

このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報については[サービス別資料](#)もしくはサービスのドキュメントをご確認ください

AWS Directory Service

AWS Black Belt Tech Webinar 2015 (旧マイスターシリーズ)

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 渡邊源太

2015.12.14



内容についての注意点

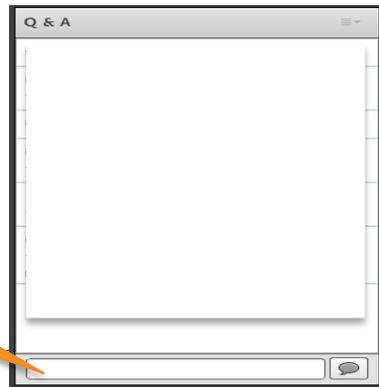
- ❖ 本資料では2015年12月24日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<http://aws.amazon.com>)にてご確認ください。
- ❖ 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- ❖ 価格は税抜表記となっております。日本居住者のお客様がサービスを使用する場合、別途消費税をご請求させていただきます。

AWS Black Belt Tech Webinar へようこそ！

📦 質問を投げることができます！

- Adobe Connectのチャット機能を使って、質問を書き込んでください。（書き込んだ質問は、主催者にしか見えません）
- Twitterへツイートする際はハッシュタグ**#awsblackbelt**をご利用ください。

①画面右下のチャットボックスに質問を書き込んでください



②吹き出しマークで送信してください

AWS Black Belt Tech Webinar 2015

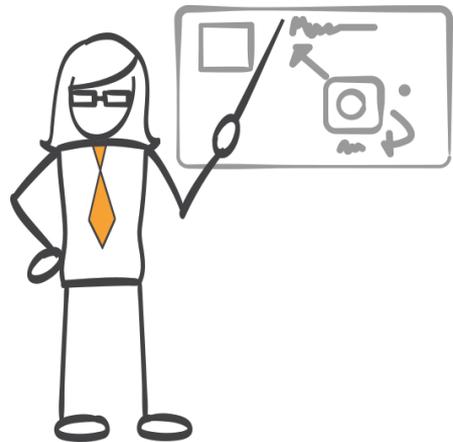
- 今後の配信予定

10月は「**re:Invent**月間」です！

- 10/9 (金) 現地ラスベガスよりお届け！re:Invent速報 (12:00-13:00)
- 10/13 (火) 俺の re:Invent 2015(仮) (12:00-13:00)
- 10/14 (水) AWS re:Invent 2015 SA座談会
- 10/21 (水) AWS Directory Service
- 10/28 (水) AWS CodeCommit & AWS CodePipeline & AWS CodeDeploy

- イベントスケジュール

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



アジェンダ

- AWS Directory Serviceとは
 - Active Directory on AWS
 - ディレクトリタイプの選択
 - Simple ADの管理
- AWS Management Consoleとの認証フェデレーション
 - Active Directoryフェデレーションサービス (ADFS)
 - AD Connectorによるフェデレーション
- AWSアプリケーションとの連携
 - シングルサインオン (SSO) の有効化
- まとめ

ディレクトリとは

- ユーザに関わる各種情報を保管する仕組み
 - ユーザ名
 - 姓・名、部署、電話番号
 - メールアドレス
 - パスワード
 - グループ
など
- ツリー状の構成とする事が多いことから、ディレクトリと呼ばれる
- 関連用語：LDAP、Active Directory、OpenLDAP

Active Directoryとは

- Windowsネットワークの基本的な認証とセキュリティ基盤
- Windows 2000から標準機能として実装されたディレクトリサービス
- NTドメインからの反省をふまえたアーキテクチャー
 - ドメイン間の階層構造がとれない
 - 同一ネットワーク上に同じコンピュータ名が共存できない
 - Security Account Manager (SAM) データベースの最大容量が40MBまで

Active Directoryの必要性

- IDとアクセス管理
 - 運用効率の向上
 - コンプライアンスの推進
 - セキュリティの強化
 - エクストラネットへの拡張
- アプリケーションによる使用
 - Exchange/SharePoint/SQL Server
 - ファイル共有・パッチ管理など

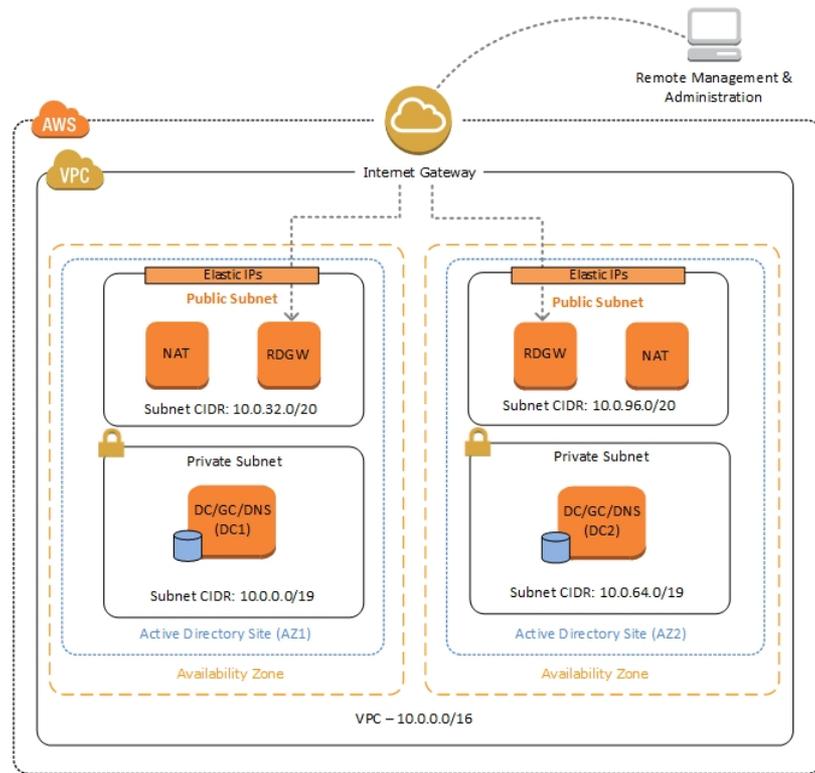
Windowsシステムでは、Active Directoryがほぼ必須

Active Directoryドメインサービス (AD DS)

- 名前解決 (DNS)
- ディレクトリサービス (LDAP)
- ユーザー認証 (Kerberosバージョン5)
- クライアント管理 (SMB:ファイル共有)

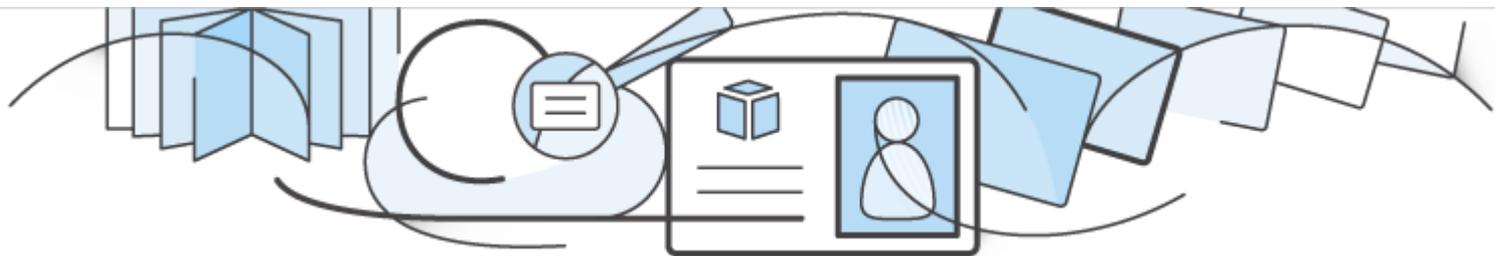
Active Directory on AWS

- Active Directory Domain ServicesのAWS上でのデプロイに関するリファレンスとCloudFormationテンプレート
- 新しいクラウドベースのAD DSのデプロイと既存のオンプレミスのAD DSのAWSクラウドへのデプロイの拡張をサポート
 - \$3/時
 - 展開時間：約1時間



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



AWS Directory Service

Simple AD

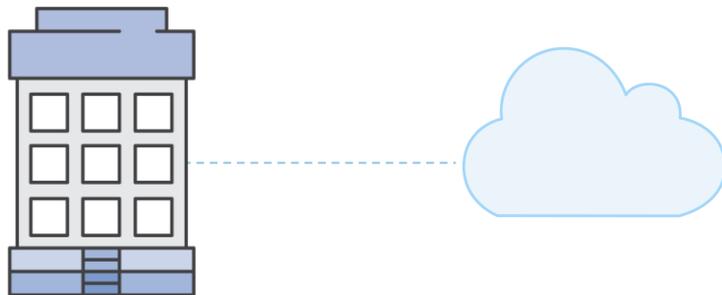
Samba 4がベース



AWS上の新規ディレクトリ

AD Connector

カスタムのフェデレーションプロキシ



On-premises

既存のディレクトリをAWSに接続

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

Simple ADの作成

- ドメインと管理者アカウントを作成する
 - Directory DNS
 - NetBIOS Name
 - Administrator Password
 - Directory Size
- 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

ディレクトリを作成する

- アジアパシフィック（東京）リージョンに変更してディレクトリを作成します。

1. リージョン選択メニュー

The screenshot shows the AWS Directory Service console interface. At the top, there is a navigation bar with 'Services' and 'Edit' dropdowns on the left, and the user name 'Genta Watanabe', the current region 'Tokyo', and 'Support' on the right. A dropdown menu is open for the 'Tokyo' region, listing various AWS regions: US East (N. Virginia), US West (Oregon), US West (N. California), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), and South America (São Paulo). The 'Asia Pacific (Tokyo)' option is highlighted with a red box. In the main content area, the text 'AWS Directory Service' is visible, along with a description: 'AWS Directory Service enables you to use your corporate access AWS services, and simplifies deployment of Microsoft Windows applications in the AWS'. A blue button labeled 'Get Started Now' is also visible, with a red box around it. Red arrows point from the text annotations to the 'Tokyo' dropdown and the 'Get Started Now' button.

