AWS Summit

Tokyo

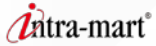
amazon web services

■Gold Sponsors

■Global Sponsors

■Silver Sponsors

■Bronze Sponsors

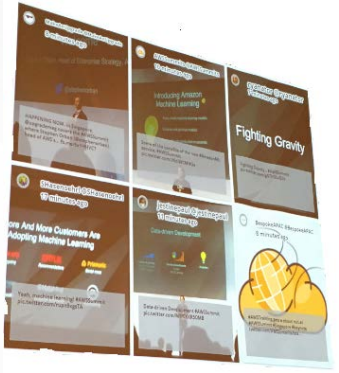


■Global Tech Sponsors

■Logo Sponsors

amazon web services

ハッシュタグ #AWSSummit
で、**皆さんのツイート**が展示エリア
の**大画面に表示されます**



公式アカウント@awscloud_jp
を**フォローすると**、ロゴ入り
コースターを**プレゼント**

【コースター配布場所】
メイン展示会場、メイン会場1F受付、デベロッパーカンファレンス会場

amazon web services

Enterprise Applications Deep Dive
(Amazon WorkSpaces/WorkDocs/WorkMail)

アマゾンデータサービスジャパン株式会社
ストラテジックソリューション部ソリューションアーキテクト
渡邉 源太

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ストラテジックソリューション部（エンタープライズ担当）
  - 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

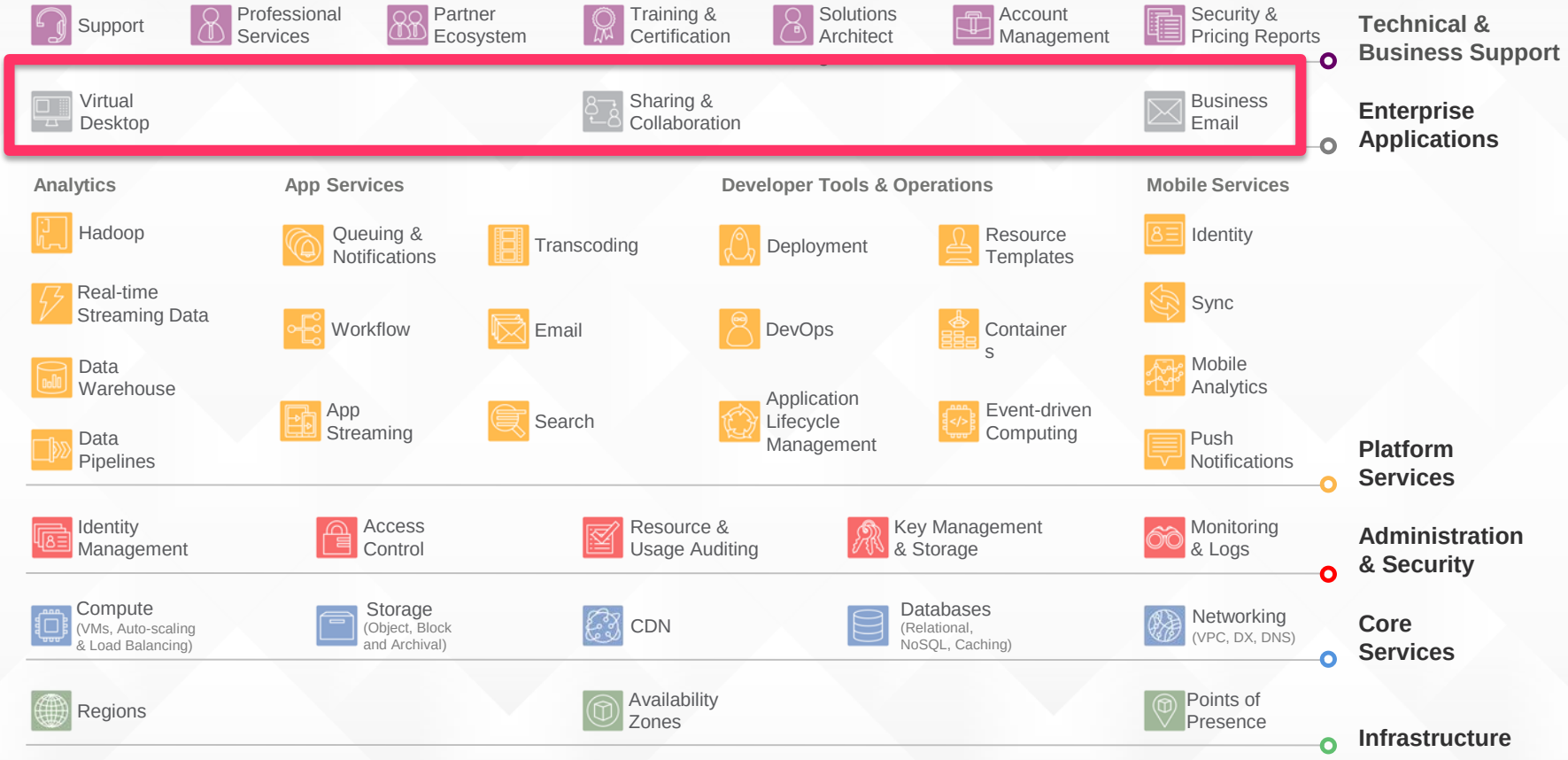
アジェンダ

- AWSのエンタープライズアプリケーション
- AWS Directory Service
- Amazon WorkSpaces
- Amazon WorkDocs
- Amazon WorkMail

AWSのエンタープライズアプリケーション

amazon web services

AWSが提供する40以上のサービス



http://aws.amazon.com/jp/products/

amazon web services

エンタープライズアプリケーション

仮想デスクトップサービス

amazonWorkSpaces

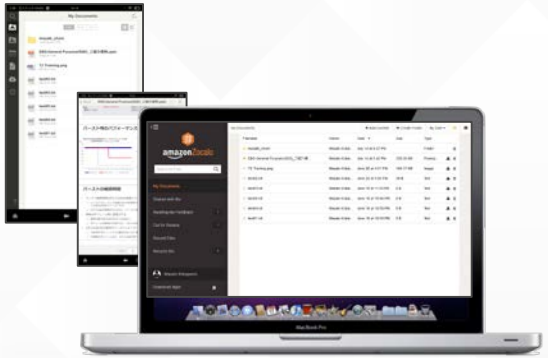
マネージド型電子メール・カレンダー

amazonWorkMail

Preview

企業向けファイル共有サービス

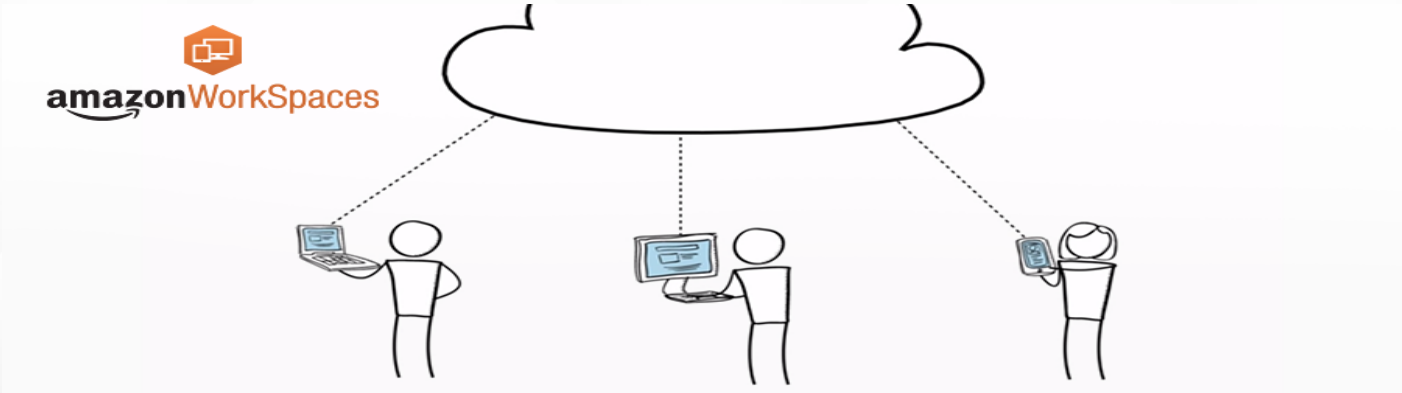
amazonWorkDocs



amazon web services

Amazon WorkSpaces

- クラウドで動作する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
  - Windows/Mac/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



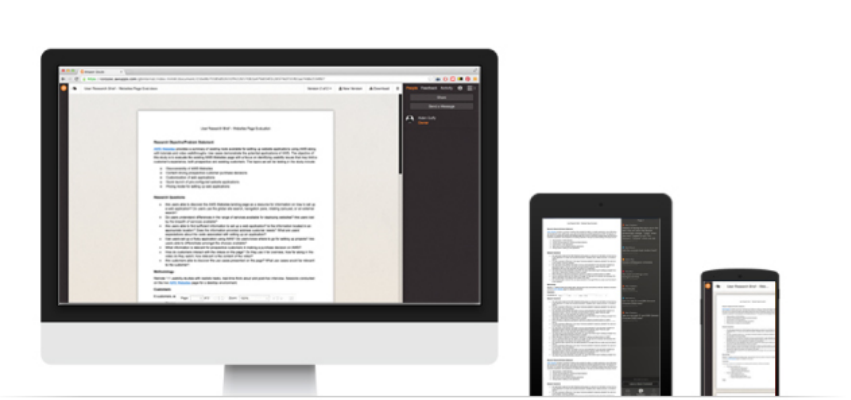
Amazon WorkSpacesへの接続

amazon web services

Amazon WorkDocs

amazonWorkDocs

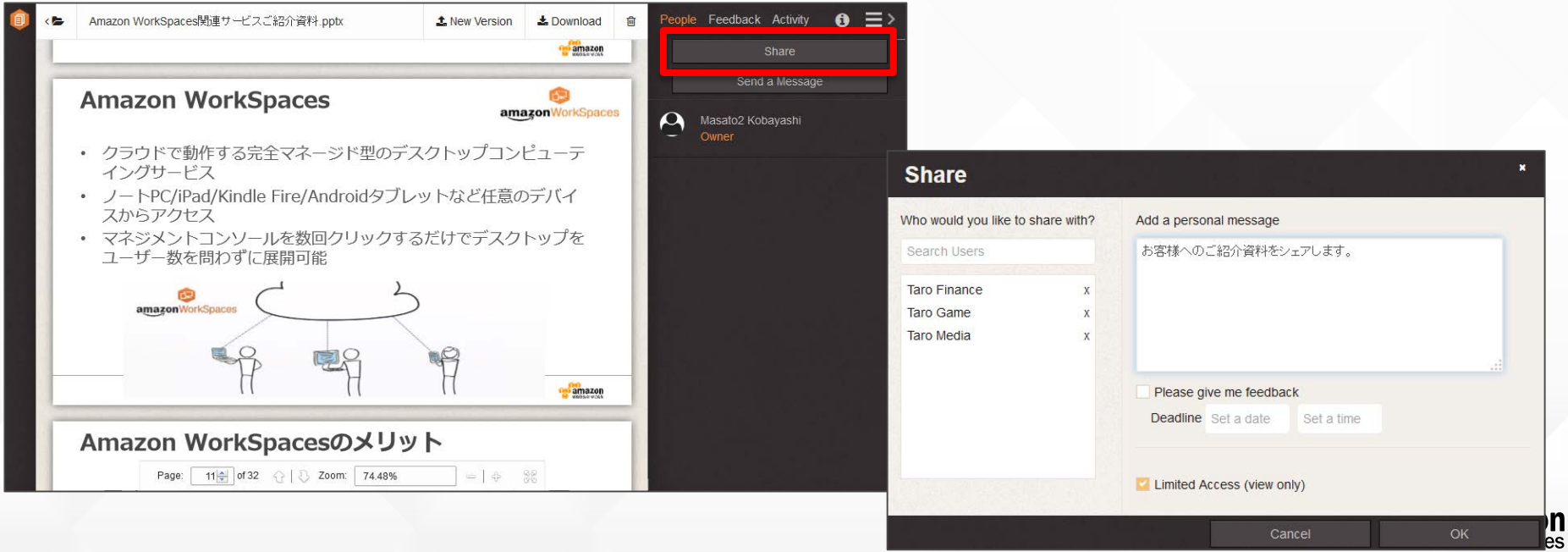
- フルマネージド型のセキュアなエンタープライズストレージおよび共有サービス
  - ユーザーの生産性を高める強力な管理制御とフィードバック機能
  - ユーザーはWindows、Mac、iOS/Androidタブレットなどのデバイスからどこにいてもアクセスが可能



