

AWS WorkSpaces での利用

USB リダイレクトを有効にすることで Matrix キーを利用できるようになります。

参考サイト

<https://dev.classmethod.jp/articles/try-amazon-workspaces-yubikey-auth/>

<https://dev.classmethod.jp/articles/amazon-workspaces-pcoip-64bit-agent-already-released-etc/>

https://docs.aws.amazon.com/ja_jp/workspaces/latest/adminguide/group_policy.html#gp_install_template

1. 前提条件：

1. AWS Managed Microsoft AD の事前セットアップ。
(Admin アカウントのパスワードは忘れないように)
2. PCoIP 環境 WorkSpaces。作成時、セットアップした AD ドメインに参加

2. グループポリシーの設定

起動した Workspaces の以下フォルダをディレクトリサーバのセントラルストアにコピー。

コピー元

C:¥Program Files¥Teradici¥PCoIP Agent¥configuration¥policyDefinitions

コピー先

¥¥FQDN¥sysvol¥FQDN¥Policies

(FQDN は AD ドメイン)

コピー先のディレクトリサーバのフォルダにはアクセス可能だが、書き込み権限がないためコピー不可、AWS Managed Microsoft AD をホストするサーバに直接ログインすることも不可。このため AWS Managed Microsoft AD を管理するために同じ AD ドメインに参加する別サーバを立ち上げて、AD リモート管理ツールをインストール。そのサーバを踏み台して AWS Managed Microsoft AD をリモート管理する必要あり。

踏み台サーバから policyDefinitions フォルダを [¥¥FQDN¥sysvol¥FQDN¥Policies](#) フォルダ内にコピー後、

1. 踏み台サーバーでグループポリシー管理(gpmc.msc)を起動
2. フォレストを開く (Forest: **FQDN**).
3. ドメインを開く
4. ドメイン FQDN を開く (例えば, **example.com**).
5. グループポリシーオブジェクトを開く.
6. デフォルトドメインポリシーを選択、右クリックして編集.

AWS Managed Microsoft AD を使っている場合、デフォルトドメインポリシーは編集不可。ドメインルートにドメイン名で OU が作成されているので、そこで右クリックして、“このドメインに GPO を作成してリンクする”を選択

7. 作成した GPO を右クリックで編集。コンピュータの構成→ポリシー→管理テンプレート→ **PCoIP Session Variables** 選択

Enable/disable USB in the PCoIP session

有効化

Configure PCoIP USB allowed and unallowed device rules

有効化

Enter the USB authorization table

10E500002