AWS Summits 2014

AWSクラウドにおける仮想デスクトップ（VDI）実現のシナリオ

Genta Watanabe

July 18, 2014

Session TA-07

amazon web services

自己紹介

- 名前
  - 渡邉源太
- 所属
  - アマゾンデータ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
- Twitter ID
  - @gentaw0
- 好きなAWSサービス
  - Amazon WorkSpaces

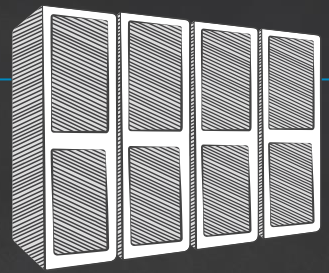
Agenda

1 仮想デスクトップ実現の方式

2 Citrix XenDesktop on AWS

3 Amazon WorkSpaces

4 まとめ



仮想デスクトップ実現の方式

サーバー共有方式	共有されたサーバーデスクトップおよびアプリケーションの画面をクライアントに配信
仮想デスクトップインフラ(VDI)方式	仮想化されたデスクトップ画面を個別にクライアントに配信

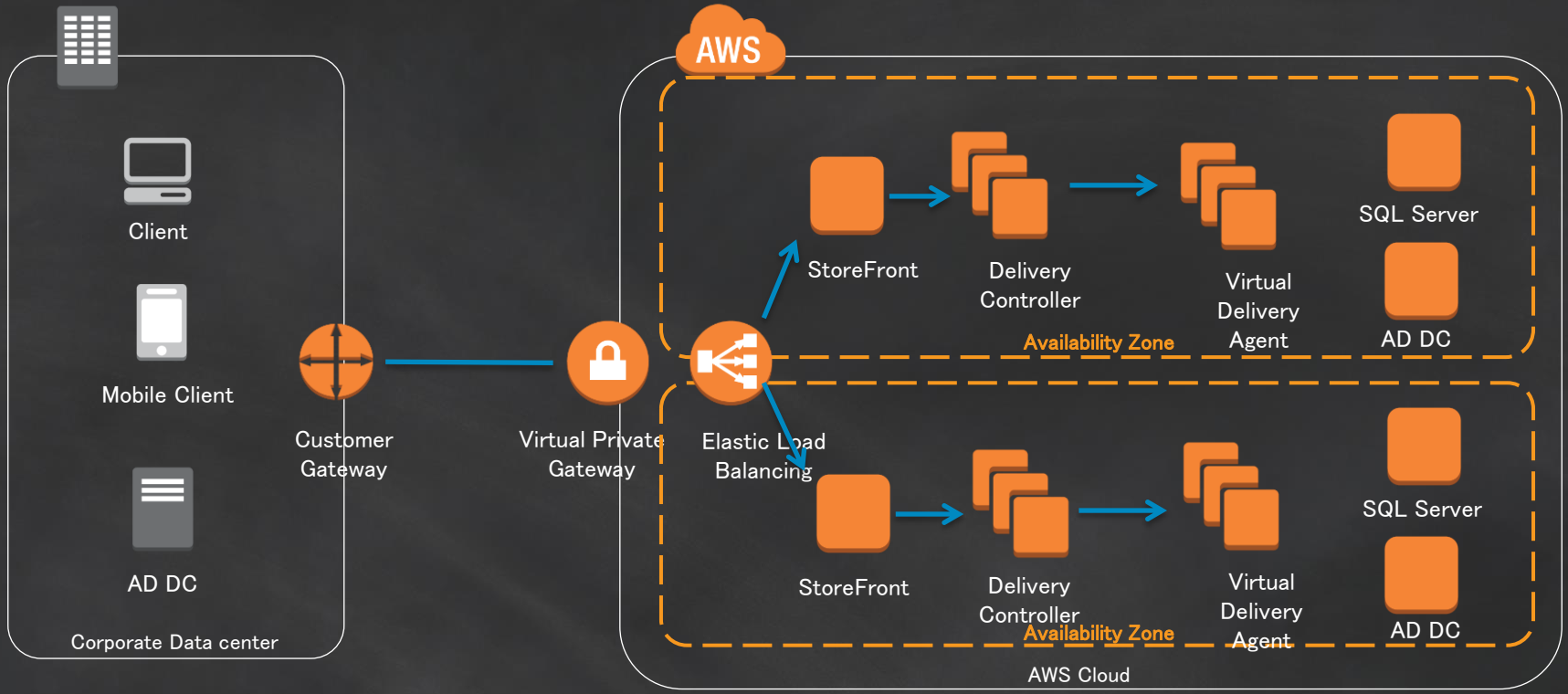
サーバー共有方式

Microsoft Windows リモートデスクトップ	Windowsの標準機能として利用可能
	RDS CALのライセンス持ち込み（BYOL）が可能に
	デスクトップとアプリケーションの配信（RemoteApp）
Citrix XenApp	AWSへの展開をサポート
	リモートデスクトップ機能を利用
	デスクトップとアプリケーションの配信

仮想デスクトップインフラ（VDI）方式

Citrix XenDesktop	AWSへの展開をサポート
	デスクトップとアプリケーションの配信（XenApp）
	サーバーOSを利用可能（サーバーVDI）
Amazon WorkSpaces	AWSで動作するフルマネージド型の仮想デスクトップサービス
	デスクトップの配信
	サーバーOSを利用

Citrix XenDesktop on AWS構成例



Citrix XenDesktopのコンポーネント

StoreFront

Delivery Controller

サイト構成データベース

ドメインコントローラー

Virtual Delivery Agent（VDA）

StoreFront

- XenDesktopを利用するユーザーのアクセス先となるポータルを提供するコンポーネント
  - Internet Information Service(IIS)が前提
  - ELBやCitrix NetScalerによる負荷分散が可能
- インターネットからのセキュアなアクセスにはNetScaler Gatewayが必要
    - NetScaler GatewayによりICAをSSL（HTTPS）にトンネリング

Citrix NetScaler on AWS

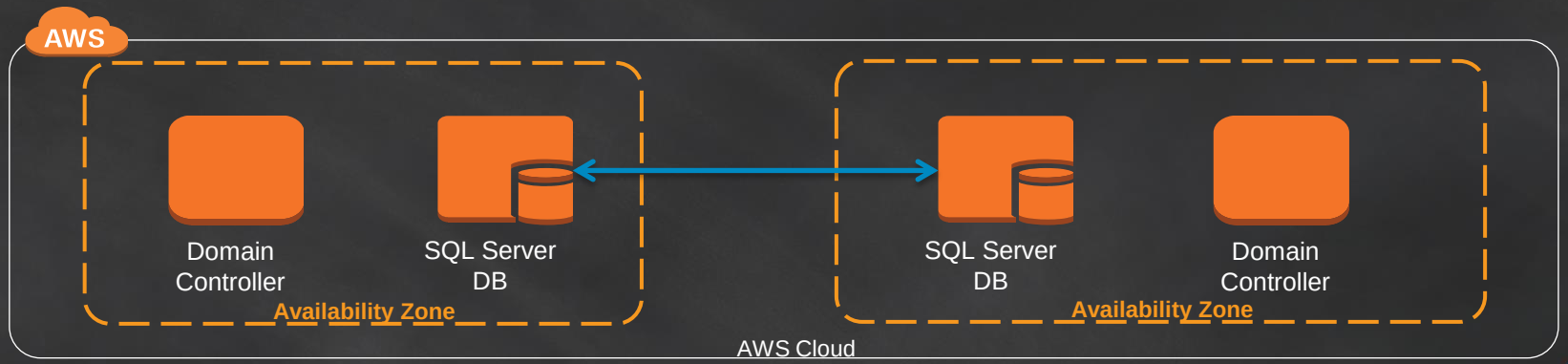
- Citrix NetScalerをAWS上で稼働させることが可能
  - AWS Marketplaceによる提供
  - 従量課金もしくはBYOLでの利用
- Citrix Networking on AWSベストプラクティスガイド
  - http://www.citrix.co.jp/products/pdf/Citrix_NetScaler_best_practice_guide.pdf