2. [Asia Pacific (Tokyo)] を選択

3. [Get Started Now] を選択

Get Started Now

Getting Started Guide

ディレクトリタイプの選択

- Create a Simple ADを選択

Services Edit Genta Watanabe Tokyo Support

Directory Setup

Step 1: Directory Type

Step 2: Directory Details

Step 3: Review

Choose Directory Type

AWS Directory Service allows you to set up a standalone Simple AD directory in the AWS cloud or link with your existing on-premises directory using AD Connector. Both options enable users in your directory to access AWS applications and services using their credentials. AWS Directory Service provides a single sign-on experience to domain-joined EC2 Windows instances and Microsoft Windows application workloads. Administrators can apply security policies and use existing management tools. Developers can continue to use the code, applications, and tools they use today with traditional directories.

Create a Simple AD

 Simple AD is managed Samba 4 Active Directory Compatible Server hosted on the AWS cloud. It provides commonly used Microsoft Active Directory capabilities like users, group membership, domain join EC2 Windows instances, Kerberos single sign-on and group policies. Users in Simple AD can access Amazon WorkSpaces and Amazon Zocalo. Administrators can also manage AWS resources using AWS Management Console.

[Create Simple AD](#)

Connect using AD Connector

 AD Connector is a directory gateway to your on-premises Microsoft Active Directory. It enables users in your on-premises Active Directory to access Amazon WorkSpaces and Amazon Zocalo. Administrators can also manage AWS resources using AWS Management Console. AD Connector requires a hardware virtual private network (VPN) or an AWS Direct Connect between your corporate datacenter and your VPC in the AWS cloud.

[Create AD Connector](#)

[Cancel](#)

[Create Simple AD]を選択

Simple ADの作成 (1/2)

The screenshot shows the 'Create Simple AD' page in the AWS Management Console. The page is titled 'Directory Setup' and 'Create Simple AD'. It includes a sidebar with navigation steps: 'Step 1: Directory Type', 'Step 2: Directory Details', and 'Step 3: Review'. The main content area contains several form fields: 'Directory DNS' (value: corp.example.com), 'NetBIOS name' (value: CORP), 'Administrator password' (masked with dots), 'Confirm password' (masked with dots), 'Description' (value: Optional), and 'Directory size' (radio buttons for 'Small' and 'Large', with 'Small' selected). Below these fields is the 'VPC Details' section, which includes a 'VPC' dropdown menu (value: vpc-a79d4ece (10.0.0.0/16)) and a 'Create a new VPC' button. Red annotations with arrows point to specific fields: '1. [Directory DNS] を入力' points to the Directory DNS field; '2. [NetBIOS name] を入力 (オプション)' points to the NetBIOS name field; '3. [Administrator password] を入力' points to the Administrator password field; and '4. [Small] を選択' points to the Small radio button in the Directory size section.

1. [Directory DNS] を入力

2. [NetBIOS name] を入力
(オプション)

4. [Small] を選択

3. [Administrator password] を
入力

Simple ADの作成 (2/2)

- 既存のVPCを選択、または新規にVPCとSubnetを作成

VPC Details

1. [VPC] を選択

To set up a directory you need to select a VPC and two subnets, each in a different Availability Zone. This ensures that your directory is isolated and reachable only by your instances. Directory servers in two Availability Zones ensure high availability.

VPC

vpc-a79d4ece (10.0.0.0/16)



Create a new VPC



2. 2つの [Subnets] を選択

Subnets

10.0.0.0/24 (ap-northeast-1a)



10.0.1.0/24 (ap-northeast-1c)



Create a new Subnet



3. [Next Step]をクリック

Cancel

Previous

Next Step

入力内容の確認

Directory Setup

- Step 1: Directory Type
- Step 2: Directory Details
- Step 3: Review

Review

Before clicking "Create Simple AD" below, review your choices and make any necessary changes.

Directory name corp.example.com

NetBIOS name CORP

Administrator password *****

Description

Directory size Small

VPC vpc-a79d4ece

Subnets 10.0.0.0/24 (ap-northeast-1a) and 10.0.1.0/24 (ap-northeast-1c)

Note

You are charged for each directory you create. See the [AWS Directory Service Pricing page](#) for more information.

[Create Simple AD]をクリック

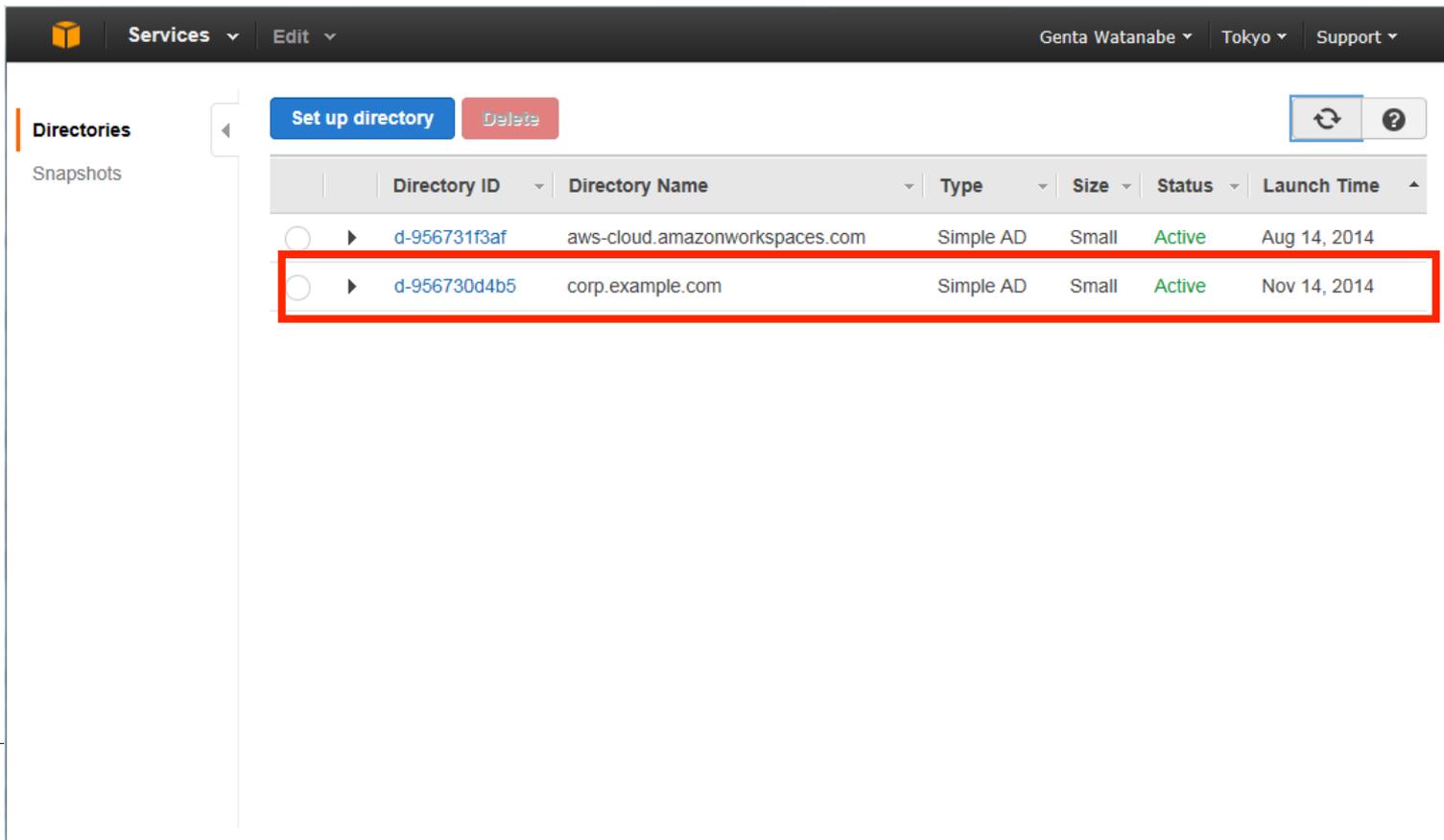
Cancel

Previous

Create Simple AD

Simple ADの確認 (1/2)

