

Azure AD で
Windows 仮想マ
シンへログイン
RDP 接続する場合



概要

Azure AD のお作法的なものに慣れていないこともあって、少し手間取ったのでメモ。

- 設定
- 接続
- その他

設定

仮想マシン側の設定

機能の追加

VM 作成時に「管理」タブで「Azure AD でログインする」を選択することで各種設定が行われる。後からでも変更できるが、Azure CLI 等が必要なもよう(2021-06 時点)。

ホーム > リソースの作成 >

仮想マシンの作成 ...

ID

システム割り当てマネージド ID



i Azure AD 資格情報でログインするには、システム マネージド ID がオンになっている必要があります。 [詳細情報](#)

Azure AD

Azure AD でログインする







i Azure AD ログインを使用する場合は、仮想マシン管理者ログインまたは仮想マシン ユーザーログインの RBAC ロールの割り当てが必要です。 [詳細情報](#)

ロールの割り当て

作成後、RDP 接続に使いたいユーザーへ「仮想マシンのユーザーログイン」か「仮想マシンの管理者ログイン」ロールを割り当てる。

2 個のアイテム (2 個のグループ)

<input type="checkbox"/> 名前	種類	役割
仮想マシンの管理者ログイン		
<input type="checkbox"/>  	グループ	仮想マシンの管理者ログイン ①
<input type="checkbox"/>  	グループ	仮想マシンの管理者ログイン ①

クライアント PC 側の設定

RDP で Azure AD の資格情報を使う場合、クライアント側にも追加の設定が必要となるが、時期や Windows のバージョン、オンプレミスの AD に参加しているか等で必要な要件が異なる。

Windows 10 Pro 以上でオンプレミスの AD がなければクライアント PC を Azure AD のデバイスへ「参加」させるのが簡単。Windows 10 Home でも 20H1 以降であれば、デバイスへ「登録」で RDP 接続ができるようになる。

参考: [Azure Active Directory を使用して Azure 内の Windows 仮想マシンにサインインする | Microsoft Docs](#)

Windows 10 Home を Azure AD へ登録する

デバイスの「参加」はネット上に情報が多いので、Home(20H2)を「登録」した場合の操作。

- 「設定」「アカウント」「職場または学校にアクセスする」から「接続」を選択
- 「このデバイスを Azure Active Directory へ参加させる」は表示されないが、メールアドレスに Azure の ID を入力して進める
- サインインするだけでとくに確認事項はなく終了する

登録が完了すると以下のような画面が表示される。



Azure portal で確認すると「registered」となる。

名前	有効	OS	バージョン	結合の種類	所有者
<input type="checkbox"/>	✔ はい			Azure AD registered	
<input type="checkbox"/>	✔ はい	Windows	10.0.19042.1052	Azure AD registered	
<input type="checkbox"/>	✔ はい			Azure AD joined	

接続と切断

RDP 接続する

資格情報

「登録」したデバイスから接続を開始し、資格情報を入力するときに **AzureAD** を付加する。

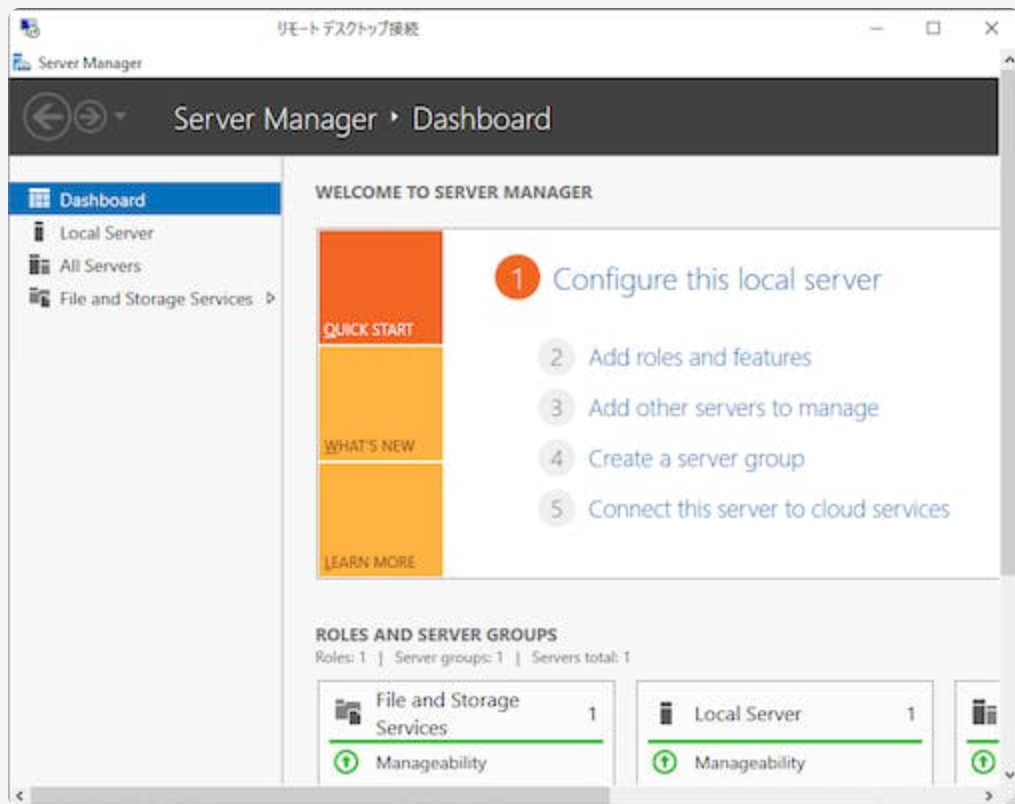


リモートコンピューターの ID

Kerberos 認証にはなっていないので、おなじみの警告が出る(「参加」したデバイスからでも同様)。



接続完了



切断

- 通常の RDP と同じ(スタートメニューなどから切断する)
- RDS のような外部からの切断や挙動の指定はできないもよう
- 「My Account」 「セキュリティ情報」から「すべてサインアウトしてください」を選択してもサインアウトされない

The screenshot shows the 'My Account' page with the 'Security Information' section selected. The page title is '自分のサインイン' (My Sign-in). The left sidebar contains navigation links: '概要' (Overview), 'セキュリティ情報' (Security Information), '組織' (Organization), 'デバイス' (Devices), and 'プライバシー' (Privacy). The main content area is titled 'セキュリティ情報' (Security Information) and includes the text 'これは、ご自分のアカウントへのサインインやパスワードの再訂' (This is for signing in to your account or resetting your password). Below this, it shows the current sign-in method: '既定のサインイン方法: Microsoft Authenticator - 通知 変更' (Default sign-in method: Microsoft Authenticator - Notification Change). A '+ 方法の追加' (+ Add method) button is visible, and the 'Microsoft Authenticator' method is listed below it.

その他

課題

継続して利用する場合、以下の点は不便なので回避したい。

- 「電話によるサインイン」を有効にしているユーザーでもパスワードを求められる
 - 条件付きアクセスで回避できる可能性はあるが未検証
- 接続時にリモートコンピューター(仮想マシン)の ID 確認が必要
 - Azure AD の設定で回避できないか？
- 利用できるクライアント環境が限定される
 - 管理されたデバイスに限定されるのは良いのだが、できれば Android の Remote Desktop も使いたい