データベース要件

- サイト構成データベース
  - SQL Server 2012 SP1 Express/Standard/Enterprise
  - SQL Serve 2008 R2 Express/Standard/Standard/Enterprise/DataCenter
- 高可用性
  - SQL Serverミラーリング
  - SQL Server 2012 AlwaysOn可用性グループ
- Windows認証が必須

SQL Server AlwaysOn 可用性グループ

- Windows Server Failover Cluster ManagerおよびSQL Server 2012 可用性グループをAWS上で構成可能
- AWS上のSQL Serverのアベイラビリティゾーンをまたいだレプリケーションと高可用性を実現



Active Directory

- Active DirectoryはXenDesktopの認証と承認の基盤
- オンプレミスのドメインコントローラー（DC）とVPNを通してレプリケーションが可能
  - オンプレミスのDCによる直接認証も可能だが、パフォーマンス上の理由でレプリケーションを推奨
  - 高可用性のためAZをまたいでDCを配置

デスクトップとアプリケーションの配信

マシンカタログ	仮想マシンおよび物理コンピュータによるプロビジョニングの単位
	AWSではサーバーOSマシンカタログまたはサーバーVDIマシンカタログのみ利用可能
デリバリーグループ	デスクトップまたはアプリケーションへのユーザーの割り当て
	1つのマシンカタログから複数のデリバリーグループを作成可能

サーバーOSマシンカタログ

- サーバーOSを共有デスクトップまたは公開アプリケーションとして配信
  - XenAppの機能に相当
- Virtual Desktop Agent（VDA） for Windows Server OSをインストール
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2 SP1

サーバーVDIマシンカタログ

- サーバーOSをデスクトップとして配信
  - Windows 7/8エクスペリエンスを利用可能
  - いくつかの機能は利用できない
- Virtual Desktop Agent（VDA） for Windows Desktop OSをコマンドラインでインストール
  - XenDesktopVdaSetup.exe /quiet /servervdi

サーバーVDIマシンカタログで利用できない機能

- Personal vDisk
- HDX 3D Pro
- Microsoft System Center Configuration Manager
- ホストされるアプリケーション
- ローカルアプリケーションアクセス
- 直接（非仲介）デスクトップ接続
- リモートPCアクセス

インスタンスタイプの選択

サーバーOSマシンカタログ	高い集約率のためにはCPU、メモリが重要
	HDX 3D Proをサポート
	c3.8xlarge/g2.2xlargeなど
サーバーVDIマシンカタログ	より高いコストパフォーマンス
	t2.small/t2.mediumなど※

※InstanceTypes.xmlのアップデートが必要

T2インスタンス - 汎用タイプ

バースト可能なCPU性能のコストパフォーマンスにすぐれたタイプ

特徴

- 2.5GHzから3.3GhzにTurbo可能なIntel Xeonプロセッサ
- CPUクレジットにもとづいてバースト可能なCPU性能

モデル	vCPU	CPUクレジット/時	メモリ (GiB)	SSDストレージ (GB)	オンデマンド料金（東京)
t2.micro	1	6	1	EBSのみ	$0.025
t2.small	1	12	2	EBSのみ	$0.050
t2.medium	2	24	4	EBSのみ	$0.100

C3インスタンス - CPU最適化

CPU性能に特化したタイプ。CPUあたりの料金が最も安い

特徴

- Intel Xeon E5-2670 v2 **(Ivy Bridge)**
- **SSD**インスタンスストレージ
- 低レイテンシー、低ジッタ、高い秒間あたりのパケット性能を持つ拡張されたネットワーク (SR-IOV, VPCのみ)
- クラスタネットワークサポート

モデル	vCPU	メモリ (GiB)	SSD ストレージ (GB)	オンデマンド料金 （東京）
c3.large	2	7	2 x 16	$0.231
c3.xlarge	4	14	2 x 40	$0.462
c3.2xlarge	8	28	2 x 80	$0.925
c3.4xlarge	16	55	2 x 160	$1.849
c3.8xlarge	32	108	2 x 320	$3.699

G2インスタンス - GPU

グラフィックと汎用的な GPU コンピューティングアプリケーション向け

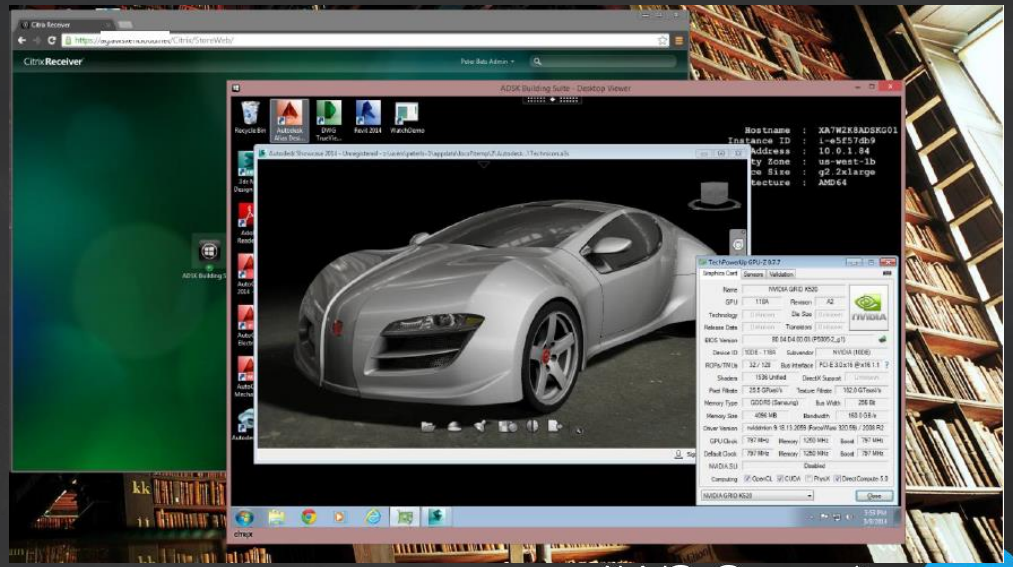
特徴

- Intel Xeon E5-2670 (Sandy Bridge)
- 1,536 CUDA コアと 4GB のビデオメモリを搭載した高パフォーマンスの NVIDIA GPU
- SSDのインスタンスストレージ