amazon web services

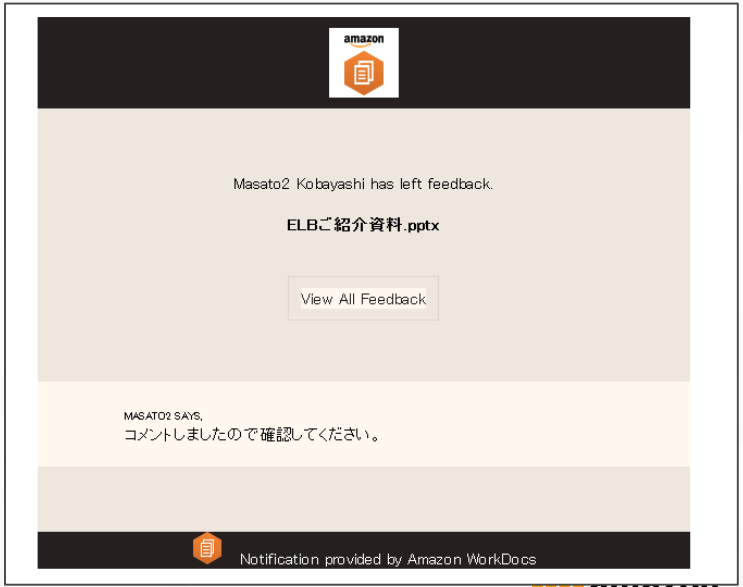
ドキュメントのプレビューと共有

- 主要な形式のファイルについてはWebUIで直接内容を閲覧できる
- 共有メニューから他ユーザに対する権限（読み取りのみ、読み書き）を設定する。権限付与されたユーザにはメールで通知される



フィードバック機能

- 共有されたドキュメントにはコメントやメッセージで相互にフィードバックを行える。対象となる箇所をハイライトすることも可能
- コメントが投稿されるとメールによる通知が行われる



Amazon WorkMail（プレビュー）

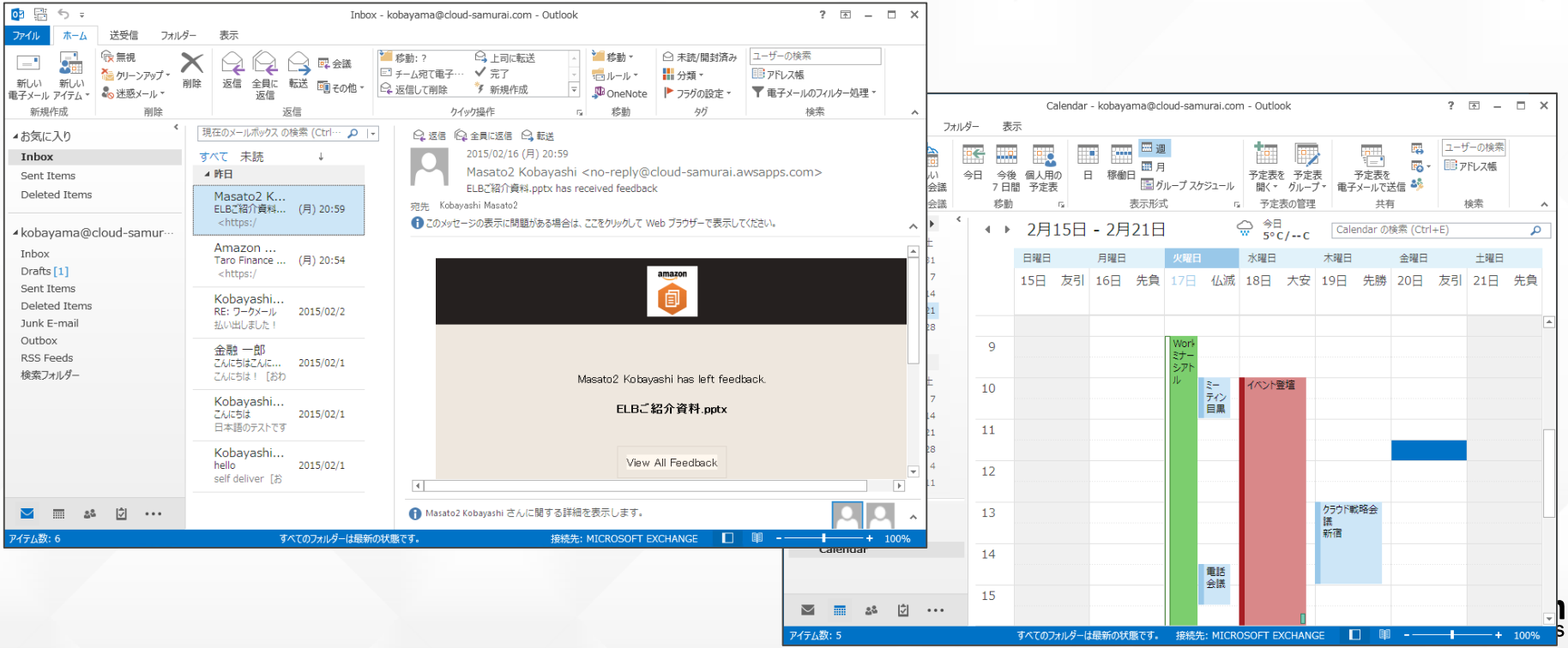
amazonWorkMail

- セキュリティにすぐれたマネージド型の企業向けEメールおよびカレンダーサービス
  - Microsoft Outlook、Webブラウザ、iOS/Androidネイティブの Eメールアプリケーションからのアクセス
  - データを暗号化するためのキーとデータを保存する場所を管理することが可能

