



AWS
Black Belt
Online Seminar

【AWS Black Belt Online Seminar】 Amazon WorkSpaces

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 渡邊源太

2016.12.21

内容についての注意点

- ❏ 本資料では2016年12月21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おります。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.

Agenda

- Amazon WorkSpacesとは
- セットアップと管理
- 最新アップデート
- 設計のベストプラクティス

Agenda

- Amazon WorkSpacesとは
- セットアップと管理
- 最新アップデート
- 設計のベストプラクティス

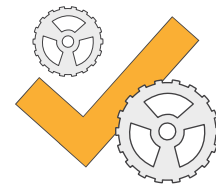
Amazon WorkSpaces – マネージド型クラウドデスクトップ



セキュア



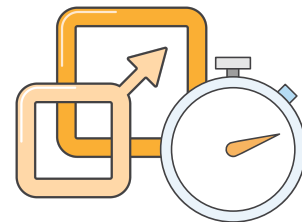
高度にインタラクティブでつかいやすい
セキュアなデスクトップ



シンプルなデプロイと管理



従量課金



スケール&パフォーマンス

Amazon WorkSpaces のユースケース

Amazon WorkSpacesは多くのシナリオでメリットを発揮します



BYOD



合併と買収



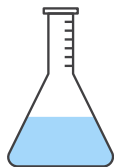
モバイルワーカー



テンポラリーワーカー



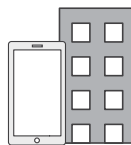
データのセキュア化



開発/テスト



コンプライアンス要件



コールセンター



トレーニングとラボ



デモ

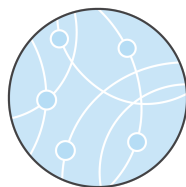
特長: デスクトップ展開をシンプルに



ロジスティクス



ストレージ



ネットワーク



モニタリング



グローバルスケール

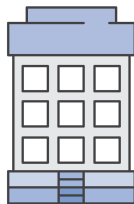


Amazon WorkSpacesは物理と仮想デスクトップ展開をシンプルにします

特長: 既存のツールとの**統合**



Microsoft Active Directory



イントラネット



MFA (Radius)

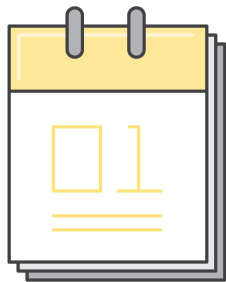


SCCM



Amazon WorkSpacesはオンプレミスのツールやネットワークと容易に統合が可能です

特長: 柔軟な課金オプション



Monthly

主な用途

- フルタイムの従業員
- AWS料金のシンプルさ
- いつでもアクセス
- 日常業務



Hourly

主な用途

- パートタイムの従業員
- AWS料金の最適化
- クイックにアクセス
- 一時的なタスクの実行

CPU、ストレージ、ソフトウェアを選ぶだけ

Value Plus (\$49 USD)

Microsoft Office Pro, Trend Micro,
Utilities bundle

Value (\$34 USD)

- 1 vCPU, 2 GB memory
- 10 GB storage
- Utilities software bundle

Standard Plus (\$62 USD)

Microsoft Office Pro, Trend Micro,
Utilities bundle

Standard (\$47 USD)

- 2 vCPU, 4 GB memory
- 50 GB storage
- Utilities software bundle

Performance Plus (\$93 USD)

Microsoft Office Pro, Trend Micro,
Utilities bundle

Performance (\$78 USD)

- 2 vCPU, 7.5 GB memory
- 100 GB storage
- Utilities software bundle

Amazon WorkSpaces には、ユーティリティとして
Internet Explorer 11, Firefox, 7-Zipが含まれます

多様なデバイスへの対応



- デスクトップ, ラップトップ: Windows, Mac
- タブレット: iOS, Android, Kindle Fire
- ゼロクライアント
- シンククライアント *
- Chrome OS


* ベンダーおよびOSによる

グローバルなカバレッジ
























Connection Health Check サイト


<https://clients.amazonworkspaces.com/Health.html>



Connection Health Check

	Recommended Region 	Asia Pacific (Tokyo)	Asia Pacific (Singapore)	US West (Oregon)	US East (N. Virginia)	Europe (Ireland)	Europe (Frankfurt)	Asia Pacific (Sydney)
Service Availability								
Registration Services 								
Workspace Services 								
Round Trip Time (ms) 	22	58	99	110	150	181	227	
Speed Rating 	FAST	FAST	FAST	ACCEPTABLE	ACCEPTABLE	ACCEPTABLE	ACCEPTABLE	

Check Again

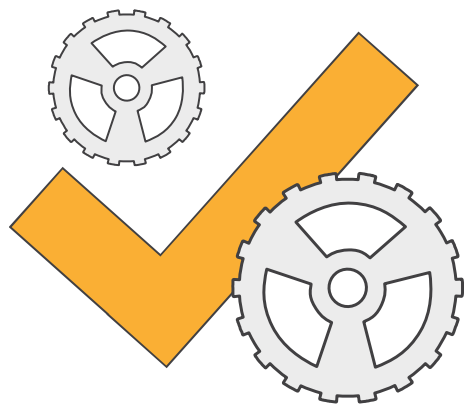
 Some checks were not performed because the required Java plugin is not enabled.

セキュリティと信頼性



- ❏ クライアントデバイスにデータは保存されない
- ❏ パブリックネットワークに接続する際のセキュリティリスクを低減
- ❏ 多要素認証に対応 (MFA)
- ❏ デスクトップのドライブを暗号化
- ❏ ユーザデータは、Amazon S3にバックアップ

シンプルな管理



- ❏ 現在利用中のツールやプロセスによって集中管理
- ❏ Active Directoryとの連携
- ❏ アプリケーションの展開、アップグレード、パッチ、撤去を合理化
- ❏ 迅速に、また簡単にユーザーを他のリージョンに展開可能

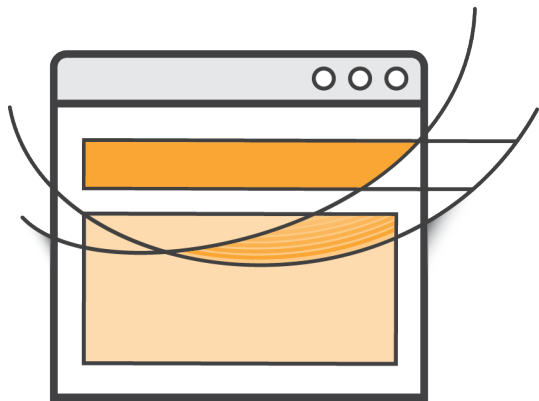
Amazon WorkDocs



Amazon WorkSpaces には Amazon WorkDocs が付帯

- ❏ フルマネージドな、セキュア エンタプライズ ストレージとコラボレーション サービス
- ❏ 強固な管理者制御と監査機能
- ❏ ファイル添付のメールを送ることなく、ドキュメントの共有、コメントの送付が可能
- ❏ Microsoft Office や PDF に対応
- ❏ 50 GB までの利用を付帯、容量の追加も可能

アプリケーション



WorkSpaces Application Manager (Amazon WAM)

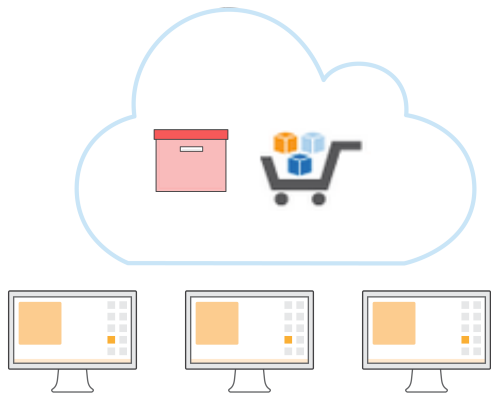
- 📦 アプリケーションを高いスケールで簡単に管理
- 📦 利用の可視化と制御
- 📦 ITの負荷を低減
- 📦 アプリケーションの展開、アップグレード、パッチ、撤去を合理化

デスクトップアプリ向けAWS Marketplace

- 📦 多様なアプリケーションをマーケットプレイスに
- 📦 使った分だけの費用

Amazon WorkSpaces Application Manager (WAM)

