

「ThemiStruct(テミストラクト) Identity Platform」 クックブック

株式会社 オージス総研
サービス事業本部 テミストラクトソリューション部
杉野 真士

ある日 . . .



「明日までに認証基盤用意してね」
by 某ボス



明日までに認証基盤って・・・

社内のいろんな
アプリケーションを
シングルサインオンでき
るようにしないと・・・

認証基盤が停止したら
アプリケーションが使え
なくなるので、構成考え
ないと・・・

今後利用したいアプリケー
ション増えてくるだろうから、追加時の作業が多いと
運用きつくなりそう

すぐに社外からも
セキュアにアクセス
したいとかの要望が
でるだろうな

月末月初とかのアクセス
が殺到するピークの時に
遅くなったらダメだよな



そんな無茶な . . .



そんなとき



某同僚
「すぎのさん、すぎのさん。
最近こんなの作ってみたんだけど
試してみてくださいよ」



ThemiStruct Identity Platform ?



ThemiStruct Identity Platformは



ブラウザからの操作で短時間で構築できる

AWSのサービスを利用した高い可用性を持ち、
大量ユーザアクセスも対応できる認証基盤に仕上がる

クラウドサービスや業務アプリケーションに
フェデレーション/エージェント/リバースプロキシ方式
で接続できる

アプリケーションへの接続は
少ない作業で簡単に接続できる

IPアドレスによる制御やOTPなどの多要素認証などで
認証強化を行うことができる

という認証基盤です。

これ使ったら・・・

社内やクラウドサービスなどの
アプリとも接続できそう

社内のいろいろな
アプリケーションを
シングルサインオンでき
るようにしないと・・・

認証基盤が停止したら
アプリケーションが使え
なくなるので、構成考え
ないと・・・

AWSのサービスを利用して
可用性高い構成みたい

今後利用したいアプリケー
ション増えてくるだろうから、追加時の作業が多いと
運用きつくなりそう

アプリ接続作業
も難しくなさそう

月末月初とかのアクセス
が殺到するピークの時に
遅くなったらダメだね

突発的なスパイクアクセス
にも対応できそう

すぐに社外からも
セキュアにアクセス
したいとかの要望が
でるだろうな

OTPなどを組み合わせた
多要素認証でできそう



これなら明日までに
できるかも！

Let's get cooking.



調理の流れ

- 下ごしらえ
- 認証基盤調理
 - マネジメントコンソール作成
 - Identity Platform作成
- 盛り付け
 - アプリケーション接続
 - Office 365 も接続



調理作業時間目安
10分

第 1 章

下ごしらえ

下記しえ

- AWSのご契約
- 構築用ユーザの作成
- VPC及びサブネット作成
- 認証基盤用ドメイン登録

etc



AWSアカウントの作成



サインイン、または AWS アカウントを作成

Eメールアドレスまたは携帯電話の番号を入力してください。

Eメールまたは携帯番号:

☒ 私は新規ユーザーです。

☐ 私は既存のユーザーです
パスワード:

[サインイン\(セキュリティシステムを使う\)](#)

[パスワードをお忘れですか？](#)

[AWS Identity and Access Management](#) および [AWS Multi-Factor Authentication](#) の詳細、および AWS アカウントのセキュリティを強化するための特徴を確認してください。 [AWS 無料利用枠提供規約](#)の詳細を参照してください。

Amazon.com のサインインについて

アマゾン ウェブ サービスは、Amazon.com アカウントの情報をを使用してユーザーを識別し、アマゾン ウェブ サービスへのアクセスを許可します。このサイトの利用は、以下のリンクにある利用規約およびプライバシーポリシーによって管理されます。アマゾン ウェブ サービスの製品およびサービスの利用は、AWS 付加価値再販業者からそれらの製品およびサービスを購入した場合を除き、以下のリンクにある AWS カスタマーアグリーメントによって管理されます。

[利用規約](#) [プライバシーポリシー](#) [AWS カスタマーアグリーメント](#) © 1996-2016, ©1996-2014, Amazon.com, Inc. or its affiliates.

An [amazon.com](#) company

新しい AWS アカウントには以下の特典が含まれます。

AWS 無料利用枠を 12 か月間利用可能

Amazon EC2: Amazon EC2: Windows および Linux t2.micro のインスタンスを 1 か月あたり 750 時間利用可能

Amazon S3: 5 GB のストレージ

Amazon RDS: マイクロ DB インスタンスを 1 か月あたり 750 時間利用可能

Amazon DynamoDB: 25GB のストレージ、月に最大 2億件の要求

AWS ベーシックサポートの特徴

カスタマーサービス: 1 日 24 時間/週 7 日/年 365 日

サポートフォーラム

ドキュメント、白書およびベストプラクティスガイド

その他の使用条件については aws.amazon.com/jp/free にアクセスしてください。

構築用ユーザの作成

IAM画面からユーザを作成

アクセスキーIDとシークレットアクセスキーを取得

ダッシュボード

IAM の検索

詳細

グループ

ユーザー

ロール

ポリシー

ID プロバイダ

アカウント設定

認証情報レポート

暗号化キー

Identity and Access Management へようこそ

IAM ユーザーのサインインリンク:
[https://\[redacted\].signin.aws.amazon.com/console](https://[redacted].signin.aws.amazon.com/console) [カスタマイズ](#) | [リンクのコピー](#)

IAM リソース

ユーザー: 43	ロール: 70
グループ: 9	ID プロバイダ: 2
カスタマー管理ポリシー: 6	

セキュリティステータス

5 項目中 4 項目が完了しています

- ☒ ルートアカウント
- ☒ 個々の IAM ユーザー
- ☒ グループを付与
- ☒ IAM パスワード

☒ 1 ユーザーが正常に作成されました。
これは、これらのユーザーセキュリティ認証情報をダウンロードできる最後の機会です。
これらの認証情報はいつでも管理および再作成できます。

▼ ユーザーのセキュリティ認証情報を非表示

IPUSER	
アクセスキー ID:	[redacted]
シークレットアクセスキー:	[redacted]

VPCとサブネット作成

ThemiStruct Identity Platformを構築するVPCを作成

1 個のパブリックサブネットを持つ VPC

パブリックとプライベート サブネットを持つ VPC

パブリックとプライベート サブネットおよびハードウェア VPN アクセスを持つ VPC

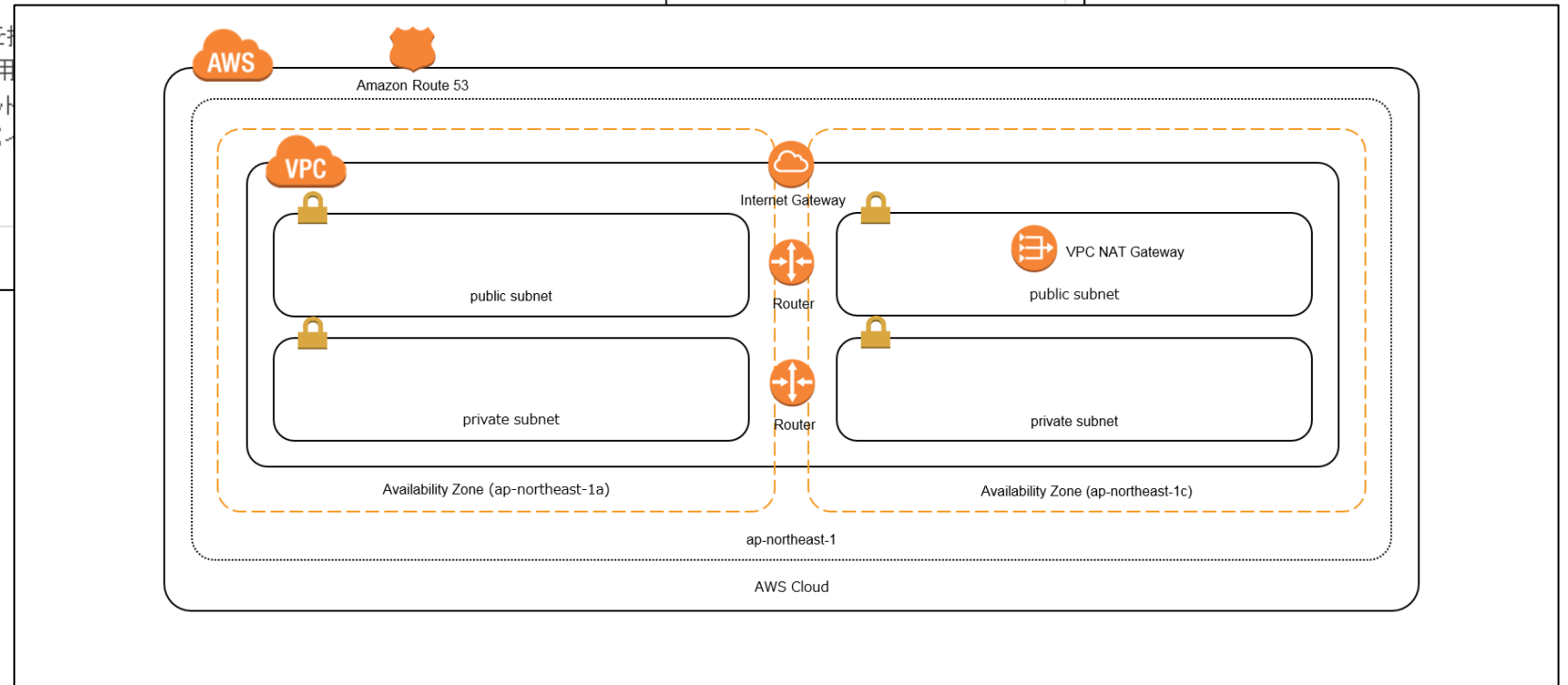
プライベートのサブネットおよびハードウェア VPN アクセスを持つ VPC

この設定は、パブリックサブネットに加えて、インスタンスにインターネットからアドレスを指定できないプライベートサブネットを追加します。プライベートサブネットのインスタンスでは、ネットワークアドレス変換(NAT)を使用してパブリックサブネットを介してインターネットへのアウトバウンド接続を確立できます。

