Amazon WorkSpaces Web ワークショップ

2022/08/16

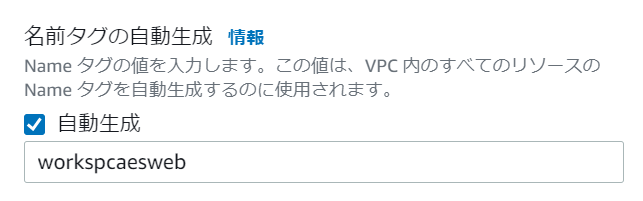
シニアエバンジェリスト 亀田

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。

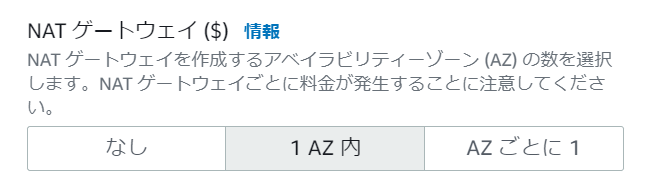
また、Amazon WorkSpacesはDirectoryが必須ですがAmazon WorkSpaces Webは、SAMLのIdpが必須となり、Directoryは不要です。このワークショップではAWS IAM Identity Center (旧ＳＳＯ)を用いますが、任意のSAML Idpとの連携が可能です。

Amazon WorkSpaces Webと近し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。

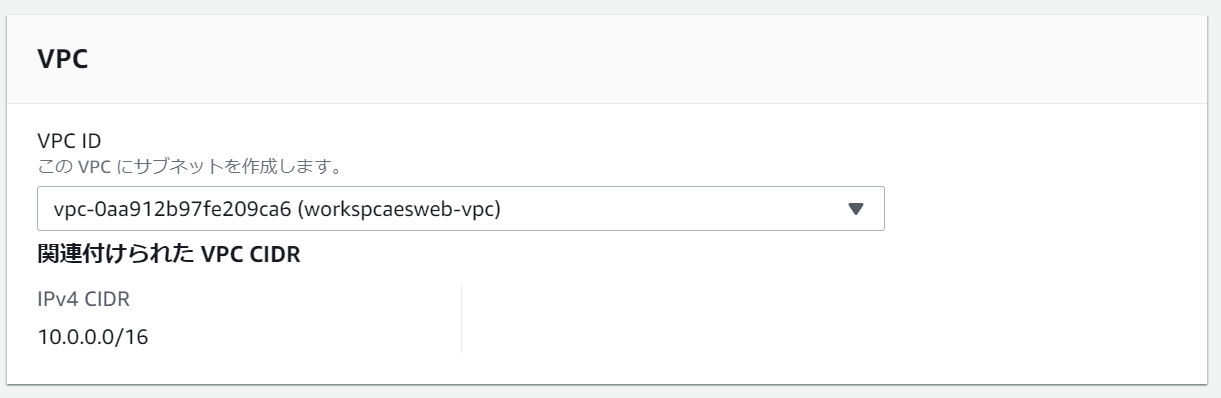
1. VPCのマネージメントコンソールに移動します
2. [VPCを作成]をおします
3. [名前タグの自動生成]にworkspaceswebと入力します
4. AZの数を1個に指定します。商用環境では可用性を考慮し2以上を指定することをお勧めします



