

AWS Management Console

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
プロフェッショナルサービス コンサルタント 千葉 悠貴

アジェンダ

- AWS Management Consoleの概要
- セキュリティベストプラクティス
- Management Consoleの管理方法
- その他のAWS管理ポータル
- まとめ

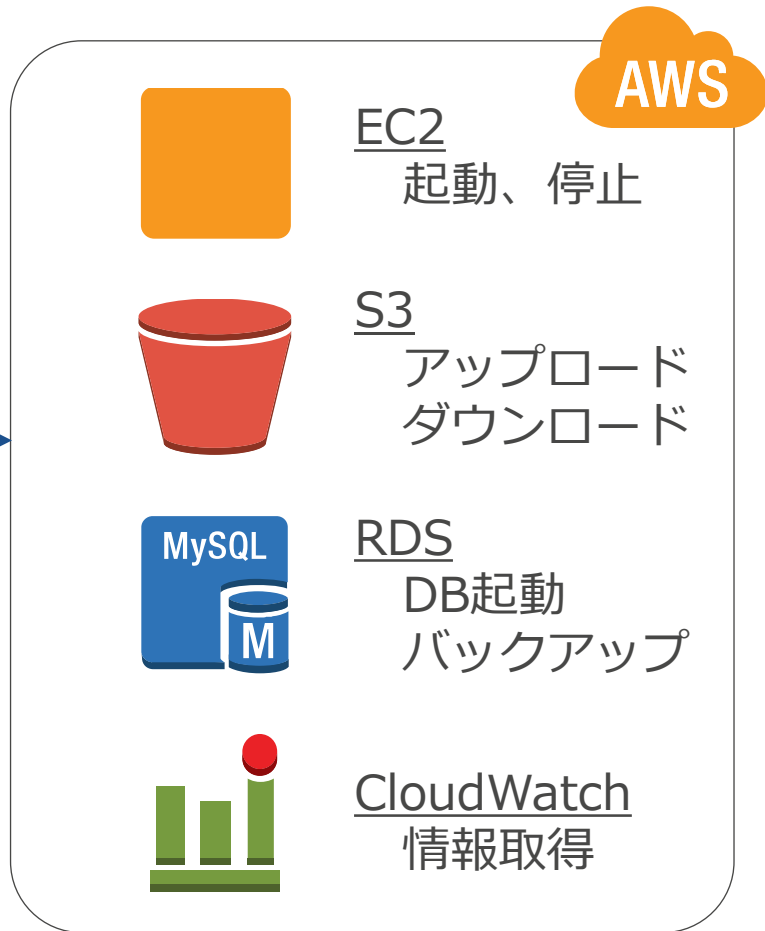
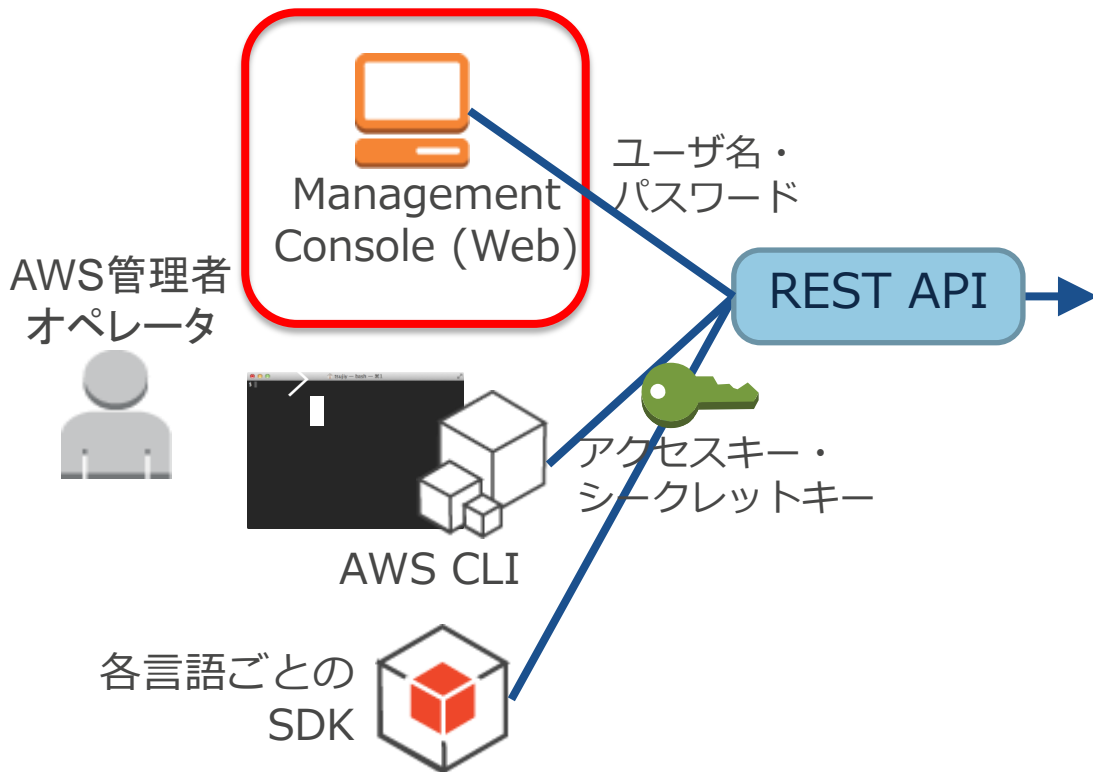


アジェンダ

- AWS Management Consoleの概要
- セキュリティベストプラクティス
- Management Consoleの管理方法
- その他のAWS管理ポータル
- まとめ



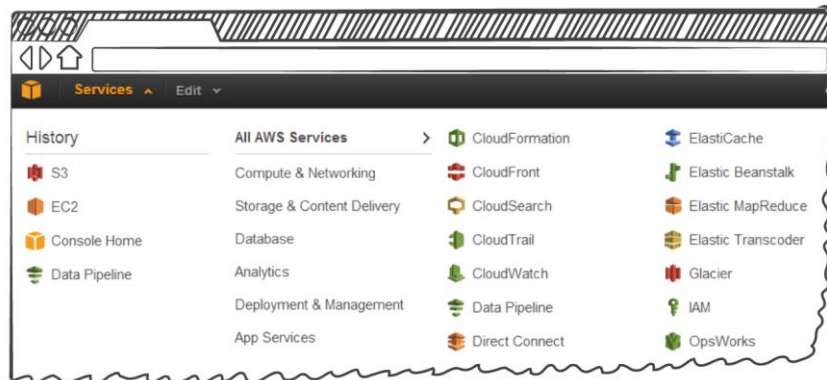
AWSの操作方法



AWS Management Console

- AWSのサービス/リソースにアクセスするための管理ツールです。
- AWSサービスのイノベーションに追従し、利用者にさらなる素晴らしい体験を提供するために、Management Consoleも日々進化しています。

本資料の情報は2015年4月27日時点のものです。



Management Console日本語対応

NEW

- 対応言語

- **日本語**、中国語、英語

- 対応サービス

- EC2、RDS、S3、VPC、IAM、SQS、EMR、DynamoDB、CloudWatch

- 言語切り替え

- 日本語ブラウザを利用している場合デフォルトは日本語
 - 表示言語の切り替えはフッターのメニューから

The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, a 'サービス' (Services) dropdown, and a user profile 'yukichib' with a location of '東京' (Tokyo). The main content area is titled 'リソース' (Resources) and displays usage statistics for Amazon EC2 in the Asia Pacific (Tokyo) region. A blue notification box highlights that Ruby, PHP, Java, .NET, Python, Node.js, and Docker applications can be easily deployed using Elastic Beanstalk. A language switch menu is open at the bottom, with '日本語' (Japanese) selected and highlighted by a red box. Other visible options in the menu include English, Deutsch, Español, Français, Português, 한국어, and 中文(简体). The footer contains a 'フィードバック' (Feedback) link, the '日本語' language selector, and links for 'プライバシーポリシー' (Privacy Policy) and '利用規約' (Terms of Use).