- [Status]が[Active]になれば作成完了

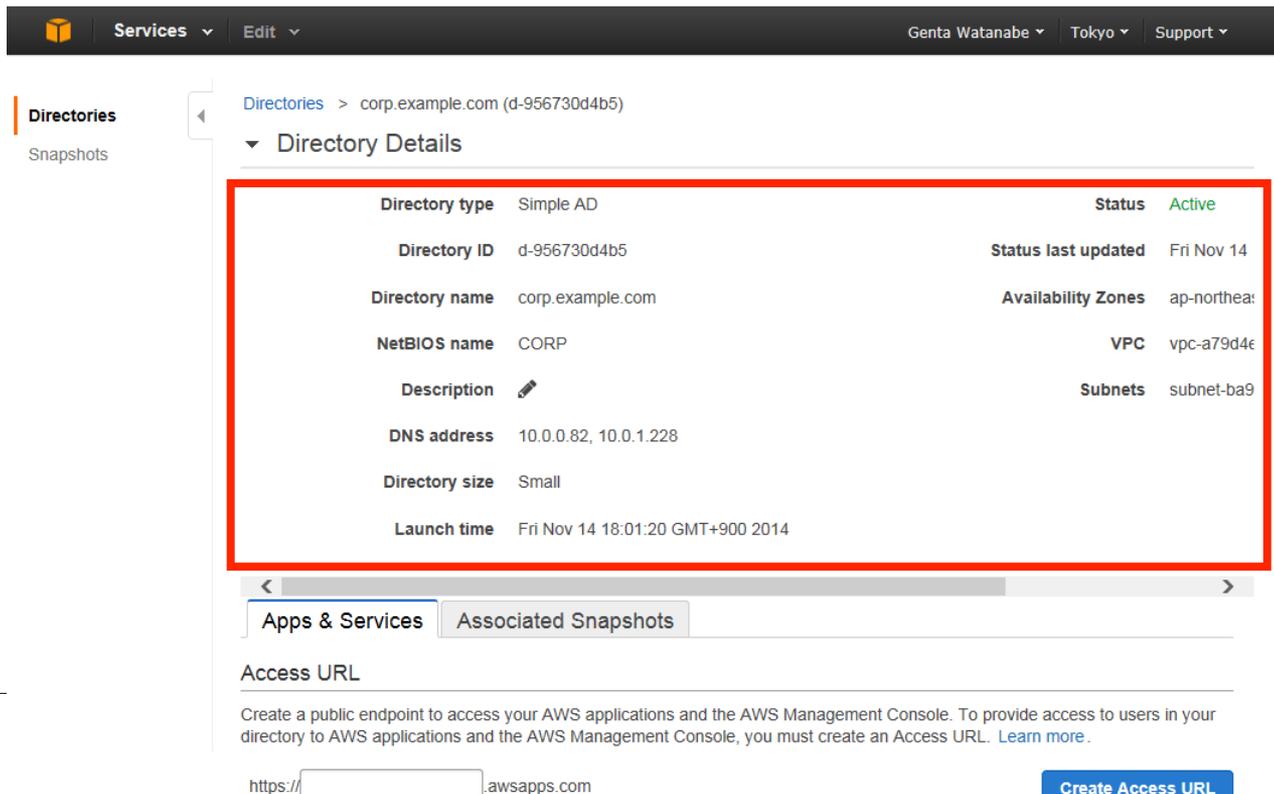


The screenshot displays the AWS IAM console interface for managing Simple AD instances. The top navigation bar shows the user 'Genta Watanabe' in 'Tokyo' with 'Support' options. The left sidebar indicates the current view is 'Directories' under 'Snapshots'. The main content area features a table of Simple AD instances. The table has columns for Directory ID, Directory Name, Type, Size, Status, and Launch Time. Two instances are listed: one for 'aws-cloud.amazonworkspaces.com' (launched Aug 14, 2014) and another for 'corp.example.com' (launched Nov 14, 2014). The second instance is highlighted with a red border, and its status is 'Active'.

Directory ID	Directory Name	Type	Size	Status	Launch Time
d-956731f3af	aws-cloud.amazonworkspaces.com	Simple AD	Small	Active	Aug 14, 2014
d-956730d4b5	corp.example.com	Simple AD	Small	Active	Nov 14, 2014

Simple ADの確認 (2/2)

- [Directory ID]をクリックして[Directory Details]を確認



The screenshot shows the AWS Management Console interface for a Simple AD directory. The breadcrumb navigation is "Directories > corp.example.com (d-956730d4b5)". The "Directory Details" section is expanded and highlighted with a red border. Below this, there are tabs for "Apps & Services" and "Associated Snapshots". The "Access URL" section is partially visible at the bottom.

Directory type	Simple AD	Status	Active
Directory ID	d-956730d4b5	Status last updated	Fri Nov 14
Directory name	corp.example.com	Availability Zones	ap-northea:
NetBIOS name	CORP	VPC	vpc-a79d4e
Description		Subnets	subnet-ba9
DNS address	10.0.0.82, 10.0.1.228		
Directory size	Small		
Launch time	Fri Nov 14 18:01:20 GMT+900 2014		

Apps & Services | Associated Snapshots

Access URL

Create a public endpoint to access your AWS applications and the AWS Management Console. To provide access to users in your directory to AWS applications and the AWS Management Console, you must create an Access URL. [Learn more.](#)

https://[]_awsapps.com [Create Access URL](#)

スナップショットの管理

- デフォルトで日時のスナップショットによるバックアップを実行し、ポイントインタイムリカバリーが可能
 - 5日分のスナップショットが保存される
 - マニュアルでのスナップショットにも対応

Apps & Services Associated Snapshots

Create Snapshot Restore Delete  

[Create Snapshot]をクリック

Snapshot ID	Snapshot Name	Snapshot Created Date	Snapshot Type	Status
s-956730d440		Thu Nov 27 22:09:35 GMT+900 2014	Auto	Completed
s-956730d7b4		Fri Nov 28 22:52:11 GMT+900 2014	Auto	Completed
s-956730d2e5		Sat Nov 29 23:27:18 GMT+900 2014	Auto	Completed
s-956730dddb		Mon Dec 01 00:05:14 GMT+900 2014	Auto	Completed
s-956730d90f		Tue Dec 02 00:43:59 GMT+900 2014	Auto	Completed

DHCPオプションセットの作成

- VPC全体でディレクトリを参照できるようにするためには、DHCPオプションセットを作成してVPCに適用する

DHCP オプションセットの作成

DHCP(Dynamic Host Configuration Protocol)は、TCP/IP ネットワークのホストに設定情報を渡すための規格です。DHCP メッセージのオプションフィールドの内容は設定パラメータです。

ネームタグ **ネームタグを入力 (オプション)**

少なくとも次のいずれかの設定パラメータを指定してください

ドメイン名 **Directory Nameを入力**

ドメインネームサーバー **DNSアドレスを入力**

NTP サーバー

NetBIOS ネームサーバー

NetBIOS ノードの種類

キャンセル **作成をクリック**

Amazon EC2 Simple Systems Manager (SSM)

- 実行中のインスタンスの設定を管理するサービス
 - Windowsインスタンスのみサポート
 - US East (N. Virginia) /US West(Oregon)/EU(Ireland)リージョンで利用可能
- インスタンスの準備
 - SSM APIを使用するアクセス権限の付与
 - 最新のEC2 Configのインストール
 - JSONファイルの作成

Windowsインスタンスのドメインへの参加

- インスタンスの起動時にドメインを指定して自動的に参加させることが可能

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage, and more.

Number of instances	<input type="text" value="1"/>
Purchasing option	<input type="checkbox"/> Request Spot Instances
Network	<input type="text" value="vpc-7f2aeb1a (172.16.0.0/16)"/> Create new VPC
Subnet	<input type="text" value="subnet-27f6e561(172.16.2.0/24) us-west-2c"/> Create new subnet 250 IP Addresses available
Auto-assign Public IP	<input type="text" value="Enable"/>
Domain join directory	<input type="text" value="corp.gentaw.com (d-92673260bb)"/> Create new Directory
IAM role	<input type="text" value="allow-all-ssm"/> Create new IAM role
Shutdown behavior	<input type="text" value="Stop"/>
Enable termination protection	<input type="checkbox"/> Protect against accidental termination
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring

1. [Enable]に設定

2. Directory Serviceドメインを指定

3. SSMへのアクセスを有効にしたロールを指定

SSMによるドメインへの参加 (1/2)

- 設定ドキュメントにディレクトリID、ドメイン名およびIPアドレスを指定してファイルを.jsonで保存

```
{
  "schemaVersion": "1.0",
  "description": "Sample configuration to join an instance to a domain",
  "runtimeConfig": {
    "aws:domainJoin": {
      "properties": {
        "directoryId": "d-1234567890",
        "directoryName": "corp.example.com",
        "dnsIpAddresses": [
          "198.51.100.1",
          "198.51.100.2"
        ]
      }
    }
  }
}
```

SSMによるドメインへの参加(2/2)

- 保存したJSONファイルから設定ドキュメントを作成

```
PS C:\> $doc = Get-Content C:\temp\myconfigfile.json | Out-String
PS C:\> New-SSMDocument -Content $doc -Name "My_Custom_Config_File"
```

- EC2インスタンスを起動

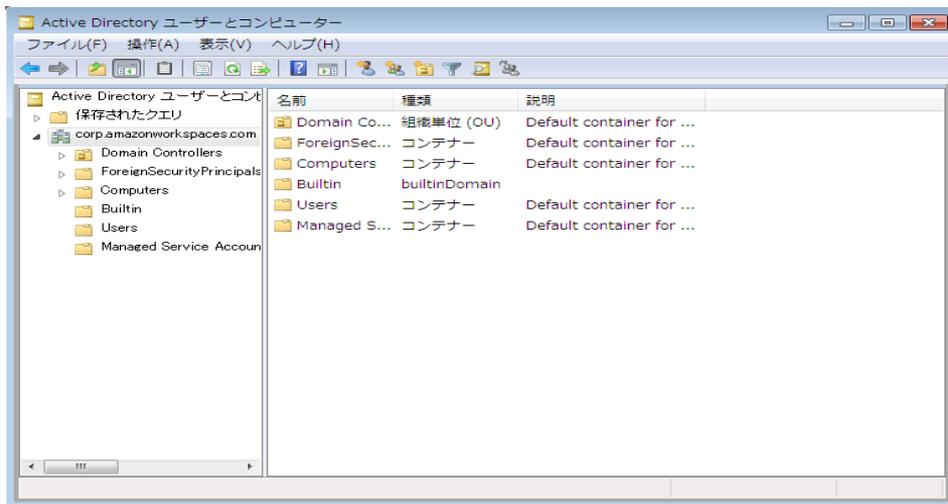
```
PS C:\> New-EC2Instance -ImageId ami-1a2b3c4d -SubnetId subnet-33cc44dd -
KeyName my-key-pair -InstanceType m1.large -InstanceProfile_Id
MyInstanceProfile -associatePublicIp $true
```

- 設定ドキュメントをインスタンスに関連付け

```
PS C:\> New-SSMAssociation -InstanceId i-11aa22bb -Name
"My_Custom_Config_File"
```

ユーザーとコンピュータの管理

- ドメインに参加させたEC2インスタンスに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`



Active DirectoryからSimple ADへの移行

- csvdeツールを使用するためにSimple ADに参加したWindowsインスタンスにAD DSツールをインストール

```
PS C:\> Install-WindowsFeature RSAT-ADDS-Tools
```

