Azureテナント移行について

前提として）

ソフトバンク経由でテナントをイチから構築すれば、ディスカウントを受けられる。

すでに 2 つテナントを持っているが、これはソフトバンクによるディスカウントの対象にならない。

したがって、サーバをもう一つのテナントに移動させても、ディスカウントは得られない。

現状）

テナントA（systemfrontier-mgmt）

テナントB（frontier-mgmt.com）＝　E 5 ライセンスとセットのテナント

テナントAにADサーバがあり、セカンダリのADがオンプレにある状況

同じテナントにある他のAzureVMは、このADが管理するドメインに参加している

AIに質問して、わかったことまとめ

①ADサーバのプライマリとセカンダリを異なるテナントに配置することは現実的ではない。可能にする方法はあるが、MSのサポートがなく非推奨となっている。

（※「Vnetピアリング」という設定を行えば、可能。）

②ADサーバがあるテナントとは異なるテナントにあるAzureVM（例えばskyseaのサーバ）をこのADサーバにドメイン参加させることは可能だが、ハードルが高い。

（※「Vnetピアリング」という設定を行えば、可能。）

③2016→2025へのアップグレードは、新規構築→データ移行のほうがおすすめ

（※それ以外の方法としては、ISOイメージを別に取得してきて、それをAzureにアップロードしてマウントしてアップグレードするという「インプレースアップグレード」という方法などがある）

④AzureVPNをいまのテナントAで有効にする場合は、P1ライセンスを購入する必要がある。ExpressRouteを廃止しても、コスト削減幅は小さい。

今後の選択肢として

まずは、2016サーバのアップグレードにだけ、フォーカスする、というのはどうか？

①テナントAにあるADサーバ（プライマリ）と、テナントBにあるADサーバ（セカンダリ）で、一つのドメインを管理できるか

「プライマリDCとセカンダリDCを異なる Azure テナントに配置して、1つのADドメインを構成する」ことは、Microsoft がサポートしていません。**

理由を、公式情報に基づきながら整理して説明します。

■ なぜできないのか（技術・サポート両面の理由）

① Azure テナントは完全に独立した ID／管理境界

Azure の公式ドキュメントでは、**テナントをまたいだ形でのリソース移動・管理はサポート外**であると明記されています。

特に AD DS のような常時レプリケーションが必要なものは、テナント境界での分離と相容れません。

[c-sharpcorner.com]

② 1つのフォレストは“統一された信頼ネットワーク”を前提として構築される

ドメインコントローラー（DC）は 1 つのフォレストの中で

- スキーマ
- コンフィグレーション
- グローバルカタログ
- ドメインレプリケーション

を共有します。

これは **同一の管理境界・信頼境界の中に DC を置く**ことを前提とした仕組みです。

Azure テナントが違うと

- RBAC
- サブスクリプション所有者
- ネットワーク制御
- セキュリティポリシー
- VM / VNet の権限

すべてが別管理となるため、**“統一された AD フォレスト”としての前提を満たせません。**

③ Azure AD Connect やマルチテナント同期は DC の複製ではない

Azure AD Connect のマルチテナント同期は

オンプレAD → 複数Azureテナントへユーザー同期する“だけ”であり、

“DCをテナントに分散して冗長構成にする”ような機能ではありません。

[docs.azure.cn]

つまり、**同期とレプリケーションは全く別物**です。

■「技術的にネットワークを繋げれば動くのでは？」について

Azure には **クロステナント VNet ピアリング**が存在しており、異なるテナント間の仮想ネットワークをつなぐこと自体は可能です。

[cambaysolutions.com]

そのため、通信要件をすべて満たせば **DC 間のレプリケーションが動作"する可能性"**はあります。

しかし、これは **Microsoft のサポート対象外**であり、

- 障害時にサポート不可
- セキュリティ／RBAC管理の分離
- VNet・NSG 管理者がテナントごとに異なり構成ズレのリスク
- 変更管理が複雑化
- DR時の切り戻しが複雑
- 監査・コンプライアンス上の問題

など、企業システムとしては現実的ではありません。

②　テナントAにあるAzureVMをテナントBに移行して、このVMをテナントAにあるADにドメイン参加させることはできる？

結論から言うと――

✅ **できます。

テナントAのオンプレAD／Azure内ADドメインに、テナントBのVMを参加（ドメイン参加）させることは可能です。**

ただし、**AzureテナントはAD DS（ドメイン）の境界とは無関係** なので、

「必要なネットワーク接続が確立されていること」が唯一のポイントです。

■ Microsoft公式情報に基づくポイント

Azure VM がドメイン参加できる条件は **“ドメインコントローラーに通信できること”** だけです。

Azure AD（Entra ID）テナントの境界は、この通信要件に影響しません。

✔️ 前提：テナントとドメインは完全に別物

今回のケース：

- **テナントA**
  - AD DS（ドメイン）を持っている
- **テナントB**
  - ここに作った Azure VM を、テナントAのADドメインに参加させたい

→ **Azure ADテナントが違っても問題なし**です。

■ 必要条件（重要）

Microsoft の Azure Files ネットワーク要件にあるように、ネットワークの疎通が必要という概念が説明されています。

つまり、Azure VM が AD にアクセスするためには、

✔️ 1. テナントAのドメインコントローラーとテナントBのVMがIPレベルで通信できること

具体的には下記のいずれかのネットワーク接続が必要：

● Azure クロステナント VNet ピアリング（公式に可能）

異なるテナント間でも VNet ピアリングは利用可能。

■ クロステナントVNetピアリングは2018年から利用可能と情報あり

[blog.sebas...laesson.se]

● VPN接続（Site-to-Site / Point-to-Site）

● ExpressRoute（施設間専用線）

✔️ 2. AD DS が必要とするポートが通信可能であること

（例：LDAP 389、Kerberos 88、DNS 53、SMB 445、RPC 135 + 動的RPC等）

✔️ 3. DNS の設定が正しいこと

- テナントB側VMの DNS を

テナントAのDC（DNSサーバ）に向ける

- Azure既定の DNS (168.63.129.16) ではドメイン参加できません

■ 実際に Microsoft が述べている “本質” 部分

Azure や AD の公式情報では、

ドメイン参加の可否は “ネットワークの到達性” のみが条件 と明記されています（ネットワーク条件の重要性が強調されている）。

（Azure Files のSMBアクセスもネットワーク条件が要という記述）
[learn.microsoft.com]

■ よくある誤解

❌ Azureテナントが違うとVMはドメイン参加できない

→ 関係ありません

Azure ADテナントとAD DSドメインは全く別の技術です。

❌ テナントBのVMはテナントAのリソースにアクセスできない

→ ネットワーク接続を作れば可能

■ 図でイメージすると：

Plain Text

```
[テナントA]                                [テナントB]
  ┌──────────────┐                          ┌──────────────┐
  │  VNet A      │                            │   VNet B     │
  │   + DC(AD DS)│ ◀──ピアリング──▶ │  + Azure VM  │
  └──────────────┘                          └──────────────┘

→ VNet同士が繋がれば、VMは普通に domain join 可能
```