amazon web services

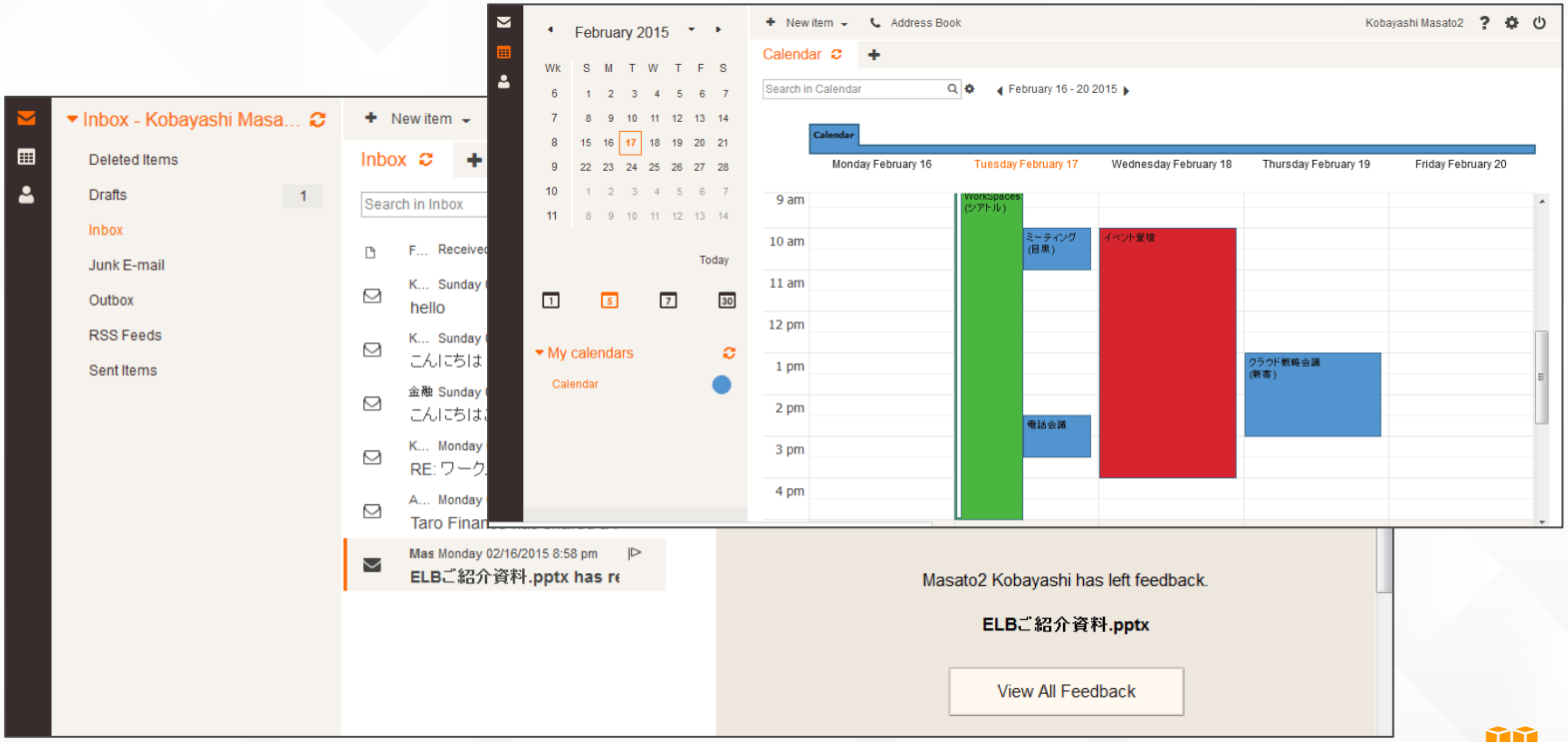
Outlookとの互換性

- WindowsおよびMac OS XのMicrosoft Outlookをネイティブでサポート

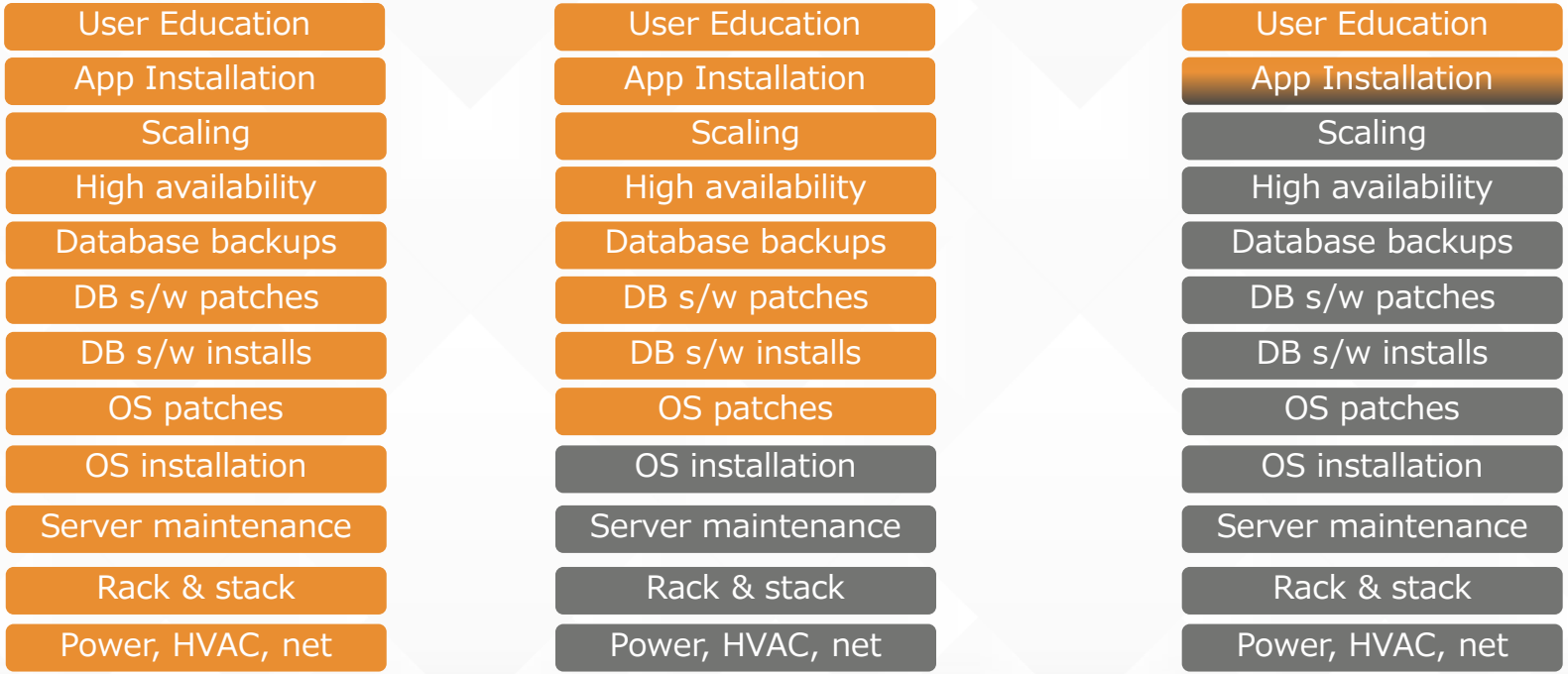


Webクライアントによるアクセス

- WebブラウザでもEメールとカレンダーにアクセス可能



マネージドサービスの利点



amazon web services

さまざまなデバイスからのアクセス

- iOS
- Kindle Fire HDX
- Android
- Windows
- Mac OS X
- PCoIPゼロクライアント

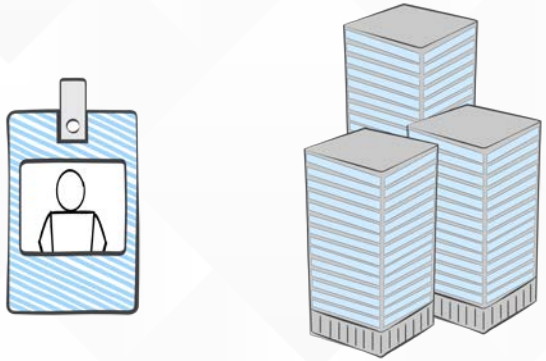
高いセキュリティ

- PCoIPプロトコルによるストリーミング
- 多要素認証（MFA）

- すべてのデータを暗号化して保存
- CloudTrailによる監査ログの取得

- AWS Key Management Service（KMS） による鍵管理
- データ保管場所の選択が可能

Active Directoryとの統合



- AWS Directory Service
  - ユーザー: 既存のエンタープライズの認証を利用
  - IT管理者: 通常のデスクトップのようにワークスペースをコントロール

AWS Directory Service

amazon web services

AWS Directory Service

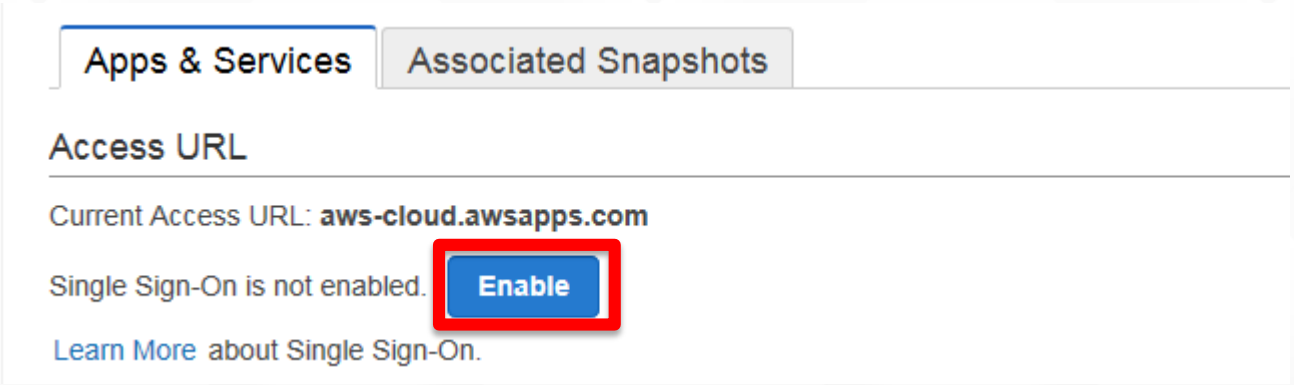
- フルマネージド型のディレクトリサービス
  - AWS上のスタンドアロンのディレクトリを新規に作成
  - 既存のActive Directory認証を利用して：
    - AWSアプリケーションへのアクセス(Amazon WorkSpaces, WorkDocs, WorkMail)
    - IAMロールによるAWS Management Consoleへのアクセス

ディレクトリタイプの選択

- Simple AD
  - フルマネージドのディレクトリ サービス
  - Samba 4 Active Directory互換サーバーを利用
  - AWS上に独立したドメインを作成
- AD Connector
  - 既存のディレクトリ サービスへの接続
  - オンプレミスまたは VPC 上のドメインを指定
  - 多要素認証（MFA）をサポート

シングルサインオン（SSO）の有効化

- WorkSpacesとWorkDocsの間でシングルサインオン（SSO）を設定可能
  - WorkSpacesにログオンすると自動的にWorkDocs Syncクライアントにサインインして同期を開始
  - Directory ServiceのManagement Consoleより有効化

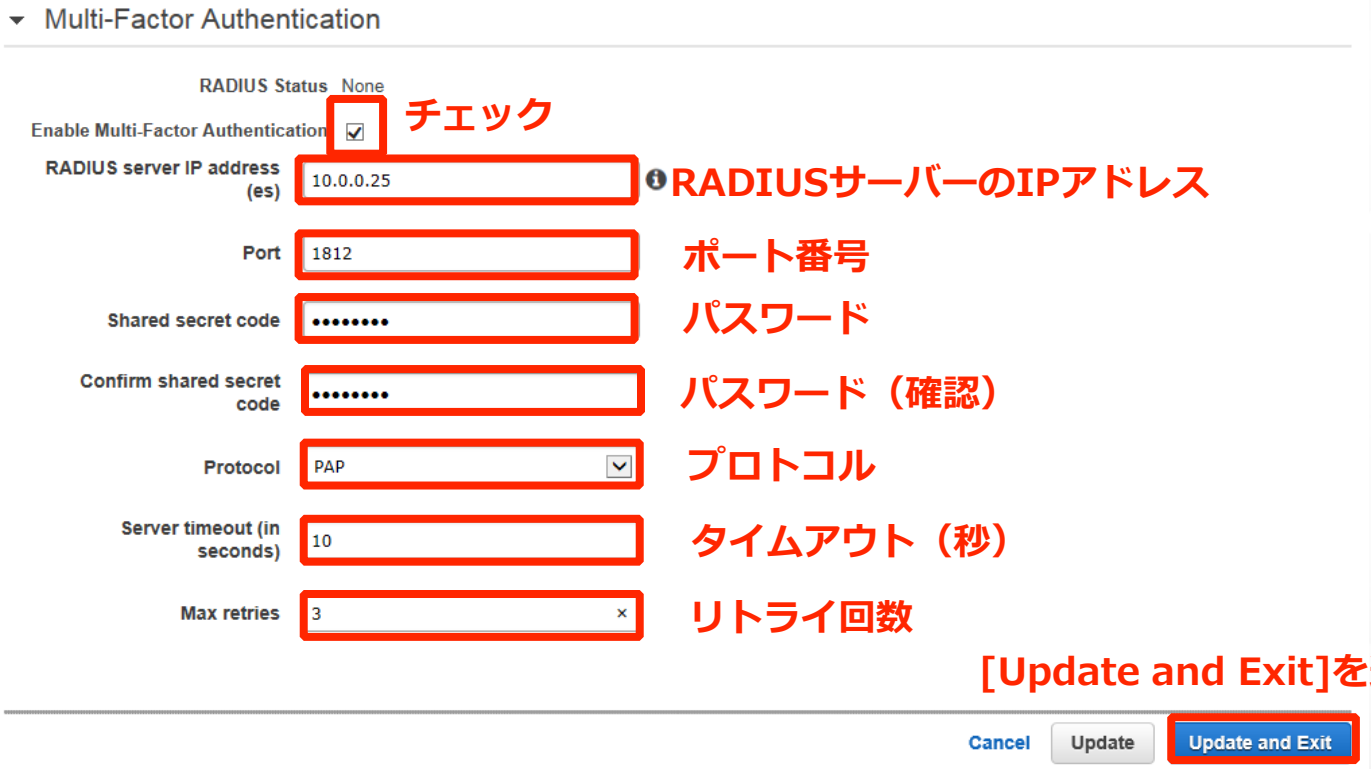


多要素認証（MFA）

- オンプレミスの RADIUS サーバーを利用した多要素認証（MFA）に対応
  - ユーザー名とパスワードに加えてワンタイム パスワード等の利用が可能
- PAP/CHAP/MS-CHAP1/MS-CHAP2 をサポート
  - Symantec Validation and ID Protection Service (VIP)
  - Microsoft RADIUS Server

MFAの設定

- [Multi-Factor Authentication]にRADIUSサーバーの情報を入力して[Update and Exit]を選択



(例) Google Authenticatorを使った方法

- スマートフォンに無料でインストールできる Google Authenticator をソフトウェアトークンとして使用する。
- サーバ側は、オープンソースのFreeRADIUSと Google AuthenticatorのPAM（Pluggable Authentication Module）を連携させて実現させる。