基本的な画面構成

① Home

② タグエディター・リソースグループ

③ AWSサービス

④ ショートカット

⑤ アカウント情報

⑥ リージョン選択

⑦ サポートセンター

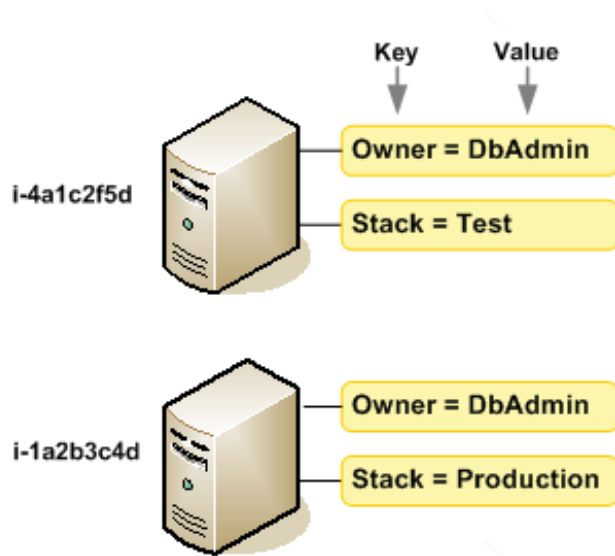
⑧ 操作メニュー

⑨ 操作画面

タグエディター

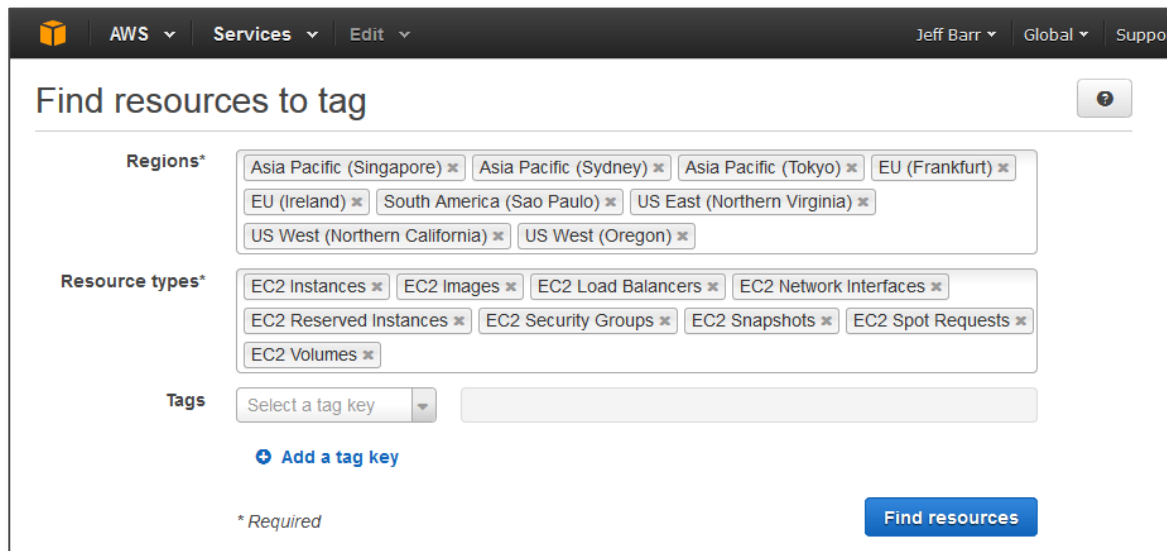
タグ

- 各AWSリソースに割り当てることができるメタデータ
 - リソース：EC2インスタンス、EBSボリュームなど
- キーと値で管理
- 使用例
 - インスタンス所有者にタグを付け課金を管理
 - 環境名にタグをつけバックアップスクリプトと連携
- 制限事項
 - リソースあたりのタグの最大数：10
 - キーの最大長：127文字（Unicode）
 - 値の最大長：255文字（Unicode）
 - キーと値の大文字小文字は区別される
 - キーおよび値に“aws:”というプリフィックスは使えない



タグエディター

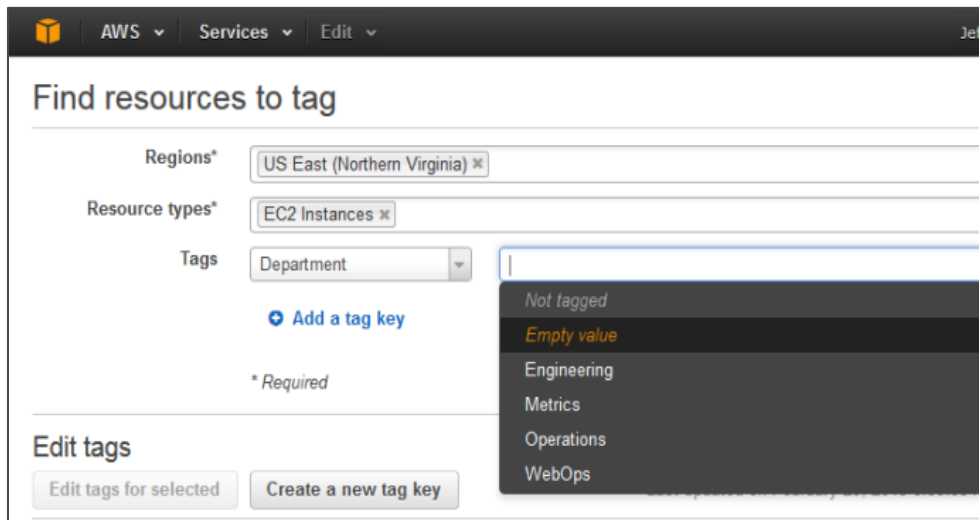
- AWSリソースのタグを一括で検索、作成、編集が可能
- リージョンをまたいだタグ管理が可能



The screenshot displays the AWS Tag Editor interface. At the top, there is a navigation bar with the AWS logo, 'AWS', 'Services', and 'Edit' dropdown menus, along with user information 'Jeff Barr', 'Global', and 'Support'. The main heading is 'Find resources to tag'. Below this, there are three main sections: 'Regions*', 'Resource types*', and 'Tags'. The 'Regions*' section contains ten tags for various AWS regions: Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), EU (Frankfurt), EU (Ireland), South America (Sao Paulo), US East (Northern Virginia), US West (Northern California), and US West (Oregon). The 'Resource types*' section contains eight tags for EC2-related resources: EC2 Instances, EC2 Images, EC2 Load Balancers, EC2 Network Interfaces, EC2 Reserved Instances, EC2 Security Groups, EC2 Snapshots, and EC2 Spot Requests. The 'Tags' section has a dropdown menu for 'Select a tag key' and a text input field. Below the 'Tags' section is a blue button labeled 'Add a tag key'. At the bottom right, there is a blue button labeled 'Find resources'. A note '* Required' is located at the bottom left of the interface.

タグエディター操作方法① -検索-

- 検索するリソースのリージョン、リソースタイプを設定
- 検索するタグのキーと値を設定
 - 任意の文字列
 - Empty value (タグの値が空白)
 - No Tagged (タグが未設定)



タグエディター操作方法② -編集-

- 複数のリソースを選択してタグを一括編集

Add / edit tags 155 Selected

Apply tags to your resources to help organize and identify them.
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. Learn more about tagging your AWS resources.

▼ Applied tags

Key	Value	Delete
app	<input type="text" value="Multiple values"/>	<input type="checkbox"/>
Created by Amazon WorkSpaces	<input type="text" value="Multiple values"/>	<input type="checkbox"/>
department	<input type="text" value="Multiple values"/>	<input type="checkbox"/>
mode	<input type="text" value="Multiple values"/>	<input type="checkbox"/>
Name	<input type="text" value="Multiple values"/>	<input type="checkbox"/>
owner	<input type="text" value="Multiple values"/>	<input type="checkbox"/>
UserTagDemo	<input type="text" value="Multiple values"/>	<input type="checkbox"/>

Value	Resources
AWS Blog Authoring Host	1
database	1
OutsideAccess	1
RoadTripBlogServer	1
1 other values	
Not Tagged	150

Multiple values

Multiple values

Multiple values

Multiple values

Multiple values

Multiple values

選択したリソースに異なるタグが付いている場合、“Multiple Values”と表示

リソースグループ

リソースグループ

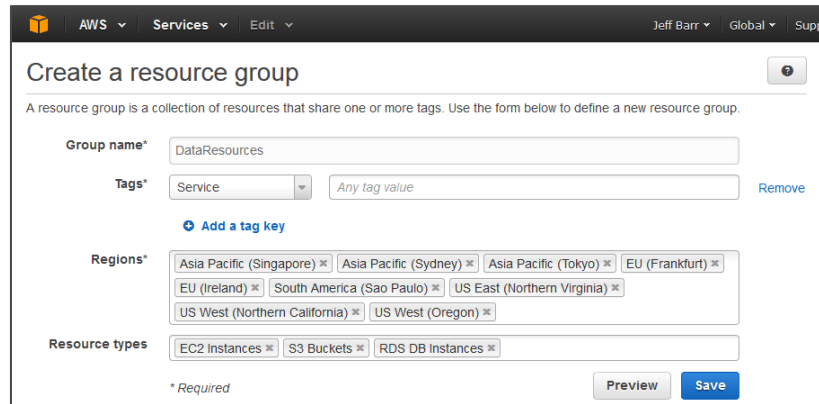
- 共通のタグが付与されたリソースをグループ化
- リージョンをまたいだリソース管理が可能
 - リソース構成情報
 - タグ情報
 - CloudWatch監視状況

The screenshot displays the AWS Management Console for 'DocShare Production Resources'. The left sidebar shows a navigation menu with categories like CloudFormation, EC2, Load Balancers, Volumes, Elastic Beanstalk, RDS, S3, Buckets, and VPC. The main content area shows a list of EC2 instances with columns for Instance ID, Region, Instance state, and Status checks. One instance, i-cbe5309b, is highlighted with a red circle and an alarm icon. Below the list, there are sections for Status checks, Alarms, Metrics, and Tags. The Tags section shows a table with keys like Name, opsworks:instance, opsworks:layer:php-app, opsworks:stack, owner, scd, scott, and test, and their corresponding values.

Key	Value
Name	TomStack-sd - php-app1
opsworks:instance	php-app1
opsworks:layer:php-app	PHP App Server
opsworks:stack	TomStack-sd
owner	SCD1
scd	
scott	EC2instance
test	scott ec2 vol

リソースグループ作成方法

- リソースのフィルタ条件を設定
 - フィルタ方法はタグエディターと同様
- リソースグループはIAMユーザーごとに作成
 - 同じAWSアカウント内のユーザーに設定を共有可能



Create a resource group

A resource group is a collection of resources that share one or more tags. Use the form below to define a new resource group.

Group name* DataResources

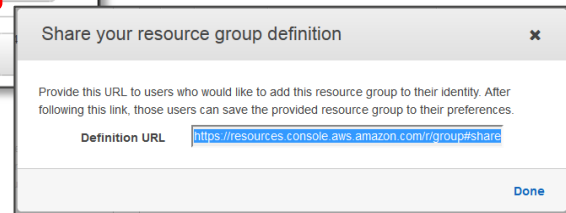
Tags* Service Any tag value Remove

Add a tag key

Regions* Asia Pacific (Singapore) x Asia Pacific (Sydney) x Asia Pacific (Tokyo) x EU (Frankfurt) x EU (Ireland) x South America (Sao Paulo) x US East (Northern Virginia) x US West (Northern California) x US West (Oregon) x

Resource types EC2 Instances x S3 Buckets x RDS DB Instances x

*Required Preview Save



Share your resource group definition x

Provide this URL to users who would like to add this resource group to their identity. After following this link, those users can save the provided resource group to their preferences.