作成:

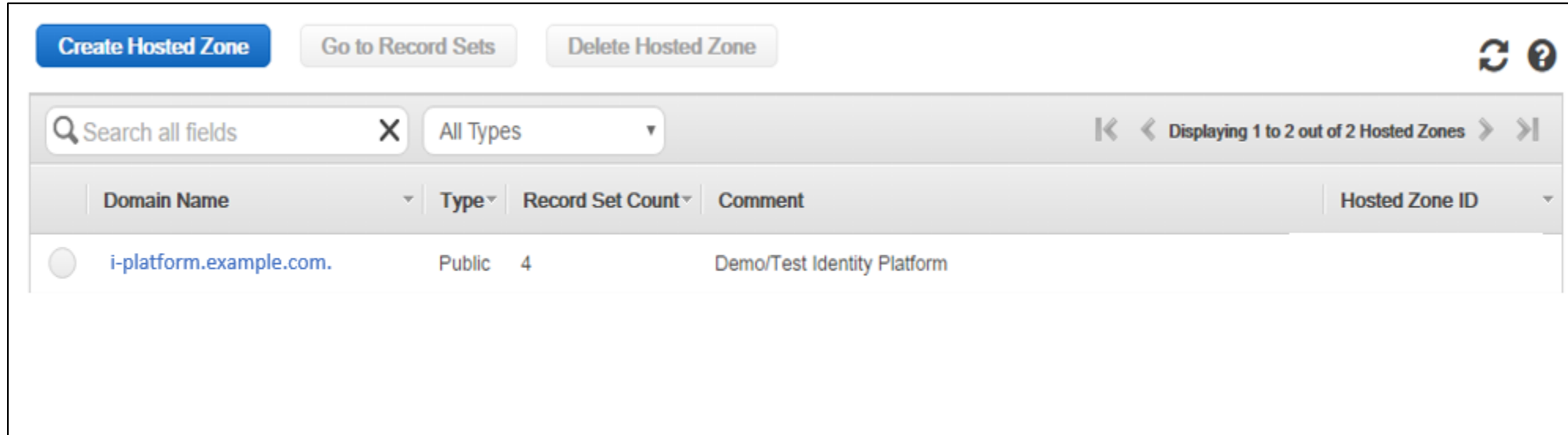
2 個の /24 サブネットを持つ VPC は Elastic IP を使用したインスタンスは、ネットワークアドレス変換(NAT) デバイスを使用します。(NAT デバイス)

インターネット、S3、DynamoDB、SNS、SQS、その他



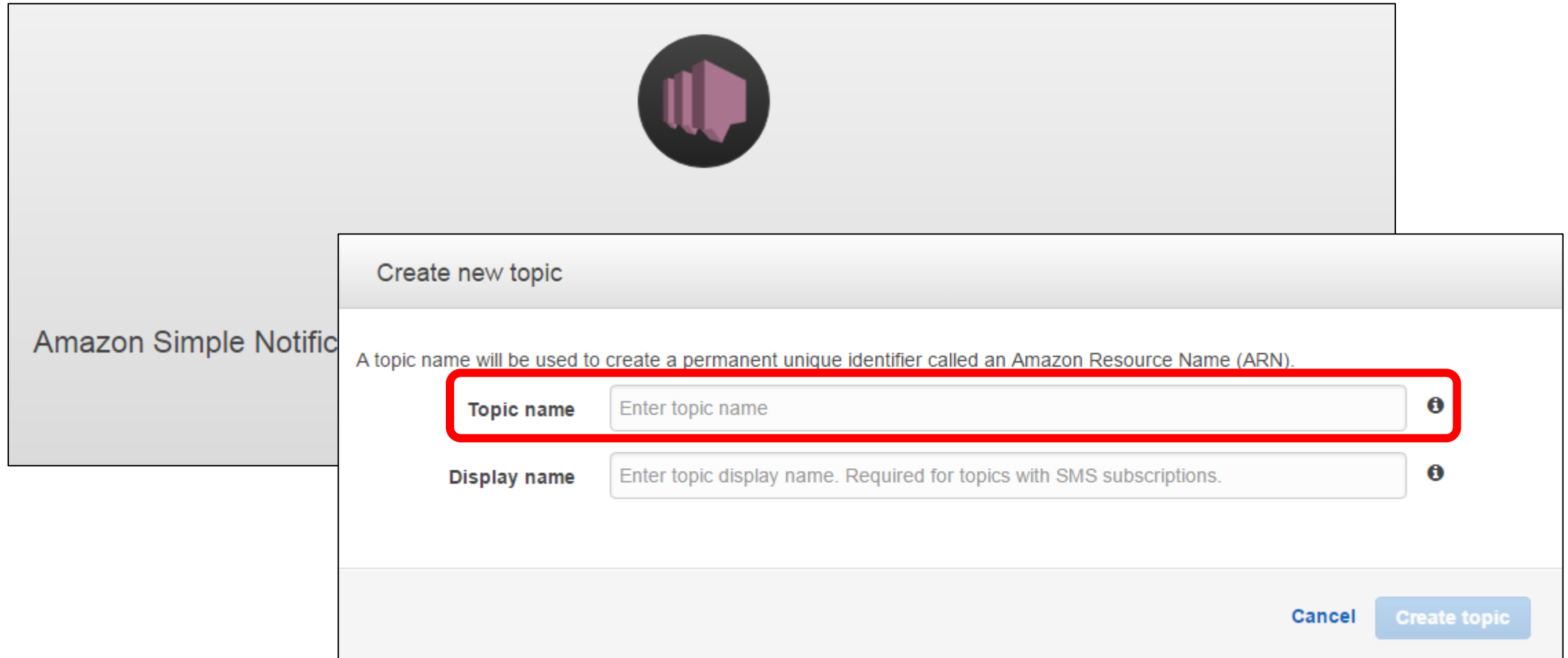
DNSへのドメイン設定 (Route53)

ThemiStruct Identity Platform用ドメインをRoute53に登録



通知用TOPICの作成

各種通知用のSNS TOPICを作成



The screenshot shows the Amazon Simple Notification Service (SNS) console. In the background, there is a large gray box with the Amazon SNS logo and the text "Amazon Simple Notific". In the foreground, a "Create new topic" dialog is open. The dialog has a title bar "Create new topic" and a subtitle "A topic name will be used to create a permanent unique identifier called an Amazon Resource Name (ARN)". There are two input fields: "Topic name" and "Display name". The "Topic name" field is highlighted with a red rectangle. The "Display name" field has a placeholder text "Enter topic display name. Required for topics with SMS subscriptions." At the bottom right of the dialog, there are two buttons: "Cancel" and "Create topic".

Amazon Simple Notific

Create new topic

A topic name will be used to create a permanent unique identifier called an Amazon Resource Name (ARN).

Topic name Enter topic name ⓘ

Display name Enter topic display name. Required for topics with SMS subscriptions. ⓘ

Cancel Create topic

次工程のために以下を準備&メモしておきます

アクセスキーID

シークレットアクセスキー

インストール先のVPCのID

インストール先のサブネットのID

Identity Platform用のドメイン名

通知のためのSNS TOPIC名

Identity Platform用サーバ証明書

マネージメントコンソール用サーバ証明書

メンテナンス通信（SSH）用の公開鍵

下ごしらえ完了

調理の目安
2時間00分

第 2 章

認証基盤の調理

認証基盤の調理の流れ

- マネージメントコンソール作成
- ThemisStruct

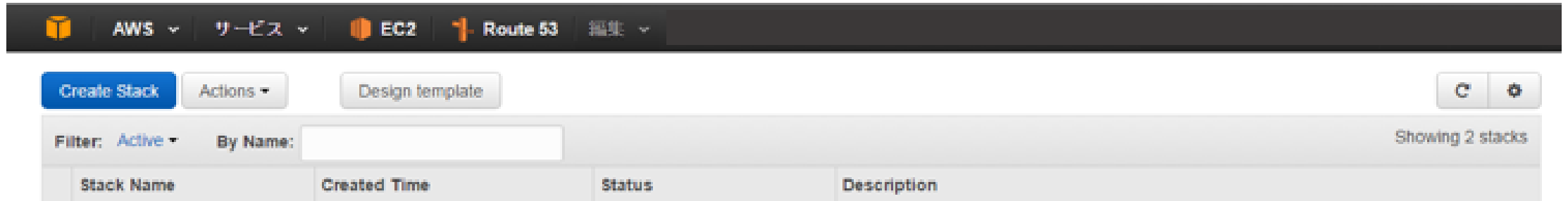
Identity Platform作成



マネージメントコンソール 作成開始！

Create Stack

CloudFormationからCreate Stackをクリック



Identity Platformテンプレート選択

ThemiStruct Identity Platform用テンプレートをアップロード

Create stack

Select Template

Specify Details

Options

Review

Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template

Use AWS CloudFormation Designer to create or modify an existing template. [Learn more.](#)

Design template

Choose a template

A template is a JSON-formatted text file that describes your stack's resources and their properties. [Learn more.](#)

☐ Select a sample template

☒ Upload a template to Amazon S3

ファイルを選択 identityplat...m-setup.json

☐ Specify an Amazon S3 template URL

Cancel

Next

マネジメントコンソール作成時情報入力

インストールするVPC

インストールするサブネット

MCへアクセス可能なIPアドレス

MCへSSHするためのユーザ名

MCへSSHするためのSSH公開鍵

インストールするドメイン名

通知のためのSNS TOPIC名

ThemiStruct Identity Platform用アクセスキー

ThemiStruct Identity Platform用シークレットキー

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more](#)

Stack name

Parameters

Network Configuration

VPC

Specifies the VPC ID to launch the EC2 of the Management Console.

