

AWS Client VPN で作るリモート接続環境③

2020年9月25日 2021年1月22日

こんにちは。米須です。

今回は Active Directory 認証の設定について説明したいと思います。

目次

1. Active Directory 認証の方法
2. SimpleAD の構築
3. AD へのユーザ登録
 - 3.1. Active Directory 管理ツールのインストール
 - 3.2. EC2 をドメインへ参加させる
 - 3.3. ユーザの登録
4. さいごに

Active Directory 認証の方法

AWS Client VPN で Active Directory 認証を行う場合、下記の3つの方法があります。

- Simple AD による認証
- AWS Managed Microsoft AD による認証
- オンプレのAD + AD Connector の認証

[AWS ドキュメント]

Active Directory 認証

https://docs.aws.amazon.com/ja_jp/vpn/latest/clientvpn-admin/client-authentication.html#ad

社内（オンプレ）にある AD も利用できたのですが、管理を別にしたかったので新しく Simple AD を構築しました。

ちなみに、後で気づいたのですが、利用者の接続可否は Simple AD に登録されているユーザを有効化／無効化することでコントロールできるので、AWS Client VPN 用に AD を構築する方法もアリだなと思いました。

SimpleAD の構築

では、SimpleAD を構築してみましょう。手順は下記にありますが、2020/9 時点ではまだ英語ですね(^^;

[AWS ドキュメント]

Simple AD ディレクトリを作成する

https://docs.aws.amazon.com/ja_jp/directoryservice/latest/admin-guide/how_to_create_simple_ad.html

まず、AWS Certificate Manager を開き、「ディレクトリ」から「ディレクトリのセットアップ」を押します。

ディレクトリタイプの選択で「Simple AD」を選択し、「次へ」を押します。

「ディレクトリのサイズ」で適切なサイズを選択し、「ディレクトリの DNS 名」、「管理者パスワード」を入力し、「次へ」を押します。

AD を構築する VPC と サブネットを 2 つ設定し、「次へ」を押します。（異なるサブネットに 1 つずつドメインコントローラが作成されるので、料金が 2 つ分なんですよね。。。）

設定内容を確認したら、「ディレクトリの作成」を押します。

新しい Simple AD が作成されているのが確認できると思います。Simple なだけあって、結構サクッと構築できたのではないのでしょうか。

AD へのユーザ登録

Simple AD もできたし、よし、ユーザ登録だ！。。。と言いたところですが、実は Simple AD はマネコンからユーザ登録できないんです(´-ω-`) ドメインに参加しているサーバから Active Directory 管理ツールでユーザ登録しなければならないので、まずはユーザ登録できる環境の構築から始めます。

[AWS ドキュメント]

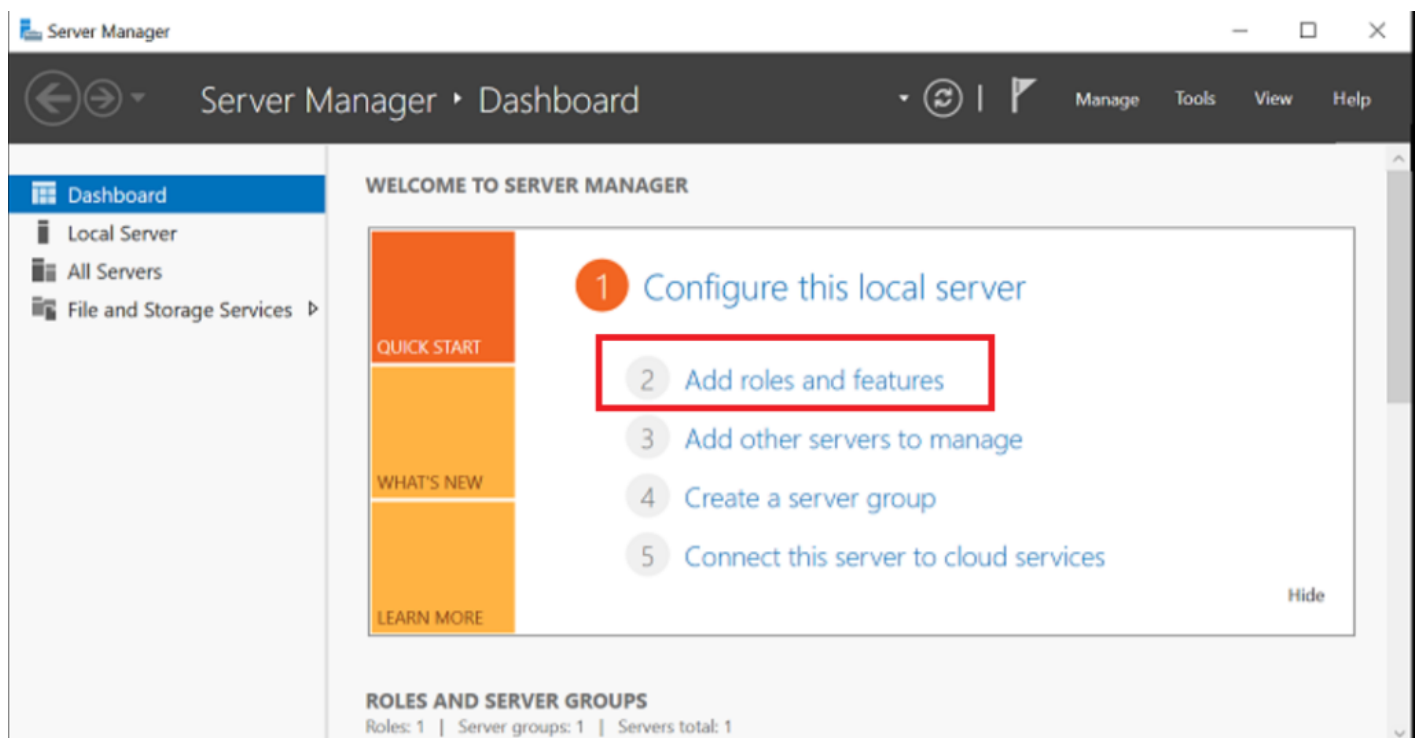
Simple AD のユーザとグループを管理する

https://docs.aws.amazon.com/ja_jp/directoryservice/latest/admin-guide/simple_ad_manage_users_groups.html