モデル	vCPU	メモリ (GiB)	SSD ストレージ (GB)	オンデマンド料金 （東京）
g2.2xlarge	8	15	1 x 60	$1.010

G2インスタンス+HDX 3D Pro

- g2.2xlargeではHDX 3D Proを有効にして3Dアプリケーションの実行が可能
  - 3D CAD
  - 医療用画像処理



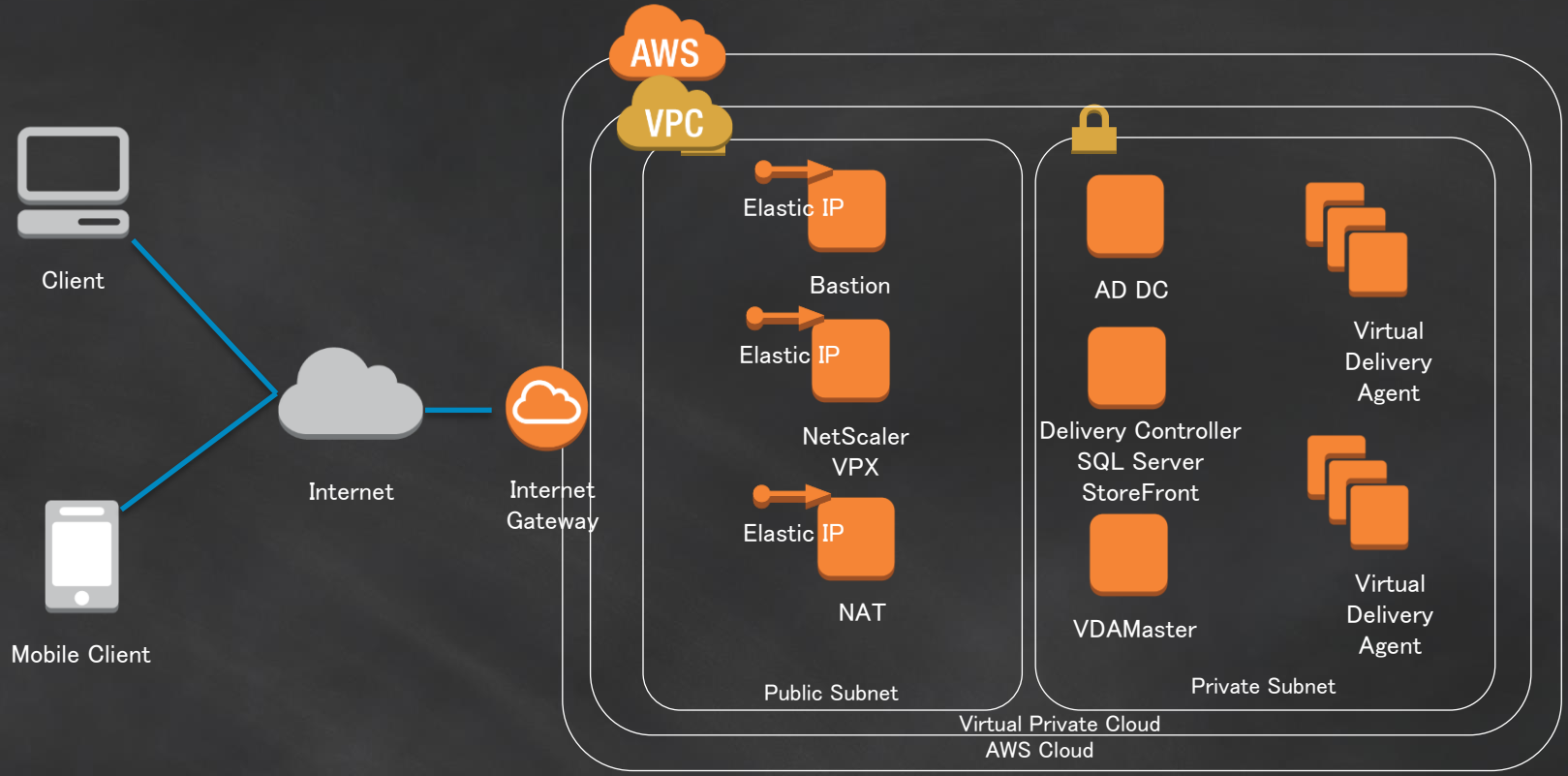
EBS General Purpose (SSD)ボリューム

- EBSのボリュームとしてGeneral Purpose（SSD）ボリュームタイプを追加
  - General Purpose（SSD）
  - Provisioned IOPS （SSD）
  - Magnetic
- 1GBあたりのベースラインは3IOPS
- 最大3000IOPSまでバースト

CloudFormationによる展開

- Amazon VPCによるXenAppおよびXenDesktop 7.5の展開
  - http://support.citrix.com/article/CTX140630
- CloudFormationテンプレートによりXenApp/XenDesktopのインフラストラクチャスタックが作成される

CloudFormationにより展開される環境



CloudFormationテンプレートの利用

- NetScalerをAWS Marketplaceで有効にしておく
- テンプレートのURLは最新のものを使用する
  - https://s3.amazonaws.com/cf-XenDesktop/XD75NSonAWS_CF_v1_**3**.json
- XenDesktopのセットアップは手動で実行する必要がある

Citrix XenDesktop on AWSまとめ

- 従来とほぼ同じ考え方でXenApp/XenDesktopをAWS上に展開可能
- G2インスタンス + HDX 3D PROでCADなどの3Dアプリケーションを実行
- デスクトップおよびアプリケーションの配信に対応

amazon WorkSpaces

Amazon WorkSpaces

- クラウドで動作するフルマネージド型のデスクトップコンピューテイングサービス
- ノートPC/iPad/Kindle Fire/Androidタブレットなど任意のデバイスからアクセス
- マネジメントコンソールを数回クリックするだけでデスクトップをユーザー数を問わずに展開可能

自社構築 vs. EC2 vs. フルマネージド

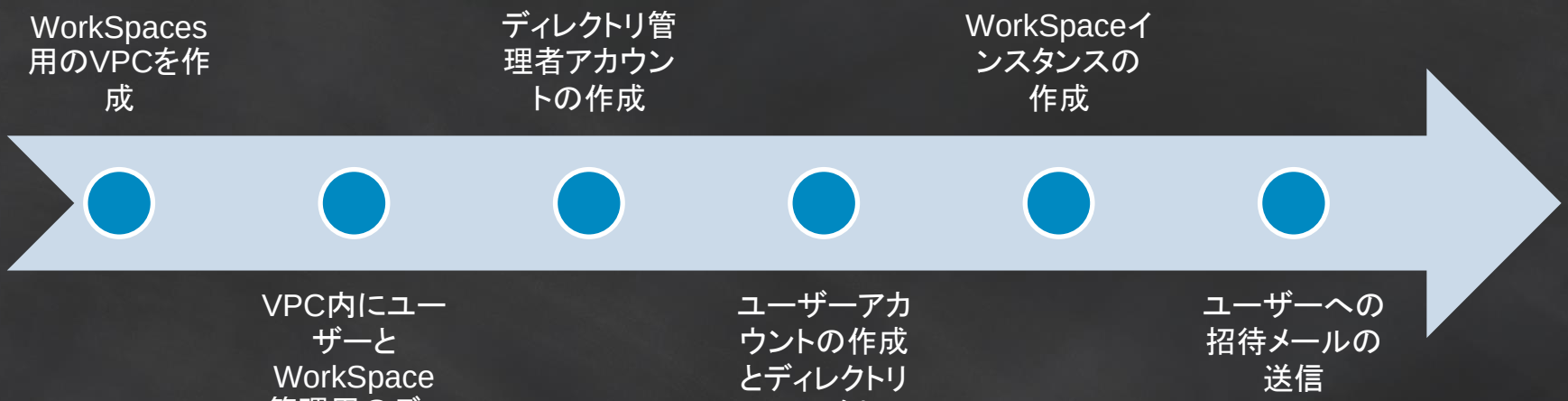
オンプレミス	XenDesktop on EC2	WorkSpaces
App installs	App installs	App installs
Scaling	Scaling	Scaling
High availability	High availability	High availability
Backups	Backups	Backups
s/w patches	s/w patches	s/w patches
s/w installs	s/w installs	s/w installs
OS patches	OS patches	OS patches
OS installation	OS installation	OS installation
Server maintenance	Server maintenance	Server maintenance
Rack & stack	Rack & stack	Rack & stack
Power, HVAC, net	Power, HVAC, net	Power, HVAC, net

