type

Elastic Load Balancer

create

Service

- Maintain n running copies
- Integrated with ELB
- Unhealthy tasks automatically replaced

create

Cluster

- Infrastructure Isolation boundary
- IAM Permissions boundary

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

Fargateでのコンテナ実行

同一スキーマのTask Definition

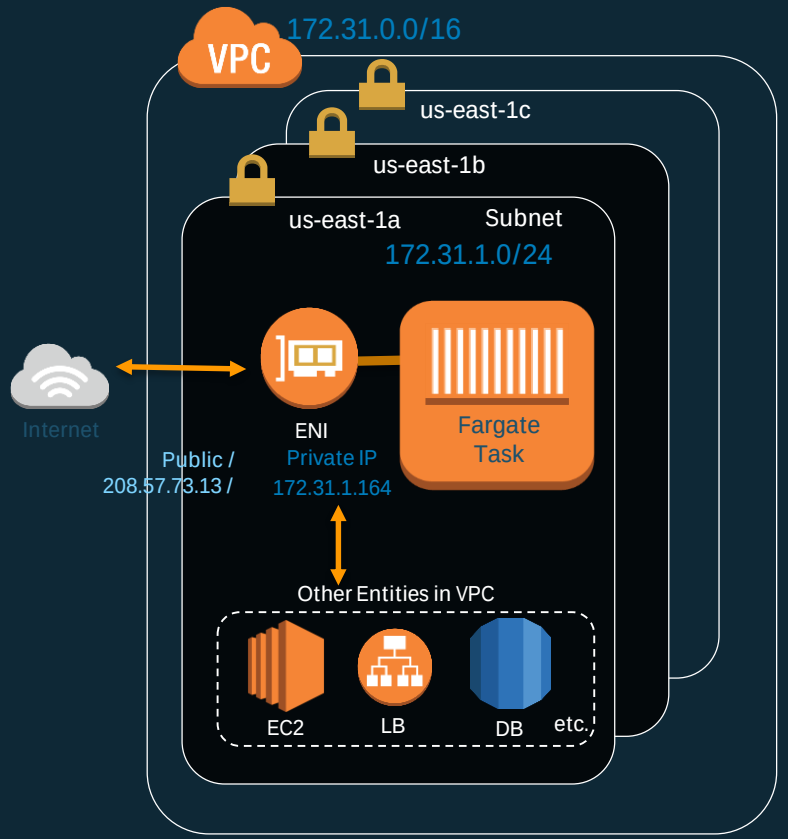
ECS APIを使用した起動

容易な移行 - 同一クラスタ内でFargateとEC2のローンチタイプ

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

VPC INTEGRATION

- AWS VPC Networking Mode – 各タスクがネットワーク・インターフェースを持つ
- Fargateのタスクはユーザの**VPC**/サブネット内で実行
- インバウンド/アウトバウンドのトラフィックを制御するためにセキュリティグループを構成
- Public IPのサポート
- 複数AZ内のサブネットをまたがってアプリケーションを分散してレジリエンシを高める



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

LOAD BALANCING

APPLICATION LOAD BALANCER ☑

NETWORK LOAD BALANCER ☑

Task定義でnetwork modeがawsvpcの場合
ALB/NLBのターゲットグループのtarget typeは ip とする（ECS/Fargate両方）

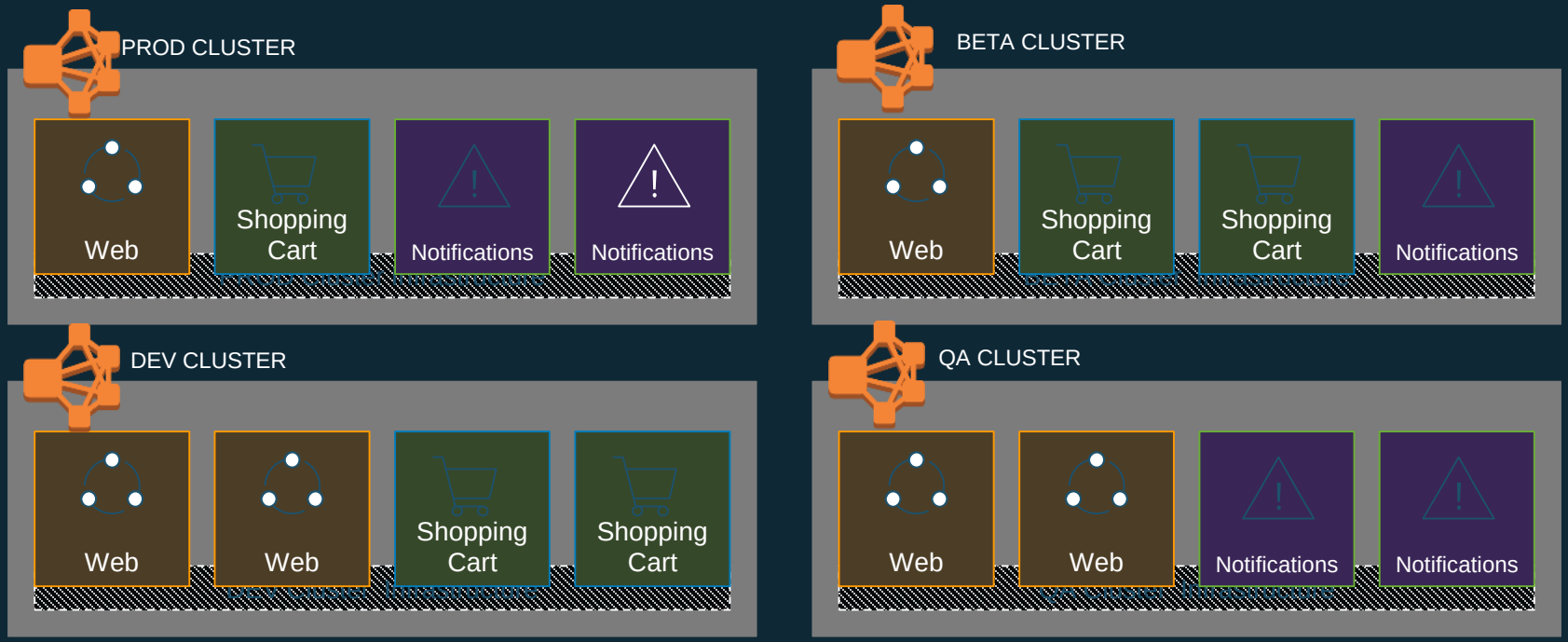
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

SECURITY

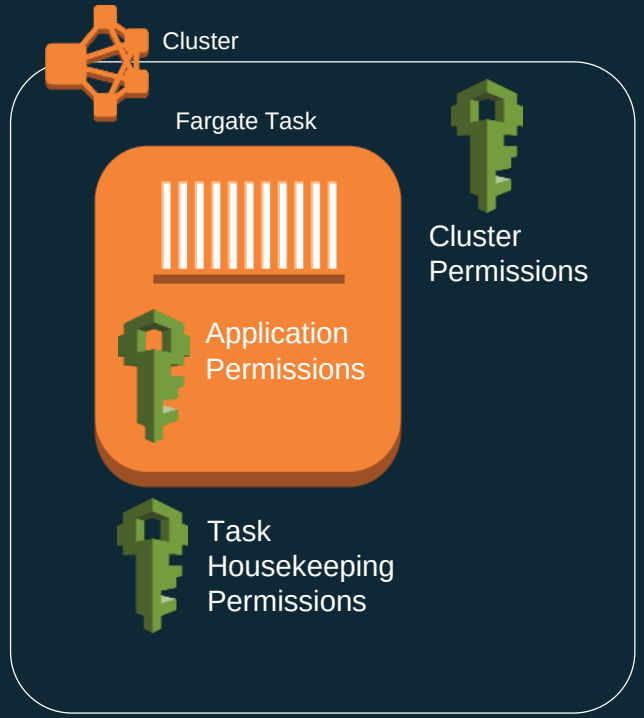
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

クラスタレベルのアイソレーション



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

PERMISSION TIERS



Cluster Permissions:

誰がタスクを実行/参照できるか？

Application (Task) Permissions:

アプリケーションがアクセス可能なAWSリソースはどれか？

Housekeeping Permissions:

ECSに操作を許可したいパーミッションは何か？

e.g.