Amazon WorkSpaces
Application Manager
(Amazon WAM)



動的アプリ配信 – アプリの展開, トレース,
アップデートを高スケールで

ソフトウェアライセンスを所有しているアプリ
を追加

AWS Marketplace for Desktop Apps からの
サブスクライブ

US-East(N. Virginia)/US-West(Oregon)/
EU(Ireland)/Asia Pacific(Singapore)/Asia
Pacific(Sydney)リージョンにてサービス提供
中

高いスケールでのアプリ管理

 **awsmarketplace**
for Desktop
Apps



自社開発アプリ



市販アプリ
(ライセンス所有)



アプリの
展開



WorkSpaces

アプリケーションカタログの作成



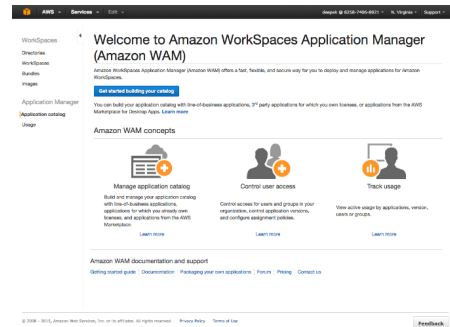
所有するアプリ



WAM Studio を利用
してパッケージ化

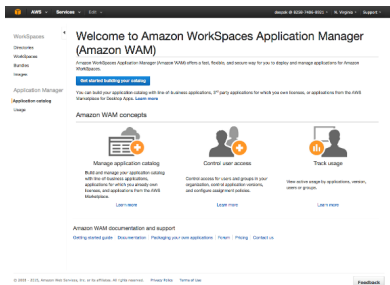


Amazon WAM
Player にて動作確認

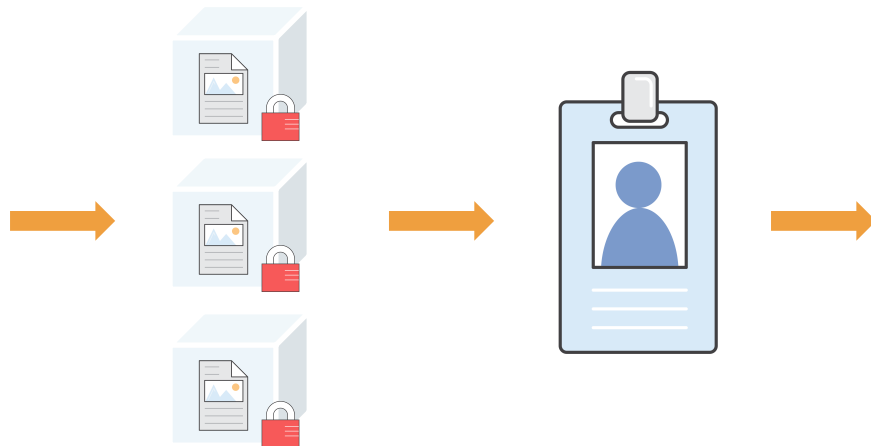


アプリケーションカタログ
にアップロード
(WorkSpaces Console)

カタログからアプリをユーザーに適用



作成したアプリケーションカタログ
(Amazon WAM Console)



アプリを選択

ディレクトリで、
ユーザまたはグループを検索し、アプリ
をアサイン

Amazon WAM
desktop appから、
配信されたアプリに
アクセス

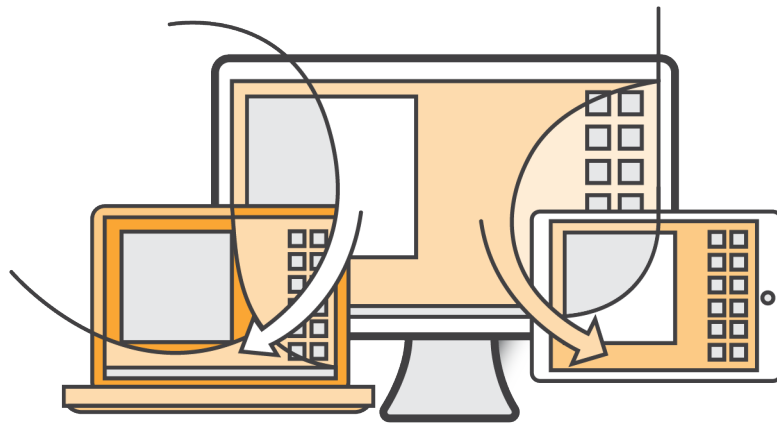
Agenda

- Amazon WorkSpacesとは
- セットアップと管理
- 最新アップデート
- 設計のベストプラクティス

Amazon WorkSpaces を使ってみましょう

簡単に利用開始可能:

1. “Quick Start” を使って評価を開始
2. バンドルを選択
3. ユーザー用の WorkSpaces を起動
4. プロビジョンが完了するとユーザーはメールを受信



Amazon WorkSpacesへの接続



WorkSpacesクライアント

- サポートするプラットフォーム
 - Windows 7/Windows Server 2008以降
 - Mac OS X (10.8.1)以降
 - iPadまたはiPad Retina(iOS 7.0以降)
 - Kindle Fire HDXまたはHD 7/Android 4.2以降のタブレット
 - Chrome OSバージョン45以降のChromebook
- クライアントポート
 - TCP/UDP 4172
 - TCP 443 (HTTPS)
 - 最適なパフォーマンスのためにはRTT 100ms以下を推奨

ネットワークヘルスチェック

- WorkSpacesクライアントにネットワークヘルスチェックの機能を追加
 - ネットワーク接続
 - インターネット接続
 - WorkSpacesと関連する登録サービスへのアクセス
 - TCP/UDP 4172
 - 往復時間



PCoIPゼロクライアント

- AWS Marketplaceから Teradici PCoIP Connection Manager for Amazon WorkSpacesを VPCにデプロイして設定
- ファームウェアバージョン 4.6.0以降のTera 2ゼロクライアントデバイスからPCoIP Connection Managerに接続

The screenshot shows the AWS Marketplace product page for Teradici PCoIP Connection Manager for Amazon WorkSpaces. The page includes a search bar, a product title, a description, a 'Continue' button, and a pricing table.

Teradici PCoIP Connection Manager for Amazon WorkSpaces
Sold by: Teradici | See product video

teradici The Teradici PCoIP Connection Manager is a free software appliance that enables the connection of PCoIP Zero Clients with Amazon WorkSpaces. PCoIP Zero Clients combined with Amazon WorkSpaces provide a simple, secure, easy to manage cloud desktop solution that delivers a seamless user experience. Together they deliver the flexibility to scale your cloud desktop deployment up or down as your business changes. These stateless devices with an average lifespan of 7 years, cost less than traditional PCs or laptops, and consume a fraction of the energy and deliver a high performance desktop experience ... [Read more](#)

Customer Rating Be the first to review this product

Latest Version 1.0.0

Base Operating System Linux/Unix, Ubuntu 12.04.5 LTS

Delivery Method 64-bit Amazon Machine Image (AMI) [\(Learn more\)](#)

Support [See details below](#)

AWS Services Required Amazon EC2, Amazon EBS

Highlights

- Ultra secure
- Easy to manage and deploy
- Rich user experience

Product Description

The Teradici PCoIP Connection Manager is a free software appliance that enables the connection of PCoIP Zero Clients with Amazon WorkSpaces. PCoIP Zero Clients combined with Amazon WorkSpaces provide a simple, secure, easy to manage cloud desktop solution

Continue You will have an opportunity to review your order before launching or being charged.

Pricing Details

For region: **US East (Virginia)**

Hourly Fees
Total hourly fees will vary by instance type and EC2 region.

