ADに依存しないクラスタの世界へ(前半)

On-PremからAzure Localまで

胡田 昌彦（日本ビジネスシステムズ株式会社 / Microsoft MVP）

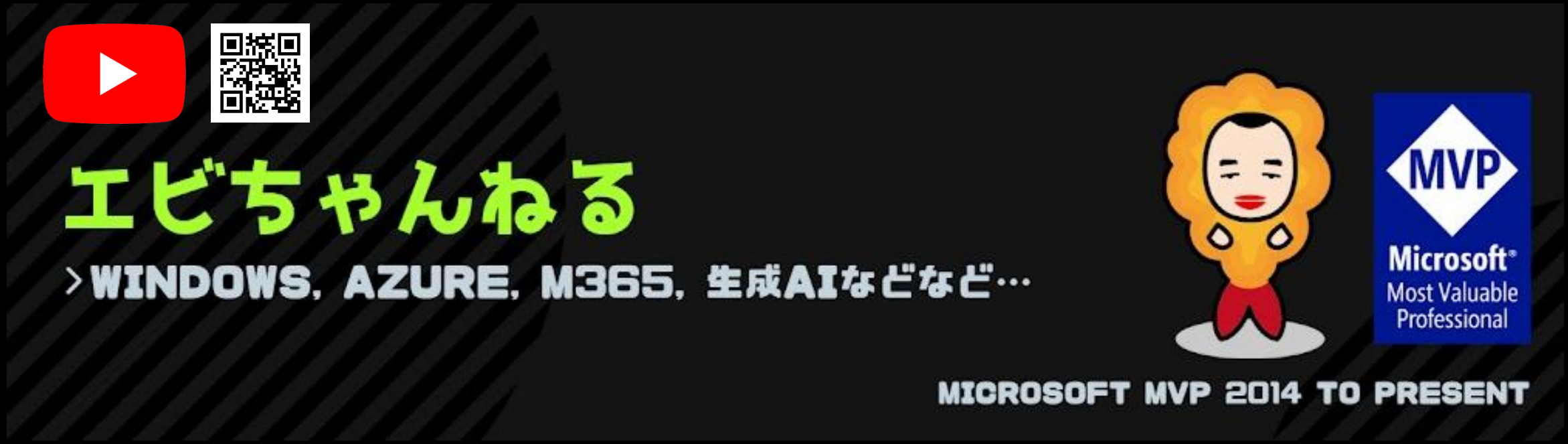
HCCJP 第67回勉強会
2025年11月14日

自己紹介

日本ビジネスシステムズ株式会社
胡田 昌彦(えびすだ まさひこ)

Youtube https://youtube.com/@ebibibi

こんな方にオススメ!
- ✓ 企業の情報システム部で働く方
- ✓ 一般ユーザーだけど、コンピューターに興味があって、もっと詳しくなりたい方
- ✓ Windows, Azure, M365等のMicrosoft関連技術に興味がある方



チャンネル登録よろしくお願いします!

前半のアジェンダ

Windows フェールオーバークラスタのAD非依存構成の進化

1. **フェールオーバークラスタの基本**
2. **従来のAD依存構成**
3. **Windows Server 2012 R2**: AD-detached
4. **Windows Server 2016**: ワークグループクラスター
5. **Windows Server 2025**: Hyper-V完全サポート
6. **ADの役割と代替手段**
7. **まとめと展望**

⏱️ 約20分

フェールオーバークラスタの基本

高可用性を実現する仕組み

- **複数のノード**を連携させてサービスを提供
- 障害時に**自動フェールオーバー**でサービス継続
- **ハートビート監視**で問題を検知
- サーバー障害時もサービス停止を最小限に

代表的な用途

- Hyper-V仮想マシンの高可用性
- SQL Server (FCI / Always On AG)
- ファイルサーバー

従来のAD依存構成

Active Directoryが前提だった時代

ADが担っていた重要な役割

- **クラスター名オブジェクト (CNO)** をAD上で管理
- **CNOが仮想コンピューターオブジェクト (VCO)** をAD上で作成
- **ノード間認証**: Kerberos認証で安全な通信
- **DNS連携**: 動的DNS更新で名前解決
- **権限管理**: ドメイングループでアクセス制御
- **管理の容易性**: GPOによる統一設定

問題点: 小規模環境やエッジではAD構築が負担に

Windows Server 2012 R2: AD-detached

初めてのAD非依存への試み

主な特徴

- **クラスター名オブジェクト (CNO)を作成しない**構成が可能
- New-Cluster -AdministrativeAccessPoint Dns で構成
- DNS名だけで管理するクラスター
- ノード間通信 → Kerberos認証
- クラスタ名に対するクライアント認証 → NTLM認証

制約

- ✅ ノードは依然として**ADドメイン参加が必要**
- ✅ 主に**SQL Server Always On AG**向けにサポート
- ❌ Hyper-Vやファイルサーバーは非推奨　→　SMB / LiveMigrationでKerberosが使えないから

位置づけ: 限定的だが重要な第一歩

Windows Server 2016: ワークグループクラスター登場

真のAD非依存クラスターへ

画期的な進化

- **ドメイン非参加ノード**だけでクラスター構成が可能に
- ワークグループ環境でも高可用性を実現(※マルチドメイン構成も可能)

主な要件

- **ノード間認証**: 同一のローカル管理者アカウント + NTLM
- **DNS**: 手動でクラスター名を登録
- **クォーラム**: Cloud Witness または Disk Witness
  - ファイル共有Witnessは非サポート

