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

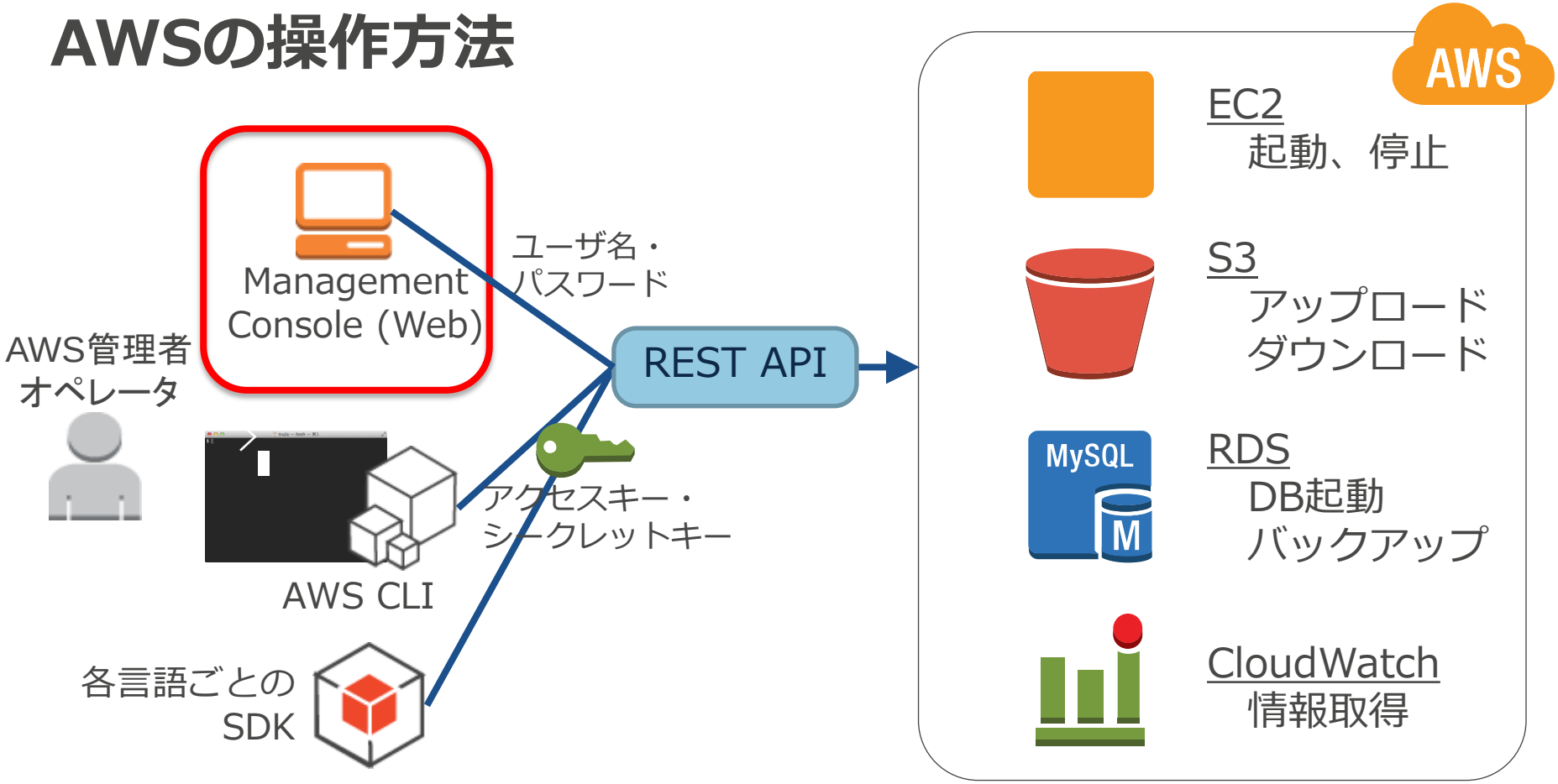
アジェンダ

- 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

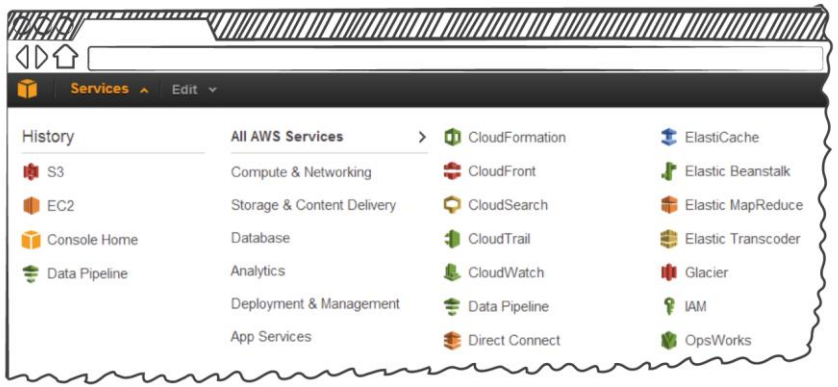
AWSの操作方法


AWS
Management Console (Web)
ユーザ名・
パスワード
AWS管理者
オペレータ
REST API
アクセスキー・
シークレットキー
AWS CLI
各言語ごとの
SDK
EC2
起動、停止
S3
アップロード
ダウンロード
MySQL
M
RDS
DB起動
バックアップ
CloudWatch
情報取得