EC2 Instance Type	EC2 Usage	Software	Total
hs1.xlarge	\$4.60/hr	\$0.00/hr	\$4.60/hr
m3.medium	\$0.07/hr	\$0.00/hr	\$0.07/hr
m3.large	\$0.14/hr	\$0.00/hr	\$0.14/hr
m3.xlarge	\$0.28/hr	\$0.00/hr	\$0.28/hr
r3.xlarge	\$0.56/hr	\$0.00/hr	\$0.56/hr
i2.xlarge	\$0.853/hr	\$0.00/hr	\$0.853/hr
i2.xlarge	\$1.705/hr	\$0.00/hr	\$1.705/hr
i2.4xlarge	\$3.41/hr	\$0.00/hr	\$3.41/hr
i2.8xlarge	\$6.82/hr	\$0.00/hr	\$6.82/hr

オーディオ入力と高DPIデバイス

- オーディオ入力
 - Lync、Skype、WebExなどの一般的なコミュニケーションツールを使用してコールが可能
 - WindowsとMac用のWorkSpacesクライアントをサポート
- 高DPIデバイスのサポート
 - Surface Pro 4やLenovo Yogaのようなデバイスに対応
 - 高DPI（Full HD/Ultra HD/QHD+）ディスプレイにあわせて自動的にスケール

ルートボリュームの拡大

- ルートボリューム（C:）の容量が従来の60GBから80GBに拡大
 - 新規のWorkSpacesは自動的にルートボリュームが80GBで作成される
 - 既存のWorkSpacesはRebuildすることでルートボリュームを80GBに拡張可能

ドライブの暗号化

- WorkSpacesのボリュームを暗号化
 - AES-256 bit 暗号化
 - AWS KMS サービスと統合
 - カスタマーのKMS キーによる暗号化
 - キー 1 つあたり、30台のWorkSpacesを暗号化可能
 - CドライブおよびDドライブに対応
 - パフォーマンスへの影響なし
- 課金
 - Amazon WorkSpaces側には追加料金なし
 - KMSキーは課金
 - 10,000 リクエストあたり、\$0.03



ユーザーデータのバックアップ

- ユーザーボリューム（D:）は12時間おきにバックアップされる
- WorkSpaceに障害が発生した場合、バックアップからボリュームを復旧
- Amazon WorkDocs Syncが有効になっている場合、同期を選択したフォルダは継続的にバックアップされる

Amazon WorkDocs Sync

- デスクトップのフォルダをAmazon WorkDocsサービスと同期
 - ユーザーあたり50GB
 - 管理者により有効・無効化することが可能
- Amazon WorkDocs Syncアプリケーションを別途導入して実行



WorkSpacesバンドルの管理

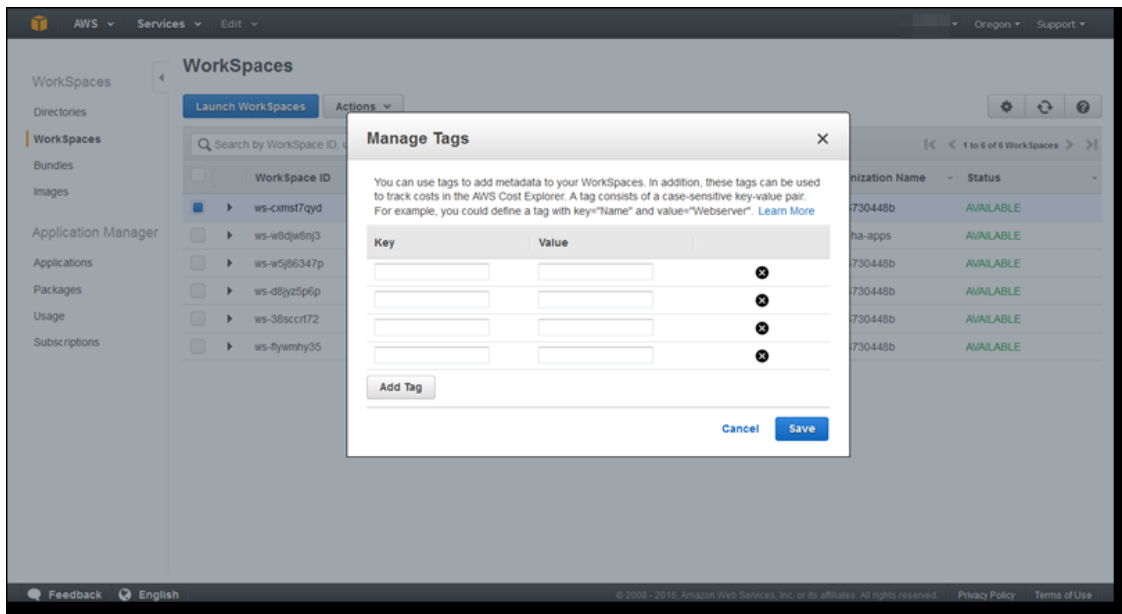
- カスタムイメージを作成してアプリケーションをインストール済みのカスタムバンドルを利用可能
- 要件
 - インストールするアプリケーションがSysprepと互換性がある
 - Workspaceのユーザープロファイルを削除しない
 - ユーザープロファイルの合計サイズが10GB未満
 - ドメインユーザー認証を利用するサービスが存在しない（SQL Server Expressなど）

イメージ作成のベストプラクティス

- Cドライブにアプリケーションをインストールするために十分な容量があること
- OSとアプリケーションの最新の更新プログラムやパッチをすべてインストールする
- 必要のないキャッシュされたデータをWorkSpaceから削除する
 - ブラウザの履歴、キャッシュファイル、ブラウザのCookieなど
- イメージを識別しやすくなるためにイメージ名に日付やバージョンなどをふくめて管理する

WorkSpacesのタグ付け

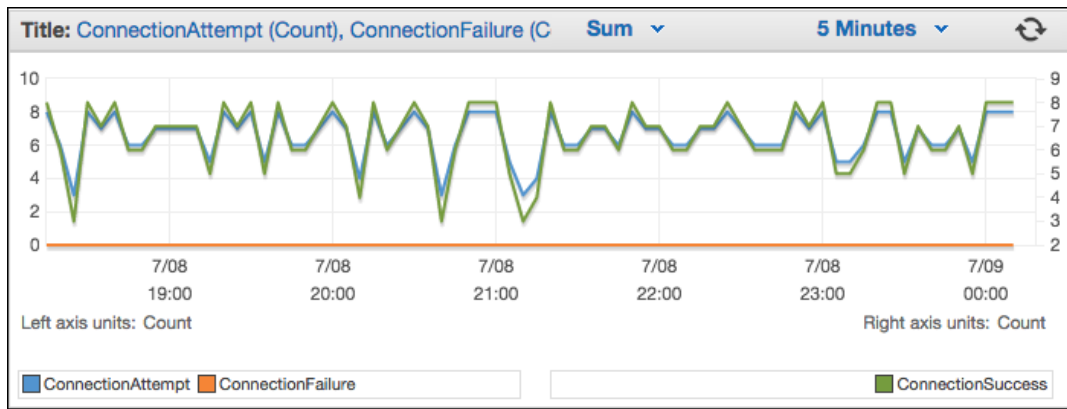
- それぞれWorkSpacesに50個までのタグ（Key-Value）をつけて管理することが可能に



CloudWatchメトリックス

CloudWatchコンソールまたはCLI、APIを使用してモニタリングおよびアラートの設定が可能

- 以下のようなメトリックスを取得可能
 - Available
 - Unhealthy
 - ConnectionAttempt
 - ConnectionSuccess
 - ConnectionFailure
 - SessionLaunchTime
 - InSessionLatency
 - SessionDisconnect
 - UserConnected
 - Stopped
 - Maintenance



Amazon WorkSpaces API

- AWS SDKやCLI、PowerShellからWorkSpacesの作成・表示やメンテナンスが実行可能
 - オペレーションの自動化
 - ディザスタリカバリイメージの展開
- AWS CloudTrailによるロギングをサポート



Amazon WorkSpacesの展開

*blackbelt_demo_user*というユーザーに*Performance Bundle*の*WorkSpaces*を作成

```
New-WKSWorkspace -workspace @{"BundleID" = "wsb-  
b0s22j3d7"; "DirectoryId" = "d-92673ef59b";  
"UserName" = "blackbelt_demo_user"}
```

