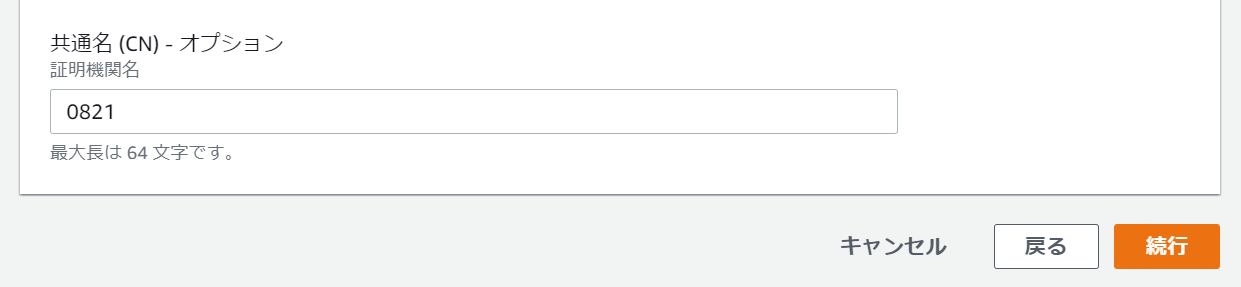
1. Trust AnchorとしてACM (Amazon Certificate Manager) のPCA (Private Certificate Authority) を起動します。マネージメントコンソールのACMに移動します
2. 左ペインから[AWS プライベートCA]をクリックします
3. [CAの作成]をおします
4. [ルートCA]を選び、[続行]をおします



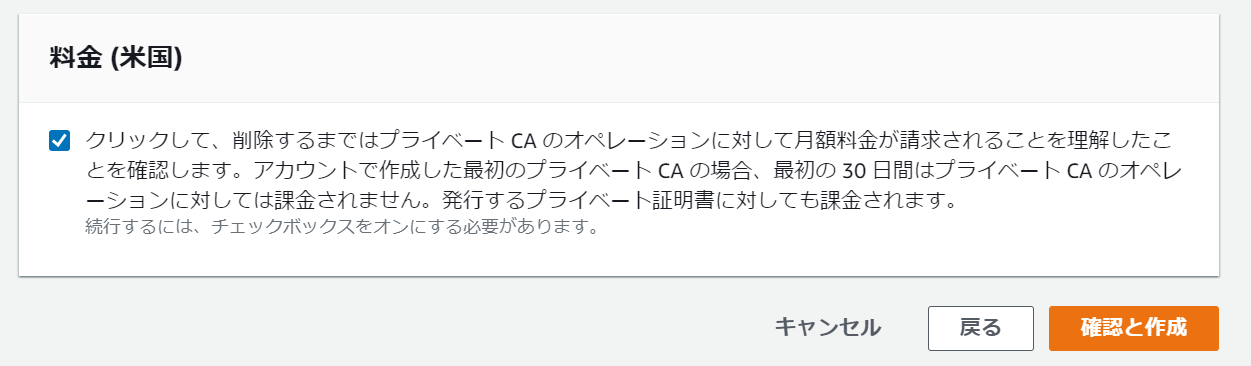
1. 共通名（CN）にMMDDを入力し、[続行]をおします。（MMDDは日付です）



1. 鍵はデフォルトのまま[続行]をおします
2. 失効の設定もデフォルトのまま[続行]をおします。（IAM Roles AnywhereはCRLに対応しており、有効期間中であっても失効された電子証明書用いた認証を拒否することが可能ですので商用環境では[CRLのディストリビューション]にチェックをつけることをお勧めします

<https://docs.aws.amazon.com/ja_jp/rolesanywhere/latest/APIReference/API_ImportCrl.html>

1. 2回[続行]を押した後、以下にチェックをつけて[確認と作成]をおします



1. [CA証明書をインストールする]をおします



1. [続行]、[確認及びインストール]をおします
2. ブラウザの別タブでIAMロールのマネージメントコンソールに移動します
3. 画面下部に以下の通りRoles Anywhereが出ています



はじめて作業される方は違う表示がされるかもしれませんが、画面に応じ初期設定を行います。

1. [管理]をおします
2. [信頼アンカーを作成する]をおします
3. 適当な名前を入力します
4. 先程作成したプライベートCAを選びます。この認証局から発行された証明書により署名されたSTSリクエストに対して一時クレデンシャルを発行する、というのがRoles Anywhereの基本動作です
5. [信頼アンカーを作成する]をおします
6. 左ペインの[ロール]をクリックして[ロールの作成]をおします
7. エンティティ[カスタム信頼ポリシー]を選んで以下をコピペし、[次へ]をおします