お客様がご担当する作業　　AWSが提供するマネージド機能

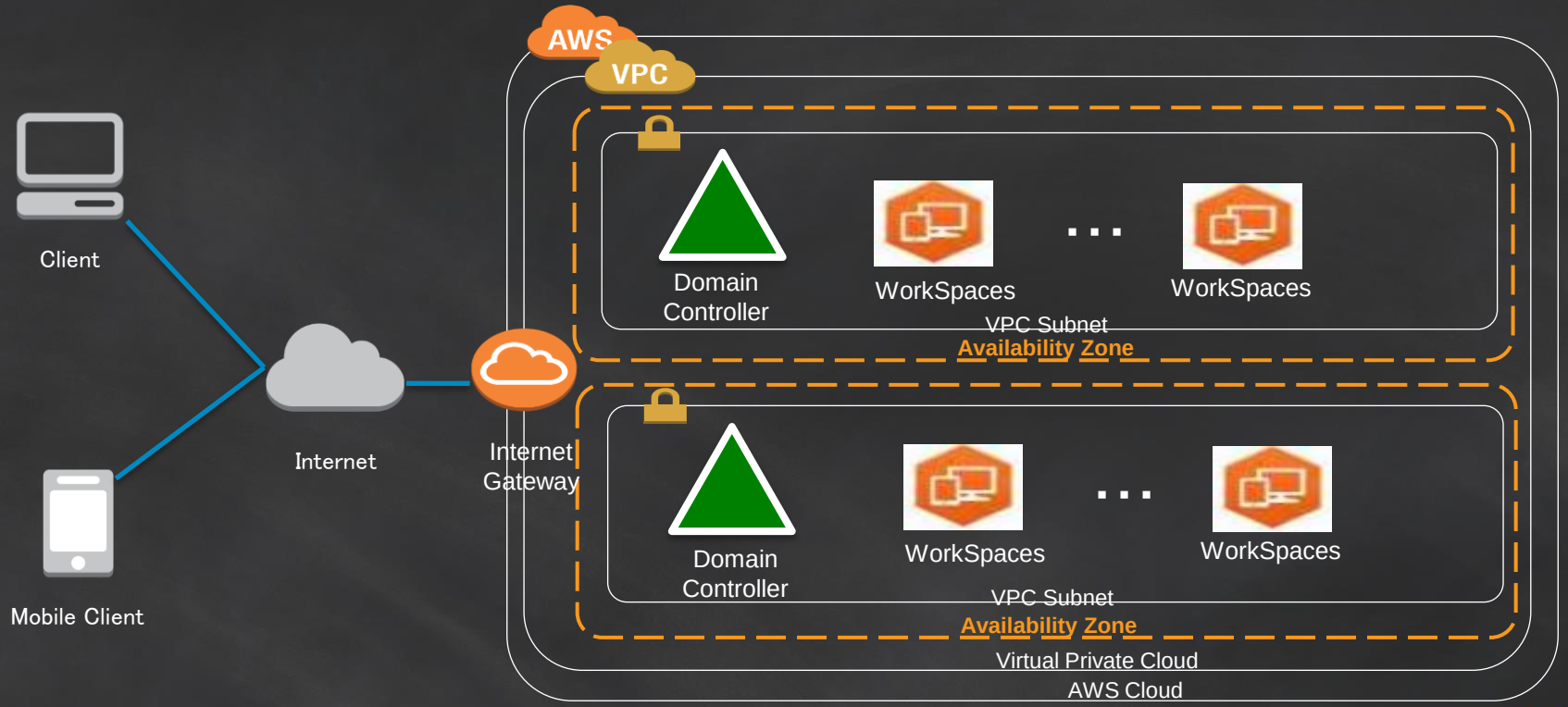
Amazon WorkSpacesセットアップ

Quick Setup	必要な環境を自動的に作成
	20分でWorkSpaceを利用可能
Advanced Setup	VPCやディレクトリの選択が可能
	社内Active Directoryとの統合

Quick Setupで実行されるプロセス



Quick Setupで作成される環境



Advanced Setup

- 既存のVPCやオンプレミスのActive Directoryとの連携を行う場合はこちらを選択
- 以下の手順を手動で実行する
  - WorkSpaces用のVPCの作成
  - ディレクトリのセットアップ
  - WorkSpaceのプロビジョニング

ディレクトリの選択

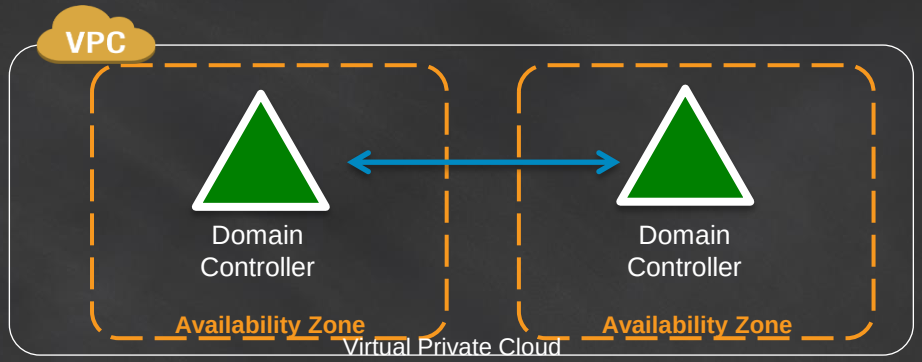
WorkSpaces Cloud Directory	フルマネージドのディレクトリサービス
	WorkSpaces用に独立したドメインを作成
WorkSpaces Connect	既存のディレクトリへの接続
	オンプレミスまたはVPC上のドメインを指定

WorkSpaces Cloud Directory

- Active Directoryドメインと管理者アカウントを作成する
  - Organization Name
  - Directory DNS
  - NetBIOS Name
  - Administrator Password
- ディレクトリを作成するVPCを選択
  - VPCには異なるAvailability Zoneに２つ以上のSubnetが存在する必要がある