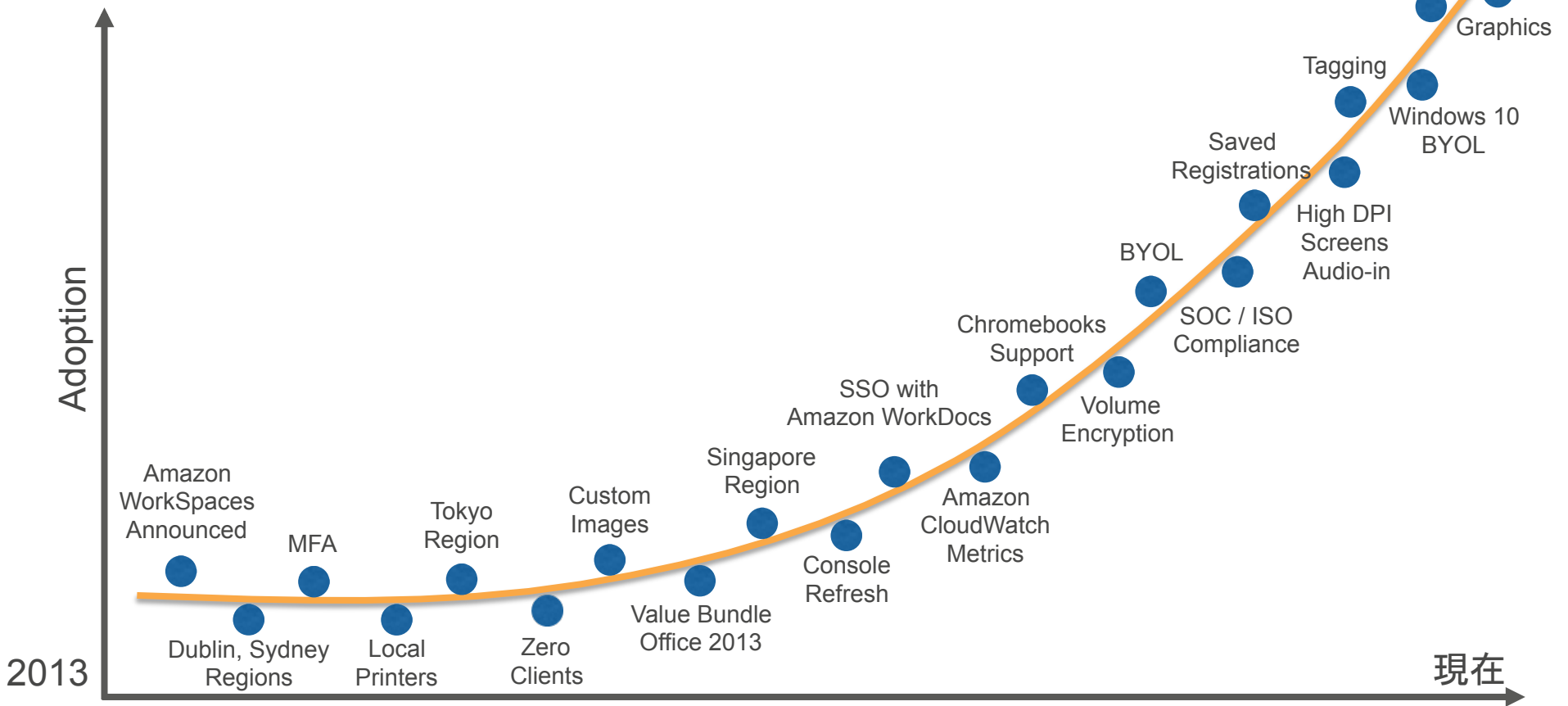
*UserName = blackbelt_demo_user*の*WorkSpaceId*を取得

```
Get-WKSWorkspaces | select UserName, BundleId,  
WorkspaceId, DirectoryId | where UserName -eq  
'blackbelt_demo_user'
```

Agenda

- Amazon WorkSpacesとは
- セットアップと管理
- 最新アップデート
- 設計のベストプラクティス

イノベーション: Amazon WorkSpaces



最新アップデート (過去 6ヶ月)

- **Windows 10 BYOL Amazon WorkSpaces** - Windows 10のライセンスを持ち込んで利用可能
- **Hourly WorkSpaces** - 時間課金での利用、ユーザーが切断状態のときに自動的にストップ
- **グローバル展開** - フランクフルト
- **Graphics Bundle** - 3D、CAD/CAMアプリケーションのためのGPUが有効なAmazon WorkSpaces
- **Web Access for Amazon WorkSpaces** - Webブラウザ (Firefox/Chrome)からのアクセス
- **Windows 10 WorkSpaces** - Windows 10 (Server 2016) WorkSpacesのサポート

Windows 10 BYOL WorkSpaces

- **Windows 7/10のライセンスが利用可能**
 - ライセンスコストの削減
 - 共有のユーザエクスペリエンス
 - カスタムイメージの管理を改善
 - MS OfficeのBYOLも可能
- **価格と要件**
 - すべてのリージョンで、バンドル価格を \$4/月 削減
 - 200台の利用から



BYOLイメージの前提条件

- Windows 7またはWindows 10 Enterprise/Professional 64bit
- Key Management Server (KMS) によってアクティベートされていること
- 主な表示言語をEnglish(US)に設定
- OS標準以外のソフトウェアをインストールしない
- WorkSpaces_BYOLという管理者アカウントを作成
- OVA形式で80GB以下のシングルボリューム

Hourly WorkSpaces

WorkSpaces Configuration

Running Mode

Choose how you will run and pay for your WorkSpaces. Learn more [here](#).

AlwaysOn
Billed monthly. Instant access to an always running WorkSpace.

Auto Stop
Billed by the hour. WorkSpaces start automatically when you login, and stop when no longer being used.
Auto Stop Time (hours)

Note: When possible AutoStop will snapshot the state of the desktop to the root volume of the WorkSpace. When a user next logs into their WorkSpace it is resumed and all open documents and running programs return to their previous state. To further enhance the security of your WorkSpaces we recommend you encrypt all storage volumes (see below).

Encryption

To further enhance the security of your WorkSpaces we recommend you encrypt all storage volumes. To configure volume encryption you need to use KMS keys in your account. You may use the [IAM console](#) to create additional KMS keys. To learn more about encryption on WorkSpaces, please see our documentation [here](#).

Root Volume (C: Drive) Encryption

User Volume (D: Drive) Encryption

Encryption Key [Refresh](#)

- Running Mode
 - Always On
 - Auto Stop

Running ModeをAuto Stopにすると、時間課金モデルに変更される

実行モード

- AlwaysOn

- 月額固定料金でWorkSpacesを無制限に利用可能
- プライマリのデスクトップでのフルタイム利用に最適

- AutoStop

- WorkSpacesの利用に対して時間単位で料金が発生
- セッション切断後に[AutoStop Time(Hours)]で設定した時間が経過すると停止するが、アプリとデータの状態は保管される

実行モードの切り替え

The screenshot shows the AWS WorkSpaces console interface. The top navigation bar includes 'AWS', 'サービス', and '編集'. The user is identified as 'DAISUKE SAWADA' in the 'オレゴン' region, with a 'サポート' link. The left sidebar lists navigation options: WorkSpaces, Directories, WorkSpaces (selected), Bundles, Images, Application Manager, Applications, Packages, Usage, and Subscriptions. The main content area is titled 'WorkSpaces' and features a 'Launch WorkSpaces' button and an 'Actions' dropdown menu. The 'Actions' menu is open, displaying options: Edit User, Invite User, Reboot WorkSpaces, Start WorkSpaces, Stop WorkSpaces, Rebuild WorkSpace, Remove WorkSpaces, Create Image, **Modify Running Mode Properties** (highlighted with a yellow border), and Manage Tags. An orange arrow points from the 'Modify Running Mode Properties' option to the table below. The table lists five WorkSpaces, all with a status of 'STOPPED' and a running mode of 'AutoStop'. The columns are: Workspace ID, Name, Volume Encryption, Organization Name, Running Mode, and Status.