- http://aws.typepad.com/sajp/2014/10/google-authenticator.html

※ユーザ登録時のGUIは無くコマンドライン操作が必要になります。

amazon web services

Directory Service API

- ディレクトリやコンピュータアカウント、エイリアスの作成・削除などのオペレーションがAPIやCLIから操作可能
  - CreateDirectory
  - CreateSnapshot
  - EnableSSOなど
- CloudTrailとの統合
  - APIアクション（SDK、コンソールまたはCLI経由）はロギング可能

```
CreateDirectory
{"Name": "corp.snackers.org",
 "ShortName": "corp",
 "Password": "Westbay@123",
 "Description": "corp",
 "Size": "Large",
 "VpcSettings":
  {"VpcId": "vpc-c3dd04a2",
   "SubnetIds":
    ["subnet-9add04fb", "subnet-
66dc0507"]
  }
}
```

Amazon WorkSpaces Deep Dive

amazon web services

WorkSpacesバンドル

Value

- 1vCPU
- 2GiB Memory
- 10GB User Storage

Standard

- 2vCPU
- 4GiB Memory
- 50GB User Storage

Performance

- 2vCPU
- 7.5GiB Memory
- 100GB User Storage

+

Plus

- Microsoft Office Professional 2010/2013
- Trend Microビジネスセキュリティクライアント

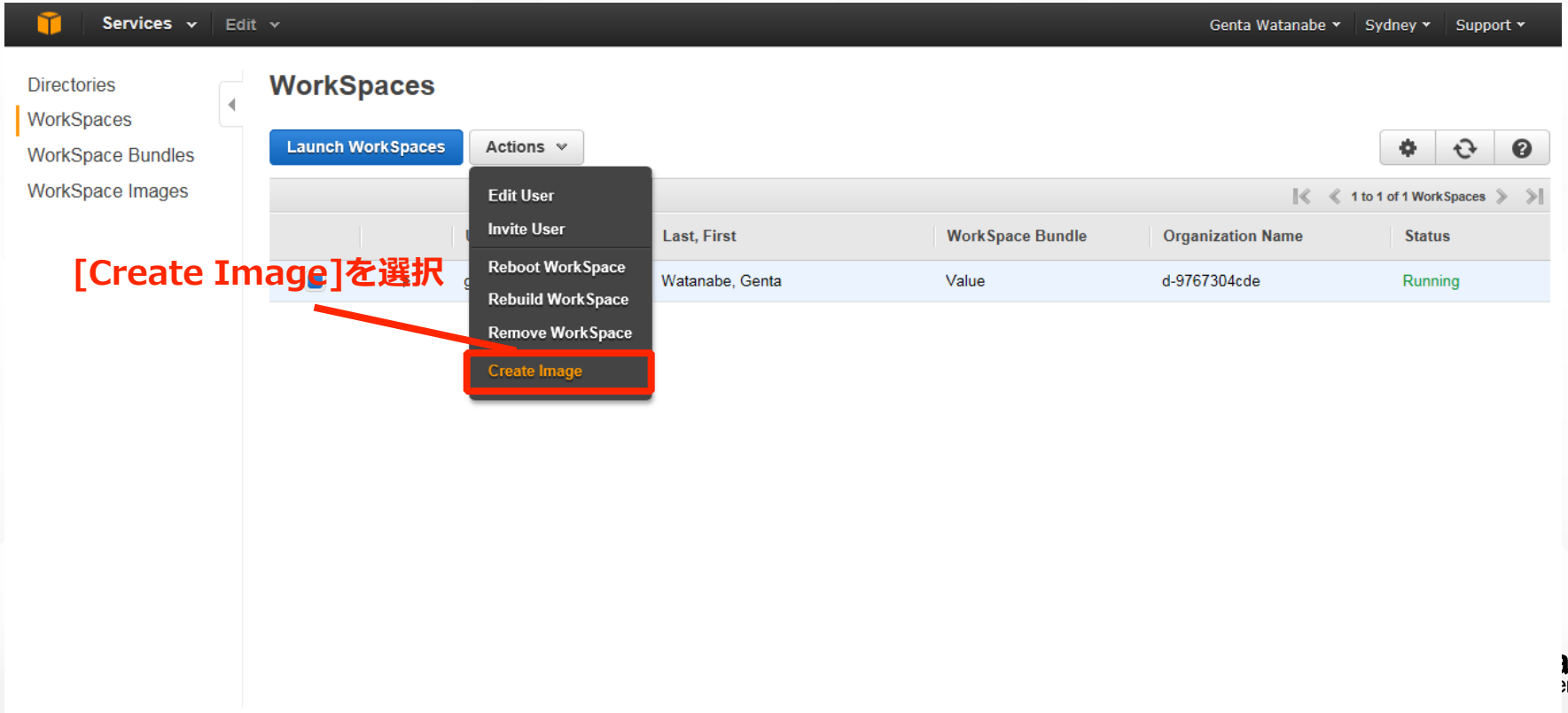
amazon web services

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）

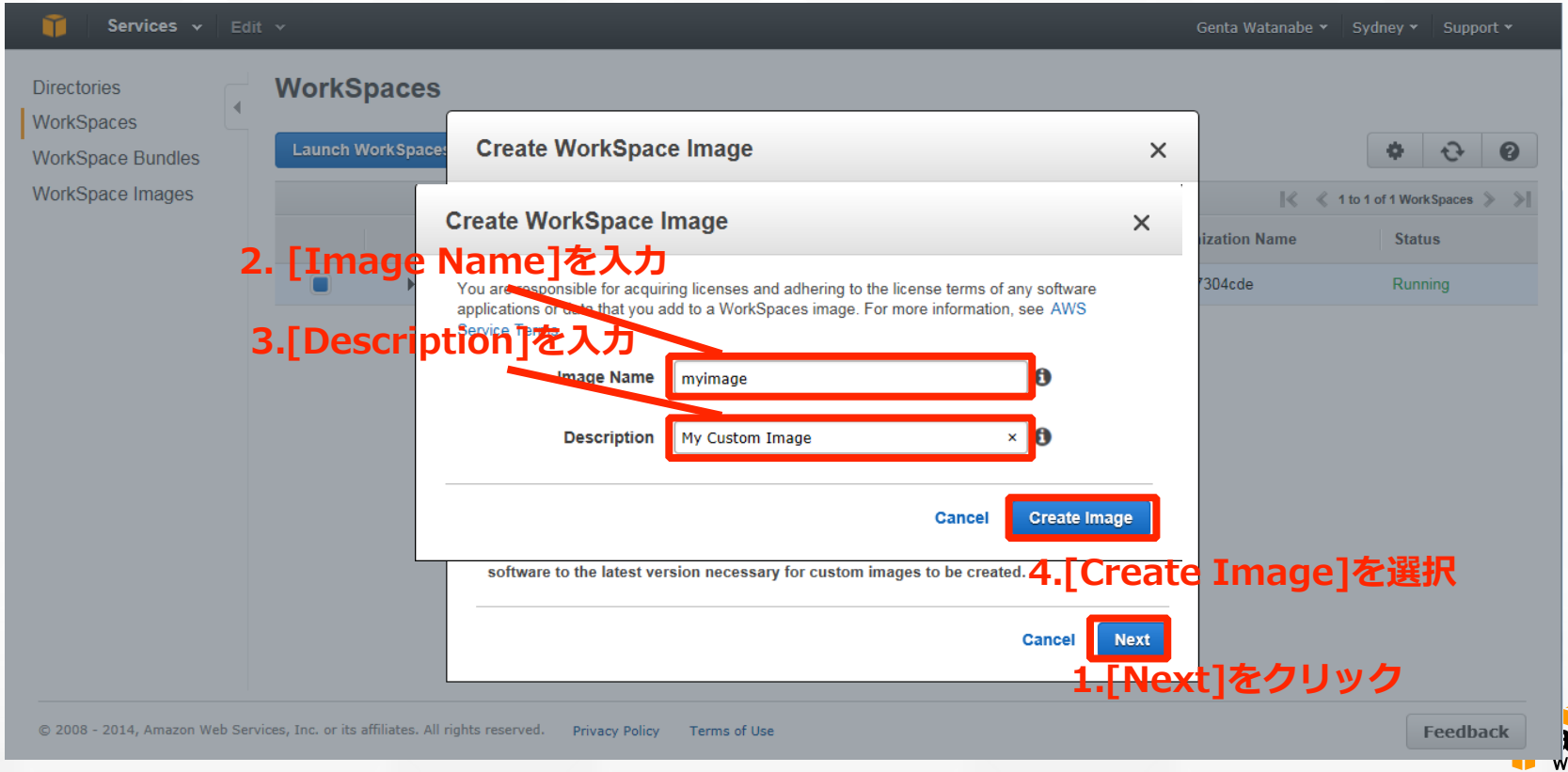
Custom Imageの作成（1/2）

- ワークスペースにアプリケーションをインストールして、[Actions]から[Create Image]を選択



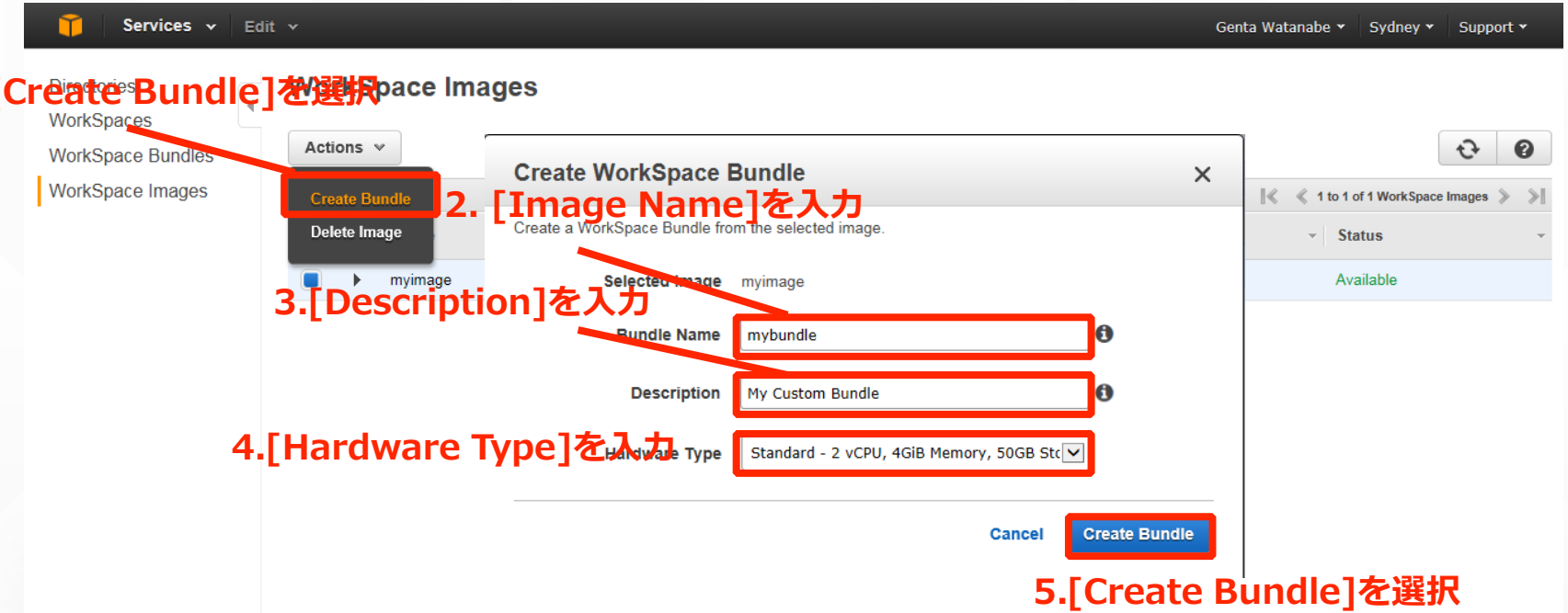
Custom Imageの作成（2/2）

- [Image Name][Description]を入力し、Custom Imageを作成



Custom Bundleの作成

- [WorkSpaces Images]タブから、Custom Bundleを作成

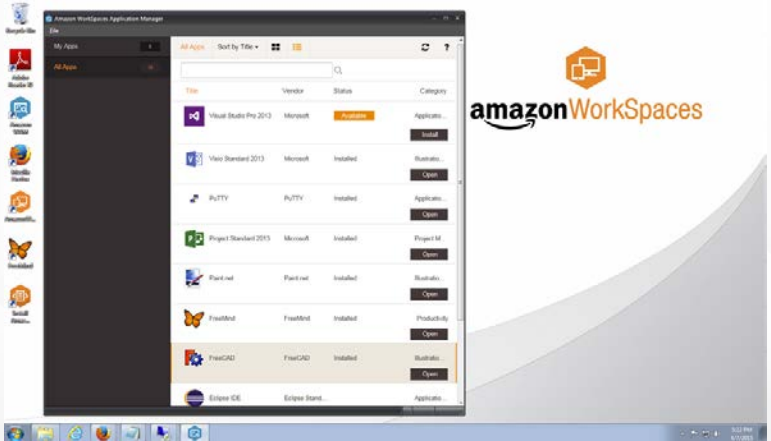


イメージ作成のベストプラクティス

- 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

Amazon WorkSpaces Application Manager

- Amazon WorkSpaces向けのアプリケーションをデプロイおよび管理
  - Windowsアプリケーションを仮想化されたコンテナにパッケージ
  - AWS Marketplace for Desktop Appsの利用