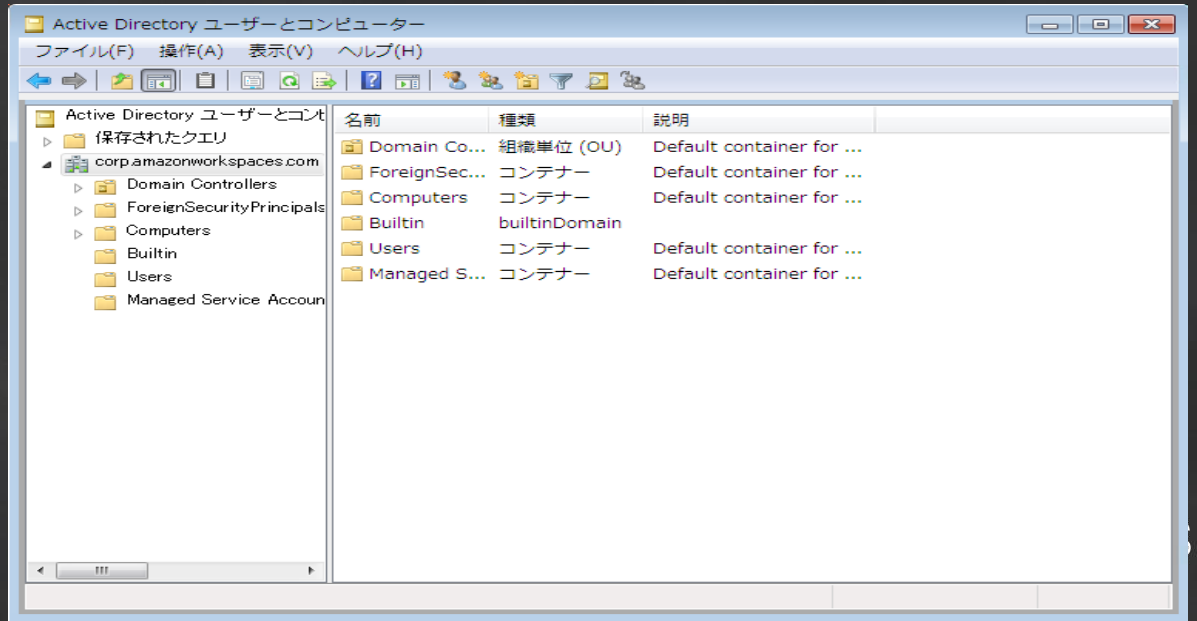
作成されたCloud Directory

- Domain ControllerはMulti-AZ構成で複数のSubnetに展開される
  - EC2インスタンスとしては表示されない
- Active Directoryの管理ツールから操作可能
  - Redircmp.exe
  - イベントビューア
  - Active Directoryユーザとコンピュータ



Cloud Directoryの管理

- Active Directory管理ツールをインストールすることによりディレクトリの管理が可能
  - %SystemRoot%¥system32¥dsa.msc



Security Groupの設定

- Domain Controller用およびWorkSpaces用のSecurity Groupは自動的に作成される
  - <organization name>_controllers
  - <organization name>_members
  - <organization name>_workspacesMembers
- EC2 Consoleから確認及び設定変更が可能

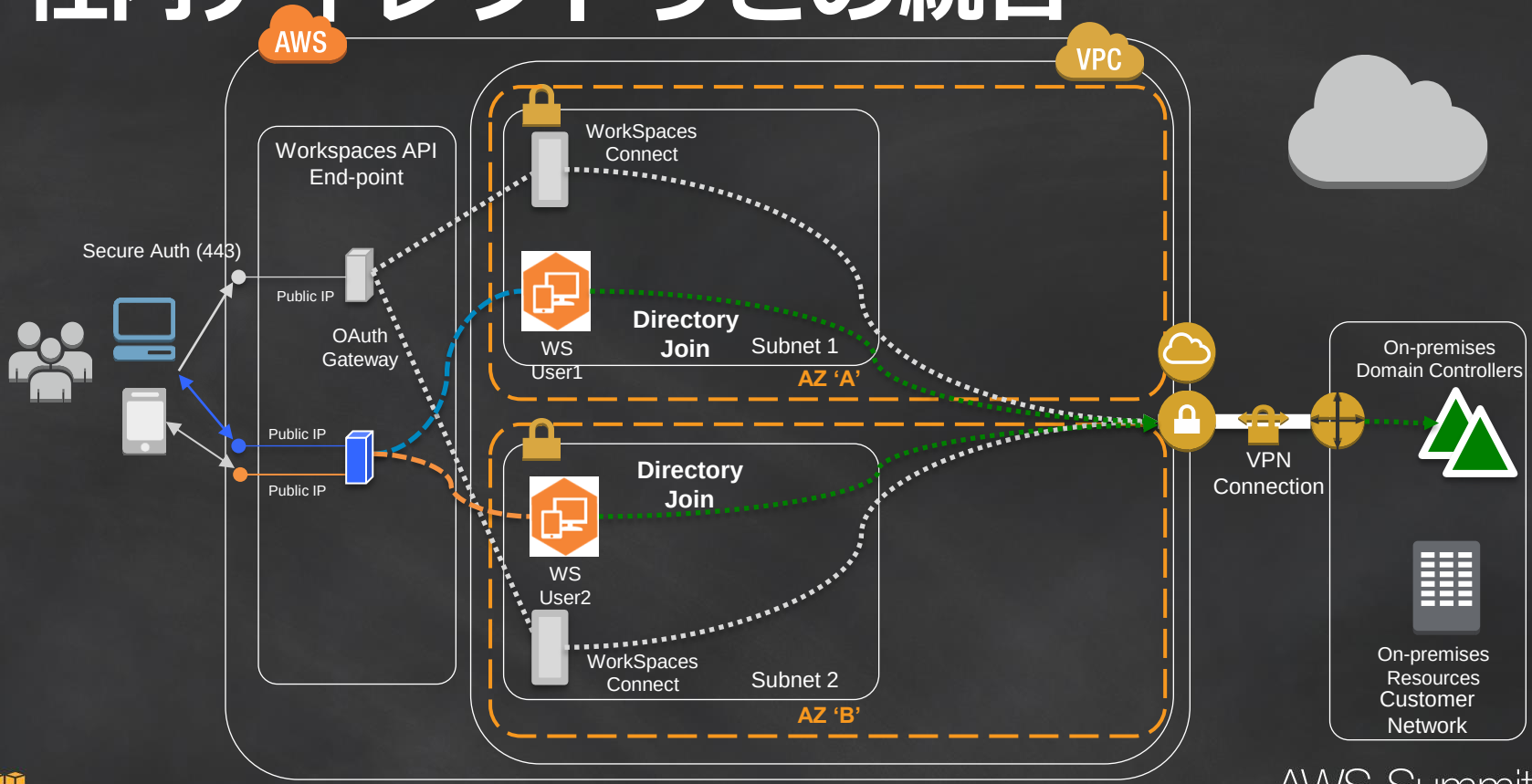
Directory Details

- Organizational Unit（OU）
  - デフォルトではComputer OUにコンピュータが作成される
  - 特定のOUを指定して変更することが可能
- Security Group
  - WorkSpacesのSecurity Groupを指定
  - デフォルトのSecurity Groupとあわせて有効になる

WorkSpaces Connect

- オンプレミスのActive Directoryと接続してディレクトリ認証を行う仕組み
- 前提として必要となるもの
  - Amazon VPC
    - Internet Gateway
    - VPN接続またはDirect Connect
  - ドメインアカウント
    - ユーザーとグループへの読み取り
    - コンピュータオブジェクトの作成
  - オンプレミスのDNSサーバーまたはドメインコントローラー2台のIPアドレス

