

Amazon WorkSpaces Web ワークショップ

2022/08/16

シニアエバンジェリスト 亀田

はじめに：Amazon WorkSpaces は AWS が提供する VDI のサービスです。Windows や Linux のデスクトップ環境がサービスとして提供されます。利用には専用クライアントが必要ですが、ブラウザでアクセス可能な Amazon WorkSpaces Web Client も存在しています。

本ワークショップで作業を行う Amazon WorkSpaces Web は、それとは別のサービスです。指定した VPC の特定プライベートサブネットの中で Chrome ブラウザを起動させることでよりセキュアなリモートワーク環境が構築可能となるものです。Amazon WorkSpaces 及び Amazon WorkSpaces Web Client はフルのデスクトップ環境が提供されるのに対して、Amazon WorkSpaces Web はブラウザのみが機能として提供されます。

また、Amazon WorkSpaces は Directory が必須ですが Amazon WorkSpaces Web は、SAML の Idp が必須となり、Directory は不要です。このワークショップでは AWS IAM Identity Center (旧 S S O) を用いますが、任意の SAML Idp との連携が可能です。

Amazon WorkSpaces Web と近い動きをするものに、Amazon AppStream2.0 があります。前者は VPC Private Subnet で動作する Chrome が提供されますが後者は任意のアプリケーション実行時の画面がリモート環境に転送される、という違いがあります。

1. VPC のマネージメントコンソールに移動します
2. [VPC を作成]をおします
3. [名前タグの自動生成]に workspacesweb と入力します

名前タグの自動生成 **情報**

Name タグの値を入力します。この値は、VPC 内のすべてのリソースの Name タグを自動生成するのに使用されます。

☒ 自動生成

workspcaesweb

4. AZ の数を 1 個に指定します。商用環境では可用性を考慮し 2 以上を指定することを

お勧めします

アベイラビリティゾーン (AZ) の数 [情報](#)

サブネットをプロビジョニングする AZ の数を選択します。可用性を高めるには、少なくとも 2 つの AZ をお勧めします。

1	2	3
---	---	---

5. NAT ゲートウェイを 1 に指定します

NAT ゲートウェイ (\$) [情報](#)

NAT ゲートウェイを作成するアベイラビリティゾーン (AZ) の数を選択します。NAT ゲートウェイごとに料金が発生することに注意してください。

なし	1 AZ 内	AZ ごとに 1
----	--------	----------

6. [VPC を作成]をおします
7. 全て作成が完了したら左ペインで[サブネット]をおします。Public, Private それぞれサブネットが 1 個できているはずです。もう一つ Private サブネットを追加するため [サブネットの作成]をおします
8. 先程作成された VPC を選びます

VPC

VPC ID
この VPC にサブネットを作成します。

vpc-0aa912b97fe209ca6 (workspcaesweb-vpc) ▼

関連付けられた VPC CIDR

IPv4 CIDR
10.0.0.0/16

9. [サブネット名]に[workspaces-private2]と入力します
10. アベイラビリティゾーンで先程作成された Private Subnet と異なるゾーンを指定します
11. [IPv4 CIDR ブロック]に 10.0.120.0/20 と入力します

サブネット 1 (1 個中)

サブネット名

「Name」というキーと、指定した値を使用してタグを作成します。

workspaces-private2

名前の長さは最大 256 文字です。

アベイラビリティゾーン [情報](#)

