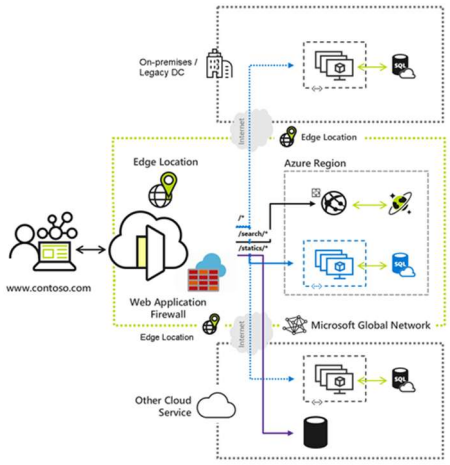
Tích Hợp AD DS Trên Azure IaaS – Cách Mở Rộng Directory Một Cách Linh Hoạt



Khi các doanh nghiệp bắt đầu hành trình chuyển đổi số và mở rộng hạ tầng hybrid cloud, một trong những câu hỏi thường gặp là: "Có nên đặt Domain Controller lên Azure hay không?". Câu trả lời là hoàn toàn nên, và dưới đây là lý do:

Tại Sao Nên Đặt Domain Controller AD DS Trên Azure VM?

Việc triển khai Domain Controller (DC) trên một máy ảo Azure IaaS mang lại nhiều lợi ích cho hạ tầng hiện hữu của bạn:

- Tăng tính sẵn sàng: AD DS trong Azure hoạt động như một điểm dự phòng cho hệ thống AD on-premises, đảm bảo tính liên tục khi có sự cố tại site chính.
- Cải thiện hiệu năng xác thực: Đối với workload chạy trên Azure, DC đặt cùng khu vực sẽ xử lý các yêu cầu xác thực nhanh hơn, giảm độ trễ.
- Mở rộng truy cập toàn cầu: Khi người dùng hoặc chi nhánh toàn cầu truy cập dịch vụ, việc có AD trên Azure giúp rút ngắn đường truyền về trung tâm dữ liệu, đồng thời hỗ trợ kiến trúc hybrid.

Các Kịch Bản Triển Khai AD DS Trên Azure

Bạn có thể triển khai dịch vụ AD DS trên Azure theo hai kiểu chính:

1. AD DS chỉ chạy trên Azure

- Một Domain Controller (hoặc nhiều) được cài đặt trực tiếp trên các Azure VM, độc lập với hệ thống on-premises.
- Thích hợp cho mô hình mới, không phụ thuộc AD hiện có.

2. AD DS vừa chạy on-premises vừa trên Azure
- Triển khai hỗn hợp để duy trì hệ thống AD hiện tại nhưng mở rộng sang Azure.
- Triển khai thêm Domain Controller: Cài đặt thêm một Domain Controller (thành viên) vào Azure để đồng bộ và phân tải xác thực.
- Triển khai Forest hoặc Domain riêng biệt có quan hệ trust: Tạo một forest/domain độc lập trên Azure, thiết lập mối quan hệ tin cậy (trust) với forest on-premises.

Ví Dụ Thực Tế

Giả sử bạn đang chạy ứng dụng ERP trên một Azure VM, và người dùng nội bộ truy cập từ nhiều vị trí toàn cầu. Nếu hệ thống AD chỉ đặt tại trung tâm dữ liệu Việt Nam, mọi xác thực từ Mỹ hoặc châu Âu sẽ bị chậm trễ. Bằng cách thêm một Domain Controller tại vùng Azure gần người dùng, bạn cải thiện đáng kể hiệu suất xác thực và đảm bảo độ ổn định.

Lời Khuyên Từ Chuyên Gia

- Hãy đảm bảo Domain Controller trên Azure được cấu hình replication phù hợp và luôn backup định kỳ.
- Kết nối site-to-site VPN hoặc ExpressRoute nên được thiết lập trước khi triển khai AD trên Azure.
- Đừng quên cấu hình DNS chuẩn để Azure VM có thể “tìm thấy” domain.

Nếu bạn đang là quản trị viên AD hoặc làm việc với hạ tầng hybrid cloud, hãy bắt đầu xây dựng mô hình AD trên Azure ngay từ hôm nay

Triển khai Domain Controller trên Azure VM – Những điều cần lưu ý

Việc triển khai Domain Controller (DC) của Active Directory Domain Services (AD DS) trong môi trường Azure VM là một phần quan trọng trong chiến lược lai (hybrid strategy) hoặc khi xây dựng hệ thống Active Directory hoàn toàn trên nền tảng cloud. Tuy nhiên, nếu triển khai không đúng cách, bạn có thể đối mặt với các sự cố về đồng bộ, bảo mật, hiệu suất hoặc khả năng phục hồi.

1. Khuyến nghị về mạng (Network Recommendations)

Đảm bảo rằng bạn đã thiết kế đúng địa chỉ IP tĩnh, DNS forwarders, và có một Virtual Network (VNet) đủ chuẩn để các máy DC hoạt động ổn định. Tránh gán IP động (Dynamic IP) vì sẽ làm hỏng cấu trúc AD.

2. Kết nối liên site (Inter-site connectivity)

Nếu bạn đang mở rộng domain từ on-premises lên Azure, cần đảm bảo có kết nối VPN hoặc ExpressRoute ổn định và có băng thông đủ để hỗ trợ quá trình replication giữa các site AD.