PublicSubnet

Specifies the Subnet ID to launch the EC2 of the Management Console.

AllowedIPAddress

Specifies the IP address(CIDR) to allow access to EC2 of the Management Console. (e.g. 192.0.2.0/24)

EC2 Instance of Management Console Configuration

SSHUserName

Specifies the ssh user name of Management Console. (e.g. operationuser)

SSHPublicKey

Specifies the public key connecting to EC2 of the Management Console via SSH.

DomainName

Specifies the domain name managed on Route 53. It's set automatically as the domain name of the Identity Platform. (e.g. example.com)

NotificationTopic

Specifies the Notification Topic ARN.

CodeCommit Configuration

RepositoryAccessKey

Specifies the key of access to the software repository.

RepositorySecretKey

Specifies the secret of access to the software repository.

Other parameters

HostName

Specifies the Host Name of Management Console.

Cancel

Previous

Next

マネジメントコンソール作成時情報入力（ここで考える項目）

インストールするVPC

インストールするサブネット

MCへアクセス可能なIPアドレス

MCへSSHするためのユーザ名

MCへSSHするためのSSH公開鍵

インストールするドメイン名

通知のためのSNS TOPIC名

ThemiStruct Identity Platform用アクセスキー

ThemiStruct Identity Platform用シークレットキー

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more](#)

Stack name

Parameters

Network Configuration

VPC

Search by ID, or Name tag value

Specifies the VPC ID to launch the EC2 of the Management Console.

PublicSubnet

Search by ID, or Name tag value

Specifies the Subnet ID to launch the EC2 of the Management Console.

AllowedIPAddress

Specifies the IP address(CIDR) to allow access to EC2 of the Management Console. (e.g. 192.0.2.0/24)

EC2 Instance of Management Console Configuration

SSHUserName

Specifies the ssh user name of Management Console. (e.g. operationuser)

SSHPublicKey

Specifies the public key connecting to EC2 of the Management Console via SSH.

DomainName

example.com
Specifies the domain name managed on Route 53. It's set automatically as the domain name of the Identity Platform. (e.g. example.com)

NotificationTopic

Specifies the Notification Topic ARN.

CodeCommit Configuration

RepositoryAccessKey

Specifies the key of access to the software repository.

RepositorySecretKey

Specifies the secret of access to the software repository.

Other parameters

HostName

console
Specifies the Host Name of Management Console.

Cancel Previous Next

インストール開始

マネージメントコンソールのインストール開始

The screenshot shows the AWS CloudFormation console interface. At the top, there's a navigation bar with 'AWS', 'サービス' (Services), 'EC2', and 'Route 53'. Below this, there are buttons for 'Create Stack', 'Actions', and 'Design template'. A filter section shows 'Filter: Active' and 'By Name:'. The main table lists stacks, with one stack 'i-Platform-demo' highlighted, showing a status of 'CREATE_IN_PROGRESS'. Below the table, there's a tabbed interface with 'Overview', 'Outputs', 'Resources', 'Events', 'Template', 'Parameters', 'Tags', 'Stack Policy', and 'Change Sets'. The 'Events' tab is selected, showing a list of events for the stack, including a 'User Initiated' event.

Stack Name	Created Time	Status	Description
i-Platform-demo	2016-07-27 15:29:46 UTC+0900	CREATE_IN_PROGRESS	AWS CloudFormation Template : Create Management Console of Identity Platform.

Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy	Change Sets
2016-07-27	Status	Type	Logical ID	Status reason				
15:29:46 UTC+0900	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	i-Platform-demo	User Initiated				

30分蒸らします

マネージメントコンソール 完成！



Identity Platform 調理開始！

15工程で調理していきます (味付け5分、焼き/蒸らし90分)



Identity Platformインストール時入力項目

アクセスキーID	複数のアベイラビリティゾーンでのレプリケーション
シークレットアクセスキー	RDSのインスタンスクラス
Availability-Zone-1aのサブネットID	データベースの名称
Availability-Zone-1cのサブネットID	データベースのユーザー
Identity Platformのホスト名	ユーザーのパスワード
DNSのHosted Zone	バックアップの保存期間
セットアップするステージ	Identity Platformのサーバ証明書
管理者のパスワード	Identity Platformの証明書の秘密鍵
踏み台として作成するEC2のAMIのID	Identity Platformの中間証明書
踏み台のホスト名	CloudFrontのログを格納するS3のバケット名
踏み台のログインユーザ名	各種コンテンツを格納するS3のバケット名
SSH接続を行う公開鍵	Management Consoleのサーバ証明書
接続を許可するCIDR IPアドレス	Management Consoleの証明書の秘密鍵
	Management Consoleの中間証明書

Identity Platformインストール時入力項目（ここで考える項目）

アクセスキーID	複数のアベイラビリティゾーンでのレプリケーション
シークレットアクセスキー	RDSのインスタンスクラス
Availability-Zone-1aのサブネットID	データベースの名称
Availability-Zone-1cのサブネットID	データベースのユーザー
Identity Platformのホスト名	ユーザーのパスワード
DNSのHosted Zone	バックアップの保存期間
セットアップするステージ	Identity Platformのサーバ証明書
管理者のパスワード	Identity Platformの証明書の秘密鍵
踏み台として作成するEC2のAMIのID	Identity Platformの中間証明書
踏み台のホスト名	CloudFrontのログを格納するS3のバケット名
踏み台のログインユーザ名	各種コンテンツを格納するS3のバケット名
SSH接続を行う公開鍵	Management Consoleのサーバ証明書
接続を許可するCIDR IPアドレス	Management Consoleの証明書の秘密鍵
	Management Consoleの中間証明書

1. AWS情報設定

入力項目

- アクセスキーID
- シークレットアクセスキー

The screenshot displays the 'Identity Platform' setup interface. At the top, a progress bar shows 15 steps. Step 1, 'AWS情報設定' (AWS Information Setting), is the current step and is highlighted with a green circle. Below the progress bar, the title 'AWS情報設定' is displayed. The main area contains two input fields: 'アクセスキーID*' (Access Key ID) and 'シークレットアクセスキー*' (Secret Access Key). Both fields are currently empty. At the bottom of the form, there are 'Previous' and 'Next' buttons. The 'Next' button is green and active. The footer of the page contains the copyright notice: 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

Identity Platform

Identity Platformのセットアップ

Step 1 Step 2 Step 3 Step 4 Step 5 Step 6 Step 7 Step 8 Step 9 Step 10 Step 11 Step 12 Step 13 Step 14 Step 15

AWS情報設定

アクセスキーID*

シークレットアクセスキー*

Previous Next

Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.

2. 共通設定

入力項目

- ・サブネットID情報
- ・Identity Platformホスト名
- ・ドメイン名
- ・ステージ名
- ・管理者のパスワード

The screenshot shows the 'Identity Platform' setup wizard. At the top, a progress bar indicates 15 steps. Step 2, '共通設定' (Common Settings), is the current step and is highlighted in green. Below the progress bar, the title 'Identity Platformのセットアップ' (Setup of Identity Platform) is displayed. The main content area is titled '共通設定' (Common Settings) and contains several input fields:

- 'Availability-Zone-1aのサブネットID*' (Subnet ID for Availability Zone 1a) with a dropdown menu.
- 'Availability-Zone-1cのサブネットID*' (Subnet ID for Availability Zone 1c) with a dropdown menu.
- 'Identity Platformのホスト名*' (Identity Platform host name) with a text input field.
- 'DNSのHosted Zone*' (DNS Hosted Zone) with a text input field.
- 'セットアップするステージ*' (Stage to set up) with a text input field.
- '管理者のパスワード*' (Administrator password) with a text input field.

At the bottom of the form, there are 'Previous' and 'Next' buttons. The 'Next' button is green and active. The footer of the page reads 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

3. 踏み台構築

入力項目

- ・ 踏み台サーバのホスト名
- ・ 踏み台サーバのユーザ名
- ・ 踏み台サーバの
SSH接続公開鍵
- ・ 踏み台サーバへの
アクセス許可IP

The screenshot shows the 'Identity Platform' setup wizard. At the top, a progress bar displays 15 steps. Step 3, '踏み台構築' (Jump Box Construction), is highlighted in green. Below the progress bar, the title '踏み台構築' is shown. The form contains five input fields, each with a label and an asterisk indicating it is required:

- 踏み台として作成するEC2のAMIのID* (EC2 AMI ID to create as jump box): A dropdown menu.
- 踏み台のホスト名* (Jump box host name): A text input field.
- 踏み台のログインユーザ名* (Jump box login username): A text input field.
- SSH接続を行う公開鍵* (Public key for SSH connection): A text input field.
- 接続を許可するCIDR IPアドレス* (CIDR IP address to allow connection): A text input field.

At the bottom of the form, there are two buttons: 'Previous' (blue) and 'Next' (green). The footer of the page contains the copyright notice: 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

4. DB構築

入力項目

- データベースのレプリケーション有無
- データベースのインスタンスサイズ
- データベースの名前
- データベースのユーザー名
- データベースのユーザパスワード
- バックアップの保存期間

 Identity Platform

Identity Platformのセットアップ

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

Step 1 Step 2 Step 3 Step 4 Step 5 Step 6 Step 7 Step 8 Step 9 Step 10 Step 11 Step 12 Step 13 Step 14 Step 15

AWS情報設定 共通設定 読み台構築 DB構築 DB設定 環境構築 デプロイ設定 デプロイ実行 証明書設定 コンテンツ設定 コンテンツ配置 CDN構築 管理機能証明書設定 管理機能設定 セットアップ完了

DB構築

複数のアベイラビリティゾーンでのレプリケーション*

RDSのインスタンスクラス*

db.r3.large

データベースの名称*

データベースのユーザー*

ユーザーのパスワード*

バックアップの保存期間*

Previous

Next

Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.