- 既存のActive DirectoryからIDのエクスポート

```
PS C:\> csvde -f users.csv -l "DN, objectclass, objectcategory, givenName, sn, name, samAccountName, displayname" -r "&(objectClass=user)(objectCategory=person)"
```

- Simple ADへのIDのインポート

```
PS C:\> csvde -i -f .\users.csv
```

Linuxインスタンスのドメインへの参加

- 必要なパッケージをAmazon Linuxインスタンスにインストール

```
$ sudo yum -y install sssd realmd krb5-workstation
```

- インスタンスのドメインへの参加

```
$ sudo realm join -U administrator@corp.example.com corp.example.com --  
verbose
```

- SSHサービスでパスワード認証を許可

```
$ sudo vi /etc/ssh/sshd_config  
PasswordAuthentication yes
```

- SSSDサービスを開始

```
$ sudo service sssd start
```

インスタンスへのSSHログインの追加

- ドメイン管理者をsudoersリストに追加

```
$ sudo visudo -f /etc/sudoers
```

```
## Add the domain administrators group from the corp.example.com domain.
```

```
%Domain\ Admins@corp.example.com ALL=(ALL:ALL) ALL
```

- インスタンスにログインできるユーザーとグループの追加

```
$ sudo realm permit jonhdoe@corp.example.com
```

```
$ sudo realm permit --groups testgroup@corp.example.com
```

Linuxインスタンスからのユーザー管理(1/2)

- Amazon Linuxに必要なパッケージをインストール

```
$ sudo yum -y install samba-common openldap-clients adcli
```

- ユーザーの作成

```
$ net ads user ADD johndoe Password123! -C "John Doe" -S corp.example.com
```

- ユーザーオブジェクトのuserAccountControlを512に設定

```
$ sudo vi uac.ldif
```

```
dn: CN= johndoe ,CN=Users,DC=corp,DC=example,DC=com
```

```
changetype: modify
```

```
replace: userAccountControl
```

```
userAccountControl: 512
```

Linuxインスタンスからのユーザー管理 (2/2)

- グループの作成

```
$ adcli create-group testgroup -v -D corp.example.com -z "This is a test group."
```

- グループのメンバーとしてユーザーを追加

```
$ adcli add-member testgroup johndoe -v -D corp.example.com
```

- 全ユーザーの検索

```
$ net ads search '(objectCategory=user)' -S corp.example.com
```

- 特定のオブジェクトの検索

```
$ net ads search '(sAMAccountName=johndoe)' -S corp.example.com
```

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



PowerShellスクリプトによるSimple ADの作成

#ディレクトリ名とサイズの設定

```
$directoryname = "corp.example.com"
```

```
$directorysize = "small"
```

#管理者パスワードの取得

```
$password = (Get-Credential -Credential Administrator).Password
```

#VPC IDの取得

```
$vpcname = "Examples"
```

```
$vpcId = (Get-EC2Vpc -Filter @{Name="Tag:Name"; Values=$vpcname}).VpcId
```

#Simple ADディレクトリの作成

```
New-DSDirectory -Name $directoryname -Password $password -Size $directorysize -  
VpcSettings_SubnetId $subnetId -VpcSettings_VpcId $vpcId
```

#作成したSimple ADディレクトリの確認

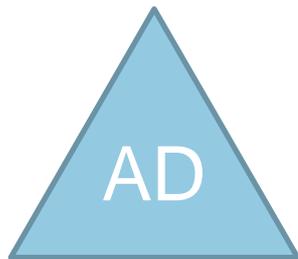
```
Get-DSDirectory | Where-Object -FilterScript {$_ .Name -eq $directoryname}
```

Simple ADの制限事項

- Active Directoryの互換性
 - Windows Server 2008 R2機能レベル
- サポートされない機能
 - Windows PowerShellコマンドレット
 - スキーマ拡張
 - ドメイン-フォレストの信頼関係
 - ドメインコントローラーの追加
 - LDAP-S

AWS Management Consoleとの認証フェデレーション

- SAMLインフラのセットアップと管理
- 手動でユーザーにロールをアサイン
- より簡単にフェデレーションをセットアップ可能に ←NEW !



AWS Identity and Access Management (IAM)

- AWS操作をよりセキュアに行うための認証・認可の仕組み
- AWS利用者の認証と、アクセスポリシーを管理
 - AWS操作のためのグループ・ユーザー・ロールの作成が可能
 - グループ、ユーザーごとに、実行出来る操作を規定できる
 - ユーザーごとに認証情報の設定が可能



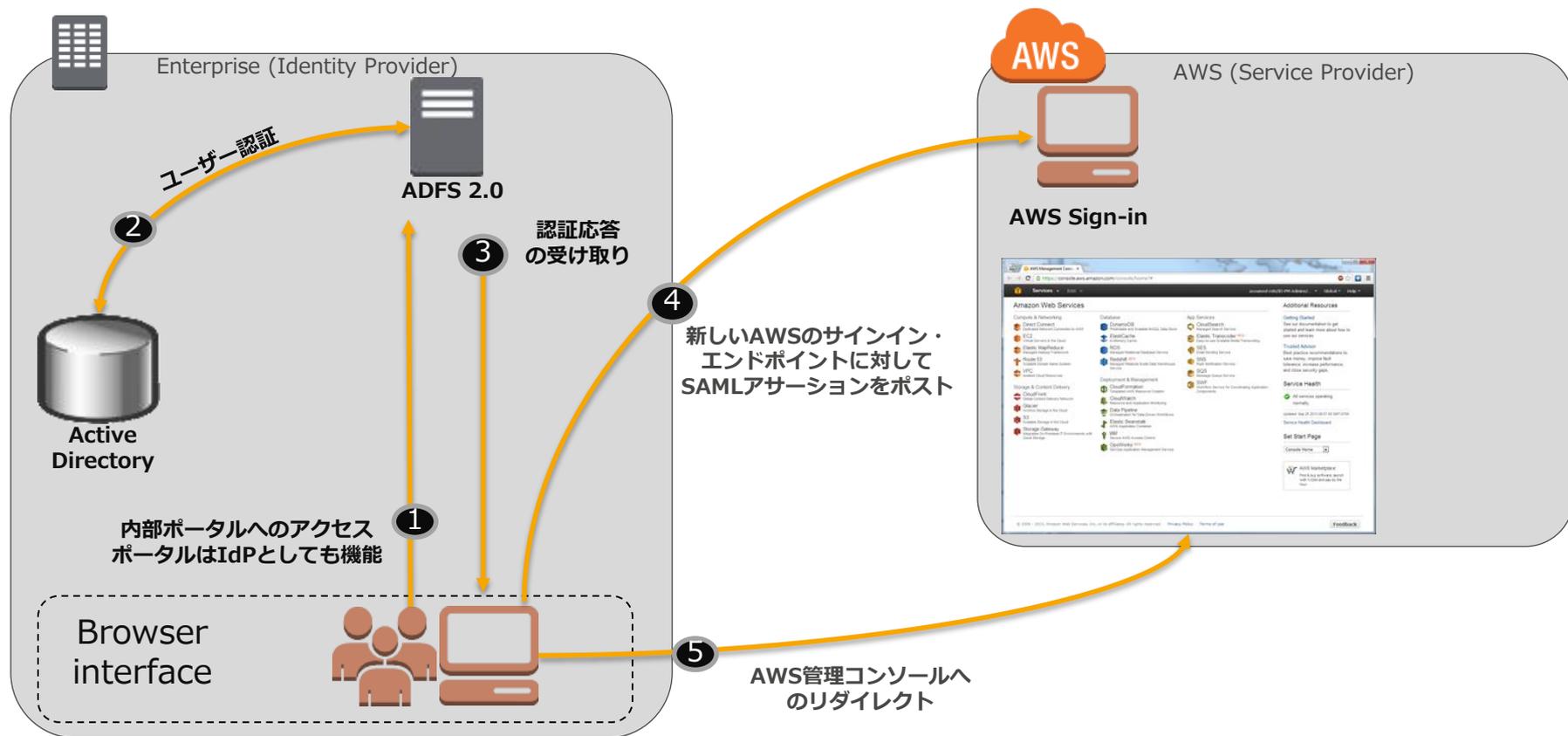
SAML 2.0によるSSOフェデレーション

- Security Assertion Markup Language (SAML) のサポート
- AWSリソースへのアクセスにSAMLを利用した既存のID管理ソフトウェアを利用 (ADFS, Shibboleth etc)
- AWS管理コンソールへのSSOにも利用可能
- 新しいassumeRoleWithSAML APIによりAPIフェデレーション実施

Active Directory フェデレーションサービス (ADFS)

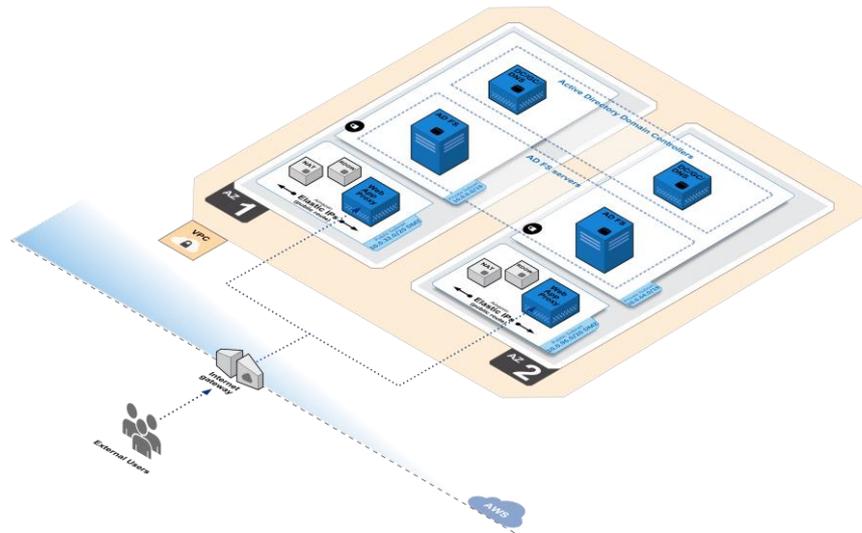
- セキュリティで保護されたID連携（フェデレーション）とWebシングルサインオン（SSO）を提供
- AD DS/AD LDSで認証されたユーザーに対してセキュリティトークンを発行（SAML 1.1/2.0）
- Office 365やGoogle Appsへのシングルサインオン（SSO）にも利用される
 - http://community.office365.com/ja-jp/b/office_365_community_blog/archive/2012/01/14/adfs-in-office-365.aspx