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。

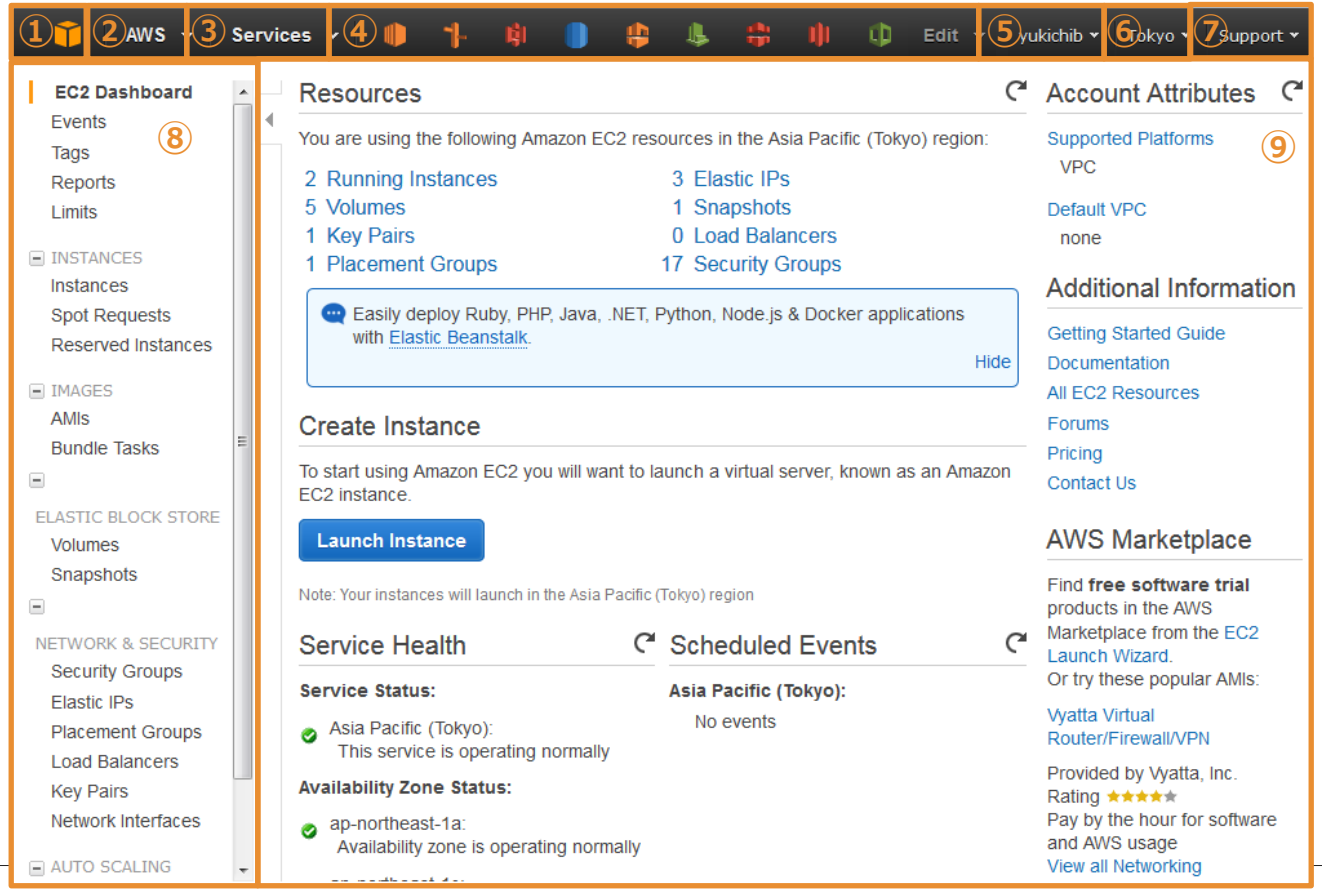


Management Console日本語対応

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

基本的な画面構成



①Home

②タグエディター・
リソースグループ

③AWS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

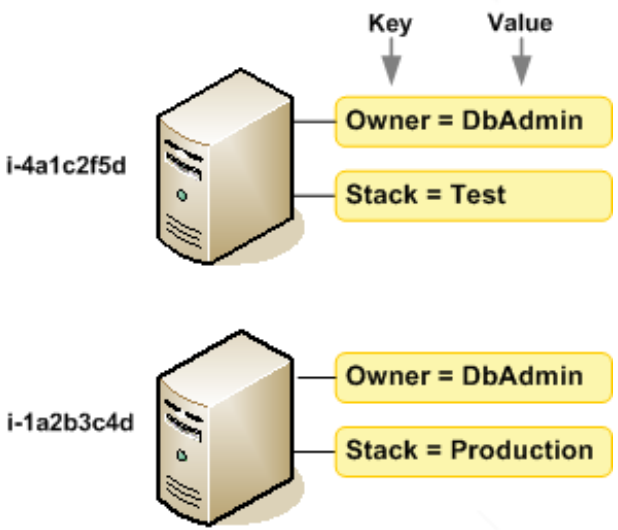
⑧操作メニュー

⑨操作画面

タグエディター

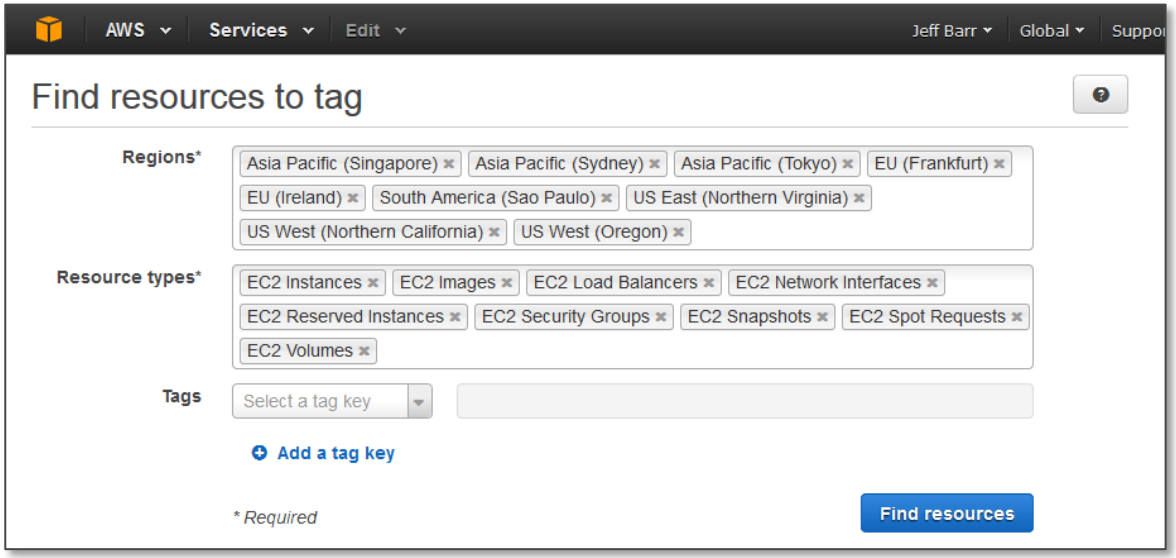
タグ

- 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



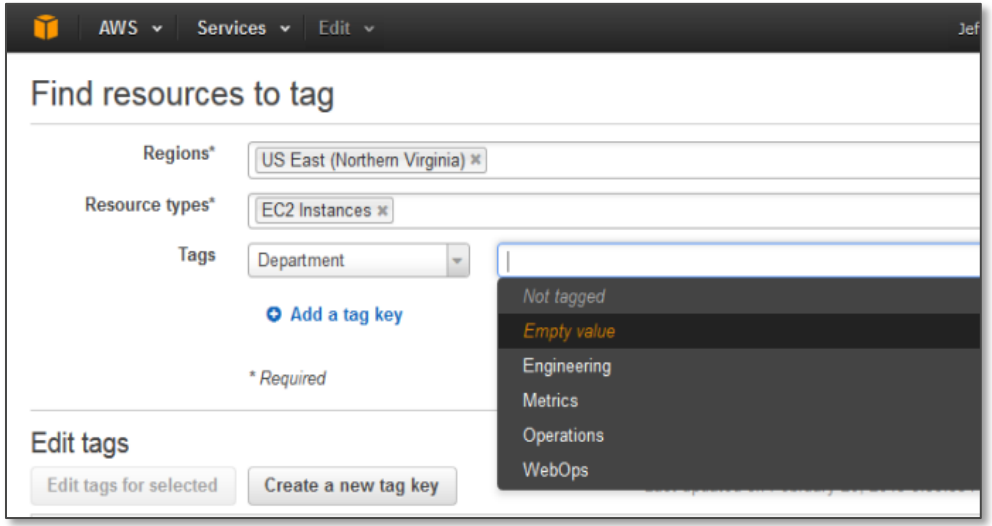
タグエディター

- 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



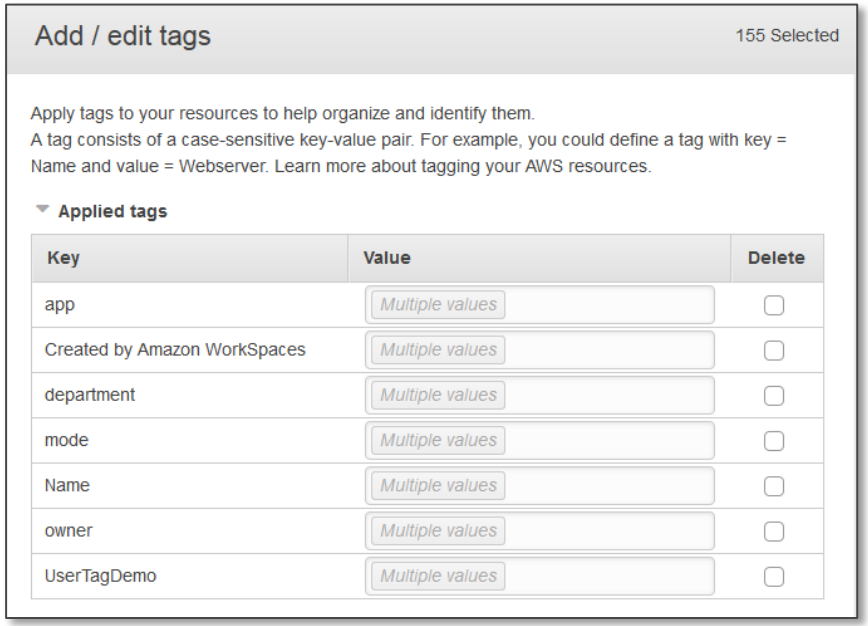
タグエディター操作方法① -検索-

- 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

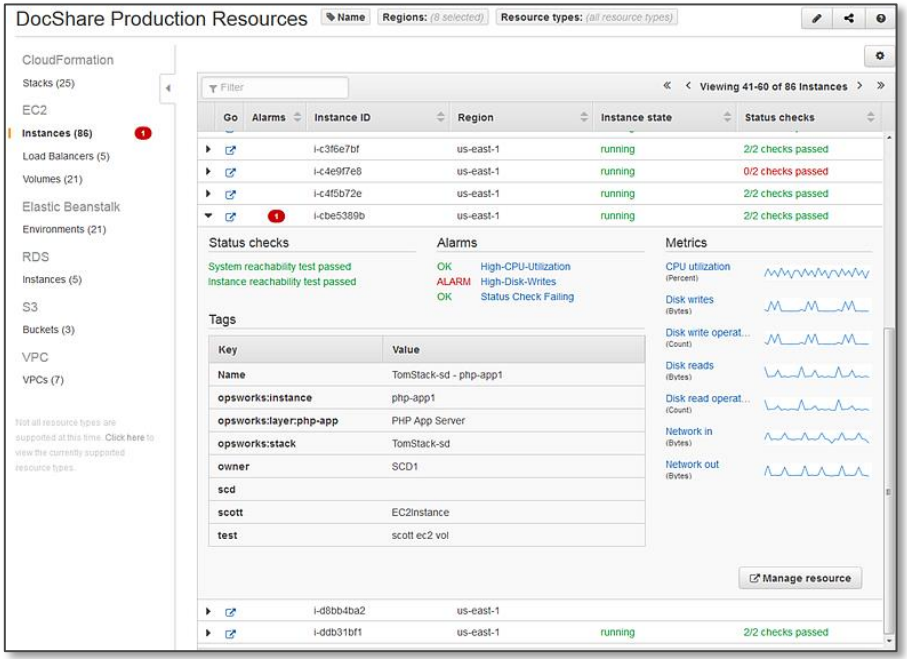


選択したリソースに異なるタグが付いている場合、“Multiple Values”と表示

リソースグループ

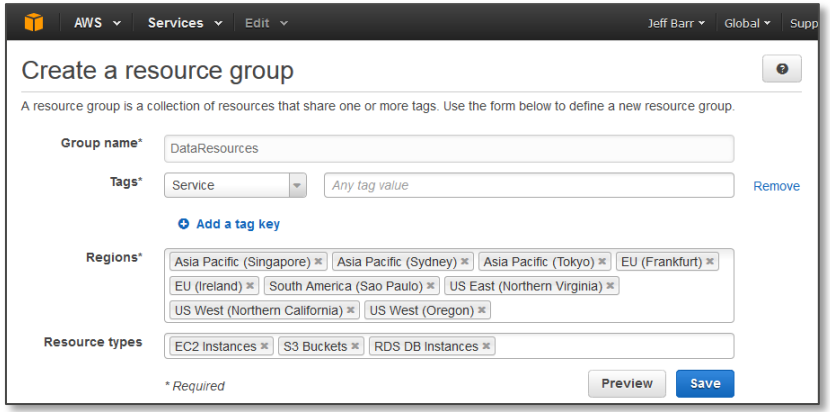
リソースグループ

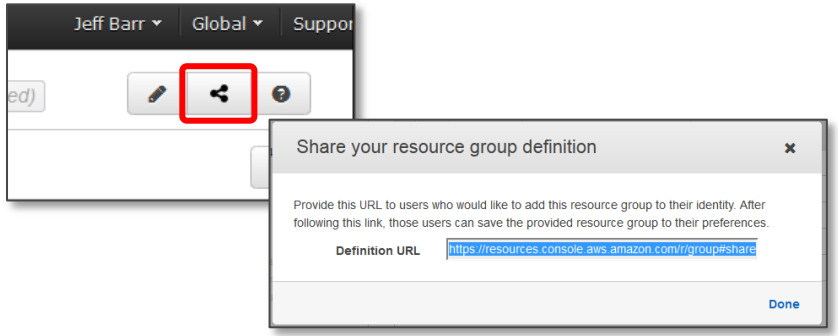
- 共通のタグが付与されたリソースをグループ化
- リージョンをまたいだ
  リソース管理が可能
  - リソース構成情報