5. DB設定

「Next」をクリックするだけ

The screenshot displays the 'Identity Platform' setup wizard. At the top, the title 'Identity Platform' is shown with a logo. Below it, the section 'Identity Platformのセットアップ' contains a progress bar with 15 steps. Step 5, 'DB設定', is highlighted in green. The steps are: Step 1 (AWS情報設定), Step 2 (共通設定), Step 3 (踏み台構築), Step 4 (DB構築), Step 5 (DB設定), Step 6 (環境構築), Step 7 (デプロイ設定), Step 8 (デプロイ実行), Step 9 (証明書設定), Step 10 (コンテンツ設定), Step 11 (コンテンツ配置), Step 12 (CDN構築), Step 13 (管理機能証明書設定), Step 14 (管理機能設定), and Step 15 (セットアップ完了). Below the progress bar, the title 'DB設定' is displayed. The main content area contains the instruction: 'データベースの初期設定を行います。「Next」ボタンを押下してください。' At the bottom, there are 'Previous' and 'Next' buttons. The footer of the wizard shows the copyright: 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

Step	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8	Step 9	Step 10	Step 11	Step 12	Step 13	Step 14	Step 15
Label	AWS情報設定	共通設定	踏み台構築	DB構築	DB設定	環境構築	デプロイ設定	デプロイ実行	証明書設定	コンテンツ設定	コンテンツ配置	CDN構築	管理機能証明書設定	管理機能設定	セットアップ完了

DB設定

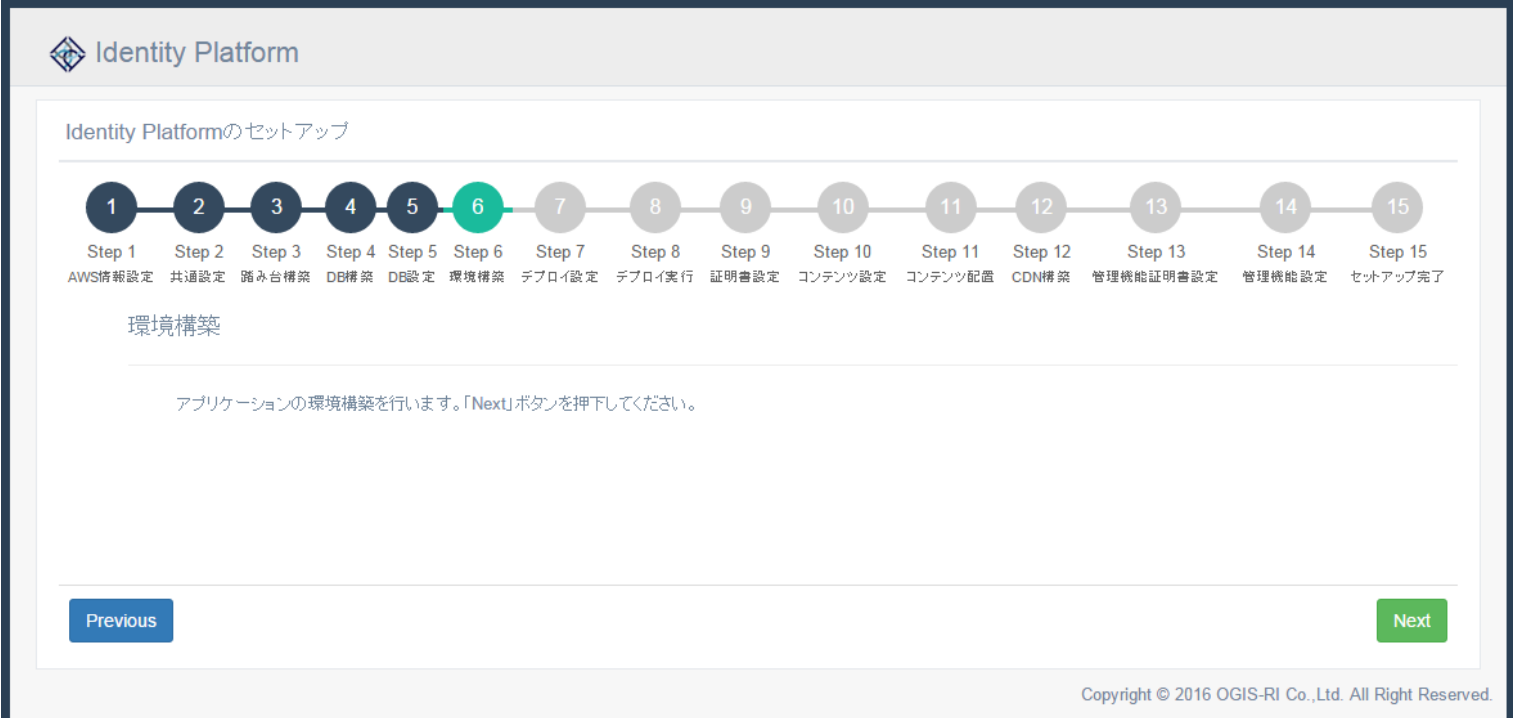
データベースの初期設定を行います。「Next」ボタンを押下してください。

Previous Next

Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.

6. 環境構築

「Next」をクリックするだけ



The screenshot shows the 'Identity Platform' setup wizard. At the top, it says 'Identity Platform'. Below that, 'Identity Platformのセットアップ' (Setup of Identity Platform) is displayed. A progress bar with 15 steps is shown, with Step 6 '環境構築' (Environment Setup) highlighted in green. The steps are: Step 1: AWS情報設定, Step 2: 共通設定, Step 3: 踏み台構築, Step 4: DB構築, Step 5: DB設定, Step 6: 環境構築, Step 7: デプロイ設定, Step 8: デプロイ実行, Step 9: 証明書設定, Step 10: コンテンツ設定, Step 11: コンテンツ配置, Step 12: CDN構築, Step 13: 管理機能証明書設定, Step 14: 管理機能設定, Step 15: セットアップ完了. Below the progress bar, the title '環境構築' is shown, followed by the instruction: 'アプリケーションの環境構築を行います。「Next」ボタンを押下してください。' (We will perform environment setup for the application. Please click the 'Next' button.) At the bottom, there are 'Previous' and 'Next' buttons. The 'Next' button is green and highlighted. The footer contains the copyright notice: 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

Step	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8	Step 9	Step 10	Step 11	Step 12	Step 13	Step 14	Step 15
Label	AWS情報設定	共通設定	踏み台構築	DB構築	DB設定	環境構築	デプロイ設定	デプロイ実行	証明書設定	コンテンツ設定	コンテンツ配置	CDN構築	管理機能証明書設定	管理機能設定	セットアップ完了

7. デプロイ設定

「Next」をクリックするだけ

The screenshot displays the 'Identity Platform' setup wizard. At the top, a progress bar shows 15 steps. Step 7, 'デプロイ設定' (Deploy Settings), is highlighted in green, indicating the current step. The steps are: Step 1 (AWS情報設定), Step 2 (共通設定), Step 3 (踏み台構築), Step 4 (DB構築), Step 5 (DB設定), Step 6 (環境構築), Step 7 (デプロイ設定), Step 8 (デプロイ実行), Step 9 (証明書設定), Step 10 (コンテンツ設定), Step 11 (コンテンツ配置), Step 12 (CDN構築), Step 13 (管理機能証明書設定), Step 14 (管理機能設定), and Step 15 (セットアップ完了).

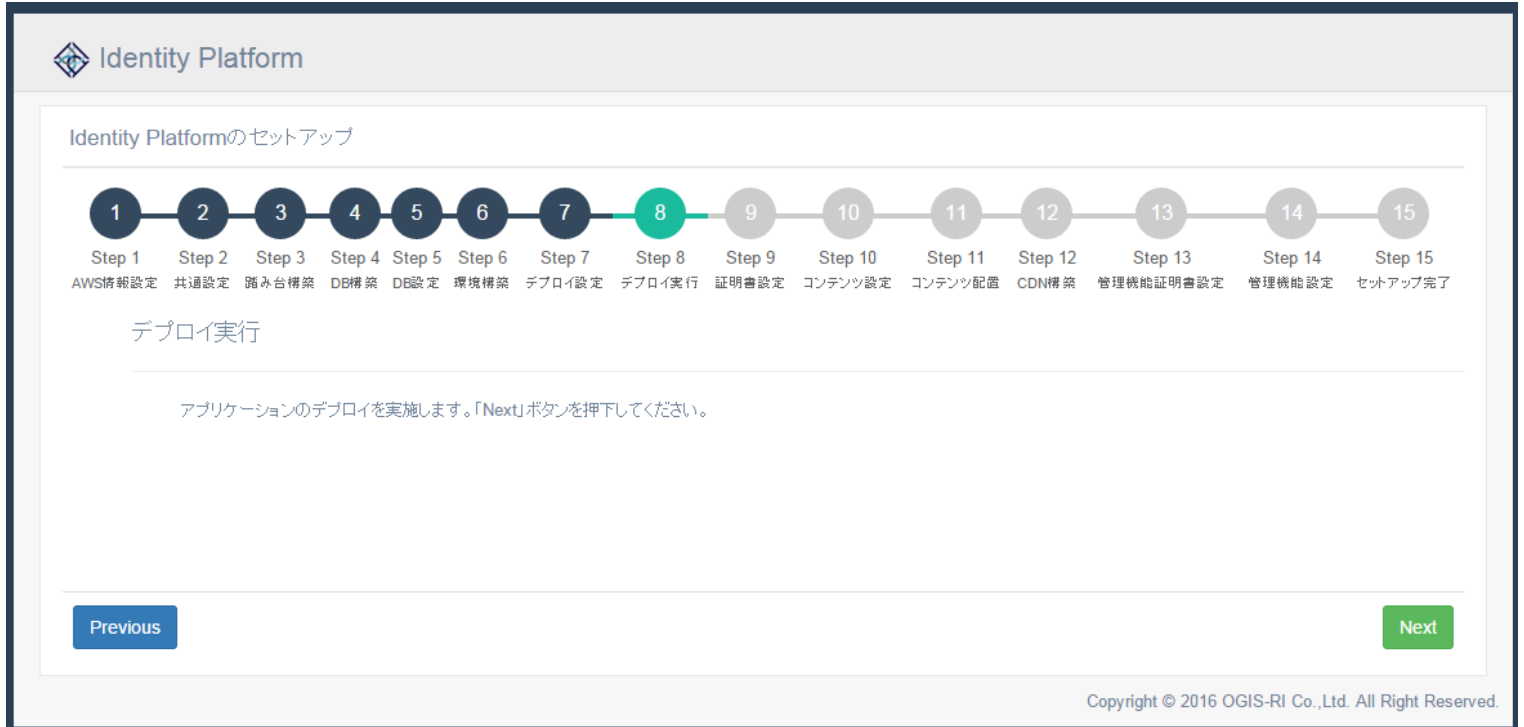
Below the progress bar, the title 'デプロイ設定' is displayed. The main content area contains the instruction: 'アプリケーションのデプロイ設定を実施します。「Next」ボタンを押下してください。' (Implement the application's deploy settings. Press the 'Next' button).