ADFSによるConsole Federationの動作



ADFS on AWS

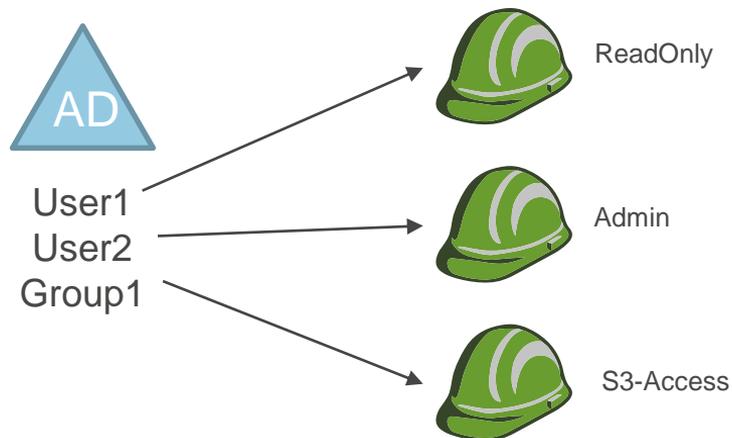
- Web Application ProxyとActive Directory Federation ServicesのAWS上でのデプロイに関するリファレンスとCloudFormationテンプレート
- 新しいVPCへのデプロイと既存のVPCとAD DSインフラストラクチャへのデプロイをサポート
 - \$5.50/時
 - 展開時間：約1時間半



AD Connectorによるフェデレーション

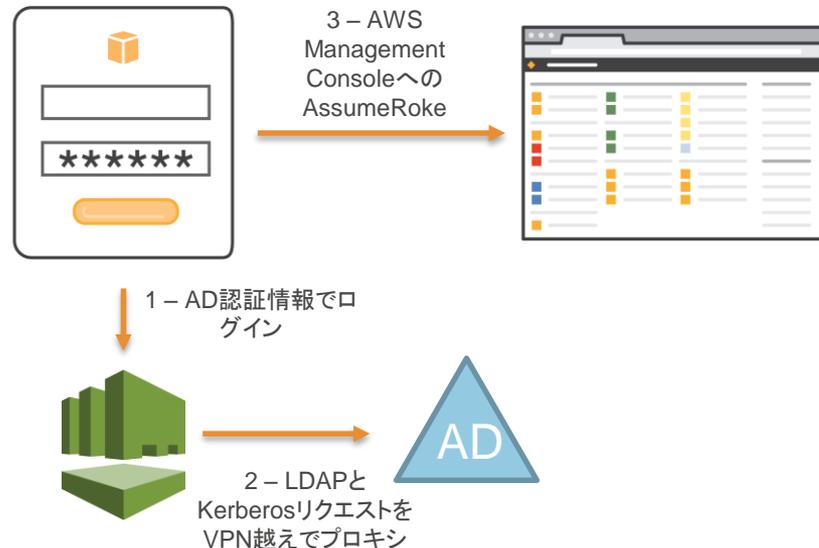
1) IAMロールをADユーザーにアサイン

AWS Directory Serviceコンソール経由



2) ADユーザーはaccess URL経由でログイン

mycompany.awsapps.com/console



AD Connectorの作成 (1/2)

1. [Directory DNS] を入力

Create AD Connector

AD Connector is a directory gateway to your on-premises Microsoft Active Directory. It enables users in your on-premises Active Directory to access Amazon WorkSpaces, Amazon WorkDocs, and Amazon WorkMail. Administrators can also manage AWS resources using AWS Management Console. See [How to setup AD Connector](#) or [Instructions on setting up a VPN Network](#) for more information.

Directory DNS

NetBIOS name

Connector account username

Connector account password

Confirm password

DNS address

Description

Directory size Small

Large

Large directories cost more. [Learn more.](#)

2. [NetBIOS name] を入力
(オプション)

3. [Connector account username] を入力

4. [Connector account password] を入力

5. [DNS address] を入力

6. [Small] を選択

AD Connectorの作成 (2/2)

- 既存のVPCを選択、または新規にVPCとSubnetを作成

VPC Details

1. [VPC] を選択

To set up a directory you need to select a VPC and two subnets, each in a different Availability Zone. This ensures that your directory is isolated and reachable only by your instances. Directory servers in two Availability Zones ensure high availability.

VPC

vpc-a79d4ece (10.0.0.0/16)

2. 2つの [Subnets] を選択

Subnets

10.0.0.0/24 (ap-northeast-1a)

10.0.1.0/24 (ap-northeast-1c)

3. [Next Step]をクリック

Cancel

Previous

Next Step

Access URLの設定

- Access URLはAWSアプリケーションとの連携のために利用される
 - 設定するURLはグローバルでユニーク（一意）である必要がある
 - 一度設定すると変更・削除はできない

Apps & Services Associated Snapshots

Access URL

Create a public endpoint to access your AWS applications and the AWS Management Console. To provide access to users in your directory to AWS applications and the AWS Management Console, you must create an Access URL. **Once you create an Access URL for this directory, it cannot be changed.** [Learn more.](#)

https://aws-cloud| x awsapps.com [Create Access URL](#)

Apps & Services

1. Access URLを設定 **2. [Create Access URL]をクリック**

Select AWS applications and services you want to enable for this directory. This will enable user accounts in this directory to authenticate to the selected applications. The application level access policies will control what the users will be able to do. [Learn more.](#)

Amazon WorkSpaces	Not Enabled	Go to WorkSpaces	
Amazon WorkDocs	Not Enabled	Go to WorkDocs	
AWS Management Console	Not Enabled	Manage Access	

AWS Management Console連携の設定

- 作成したAccess URLを利用したAWS Management Consoleへのアクセスを設定

The screenshot shows the 'Apps & Services' tab in the AWS Management Console. Under the 'Access URL' section, the current URL is 'aws-cloud.awsapps.com'. In the 'Apps & Services' list, 'AWS Management Console' is shown as 'Not Enabled' with a 'Manage Access' button highlighted by a red box. A modal dialog box titled 'Enable AWS Management Console' is open, asking if the user wants to enable directory users to access the console. The 'Enable Access' button in the dialog is also highlighted with a red box.

Apps & Services | Associated Snapshots

Access URL

Current Access URL: aws-cloud.awsapps.com

Apps & Services

Select AWS applications and services you want to enable for this directory. This will enable user access. Application level access policies will control what the users will be able to do. [Learn more](#).

Amazon WorkSpaces	Enabled	Go to WorkSpaces	?
Amazon Zocalo	Not Enabled	Go to Zocalo	?
AWS Management Console	Not Enabled	Manage Access	?

Enable AWS Management Console

Would you like to enable directory users to access AWS Management Console to manage AWS resources using their directory credentials?

You'll need to perform additional setup to enable specific users to access AWS Management Console.

[Cancel](#) [Enable Access](#)

1. Manage Accessを選択

2. [Enable Access]をクリック

ユーザー/グループとIAMロールのマッピング

- 適切な権限を設定するために、ユーザー/グループとIAMロールのマッピングを行う
 - この例ではEC2ReadOnlyロールとPowerUserロールにそれぞれグループとユーザーを割り当て

Directories > aws-cloud.amazonworkspaces.com (d-956731f3af) > AWS Management Console Access

New Role Remove Role  

[New Role]をクリック

Role	Policy
<input type="checkbox"/> EC2ReadOnly	View Role in IAM
Enabled Users 0	Enabled Groups 1 Users
<input type="checkbox"/> PowerUser	View Role in IAM
Enabled Users 1 gentaw	Enabled Groups 0

AWS Management Consoleへのシングルサインオン (SSO)

- `https://<access_url>.awsapps.com/console/`にアクセスしてログオンすることによりManagement ConsoleへのWebベースでのシングルサインオン (SSO) が可能



The screenshot shows the AWS Management Console login interface. At the top is the Amazon Web Services logo with the text "amazon web services management console". Below the logo is the instruction "次の情報を使用してログインしてください" (Please log in using the following information) and "aws-cloud 認証情報" (aws-cloud authentication information). The form contains two input fields: "ユーザー名" (Username) with the value "gentaw" and "パスワード" (Password) with masked characters. A yellow "サインイン" (Sign In) button is positioned below the password field. At the bottom of the form is a blue link that says "パスワードを忘れた場合" (Forgot your password?).