  - タグ情報
  - CloudWatch監視状況



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

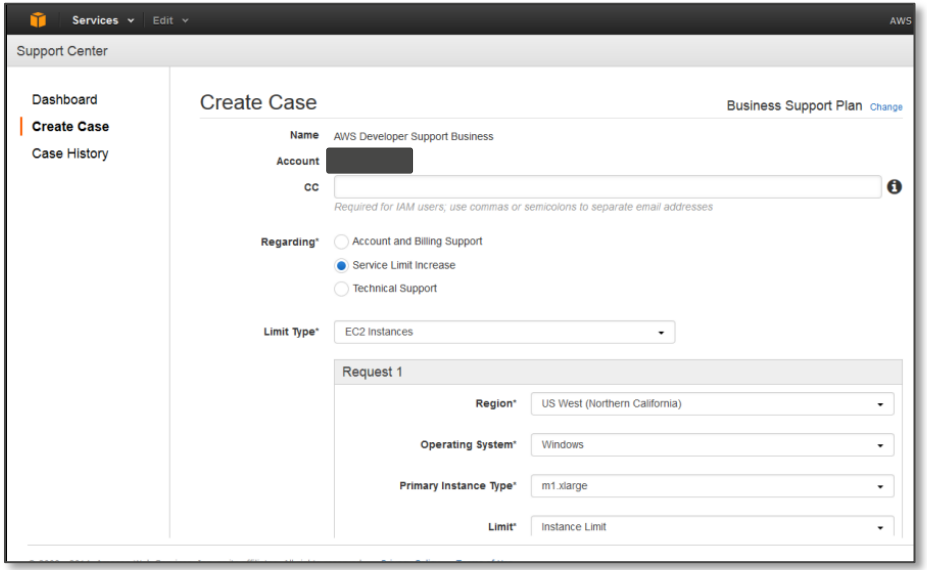




サポートセンター

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

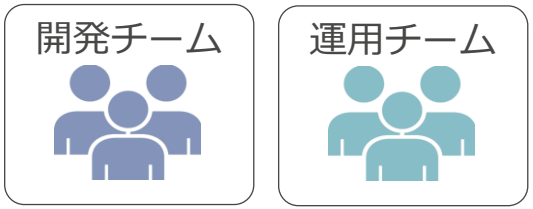


アジェンダ

- 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



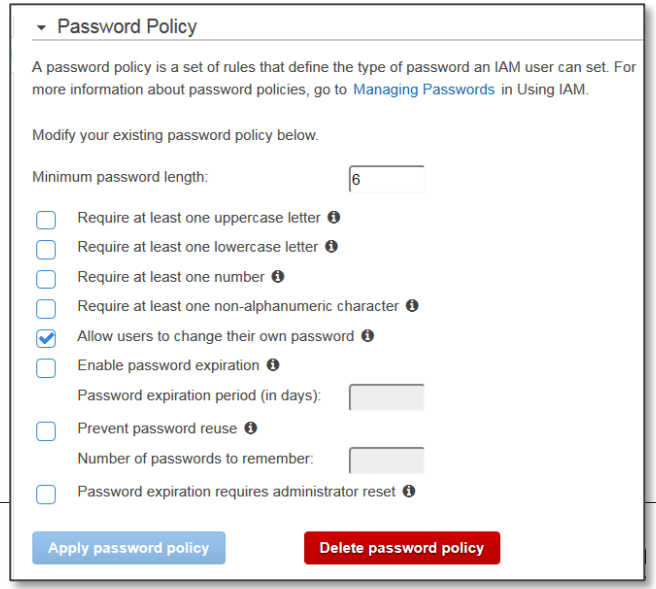
IAM ベストプラクティスのトップ 10

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

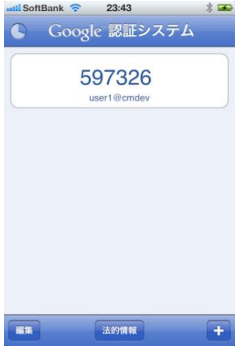
パスワードポリシー

- 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



MFA(多要素認証)

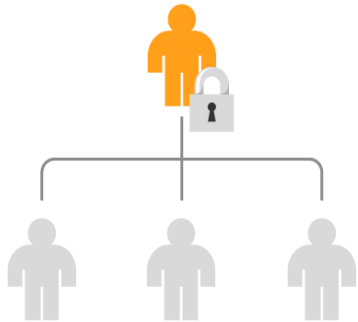
- アカウント・パスワードに加えて、一時認証コードを利用してログイン
- ハードウェアMFA
  - Gemalto社からAWS用のデバイスを購入
  - Tokenタイプ／カードタイプ
- 仮想MFA
  - スマートフォンやPCにインストール
  - Google AuthenticatorなどTOTP実装のソフトが利用可能



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	・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	・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