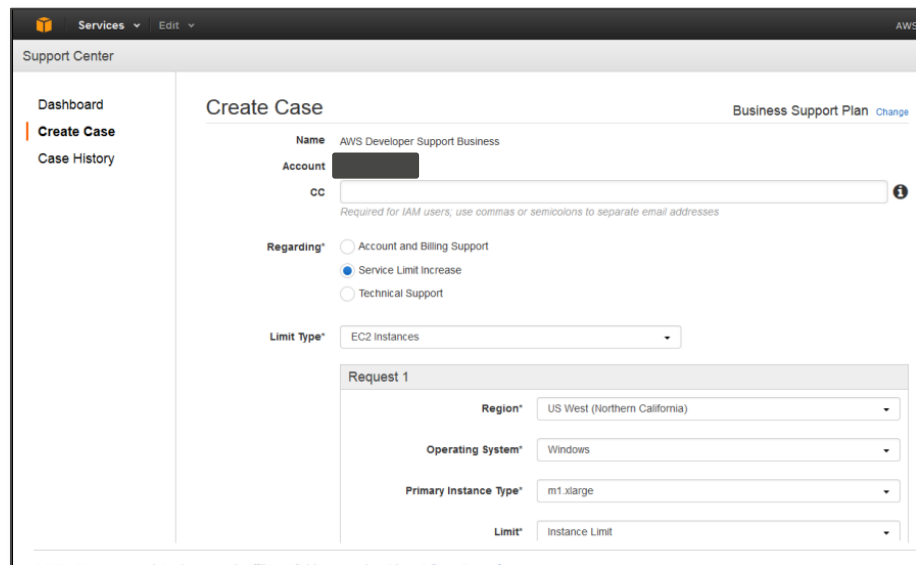
Definition URL <https://resources.console.aws.amazon.com/r/group#share>

Done

サポートセンター

サポートセンター

- 2014年11月からAWSサポートセンターが Management Console内に移動
- ケース作成
- ケース履歴参照
- ID連携アクセスのサポート



The screenshot shows the AWS Support Center interface for creating a case. The page title is "Support Center" and the main heading is "Create Case". The user is logged in as "AWS Developer Support Business" under the "Business Support Plan". The form includes the following fields:

- Name:** AWS Developer Support Business
- Account:** [Redacted]
- CC:** [Empty field with a help icon and a note: "Required for IAM users; use commas or semicolons to separate email addresses"]
- Regarding*:** Radio buttons for "Account and Billing Support", "Service Limit Increase" (selected), and "Technical Support".
- Limit Type*:** A dropdown menu currently showing "EC2 Instances".
- Request 1:** A section with the following fields:
 - Region*:** US West (Northern California)
 - Operating System*:** Windows
 - Primary Instance Type*:** m1.xlarge
 - Limit*:** Instance Limit

アジェンダ

- AWS Management Consoleの概要
- セキュリティベストプラクティス
- Management Consoleの管理方法
- その他のAWS管理ポータル
- まとめ



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



IAM ベストプラクティスのトップ 10

Top 10 AWS Identity and Access Management (IAM) Best Practices (SEC301) | AWS re:Invent 2013

<http://www.slideshare.net/AmazonWebServices/top-10-aws-identity-and-access-management-iam-best-practices-sec301-aws-reinvent-2013>

1. ユーザー 利用者ごとに個別のIAMユーザーを作成する
2. グループ IAMグループを使って権限を管理する
3. パーミッション 最小限の権限を付与する
4. パスワード 強力なパスワードポリシーを構成する
5. MFA 特権ユーザーに対して、MFA を有効化する
6. ロール EC2 インスタンスにはIAM ロールを適用する
7. 共有 IAM ロールを使って、アクセスを共有する
8. ローテーション 認証情報を定期的にローテーションする
9. 条件 条件を使って特権的アクセスをさらに制限する
10. Root Rootアカウントの使用を削減/削除する

パスワードポリシー

- デフォルトは未設定（ログインできない）
- 128文字までのBasic Latin文字
- パスワード変更時のポリシー設定が可能
 - 最低パスワード長
 - 必須文字(大文字/小文字/数字/記号)
 - ユーザーへのパスワード変更許可
 - パスワード有効期限
 - 過去パスワードの再使用拒否
 - 管理者によるパスワードリセット

▼ Password Policy

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to [Managing Passwords](#) in Using IAM.

Modify your existing password policy below.

Minimum password length:

Require at least one uppercase letter ⓘ

Require at least one lowercase letter ⓘ

Require at least one number ⓘ

Require at least one non-alphanumeric character ⓘ

Allow users to change their own password ⓘ

Enable password expiration ⓘ

Password expiration period (in days):

Prevent password reuse ⓘ

Number of passwords to remember:

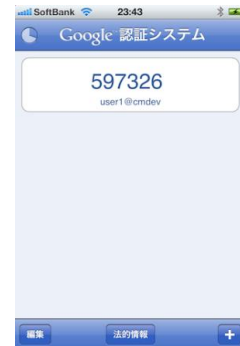
Password expiration requires administrator reset ⓘ

MFA(多要素認証)

- アカウント・パスワードに加えて、一時認証コードを利用してログイン
- ハードウェアMFA
 - Gemalto社からAWS用のデバイスを購入
 - Tokenタイプ/カードタイプ
- 仮想MFA
 - スマートフォンやPCにインストール
 - Google AuthenticatorなどTOTP実装のソフトが利用可能



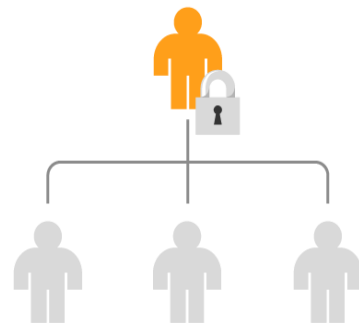
The screenshot shows the Amazon Web Services login interface. At the top left is the Amazon Web Services logo. Below it are several input fields: 'アカウント:' (Account) with a redacted value, 'ユーザー名:' (Username) with 'mfauser', 'パスワード:' (Password) with redacted characters, and 'MFAコード:' (MFA Code) with '607174'. A checkbox labeled 'MFAトークンを持っています (詳細)' (I have an MFA token (details)) is checked. A blue 'サインイン' (Sign In) button is positioned below the MFA code field. A link below the button reads 'ルートアカウントの認証検証を使用してサインイン' (Sign in using authentication verification for the root account). At the bottom, there is a small copyright notice: '利用規約 プライバシーポリシー © 1996-2014, Amazon Web Services, Inc. or its affiliates.'



rootアカウントとIAMユーザーアカウント

アカウント種別	権限	運用方法
root	フルパーミッション	<ul style="list-style-type: none">・ 基本的には使用不可・ ハードウェアMFAを適用し金庫に保管・ 利用時の申請フローを作成
IAMユーザー	必要最低限のパーミッション	<ul style="list-style-type: none">・ 利用者ごとに個別アカウントを提供・ 全ユーザーにパスワードポリシーを適用・ 特権ユーザーにはMFA適用を必須

- ・ rootアカウントの漏洩／誤使用リスクを低減
- ・ IAMユーザーには必要最低限の権限を持たせ、必要最低限の利用者に提供



アジェンダ

- AWS Management Consoleの概要
- セキュリティベストプラクティス
- Management Consoleの管理方法
- その他のAWS管理ポータル
- まとめ



よくある課題①

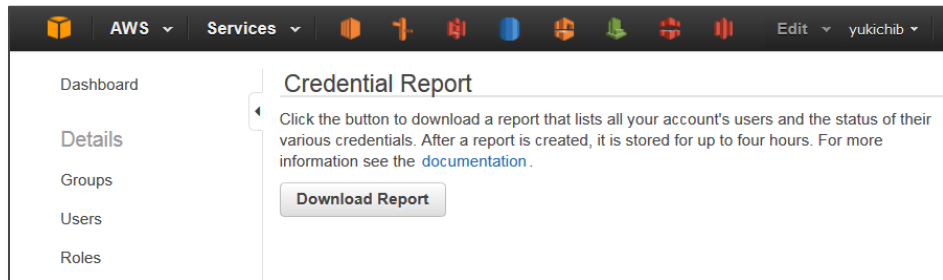
利用者に提供したIAMユーザーの
使用状況を確認したい・・・



Credential Report

Credential Report

- アカウント内のすべてのIAMユーザーの各種認証情報のレポートを生成し、CSV形式でダウンロード可能
 - ユーザー作成日
 - パスワード有無
 - 最終ログイン日時
 - 最終パスワード変更日時
 - 次回パスワードローテーション日時
 - MFA有無
- CLI、APIからもダウンロード可能
 - `aws iam generate-credential-report`
 - `aws iam get-credential-report`