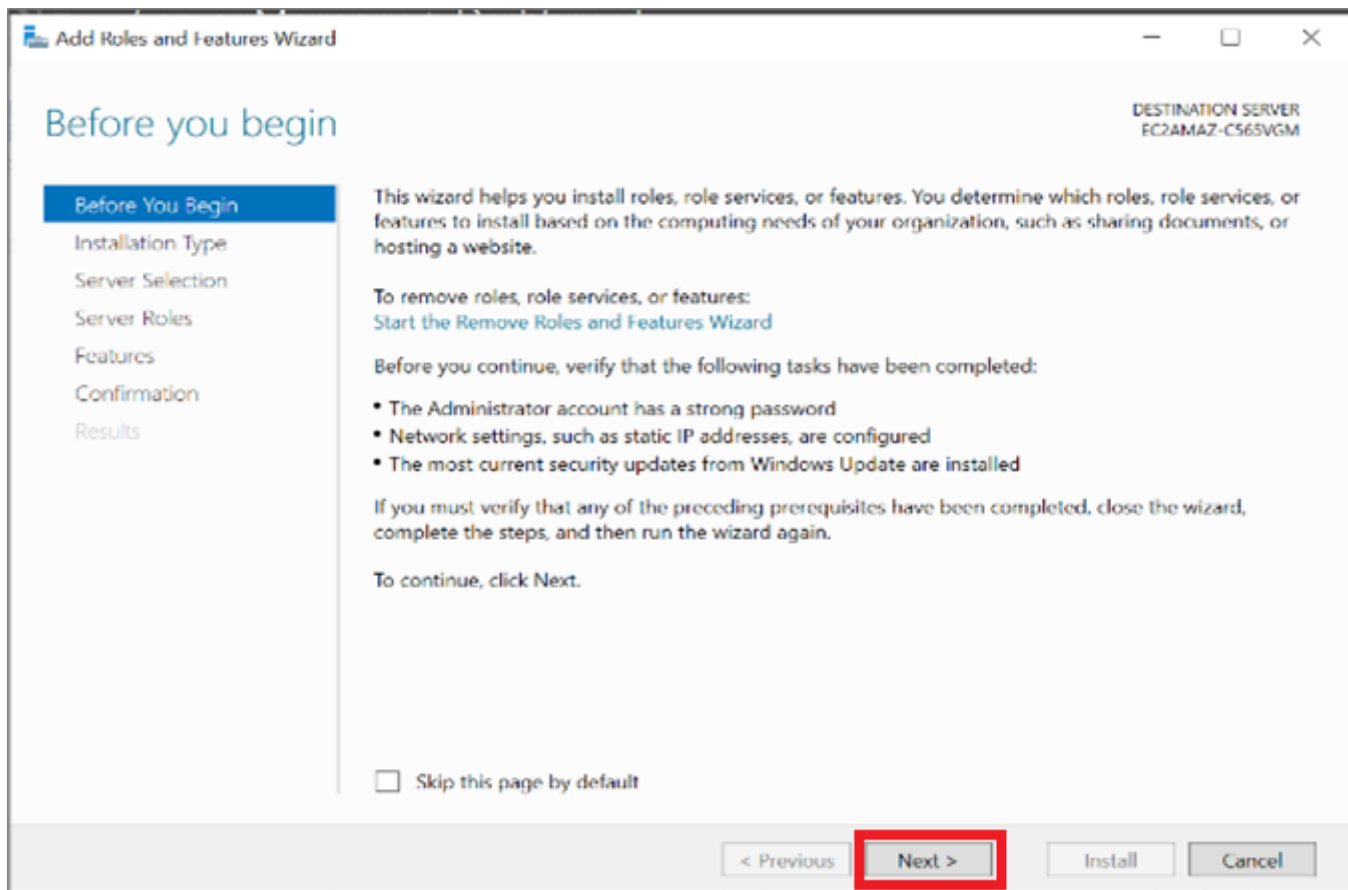
Active Directory 管理ツールのインストール

(英語版の OS で構築したためメニューが英語になっているので、日本語版の OS