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

(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。

MFAの設定

- [Multi-Factor Authentication]タブにRADIUSサーバーの情報を入力して[Update Directory]を選択

Apps & Services Connector Account **Multi-Factor Authentication**

AD Connector supports Multi-Factor Authentication by integrating with your existing on-premises RADIUS Multi-Factor Authentication infrastructure. [Learn more.](#)

RADIUS Status Completed

Enable Multi-Factor Authentication	<input checked="" type="checkbox"/>	チェック
RADIUS server IP address(es)	<input type="text" value="10.0.0.25"/>	RADIUSサーバーのIPアドレス
Port	<input type="text" value="1812"/>	ポート番号
Shared secret code	<input type="text" value="....."/>	パスワード
Confirm shared secret code	<input type="text" value="....."/>	パスワード (確認)
Protocol	<input type="text" value="PAP"/>	プロトコル
Server timeout (in seconds)	<input type="text" value="10"/>	タイムアウト (秒)
Max retries	<input type="text" value="3"/>	リトライ回数

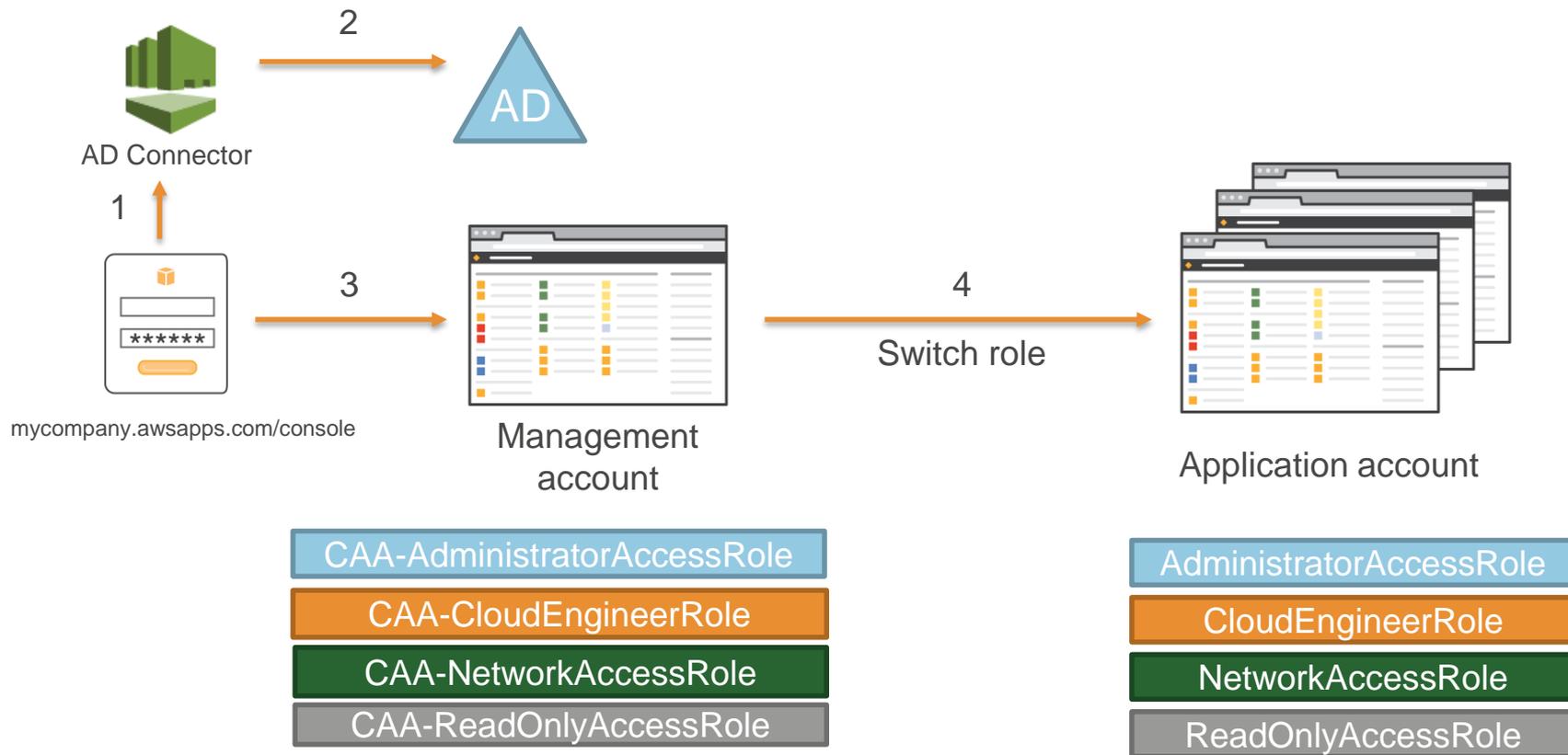
[Update Directory]を選択

Update Directory



amazon
aws services

AD Connectorによるクロスアカウントアクセス



AWSアプリケーションとの連携

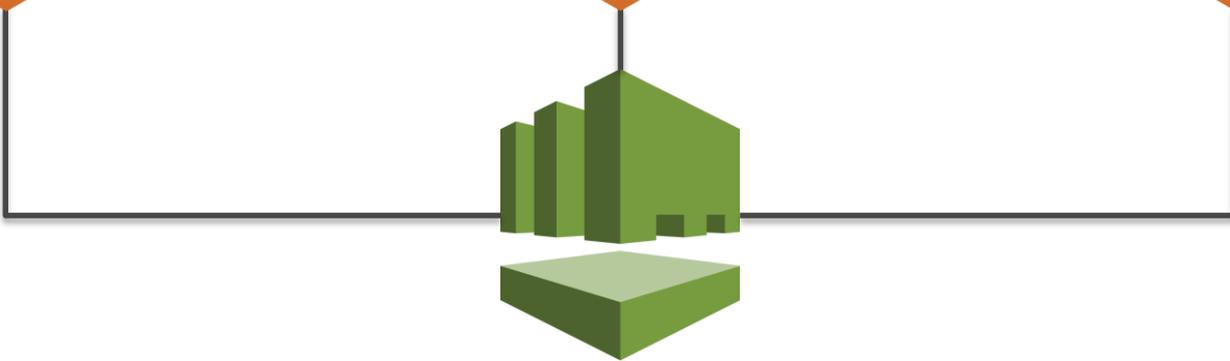
- WorkSpaces



- WorkDocs



- WorkMail



Simple AD/AD Connector

AWSアプリケーション連携の設定

- App & Servicesから各サービスのコンソールにリダイレクトされる

The screenshot shows the AWS IAM console interface. At the top, there are two tabs: 'Apps & Services' (selected) and 'Associated Snapshots'. Below the tabs, the 'Access URL' section shows the current URL as 'aws-cloud.awsapps.com' and a 'Disable' button for Single Sign-On. The 'Apps & Services' section lists several services as 'Enabled', with a 'Go to WorkSpaces' button highlighted by a red box. To the right, a 'Manage Amazon WorkSpaces Access' dialog box is open, asking 'Would you like to proceed?' with 'Cancel' and 'Continue' buttons. The 'Continue' button is also highlighted by a red box. Below the screenshot, two red numbered instructions are provided: '1. Go to WorkSpacesを選択' and '2. [Continue]をクリック'.

Apps & Services Associated Snapshots

Access URL

Current Access URL: aws-cloud.awsapps.com

Single Sign-On is enabled. [Disable](#)

[Learn More](#) about Single Sign-On.

Apps & Services

Select AWS applications and services you want to enable for this directory. This will enable user access to. [Learn more](#).

- Amazon WorkSpaces Enabled [Go to WorkSpaces](#) ⓘ
- Amazon WorkDocs Enabled [Go to WorkDocs](#) ⓘ
- AWS Management Console Enabled [Manage Access](#) ⓘ

Manage Amazon WorkSpaces Access

You will be redirected to the Amazon WorkSpaces console to manage access for this directory.

Would you like to proceed?

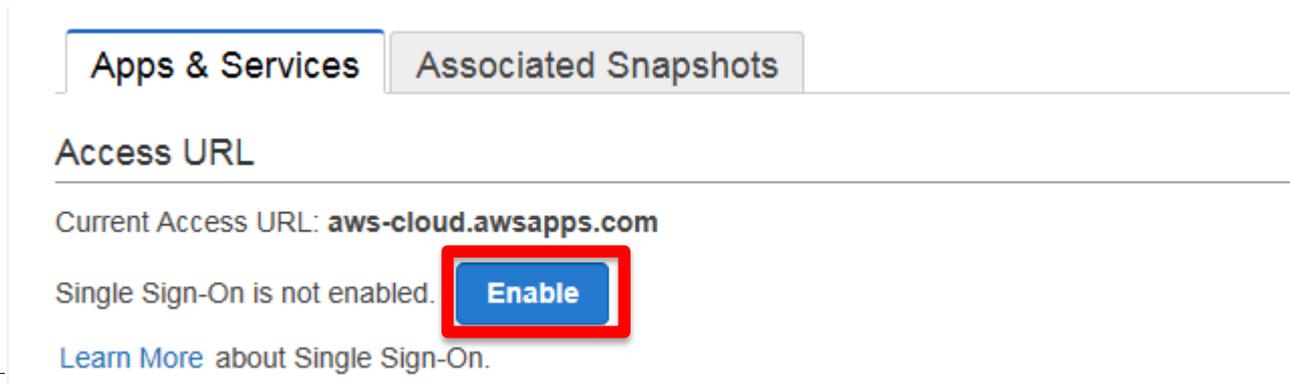
[Cancel](#) [Continue](#)

1. Go to WorkSpacesを選択

2. [Continue]をクリック

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



Apps & Services Associated Snapshots

Access URL

Current Access URL: **aws-cloud.awsapps.com**

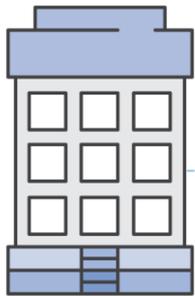
Single Sign-On is not enabled. **Enable**

[Learn More](#) about Single Sign-On.

AWS Directory Service

Microsoft AD

Windows Server 2012 R2



On-premises



既存のオンプレミス環境との信頼関係
AWSとの新想を拓く

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
- Microsoft AD
 - フルマネージドのディレクトリサービス
 - Windows Server 2012 R2がベース
 - 既存ドメインとの信頼関係をサポート

Microsoft ADの作成

- ドメインと管理者アカウントを作成する
 - Directory DNS
 - NetBIOS Name
 - Admin 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

ディレクトリを作成する

- アジアパシフィック（東京）リージョンに変更してディレクトリを作成します。

1. リージョン選択メニュー

The screenshot shows the AWS Directory Service console interface. At the top, there is a navigation bar with 'Services' and 'Edit' dropdowns on the left, and the user name 'Genta Watanabe', the current region 'Tokyo', and 'Support' on the right. A dropdown menu is open for the 'Tokyo' region, listing various AWS regions: US East (N. Virginia), US West (Oregon), US West (N. California), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), **Asia Pacific (Tokyo)**, Asia Pacific (Sydney), and South America (São Paulo). The 'Asia Pacific (Tokyo)' option is highlighted with a red box. In the main content area, the text 'AWS Directory Service' is visible, along with a description: 'AWS Directory Service enables you to use your corporate access AWS services, and simplifies deployment of Microsoft Windows applications in the AWS'. A blue button labeled 'Get Started Now' is also visible, with a red box around it. Red arrows point from the text annotations to the 'Tokyo' dropdown and the 'Get Started Now' button.