Workspace ID	Name	Volume Encryption	Organization Name	Running Mode	Status
ws-ghfys1xj3	...nce Plus with Office 2013	Disabled	zocalo-demo-j	AutoStop	STOPPED
ws-xq7cdszb	...bundle	Disabled	zocalo-demo-j	AutoStop	STOPPED
ws-ffcs82gfc	... Plus with Office 2013	Disabled	zocalo-demo-j	AutoStop	STOPPED
ws-9witkw2l8	... Plus with Office 2013	Disabled	zocalo-demo-j	AutoStop	STOPPED
ws-wk1kfnfcb	...s with Office 2013	Disabled	zocalo-demo-j	AutoStop	STOPPED

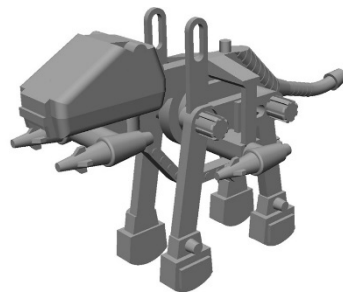
WorkSpacesをプロビジョン後でも、実行モードはいつでも
変更可能

メンテナンスモード

- Auto Stopに設定したWorkSpacesにメンテナンスモードを有効にすると自動的に更新されるよう設定することが可能
- 月1回、重要なサービス、セキュリティ、Windows更新プログラムをアップデートするため起動される
- メンテナンス中のWorkSpacesにはログオンすることができないため注意

Graphics Bundle

- GPUを搭載したWorkSpacesによりグラフィック処理が高速化
 - GPUを搭載することで、3D CAD等の利用において、画面が滑らかに動き、細かな場所まで正確に描画されるなど、グラフィック処理が改善
 - 仮想デスクトップ環境でもGPUによる恩恵を受けることができる
- ユースケース
 - CAD/CAM/CAE Workloads
 - 3D エンジニアリング
 - ビジュアルデザイン
 - アニメーション



Graphics Bundle スペック

- GPU
 - NVIDIA GRID K520
 - GPUあたり 1,536 CUDA cores, 4GiBグラフィックメモリ
- CPU
 - 8vCPU
- メモリ
 - 15 GiB
- ディスク
 - 100GB ルートボリューム
 - 100GB ユーザーボリューム

Graphics WorkSpaces 価格 (東京リージョン)

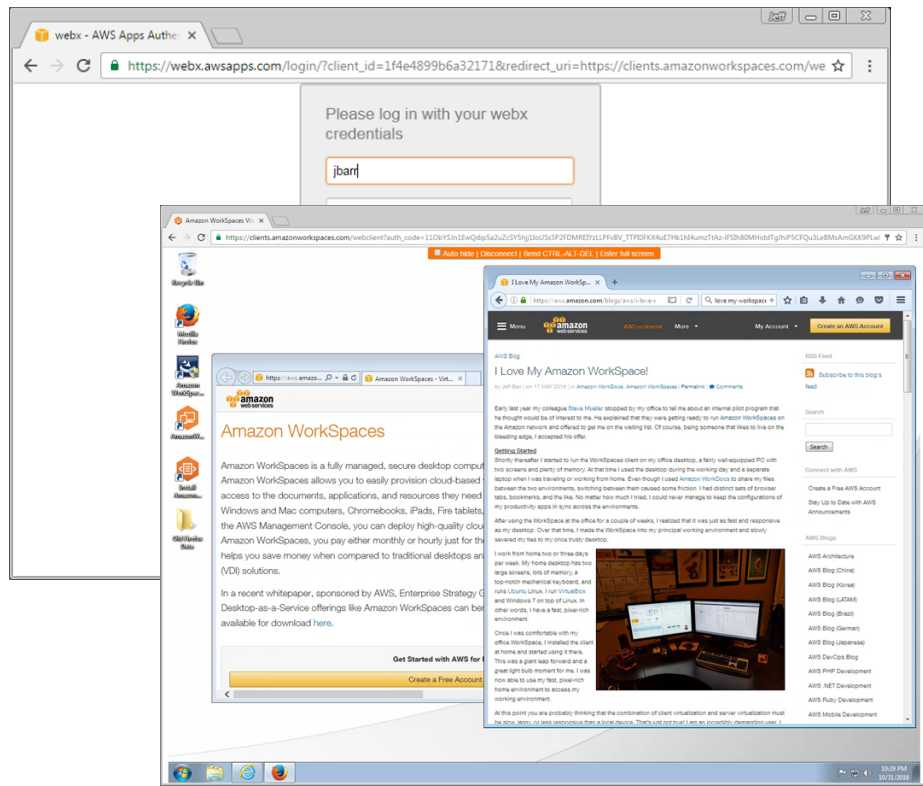
ハードウェアオプション

バンドル	ハードウェア構成	月額料金*	時間料金**
バリュー	1 vCPU、2 GiB メモリ、10 GB ユーザーストレージ	34 USD	10.00 USD/月 + 0.30 USD/時
スタンダード	2 vCPU、4 GiB メモリ、50 GB ユーザーストレージ	47 USD	14.00 USD/月 + 0.40 USD/時
パフォーマンス	2 vCPU、7.5 GiB メモリ、100 GB ユーザーストレージ	78 USD	19.00 USD/月 + 0.74 USD/時
グラフィックス	8 vCPU、15 GiB メモリ、1 GPU、4 GiB ビデオメモリ、100 GB ユーザーストレージ	-	30.00 USD/月 + 2.41 USD/時

※月額課金プランおよびBYOLも個別に対応可能

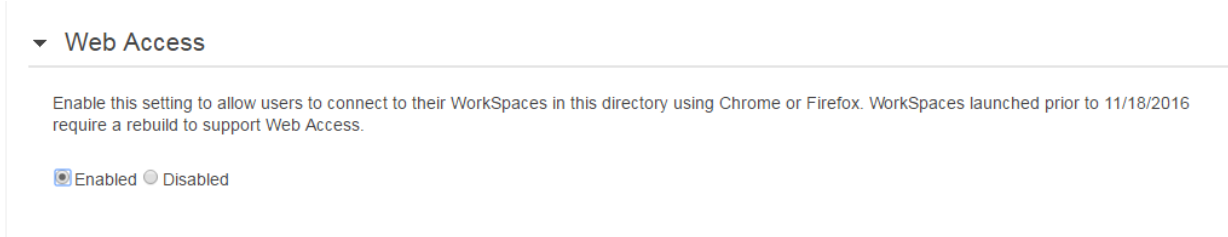
Web Access for Amazon WorkSpaces

- Windows/Mac/Linuxを実行するChromeまたはFirefoxのWebブラウザからWorkSpacesにアクセスが可能に
- インターネットにアクセス可能なネットワークに接続されたコンピュータからアクセス可能
- English (US)のValue/Standard/PerformanceおよびPlusバンドルに対応



Web Accessの有効化

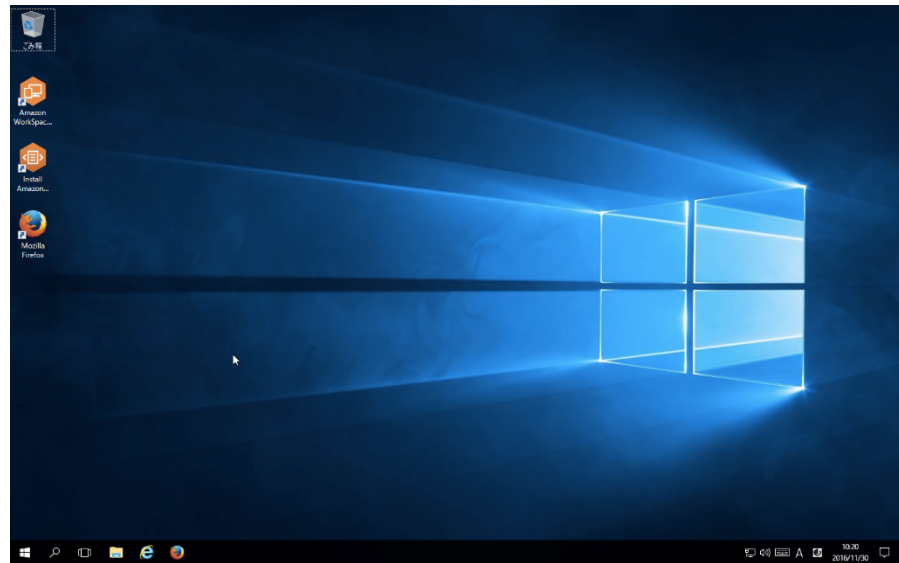
- Update Directory DetailsでWeb AccessをEnableに設定する



- 2016/11/18以前に起動したWorkSpacesは再構築が必要
- English (US)のWorkSpacesのみがサポートされるため、日本語環境が必要な場合は言語パックをインストールする