Amazon WAMオーバービュー

さまざまな種類のアプリケーションを提供

カタログの作成

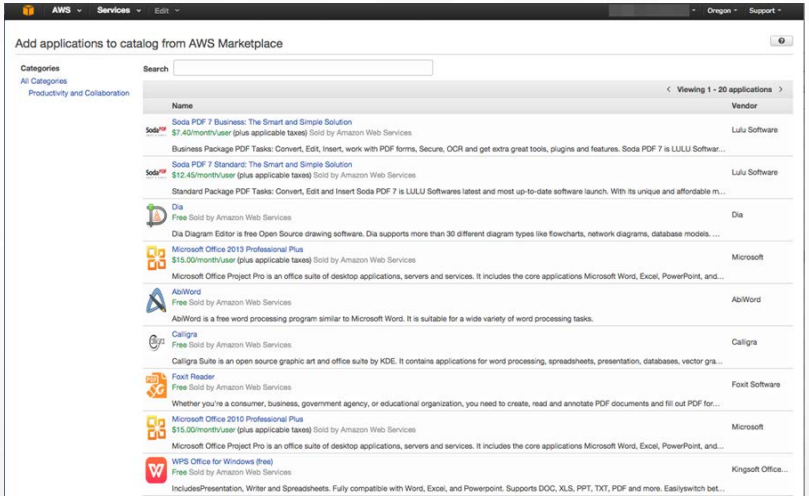
- アプリケーションのアップロード
  - 独自のアプリケーションをパッケージ化して提供
  - Admin StudioおよびAdmin Playerによりアプリケーションをコンテナにパッケージして検証
- AWS Marketplace for Desktop Appsからのサブスクリプション
  - AWS Marketplace for Desktop Appsに登録されているアプリケーションを選択して利用
  - アプリケーション開発、イラストおよびデザイン、オフィスアプリなど

アプリケーションのアップロード

- Amazon WorkSpacesのManagement パッケージ化したアプリケーションをアプリケーションカタログに追加
- カタログからアプリケーションを選択してユーザーまたはグループにアサイン
  - Required（必須）またはOptional（任意）が選択可能
  - Requiredを選択するとアプリケーションは自動的にインストールされる

AWS Marketplace for Desktop Apps

- Amazon WorkSpaces用のデスクトップアプリケーションのためのAWS Marketplaceの新しいカテゴリ
  - 10以上のカテゴリのアプリケーションを選択してWorkSpacesにデプロイ
  - 月単位のサブスクリプションでデスクトップアプリケーションを利用可能



AWS Marketplace for Desktop Appsに登録されているアプリケーション

アプリケーションおよびWeb 開発

Microsoft Visual Studio

Python

生産性およびコラボレーション

Microsoft Office

Kingsoft Office

Libre Office

セキュリティ, ストレージ & アーカイブ

Zscaler Security Cloud

McAfee Anti-Virus

Areca Backup

ユーティリティ

Foxit PhantomPDF

TechSmith Snagit

7-Zip

メディアおよびエンコーディング

aTunes

VLC Media Player

ネットワーク

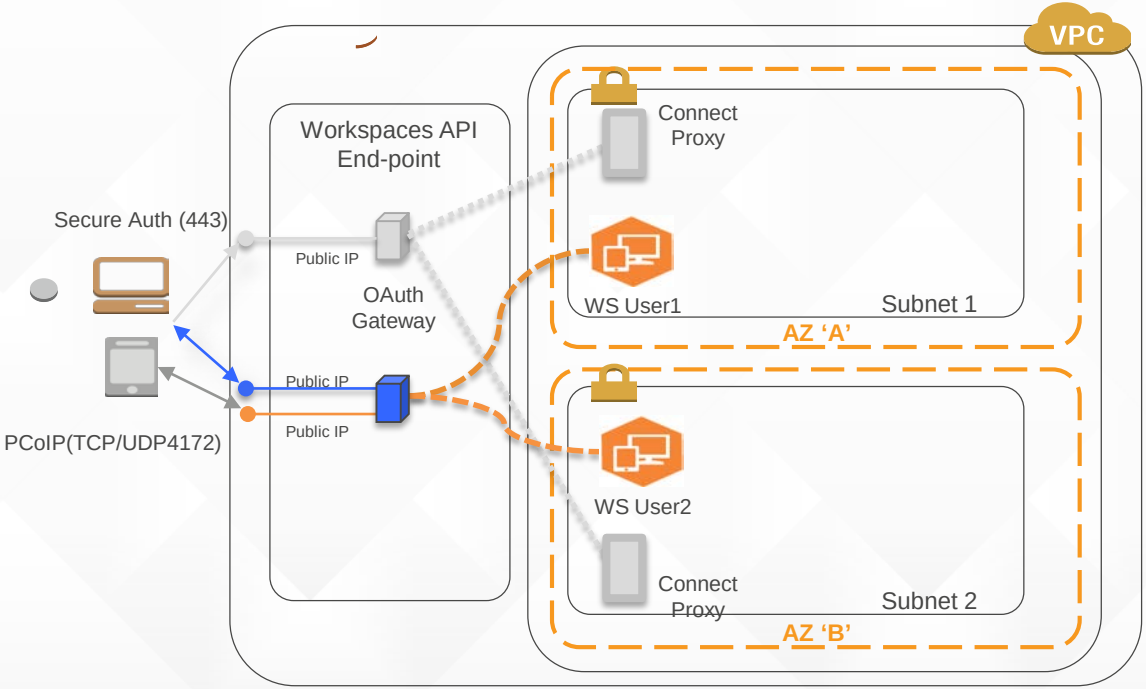
- それぞれのWorkSpaceは 2 つのネットワークインターフェースをもつ
  - VPCおよびインターネット接続用ネットワーク
  - WorkSpace管理用および画面転送用ネットワーク
- 管理用ネットワークでは以下のポートを利用する
  - インバウンド
    - TCP/UDP 4172
    - TCP 8200
  - アウトバウンド
    - UDP 55000

ネットワーク要件

- AD Connectorでドメイン 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

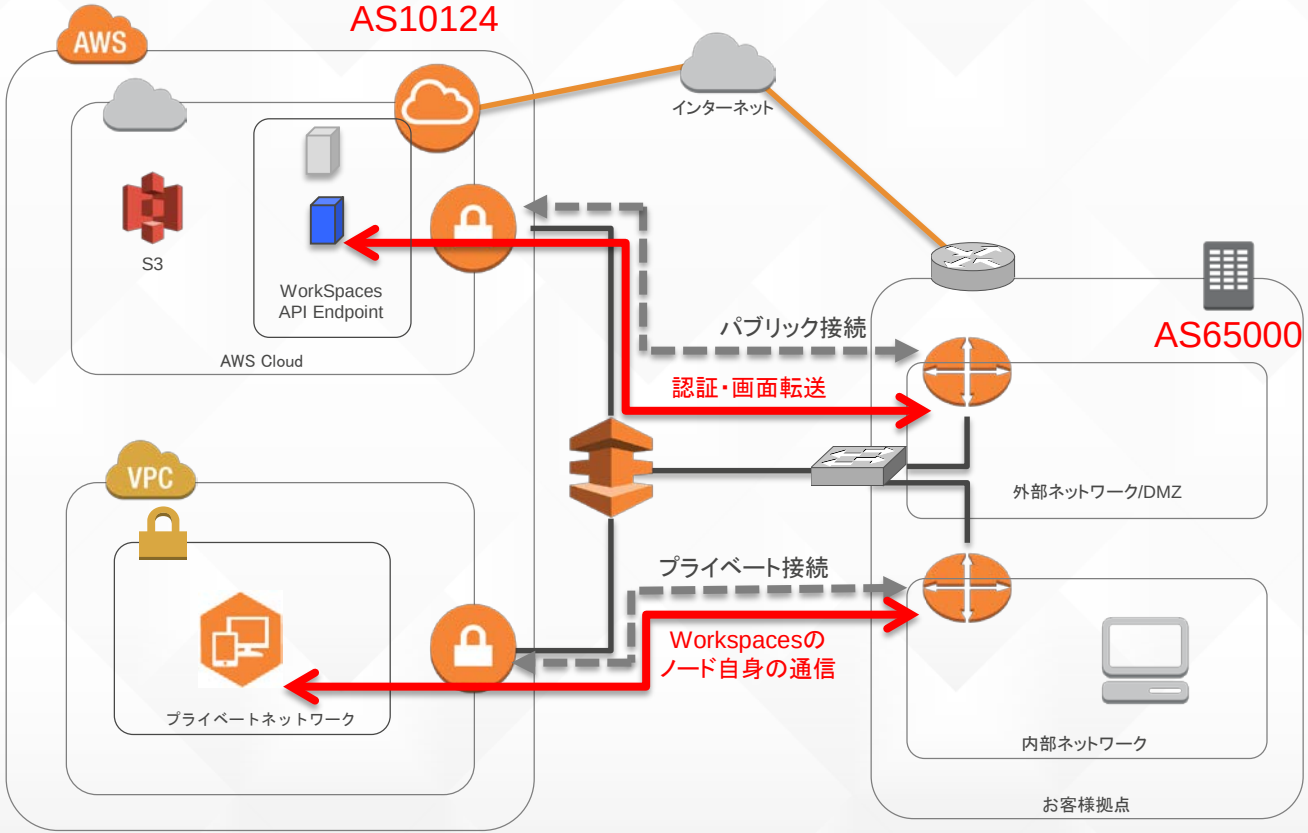
WorkSpacesへのアクセス

- クライアントからの接続はインターネット経由で行われるため、AWSのIPアドレス範囲に対してTCP/UDP 4172をオープンする
  - https://ip-ranges.amazonaws.com/ip-ranges.json