社内ディレクトリとの統合

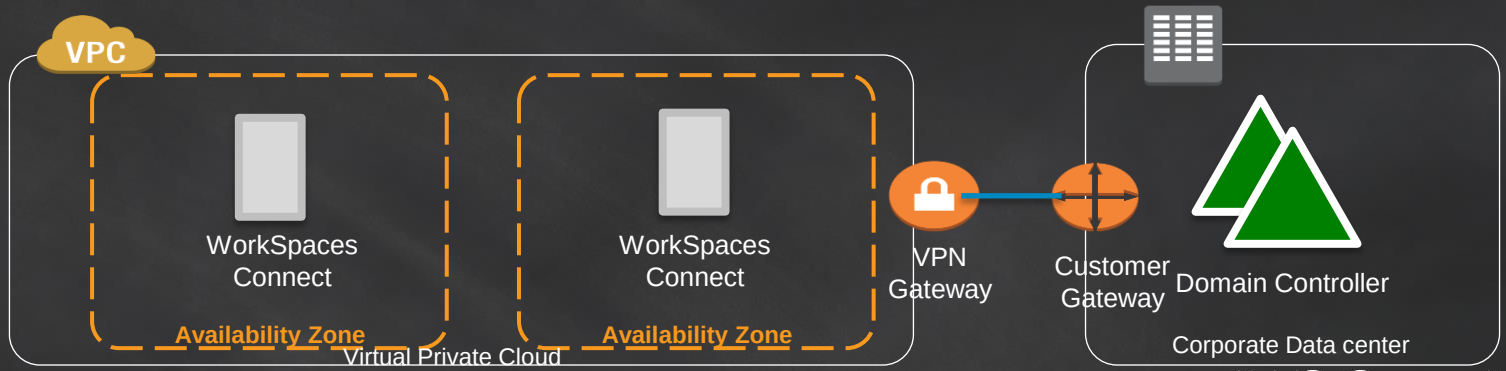


WorkSpaces Connectの作成

- 既存のActive Directoryドメイン情報を入力
  - Organization Name
  - Directory DNS
  - NetBIOS Name
  - Account username
  - Administrator Password
- ディレクトリを作成するVPCを選択
  - VPCには異なるAvailability Zoneに２つ以上のSubnetが存在する必要がある

作成されたWorkSpaces Connect

- VPC上に認証用プロキシが作成される
  - ディレクトリにVPN接続を経由して認証する
  - 既存のユーザー認証およびポリシーを適用可能



WorkSpaces Bundle

WorkSpaces Bundle	ハードウェア	アプリケーション
Standard	1 vCPU, 3.75 GiB Memory, 50 GB User Storage	ユーティリティ (Adobe Reader, Internet Explorer 9, Firefox, 7-Zip, Adobe Flash)
Standard Plus	1 vCPU, 3.75 GiB Memory, 50 GB User Storage	Microsoft Office Professional 2010, Trend Micro Worry-Free Business Security, ユーティリティ (Adobe Reader, Internet Explorer 9, Firefox, 7-Zip, Adobe Flash)
Performance	2 vCPU, 7.5 GiB Memory, 100 GB User Storage	ユーティリティ (Adobe Reader, Internet Explorer 9, Firefox, 7-Zip, Adobe Flash)
Performance Plus	2 vCPU, 7.5 GiB Memory, 100 GB User Storage	Microsoft Office Professional 2010, Trend Micro Worry-Free Business Security, ユーティリティ (Adobe Reader, Internet Explorer 9, Firefox, 7-Zip, Adobe Flash)

WorkSpacesの日本語化

- Windows Server 2008 R2 SP1用のMUIパックを インストールする
  - http://www.microsoft.com/ja- j p/download/details.aspx?id=2634
- コントロールパネルの「Change display language」から日本語を選択してログオフ

ネットワークインターフェース

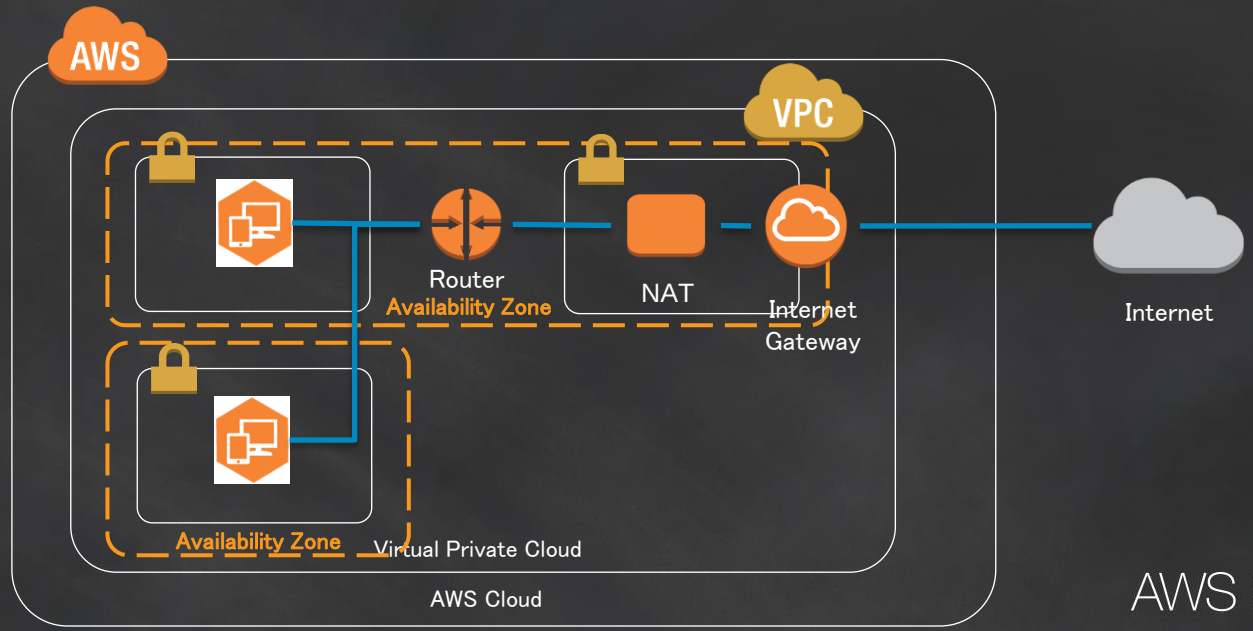
- それぞれのWorkSpaceは 2 つのネットワークインターフェース（ENI）をもつ
  - VPCおよびインターネット接続用ネットワーク
  - WorkSpace管理用および画面転送用ネットワーク
- 管理用ネットワークでは以下のポートを利用する
  - インバウンド
    - TCP/UDP 4172
    - TCP 8200
  - アウトバウンド
    - UDP 55000

インターネットへの接続

- WorkSpacesがインターネット接続するためにはNATインスタンスもしくはEIPの付与が必要
  - Cloud Directory NAT Instanceパターン
  - Connected Directory NAT Instanceパターン
  - On-Premise Firewallパターン
  - Elastic IP Addressパターン