サブネットが存在するゾーンを選択するか、Amazon が選択するゾーンを受け入れます。

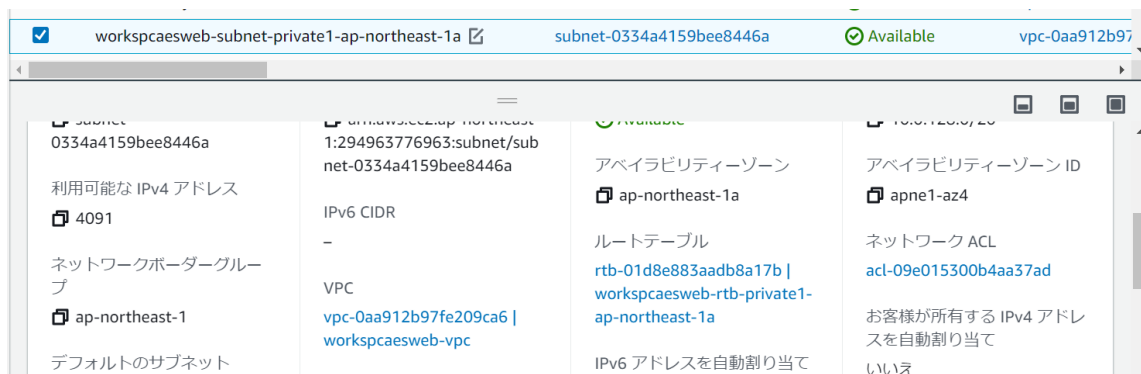
アジアパシフィック (東京) / ap-northeast-1c

IPv4 CIDR ブロック [情報](#)

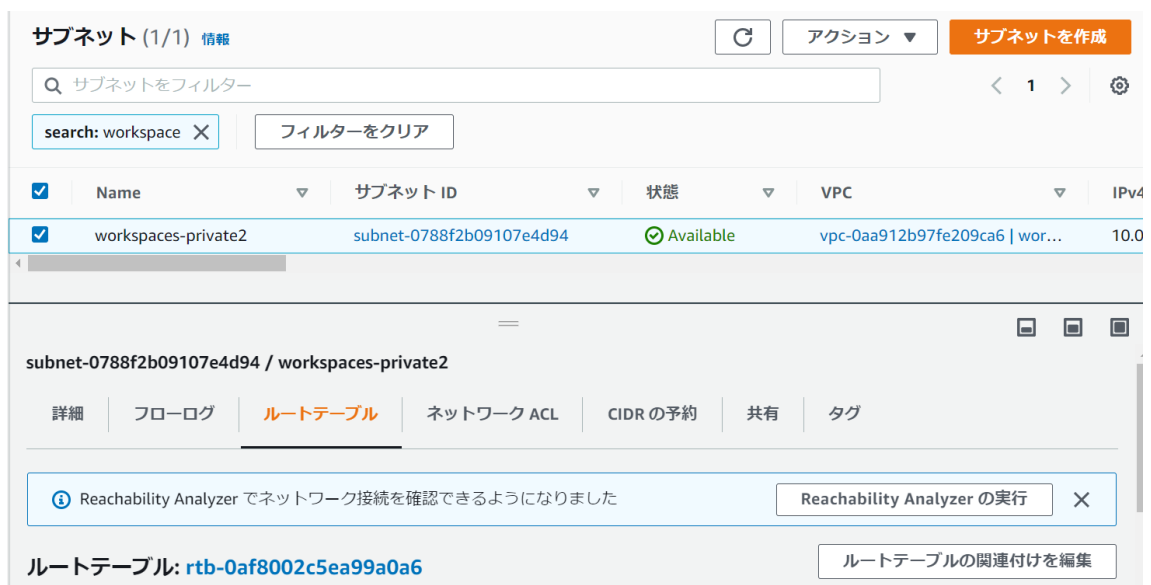
10.0.0.10/20

▼ タグ - オプション

- 作成が完了したら、もともとあった方の Private Subnet の詳細画面からルートテーブルの名前を特定しコピーしておきます




- 新しく作成したサブネットの詳細画面で[ルートテーブル]をタブをクリックし、[ルートテーブルの関連付けを編集]をおします



- 先程コピーしたルートテーブルに置き換え、[保存]をおします

サブネットルートテーブル設定

サブネット ID
 subnet-0788f2b09107e4d94

ルートテーブル ID
 rtb-01d8e883aadb8a17b (workspcaesweb-rtb-private1-ap-northeast-1a) ▼ 

15. 左ペインからエンドポイントをクリックします。VPC Wizard で作成された S3 エンドポイントが表示されているはずです。表示されていない場合は何度か画面をリロードしてみてください
16. [エンドポイントを作成]をおします
17. [名前]に kms と設定し、以下を選択します