Direct Connectによる閉域網からのアクセス

- DXのパブリック接続を利用することにより画面転送も専用線経由に

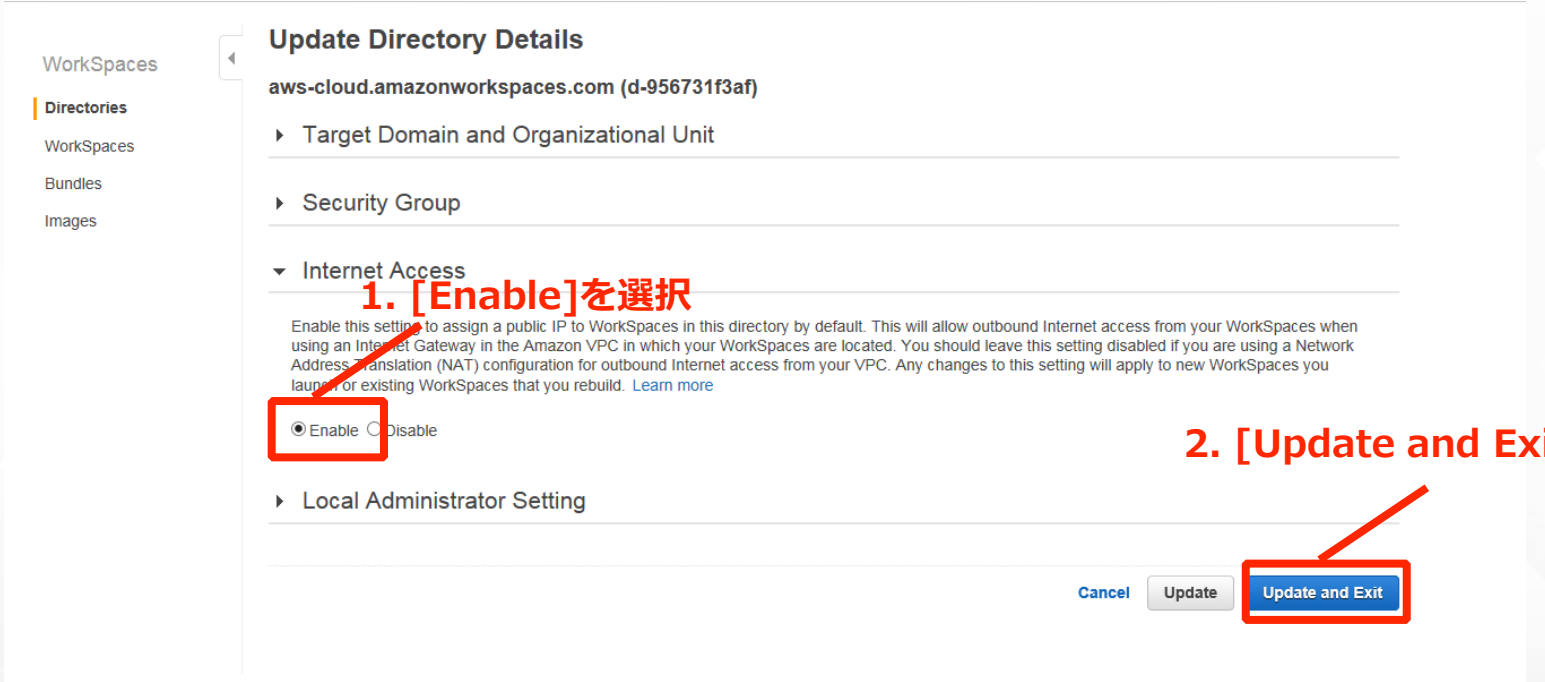


インターネットへの接続

- 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Public IPアドレスの付与が必要
  - NAT Instanceパターン
  - On-Premise Firewallパターン
  - Public IP Addressパターン
- ディレクトリ設定からインターネットアクセスを設定可能