At the bottom, there are two buttons: 'Previous' (blue) and 'Next' (green). The 'Next' button is the primary action for this step.

Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.

8. デプロイ実行

「Next」をクリックするだけ



The screenshot shows the 'Identity Platform' setup progress bar. It consists of 15 steps, each represented by a numbered circle. Step 8 is highlighted in green, indicating the current step. The steps are as follows:

Step	Step Name
1	Step 1: AWS情報設定
2	Step 2: 共通設定
3	Step 3: 踏み台構築
4	Step 4: DB構築
5	Step 5: DB設定
6	Step 6: 環境構築
7	Step 7: デプロイ設定
8	Step 8: デプロイ実行
9	Step 9: 証明書設定
10	Step 10: コンテンツ設定
11	Step 11: コンテンツ配置
12	Step 12: CDN構築
13	Step 13: 管理機能証明書設定
14	Step 14: 管理機能設定
15	Step 15: セットアップ完了

Below the progress bar, the text 'デプロイ実行' (Deploy Execution) is displayed. Underneath, a message reads: 'アプリケーションのデプロイを実施します。「Next」ボタンを押下してください。' (We will deploy the application. Please click the 'Next' button.). At the bottom of the interface, there are two buttons: 'Previous' (disabled) and 'Next' (active/green). The footer of the page states: 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

9. Identity Platform用サーバ証明書設定

入力項目

- Identity Platform用の
サーバ証明書
秘密鍵
中間証明書

The screenshot shows the 'Identity Platform' setup wizard. At the top, a progress bar displays 15 steps. Step 9, '証明書設定' (Certificate Setting), is highlighted in green. Below the progress bar, the title '証明書設定' is shown. The main area contains three file selection fields, each with a 'select file' button and a folder icon:

- Identity Platformのサーバ証明書* (select file)
- Identity Platformの証明書の秘密鍵* (select file)
- Identity Platformの中間証明書* (select file)

At the bottom, there are 'Previous' and 'Next' buttons. The footer text reads: 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

10. コンテンツ設定

入力項目

- ログの格納先バケット名
- コンテンツ格納先バケット名

The screenshot shows the 'Identity Platform' setup wizard. At the top, a progress bar displays 15 steps. Step 10, 'コンテンツ設定' (Content Settings), is highlighted in green. Below the progress bar, the title 'Identity Platformのセットアップ' is followed by 'コンテンツ設定'. The main area contains two input fields: 'CloudFrontのログを格納するS3のバケット名*' and '各種コンテンツを格納するS3のバケット名*'. At the bottom, there are 'Previous' and 'Next' buttons. The footer text reads 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

Identity Platform

Identity Platformのセットアップ

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Step 1 Step 2 Step 3 Step 4 Step 5 Step 6 Step 7 Step 8 Step 9 Step 10 Step 11 Step 12 Step 13 Step 14 Step 15

AWS情報設定 共通設定 踏み台構築 DB構築 DB設定 環境構築 デプロイ設定 デプロイ実行 証明書設定 コンテンツ設定 コンテンツ配置 CDN構築 管理機能証明書設定 管理機能設定 セットアップ完了

コンテンツ設定

CloudFrontのログを格納するS3のバケット名*

各種コンテンツを格納するS3のバケット名*

Previous Next

Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.

1 1. コンテンツ配置

「Next」をクリックするだけ

The screenshot displays the 'Identity Platform' setup interface. At the top, the title 'Identity Platform' is shown. Below it, a progress bar indicates the current step is 'Step 11: コンテンツ配置' (Content Configuration), which is highlighted in green. The progress bar consists of 15 steps, each with a number and a label. Steps 1 through 10 are in dark blue, Step 11 is green, and Steps 12 through 15 are in light gray. The labels for the steps are: Step 1: AWS情報設定, Step 2: 共通設定, Step 3: 踏み台構築, Step 4: DB構築, Step 5: DB設定, Step 6: 環境構築, Step 7: デプロイ設定, Step 8: デプロイ実行, Step 9: 証明書設定, Step 10: コンテンツ設定, Step 11: コンテンツ配置, Step 12: CDN構築, Step 13: 管理機能証明書設定, Step 14: 管理機能設定, Step 15: セットアップ完了.

Below the progress bar, the section 'コンテンツ配置' (Content Configuration) is displayed. It contains the instruction: 'コンテンツのアップロードを実施します。「Next」ボタンを押下してください。' (We will perform content upload. Please click the 'Next' button.)

At the bottom of the interface, there are two buttons: 'Previous' (blue) and 'Next' (green). The 'Next' button is highlighted, indicating it is the next step to click.

Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.

12. CDN構築

「Next」をクリックするだけ

The screenshot shows the 'Identity Platform' setup wizard. At the top, it says 'Identity Platformのセットアップ'. Below this is a progress bar with 15 steps. Step 12, 'CDN構築', is highlighted in green. The steps are: Step 1 (AWS情報設定), Step 2 (共通設定), Step 3 (踏み台構築), Step 4 (DB構築), Step 5 (DB設定), Step 6 (環境構築), Step 7 (デプロイ設定), Step 8 (デプロイ実行), Step 9 (証明書設定), Step 10 (コンテンツ設定), Step 11 (コンテンツ配置), Step 12 (CDN構築), Step 13 (管理機能証明書設定), Step 14 (管理機能設定), and Step 15 (セットアップ完了). Below the progress bar, the title 'CDN構築' is displayed. The main content area contains the text: 'コンテンツデリバリーネットワークの構築を行います。「Next」ボタンを押下してください。' At the bottom, there are 'Previous' and 'Next' buttons. The footer of the wizard says 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

13. 管理機能証明書設定

入力項目

- マネジメントコンソール用の
サーバ証明書
秘密鍵
中間証明書

Identity Platform

Identity Platformのセットアップ

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Step 1 Step 2 Step 3 Step 4 Step 5 Step 6 Step 7 Step 8 Step 9 Step 10 Step 11 Step 12 Step 13 Step 14 Step 15

AWS情報設定 共通設定 読み台構築 DB構築 DB設定 環境構築 デプロイ設定 デプロイ実行 証明書設定 コンテンツ設定 コンテンツ配置 CDN構築 管理機能証明書設定 管理機能設定 セットアップ完了

管理機能証明書設定

Management Consoleのサーバ証明書

Management Consoleの証明書の秘密鍵

Management Consoleの中間証明書

Previous Next

Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.

14. 管理機能設定

「Next」をクリックするだけ

The screenshot displays the 'Identity Platform' setup wizard. At the top, it says 'Identity Platform' with a logo. Below that, 'Identity Platformのセットアップ' (Setup of Identity Platform) is written. A progress bar shows 15 steps. Step 14, '管理機能設定' (Management Function Setting), is highlighted in green. The steps are: Step 1: AWS情報設定, Step 2: 共通設定, Step 3: 踏み台構築, Step 4: DB構築, Step 5: DB設定, Step 6: 環境構築, Step 7: デプロイ設定, Step 8: デプロイ実行, Step 9: 証明書設定, Step 10: コンテンツ設定, Step 11: コンテンツ配置, Step 12: CDN構築, Step 13: 管理機能証明書設定, Step 14: 管理機能設定, Step 15: セットアップ完了. Below the progress bar, the title '管理機能設定' is shown. The main content area contains the instruction: '管理コンソールの設定を行います。「Next」ボタンを押下してください。' (Configure the management console. Press the 'Next' button). At the bottom, there are 'Previous' and 'Next' buttons. The footer contains the copyright notice: 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

15. 管理コンソールの再起動

「再起動」をクリックするだけ



Identity Platform

Identity Platformのセットアップ

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Step 1 Step 2 Step 3 Step 4 Step 5 Step 6 Step 7 Step 8 Step 9 Step 10 Step 11 Step 12 Step 13 Step 14 Step 15

AWS情報設定 共通設定 読み台構築 DB構築 DB設定 環境構築 デプロイ設定 デプロイ実行 証明書設定 コンテンツ設定 コンテンツ配置 CDN構築 管理機能証明書設定 管理機能設定 セットアップ完了