を利用されている方は適度に読み替えてください(^^;)

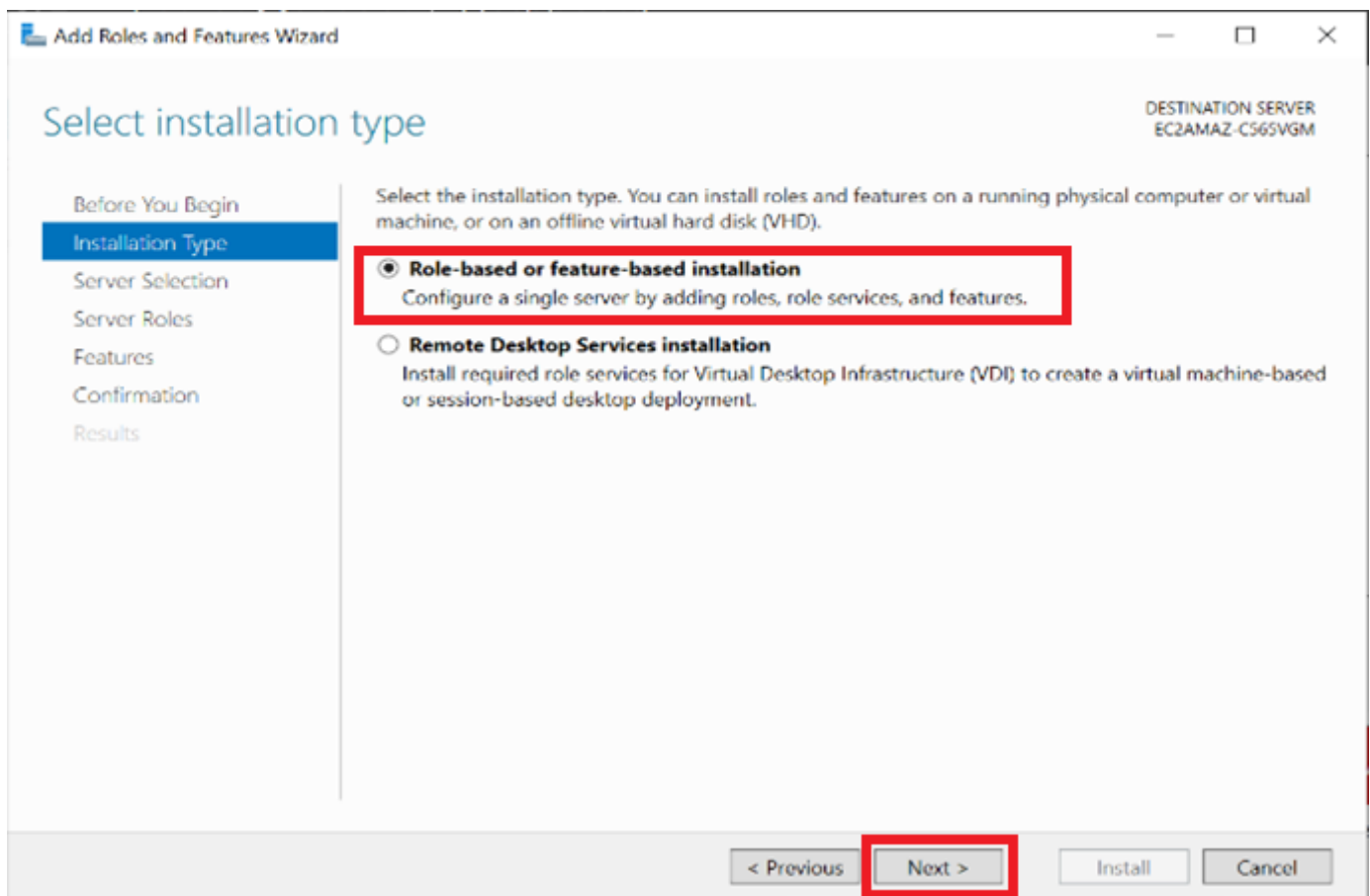
サーバーマネージャの「Add roles and features」を選択します。