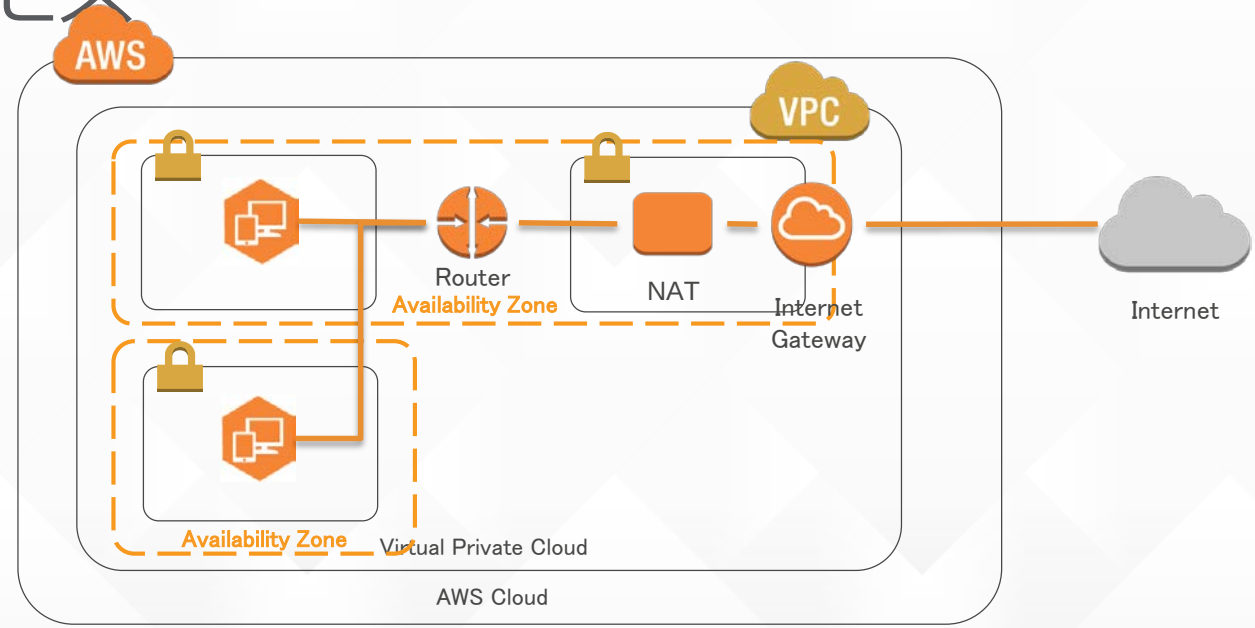
インターネット接続の有効化

- [Directory Details]から[Internet Access]を[Enable]に指定



構成例:NAT Instanceパターン

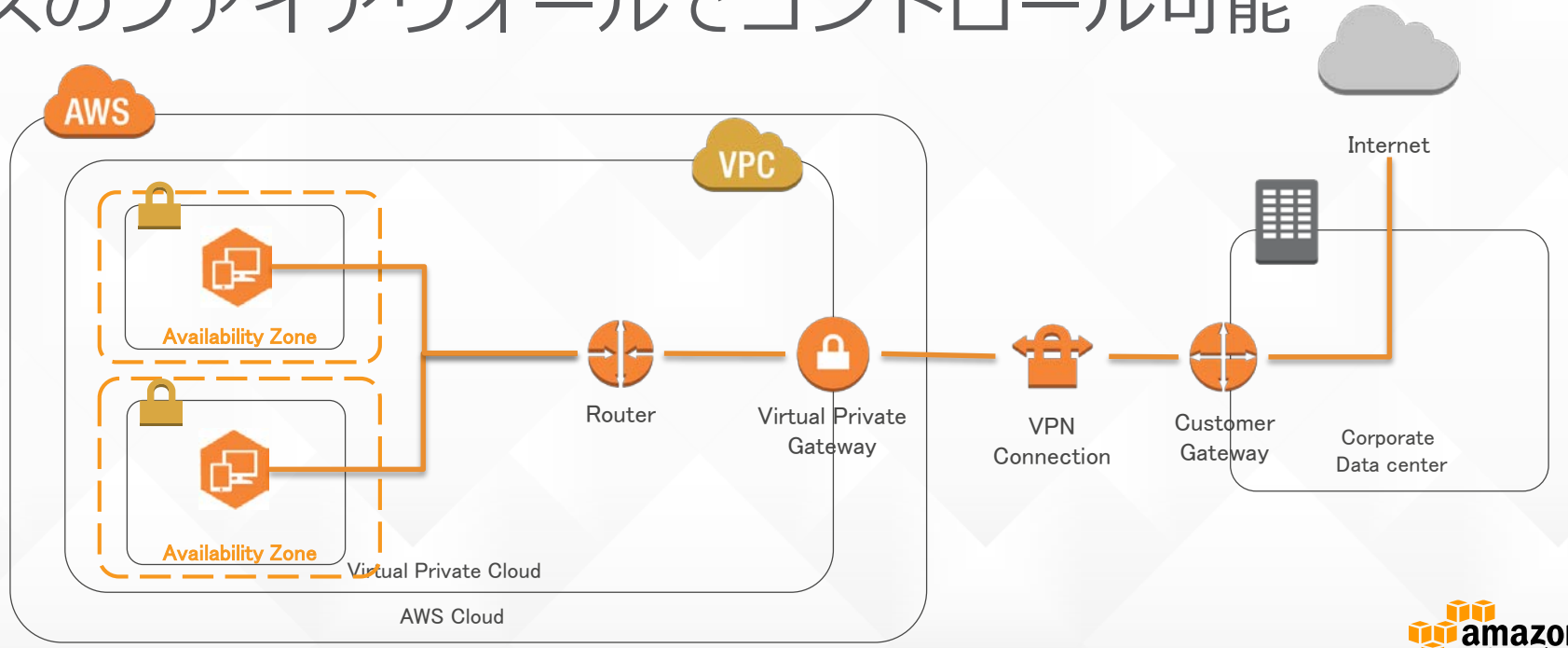
- NATインスタンスを経由してインターネットへアクセス



amazon web services

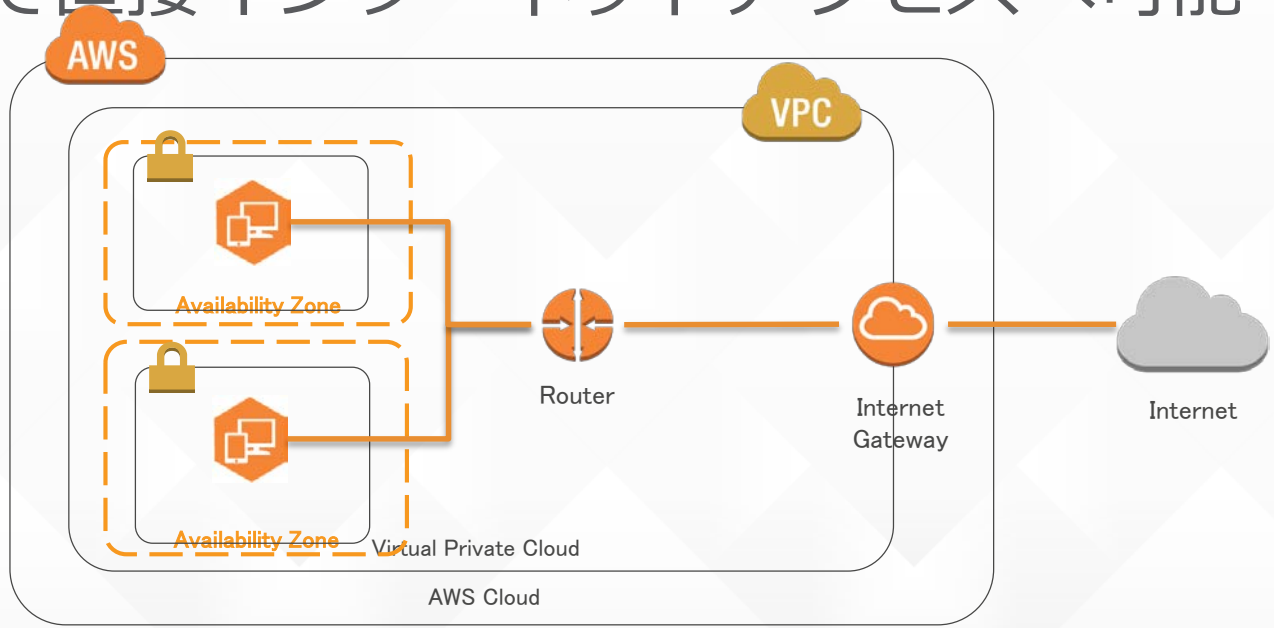
構成例:On-Premise Firewallパターン

- 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



構成例:Public IP Addressパターン

- ワークスペースにPublic IPアドレスを付与することで直接インターネットアクセスへ可能



ローカルプリンターへの印刷

- ワークスペースから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
  - Cordado ThinPrint/Google Cloud Printなどのクラウドプリント

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Amazon WorkSpaces固有の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

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

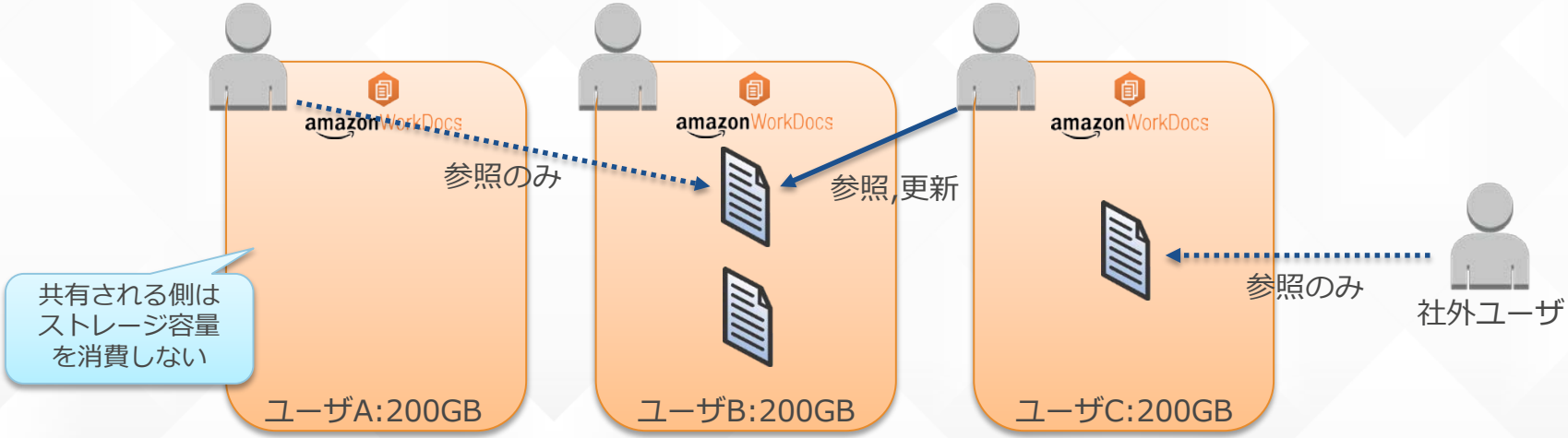
```
}
[ @c82a14544422]~>aws workspaces create-workspaces --workspaces DirectoryId=d-926735ab8f,BundleId=wsb-jnyscd6pb,UserName=olivia
{
    "PendingRequests": [
        {
            "UserName": "olivia",
            "DirectoryId": "d-926735ab8f",
            "State": "PENDING",
            "WorkspaceId": "ws-4w79y1g1x",
            "BundleId": "wsb-jnyscd6pb"
        }
    ],
    "FailedRequests": []
}
```

Amazon WorkDocs Deep Dive

amazon web services

Amazon WorkDocs - セントラルハブ

- ファイルやフォルダ単位で他ユーザに対してファイルの読み取り/書き込み権限を付与することでファイル共有が可能
- 社外ユーザにも読み取りを許可することもできる（ポリシーで社外共有を不許可にすることも可能）



アクセス権の設定

- フォルダおよびファイルのアクセス許可はロールに基づいて付与される
  - 所有者 - フォルダまたはファイルの所有者
  - 共同編集者 - フォルダが共有され、フォルダへのアクセスは制限されていないユーザー
  - 閲覧者 - フォルダが共有されたが、フォルダへのアクセスが制限されている（表示のみ）ユーザー
  - 匿名の閲覧者 - 外部の表示リンクを介して共有されたファイルを表示できる、組織外部の登録されていないユーザー

組織外のユーザーに対するドキュメントの共有

- 「匿名の閲覧者」ロールによって組織外のユーザーに対してフォルダまたはファイルの共有が可能
  - 組織外への共有ポリシー
    - ユーザーはドキュメント参照リンクを誰にでも送信できる
    - ユーザーはドキュメント参照リンクを指定されたドメインのみに送信できる
  - 新規ユーザー招待のポリシー
    - 管理者のみが新しいユーザーを招待できる

例：共有フォルダにあるファイルのアクセス許可

アクセス許可	フォルダ所有者	ファイル所有者	フォルダ共同編集者	フォルダ閲覧者	匿名の閲覧者
表示	X	X	X	X	X
共有の表示	X	X	X	X	X
ダウンロード	X	X	X	X	
注釈	X	X	X		
注釈の表示	X	X	X		
アクティビティの表示	X	X	X		
バージョンの表示	X	X	X		
アップロード	X	X	X		
削除	X	X	X		
ダウンロードの禁止	X	X			
共有	X	X			
共有の取り消し	X	X			

CloudTrailによるAPIコールの記録

- 詳細なアクセスログを記録したい場合はCloudTrailを利用する
- APIコール単位でアクセスが記録されるため、詳細な監査が可能

AWS CloudTrail

JSON形式のログ


```
{
        "eventVersion" : "1.02",
        "userIdentity" : {
                "principalId" : "S-1-5-21-3312768711-3070474699-4104396599-1120\u0026d-90673679db",
                "accountId" : "762789334655",
                "userName" : "fintaro",
                "type" : "Directory"
        },
        "eventTime" : "2015-02-16T11:54:01Z",
        "eventSource" : "WorkDocs.amazonaws.com",
        "eventName" : "GetFolder",
        "awsRegion" : "us-east-1",
        "sourceIPAddress" : "72.21.196.64",
        "userAgent" : "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko",
        "requestParameters" : {
                "Attributes" : null,
                "AuthenticationToken" : "\u003c**-redacted-**\u003e",
                "FolderId" : "022f3fed81a53b0a45ab3faa61aa15cf9a5888e978749754833c9ef0f8fc1536",
                "Marker" : null,
                "MaxItems" : null,
                "Order" : null,
                "SortBy" : null
        },
```

Amazon WorkMail Deep Dive

amazon web services

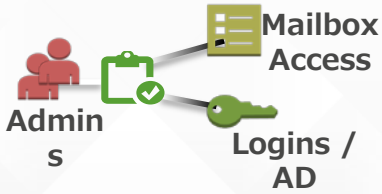
Amazon WorkMail– マネージド&セキュア

お客様自身の管理するキーでの暗号化

Amazon WorkMailはAWS Key Management Serviceとの統合によりお客様自身の管理するキーでのデータを暗号化

リージョンによるデータのコントロール

メールボックスのデータが格納されるリージョンが選択可能なため低レイテンシーと地域ごとのコンプライアンス基準に適合

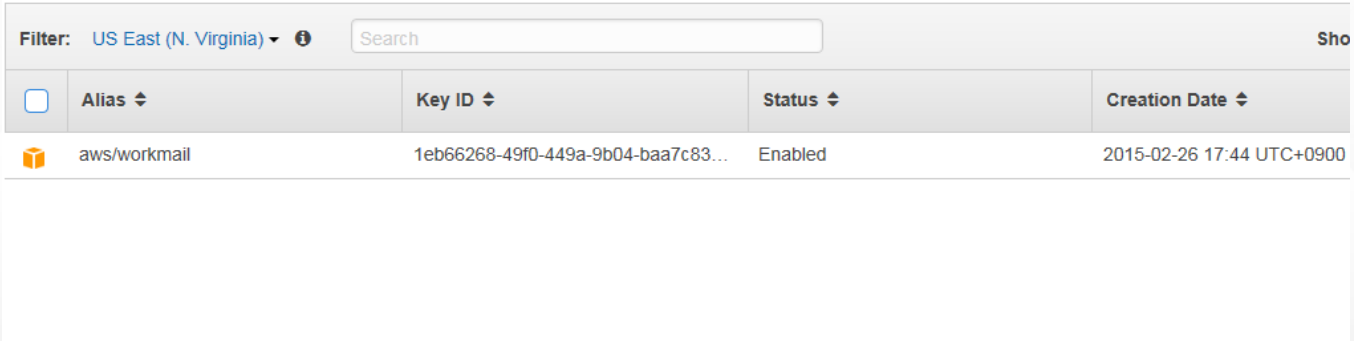


シンプルな利用

Amazon WorkMailは企業内の電子メールインフラ管理を容易にし、既存のディレクトリサービスとセキュアに統合

AWS Key Management Serviceによる鍵管理

- KMSは保存されたのデータ（メッセージ、連絡先、添付とメタデータ）の暗号化に利用される
  - Quick setupではデフォルトのキーが作成され利用される
  - Custom setupでは自分で作成したキーを選択可能