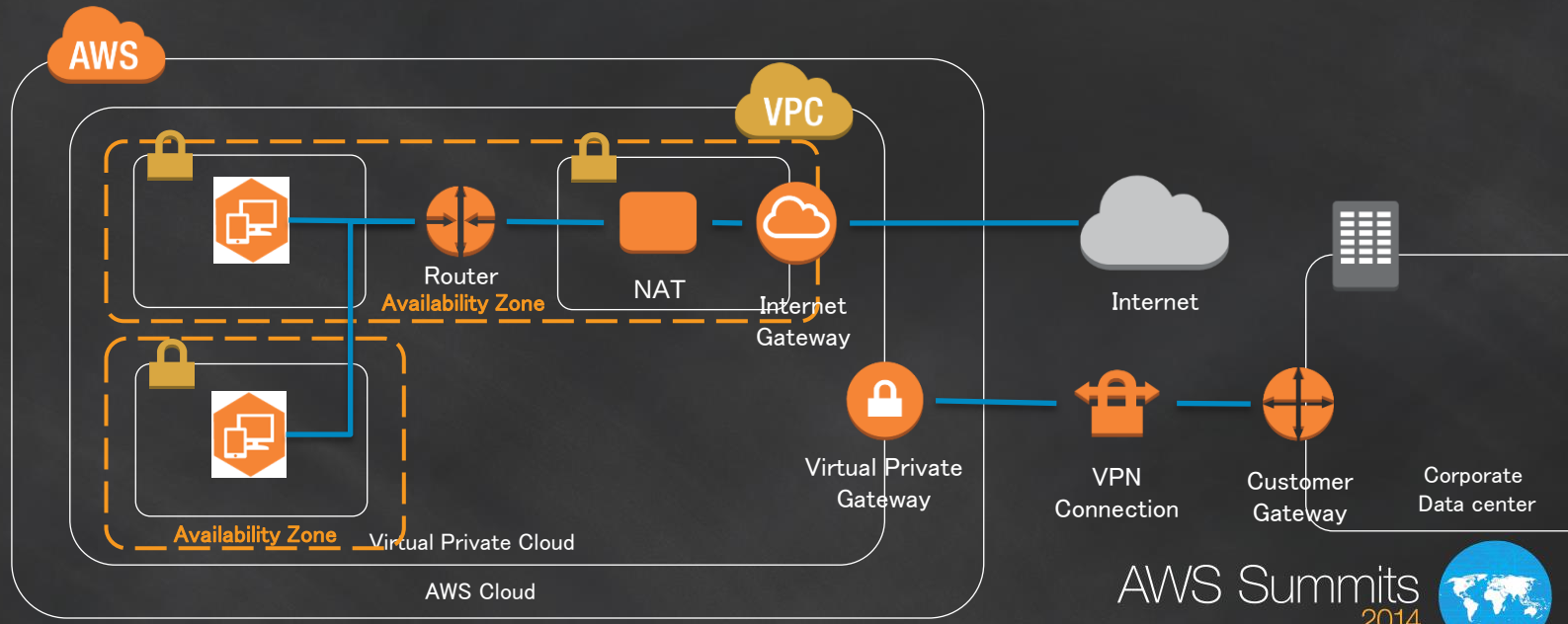
構成1:Cloud Directory NAT Instanceパターン

- NATインスタンスを経由してインターネットへアクセス



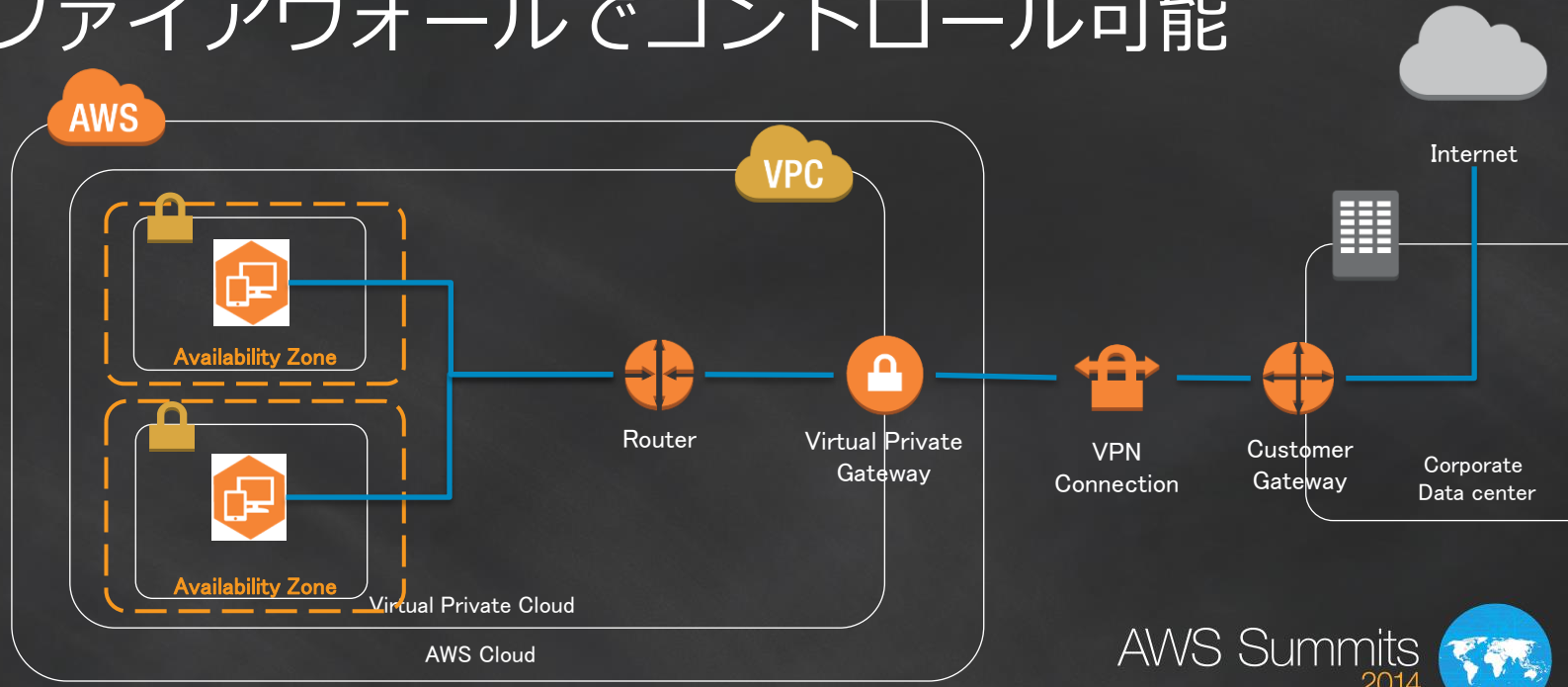
構成2:Connected Directory NAT Instanceパターン