よくある課題②

IAMユーザーの権限管理を
企業の認証機構に統合したい・・・



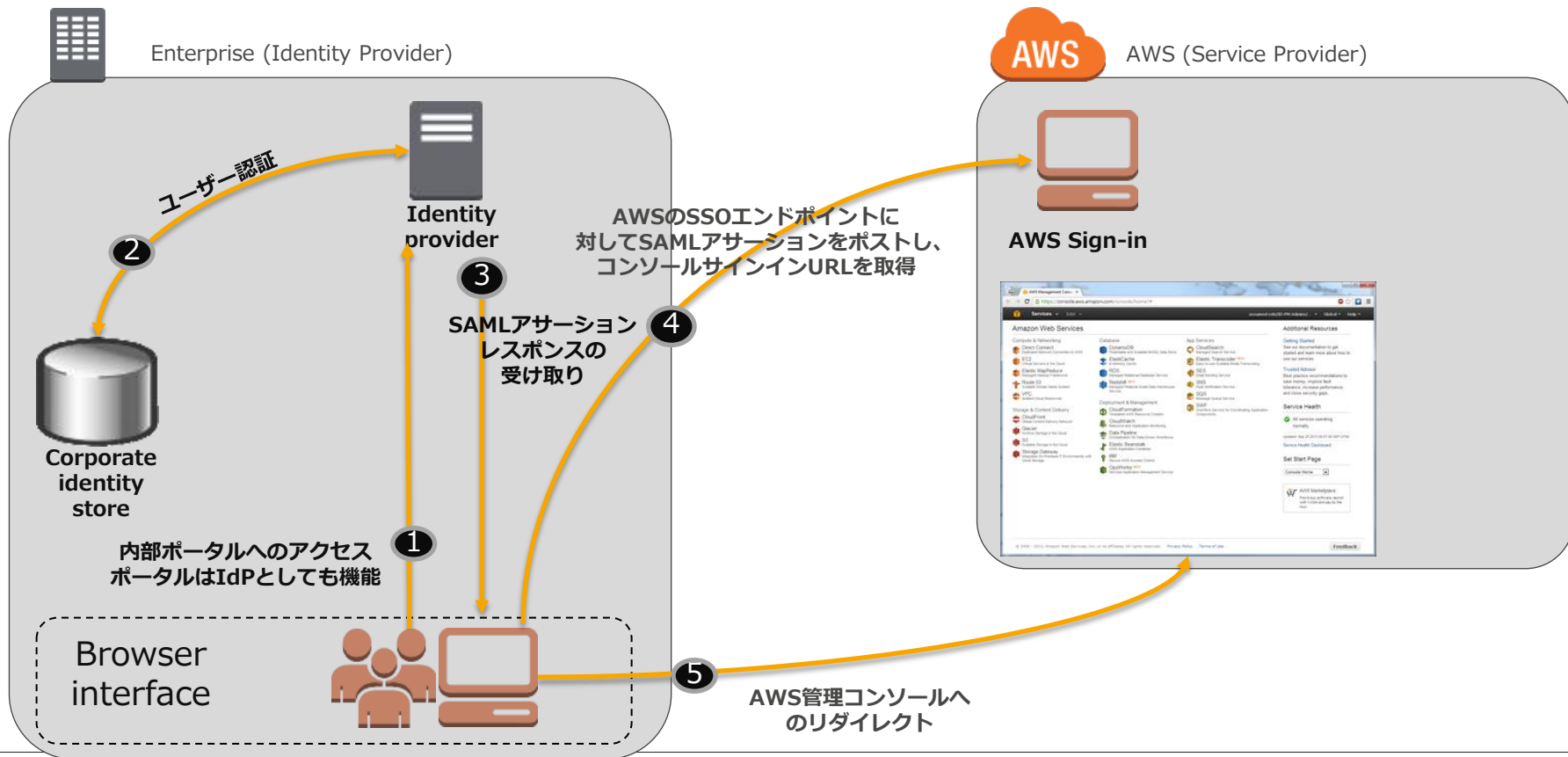
アカウント管理者

Console Federation

Console Federation

- 企業ディレクトリの認証機構を利用してManagement Consoleへのシングルサインオンが可能
- 企業ドメインのグループに応じたAWSサービスの権限管理が可能
- SAML2.0をサポート
- IDプロバイダーとしてAWS Directry Serviceを利用可能

SAMLによるConsole Federationの動作

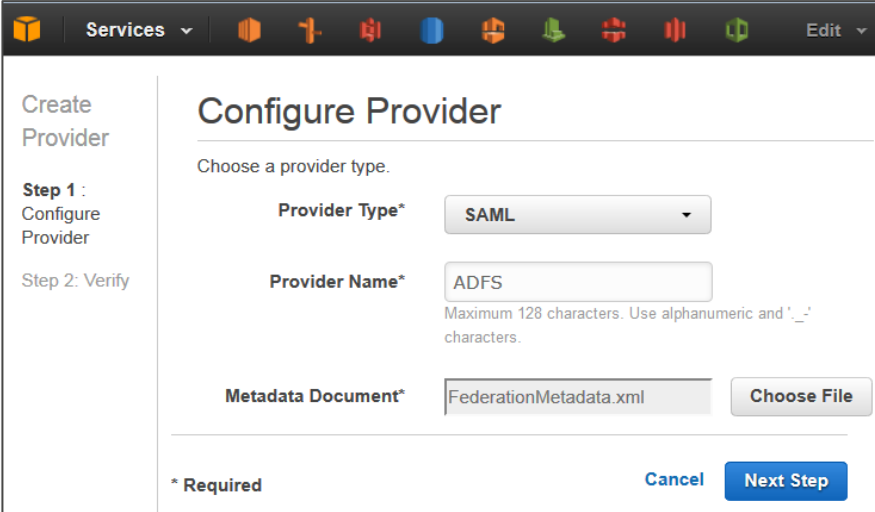


設定手順① -IDプロバイダー設定-

- 企業ディレクトリの設定
 - フェデレーションユーザーが属するドメイングループを作成
 - ドメインユーザーを作成、ドメイングループに追加
- IDプロバイダー(IdP)を構成
 - IdPソフトウェアをインストール
 - IdPにサービスプロバイダーとしてAWSを追加
 - ドメイングループとIAMロールをマッピングするクレームルールを作成
- IdPからSAMLメタデータドキュメントをダウンロード

設定手順② -SAMLプロバイダー作成-

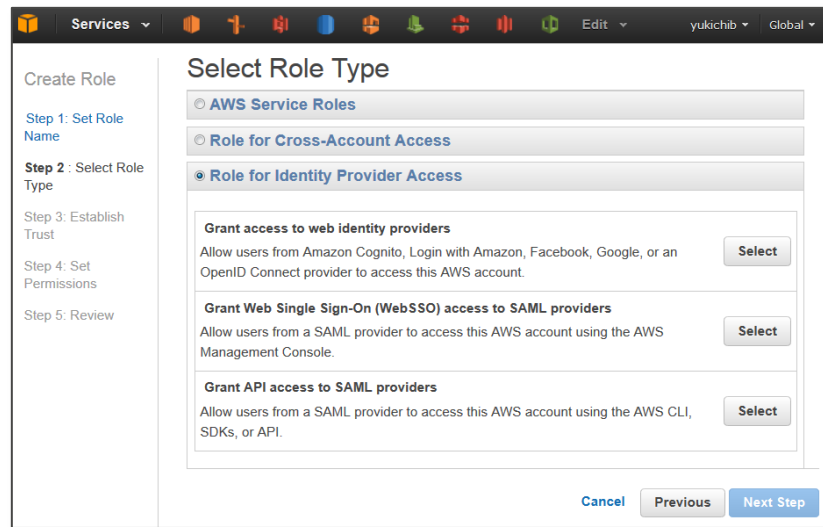
- IAMコンソールでSAMLプロバイダーを作成
 - Provider Type
 - SAML
 - Provider Name
 - IdPの設定内容
 - Metadata Document
 - 設定手順①でダウンロードしたSAMLメタデータドキュメント



The screenshot shows the AWS IAM console interface for configuring a SAML provider. The page is titled "Configure Provider" and is part of the "Create Provider" workflow. The "Provider Type" is set to "SAML". The "Provider Name" is "ADFS", with a note indicating a maximum of 128 alphanumeric and underscore characters. The "Metadata Document" is "FederationMetadata.xml", with a "Choose File" button. The page includes a "Cancel" button and a "Next Step" button. The left sidebar shows the "Create Provider" steps: "Step 1: Configure Provider" and "Step 2: Verify".

設定手順③ -IAMロール作成-

- フェデレーションを許可するIAMロールの作成
 - Role Type
 - Grant Web Single Sign-On (WebSSO) access to SAML providers
 - SAML Provider
 - 設定手順②のSAMLプロバイダー名
 - Permission
 - IAMロールの権限を設定