- ECR Image Pull
- CloudWatch Logs pushing
- ENI creation
- Register/Deregister targets into ELB

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

CONTAINER REGISTRIES

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

REGISTRY SUPPORT

Amazon Elastic Container Registry (ECR)

Public Repositories supported

3rd Party Private Repositories (coming soon!)

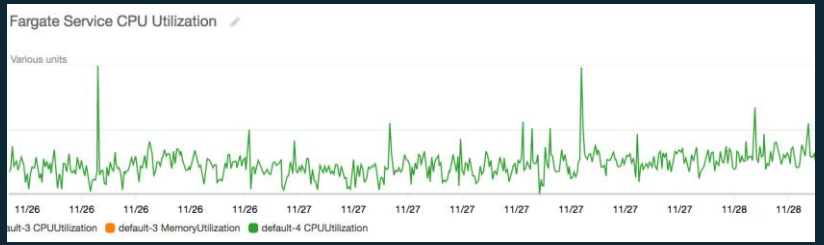
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

VISIBILITY AND MONITORING

CloudWatch Logs
CloudWatch Events

サービスレベルのメトリクスも
利用可能



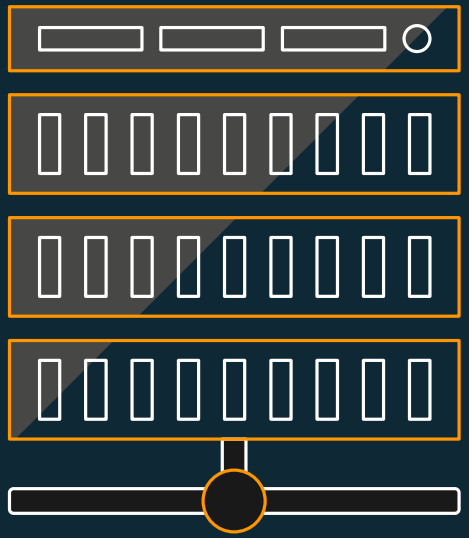
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

STORAGE

Ephemeral storage backed by EBS

Container Storage Space – 10GB

タスク内のコンテナ用共有ボリュームスペース – 4GB



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

FargateかEC2か

- Fargateでは難しいもの
  - Windows Containers
  - GPU Support
  - docker execのようなインタラクティブなデバッグ
  - SpotやRIベースの価格モデルの適用
  - Taskレベルのメトリクス

- これ以外はFargateでOK

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

FargateとLambdaの使い分け

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

kubernetes

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

What is Kubernetes?

オープンソースの
コンテナ管理プラットフォーム

コンテナの大規模な
運用に有用

モダンなアプリケーション
開発のための基本要素を提供

63%

of Kubernetes workloads run on AWS today

—CNCF survey

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Kubernetes on AWS

3x Kubernetes masters for HA

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Kubernetes master

API server

Controller manager

Cloud controller

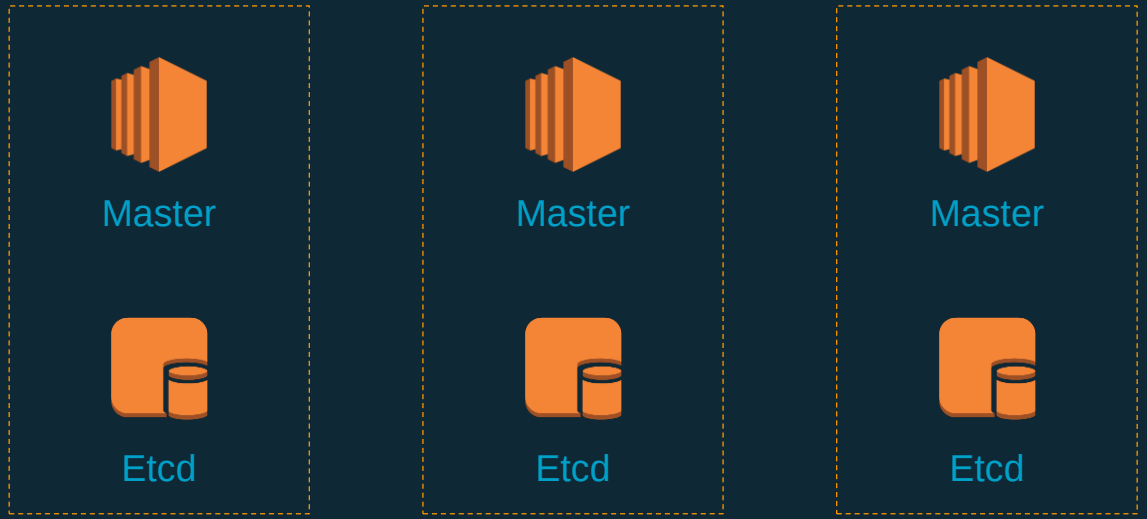
Scheduler

KubeDNS

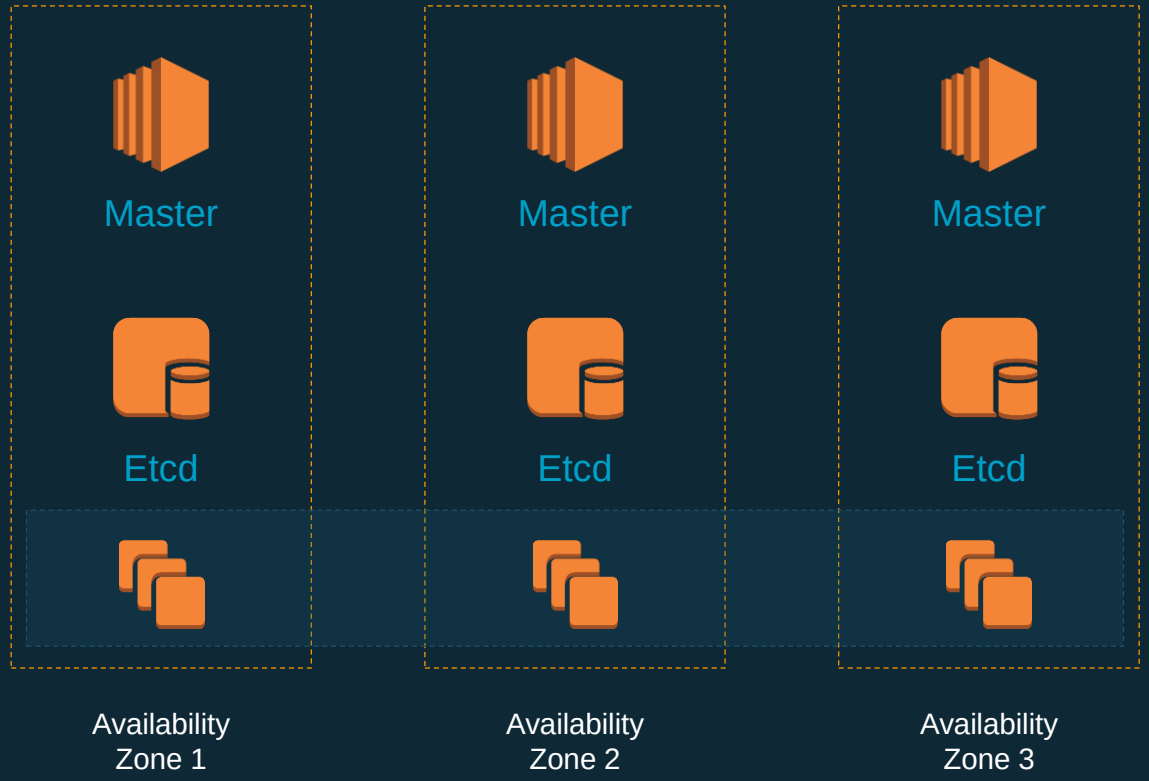
Add-ons

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

“Run Kubernetes for me.”

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

“Native AWS Integrations.”

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

”An Open Source Kubernetes Experience.”

