Azure AD で Linux 仮想マシンへログイン

SSH 接続する場合

概要

証明書の使い方が興味深かったのでメモ。

- 設定
- 接続、エクスポート、切断
- その他

設定

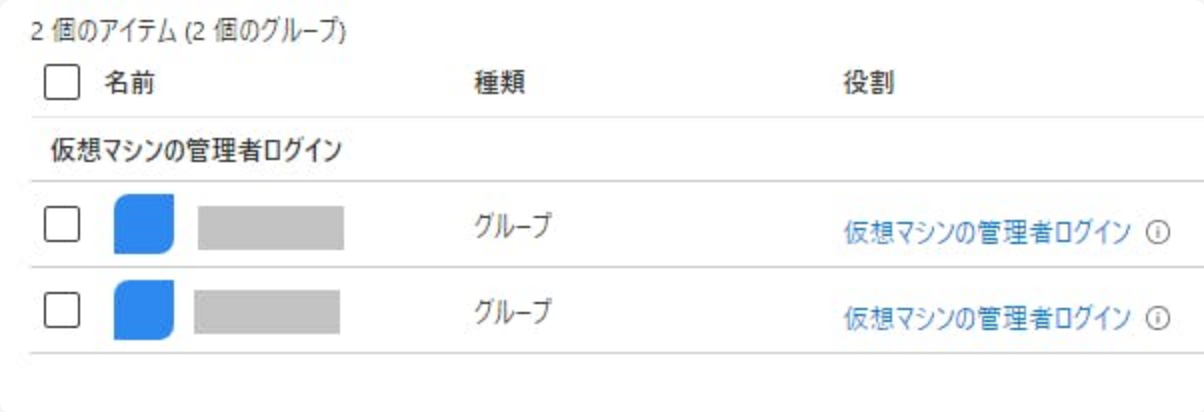
仮想マシン側の設定

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)。

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。



クライアント PC 側の設定

Azure CLI の Docker イメージを使うのが手軽で確実。

- `docker run --rm -it mcr.microsoft.com/azure-cli`
- `az extension add --name ssh` で Az CLI 用 SSH 拡張機能をインストール(ここでやらなくても SSH 接続時に自動的にインストールされる)
- `az login` で Azure へサインイン
  - 通常はブラウザーを開いてのデバイスログインになる
  - ブラウザーでサインインするときには「電話によるサインイン」等も利用可能

接続、エクスポート、切断

Azure CLI から SSH 接続する

仮想マシンのパブリック IP を利用

Azure portal 等からパブリック IP をコピーしておき Azure CLI のコンテナで以下のコマンドを実行。

```
az ssh vm --ip <addr>
```

なお、ホスト認証で署名された鍵が使われる様子はなかった(後述の方法でも同様)。

仮想マシンの名前を利用

Azure portal 等から仮想マシンの名前とリソースグループ名をコピーしておき Azure CLI のコンテナで以下のコマンドを実行。

```
az ssh vm -n <vmname> -g <rgname>
```

なお、「仮想マシンのユーザーログイン」ロールだと `Microsoft.Network/networkInterfaces/read` の権限でエラーとなることがあった(2021-06-13 時点)。現在は発生しないもよう。エラーになったのは勘違いの可能性が高いが念のため。

接続設定をエクスポートする

エクスポートの実行

OpenSSH 証明書用に設定をエクスポートできるが、証明書の有効期間が 1 時間程度なので、どちらかと言うと短期間の証明書発行に近いイメージ。

- `az ssh config --file ~/.ssh/config -n <vname> -g <rgname>` 等で設定が `~/.ssh/config` へ追加される
- `~/.ssh/config` の内容を確認し `ssh <addr>` などで接続する

有効期間

有効期間は以下のように確認できる。

```
$ ssh-keygen -L -f /tmp/aadsshcertXXXXXXXX/id_rsa.pub-aadcert.pub

        Type: ssh-rsa-cert-v01@openssh.com user certificate
        Public key:
        snip...
        Valid: from 2021-06-18T07:56:15 to 2021-06-18T09:01:15
```

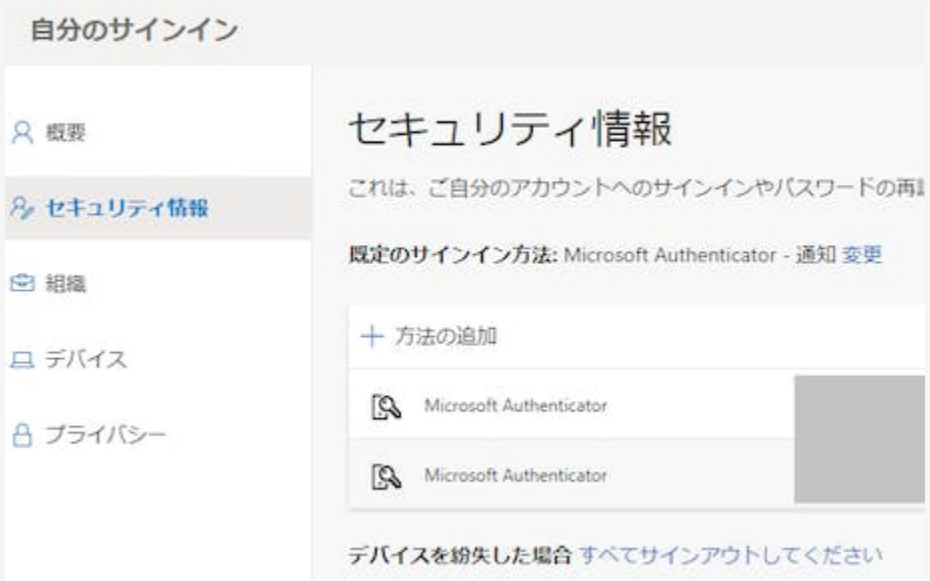
ホスト認証

エクスポートを行ってもホスト認証で証明書が使われるようには設定されない。VM 側の `/etc/ssh/ssd_config` 等を確認した感じでは証明書対応は Azure 実装(なのかな)のユーザー認証用のもよう。

```
AuthorizedKeysCommand /usr/sbin/aad_certhandler %u %k
AuthorizedKeysCommandUser root
```

切断

- 通常の `exit` などで切断できる
- 「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」を選択しても接続されたまま
  - Azure CLI はサインアウトされる



その他

所感

最初は「設定のエクスポート？ファイルの管理とか面倒そう」と思っていたのだが、シンプルに使えそうな印象になった。

- コンテナを開始てして `az login` (電話によるサインイン等も利用可能)
- 通常の SSH は `az ssh vm`
- SCP などを使う場合は `az ssh config` で設定をエクスポート(証明書は短期間だけ有効)
- `az logout` してコンテナを終了すれば認証情報は削除される