1. NATゲートウェイを1に指定します



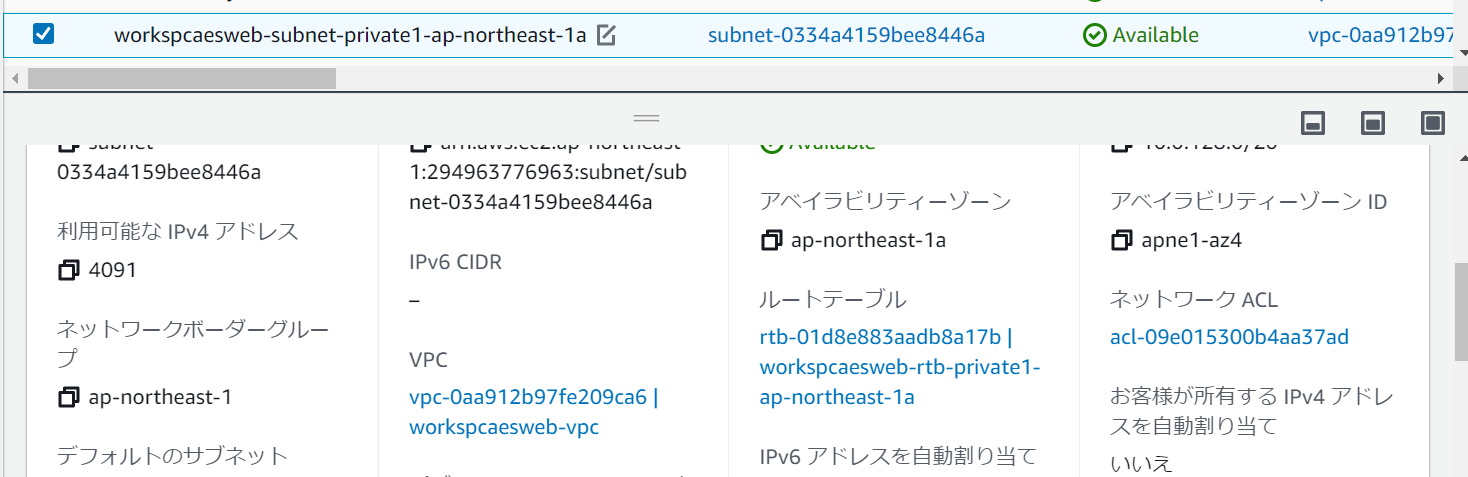
1. [VPCを作成]をおします
2. 全て作成が完了したら左ペインで[サブネット]をおします。Pubic, Private それぞれサブネットが1個できているはずです。もう一つPrivateサブネットを追加するため[サブネットの作成]をおします
3. 先程作成されたVPCを選びます



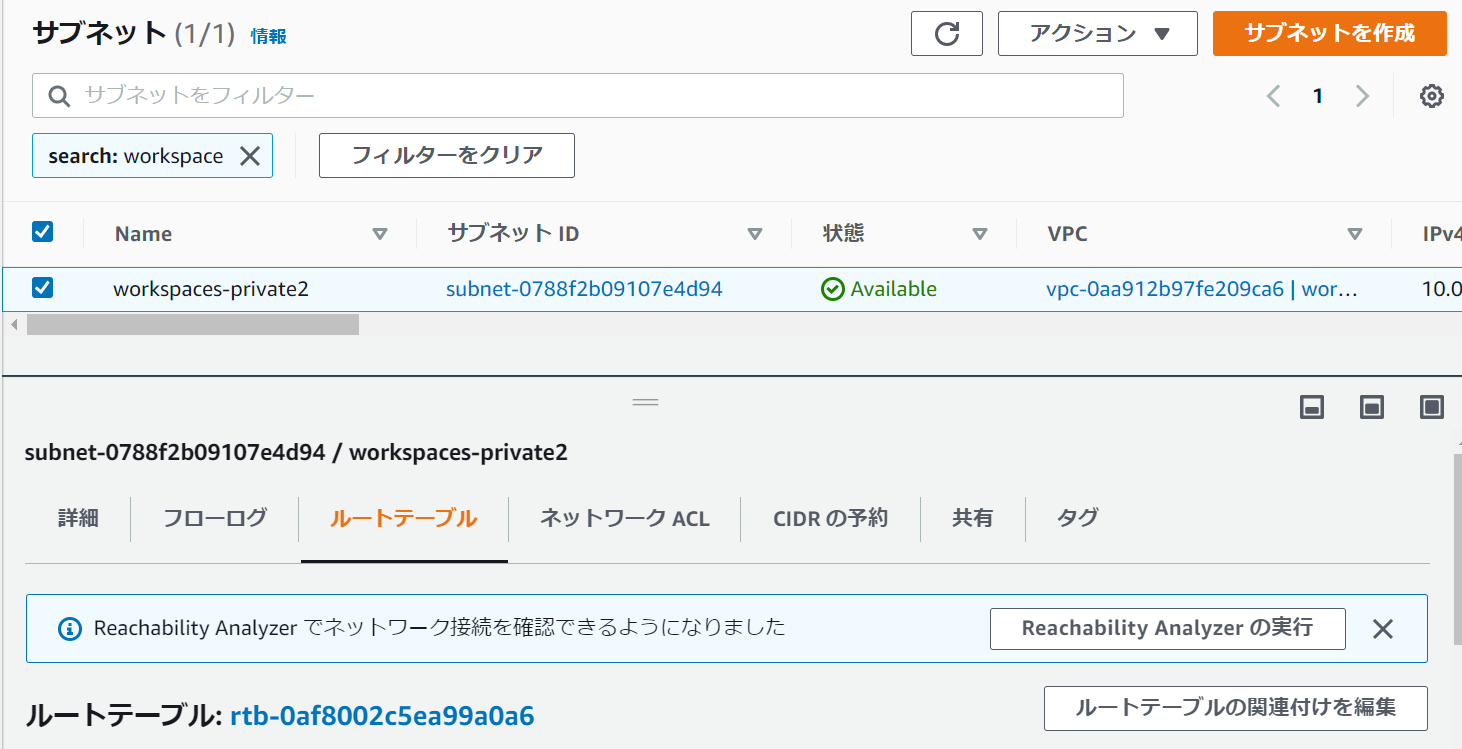
1. [サブネット名]に[workspaces-private2]と入力します
2. アベイラビリティゾーンで先程作成されたPrivate Subnetと異なるゾーンを指定します
3. [IPv4 CIDRブロック]に10.0.120.0/20と入力します