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

Amazon EKS

Amazon Elastic Container Service for Kubernetes (EKS)

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

Tenet 1

EKSはエンタープライズ企業が本番のワークロードを実行するためのプラットフォームであること

Tenet 2

EKSはネイティブで最新のKubernetesの体験を提供すること

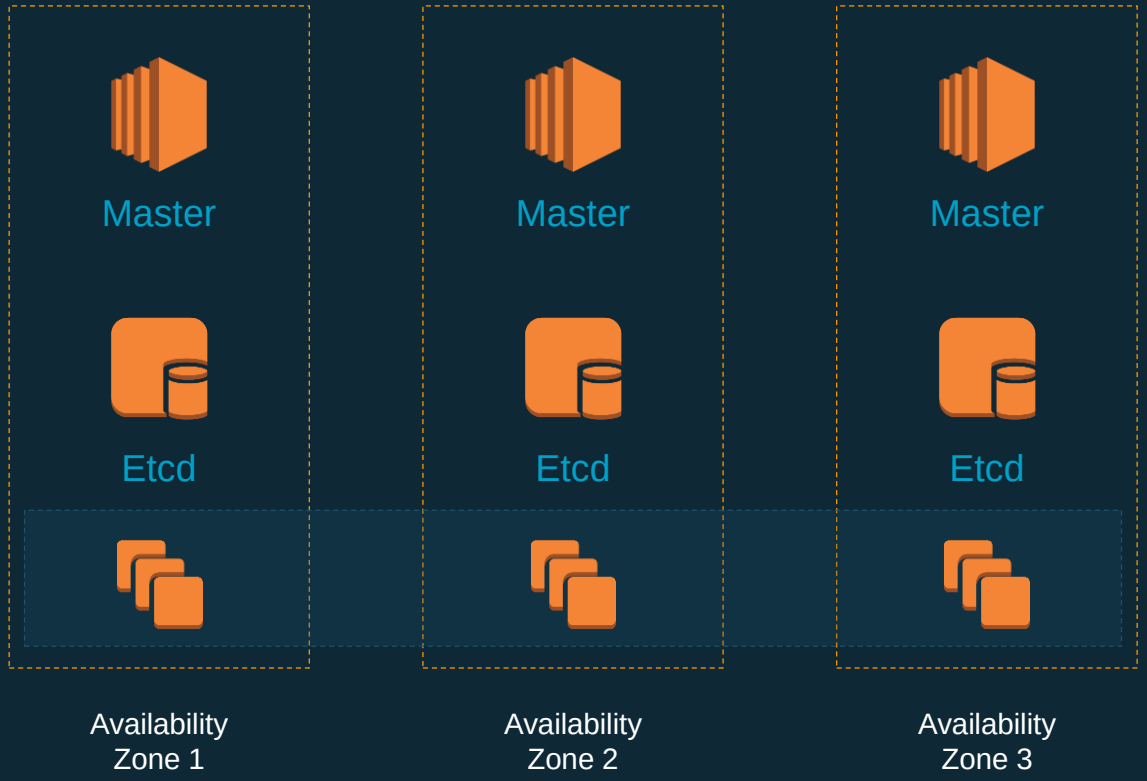
Tenet 3

EKSユーザが他のAWSサービスを使う時、シームレスな連携を実現し不要な作業を取り除くこと

Tenet 4

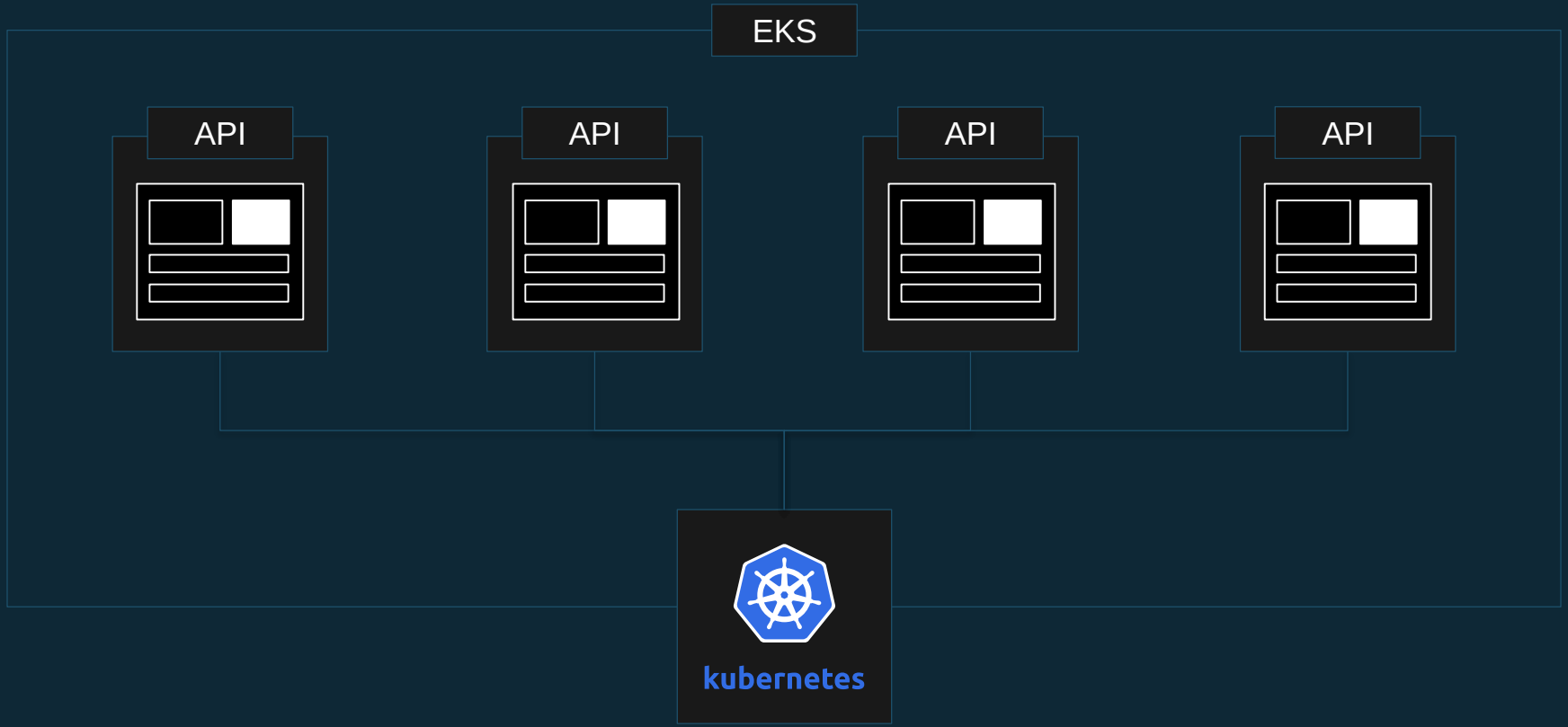
EKSチームは積極的にKubernetesプロジェクトに貢献していくこと

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

```
aws eks create-cluster –cluster-name reinvent2017 –desired-master-version
1.7.1 –role-arn arn:aws:iam::account-id:role/role-name
```

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

```
aws eks create-cluster

HTTP/1.1 200 Content-type:
application/json

{ "cluster":
    {
    "clusterName": "string",
    "createdAt": number,
    "currentMasterVersion": "string",
    "desiredMasterVersion": "string",
    "masterEndpoint": "string",
    "roleArn": "string",
    "status": "string",
    "statusMessage": "string"
    }
}
```

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

```
aws eks describe-cluster –cluster-name reinvent2017
```

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

```
aws eks describe-cluster –cluster-name reinvent2017

HTTP/1.1 200 Content-type:
application/json

{ "cluster":
    { "clusterName": "string",
    "createdAt": number,
    "currentMasterVersion": "string",
    "desiredMasterVersion": "string",
    "masterEndpoint": "string",
    "roleArn": "string",
    "status": "string",
    "statusMessage": "string" }
}
```

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

```
aws eks list-clusters
```

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

```
aws eks list-clusters


HTTP/1.1 200
Content-type: application/json
{
"clusterArns": [ "string" ],
"nextToken": "string"
}
```

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

```
aws eks delete-cluster –cluster-name
reinvent2017
```

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

```
aws eks delete-cluster –cluster-name reinvent2017

HTTP/1.1 200 Content-type:
application/json

{ "cluster":
    { "clusterName": "string",
    "createdAt": number,
    "currentMasterVersion": "string",
    "desiredMasterVersion": "string",
    "masterEndpoint": "string",
    "roleArn": "string",
    "status": "string",
    "statusMessage": "string" }
}
```