- インターネットと社内リソースの両方にアクセスすることが可能



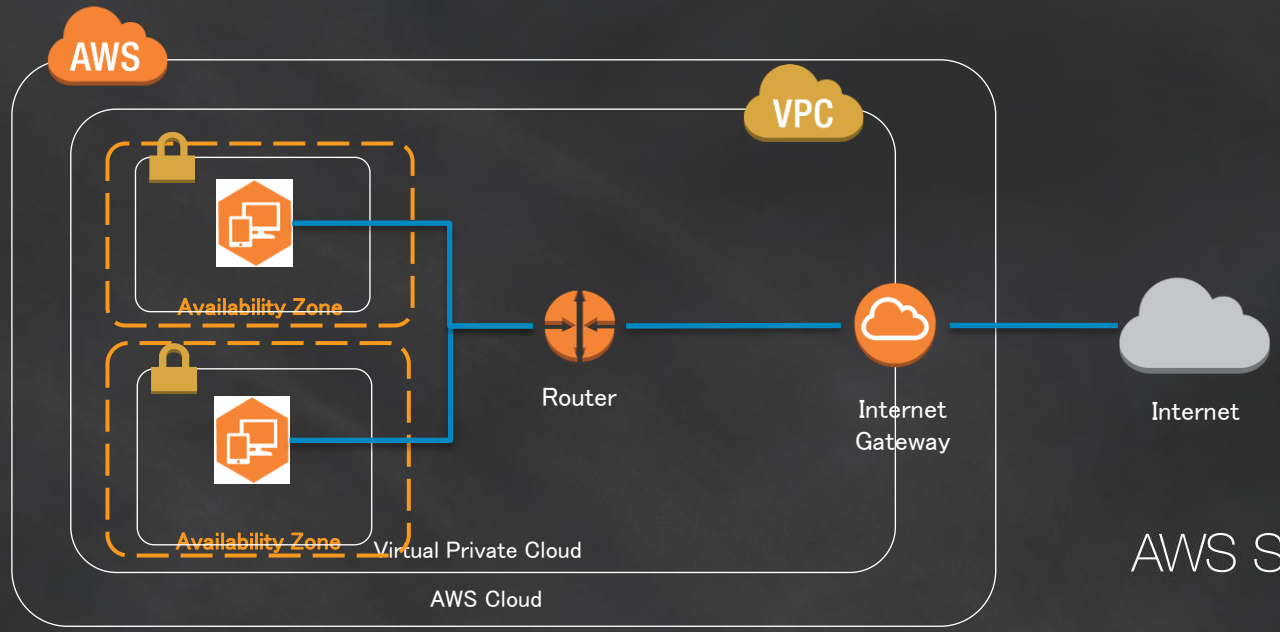
構成3:On-Premise Firewallパターン

- インターネットへの接続ポリシーをオンプレミスのファイアウォールでコントロール可能



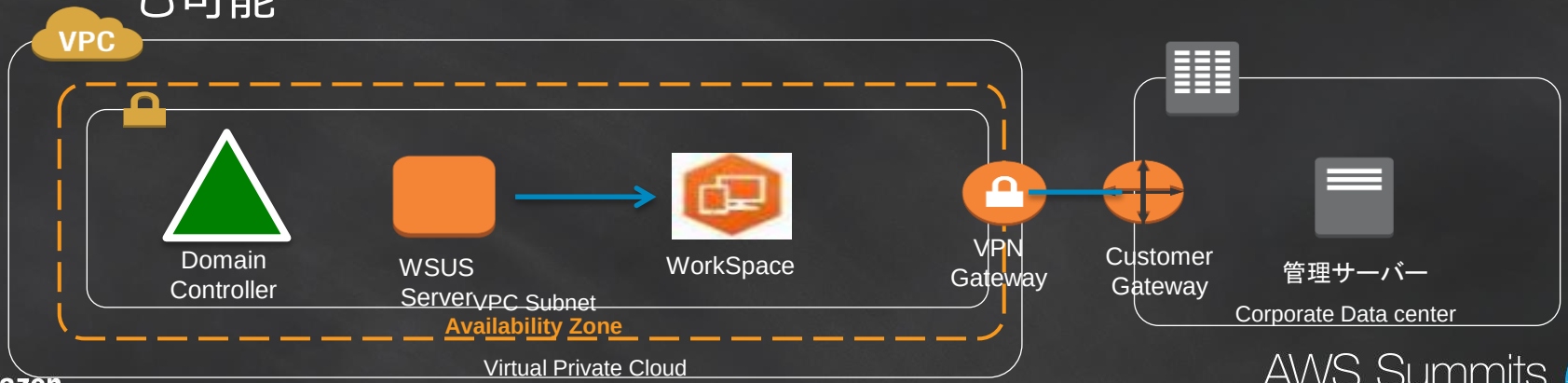
構成4:EIP（Elastic IP Address）パターン

- WorkSpacesのENIに直接EIPを付与することで直接インターネットアクセスへ可能



WorkSpacesのポリシー管理・パッチ管理

- それぞれのWorkSpacesはActive Directoryドメインのコンピュータとして管理される
  - 既存の管理ツールを利用しての管理
  - VPC内にEC2インスタンスとして管理サーバーを配置することも可能



LAN Scope Catによる管理

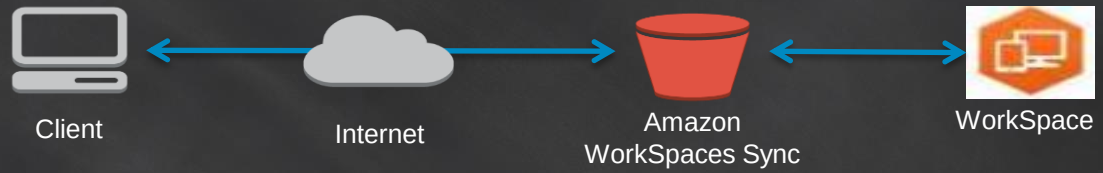
- MOTEXのLAN Scope Cat Ver. 8.0がAmazon WorkSpacesに対応
  - 仮想デスクトップのインベントリ管理や操作ログの取得が可能

WorkSpacesクライアント

- サポートするプラットフォーム
  - Windows 7以降
  - Mac OS X 10.7以降
  - iOS 6.1.2以降
  - Android 2.3.5以降
  - Kindle Fire HDX, Kindle Fire Gen2, Fire 8.9, HD7
- ネットワーク要件
  - TCP/UDP 4172
  - TCP 443
  - RTT 100ms以下を推奨

Amazon WorkSpaces Sync

- ローカルのフォルダをWorkSpaceと同期
  - ユーザーあたり10GB上限
  - 管理者により無効化することが可能
- Amazon WorkSpacesとは独立して動作する
  - http://sync.amazonworkspaces.comより AmazonWorkSpacesSync.exeを別途導入して実行



Amazon Zocalo

- フルマネージド型の企業向け文書保存・共有サービス
  - データは暗号化のうえ、指定したリージョンに保管される
  - 既存ADとも連携可能なユーザ権限管理機能を備える
- 1人あたり200GBの容量を月額5ドルで利用可能
  - 1GBあたり月額0.03ドルの追加料金でストレージの増量にも対応
- WorkSpacesユーザは50GBまで無料でZocaloを利用できる
  （月額2ドルで200GBにアップグレード）

まとめ

- 仮想デスクトップをAWS上で利用することが可能
  - 共有サーバー方式
  - 仮想デスクトップインフラ（VDI）方式
- Amazon WorkSpacesはフルマネージドで仮想デスクトップを配信
  - 既存のActive Directoryと連携が可能
  - Amazon Zocaloとの統合

AWS Summits
2014

amazon web services

AWS Summits
2014

2014.09.09 SAVE THE DATE

http://csd.awseventsjapan.com/

Cloud Storage & DB Day　検索

amazon web services

AWS Summits 2014