3. Cấu hình Site AD (Active Directory Sites)

Cấu hình đúng các AD Sites và Subnets để hệ thống hiểu được ranh giới mạng logic và điều hướng truy vấn cũng như replication chính xác giữa các DC.

4. Mối quan hệ tin cậy (Trust Relationship)

Nếu triển khai Domain Controller trong môi trường đa forest hoặc đa domain, bạn cần xác định rõ các mối quan hệ trust (one-way hoặc two-way) giữa các miền, và đảm bảo các cổng mạng tương ứng được mở.

5. Read-Only Domain Controllers (RODCs)

Xem xét sử dụng RODC nếu bạn triển khai DC ở chi nhánh hoặc khu vực mà bạn không kiểm soát được hoàn toàn mặt vật lý hoặc bảo mật.

6. Vai trò FSMO và Global Catalog

Đừng đặt tất cả FSMO roles lên các máy DC trong Azure mà không phân tích kỹ. Cần lên kế hoạch cụ thể cho việc phân phối vai trò như Schema Master, RID Master, Infrastructure Master, và Global Catalog placement để đảm bảo tính khả dụng và hiệu suất.

7. Tính sẵn sàng (Availability)

Hãy triển khai ít nhất hai domain controllers trong Azure, ở các Availability Zone khác nhau nếu có thể, để giảm rủi ro đơn điểm lỗi (SPOF). Sử dụng Azure Availability Sets hoặc Availability Zones để nâng cao độ tin cậy.

8. Sao lưu và phục hồi (Backup and Restore)

Triển khai giải pháp sao lưu VSS-aware như Azure Backup để đảm bảo có thể phục hồi dữ liệu AD khi có sự cố. Không nên chỉ dựa vào snapshot.

9. Quản lý (Management)

Sử dụng các công cụ như Azure Bastion, Just-in-Time Access (JIT) và Privileged Identity Management (PIM) để truy cập và quản lý DC an toàn.

10. Giám sát (Monitoring)

Tích hợp với Azure Monitor, Log Analytics, hoặc Microsoft Defender for Identity để phát hiện các hành vi đáng ngờ như brute force, tài khoản bị xâm nhập, hoặc các sự kiện replication lỗi.

TÓM TẮT BÀI 2

Triển khai AD Domain Controller trên Azure không đơn giản chỉ là tạo một VM và dcpromo. Nó yêu cầu tư duy hệ thống, bảo mật, và tích hợp hybrid chuẩn chỉ. Trong bài tiếp theo, chúng ta sẽ đi sâu vào các bước cài đặt và cấu hình cụ thể trên Azure VM.

Triển khai Domain Controller AD DS trên Azure VM - Cấu hình Trust

Tùy chọn cấu hình Trust:

Kịch bản triển khai:
1. Người dùng On-prem cần truy cập tài nguyên trên Azure, nhưng không ngược lại
  - Trust phía On-premises: One-way, incoming
  - Trust phía Azure: One-way, outgoing

2. Người dùng trên Azure cần truy cập tài nguyên tại On-premises, nhưng không ngược lại
  - Trust phía On-premises: One-way, outgoing
  - Trust phía Azure: One-way, incoming

3. Người dùng ở cả Azure và On-prem đều cần truy cập tài nguyên lẫn nhau
  - Trust phía On-premises: Two-way, incoming and outgoing
  - Trust phía Azure: Two-way, incoming and outgoing

Trong hạ tầng Hybrid, việc thiết lập mối quan hệ Trust giữa domain controller tại Azure và On-prem là yếu tố quyết định trải nghiệm truy cập và xác thực của người dùng.

Dưới đây là các kịch bản điển hình:

1. Người dùng tại On-prem cần truy cập tài nguyên trên Azure (ví dụ như ứng dụng nội bộ, máy chủ file, VM chạy trên Azure):
  - Cấu hình trust tại On-prem: One-way, incoming (cho phép On-prem nhận xác thực từ Azure)
  - Cấu hình trust tại Azure: One-way, outgoing (Azure gửi yêu cầu xác thực sang On-prem)

2. Người dùng ở Azure (VDI, App Services, hoặc nhân viên làm việc từ xa) cần truy cập tài nguyên nội bộ tại On-prem (như cơ sở dữ liệu, ERP):
  - Cấu hình trust tại On-prem: One-way, outgoing
  - Cấu hình trust tại Azure: One-way, incoming

3. Kịch bản phổ biến trong doanh nghiệp: Cả hai bên đều cần truy cập lẫn nhau (hybrid full-access):
  - Cấu hình Two-way trust trên cả Azure và On-prem, cho phép xác thực hai chiều.

Lưu ý quan trọng:

- Trust không tự động mở port! Đảm bảo bạn đã mở đúng các cổng RPC/LDAP/SMB qua VPN hoặc ExpressRoute giữa hai bên.
- Kiểm tra phân quyền SID filtering và selective authentication nếu bạn muốn kiểm soát mức truy cập chi tiết hơn.
- Môi trường test nên được thiết lập trước để kiểm chứng trước khi áp dụng production.

Ví dụ thực tế:

Công ty A triển khai hệ thống ERP ở On-premises nhưng đồng thời mở rộng hệ thống CRM mới lên Azure. Nhân viên cần truy cập chéo lẫn nhau. Vậy giải pháp là gì?
→ Thiết lập Two-way trust, cấu hình domain controller replica trên Azure, và đảm bảo route mạng đã thông suốt giữa hai vùng.