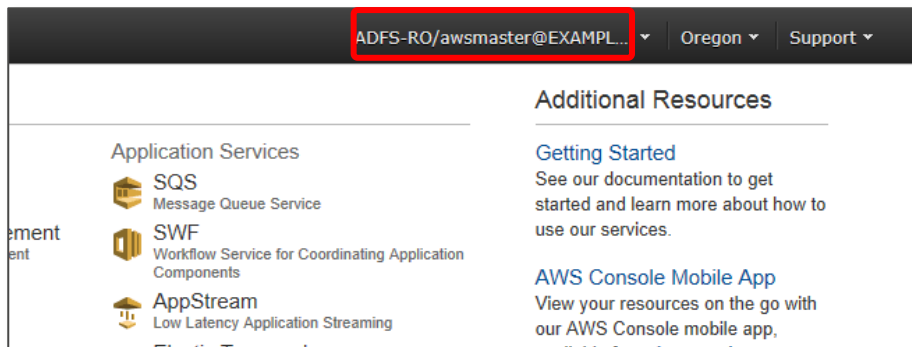
設定手順④ -動作確認-

- IdPのログインサイトにアクセス
- ドメインユーザーのアカウントでログイン

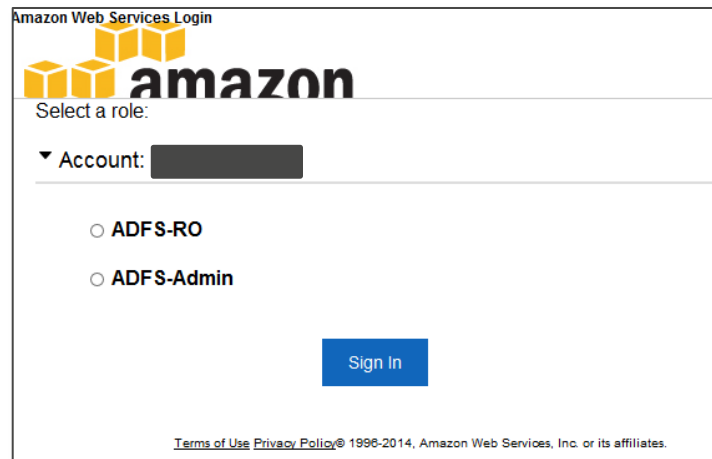


設定手順⑤ -動作確認-

- Management Consoleにリダイレクトされることを確認



ドメインユーザーが複数のIAMロールにマッピングされている場合、IAMロールの選択画面にリダイレクトされる



よくある課題③

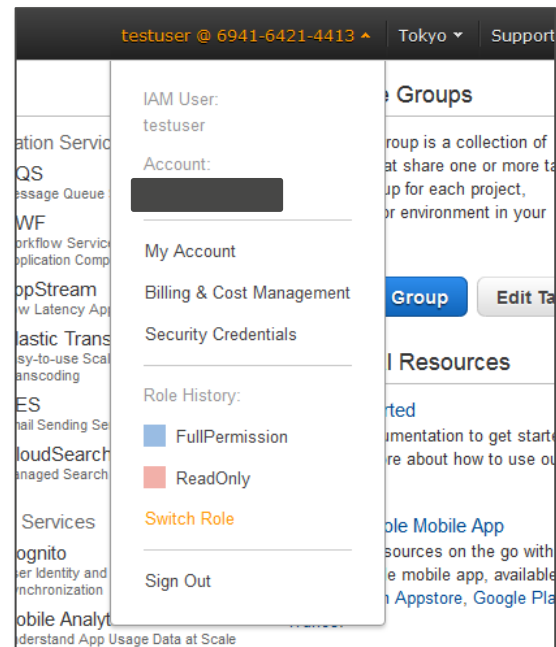
読取専用／更新用の2つの
IAMユーザーが割り当てられている。
アカウント切替が面倒・・・



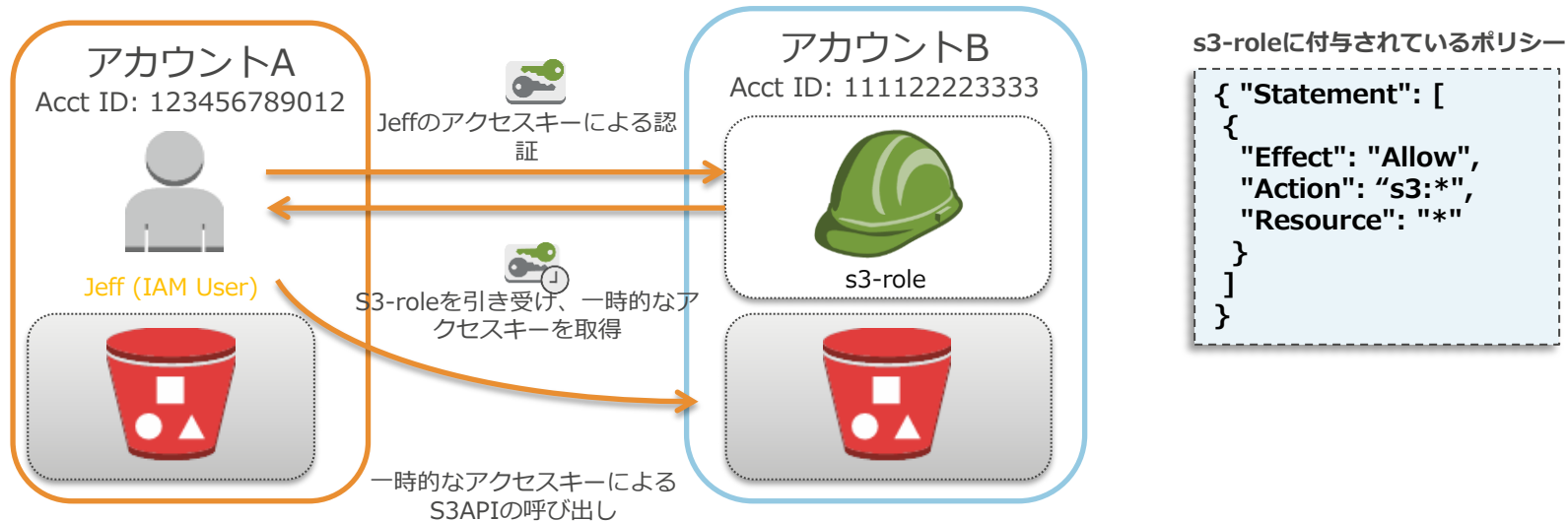
Switch Role

Switch Role

- IAMユーザーからクロスアカウントアクセス用IAMロールに切替が可能
 - 必ずしも別アカウントである必要はなく、同じアカウントでもOK
- 必要な時のみIAMユーザーの権限を“昇格”させる
 - IAMユーザーには読み取り権限のみを付与
 - IAMロールには更新権限を付与
- 認証情報の管理対象が1つのIAMユーザーに統合できる



IAMロールによるクロスアカウントアクセスの動作



s3-roleに付与されているポリシー

```
{ "Statement": [  
  {  
    "Effect": "Allow",  
    "Action": "s3:*",  
    "Resource": "*"  
  }  
]
```

```
{ "Statement": [{  
  "Effect": "Allow",  
  "Action": "sts:AssumeRole",  
  "Resource": "arn:aws:iam::111122223333:role/s3-role"  
}]  
}
```

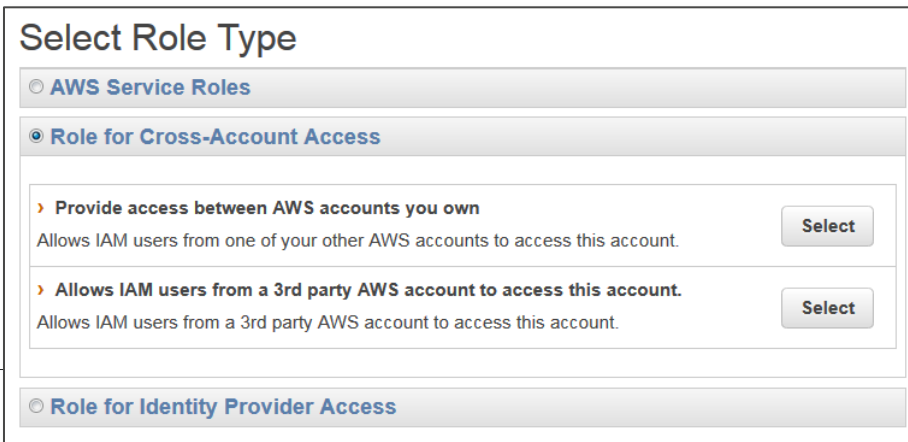
アカウントBのs3-roleを引き受けることを許可するポリシーをJeffに設定

```
{ "Statement": [{  
  "Effect": "Allow",  
  "Principal": {"AWS": "arn:aws:iam::123456789012:root"},  
  "Action": "sts:AssumeRole"  
}]  
}
```

S3-roleを誰が引き受けられるか定義したポリシーをs3-roleに設定

設定手順① -IAMユーザー／ロール作成-

- IAMユーザーの作成
 - ReadOnlyAccessポリシーを付与
- クロスアカウントアクセス用IAMロールの作成
 - 切替を許可するAWSアカウントIDを指定
 - 更新権限を持ったポリシーを付与



The screenshot shows the 'Select Role Type' dialog box in the AWS IAM console. It has three main sections: 'AWS Service Roles', 'Role for Cross-Account Access', and 'Role for Identity Provider Access'. The 'Role for Cross-Account Access' section is selected and expanded, showing two options: 'Provide access between AWS accounts you own' and 'Allows IAM users from a 3rd party AWS account to access this account.' Each option has a 'Select' button to its right.

Select Role Type

- AWS Service Roles
- Role for Cross-Account Access
 - Provide access between AWS accounts you own
Allows IAM users from one of your other AWS accounts to access this account.
 - Allows IAM users from a 3rd party AWS account to access this account.
Allows IAM users from a 3rd party AWS account to access this account.
- Role for Identity Provider Access

設定手順② -IAMロール編集-

- IAMロールのTrust Relationshipsを編集
 - 指定したAWSアカウントのrootからの切替が許可された状態
 - IAMユーザーからの切替を許可するようポリシーを変更

```
"Effect": "Allow",  
"Principal": {"AWS": "arn:aws:iam::123456789012:root"},  
"Action": "sts:AssumeRole"
```



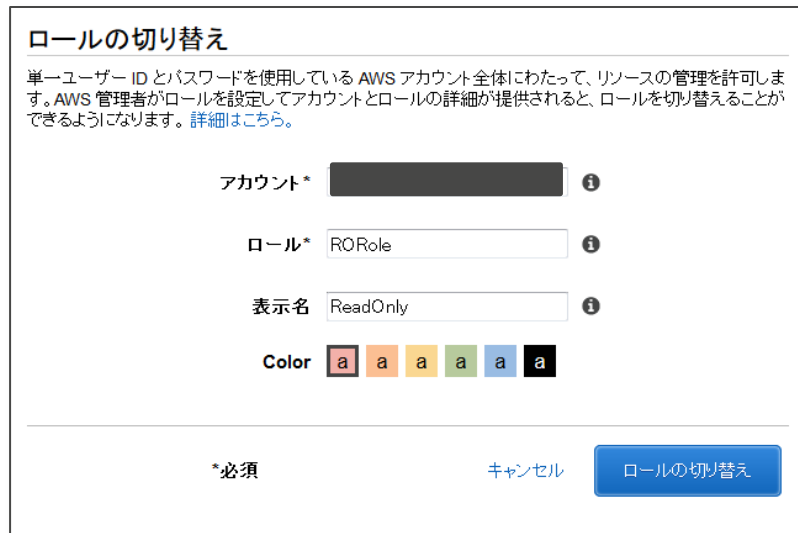
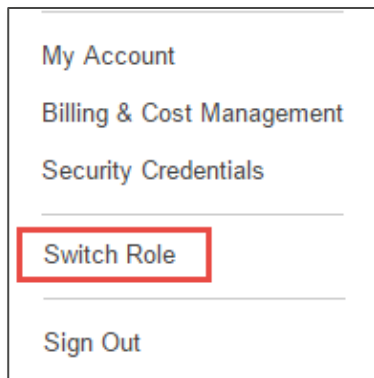
```
"Effect": "Allow",  
"Principal": {"AWS": "arn:aws:iam::123456789012:user/IAMUserName"},  
"Action": "sts:AssumeRole"
```

IAMポリシーのプリンシパルではグループ指定ができないため
ユーザーごとに追加が必要

The screenshot shows the 'Trust Relationships' section of the AWS IAM console. It includes a dropdown menu for 'Trust Relationships', a description of the role's trust policy, an 'Edit Trust Relationship' button, and a list of 'Trusted Entities'. The list shows 'The account 694164214413' as a trusted entity.