セットアップ完了

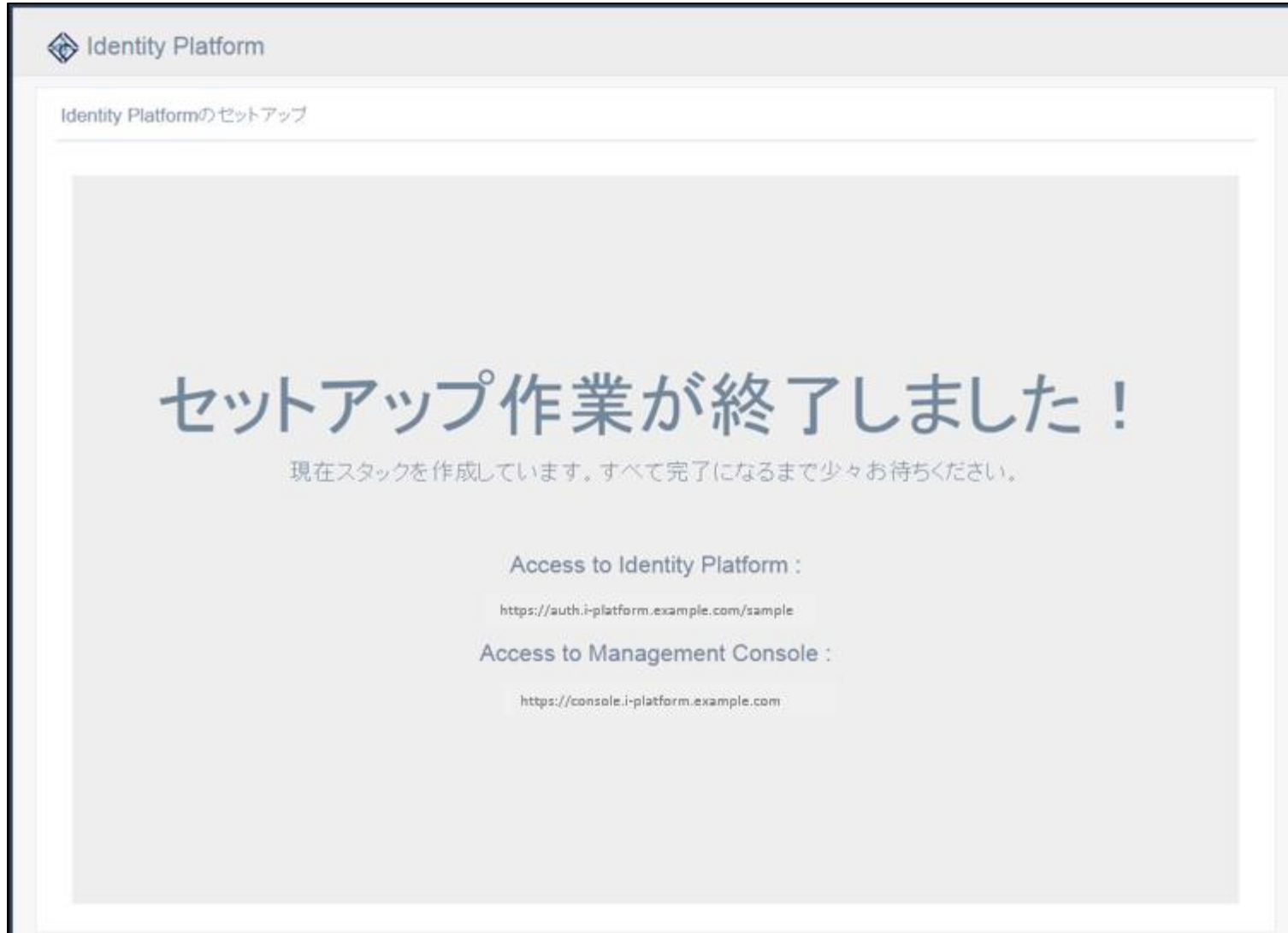
管理コンソールを再起動します。

再起動

Previous

Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.

セットアップ完了

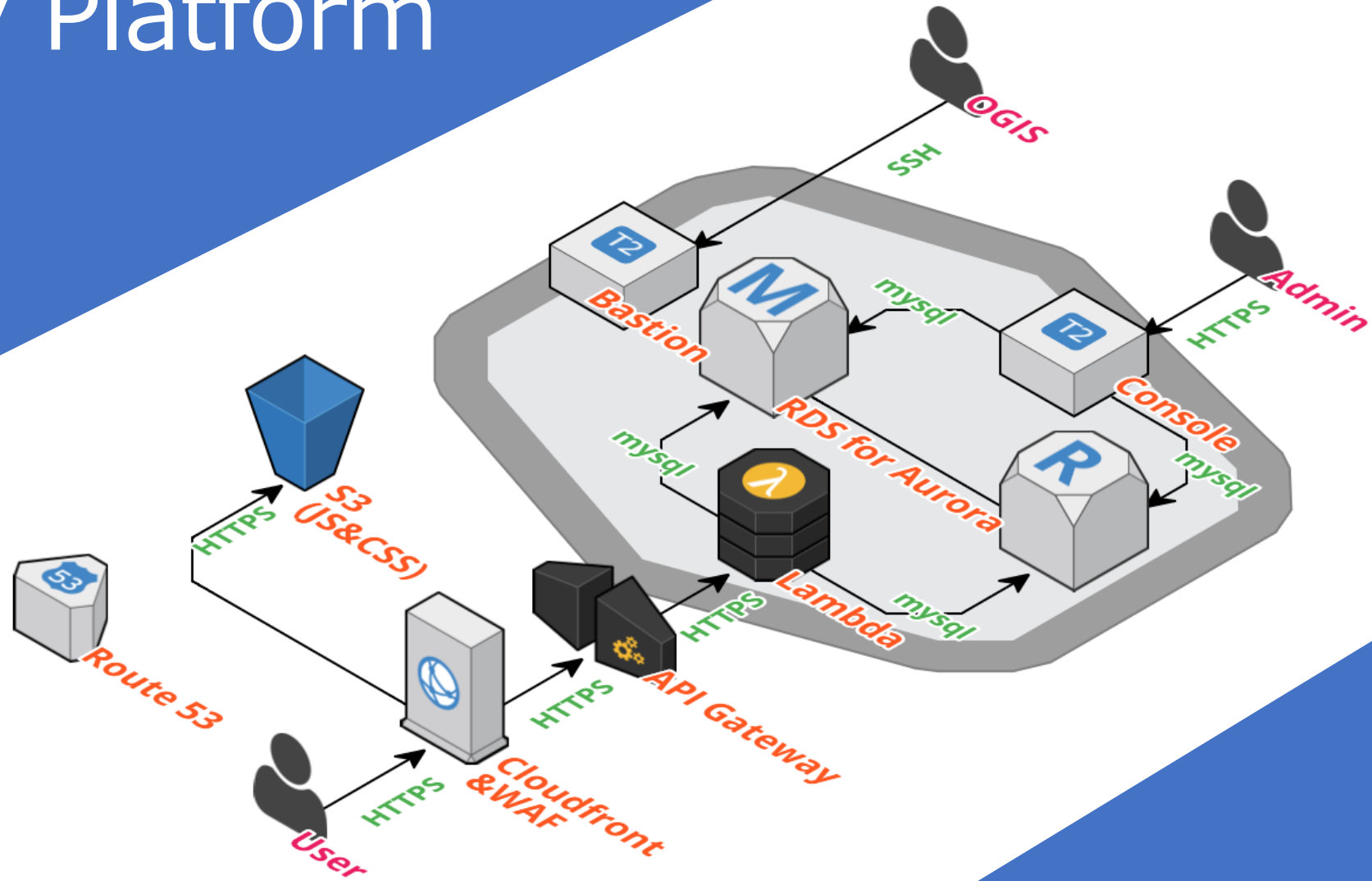


まず認証基盤できた！



デモストラクト
ThemiStruct
Identity Platform AWS
対応版

ThemiStruct Identity Platform





ID

パスワード

送信

Identity Platform Admin Page

 you can configure some of parameters.

Administrator Management Console Page

Page Description

Index

This page.

User Setting

User CRUD.

Authentication Setting

Authentication configuration CRUD.

OpenID Connect Setting

OpenID Connect configuration CRUD.