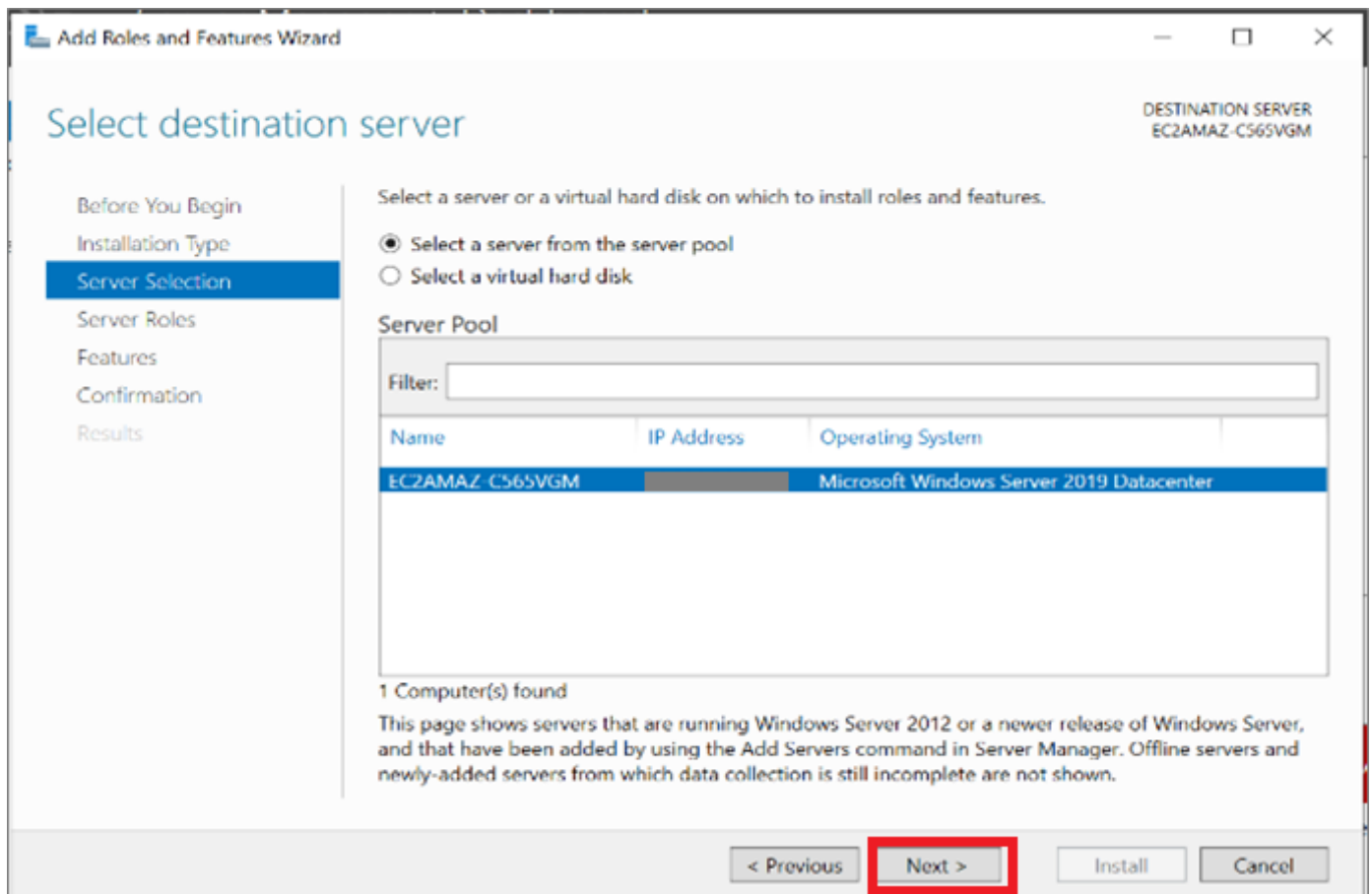
「Next」を押します。



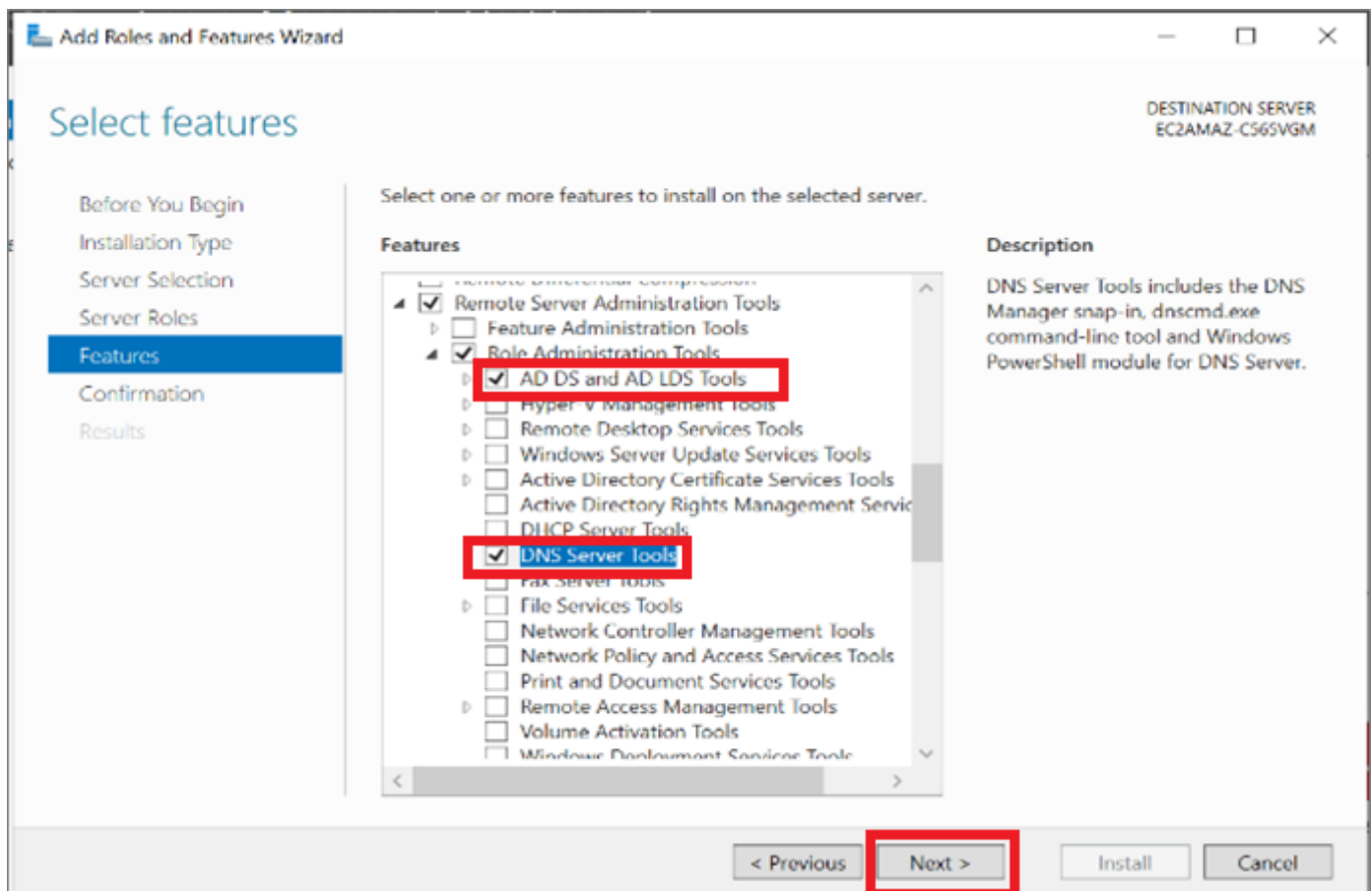
「Role-based or features-based installation」を選択し、「Next」を押します。