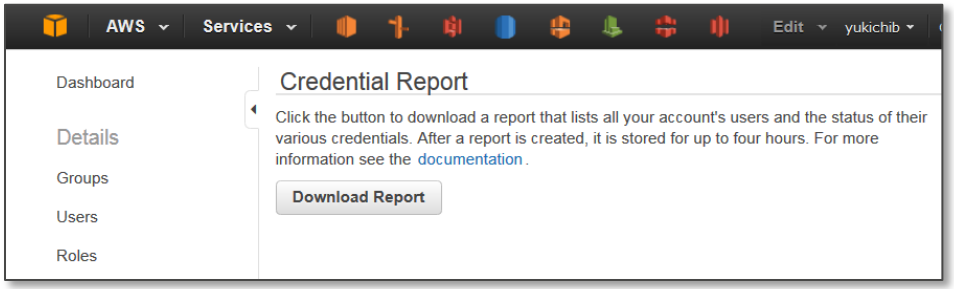
利用者に提供したIAMユーザーの
使用状況を確認したい・・・

アカウント管理者

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・・・

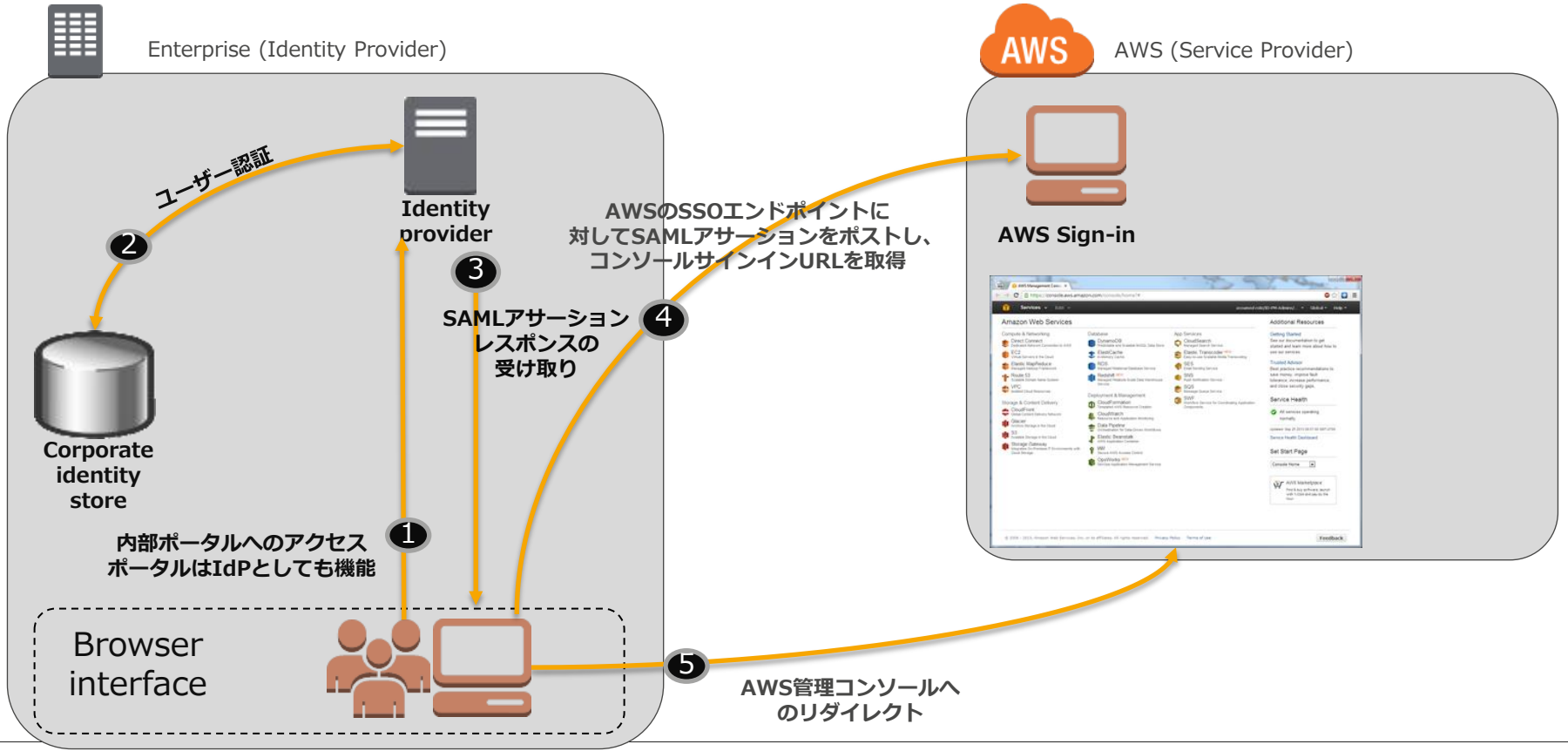
アカウント管理者

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

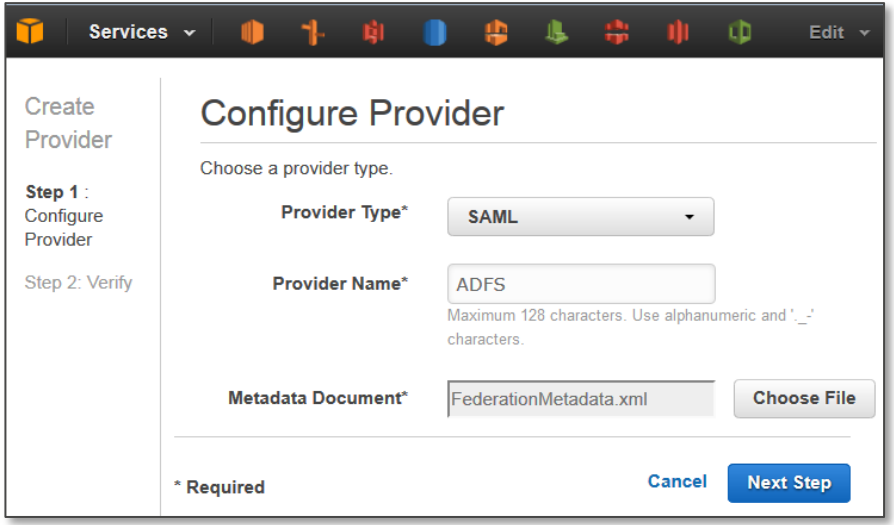


設定手順① -IDプロバイダー設定-

- 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

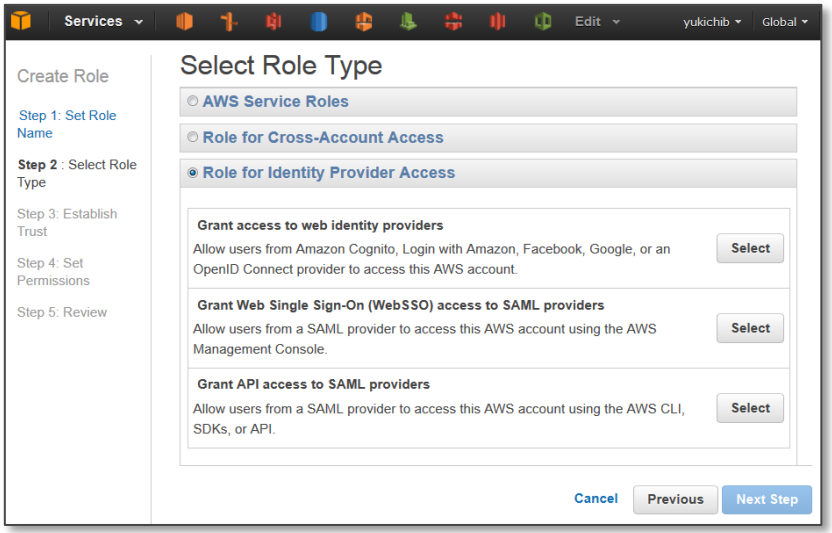
設定手順② -SAMLプロバイダー作成-

- 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