1. 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



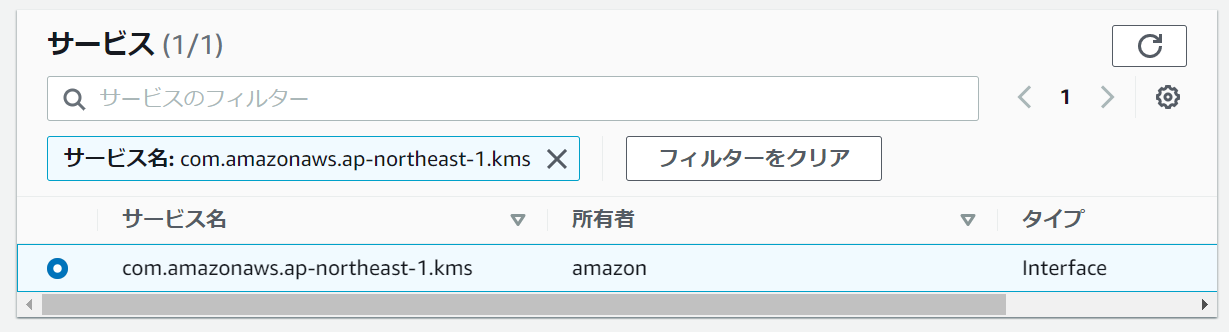
1. 新しく作成したサブネットの詳細画面で[ルートテーブル]をタブをクリックし、[ルートテーブルの関連付けを編集]をおします