THANK YOU FOR YOUR BUSINESS

 <http://www.ogis-ri.co.jp/>

第 3 章

盛り付け ～アプリケーション接続～

本日盛り付けるアプリケーション

オンプレミスのデータセンターに配置されたアプリケーション

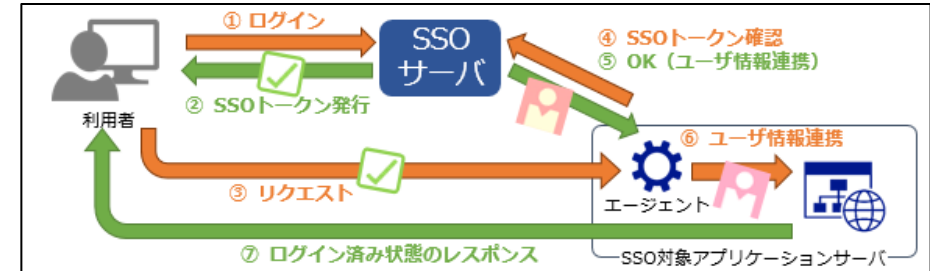


クラウドサービス

Office 365

盛り付け方は3パターンをご用意

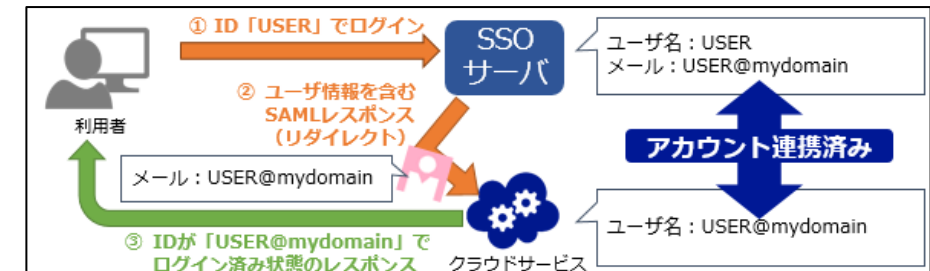
□ エージェントによる接続



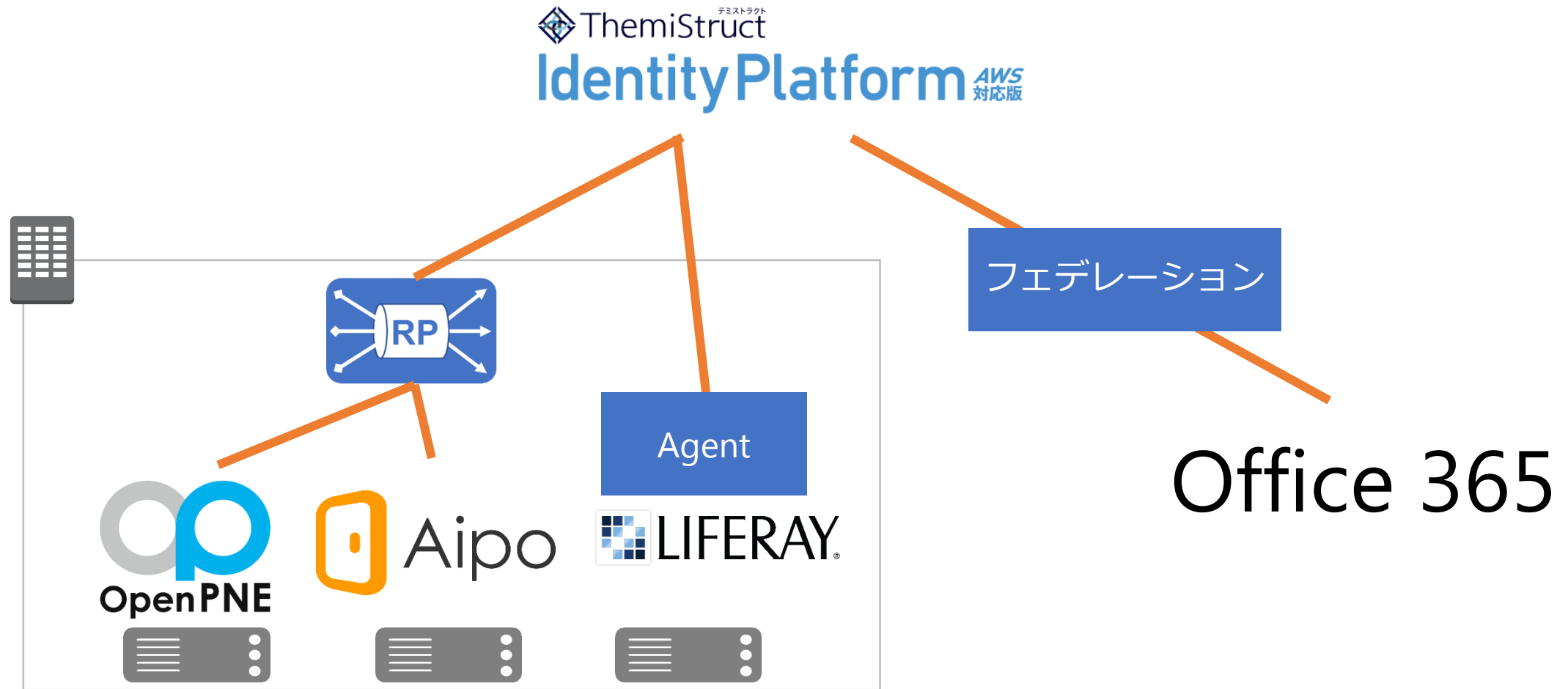
□ リバースプロキシによる接続



□ フェデレーションによる接続



盛り付け例



参考 | リバースプロキシでの接続①

リバースプロキシでアプリケーションに接続する場合

1. ThemisStruct Identity Platformへのアプリ登録

Client Registration

1 Client
Step 1 : Client Info

2 Response
Step 2 : Response Info

Client Info

Application Name*

Description

Client Registration

1 Client
Step 1 : Client Info

2 Response
Step 2 : Response Info

Response Info

Redirect URI*

Application URI*

参考 | リバースプロキシでの接続②

リバースプロキシでアプリケーションに接続する場合

2. フェデレーションプロキシ構築キットでアプリ接続

1. フェデレーションプロキシのインストールを実行

```
# /opt/federationproxy/install.sh
```

2. addappコマンドを実行

```
# /opt/federationproxy/addapp.sh ¥  
-p openpne ¥  
-v https://openpne.example.com:443 ¥  
-d https://dest.example.com:443 ¥  
-o https://op.example.com:443/prod ¥  
-c /etc/pki/tls/certs/openpne.crt ¥  
-k /etc/pki/tls/private/openpne.key ¥  
-I openpne.jNuaTZ3B ¥  
-s sX79zi3Y
```

参考 | Office 365 の接続①

Office 365 と接続する場合は、ThemiStruct Identity Platform側は管理画面で以下の設定し、

The screenshot displays the ThemiStruct Identity Platform management interface. On the left is a navigation menu with the following items: Identity Platform, Administrator, Home, User, Authentication, Federation, Application, and Global Config. The main content area is titled 'Application' and shows a list of applications including 'SaaS' and 'Office 365 SAML SP'. Two panels are overlaid on the main content to show the configuration steps:

- Left Panel (ID Configuration):** Shows a progress bar with three steps: 1 (ID, highlighted in green), 2 (SP Information), and 3. Below the progress bar, the 'ID' field is visible with the value 'o365' entered.
- Right Panel (Key and Certificate Configuration):** Shows a progress bar with three steps: 1 (ID), 2 (SP Information, highlighted in green), and 3 (Application Setting). Below the progress bar, the 'Key and Certificate' section is visible with the following fields and values:
 - Audience: urn:federation:MicrosoftOnline
 - Destination: https://login.microsoftonline.com/login.srf
 - Name ID Format: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
 - ACR: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtected
 - Attribute: {"IDPEmail": "email"}

参考 | Office 365 の接続②

完了画面に表示されるとおりに、PowerShellを実行することで Office 365 との接続は完了します。

1

ID

Step 1 : ID

2

SP Information

Step 2 : SP Information

3

Application Setting

Step 3 : Application Configuration

Office 365の連携設定を続けて下さい

Windowsクライアントに以下の4つのプログラムをインストールしてください

- Microsoft Online Services Sign-In Assistant for IT Professionals
- Azure Active Directory Module for Windows PowerShell
- SharePoint Online Management Shell
- Windows PowerShell Module for Skype for Business Online

PowerShellコマンドプロンプト上で、以下のコマンドを実行してください。Office 365の管理者アカウントのIDとパスワードを入力してください。

```
$msolcred = get-credential
connect-msolservice -credential $msolcred
```

続いて、以下のコマンドを実行し、Office 365との連携設定を行います。

```
$dom = "demo.example.com" //Office 365に登録しているドメイン名
$entity = "https://themistruct.example.com:443/prod/saml"
$uri = "https://themistruct.example.com:443/prod/saml"
$logonuri = "https://themistruct.example.com:443/v1/saml"
$logoffuri = "https://themistruct.example.com:443/v1/saml"
$secp = "https://themistruct.example.com:443/v1/saml"
$cert = "MII ... (省略) ... Q=" //Identity Platform
```

以下のコマンドを実行し、Office 365との連携設定を有効化します。

```
Set-MsolDomainAuthentication -DomainName $dom -FederationBrandName $dom -Authentication Federated
-PassiveLogOnUri $uri -SigningCertificate $cert -IssuerUri $entity -ActiveLogOnUri $secp -LogOffUri $logoffuri -PreferredAuthenticationProtocol SAML
```

各種Officeクライアントアプリケーションを使用する場合、以下のコマンドを実行し、連携設定を有効化します。

```
$sessionEO = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $msolcred -Authentication Basic -AllowRedirection
Import-PSSession $sessionEO
Set-OrganizationConfig -OAuth2ClientProfileEnabled:$true
$sessionS4B = New-CsOnlineSession -Credential $credential
Import-PSSession $sessionS4B
Set-CsOauthConfiguration -ClientAdalAuthOverride Allowed
```

最後に以下のコマンドを実行し、サンプルユーザーを作成します。事前にIdentity Platform上に「UserID」が「testuser」、メールアドレスが「testuser@demo.example.com」のプロフィール情報を持ったユーザーアカウントが作成されているとします。

```
$mail = "testuser@demo.example.com"
$uid = "testuser"
New-MsolUser -UserPrincipalName $mail -DisplayName $uid -ImmutableId $uid
Set-MsolUser -UserPrincipalName $mail -UsageLocation JP
Set-MsolUserLicense -UserPrincipalName $mail -AddLicenses tsipstest:0365_BUSINESS_PREMIUM
```

以上で、Office 365との連携設定が完了となります。

Previous

Finish

Cancel

できた！

Office 365

 デミストラクト ThemiStruct
Identity Platform AWS 対応版


OpenPNE

 Aipo

 LIFERAY®

第 4 章

認証基盤の味見

味見

味見 1

アプリケーションのSSO

味見 2

Office 365 利用

味見 1

アプリケーションのSSO

味見 2

Office 365 利用

お召し上がりください



ThemiStruct Identity Platformご紹介



- ✓ AWSネイティブな
アイデンティティ連携基盤
- ✓ ≠OpenAM
- ✓ ≠OpenIDM
- ✓ オージス総研自社商品



これからの認証プラットフォームに求められること

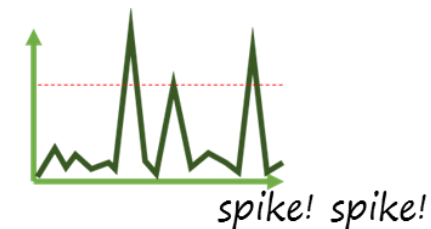
膨大なトラフィック量への対応

- 認証基盤の役割増加
- 事業者が提供するサービスの増加
- ユーザ数・デバイス数の増加
- API利用の増加



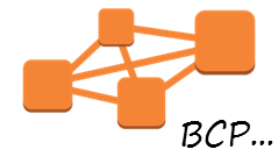
スパイクアクセスへの対応

- キャンペーンやニュースサイト掲載などにより定常的なアクセスと比較し、予想不可な大量のアクセスが発生する



システム停止回避への対応

- 認証基盤役割の増加に伴い、システム停止や遅延による機会損失が大きくなり、事業継続性や機会損失回避など可用性要求のレベルが格段にUPした



スピードスタート・スモールスタートへの対応

- 短期間でビジネスをスタートさせたり、事業規模に応じてスタート、柔軟にスケールできる必要がある



very tight.