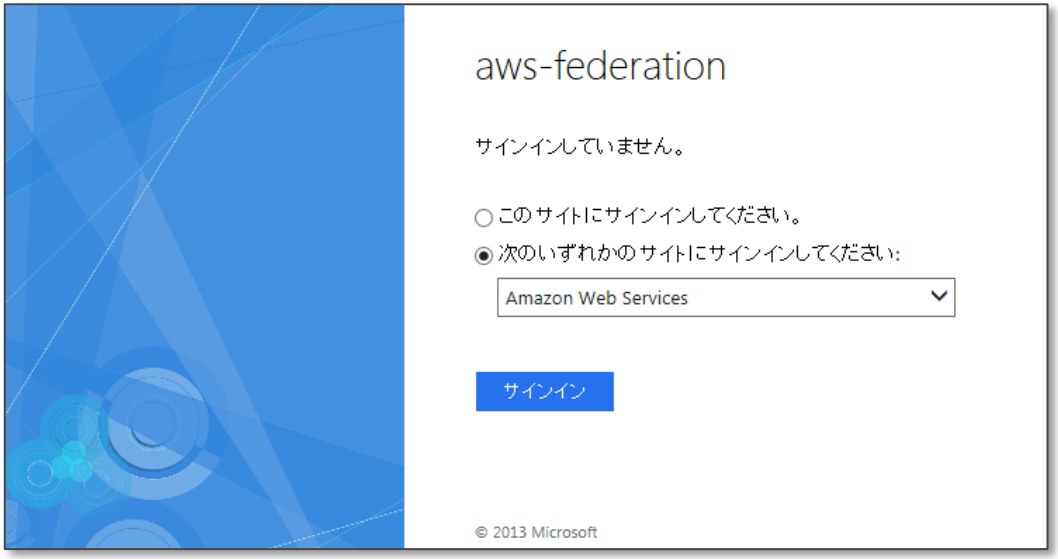
設定手順③ -IAMロール作成-

- 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



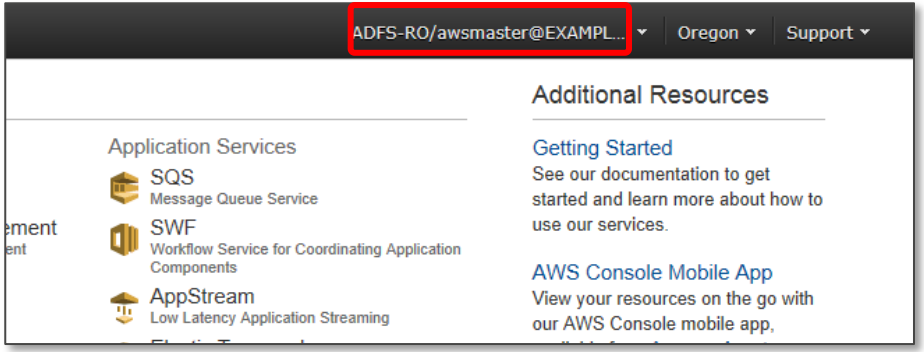
設定手順④ -動作確認-

- 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

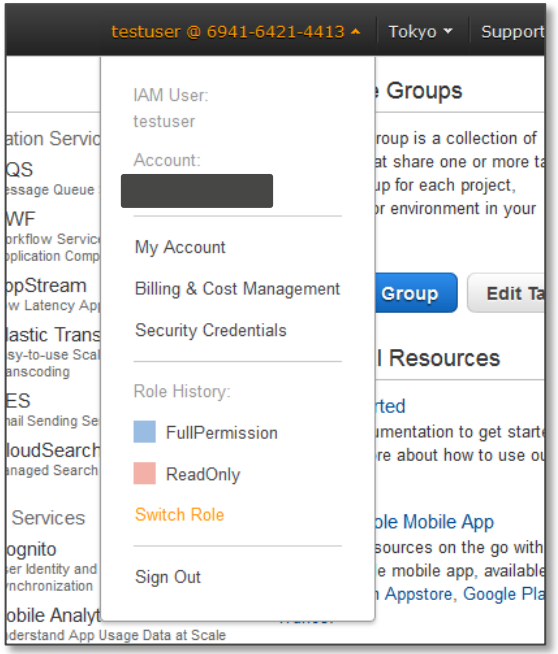
読取専用／更新用の２つの
IAMユーザーが割り当てられている。
アカウント切替が面倒・・・

運用担当者

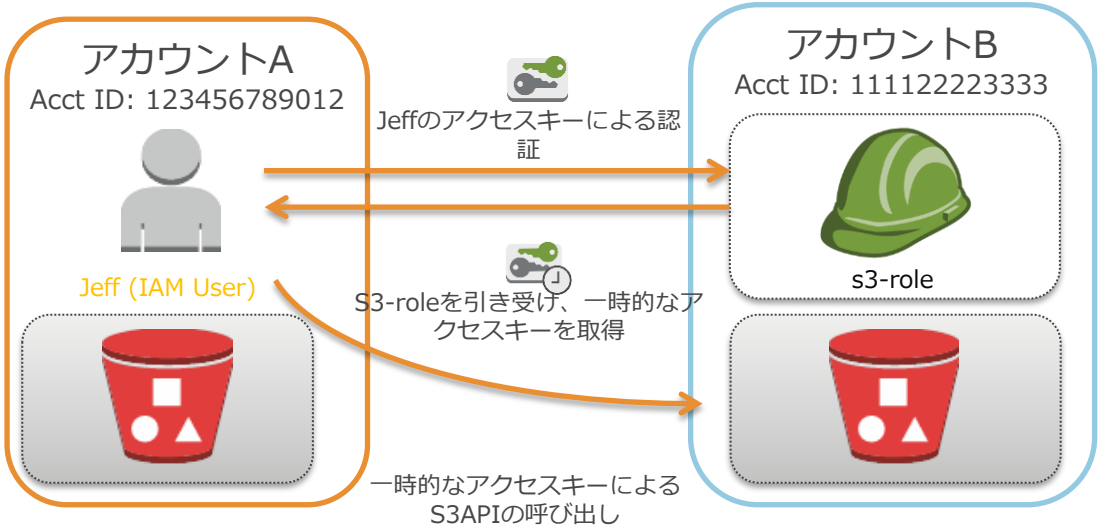
Switch Role

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"
  }
 ]
}
```

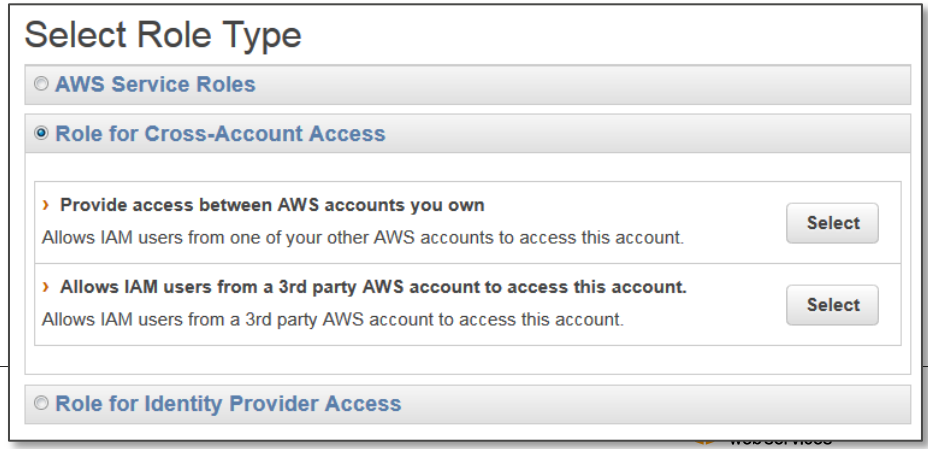
アカウントBのs3-roleを引き受けることを許可するポリシーをJeffに設定