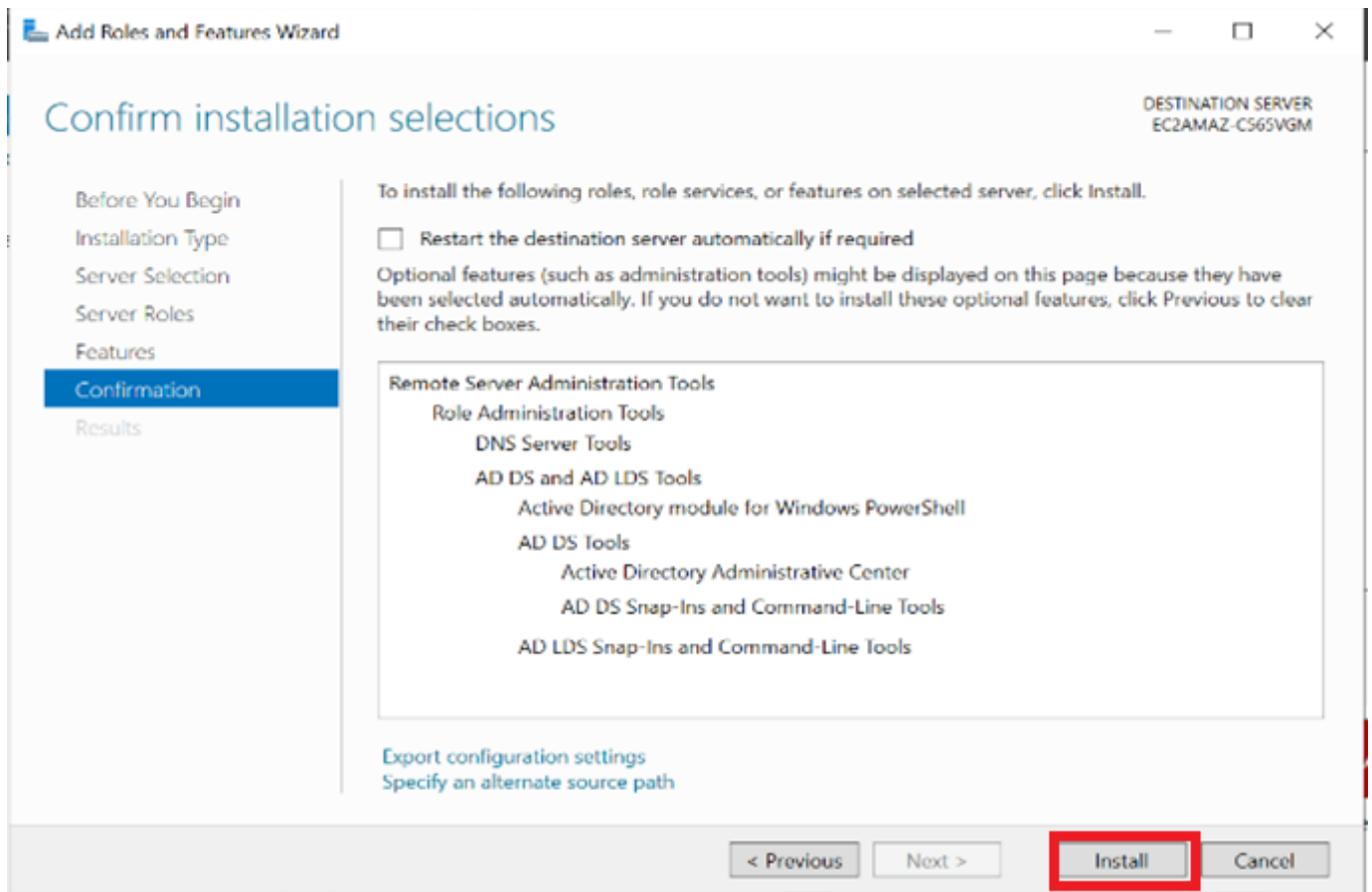
「Next」を押します。



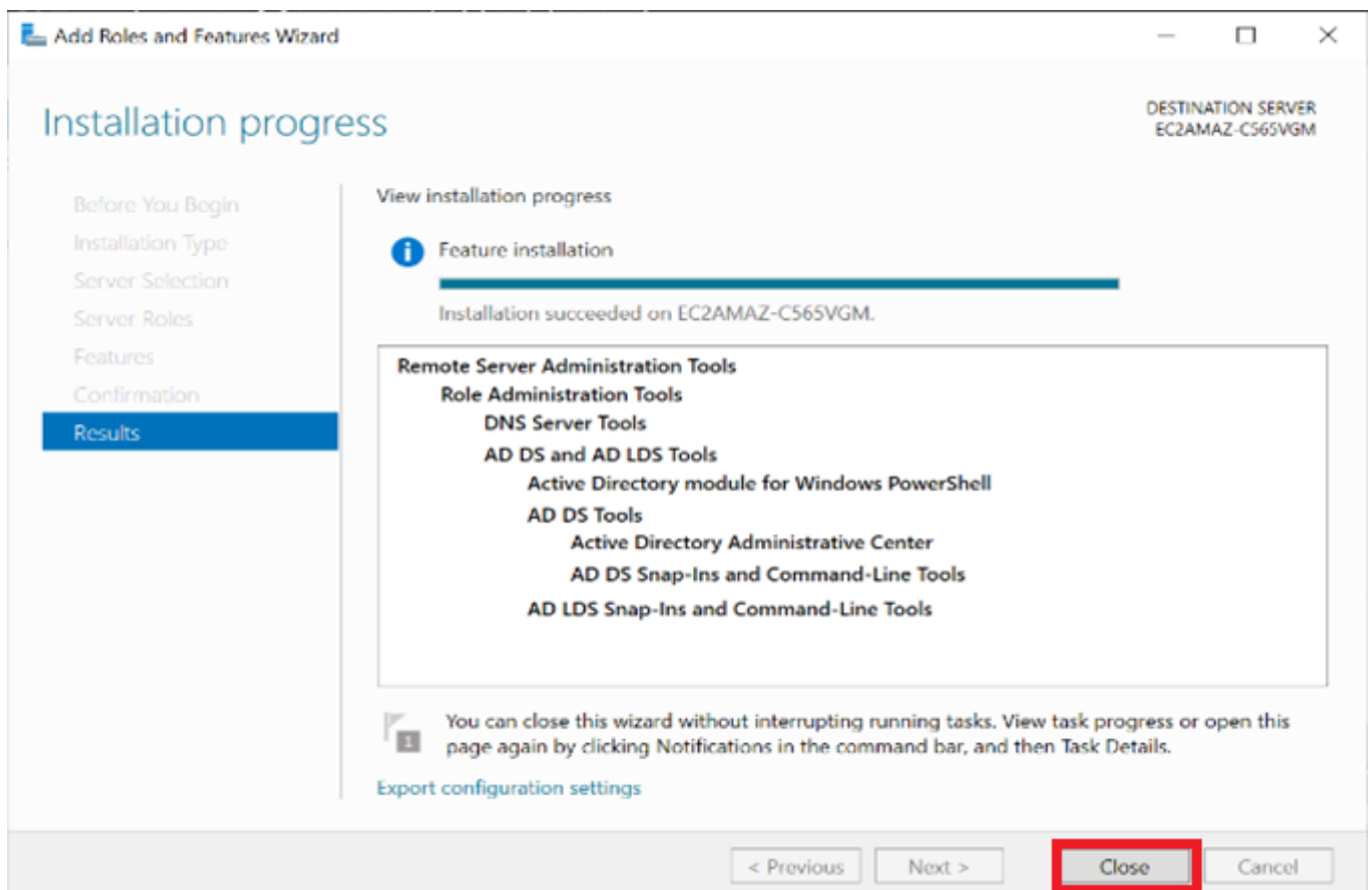
「AD DS and AD LDS Tools」と「DNS Server Tools」を選択し、「Next」を押します。