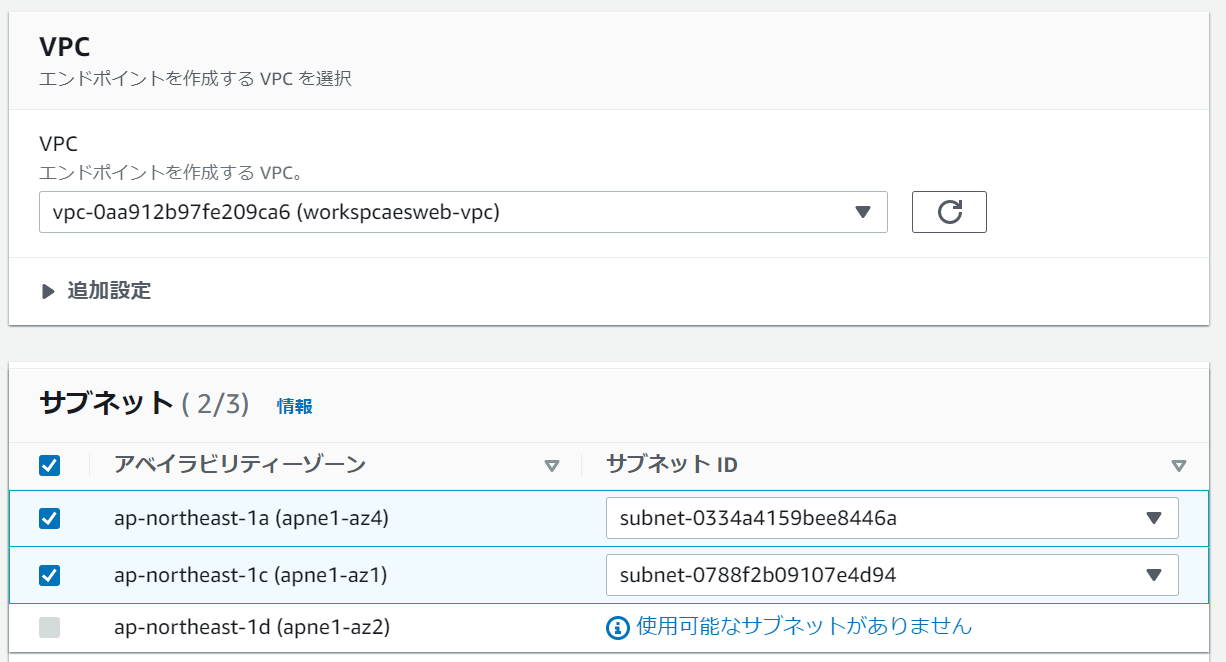
1. 先程コピーしたルートテーブルに置き換え、[保存]をおします



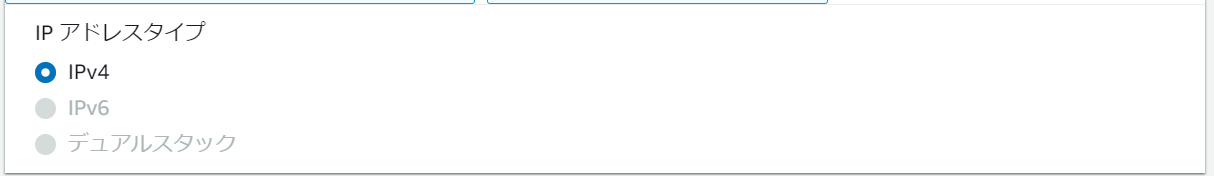
1. 左ペインからエンドポイントをクリックします。VPC Wizardで作成されたS3エンドポイントが表示されているはずです。表示されていない場合は何度か画面をリロードしてみてください
2. [エンドポイントを作成]をおします
3. [名前]にkmsと設定し、以下を選択します



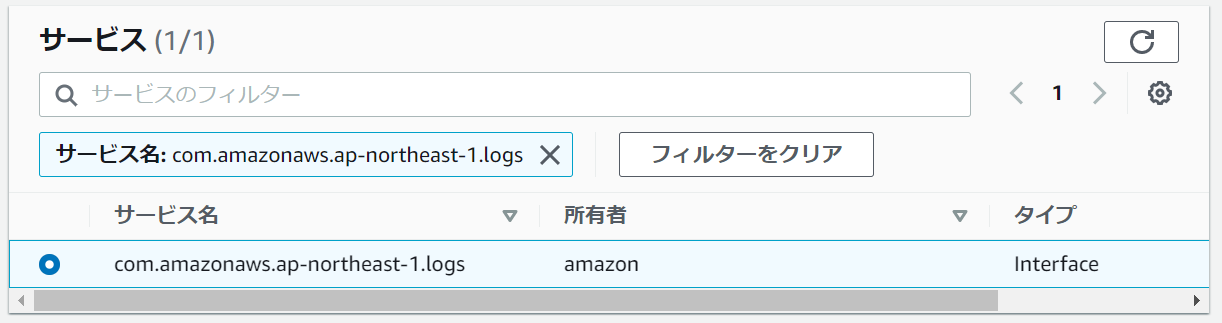
1. 先程作成したVPCとサブネットを選びます



1. IPv4を選びます



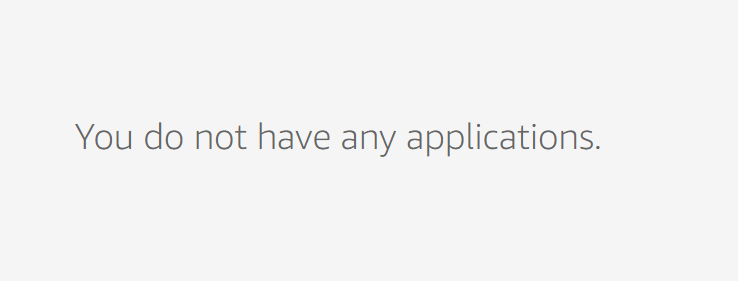
1. [エンドポイントを作成]をおします
2. 同様にlogsという名前で以下を作成します