```
{ "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



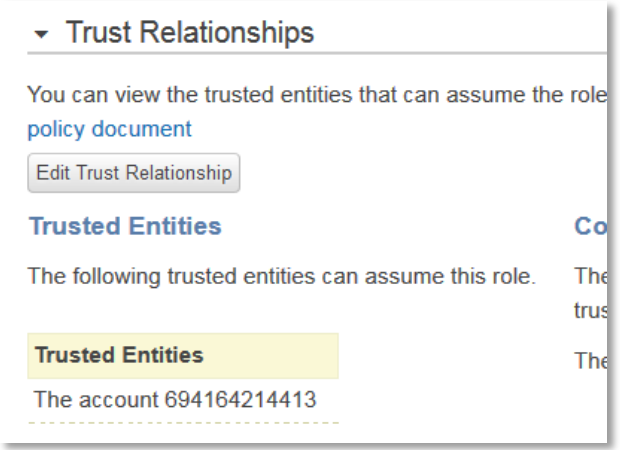
設定手順② -IAMロール編集-

- 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"
```

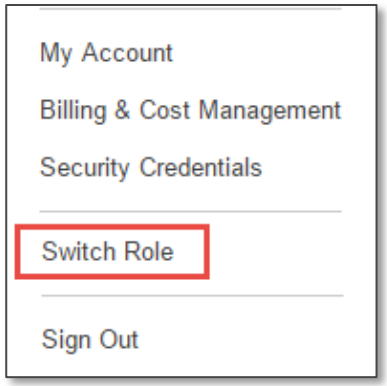
```
"Effect": "Allow",
"Principal": {"AWS": "arn:aws:iam::123456789012:user/IAMUserName"},
"Action": "sts:AssumeRole"
```

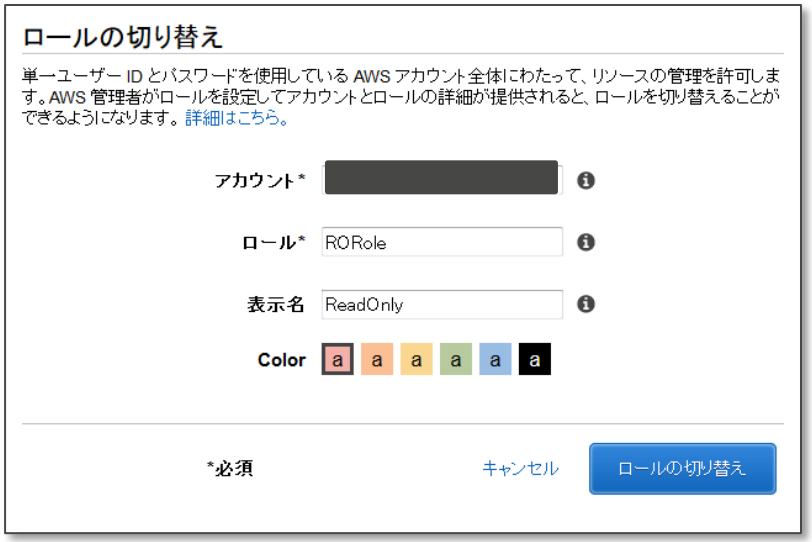
IAMポリシーのプリンシパルではグループ指定ができないため
ユーザーごとに追加が必要



設定手順③ -動作確認-

- IAMユーザーでManagement Consoleにログイン
- SwichRole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

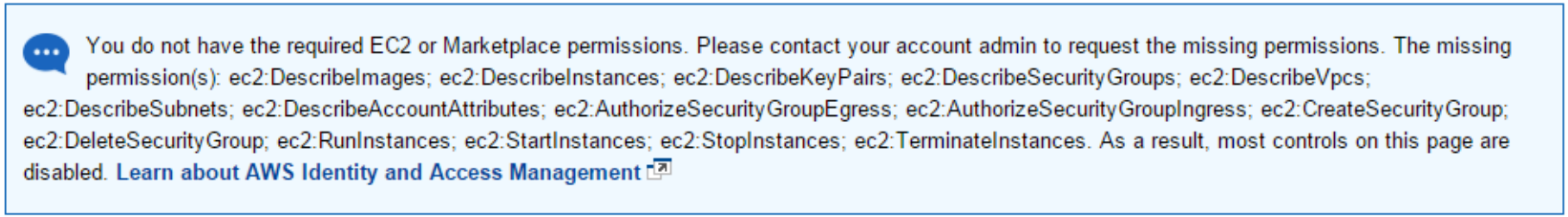
- Management Consoleにログインするipアドレスを制限することはできない
- IAMユーザーのポリシーで、操作が可能なIPアドレスを制限することは可能

```
{
   "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



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

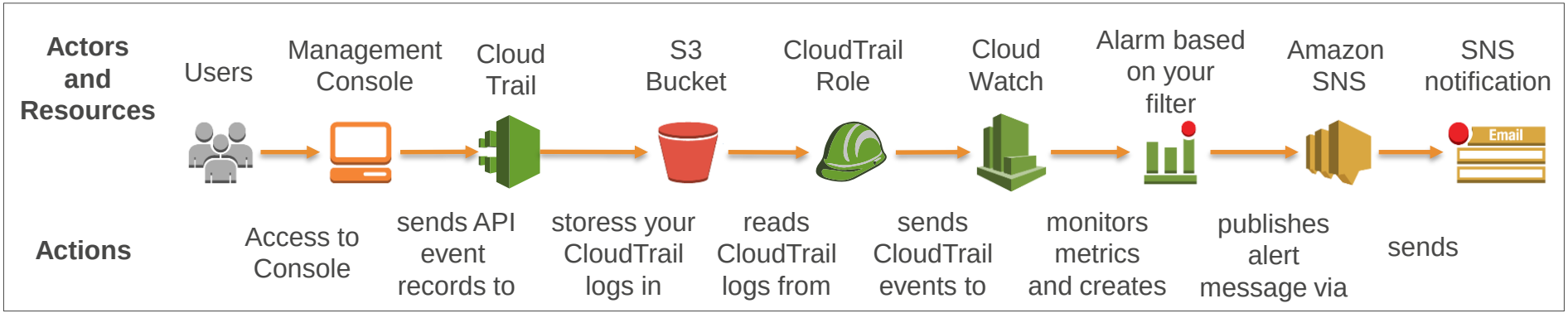
Management Consoleへの
不正ログインを監視／検知したい・・・

セキュリティ管理者

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

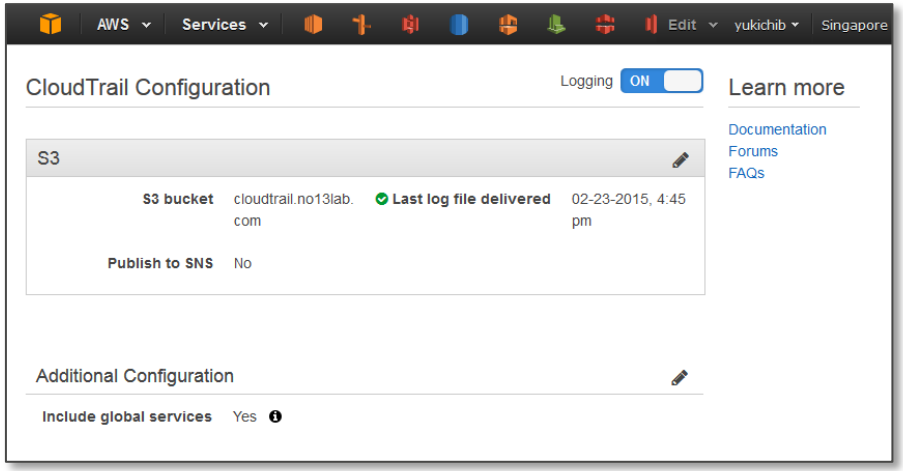


CloudTrailではrootのログイン失敗アクション、全アカウントのログオフアクションは取得不可

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

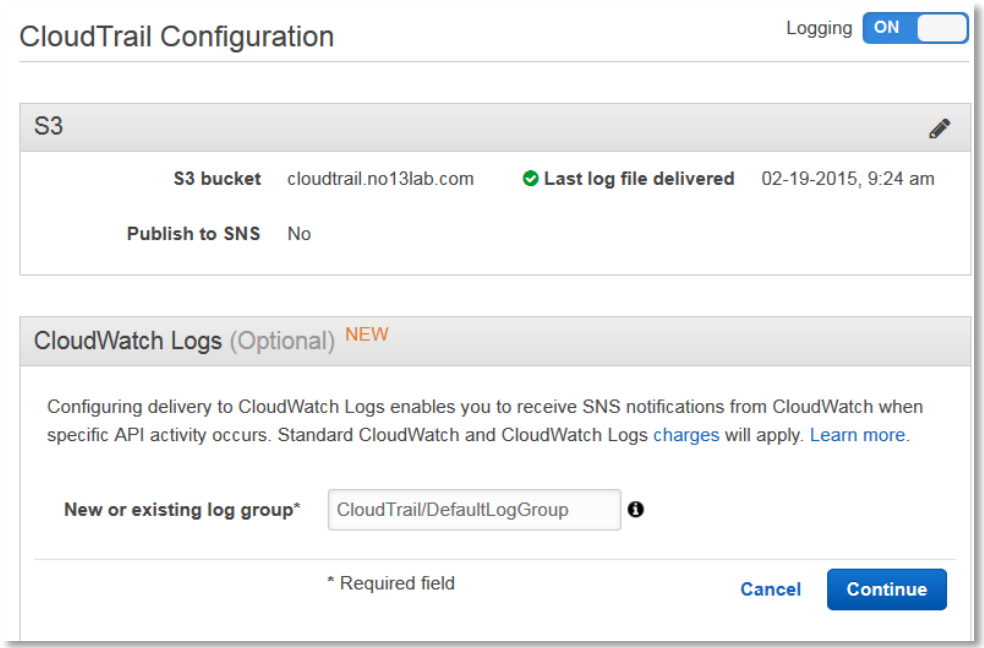
- CloudTrailを有効化
- Include global servicesがYesになっていることを確認



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



CloudTrailコンソール

設定手順③ -メトリックフィルタ作成-

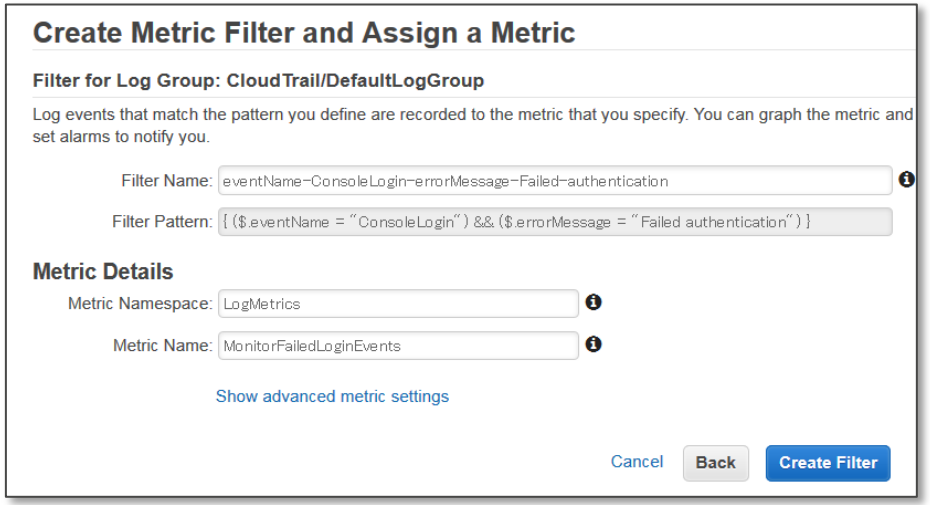
- CloudWatch Logsのメトリックフィルタを作成
  - コンソールログイン失敗