Windows Server 2016の制約

サポート範囲が限定的

✅ サポートされるワークロード

- **SQL Server Always On 可用性グループ (AG)**
  - SQL Server 2016以降で対応

❌ 制約のあるワークロード

- **Hyper-V**: 構成は可能だが…
  - ライブマイグレーション不可（クイックマイグレーションのみ）
  - ダウンタイムが発生するため実用性に欠ける
- **ファイルサーバー**: 認証の問題で非推奨
- **CAU (クラスター対応更新)**: 使用不可

結論: 主にSQL AG向けの機能として位置づけ

Windows Server 2025: 大きな進化

Hyper-V完全サポートが実現！

🚀 ついに実現した機能

- ワークグループクラスターで**Hyper-Vが正式サポート**
- **ライブマイグレーション**が可能に
- ダウンタイムなしでVMを移行

なぜ可能になったのか？

- **証明書ベース認証**の導入
- NTLMからの脱却（Microsoftは2024年にNTLM非推奨化）
- より安全な相互認証の実現

認証技術の進化

Kerberos → NTLM → 証明書認証

世代	認証方式	特徴
従来（AD環境）	Kerberos	安全・スケーラブル・AD必須
2016〜2022	NTLM	ドメイン不要・セキュリティ上の懸念
2025〜	証明書ベース	安全・AD不要・相互認証

証明書ベース認証の仕組み

- 各ノードへのローカルアカウント(同一ID、パスワード)の作成
- 各ノードに**X.509証明書**をインストール
- 相互に証明書を信頼させる設定
- TLS相互認証でノード間通信を保護
- 自己署名証明書またはCA発行証明書を使用

Windows Server 2025のワークグループクラスターのサポート範囲

何ができて、何ができない？

✅ 正式サポート

- **Hyper-V仮想マシン**（ライブマイグレーション含む）
- **SQL Server Always On AG**

🔺 引き続き~~サポートはするが非推奨~~ or 非サポート(ドキュメントに揺れあり)

- **ファイルサーバー**
  - Kerberos認証が必要なため
  - NTLM廃止の流れもあり

❌ 引き続き非サポート

- **SQL Server FCI (フェールオーバークラスタインスタンス)**

参考：Windows Server でワークグループ クラスターを作成する | Microsoft Learn https://learn.microsoft.com/ja-jp/windows-server/failover-clustering/create-workgroup-cluster?tabs=desktop#cluster-workloads

Azure LocalのADレス構成

クラウド統合でさらに進化

Windows Serverのワークグループクラスター + Azure Key Vault

後半パートでMKI松本さんから！

背景にある管理機能の強化

Azure Arc連携

- ドメインレスでも集中管理が可能
- ポリシー適用・監視・タグ付けをクラウドから

ただし、超推されているわけでもないので注意が必要

ADが担っていた役割とその代替え（まとめ）

Active Directoryは何をしていたのか？
その役割をどう置き換えるか？

役割	内容	ADレス環境での代替え手段
1. ID管理	CNO/VCOでクラスター名・役割名を管理	ローカルアカウント / DNSで管理
2. 認証	Kerberosでノード間・クライアント認証	証明書ベース認証(2025～) / NTLM (※廃止の方向)
3. DNS連携	動的DNS更新で名前解決を自動化	手動登録 / スクリプト /その他
4. 権限管理	ドメインアカウント、グループでアクセス制御	ローカルセキュリティ設定等
5. 管理性	GPO, 一元管理による運用の簡素化	スクリプト / Azure Arc / Azure Policy

メリット・デメリット

ADレス構成の評価

✅ メリット

- ドメインコントローラーの構築・維持コスト削減
- 小規模・エッジ環境での迅速な展開
- インフラのシンプル化

⚠️ デメリット

- 手動設定が増加（DNS、証明書など）
- 証明書管理の知識が必要
- ファイルサーバーなど一部ワークロードは依然AD必須
- 運用者にとって馴染みが薄い
- ツールの動作にも各種特別設定が必要なケースが多い

- クラウド時代の「AD非依存」型の仕組みは色々と増えてきている！
- Windows Serverを使う→ADも必要→DCが複数台必要… が減ってきている！
- NTLM廃止の流れが追い風のような、向かい風のような…
- ローカルのKerberos認証が登場すると景色がまたガラッと変わりそう。localKDCサービスは入ってるがまだ動かない？
- とはいえ、ADはまだまだこれからも…。

参考資料

公式ドキュメント

- フェールオーバー クラスタリング | Microsoft Learn
  https://learn.microsoft.com/ja-jp/windows-server/failover-clustering/failover-clustering-overview
- Windows Server でワークグループ クラスターを作成する | Microsoft Learn
  https://learn.microsoft.com/ja-jp/windows-server/failover-clustering/create-workgroup-cluster?tabs=desktop
- Windows Server のワークグループ クラスターを使用してライブ マイグレーションを行う | Microsoft Learn
  https://learn.microsoft.com/ja-jp/windows-server/virtualization/hyper-v/manage/live-migration-workgroup-cluster?tabs=powershell

技術ブログ

- Windows Server 2025 Hyper-V Workgroup Cluster with Certificate-Based Authentication | Microsoft Community Hub
  https://techcommunity.microsoft.com/blog/itopstalkblog/windows-server-2025-hyper-v-workgroup-cluster-with-certificate-based-authenticat/4428783

ありがとうございました！

質問・コメントをお待ちしています