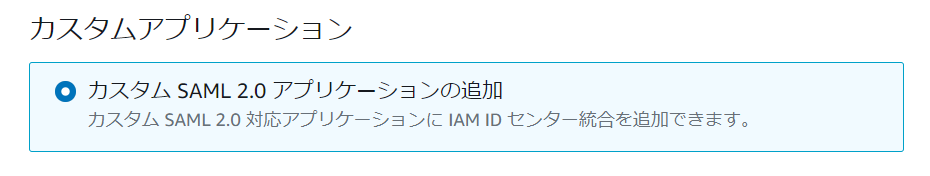
以上で、WorkSpaces Webを起動するネットワーク設定が完了です。

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。

1. 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
2. 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
3. [ユーザー名]にご自身のユーザーIDを入力します
4. [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）
5. [名][姓]に適当な値を入れて[次へ]をおします
6. 次のグループ画面は何も設定せず[次へ]をおします
7. [ユーザーを追加]をおします
8. 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
9. 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
10. 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。



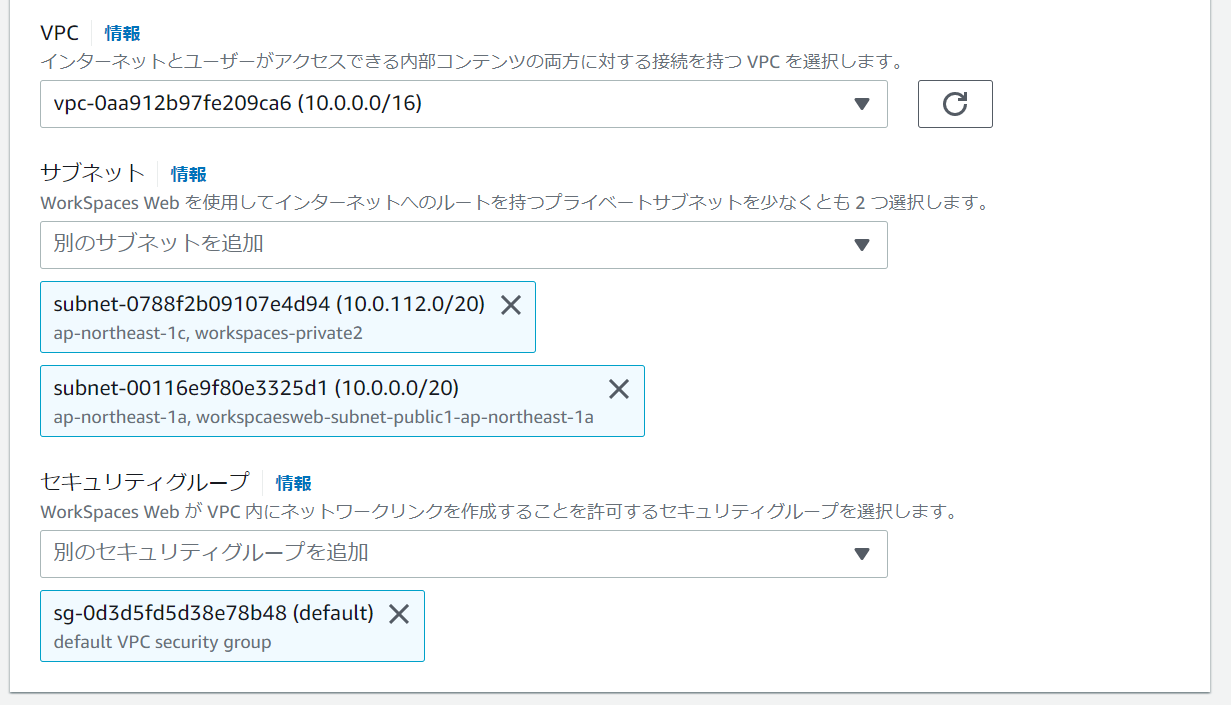
1. IAM Identity Centerの画面に戻り、左ペインから[アプリケーション]をクリックします
2. [アプリケーションを追加]をおします
3. [カスタム SAML 2.0 アプリケーションの追加]にチェックをつけます