Windows 10デスクトップエクスペリエンス

- Windows 10のデスクトップ環境をWindows Server 2016ベースで提供
- PlusバンドルではOffice 2016が利用可能
- English(US)のみ
- GraphicsおよびWeb Accessは現在利用できない

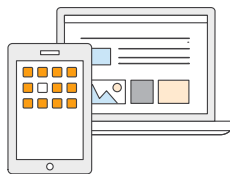


Agenda

- Amazon WorkSpacesとは
- セットアップと管理
- 最新アップデート
- 設計のベストプラクティス

想定するシナリオ

- 既存のAWSのお客様
- オンプレミスとクラウド上のアプリによるハイブリッドアーキテクチャ
- 既存のActive Directoryを使用した認証
- AWS Direct Connectを利用している
- 2,000+ ユーザー



BYOD



合併と買収

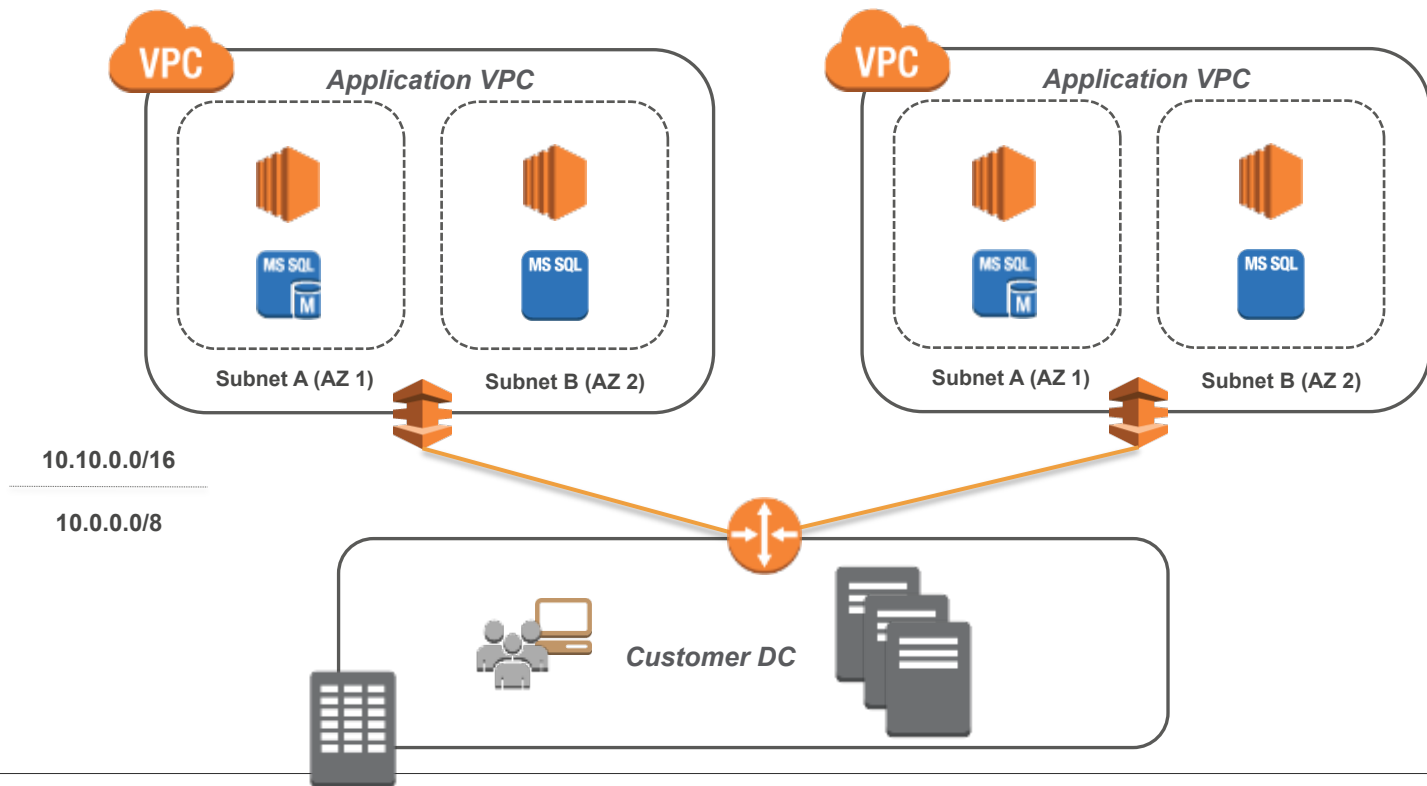


モバイルワーカー

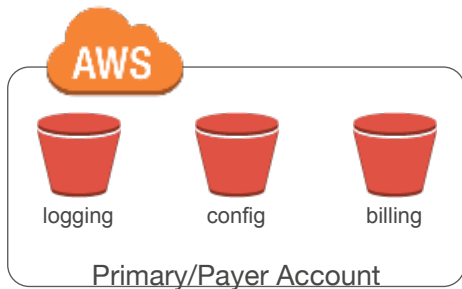


データのセキュア化

既存のアーキテクチャ例

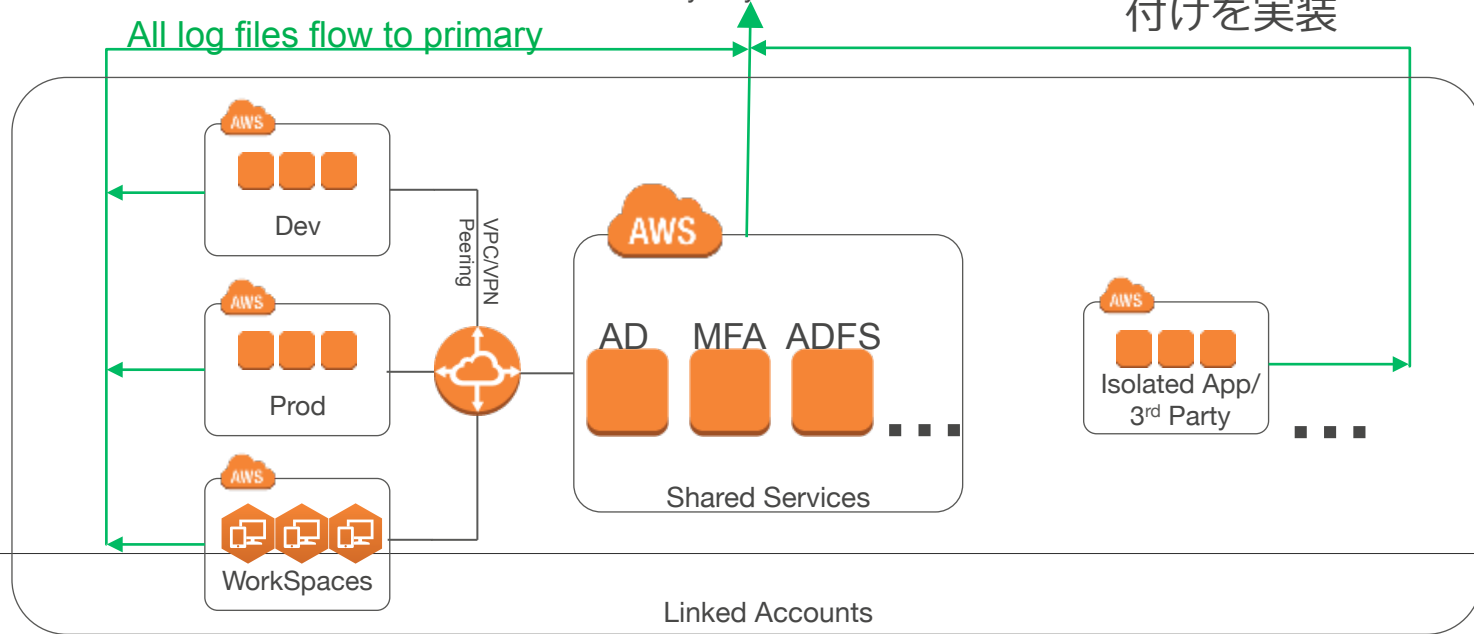


AWSアカウントの構造



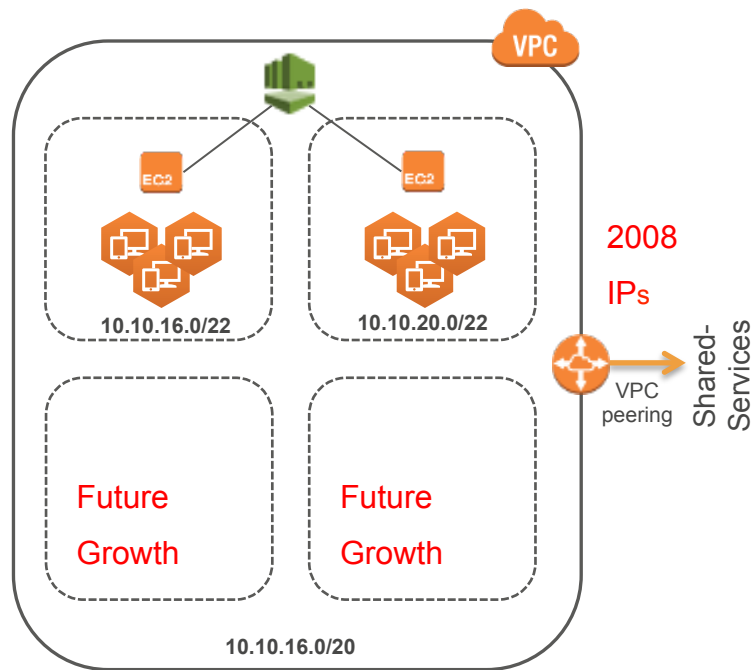
主要な推奨事項

- Payer/Linked Accountの構造
- Payer Accountでのロギング
- WorkSpaces用のアカウントを分離
- すべてのアカウントで一貫したタグ付けを実装



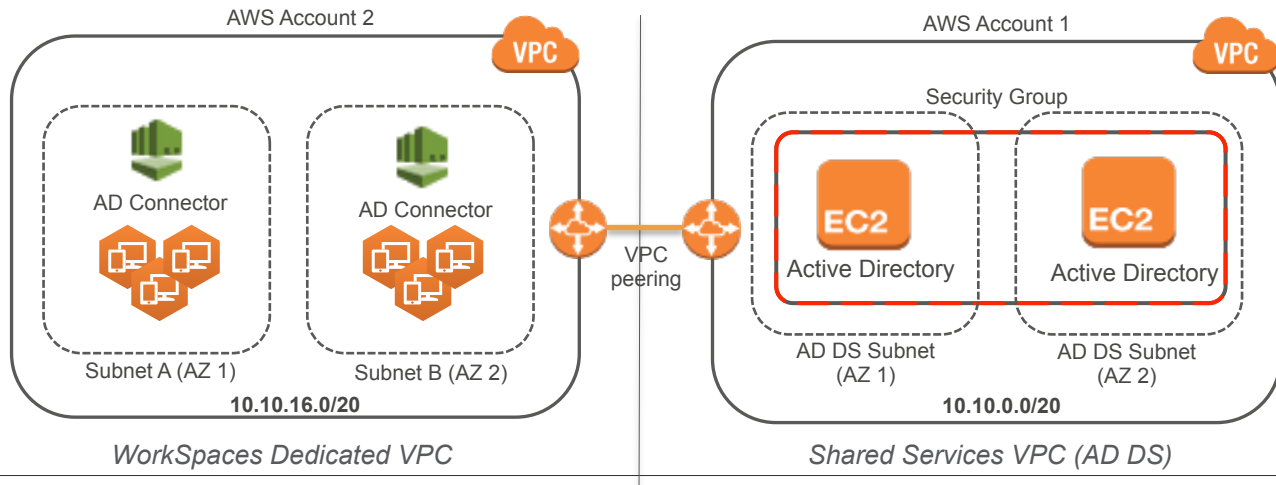
WorkSpaces VPC

- WorkSpaces用の**最小**2つのサブネット
- IP枯渇を避ける
- イニシャルで2,000台のWorkSpacesと成長の余地
- お客様がAWSで使用するために10.10.0.0/16を割り当てている
- 共有サービス用のVPC（ディレクトリ、DNS）の使用



ディレクトリ展開のコンセプト

- Active DirectoryをEC2インスタンス上のAWSに拡張
- AD Connectorを使用して、WorkSpaces認証サービスからの認証要求をプロキシ
- クロスアカウントのVPCピアリングを使用して通信



ディレクトリのコンポーネント

Active Directory on EC2

- 共有サービス用VPCに展開
- お客様自身による管理
- EC2インスタンス上にデプロイ
- お客様のディレクトリをクラウドに拡張するために使用



Active
Directory

AWS Directory Service

- WorkSpaces VPC上にAD Connectorを展開
- AD Connectorは認証のためのディレクトリゲートウェイ
- 2つのサイズ: Small (500)/ Large (5000)



AWS Directory