サービス (1/1)

🔍 サービスのフィルター


サービス名: com.amazonaws.ap-northeast-1.kms ✕ フィルターをクリア

サービス名	所有者	タイプ
com.amazonaws.ap-northeast-1.kms	amazon	Interface

18. 先程作成した VPC とサブネットを選びます


VPC

エンドポイントを作成する VPC を選択

VPC
 エンドポイントを作成する VPC。
 vpc-0aa912b97fe209ca6 (workspcaesweb-vpc) ▼ 

▶ 追加設定

サブネット (2/3) 情報

<input checked="" type="checkbox"/>	アベイラビリティーゾーン	サブネット ID
<input checked="" type="checkbox"/>	ap-northeast-1a (apne1-az4)	subnet-0334a4159bee8446a ▼
<input checked="" type="checkbox"/>	ap-northeast-1c (apne1-az1)	subnet-0788f2b09107e4d94 ▼
<input type="checkbox"/>	ap-northeast-1d (apne1-az2)	 使用可能なサブネットがありません

19. IPv4 を選びます

IP アドレスタイプ

☒ IPv4

☐ IPv6

☐ デュアルスタック

20. [エンドポイントを作成]をおします
21. 同様に logs という名前で以下を作成します

サービス (1/1) 🔄

🔍 サービスのフィルター

サービス名: `com.amazonaws.ap-northeast-1.logs` ✕ フィルターをクリア

サービス名	所有者	タイプ
<input checked="" type="radio"/> <code>com.amazonaws.ap-northeast-1.logs</code>	amazon	Interface

以上で、WorkSpaces Web を起動するネットワーク設定が完了です。

ここからの設定はブラウザのタブを 2 個開いて作業を行います。1 個は IAM Identity Center (旧 SSO)、もう 1 個は WorkSpacesWeb です。SAML 連携のためにお互いの信頼関係を設定する必要があるため同時に行います。

22. IAM Identity Center のマネージメントコンソールで[有効化]をおします
23. 左ペインでユーザーをクリックし、[ユーザーを追加]をおします
24. [ユーザー名]にご自身のユーザーID を入力します
25. [E メールアドレス]にご自身のメールアドレスを入力します。(AWS アカウントと同じアドレスでも問題ないです)
26. [名][姓]に適当な値を入れて[次へ]をおします
27. 次のグループ画面は何も設定せず[次へ]をおします
28. [ユーザーを追加]をおします
29. 登録したメールアドレスにメールが届きますので[Accept invitation]をおします
30. 表示されたブラウザのページでパスワードを設定します
31. パスワードが設定完了するとログイン画面になりますので、試しにログインをしてみます。以下が表示されれば成功です。

You do not have any applications.

32. IAM Identity Center の画面に戻り、左ペインから[アプリケーション]をクリックします
33. [アプリケーションを追加]をおします
34. [カスタム SAML 2.0 アプリケーションの追加]にチェックをつけます

カスタムアプリケーション

- カスタム SAML 2.0 アプリケーションの追加
カスタム SAML 2.0 対応アプリケーションに IAM ID センター統合を追加できます。

35. [次]をおします
 36. [IAM Identity Center SAML メタデータファイル]をダウンロードし、保存しておきます
- 今作業しているブラウザのタブは閉じずにこのままにしておき、別タブで以下作業を行います。
37. Amazon Workspaces のマネージメントコンソールに移動します
 38. [ウェブポータル]をクリックします
 39. [ウェブポータルの作成]をおします
 40. 以下の通りネット一枠を設定します。サブネットはプライベートサブネットを2つ指定します。セキュリティグループはデフォルトをしいします。