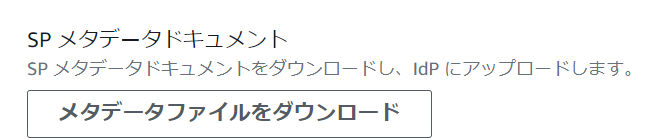
1. [次]をおします
2. [IAM Identity Center SAML メタデータファイル]をダウンロードし、保存しておきます

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。

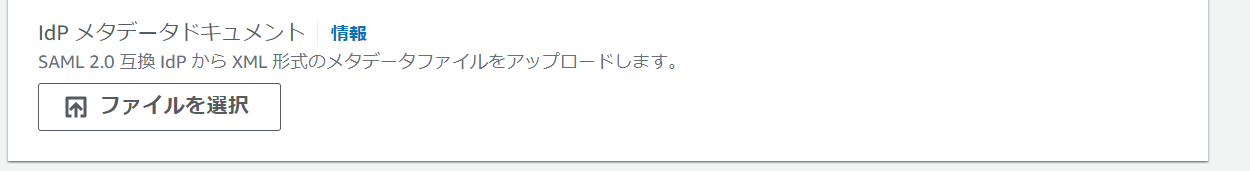
1. Amazon Workspacesのマネージメントコンソールに移動します
2. [ウェブポータル]をクリックします
3. [ウェブポータルの作成]をおします
4. 以下の通りネット―枠を設定します。サブネットはプライベートサブネットを2つ指定します。セキュリティグループはデフォルトをしていします。



1. [次へ]を3回おします
2. メタデータファイルをダウンロードします



1. 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



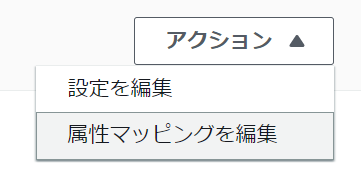
1. [次へ]をおします
2. [ウェブポータルを起動]をおします

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

1. [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



1. [アクション]から[属性マッピングを編集]を選びます



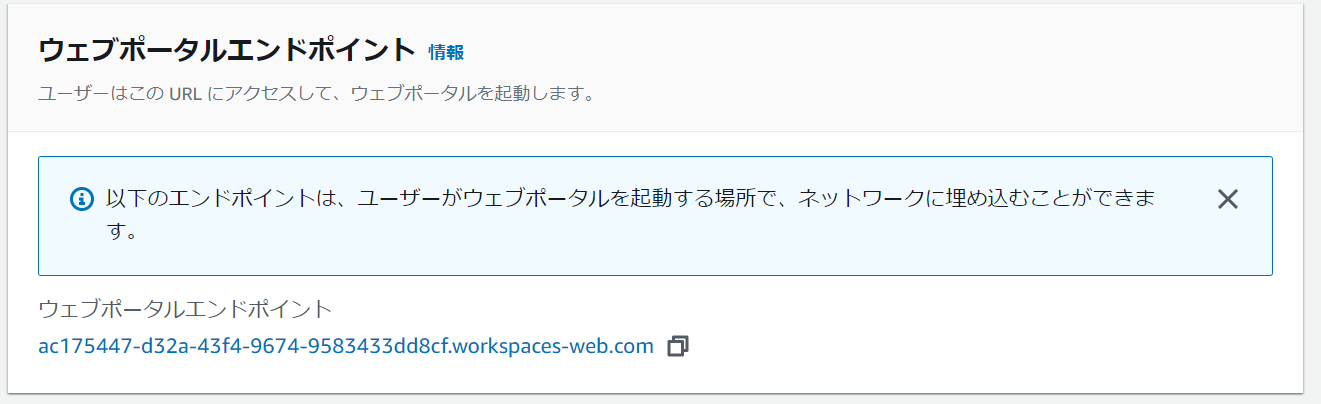
1. [この文字列値または IAM Identity Center のユーザー属性にマッピング]に[${user:email}]と入力します。 ( [ ] は含めない)。形式には[emailAddress]を指定します



1. [変更の保存]をおします
2. [ユーザーを割り当て]をおします
3. 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。



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