「Install」を押します。

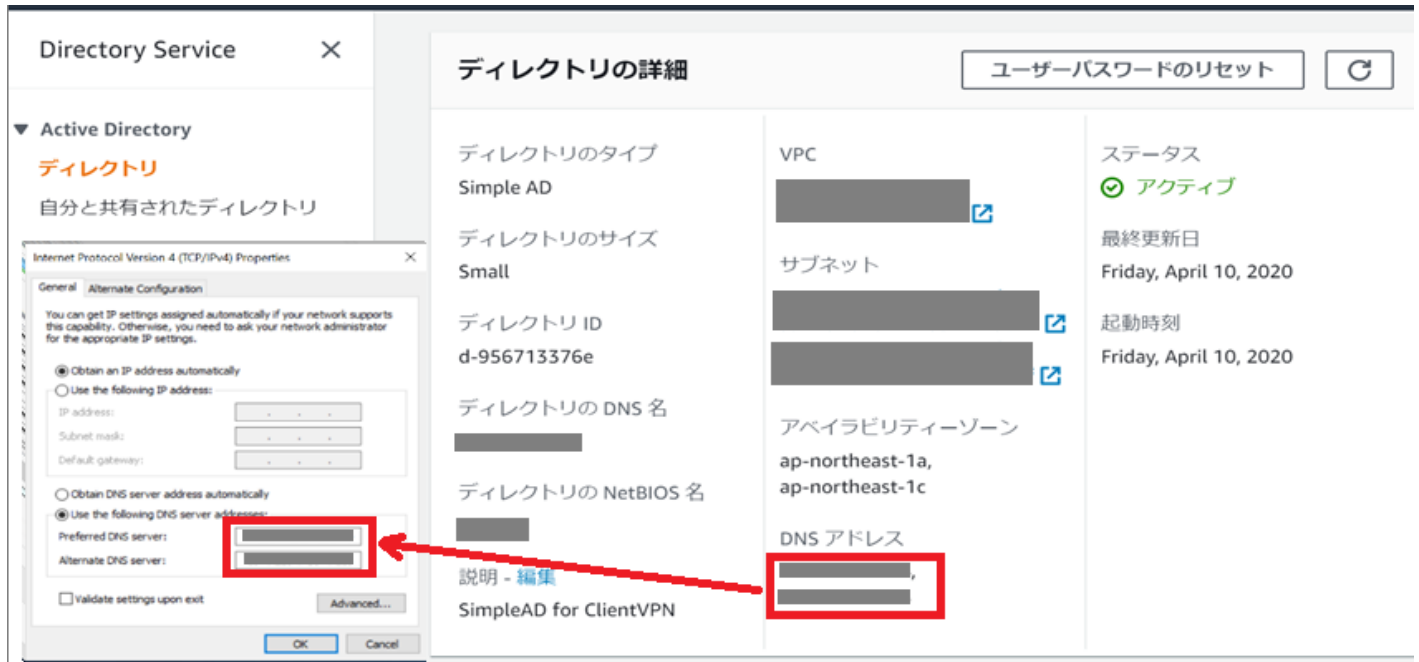


最後に「Close」を押したら Active Directory 管理ツールのインストールは終わりです。

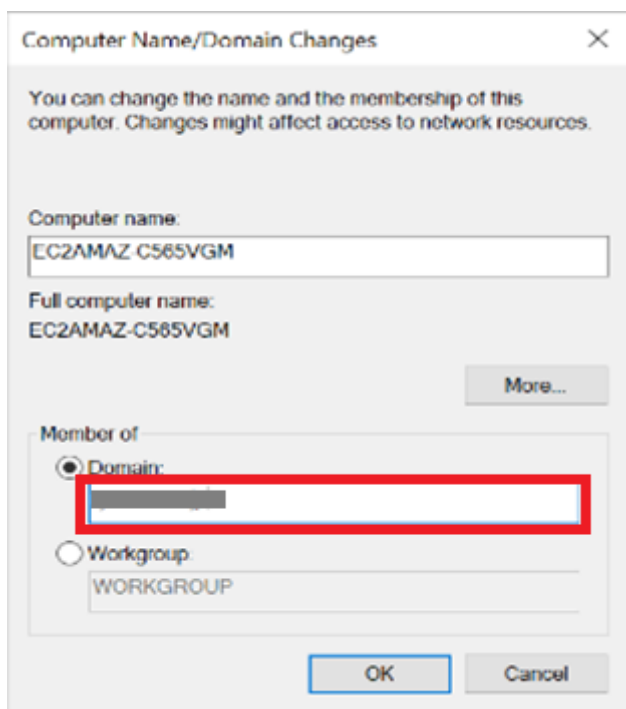


EC2 をドメインに参加させる

では、ツールをインストールした EC2 を、先ほど構築した Simple AD のドメインに参加させましょう。EC2 のネットワークのプロパティにおいて、Simple AD の DNS アドレスを設定します。



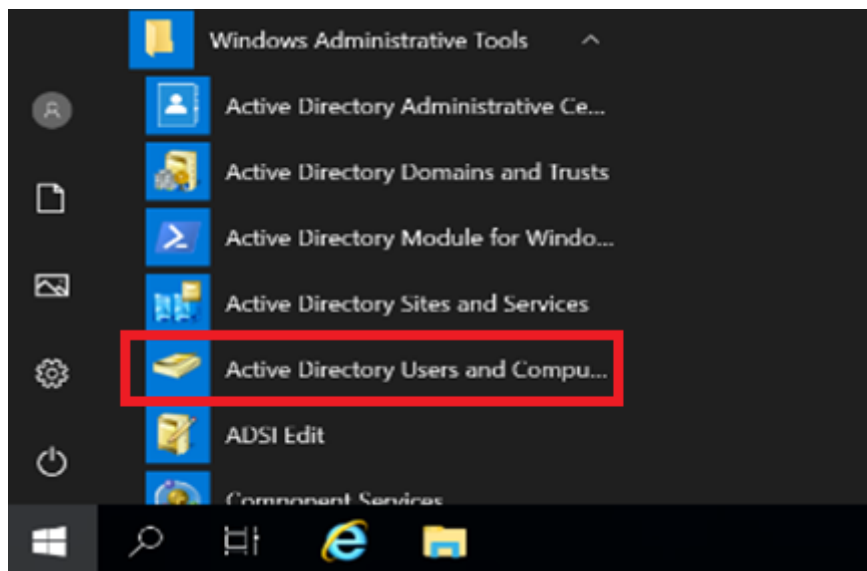
「Computer Name / Domain Changes」において、Simple AD の「ディレクトリの DNS 名」を設定し、ドメインに参加します。