Service

ネットワーク要件

- ドメイン コントローラーと疎通を行うために、以下のポートの開放が必要
 - TCP/UDP 53 - DNS
 - TCP/UDP 88 - Kerberos 認証
 - TCP 135 - RPC
 - TCP/UDP 389 - LDAP
 - TCP/UDP 445 - SMB
 - TCP 464 - Kerberos パスワードの変更/設定
 - TCP 636 - LDAPS (LDAP over TLS/SSL)
 - TCP 1024-65535 - RPC 用ダイナミックポート
 - UDP 123 - NTP
 - UDP 137-139 - Netlogon
 - UDP 464 - Kerberos パスワードの変更/設定
- DirectoryServicePortTest テストアプリケーションを利用して接続の確認が可能
 - `DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp "53,88,135,389,445,464,636,3268,3269,5722,9389" -udp "53,88,123,138,389,445,464"`
 - <http://docs.aws.amazon.com/directoryservice/latest/adminguide/samples/DirectoryServicePortTest.zip>

グループポリシーによる制御

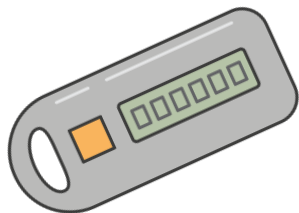
- グループポリシー管理テンプレートをインストールすることによりポリシー設定を変更可能
 - C:\Program Files (x86)\Teradici\PCoIP Agent\configuration\pcoip.adm
- 以下のような項目がグループポリシーから制御可能
 - ローカルプリンターのサポート
 - クリップボードのリダイレクト
 - セッションレジュームのタイムアウト
 - PCoIPストリーミングの暗号強度



ローカルプリンターへの印刷

- WorkSpacesからWindowsまたはMacに接続されているローカルおよびネットワークプリンターに印刷することが可能
 - ローカルプリンターは自動的に認識される(Local - <workspace username>.<directory name>.<client computer name>)
 - Windows Server 2008 R2用のドライバをインストールする必要がある
- その他の印刷方法
 - Active Directoryに登録されたネットワークプリンタ
 - Google Cloud Printなどのクラウドプリント

MFAの設定



▼ Multi-Factor Authentication

RADIUS status None

Enable Multi-Factor Authentication

RADIUS server IP
address(es)