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

  - rootアカウントログイン

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

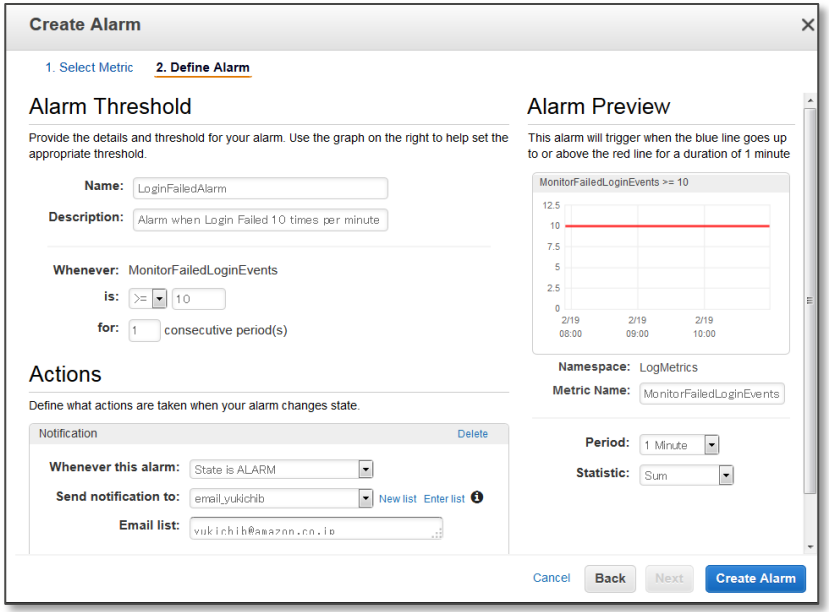
- フィルタパターン
  - 一致/比較：=, !=, <, >, <=, >=
  - 論理演算 ：&&, ||



CloudWatch Logsコンソール

設定手順④ -アラーム作成-

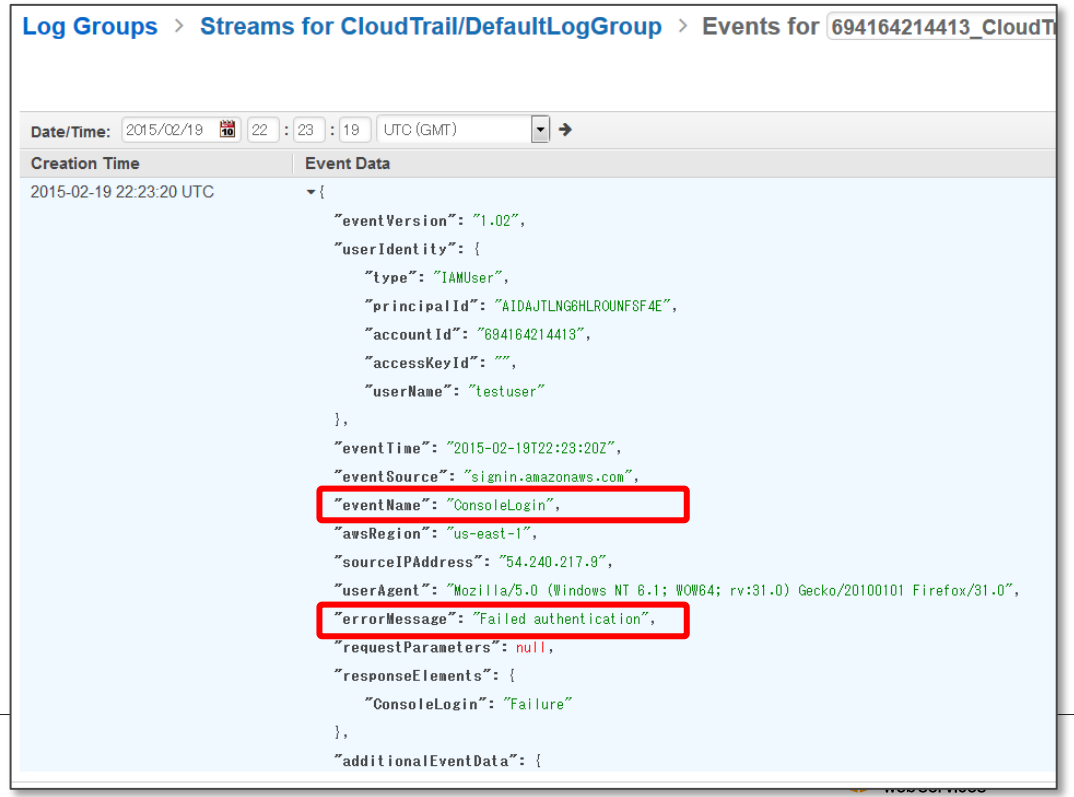
- 作成したメトリックに対するアラームを作成
  - n分間でm回以上イベントが検知された場合に通知するよう設定
  - 通知先を指定