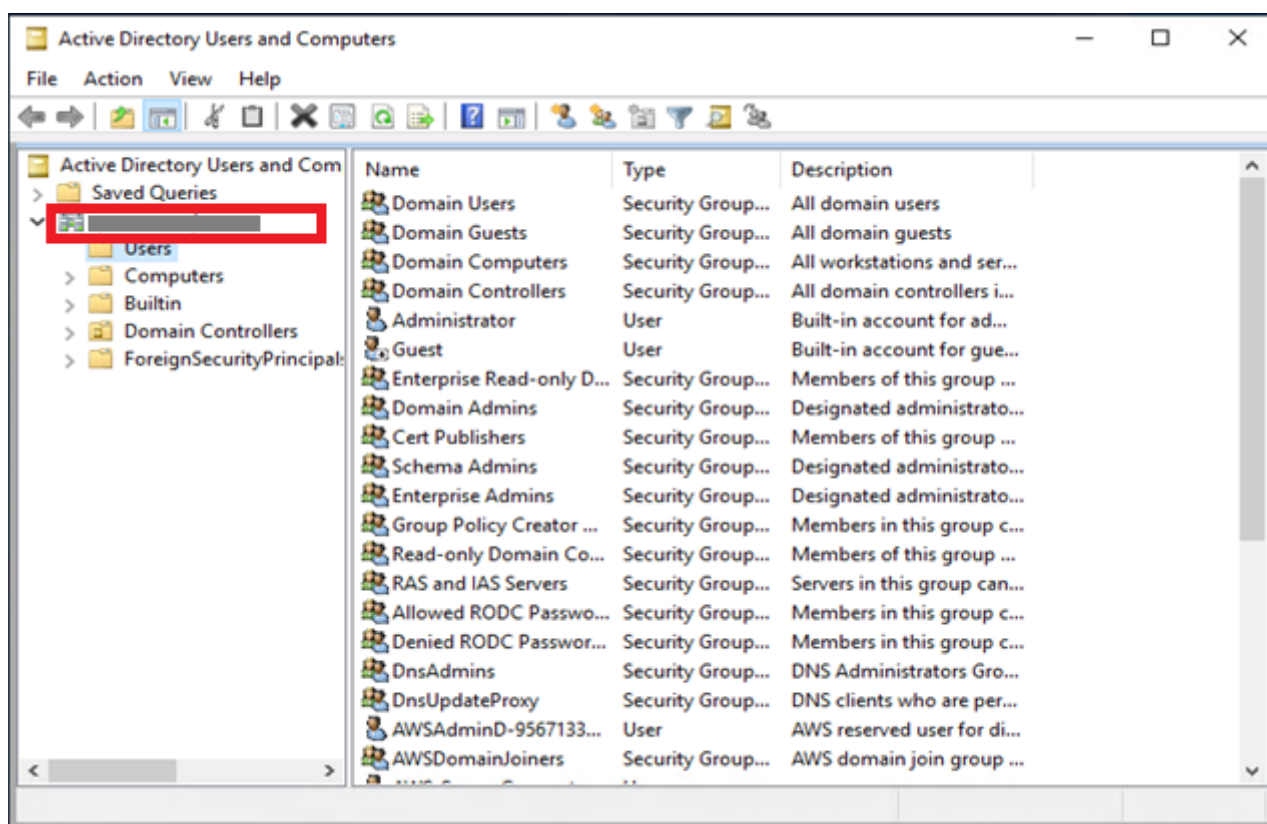
これで、やっとユーザ登録できる準備ができました。

ユーザの登録

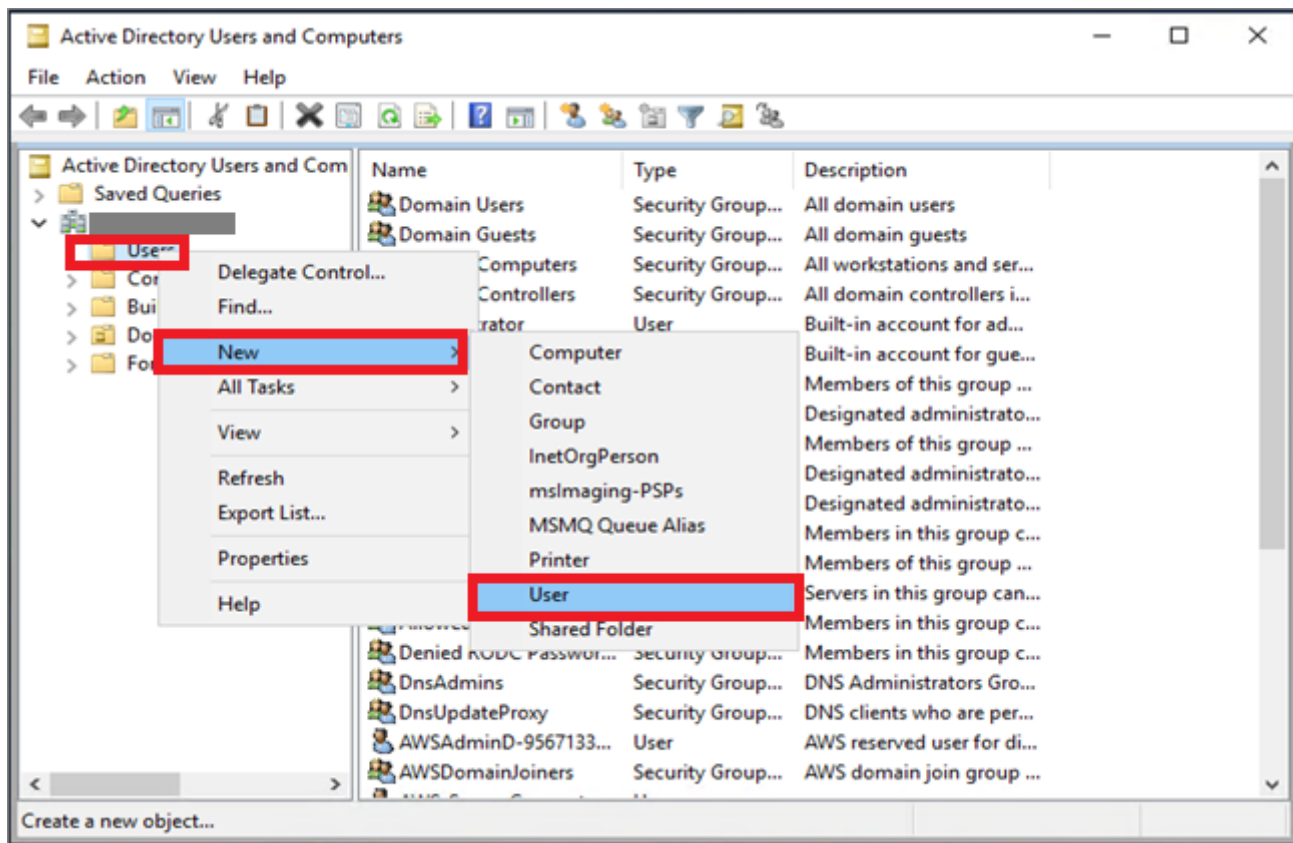
では、ユーザを登録していきましょう。「Active Directory Users and Computers」を起動します。