設定手順③ -動作確認-

- IAMユーザーでManagement Consoleにログイン
- SwitchRoleを選択し、ロールを切替
 - 表示名、表示色を指定可能
 - 設定内容は5ロールまで保存



よくある課題④

Management Consoleへアクセス
できるIPアドレスを制限したい・・・



セキュリティ管理者

IAM Policy Condition Statement

IAM Policy Condition Statement



- Management ConsoleにログインするIPアドレスを制限することはできない
- IAMユーザーのポリシーで、操作が可能なIPアドレスを制限することは可能

```
{  
  "Effect": "Deny",  
  "Action": "*",  
  "Resource": "*",  
  "Condition": {  
    "NotIpAddress": {"aws:SourceIp": "111.111.111.111/32"}  
  }  
}
```

← 111.111.111.111以外からのアクセスの場合、全てのアクションをDeny

接続元IPアドレスを制限した場合の注意事項

- 送信元を制限したIAMユーザーで作業した場合、処理が失敗するアクションがあります。
 - CloudFormationからのリソース作成
 - マーケットプレイスからのEC2インスタンス起動 など

 You do not have the required EC2 or Marketplace permissions. Please contact your account admin to request the missing permissions. The missing permission(s): ec2:DescribeImages; ec2:DescribeInstances; ec2:DescribeKeyPairs; ec2:DescribeSecurityGroups; ec2:DescribeVpcs; ec2:DescribeSubnets; ec2:DescribeAccountAttributes; ec2:AuthorizeSecurityGroupEgress; ec2:AuthorizeSecurityGroupIngress; ec2:CreateSecurityGroup; ec2>DeleteSecurityGroup; ec2:RunInstances; ec2:StartInstances; ec2:StopInstances; ec2:TerminateInstances. As a result, most controls on this page are disabled. [Learn about AWS Identity and Access Management](#) 

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/AccessPolicyLanguage_ElementDescriptions.html#Conditions_IPAddress
aws:SourceIp 条件キーは、リクエストの送信元である IP アドレスに解決します。リクエストが Amazon EC2 インスタンスから送信された場合、aws:SourceIp はインスタンスのパブリック IP アドレスに評価されます。Amazon Elastic MapReduce、AWS Elastic Beanstalk、AWS CloudFormation、Tag Editor など、ユーザーに代わって AWS への呼び出しを実行した AWS サービスからリクエストが送信された場合、aws:SourceIp はそのサービスの IP アドレスに解決します。このタイプのサービスでは、aws:SourceIp 条件を使用しないことをお勧めします。

よくある課題⑤

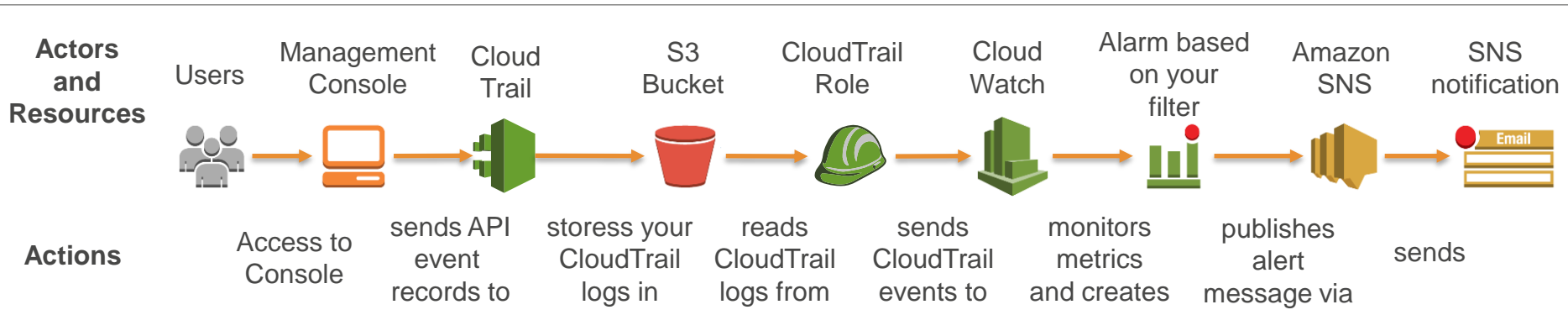
Management Consoleへの
不正ログインを監視／検知したい・・・



CloudTrail integration with CloudWatch Logs

CloudTrail integration with CloudWatch Logs

- CloudTrailのログをCloudWatch Logsで監視／検知可能
- Metricフィルターで監視したいアクションを抽出
- 監視アクション／閾値例
 - IAMユーザーでのコンソールログイン失敗アクションが5分間に100回以上
 - rootアカウントでのコンソールログイン成功アクションが5分間に1回以上

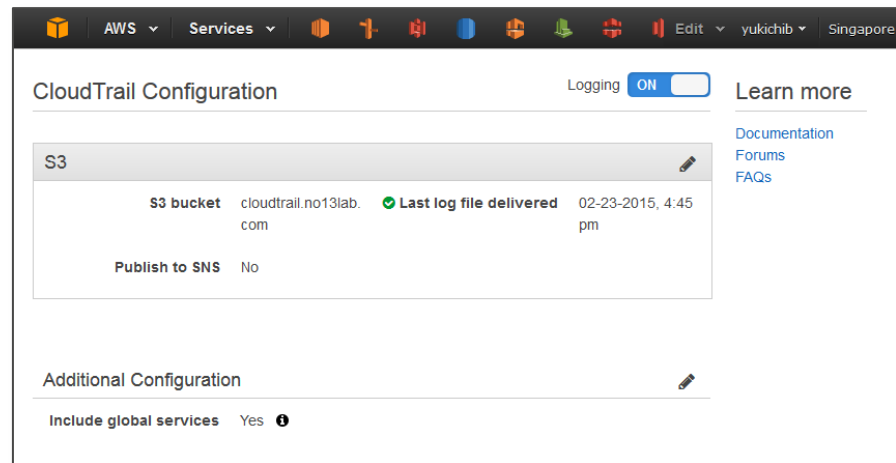


CloudTrailではrootのログイン失敗アクション、全アカウントのログオフアクションは取得不可

設定手順① -CloudTrail有効化-

ConsoleLoginイベントは全リージョンのCloudTrailログに同じ情報が出力されるため、以降の設定はN.Virginiaリージョンのみで実施

- CloudTrailを有効化
- Include global servicesがYesになっていることを確認



The screenshot shows the AWS CloudTrail Configuration console. At the top, the 'Logging' toggle is set to 'ON'. Below this, the 'S3' configuration section is visible, showing the S3 bucket 'cloudtrail.no13lab.com' and a status message 'Last log file delivered' with a timestamp of '02-23-2015, 4:45 pm'. The 'Publish to SNS' option is set to 'No'. At the bottom, the 'Additional Configuration' section shows 'Include global services' set to 'Yes'.

S3	
S3 bucket	cloudtrail.no13lab.com
Last log file delivered	02-23-2015, 4:45 pm
Publish to SNS	No

Additional Configuration	
Include global services	Yes ⓘ

CloudTrailコンソール

設定手順② -CloudWatch Logs有効化-

- CloudWatch LogsのLogグループを作成
- Log Streamを有効化

The screenshot shows the 'CloudTrail Configuration' page in the AWS console. At the top right, there is a 'Logging' toggle switch set to 'ON'. Below this, there are two main sections: 'S3' and 'CloudWatch Logs (Optional)'. The 'S3' section shows the bucket 'cloudtrail.no13lab.com' and a status 'Last log file delivered' at '02-19-2015, 9:24 am'. The 'Publish to SNS' option is set to 'No'. The 'CloudWatch Logs (Optional)' section has a 'NEW' badge and a descriptive paragraph about SNS notifications. Below the text is a required field 'New or existing log group*' with the value 'CloudTrail/DefaultLogGroup' and an information icon. At the bottom right of this section are 'Cancel' and 'Continue' buttons. A footnote '* Required field' is located at the bottom left of the CloudWatch Logs section.

CloudTrailコンソール

設定手順③ -メトリックフィルタ作成-

- CloudWatch Logsのメトリックフィルタを作成

- コンソールログイン失敗

```
{ ($.eventName = "ConsoleLogin") &&  
  ($.errorMessage = "Failed authentication") }
```

- rootアカウントログイン

```
{ ($.eventName = "ConsoleLogin") &&  
  ($.userIdentity.type = "Root") }
```

- フィルタパターン

- 一致/比較 : =, !=, <, >, <=, >=
- 論理演算 : &&, ||

Create Metric Filter and Assign a Metric

Filter for Log Group: CloudTrail/DefaultLogGroup

Log events that match the pattern you define are recorded to the metric that you specify. You can graph the metric and set alarms to notify you.