2. [Asia Pacific (Tokyo)] を選択

3. [Get Started Now] を選択



ディレクトリタイプの選択

- Create Microsoft ADを選択

Set up a directory

Step 1: Choose directory type

Step 2: Directory details

Step 3: Review

Choose directory type **[Create Microsoft AD] を選択**

AWS provides three Directory Service options. Choose from the list below to get started.

Create a new directory

-  **Microsoft AD**
Microsoft AD provides many Microsoft Active Directory features including adding trust relationships with on-premises domains. It is based on Microsoft Active Directory in Windows Server 2012 R2. [Learn more.](#)
Best for enterprise workloads requiring up to 50,000 users. [Create Microsoft AD](#)
-  **Simple AD**
A Microsoft Active-Directory compatible directory powered by Samba 4 that provides a subset of Microsoft Active Directory features. [Learn more.](#)
Best for workloads requiring up to 5,000 users. [Create Simple AD](#)

Extend your existing AD

Requires a hardware virtual private network (VPN) or AWS Direct Connect between your datacenter and your VPC in the AWS cloud.

-  **AD Connector**
AD Connector is a gateway that sends to your existing on-premises Microsoft Active Directory with AWS services. No directory information is replicated into or cached in AWS. [Learn more.](#) [Create AD Connector](#)

Microsoft ADの作成 (1/2)

AWS サービス 編集 Genta Watanabe 東京 サポート

Set up a directory

Step 1: Choose directory type
Step 2: Directory details
Step 3: Review

Directory details

A managed Microsoft Active Directory domain based on Windows Server 2012 R2. [Learn more](#).

Directory type: Microsoft AD

Directory DNS*: corp.example.com ⓘ

NetBIOS name: CORP ⓘ

Default administrative user: Admin ⓘ

Admin password*: ⓘ

Confirm password*: ⓘ

Description: Optional ⓘ

VPC Details

To set up a directory you need to select a VPC and two subnets, each in a different Availability Zone. This ensures that your directory is isolated and reachable only by your instances.

VPC*: Select a VPC... ⓘ

[Create a new VPC](#) ↻

1. [Directory DNS] を入力

2. [NetBIOS name] を入力 (オプション)

3. [Admin password] を入力

Microsoft ADの作成 (2/2)

- 既存のVPCを選択、または新規にVPCとSubnetを作成

VPC Details

1. [VPC] を選択

To set up a directory you need to select a VPC and two subnets, each in a different Availability Zone. This ensures that your directory is isolated and reachable only by your instances. Directory servers in two Availability Zones ensure high availability.

VPC vpc-a79d4ece (10.0.0.0/16)  

[Create a new VPC](#) 

2. 2つの [Subnets] を選択

Subnets 10.0.0.0/24 (ap-northeast-1a)  

10.0.1.0/24 (ap-northeast-1c) 

[Create a new Subnet](#) 

3. [Next Step]をクリック

Cancel

Previous

Next Step

入力内容の確認



AWS ▾

サービス ▾

編集 ▾

Genta Watanabe ▾

東京 ▾

サポート ▾

Set up a directory

[Step 1: Choose directory type](#)

[Step 2: Directory details](#)

Step 3: Review

Review

The configuration details for your directory.

Directory type Microsoft AD
Directory name corp.example.com
NetBIOS name CORP

Description

VPC details

The VPC details for your directory.

VPC vpc-75b76710
Subnets 10.0.0.0/24 (ap-northeast-1a) and 10.0.1.0/24 (ap-northeast-1c)

[Create Microsoft AD]をクリック

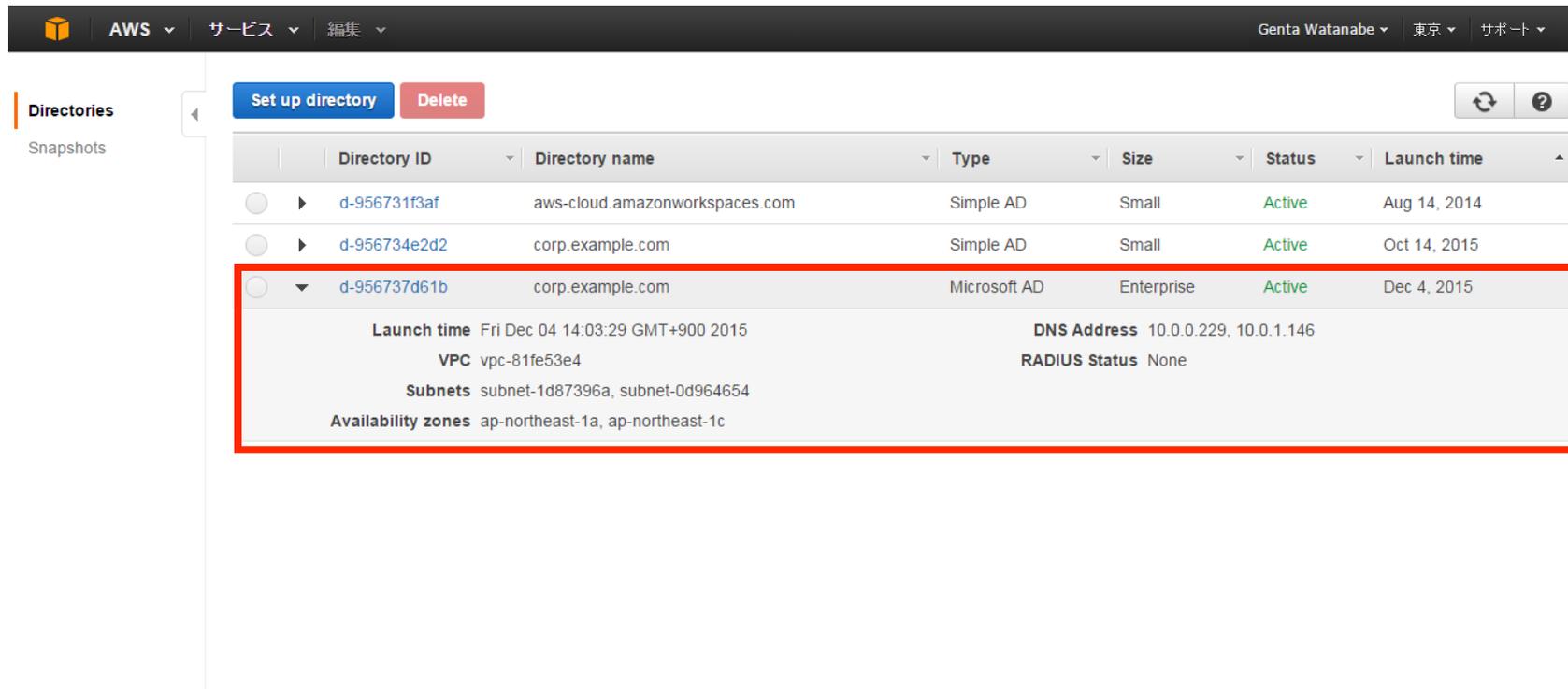
Cancel

Previous

Create Microsoft AD

Microsoft ADの確認 (1/2)

- [Status]が[Active]になれば作成完了



The screenshot shows the AWS IAM console interface for Directory Service. The top navigation bar includes the AWS logo, 'AWS', 'サービス', and '編集' menus, along with user information 'Genta Watanabe', '東京', and 'サポート'. The left sidebar shows 'Directories' and 'Snapshots'. The main content area has 'Set up directory' and 'Delete' buttons. A table lists three directory instances:

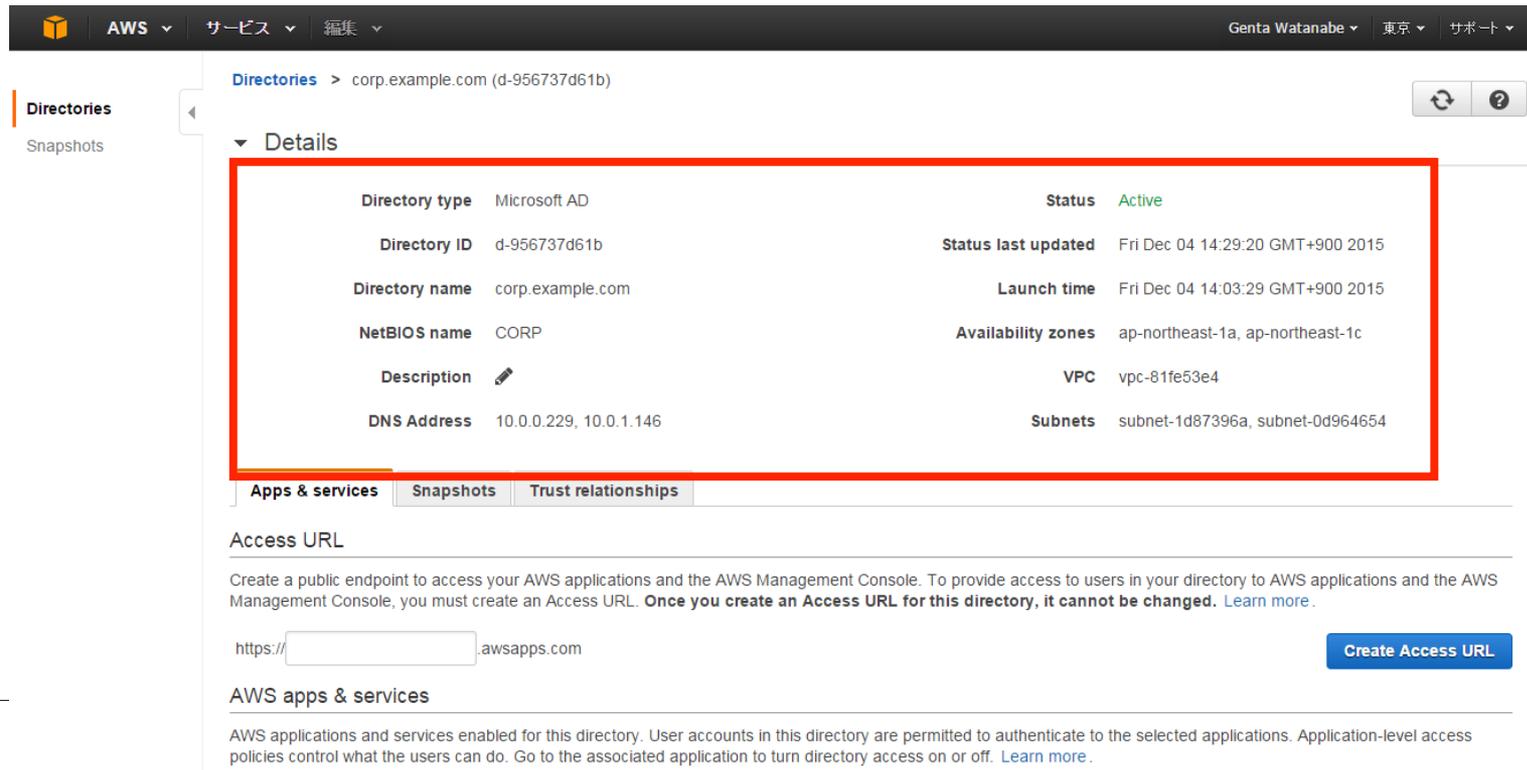
Directory ID	Directory name	Type	Size	Status	Launch time
d-956731f3af	aws-cloud.amazonworkspaces.com	Simple AD	Small	Active	Aug 14, 2014
d-956734e2d2	corp.example.com	Simple AD	Small	Active	Oct 14, 2015
d-956737d61b	corp.example.com	Microsoft AD	Enterprise	Active	Dec 4, 2015