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Principal": {

"Service": [

"rolesanywhere.amazonaws.com"

]

},

"Action": [

"sts:AssumeRole",

"sts:TagSession",

"sts:SetSourceIdentity"

]

}

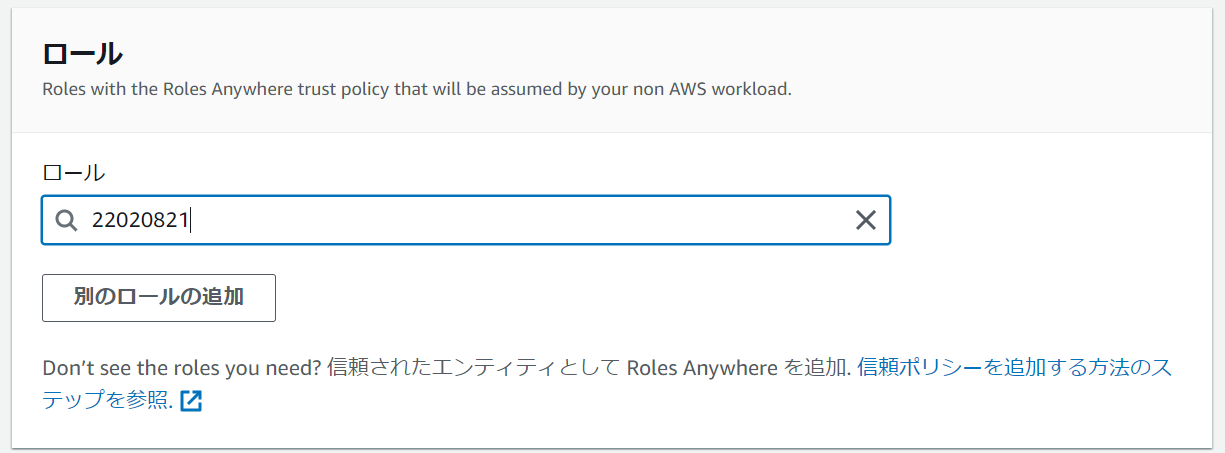
]

}

1. 許可ポリシーでは[AmazonEC2FullAccess]をセットし[次へ]をおします
2. 適当なロール名をセットし[ロールを作成]をおします
3. ロールが作成出来たらRoles Anywhereのマネージメントコンソールで[プロファイルの作成]をおします



1. [プロファイル名]に適当な名前をいれます
2. 先程作成したロールを選びます。正しくセットできていない場合ドロップダウンに表示されませんので、ロールの作成をやり直してみてください



1. [プロファイルを作成]をおします
2. 以下のようにプロファイルが正しく1個生成されれば完了です。



では実際にテストの準備を行います。先程作成したIAMロールは、Roles Anywhereが信頼している認証局から発行された証明書を持っている場合のみ、STSで一時クレデンシャルが発行可能となっています

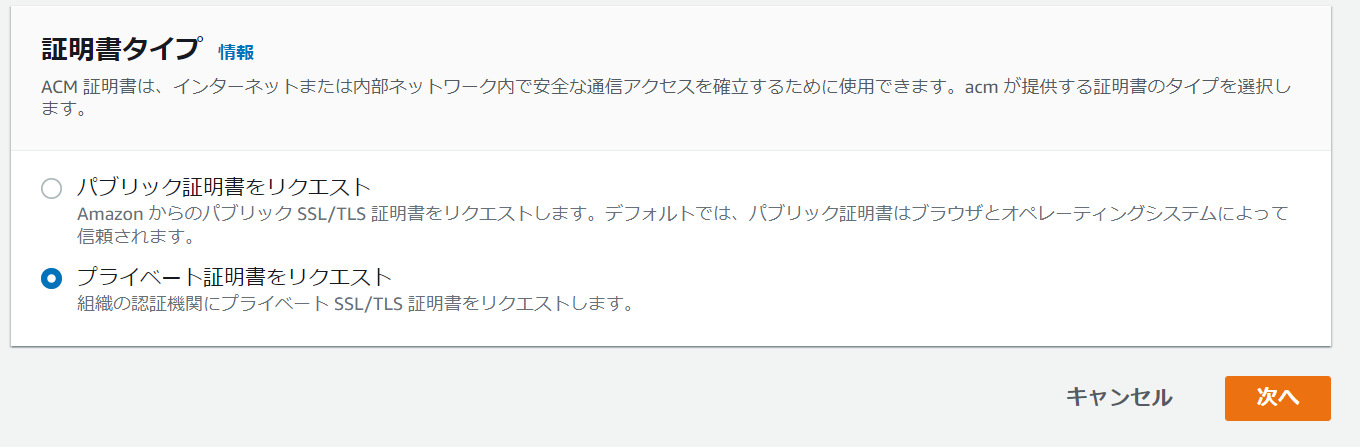
1. Cloud9のマネージメントコンソールに移動し、全てデフォルトで起動します
2. ターミナルにアクセスできたら以下のコマンドを実行し、credential\_heplerツールというRoles Anywhere用のツールをダウンロードします