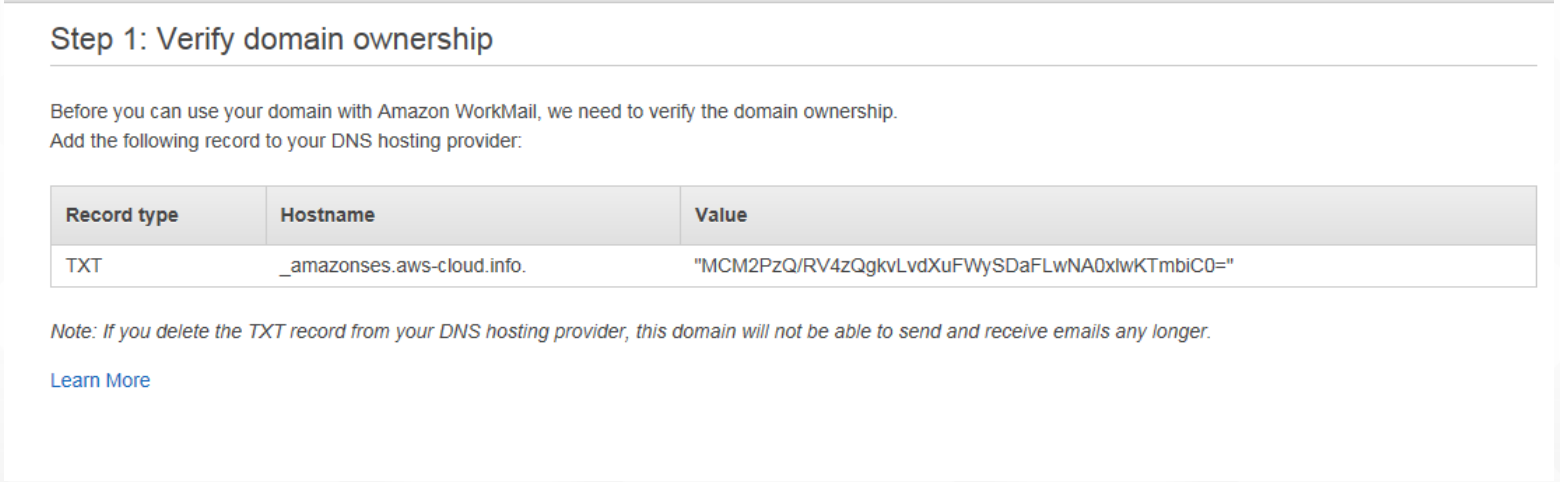
amazon web services

Amazon Simple Email Serviceとの統合

- WorkMailはアウトバウンドの電子メール送信およびドメイン検証の仕組みにSESを利用
  - WorkMailのために構成したメールドメインはSESコンソールからも確認可能

独自ドメインの設定（1/2）

- WorkMailでは独自ドメインの設定および利用が可能
  - 組織（Organization）の作成後にドメインを追加
  - ドメイン所有権の検証のためRoute 53などのDNSホスティングプロバイダにTXTレコードを追加



Step 1: Verify domain ownership

Before you can use your domain with Amazon WorkMail, we need to verify the domain ownership.
Add the following record to your DNS hosting provider:

Record type	Hostname	Value
TXT	_amazonses.aws-cloud.info.	"MCM2PzQ/RV4zQgkvLvdXuFWySDaFLwNA0xlwKTmbiC0="

Note: If you delete the TXT record from your DNS hosting provider, this domain will not be able to send and receive emails any longer.

Learn More

独自ドメインの設定（2/2）

- 以下のレコードをDNSに追加し、設定が完了するまで最大72時間まつ
  - メール受信のためのMXレコード
  - Outlookおよびモバイルクライアントからの自動検出のためのCNAMEレコード
  - DKIM署名のためのCNAMEレコード

Step 2: Finalize domain setup

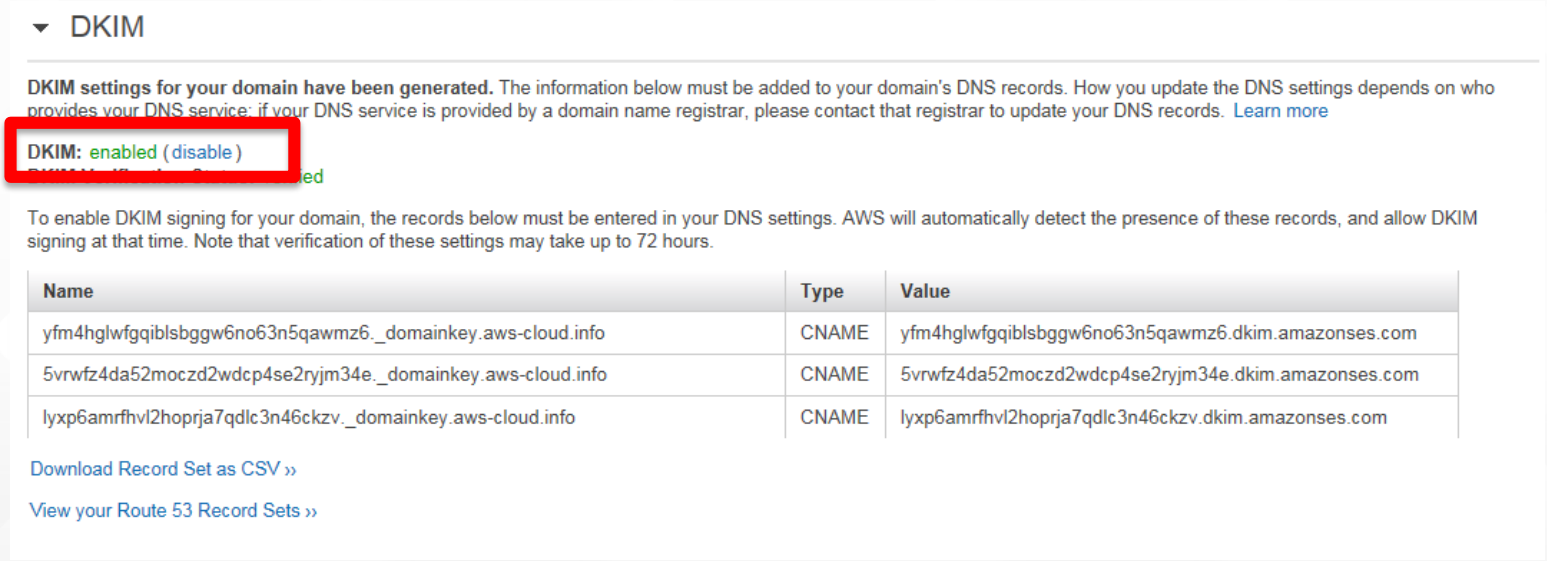
To switch your domain completely to Amazon WorkMail, add the following DNS records to your DNS hosting provider.
If your domain already has email addresses, be careful when you change MX records. To avoid email service disruption, make sure that all your user accounts and distribution lists are added.

Record type	Hostname	Value
MX	aws-cloud.info.	10 inbound-smtp.us-east-1.amazonaws.com.
CNAME	autodiscover.aws-cloud.info.	autodiscover.mail.us-east-1.awsapps.com.
CNAME	yfm4hglwfgqiblsbggw6no63n5qawmz6._domainkey.aws-cloud.info.	yfm4hglwfgqiblsbggw6no63n5qawmz6.dkim.amazonses.com.
CNAME	5vrwfz4da52moczd2wdcp4se2ryjm34e._domainkey.aws-cloud.info.	5vrwfz4da52moczd2wdcp4se2ryjm34e.dkim.amazonses.com.
CNAME	lyxp6amrfhvl2hoprja7qdlc3n46ckzv._domainkey.aws-cloud.info.	lyxp6amrfhvl2hoprja7qdlc3n46ckzv.dkim.amazonses.com.

Remove any existing MX records before adding the new MX record. It can take up to 72 hours before all DNS records are propagated.

DKIMによるメール署名の有効化

- Domain Keys Identified Mail（DKIM）によるメール署名が利用可能
  - 独自ドメインを設定した場合はドメイン検証後にSESコンソールから手動でDKIMを有効化



▼ DKIM

DKIM settings for your domain have been generated. The information below must be added to your domain's DNS records. How you update the DNS settings depends on who provides your DNS service: if your DNS service is provided by a domain name registrar, please contact that registrar to update your DNS records. Learn more

DKIM: enabled (disable)

To enable DKIM signing for your domain, the records below must be entered in your DNS settings. AWS will automatically detect the presence of these records, and allow DKIM signing at that time. Note that verification of these settings may take up to 72 hours.

Name	Type	Value
yfm4hglwfgqiblsbggw6no63n5qawmz6._domainkey.aws-cloud.info	CNAME	yfm4hglwfgqiblsbggw6no63n5qawmz6.dkim.amazonses.com
5vrwfz4da52moczd2wdcp4se2ryjm34e._domainkey.aws-cloud.info	CNAME	5vrwfz4da52moczd2wdcp4se2ryjm34e.dkim.amazonses.com
lyxp6amrfhvl2hoprja7qdlc3n46ckzv._domainkey.aws-cloud.info	CNAME	lyxp6amrfhvl2hoprja7qdlc3n46ckzv.dkim.amazonses.com

Download Record Set as CSV ››

View your Route 53 Record Sets ››

まとめ

- AWSのエンタープライズアプリケーションは仮想デスクトップ、エンタープライズストレージおよび電子メール・カレンダーなどの機能をマネージドサービスとして提供
- AWS Directory Serviceはエンタープライズアプリケーションの認証基盤
- Amazon WorkSpaces、WorkDocsおよびWorkMailはさまざまなサービスとも連携して動作するためひととおり把握しておくことが重要

参考資料

- Amazon WorkSpaces 管理者ガイド
  - http://docs.aws.amazon.com/ja_jp/workspaces/latest/adminguide/
- Amazon WorkDocs Documentation
  - http://aws.amazon.com/jp/documentation/workdocs/
- Amazon WorkMail Documentation
  - http://aws.amazon.com/jp/documentation/workmail/
- AWS Directory Service Documentation
  - http://aws.amazon.com/jp/documentation/directory-service/

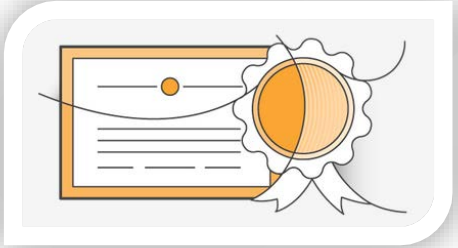
AWSトレーニング @ AWS Summit Tokyo

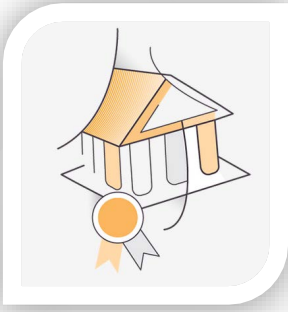
セルフペースラボ：@パミール1F 瑞光

AWS クラウドに実際に触れてみませんか？
ご自分の AWS アカウントをおつくりいただけなくても、
AWS クラウドを体験いただけます。

AWS認定試験（有償）：@ パミール1F 黄玉

特設認定試験会場を AWS Summit Tokyo 2015 会場に開設
Devopsエンジニア-プロフェッショナル認定試験を先行受験いただけます。





AWS認定資格者取得専用ラウンジ：@ パミール1F 青玉

他の AWS 認定資格をお持ちの方とのネットワーキングにぜひラウンジをご活用ください。
お席や充電器、お飲物などを用意し、皆様をお待ちしております。

amazon web services

Thank You

amazon web services