10.10.0.10,10.10.0.150



Port

1812

Shared secret code

••••••



Confirm shared secret
code

••••••



Protocol

PAP



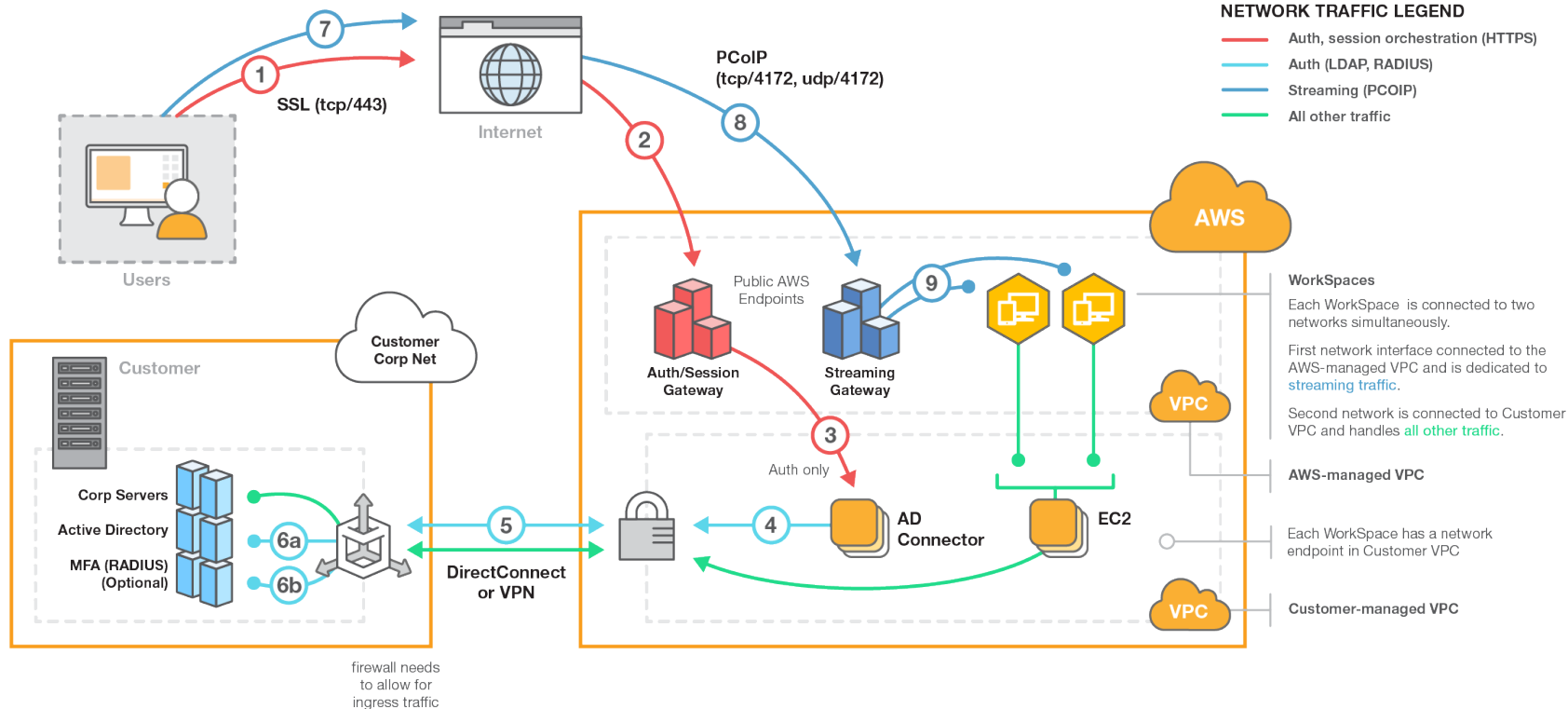
Server timeout (in
seconds)

20

Max retries

3

ネットワーク構成 - オンプレミスからの接続

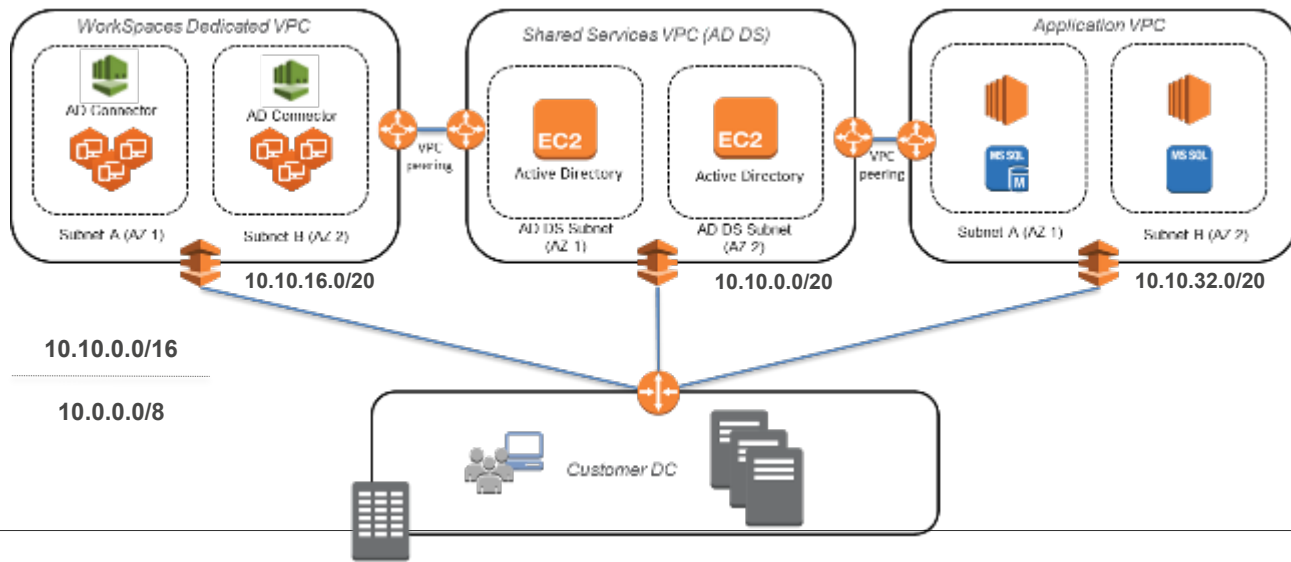


PCoIPゲートウェイのIPアドレス範囲

リージョン	PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲
米国東部 (バージニア北部)	52.23.61.0 – 52.23.62.255
米国西部 (オレゴン)	54.244.46.0 – 54.244.47.255
欧州 (アイルランド)	52.19.124.0 – 52.19.125.255
アジアパシフィック (シンガポール)	52.76.127.0 – 52.76.127.255
アジアパシフィック (シドニー)	54.153.254.0 – 54.153.254.255
アジアパシフィック (東京)	54.250.251.0 – 54.250.251.255

最終的なアーキテクチャ構成例

- Amazon WorkSpaces用の専有 AWSアカウント
- WorkSpaces用の分離したVPC + クロスアカウントピアリング
- 共有サービスVPC (Active Directory)



まとめ

- Amazon WorkSpacesはマネージド型の仮想デスクトップコンピューティングサービス
- 最新のアップデートにより時間課金、Graphic Bundle、Web Accessなどに対応
- 大規模展開には最適なアーキテクチャ設計が必要

参考資料

- Amazon WorkSpaces Administration Guide
 - http://docs.aws.amazon.com/workspaces/latest/adminguide/what_is.html
- Amazon WorkSpacesのよくある質問
 - <http://aws.amazon.com/jp/workspaces/faqs/>
- 料金表
 - <http://aws.amazon.com/jp/glacier/pricing/>

オンラインセミナー資料の配置場所

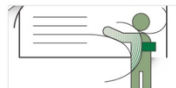
- AWS クラウドサービス活用資料集

- 「AWS 資料」で検索

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

日本語資料のカテゴリー一覧

本資料集では、この利便性を皆様にご利用いただけるよう、トレーニング、ソリューション/事例、プロダクト別、セキュリティ・コンプライアンス、その他という5つのカテゴリーで資料をご用意いたしております。



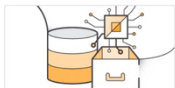
トレーニング資料

はじめてAWSをご利用いただくお客様向けに、AWS の概要、アカウント作成に関するご案内いたします。



ソリューション・事例紹介資料

実際に他のお客様がどのようにAWS をご利用いただいているかをご覧いただける参考資料をご用意いただけます。



製品・サービス別資料

無料オンラインセミナー「AWS Black Belt Tech Webinar」や各種セミナーで紹介された、ソリューションアーキテクトによる各サービスの解説資料をご用意いただけます。

- 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/>

公式Twitter/Facebook AWSの最新情報をお届けします



@awscloud_jp



検索



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！

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/>

お問い合わせ	<h2>日本担当チームへのお問い合わせ</h2>
日本担当チームへのお問い合わせ >	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、以下のフォームよりお気軽にご相談ください。平日営業時間内に日本オフィス担当者よりご連絡させていただきます。
関連リンク フォーラム	※ご請求金額またはアカウントに関する質問は こちらからお問い合わせください 。 ※Amazon.com または Kindle のサポートにお問い合わせは こちらからお問い合わせください 。
	アスタリスク (*) は必須情報となります。 姓* <input type="text"/> 名* <input type="text"/>

※「AWS お問い合わせ」で検索してください