sudo curl https://s3.amazonaws.com/roles-anywhere-credential-helper/CredentialHelper/latest/linux\_amd64/aws\_signing\_helper --output aws\_signing\_helper

1. 以下のコマンドで実行権限を付与します

sudo chmod +x aws\_signing\_helper

1. ACMのマネージメントコンソールで左ペインから[証明書をリクエスト]をおします



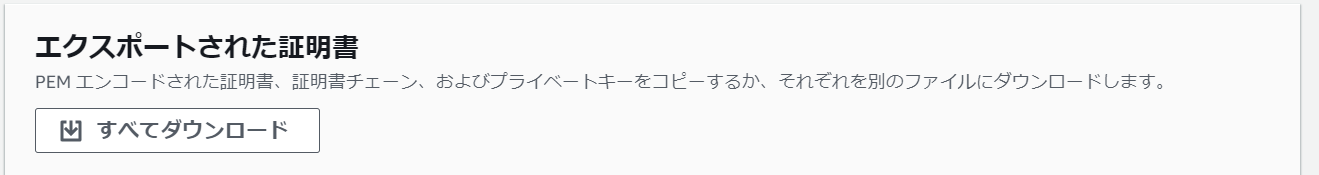
1. プライベート証明書を選択し[次へ]をおします
2. ドロップダウンから先程作成したprivateCAを選びます



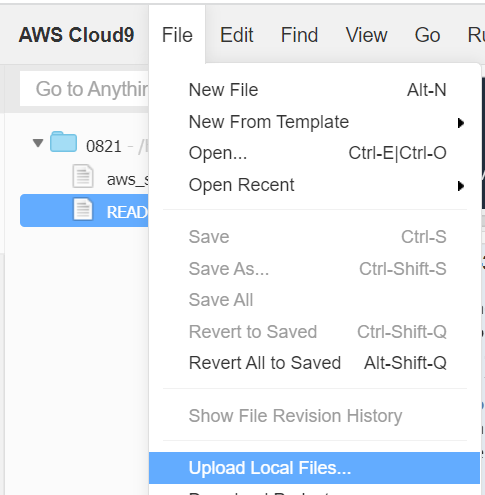
1. 適当なドメインを設定します（hkameda.com）等
2. [証明書の更新許可]にチェックをつけ[リクエスト]をおします
3. 左ペインから[証明書一覧]をクリックすると証明書が1個できています。証明書IDをクリックします



1. [エクスポートボタン]をおします
2. 適当なパスフレーズを入力し、チェックボックスをオンにして[PEMエンコーディングを作成]をおします
3. [全てダウンロード]をおします