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

FargateのEKSサポートは2018年の予定

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

FargateのEKSサポートは2018年の予定

Fargate

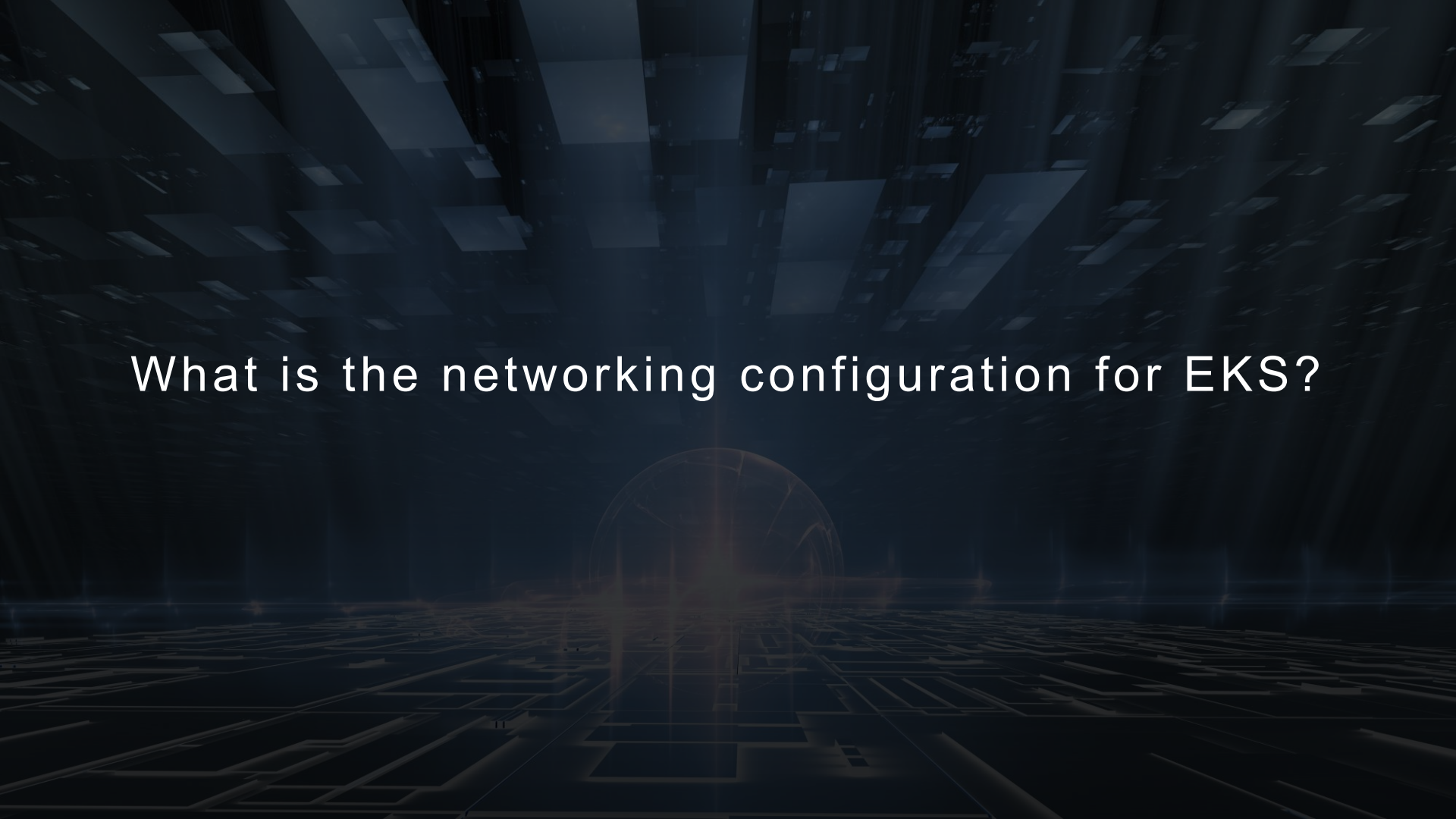
+

Amazon ECS

Amazon EKS

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws


What is the networking configuration for EKS?

CNI

VPC

Native VPC networking with CNI plugin

Pods have the same VPC address inside the pod as on the VPC

Simple, secure networking

Open source and on Github

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

How do I configure network security with EKS?

TIGERA

PROJECT CALICO

Kubernetes Network Policies enforce network security rules

Calico is the leading implementation of the network policy API

Open source, active development (>100 contributors)

Commercial support available from Tigera

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

How does IAM authentication work with Kubernetes?

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

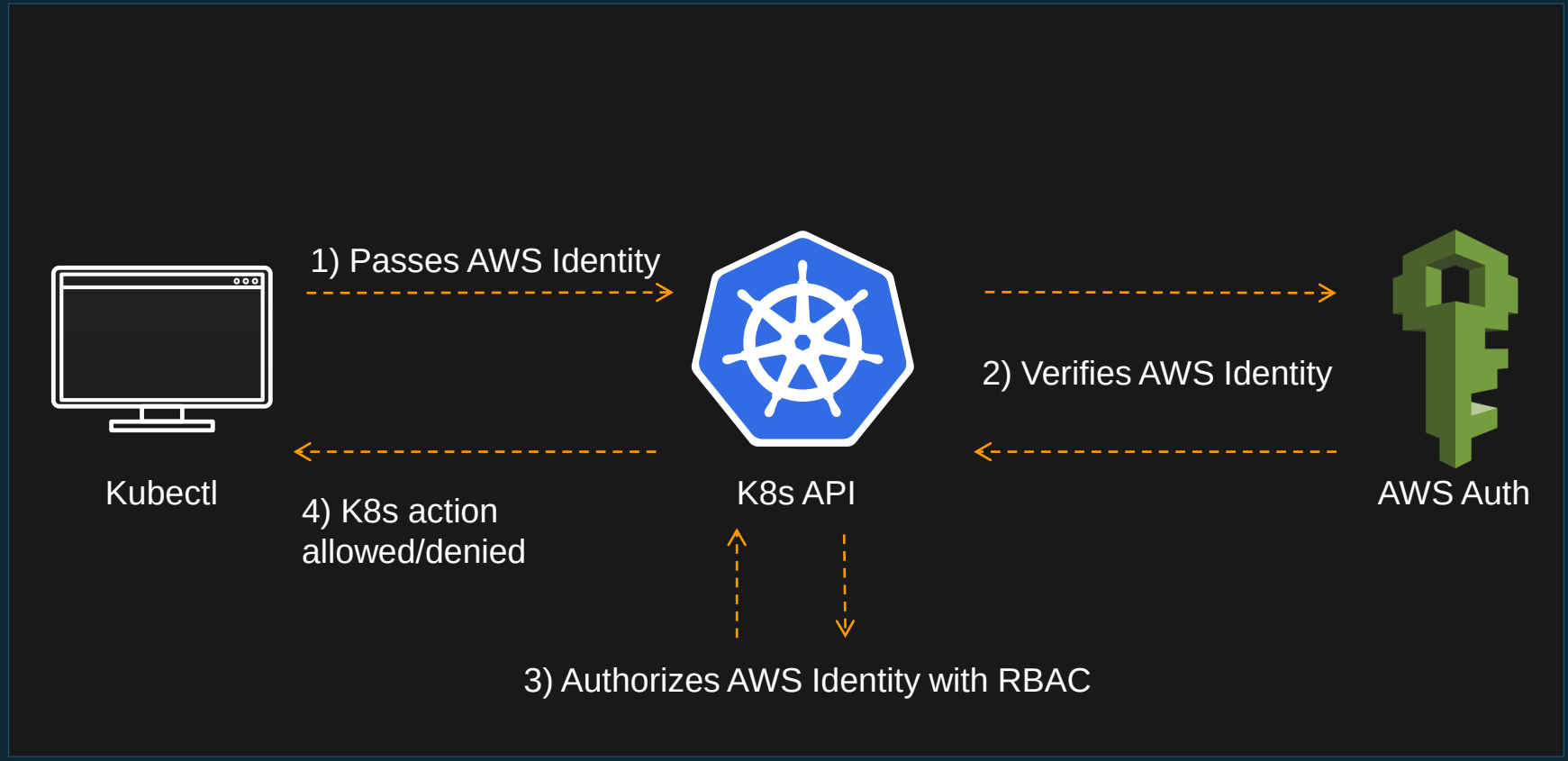
aws

Heptio IAM Authenticator

An open source approach to integrating AWS IAM authentication with Kubernetes

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws



© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Network update

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

自己紹介

名前：菊池　之裕(きくち　ゆきひろ)