Filter Name:

Filter Pattern:

Metric Details

Metric Namespace:

Metric Name:

[Show advanced metric settings](#)

CloudWatch Logsコンソール

設定手順④ -アラーム作成-

- 作成したメトリックに対するアラームを作成
 - n分間でm回以上イベントが検知された場合に通知するよう設定
 - 通知先を指定

Create Alarm

1. Select Metric 2. Define Alarm

Alarm Threshold

Provide the details and threshold for your alarm. Use the graph on the right to help set the appropriate threshold.

Name: LoginFailedAlarm

Description: Alarm when Login Failed 10 times per minute

Whenever: MonitorFailedLoginEvents

is: >= 10

for: 1 consecutive period(s)

Actions

Define what actions are taken when your alarm changes state.

Whenever this alarm:	Send notification to:	Email list:
State is ALARM	email_yukichib	yukichib@amazon.co.jp

Alarm Preview

This alarm will trigger when the blue line goes up to or above the red line for a duration of 1 minute

MonitorFailedLoginEvents >= 10

Namespace: LogMetrics
Metric Name: MonitorFailedLoginEvents

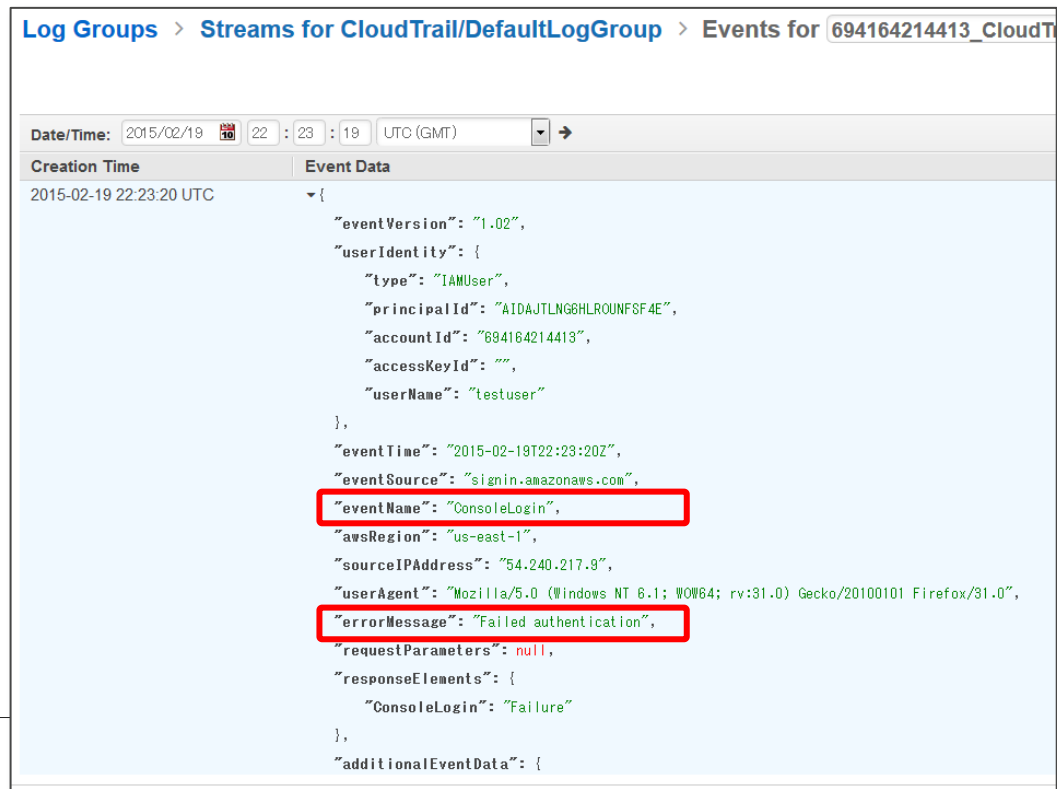
Period: 1 Minute
Statistic: Sum

Cancel Back Next **Create Alarm**

CloudWatchコンソール

設定手順⑤ -動作確認-

- CloudWatch Logsにイベントが出力されることを確認

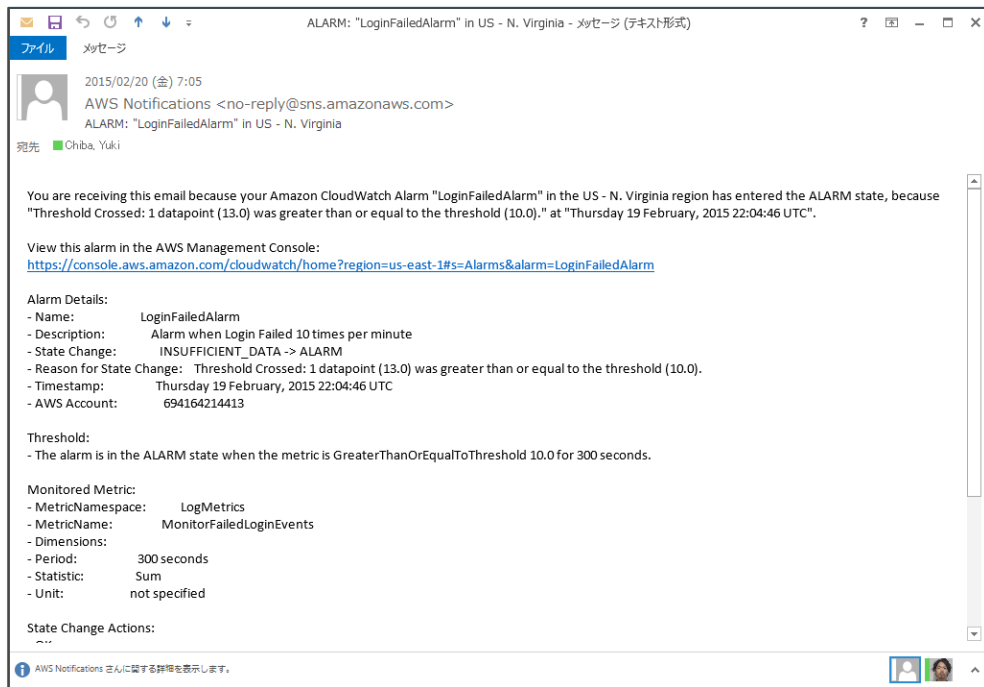


The screenshot shows the AWS CloudWatch Logs console interface. The breadcrumb navigation at the top reads: "Log Groups > Streams for CloudTrail/DefaultLogGroup > Events for 694164214413_CloudT...". Below the navigation, there is a date/time filter set to "2015/02/19 22:23:19 UTC (GMT)". The main content area is a table with two columns: "Creation Time" and "Event Data". The "Creation Time" column shows "2015-02-19 22:23:20 UTC". The "Event Data" column contains a JSON object representing the event. Two fields in the JSON are highlighted with red boxes: "eventName": "ConsoleLogin" and "errorMessage": "Failed authentication".