仮想サーバーを極力使用しないアーキテクチャで実装



Amazon
API
Gateway



AWS
Lambda



Amazon
RDS
for Aurora

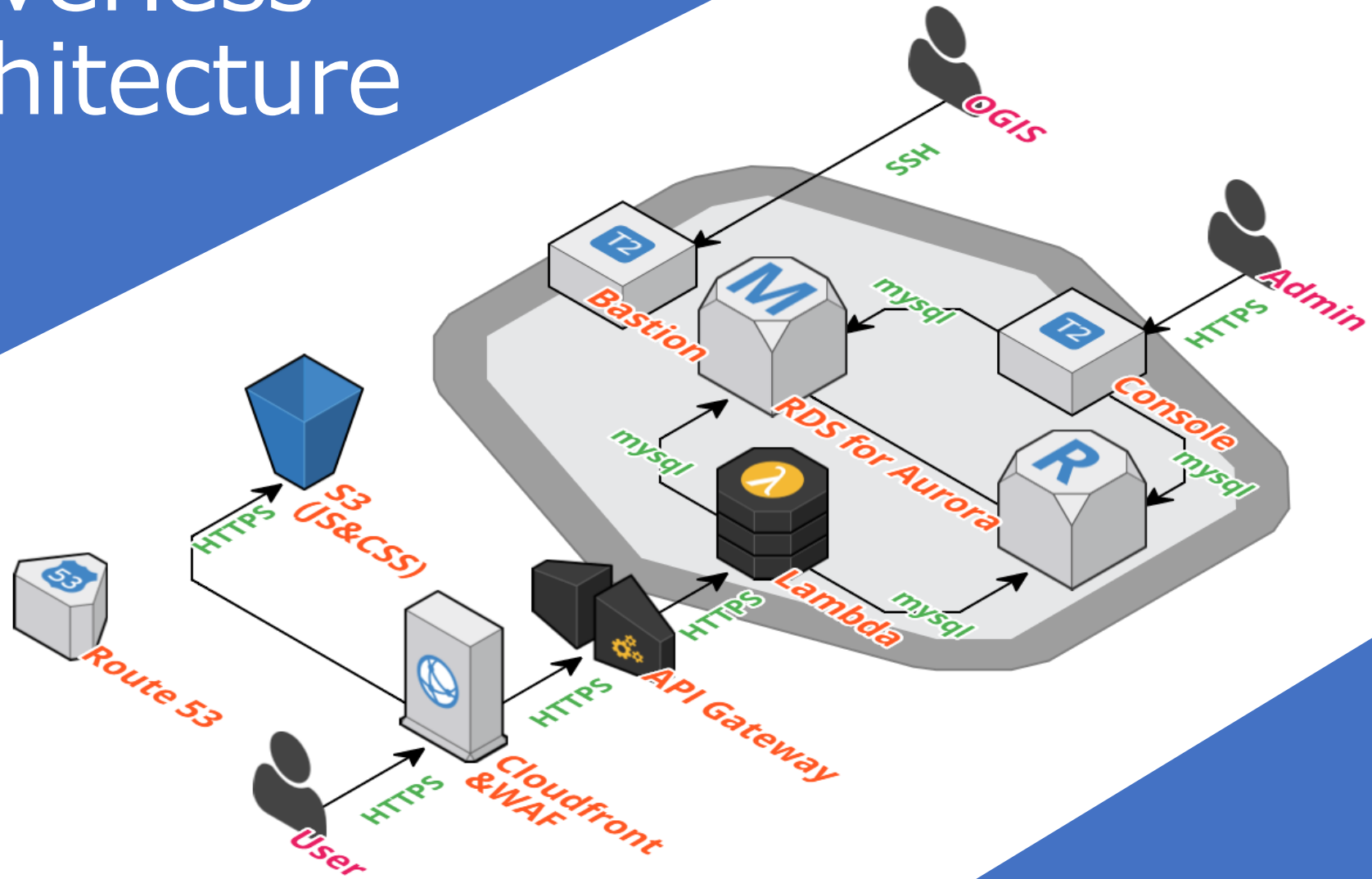
AWSネイティブなアーキテクチャにより下記の恩恵を享受

リクエストに応じた伸縮が可能

一定の可用性確保と自動復旧の実現

プロジェクトの短期間化

Serverless Architecture

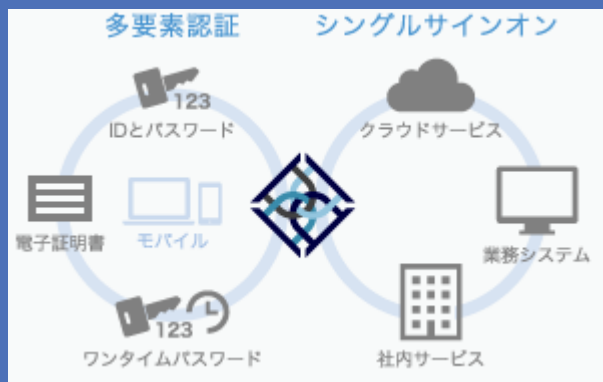


ThemiStruct Identity Platformの特徴



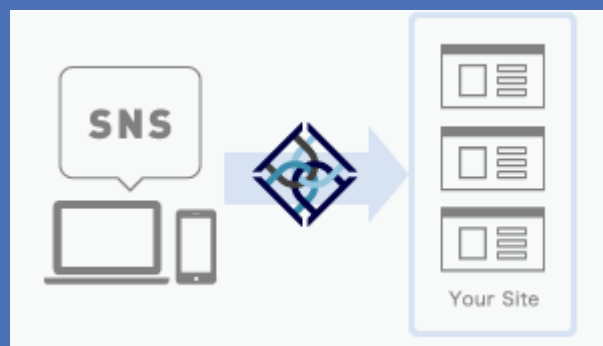
認証システムの短期導入が可能

ThemiStruct Identity Platformはクラウド上に設置され、短期間で従業員、カスタマー、ビジネスパートナーに認証サービスを提供できます。また、APIを利用し既設サイトへの組み込みも容易です。



ログインを1回に、認証方法も組合せ自由

ThemiStruct Identity Platformに一度ログインを行うことで、ユーザが利用したい各サイトへシングルサインオンすることができます。その際のログインではIDとパスワードによる認証だけでなく、ワンタイムパスワード・電子証明書、指紋・指静脈情報やインベントリー認証などを利用することができます。また利用システムごとの設定により、各サイトやコンテンツのセキュリティ、ユーザビリティ要件に応じた認証を行うことができます。



ユーザ登録のハードルを下げ、新規ユーザ登録率をアップ

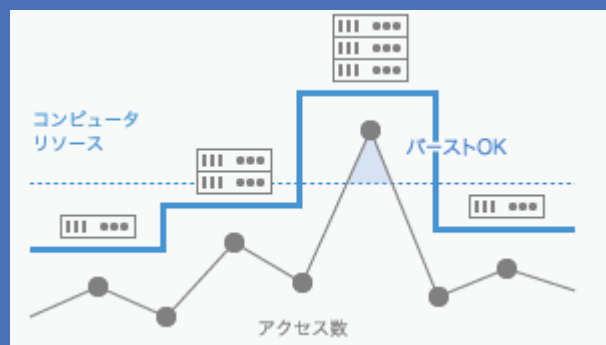
FacebookやGoogleなどのユーザが普段使っているSNSやWebサービスのアカウントを利用して、気軽にユーザ登録が可能です。サイトへの新規ユーザ登録率、ユーザビリティ、コンバージョン率を向上させます。ユーザ自身による登録や、管理者による一括登録も可能です。

ThemiStruct Identity Platformの特徴



各システムへ必要なときに、必要な情報を連携できます

ThemiStruct Identity Platformから各システムへ必要なタイミングで、必要なユーザ情報を連携することができます。各システムでユーザ情報の管理が不要になります。



事業成長に合わせたスケーリング、突発的アクセス集中への対応

サーバレスアーキテクチャにより、事業環境の変化や突発的アクセス集中に合わせて、自由にかつ自動でコンピュータリソースの拡張・縮小を行えます。

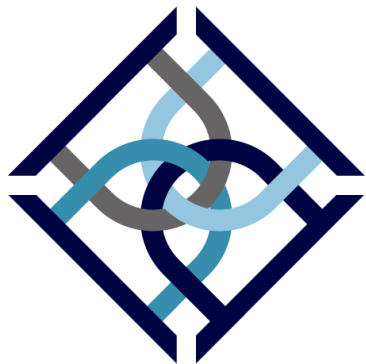
本日のまとめ

1. 「ThemiStruct Identity Platform」なら
認証プラットフォームはすぐ建てられる
2. 「ThemiStruct Identity Platform」なら
アプリケーションもすぐにつながる

**AWS上にパッと作ってサッと使える統合認証プラットフォーム
「ThemiStruct（テミストラクト）Identity Platform」**

ご清聴ありがとうございました

ASK US



ThemiStruct
テミストラクト

【お問い合わせ先】

株式会社オージス総研

TEL: 03-6712-1201 / 06-6871-7998

mail: info@ogis-ri.co.jp



本資料に掲載されている会社名、製品名は各社の登録商標または商標です。