The instance 'd-956737d61b' is expanded to show configuration details:

- Launch time:** Fri Dec 04 14:03:29 GMT+900 2015
- DNS Address:** 10.0.0.229, 10.0.1.146
- VPC:** vpc-81fe53e4
- RADIUS Status:** None
- Subnets:** subnet-1d87396a, subnet-0d964654
- Availability zones:** ap-northeast-1a, ap-northeast-1c

Microsoft ADの確認 (2/2)

- [Directory ID]をクリックして[Details]を確認



The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, 'AWS', 'サービス', '編集', and user information 'Genta Watanabe', '東京', and 'サポート'. The left sidebar shows 'Directories' and 'Snapshots'. The main content area is titled 'Directories > corp.example.com (d-956737d61b)'. Below this, the 'Details' section is expanded, showing a table of directory information. The table is highlighted with a red border. Below the table are tabs for 'Apps & services', 'Snapshots', and 'Trust relationships'. The 'Access URL' section provides instructions on how to create an Access URL and includes a text input field and a 'Create Access URL' button. The 'AWS apps & services' section provides information on enabling directory access for applications.

Directory type	Microsoft AD	Status	Active
Directory ID	d-956737d61b	Status last updated	Fri Dec 04 14:29:20 GMT+900 2015
Directory name	corp.example.com	Launch time	Fri Dec 04 14:03:29 GMT+900 2015
NetBIOS name	CORP	Availability zones	ap-northeast-1a, ap-northeast-1c
Description		VPC	vpc-81fe53e4
DNS Address	10.0.0.229, 10.0.1.146	Subnets	subnet-1d87396a, subnet-0d964654

Access URL

Create a public endpoint to access your AWS applications and the AWS Management Console. To provide access to users in your directory to AWS applications and the AWS Management Console, you must create an Access URL. **Once you create an Access URL for this directory, it cannot be changed.** [Learn more.](#)

https://.awsapps.com [Create Access URL](#)

AWS apps & services

AWS applications and services enabled for this directory. User accounts in this directory are permitted to authenticate to the selected applications. Application-level access policies control what the users can do. Go to the associated application to turn directory access on or off. [Learn more.](#)

信頼関係の追加

- ドメイン/フォレスト間の信頼関係を設定することが可能

Add a trust relationship ×

Create a trust relationship (forest trust) to another domain. [Learn more.](#)

Fully Qualified Domain Name (FQDN) of trusted domain **信頼関係相手のドメイン**

Trust password **接続用のパスワード**

Trust direction **一方向または双方向の信頼関係を選択**

管理アカウント権限

- Microsoft ADのadminアカウントはOUに対して以下の権限を持つ
 - ユーザー、グループ、およびコンピュータの作成、更新、削除
 - ファイル/プリントサーバーなどのリソースのドメインへの追加、ユーザーやOU内のグループにリソースに対するアクセス権の付与
 - 追加のOUおよびコンテナの作成
 - 権限の委譲
 - グループポリシーの作成とリンク
 - Active Directoryごみ箱からの削除されたオブジェクトのリストア
 - Active Directory WebサービスからADとDNS Windows PowerShellモジュールの実行
- またドメイン単位で以下の権限を持つ
 - DNS構成の管理（レコード、ゾーンおよびフォワーダーの追加、削除または更新）
 - DNSイベントログの参照
 - セキュリティイベントログの参照

スキーマの拡張

- ExchangeやLyncなどスキーマ拡張が必要なアプリケーションを動作させるには、フィードバックフォームからSubmitする

AWS Account Number*

Applications

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Lync 2013
- Microsoft Skype for Business Server 2015
- Microsoft System Center 2012
- Microsoft System Center 2016
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013
- Other (Please specify the applications in the text box below)

Additional Comments (optional)

Submit

Simple ADとの比較

- Active Directoryの互換性
 - Windows Server 2012 R2機能レベル
- あらたにサポートされる機能
 - ドメイン-フォレストの信頼関係
 - Active Directory管理センター
 - Windows PowerShellコマンドレット
 - Active Directoryのごみ箱
 - スキーマの拡張など

ディレクトリのサイズ

- Simple AD

- **Small:**最大で500ユーザー（2,000のユーザー、コンピュータ、グループ、その他のオブジェクト）
- **Large:**最大で5,000ユーザー（20,000のユーザー、コンピュータ、グループ、その他のオブジェクト）

- AD Connector

- **Small:**最大で500ユーザー
- **Large:**最大で5,000ユーザー

- Microsoft AD

- **Enterprise:**最大で50,000ユーザー（200,000のユーザー、コンピュータ、グループ、その他のオブジェクト）

AWS Directory Serviceの料金

- 作成したディレクトリのタイプとサイズにもとづいて課金

アジアパシフィック（東京）

ディレクトリのタイプ	サイズ	時間料金
Microsoft AD	Enterprise	0.445 USD (324.85 USD/月*)
AD Connector	Small	0.08 USD (58.40 USD/月*)
AD Connector	Large	0.24 USD (175.20 USD/月*)
Simple AD	Small	0.08 USD (58.40 USD/月*)
Simple AD	Large	0.24 USD (175.20 USD/月*)

* 月ごとの利用料金は、1 か月を 730 時間として算出しています。

<https://aws.amazon.com/jp/directoryservice/pricing/>

無料利用枠

- 無料トライアル

- ディレクトリをはじめて作成する場合は750時間分のSmallディレクトリ（Simple ADまたはAD Connector）またはMicrosoft AD（Enterprise Edition）が無料
- ディレクトリの作成後30日間で無効になる

- Amazon WorkSpaces、Amazon WorkDocs、Amazon WorkMail

- Smallディレクトリでは1アクティブユーザー、Largeディレクトリでは100アクティブユーザーが存在していればその月のAWS Directory Serviceの料金は無料
- Microsoft ADには無料枠なし

利用可能なリージョン

- 利用可能なAWSリージョン:
 - US East (N.Virginia)
 - US West (Oregon)
 - EU (Ireland)
 - Asia Pacific (Sydney)
 - Asia Pacific (Singapore) – Simple ADおよびAD Connectorのみ
 - Asia Pacific (Tokyo)
- その他のリージョンは今後予定

まとめ

- AWS Directory Serviceはフルマネージドのディレクトリサービスでスタンドアロンのディレクトリの作成、または既存のディレクトリへの接続が可能
- Active DirectoryとAWS Management Consoleへのフェデレーションを提供
- AWSアプリケーション（Amazon WorkSpaces、Amazon WorkDocs、Amazon WorkMail）との連携が可能

参考資料

- AWS Directory Service Administration Guide
 - http://docs.aws.amazon.com/directoryservice/latest/adminguide/what_is.html
- AWS Directory Serviceのよくある質問
 - <http://aws.amazon.com/jp/directoryservice/faqs/>
- 料金表
 - <http://aws.amazon.com/jp/directoryservice/pricing/>

Q&A



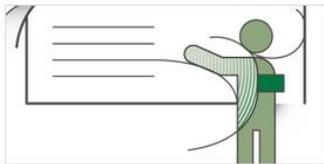
Webinar資料の配置場所

- AWS クラウドサービス活用資料集

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

日本語資料のカテゴリ一覧

本資料集では、この利便性を皆様に活用していただけるよう、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。



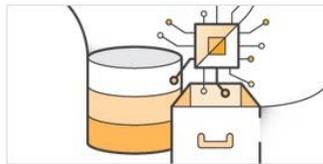
トレーニング資料

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をいたします。



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ください。参考資料をご覧ください。



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覧ください。

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初心者向けWebinar



- AWSをこれからご使用になる向けのソリューションカットのオンラインセミナー
- 申し込みサイト
 - <http://aws.amazon.com/jp/about-aws/events/>

次回のAWS Black Belt Tech Webinar は、

10月28日 18:00～

AWS CodeCommit & AWS CodePipeline & AWS CodeDeploy



ご参加ありがとうございました。