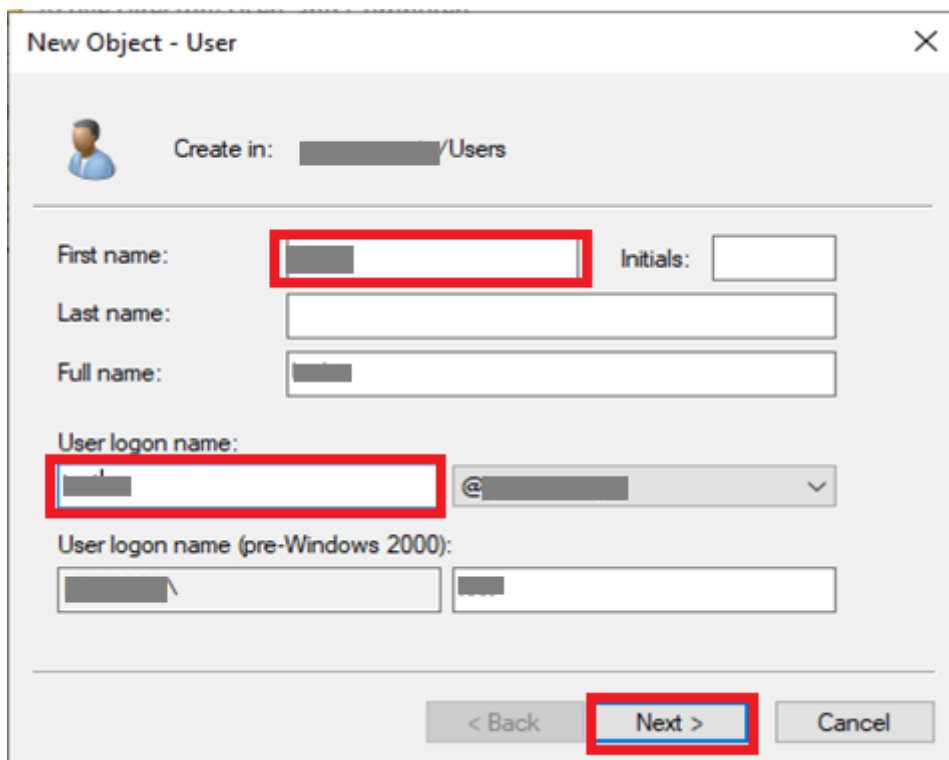
ドメインに参加できていれば、ドメイン名が表示されます。



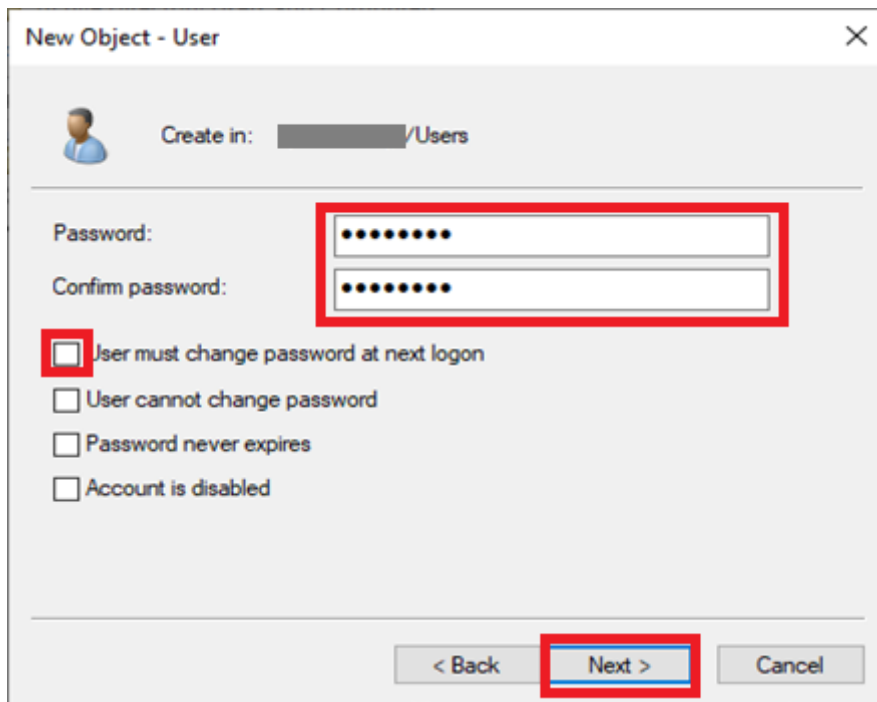
メニューから Users → New → User を選択します。



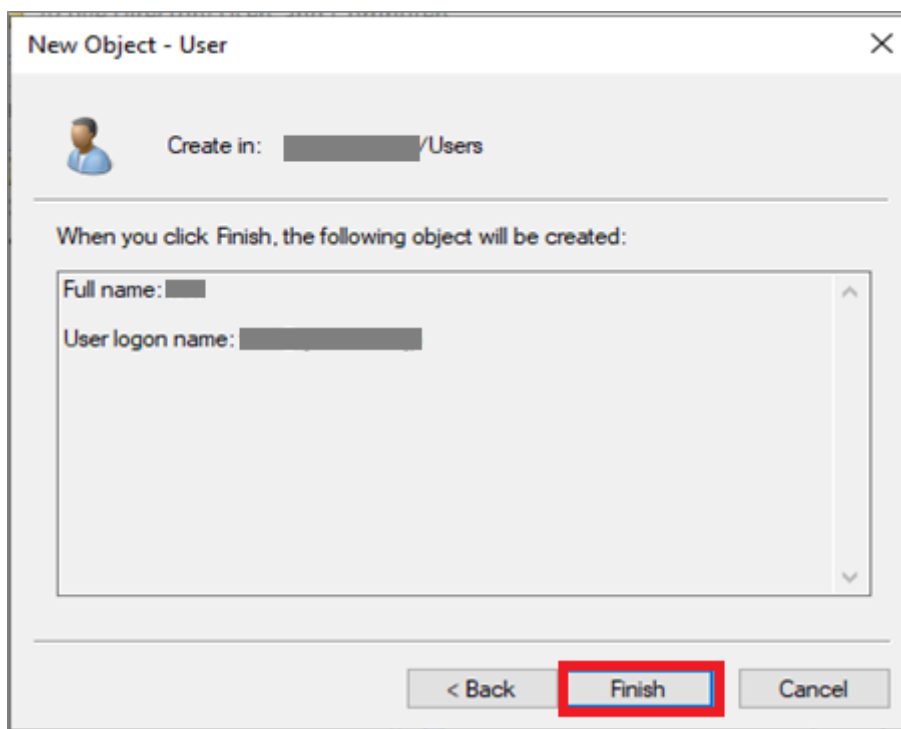
ユーザ名を入力し、「Next」ボタンを押します。



パスワードを入力し、「Next」ボタンを押下します。なお、Client VPN 接続時にリセットできないので「User must change password at next login」のチェックは外しておきます。



「Finish」ボタンを押したらユーザ登録完了です。



さいごに

これで前準備は終わりです。慣れない作業は難しいですね(^^; 次は、いよいよ Client VPN の設定をしていきます。

2021/01/22 追記

本文中に記載した「[AWS ドキュメント]**Simple AD ディレクトリを作成する**」の表示 URL とリンクされている URL が相違しておりました。表示 URL が誤りでしたので修正しております。失礼いたしました m(_ _)m