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAJTLNG6HLROUNFSF4E",
    "accountId": "694164214413",
    "accessKeyId": "",
    "userName": "testuser"
  },
  "eventTime": "2015-02-19T22:23:20Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "54.240.217.9",
  "userAgent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0",
  "errorMessage": "Failed authentication",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Failure"
  },
  "additionalEventData": {
```

設定手順⑥ -動作確認-

- 監視アクションが閾値を超えた際に通知されることを確認



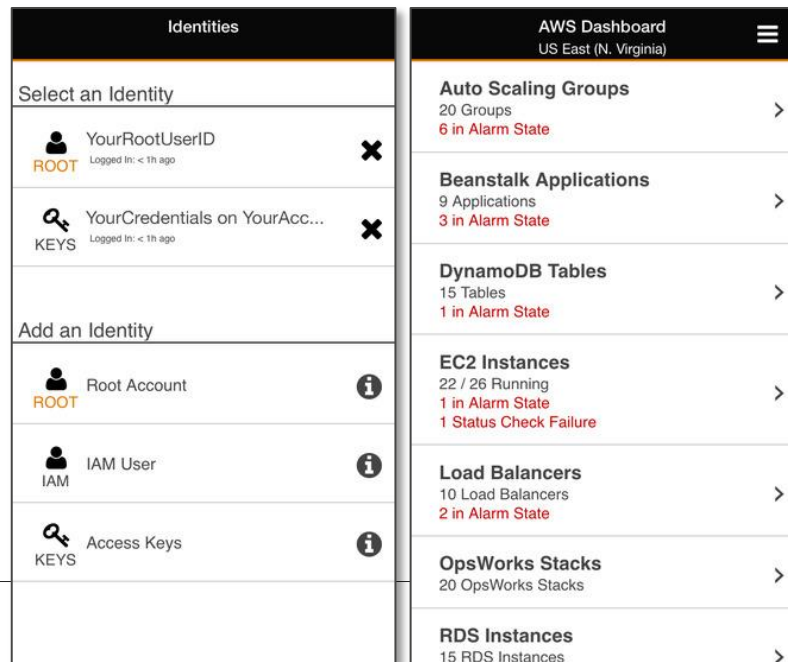
アジェンダ

- AWS Management Consoleの概要
- セキュリティベストプラクティス
- Management Consoleの管理方法
- その他のAWS管理ポータル
- まとめ



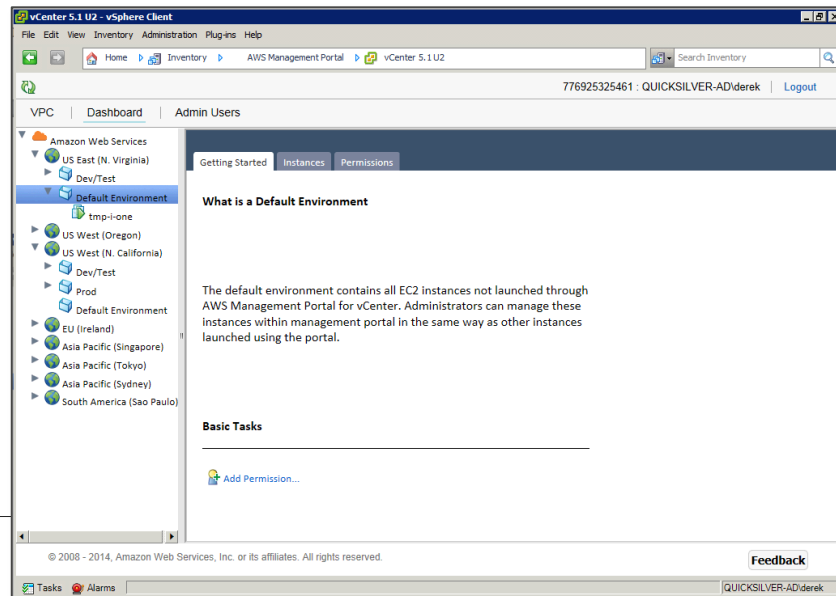
AWS Console モバイルアプリ

- サポートサービス
 - EC2、ELB、S3、Route53、RDS、AutoScaling、Elastic Beanstalk、DynamoDB、OpsWorks、CloudWatch
- サポートプラットフォーム
 - Android、iOS
- セキュリティ
 - IAMユーザーアカウントでのログイン
 - MFA利用可能



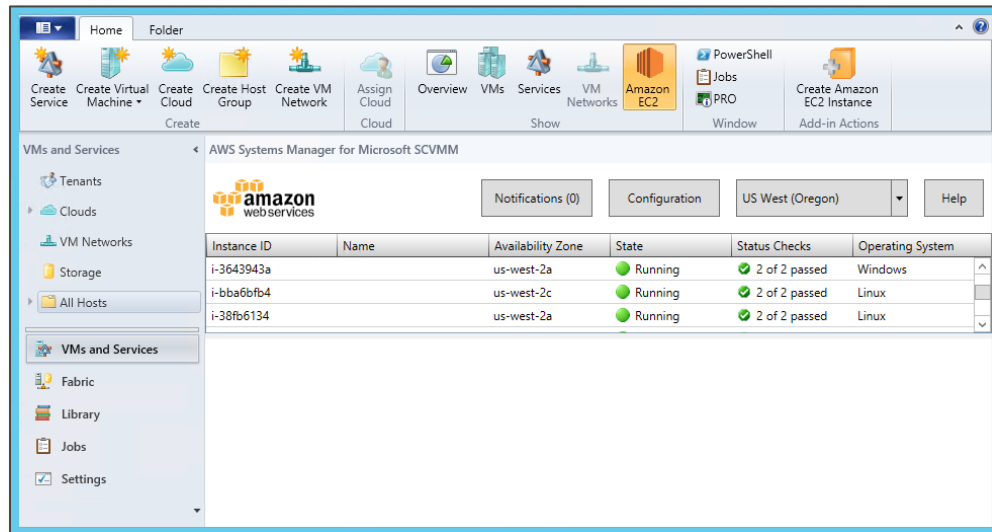
AWS Management Portal for vCenter

- vCenterのプラグイン
- vSphereクライアントを使用してAWSリソースを管理可能
 - VPC、サブネット、セキュリティグループの操作
 - キーペアの操作
 - EC2インスタンスの操作
 - VMWare仮想マシンのインポート



System Center Virtual Machine Manager(SCVMM) Add-In

- SCVMMのアドイン
- SCVMMを使用してAWSリソースを管理可能
 - EC2インスタンスの操作
 - Hyper-V仮想マシンのインポート



The screenshot displays the AWS Systems Manager for Microsoft SCVMM console. The interface includes a navigation pane on the left with categories like Tenants, Clouds, VM Networks, Storage, All Hosts, VMs and Services, Fabric, Library, Jobs, and Settings. The main content area shows the title 'AWS Systems Manager for Microsoft SCVMM' and the Amazon Web Services logo. Below the logo, there are buttons for 'Notifications (0)', 'Configuration', a region selector set to 'US West (Oregon)', and a 'Help' button. A table lists three EC2 instances:

Instance ID	Name	Availability Zone	State	Status Checks	Operating System
i-3643943a		us-west-2a	Running	2 of 2 passed	Windows
i-bba6bfb4		us-west-2c	Running	2 of 2 passed	Linux
i-38fb6134		us-west-2a	Running	2 of 2 passed	Linux

アジェンダ

- AWS Management Consoleの概要
- セキュリティベストプラクティス
- Management Consoleの管理方法
- その他のAWS管理ポータル
- まとめ



まとめ

- Management Consoleは日々進化しています！
- IAMベストプラクティスでセキュリティを確保しましょう
- Management Console自体の運用管理もお忘れなく
 - Credential Report
 - Console Federation
 - Switch Role
 - IAM Policy Condition Statement
 - CloudTrail integration with CloudWatch Logs
- ブラウザ以外からも利用可能です！
 - モバイルアプリ
 - AWS Management Portal for vCenter
 - SCVMM Add-In

Feedback!

アマゾン ウェブ サービス

コンピューティング

- EC2**
クラウド内の仮想サーバー
- Lambda**
イベント発生時にコードを実行
- EC2 Container Service**
Docker コンテナの実行と管理

ストレージ & コンテンツ配信

- S3**
スケーラブルなクラウドストレージ
- Storage Gateway**
オンプレミス IT 環境とクラウドストレージの統合
- Glacier**
クラウド内のアーカイブストレージ
- CloudFront**
グローバルなコンテンツ配信ネットワーク

データベース

- RDS**
マネージド型のリレーショナルデータベースサービス
- DynamoDB**
予測可能でスケーラブルな NoSQL データストア
- ElastiCache**
インメモリキャッシュ
- Redshift**
マネージド型のペタバイトスケールのデータウェアハウスサービス

ネットワーク

- VPC**
独立したクラウドリソース
- Direct Connect**
AWS への専用線接続
- Route 53**
スケーラブルなドメインネームシステム(DNS)

管理およびセキュリティ

- Directory Service**
クラウド上の管理型ディレクトリ
- Identity & Access Management**
アクセスコントロールとキー管理
- Trusted Advisor**
AWS クラウド最適化エキスパート
- CloudTrail**
ユーザーアクティビティと変更の記録
- Config**
リソース設定およびイベントリ
- CloudWatch**
リソースとアプリケーションのモニタリング

デプロイ & マネジメント

- Elastic Beanstalk**
AWS アプリケーションコンテナ
- OpsWorks**
DevOps アプリケーション管理サービス
- CloudFormation**
テンプレートによる AWS リソース作成
- CodeDeploy**
自動デプロイ

分析

- Elastic MapReduce**
マネージド型 Hadoop フレームワーク
- Kinesis**
ビッグデータストリームのリアルタイム処理
- Data Pipeline**
データ駆動型ワークフローに対するオーケストレーションサービス
- Machine Learning**
すばやく簡単にスマートアプリケーションを構築

アプリケーションサービス

- SQS**
メッセージキューサービス
- SWF**
アプリケーションコンポーネントを連携させるワークフローサービス
- AppStream**
低レイテンシーのアプリケーションストリーミング
- Elastic Transcoder**
使いやすいくスケーラブルなメディア変換サービス
- SES**
Eメール送信サービス
- CloudSearch**
マネージド型検索サービス

モバイルサービス

- Cognito**
ユーザー ID およびアプリケーションデータの同期
- Mobile Analytics**
大規模なアプリケーションの使用状況データの把握
- SNS**
プッシュ通知サービス

エンタープライズアプリケーション

- WorkSpaces**
クラウド内のデスクトップ
- WorkDocs**
セキュアなエンタープライズ向けストレージおよび共有サービス
- WorkMail** **プレビュー**
セキュリティ保護された Eメールとカレンダーサービス

リソースグループ

test-group

グループの作成

タグエディター

その他のリソース

はじめに

サービスを初めて使用する手順やさらに詳しい使用方法については、ドキュメントを参照してください。

AWS Console モバイルアプリ

Amazon アプリストア、Google Play、または iTunes から入手可能な AWS コンソールモバイルアプリを使用して、出先でリソースを表示します。

AWS Marketplace

ソフトウェアを検索して購入し、1-Click で起動し、時間単位で料金を支払えます。

AWS Summit – サンプルシスコ

詳細については、サンプルシスコで開催される AWS Summit で発表予定のエキサイティングな新規サービスや機能を確認ください。

サービス状態

すべてのサービスが正常に動作中です。

更新済み: Apr 27 2015 15:41:00 GMT+0900

サービス状態ダッシュボード

参考資料

- AWS Management Console Document
 - http://docs.aws.amazon.com/ja_jp/awsconsolehelpdocs/latest/gsg/getting-started.html
- AWS Management Console FAQ
 - <http://aws.amazon.com/jp/console/faqs/>
- AWS Identity and Access Management
 - http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/IAM_Introduction.html
- AWS Security Token Service
 - http://docs.aws.amazon.com/ja_jp/STS/latest/UsingSTS/Welcome.html
- Using Identity Providers
 - http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/identity-providers.html
- Switching to a Role in the AWS Management Console
 - <http://docs.aws.amazon.com/IAM/latest/UserGuide/roles-usingrole-switchconsole.html>
- Creating CloudWatch Alarms for CloudTrail Events
 - http://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cw_create_alarms.html