VPC | 情報
インターネットとユーザーがアクセスできる内部コンテンツの両方に対する接続を持つ VPC を選択します。

vpc-0aa912b97fe209ca6 (10.0.0.0/16) ▼ 

サブネット | 情報
WorkSpaces Web を使用してインターネットへのルートを持つプライベートサブネットを少なくとも 2 つ選択します。

別のサブネットを追加 ▼

subnet-0788f2b09107e4d94 (10.0.112.0/20) ✕
ap-northeast-1c, workspaces-private2

subnet-00116e9f80e3325d1 (10.0.0.0/20) ✕
ap-northeast-1a, workspacesweb-subnet-public1-ap-northeast-1a

セキュリティグループ | 情報
WorkSpaces Web が VPC 内にネットワークリンクを作成することを許可するセキュリティグループを選択します。

別のセキュリティグループを追加 ▼

sg-0d3d5fd5d38e78b48 (default) ✕
default VPC security group

41. [次へ]を 3 回おします
42. メタデータファイルをダウンロードします

SP メタデータドキュメント

SP メタデータドキュメントをダウンロードし、IdP にアップロードします。

メタデータファイルをダウンロード

43. 先程 Identity Center からダウンロードしたファイルを以下からアップロードします

IdP メタデータドキュメント | 情報
SAML 2.0 互換 IdP から XML 形式のメタデータファイルをアップロードします。

 **ファイルを選択**

44. [次へ]をおします
45. [ウェブポータルを起動]をおします
待ち時間の間にブラウザ別タブで設定中の Identity Center の画面に戻ります
46. [アプリケーションメタデータ]の個所から先程 Workspaces Web からダウンロードしたファイルをアップロードし、[送信]をおします

アプリケーションメタデータ

IAM Identity Center では、このアプリケーションを信頼する前に、クラウドアプリケーションに関する特定のメタデータが必要です。このメタデータは手動で入力するか、メタデータ交換ファイルをアップロードすることができます。

☐ メタデータ値をマニュアルで入力する
 ☒ アプリケーション SAML メタデータファイル

☒ ServiceProviderMetadata_ac175447-d32a-43f4-9674-9583433dd8cf.xml
 ファイルサイズ (バイト): 2222
 最終変更日: Aug 16, 2022

47. [アクション]から[属性マッピングを編集]を選びます

アクション ▲

設定を編集

属性マッピングを編集

48. [この文字列値または IAM Identity Center のユーザー属性にマッピング]に
 [`\${user:email}`]と入力します。（[] は含めない）。形式には[emailAddress]を指定します

アプリケーションのユーザー属性	この文字列値または IAM Identity Center のユーザー属性にマッピング	形式
Subject	<input style="width: 150px;" type="text" value="\${user: email}"/>	<input style="width: 100px;" type="text" value="emailAddress"/>

49. [変更の保存]をおします

50. [ユーザーを割り当て]をおします

51. 先程作成したユーザーを選んで[ユーザーを割り当て]をおします

以上で設定が完了です。

WorkSpaces のマネージメントコンソールに戻り、ポータルの起動が完了していれば以下のように URL が表示されます。

ウェブポータルエンドポイント 情報

ユーザーはこの URL にアクセスして、ウェブポータルを起動します。

以下のエンドポイントは、ユーザーがウェブポータルを起動する場所で、ネットワークに埋め込むことができます。



ウェブポータルエンドポイント

ac175447-d32a-43f4-9674-9583433dd8cf.workspaces-web.com

その URL にアクセスします。ログインを行い Chrome が表示されれば完了です。（先ほどテスト用にログインした状態のブラウザであれば、ログインなしでしばらく待つとブラウザが表示されます。）

見づらいですが画面右上の[en▼]をクリックすると、入力を日本語に変更できます。

お疲れ様でした！：

削除は以下を行ってください。

- NAT Gateway
- S3、KMS、CloudWatch Logs エンドポイント
- VPC
- Identity Center ユーザー
- Identity Center
- WorkSpaces Web ポータル