CloudWatchコンソール

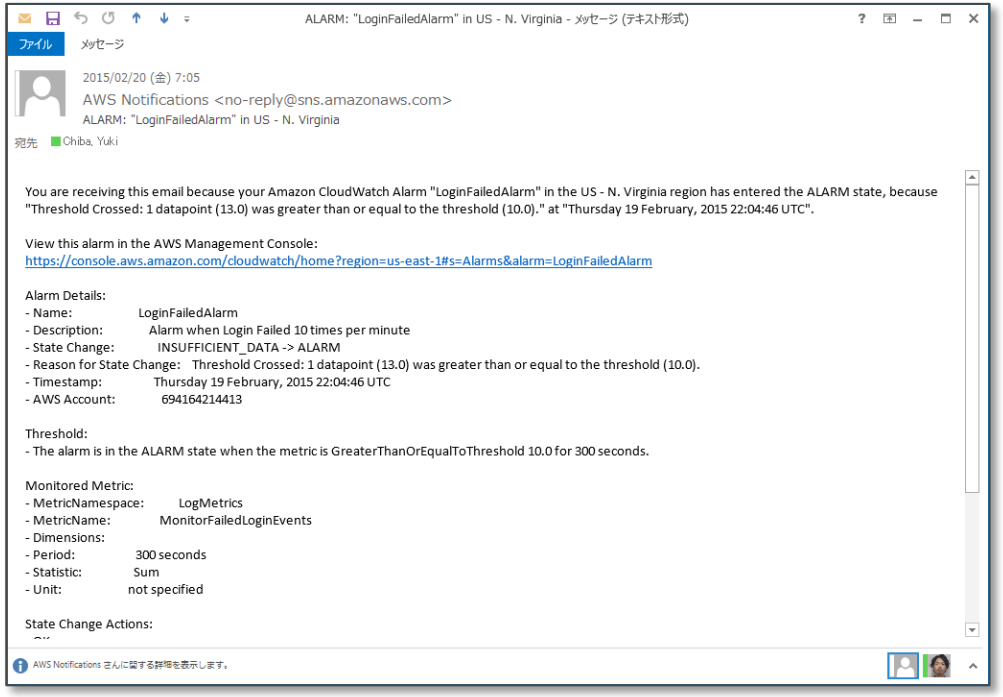
設定手順⑤ -動作確認-

- CloudWatch Logsにイベントが出力されることを確認



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

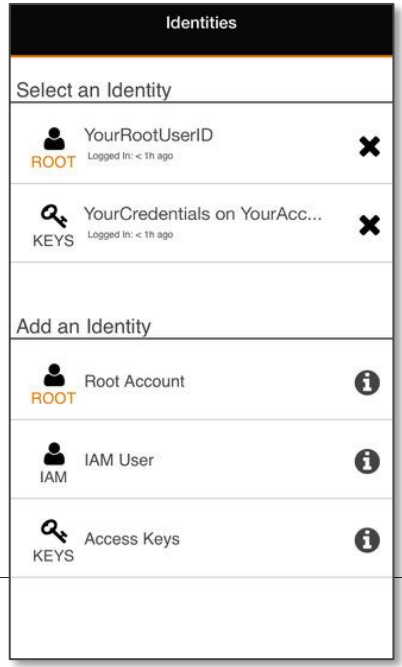


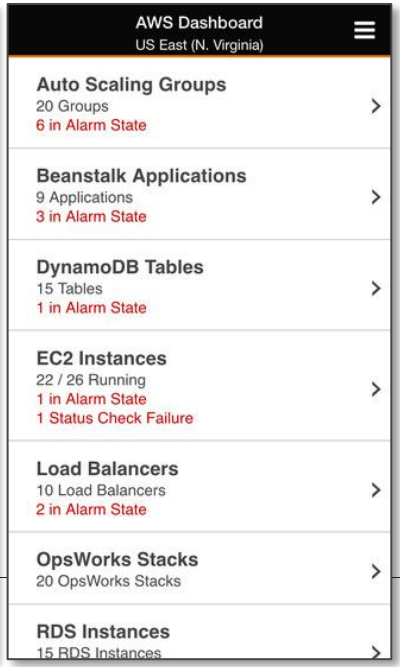
アジェンダ

- 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

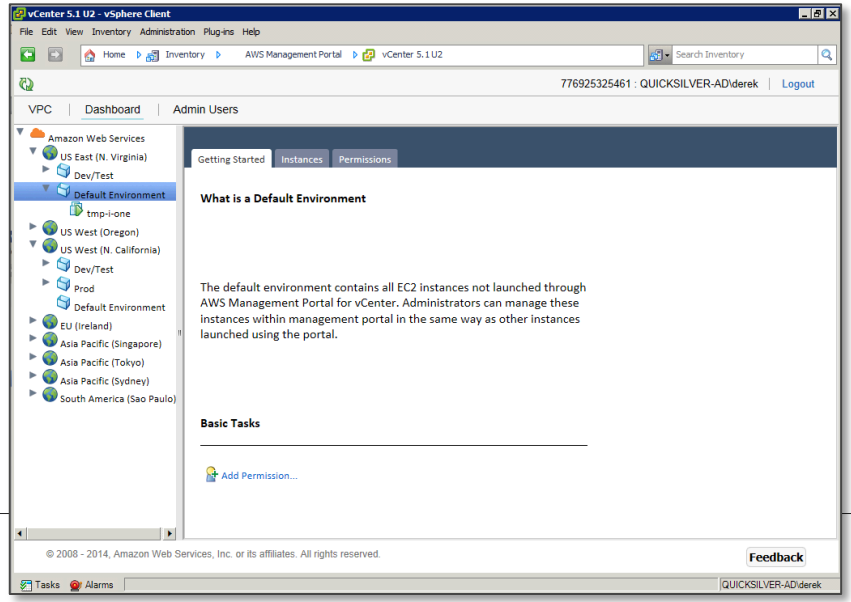
- サポートサービス
  - EC2、ELB、S3、Route53、RDS、AutoScaling、Elastic Beanstalk、DynamoDB、OpsWorks、CloudWatch
- サポートプラットフォーム
  - Android、iOS
- セキュリティ
  - IAMユーザーアカウントでのログイン
  - MFA利用可能





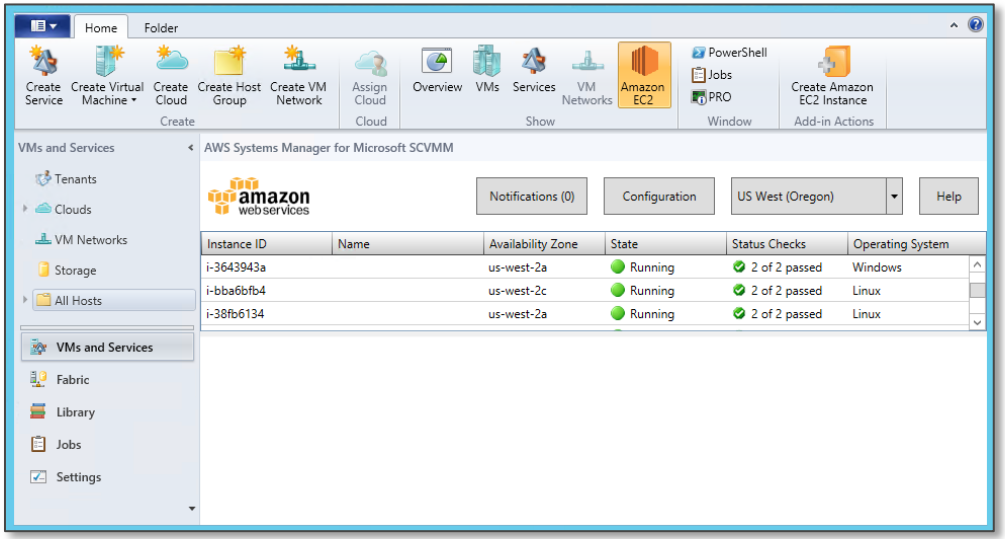
AWS Management Portal for vCenter

- 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



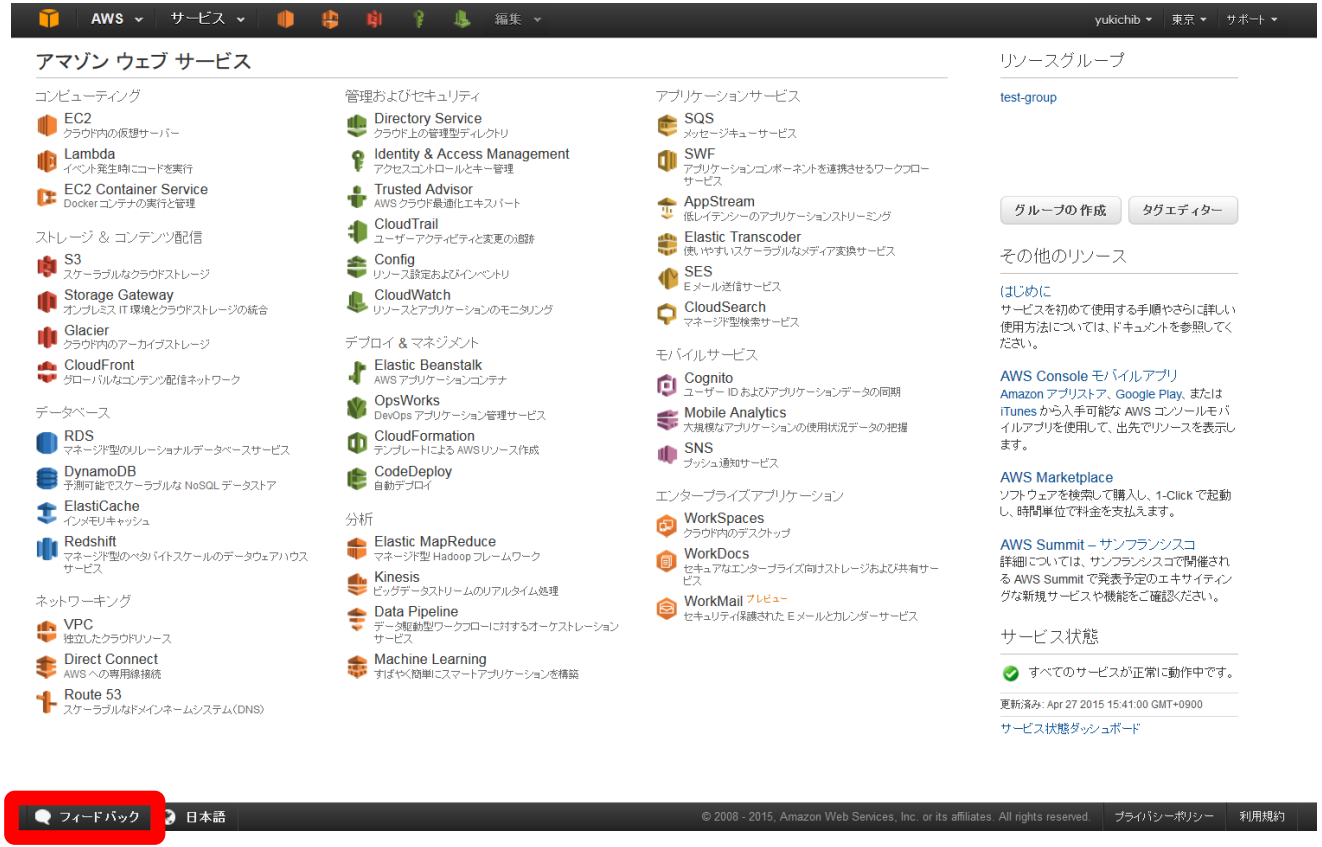
アジェンダ

- 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!


AWS
サービス
編集
yukichib
東京
サポート
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
ネットワーキング
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追跡
Config
リソース設定およびインベントリ
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 – サンフランシスコ
詳細については、サンフラン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ご確認ください。
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
フィードバック
日本語
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.
プライバシーポリシー
利用規約

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