1. Private\_key.txt 及び Certificate\_key.txtの拡張子をpemに変更します
2. Cloud9の機能を使ってファイルをアップロードします

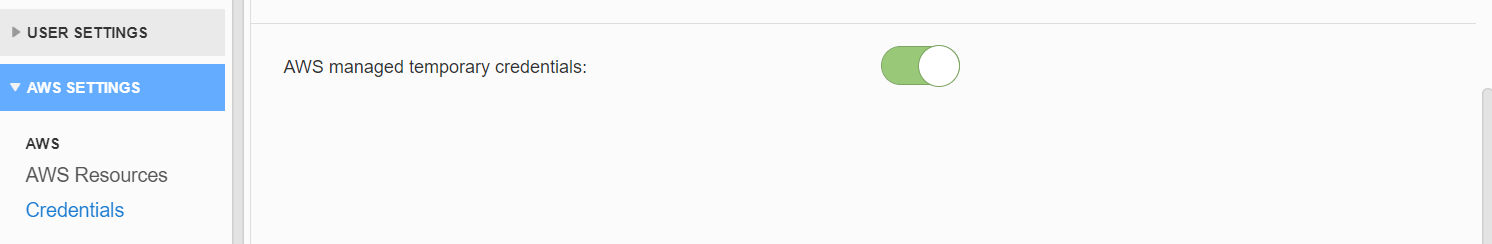


1. private\_key.pem に対してかかっているパスフレーズを以下のコマンドで外します

sudo openssl rsa -in private\_key.pem -out private\_key\_nopass.pem

先程設定したパスフレーズが求められます

1. Cloud9右上の歯車を押し以下の画面のトグルをオフにします



1. 以下のコマンドを実行します

./aws\_signing\_helper credential-process \

--certificate /path/to/certificate \

--private-key /path/to/private-key \

--trust-anchor-arn <arn1> \

--profile-arn <arn2> \

--role-arn <arn3>

arn1,2,3はそれぞれ以下の値で書き換えてください。

1: Roles Anywhere で設定されているトラストアンカー

2: Roles Anywhere で設定されているプロファイル

3: IAMロール



1. 出力された値を丸々手元のメモ帳などにコピーしてそれぞれいかに値を置換してください

export AWS\_ACCESS\_KEY\_ID=xxxx

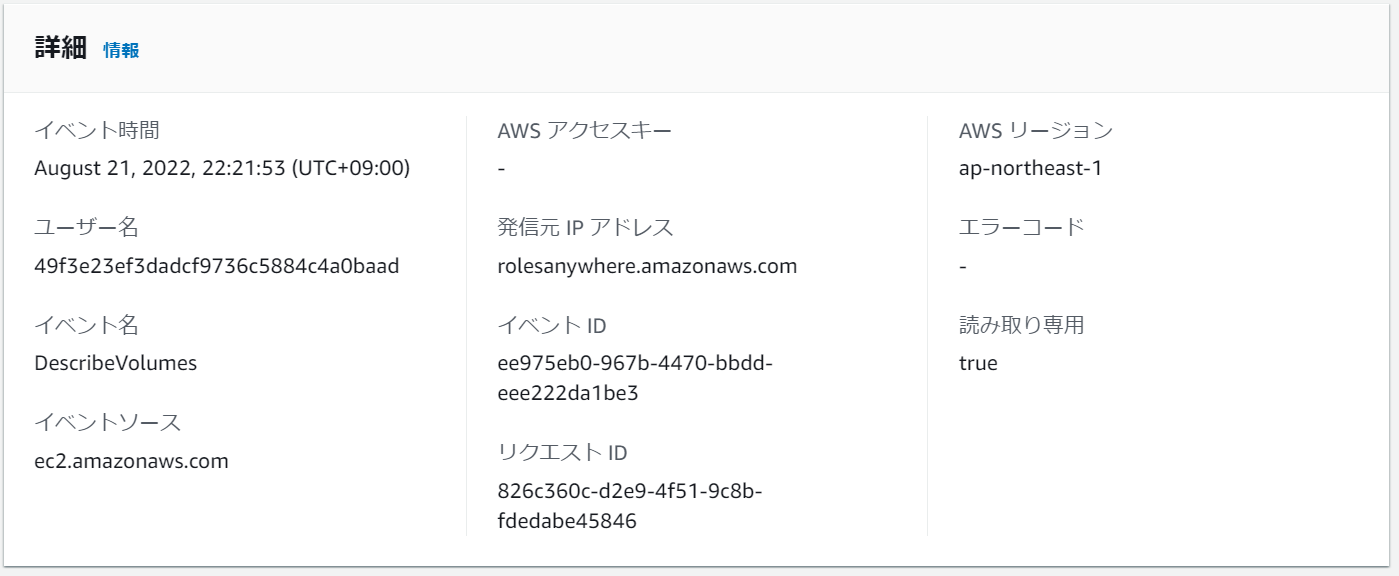
export AWS\_SECRET\_ACCESS\_KEY=xxxx

export AWS\_SESSION\_TOKEN=xxxx

1. うまく置換できれば以下のコマンドが正しく動作するはずです

ec2-user:~/environment $ aws ec2 describe-volumes --region ap-northeast-1

CloudTrailを見ると以下の通りRoles Anywhereから実行されていることがわかります



1. 最後に以下のコマンドを実行すると、今日作成したIAMロールから正しくassumeRoleされていることがわかります

aws sts get-caller-identity