所属：アマゾン ウェブ サービス ジャパン株式会社
　　ソリューションアーキテクト ネットワークスペシャリスト

ロール：Network系サービスについてのご支援

経歴：ISP,IXP,VPN運用、開発を経てネットワーク機器、仮想ルータ販売会社のプリセールス、プロダクトSEからAWSへ

好きな AWS サービス: ELB,Direct Connect,VPC,Market Place

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Agenda

- AWS Direct Connect Gateway
- AWS PrivateLink
- Amazon VPC(Inter-region VPC peering)
- AWS Time Sync Service

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

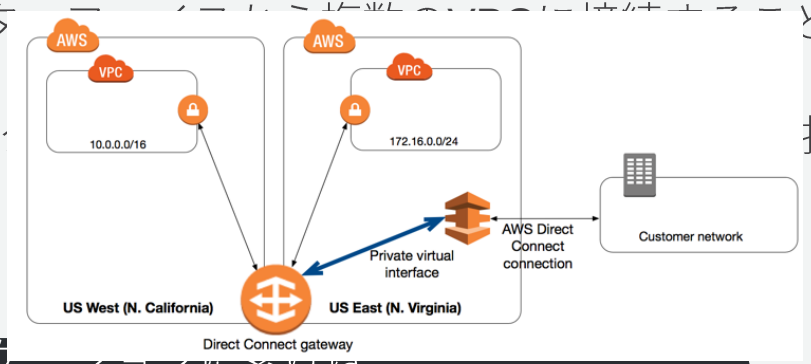
AWS Direct Connect Gateway

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Direct Connect Gateway

- Direct Connect GatewayがHubになり、同一アカウントに所属する複数のリージョンの複数のロケーションから複数リージョンの複数のVPCに接続できる機能。

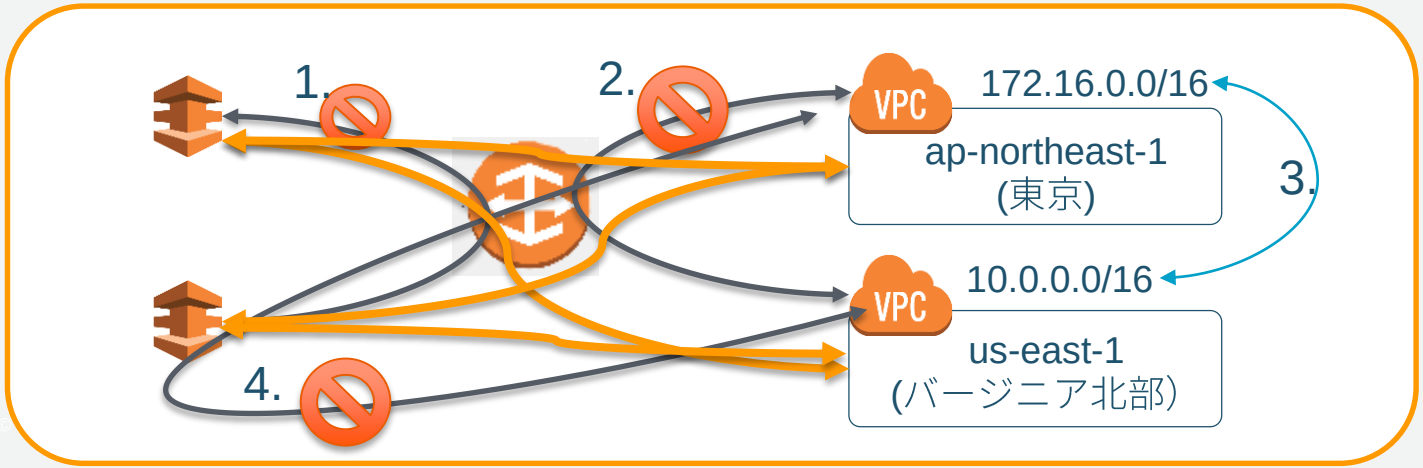
  - Direct Connectから世界の全リージョン（中国除く）のVPCに接続することができる。
  - 1つのDirect Connectの仮想インタ[illegible]とができる。
  - 複数のDirect Connectの仮想イン[illegible]接続することができる。



1つ以上のDirect Connect ロケ[illegible]ョンに繋げば
全世界の全リージョン（中国除く）に閉域網接続でき
同一リージョンまたは世界の複数リージョンをまたいで複数のVPCに接続できる機能

仕様としてできないこと

1. Direct Connect Gatewayに接続したDirect Connect同士の通信
   - 専用線接続の代わりはできません。
2. Direct Connect Gatewayに接続したVPC同士の通信
   - VPCピアリング相当のことはできません。
3. アドレスブロックが重なっているVPCのアタッチ及び通信
4. 同一VIFを使った折り返しVPC間通信（ヘアピン通信）

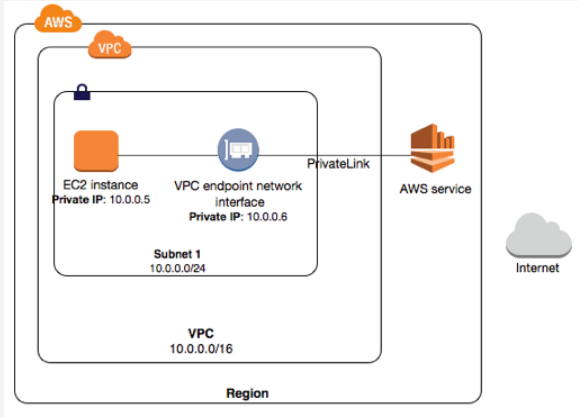


AWS PrivateLink

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

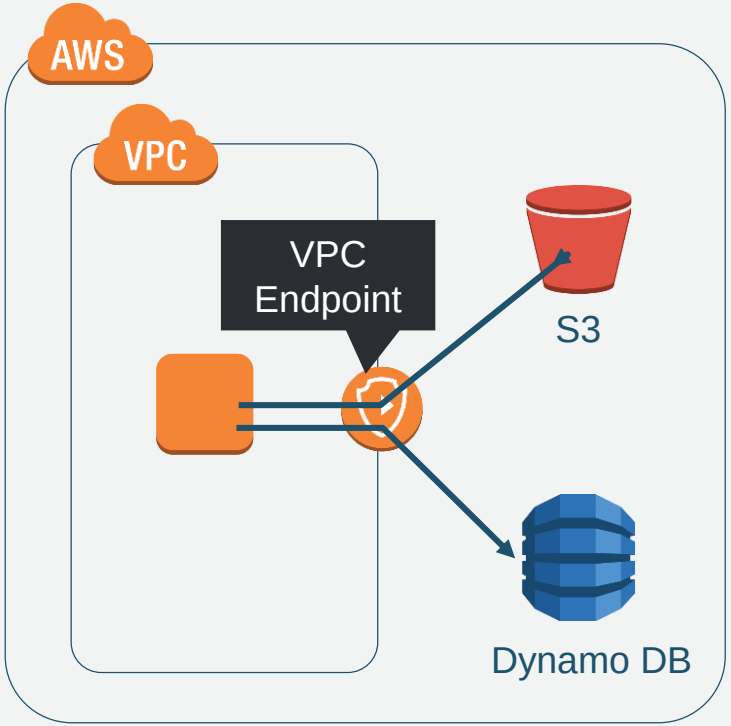
AWS PrivateLink for AWS

- https://aws.amazon.com/jp/about-aws/whats-new/2017/11/introducing-aws-privatelink-for-aws-services/
- パブリック IP を使用することなく、またインターネット全体を横断するトラフィックを必要とすることなく、Amazon Virtual Private Cloud (VPC) から AWS のサービスにプライベートにアクセスできます。
- 対応サービス
    - Amazon Kinesis Streams
    - Elastic Load Balancing API
    - Amazon Elastic Compute Cloud (Amazon EC2) API
    - Amazon EC2 Systems Manager (SSM)
    - AWS Service Catalog



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

VPC Endpoint概要

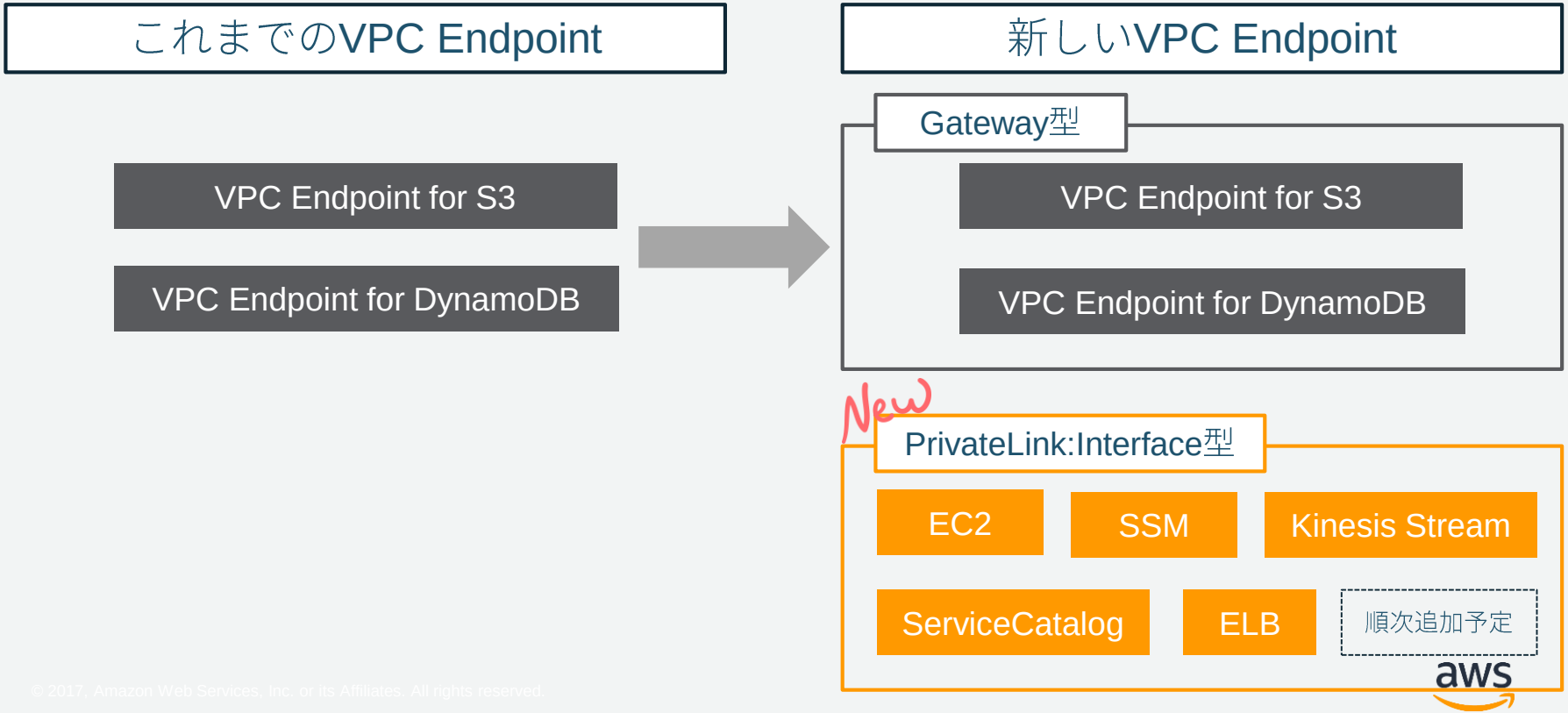


VPC Endpointは、グローバルIPをもつAWSのサービスに対して、VPC内部から直接アクセスするための出口です。

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

新しいVPC Endpoint

これまでのVPC Endpointは「Gateway型」となり、新たに「Privatelink(Interface型)」が追加されました。

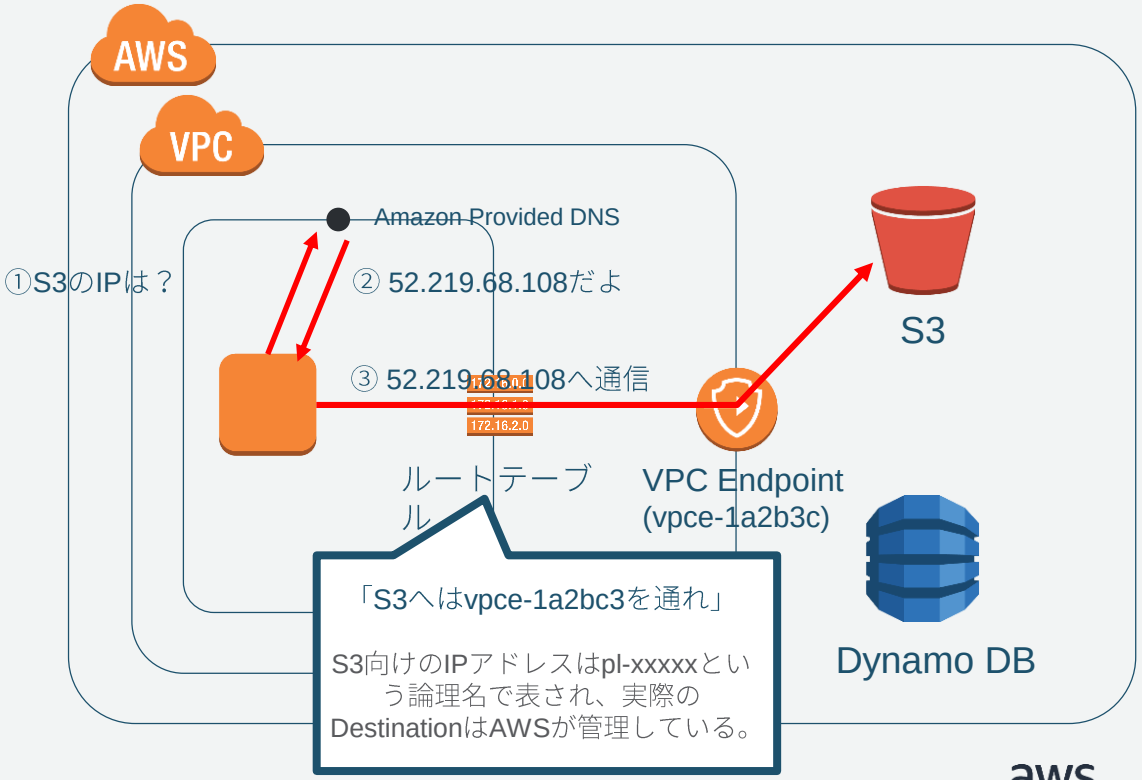


© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

動作比較

Gateway型の動作

- サブネットに特殊なルーティングを設定し、VPC内部から直接サービスと通信する。
- 通信先のIPアドレスはグローバルIPアドレス

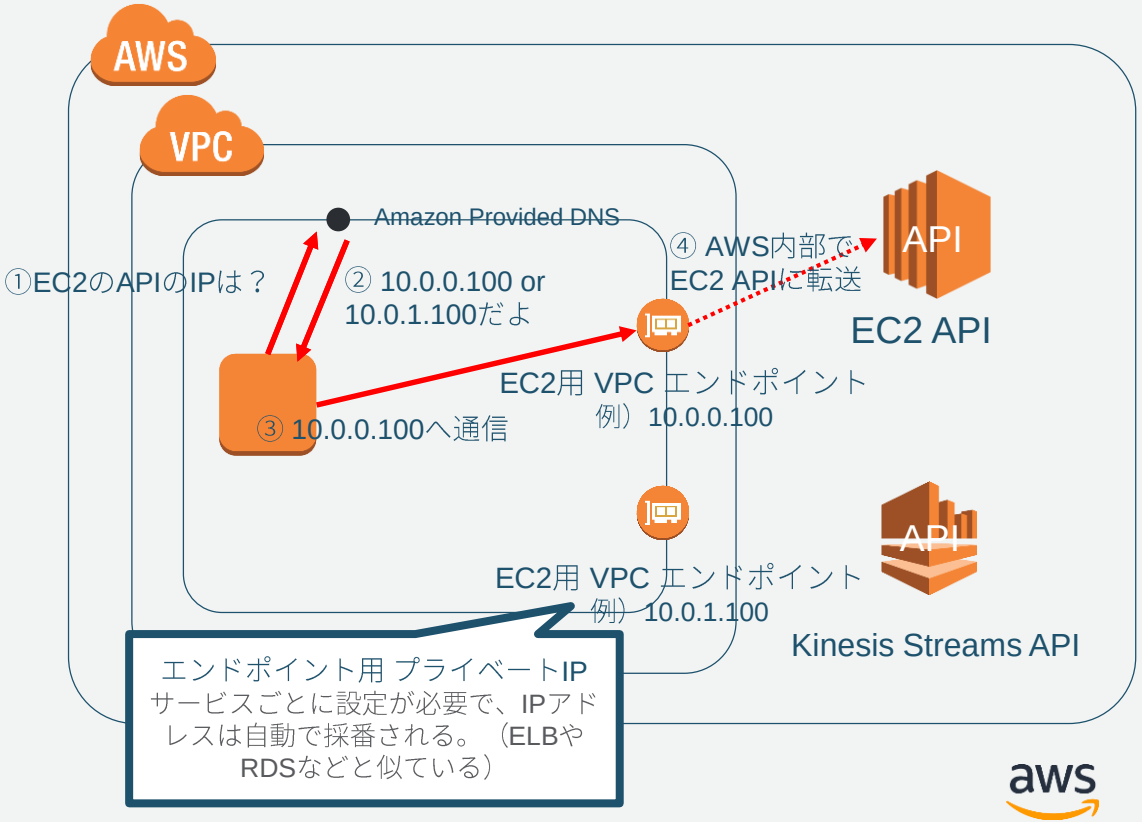


© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

動作比較

PrivateLink (Interface型)の動作

- サブネットにエンドポイント用のプライベートIPアドレスが生成される。
- VPC内部のDNSがエンドポイント向けの名前解決に対してしてプライベートIPアドレスで回答する。
- エンドポイント用プライベートIPアドレス向け通信が内部的にサービスに届けられる。



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

機能比較

	Gateway型	PrivateLink(Interface型)
アクセス制御	エンドポイントポリシー IAM Policyと同じ構文でアクセス先のリソースを制限可能。	セキュリティグループ セキュリティグループでアクセス元IP、ポートを制御可能。対象のサービスの特定のリソースへのアクセス制御は不可。
利用料金	無料	有料 サービスごとに、1プライベートIP毎に下記の料金。 0.014 USD/時間（東京）+ 0.01 USD/ GB https://aws.amazon.com/jp/vpc/pricing/
冗長性	ユーザー側で意識する必要なし	マルチAZ設計 マルチAZで配置するように設定する。

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS PrivateLink

正式リリース

Update

お客様のアプリケーション&サービス向けのVPCエンドポイント

VPCエンドポイントを利用して自分のサービスにアクセスしたり、他のユーザからサービスにアクセスいただけるようにAWS PrivateLinkを拡張。

各企業は他のAWSのお客様にプライベート接続を介したサービスを開発・提供することができるようになりました。Network Load Balancerを利用したTCPトラフィックによるサービスを作成し、直接またはAWS Marketplaceでサービスを提供することができます。

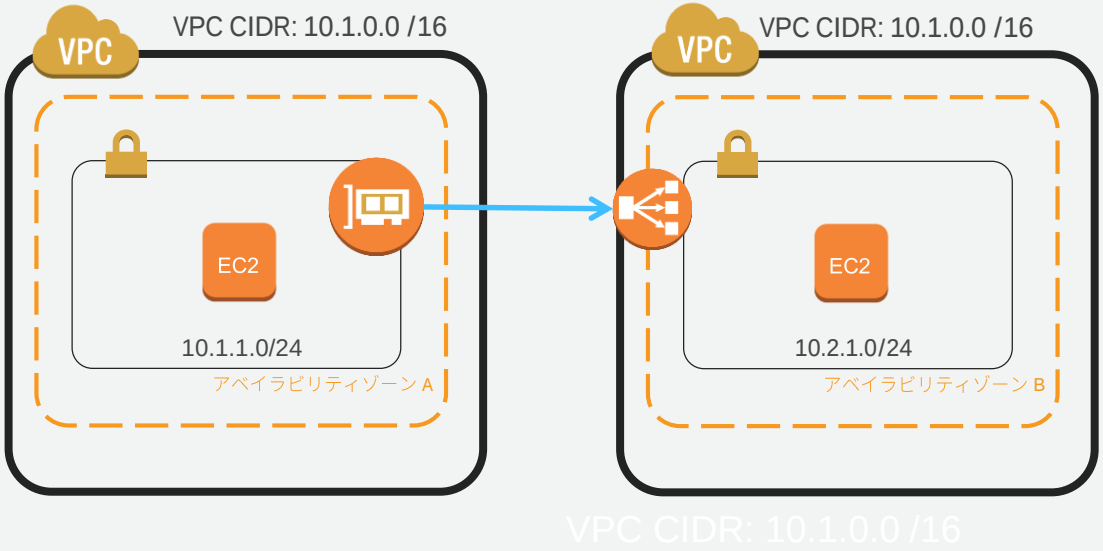
以下のSaaSはすでにエンドポイントが利用可能で、今後さらに多くのサービスが

- **CA Technologies** – CA Infrastructure Management Essentials, CA App Experience Analytics Essentials, CA Application Performance Management Essentials.
- **Aqua Security** – Aqua Container Image Security Scanner.
- **Dynatrace** – Could-Native Monitoring powered by AI.
- **Cisco Stealthwatch** – Public Cloud Monitoring – Metered, Public Cloud Monitoring – Contracts.
- **Sig Opt** – ML Optimization & Tuning.

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

Privatelink



VPC CIDR: 10.1.0.0 /16

・NLBをエンドポイントグループとして設定

- 作られたエンドポイントをホワイトリスト化
- 必要なアカウントからエンドポイントの名前 com… をサーチ
- エンドポイントとして設定
- IPアドレスの重複を許容

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

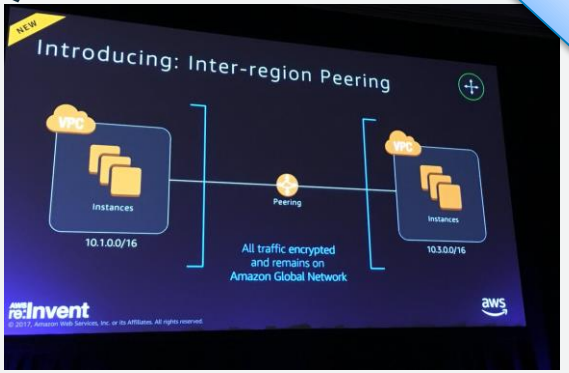
Inter-region VPC peering

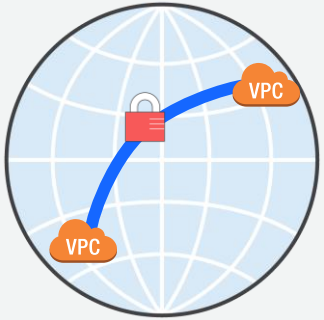
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

異なるリージョンのVPCを接続する インターリージョンVPCピアリングを発表

UPDATE

- 同一リージョン間に限定されていたVPCピアリングが別リージョンのVPC間でも設定可能に
- リージョン間の通信にはAWSが管理する回線を利用する。パブリックインターネットに迂回することはない
- 通信路はデフォルトで暗号化が適用される
- バージニア、オレゴン、オハイオ、ダブリンで先行利用可能に。他リージョンは順次展開

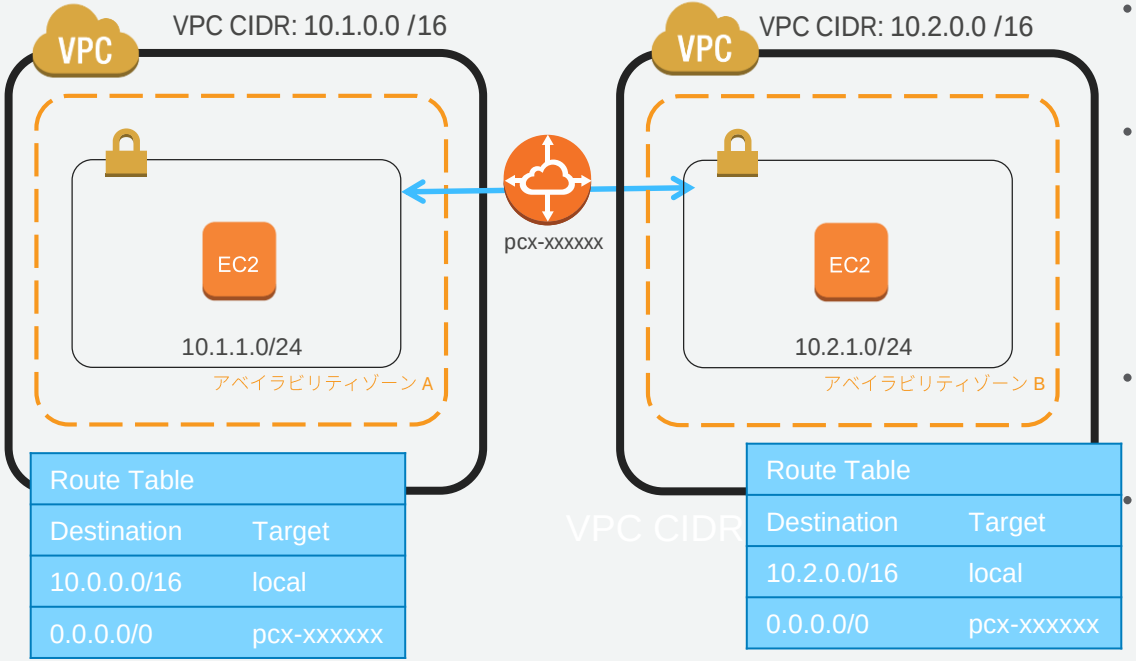




© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

VPC Peering (VPCピア接続)



- ２つのVPC間でトラフィックのルーティングが可能
- 同一のAWSアカウントはもちろん、異なるAWSアカウント間(クロスアカウント)のVPC間をピア接続することも可能
- 単一障害点や帯域幅のボトルネックは存在しない
- MTUに注意(VPC Peeringは1,500)

http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/vpc-peering.html

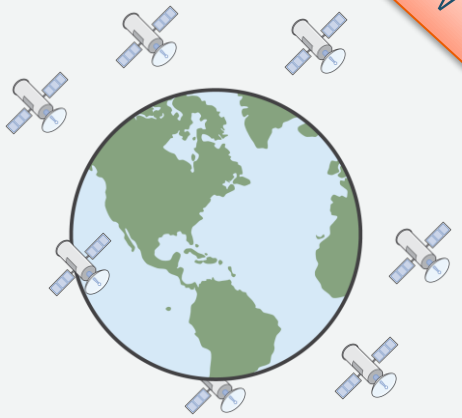
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon Time Sync Service

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

精緻な時刻同期を提供する Amazon Time Sync Serviceを発表

NEW



- VPC内で稼働する全てのインスタンスからNTPで利用できる高精度な時刻同期サービス
- EC2インスタンス内でNTPサーバのIPアドレスとしてとして169.254.169.123を設定するだけで利用できる
  - このアドレスはリンクローカルアドレスなので、外部インターネットへのアクセスは不要。プライベートサブネット内でも利用できる
- Leap Smearingによる「うるう秒」への対策が実装済み
- 無料で全リージョンで利用可能

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

Leap Smearing実例(2015/07/01)

UTC	AWS Adjusted Clock	AWS vs. UTC	Notes
11:59:59 AM June 30th, 2015	11:59:59 AM June 30th, 2015	+0	AWS clocks are synchronized to UTC.
12:00:00 PM	12:00:00 PM	+0	
12:00:01			Each second is 1/86400 longer and AWS clocks fall behind UTC. The gap gradually increases to up to 1/2 second.
	12:00:01	+1/86400	
12:00:02			
	12:00:02	+2/86400	
…	…	…	
23:59:59			
	23:59:59	+43199/86400	
23:59:60			Leap second injected to UTC.
	00:00:00 AM July 1st, 2015	-1/2	AWS clocks gain 1/2 second ahead of UTC.
00:00:00 AM July 1st, 2015			AWS clocks keep falling behind and the gap with UTC shrinks gradually.
	00:00:01	-43199/86400	
00:00:01			
	00:00:02	-43198/86400	
…	…	…	
	11:59:59 AM	-1/86400	
11:59:59 AM			
12:00:00 PM July 1st ,2015	12:00:00 PM July 1st ,2015	+0	The gap shrinks to zero. AWS clocks synchronize to UTC again.
12:00:01	12:00:01	+0	
…	…	…	

AWSの時刻はうるう秒の12時間前から 1秒の間隔1/864000秒長くなり(Smearing開始)最大1/2秒まで遅れる

うるう秒挿入により0.5秒実際の時刻より早くなる

AWSの時刻は引き続き1/864000秒長い間隔を刻み、だんだん実際の時刻に近づいていく。

うるう秒挿入12時間後にUTCと同一時刻になりSmearingは停止される。

© 2015, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

https://aws.amazon.com/jp/blogs/aws/look-before-you-leap-the-coming-leap-second-and-aws/

オンラインセミナー資料の配置場所

AWS クラウドサービス活用資料集

- http://aws.amazon.com/jp/aws-jp-introduction/

サービス別資料

無料オンラインセミナー「Black Belt Online Seminar」のサービスカット資料他、AWSのTechメンバーによる各サービスの解説資料がご覧いただけます。

ソリューション別資料

無料オンラインセミナー「Black Belt Online Seminar」のソリューションカット資料他、特定のソリューションについてのAWS活用方法がご覧いただけます。

業種別資料

無料オンラインセミナー「Black Belt Online Seminar」のインダストリーカット資料他、特定の業界のユースケースがご覧いただけます。

その他の資料

イベントに関する資料やアップデート情報などがご覧いただけます。

AWS Solutions Architect ブログ

- 最新の情報、セミナー中のQ&A等が掲載されています
- http://aws.typepad.com/sajp/

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

公式Twitter/Facebook
AWSの最新情報をお届けします

@awscloud_jp

もしくは
http://on.fb.me/1vR8yWm

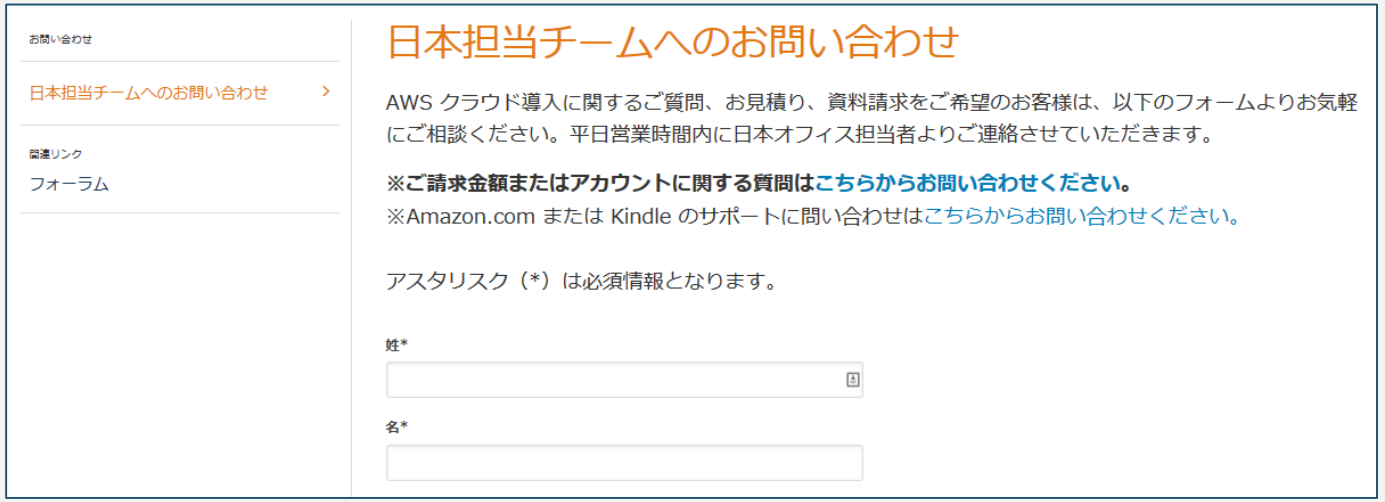
最新技術情報、イベント情報、お役立ち情報、
お得なキャンペーン情報などを日々更新しています！

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWSの導入、お問い合わせのご相談

AWSクラウド導入に関するご質問、お見積り、資料請求を
ご希望のお客様は以下のリンクよりお気軽にご相談ください

https://aws.amazon.com/jp/contact-us/aws-sales/



※「AWS　問い合わせ」で検索してください

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws