Azure Storage – Hiểu đúng từ đầu để triển khai hiệu quả VM & Lưu trữ

Trong thế giới cloud, việc chọn đúng loại storage không chỉ giúp tiết kiệm chi phí mà còn đảm bảo hiệu năng và độ bền dữ liệu. Nếu bạn đang triển khai VM, backup hoặc chia sẻ file trên Azure, thì đây là 2 khái niệm bạn phải nắm: Managed Disks và Azure Files.

1. Azure Managed Disks – "Ổ cứng" tiêu chuẩn dành cho VM

Azure Managed Disks là dịch vụ lưu trữ block được quản lý hoàn toàn, chủ yếu dùng để làm đĩa hệ điều hành và dữ liệu cho VM. Những điểm mạnh mà bạn cần nhớ:

- Độ bền cao và luôn sẵn sàng: Không cần lo về lỗi đĩa, Microsoft đã đảm bảo HA.
- Triển khai VM cực nhanh và có thể mở rộng dễ dàng.
- Tích hợp với Availability Sets/Zones giúp xây dựng hệ thống dự phòng chuẩn SLA.
- Tương thích Azure Backup cho giải pháp sao lưu tự động.
- Kiểm soát truy cập chi tiết theo RBAC.
- Hỗ trợ upload VHD để migrate từ môi trường on-premises.
- Mã hóa dữ liệu, hỗ trợ Snapshot và tạo Image để deploy hàng loạt VM.

Ví dụ thực tế: Bạn có thể tạo một Managed Disk từ snapshot rồi gắn vào một VM mới để restore dữ liệu sau khi VM cũ bị lỗi.

2. Azure Files – Chia sẻ file giữa nhiều máy, nhiều nền tảng

Khác với Managed Disks vốn dành cho từng VM cụ thể, Azure Files là dịch vụ lưu trữ file theo dạng chia sẻ (file share) sử dụng SMB protocol – quen thuộc với anh em IT dùng Windows Server.

- Tạo file share trên cloud giống như thư mục mạng nội bộ.
- Chia sẻ đa nền tảng: Windows, Linux, macOS đều dùng được.
- Dễ dàng gắn vào ứng dụng, server hoặc thậm chí mount vào container.

Ví dụ thực tế: Một hệ thống có nhiều VM cần truy cập cùng một bộ dữ liệu (như ảnh, log, config), bạn chỉ cần tạo một Azure File Share và mount vào từng VM.

Lời khuyên cho người mới

Nếu bạn cần lưu trữ đĩa hệ điều hành hoặc đĩa dữ liệu cho VM → chọn Azure Managed Disks.

Nếu bạn cần chia sẻ file dùng chung giữa nhiều hệ thống → chọn Azure Files.

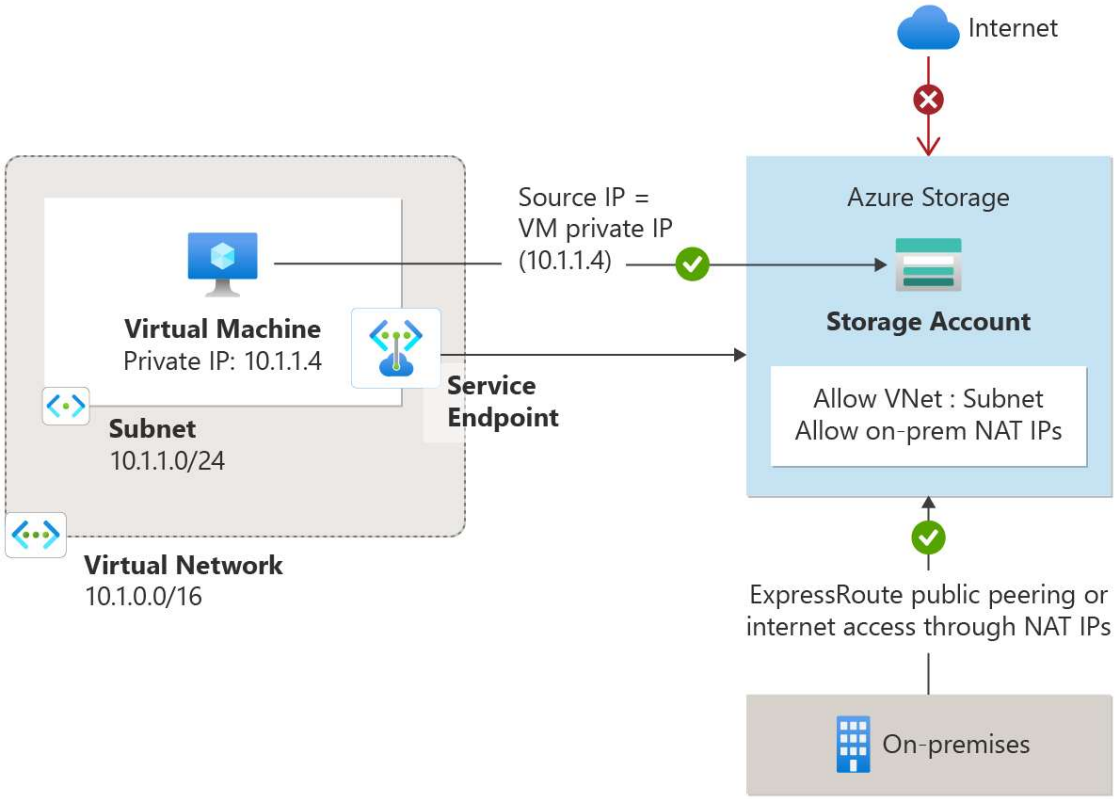
Bạn nào đang học MCSA hoặc triển khai môi trường hybrid (on-prem + cloud) thì nên lab thử cả 2 dạng này để hiểu rõ cách chúng hoạt động. Có thể bắt đầu với Azure Free Tier!

Chúc các bạn học tốt và triển khai Azure Storage vững chắc!

Giải Thích Azure Virtual Network

[GIẢI THÍCH NHANH] Azure Networking – Mạng Ảo Là Gì Và Tại Sao Nó Quan Trọng Trong Azure?

Nếu bạn đang làm việc với hạ tầng Azure hoặc mới bắt đầu với MCSA, Azure, AWS – thì bạn không thể bỏ qua khái niệm “Virtual Network”. Đây chính là "bộ não giao tiếp nội bộ" giữa các máy ảo và dịch vụ trong Azure!



1. Virtual Network trong Azure là gì?

Virtual Network (VNet) trong Azure cung cấp khả năng kết nối các tài nguyên (VM, App Service, Database...) trong cùng một không gian địa chỉ IP. Điều này cho phép bạn tạo ra một môi trường mạng riêng biệt tương tự như một mạng nội bộ trong trung tâm dữ liệu.

2. Địa chỉ IP trong VNet gồm những loại nào?

Azure hỗ trợ hai loại địa chỉ IP:
- RFC 1918 (Private IP): Đây là các địa chỉ IP nội bộ như 10.x.x.x, 172.16.x.x, 192.168.x.x.

Chúng không thể truy cập trực tiếp từ Internet.
- Non-RFC 1918 (Public IP): Đây là các IP công cộng, có thể truy cập từ Internet. Trong Azure, bạn sẽ cấu hình Public IP này khi cần truy cập VM từ ngoài.

Ví dụ thực tế:
Bạn tạo một VM chạy web server trong Azure. Khi dùng Private IP, chỉ các VM khác trong cùng VNet hoặc được peering mới truy cập được. Muốn người dùng truy cập từ trình duyệt Internet? Bạn cần gán thêm một Public IP!

3. Ranh giới logic của VNet là gì?

Mỗi VNet tạo thành một biên giới logic bằng không gian IP riêng biệt. Điều này giúp bạn cô lập và kiểm soát kết nối giữa các tài nguyên, hỗ trợ xây dựng mô hình bảo mật theo Zero Trust.

4. Tại sao kỹ sư hệ thống cần hiểu rõ VNet?

- Hiểu rõ địa chỉ IP giúp tránh xung đột khi kết nối site-to-site.
- Giúp triển khai mô hình mạng nhiều lớp, phân đoạn dịch vụ (microsegmentation).
- Quản lý và gán địa chỉ IP hiệu quả, bảo mật hơn.
- Là nền tảng khi học tiếp VNet Peering, NSG, VPN Gateway, Azure Firewall, Application Gateway...

Lời khuyên thực chiến cho anh em mới vào nghề:

Khi làm lab hoặc triển khai thực tế, hãy luôn vạch rõ sơ đồ IP, ghi lại các dải subnet bạn dùng cho từng lớp: frontend, backend, database... Điều này giúp bạn dễ quản lý, dễ debug, và mở rộng về sau. Anh em trong cộng đồng MCSA-Azure-AWS của VnPro nếu đang học CCNA Cloud, AZ-104, hay đang chuyển hướng sang Cloud Engineer – nhớ bookmark loạt bài này để hiểu rõ kiến trúc mạng Azure từ gốc nhé!

Azure Networking Cơ Bản – Kiến Thức Không Thể Bỏ Qua Cho Người Mới Bắt Đầu Cloud!

Khi mới làm quen với hạ tầng đám mây Azure, rất nhiều anh em kỹ sư hạ tầng hay gặp câu hỏi: "Mạng nội bộ trong Azure hoạt động như thế nào?", "Sử dụng IP gì?", "VM kết nối mạng ra sao?". Bài viết này sẽ giúp bạn hiểu được 2 phần kiến thức quan trọng trong thiết kế mạng Azure: IP nội bộ (RFC 1918) và cấu hình network interface cho máy ảo VM.

RFC 1918 IP addresses

Các địa chỉ lớp mạng riêng cho Azure VM

IP address subnet	Host IP address range
10.0.0.0/8	10.0.0.1 - 10.255.255.254
172.16.0.0/12	172.16.0.1 - 172.31.255.254
192.168.0.0/16	192.168.0.1 - 192.168.255.254

1. Địa chỉ IP riêng – RFC 1918 là gì?

Azure sử dụng địa chỉ IP riêng (Private IP) cho các mạng ảo (Virtual Network - VNet) của bạn. Đây là các IP không định tuyến được trên Internet, thường dùng trong nội bộ doanh nghiệp hoặc hệ thống đám mây. Theo chuẩn RFC 1918, có ba dải IP được phép sử dụng làm IP riêng như sau:

- 10.0.0.0/8 → Dải host: 10.0.0.1 – 10.255.255.254

- 172.16.0.0/12 → Dải host: 172.16.0.1 – 172.31.255.254

- 192.168.0.0/16 → Dải host: 192.168.0.1 – 192.168.255.254

Ví dụ:

Khi tạo một VNet trong Azure, bạn có thể dùng subnet 10.10.0.0/24 để cấp phát IP cho các VM.

2. Network Interface trong Azure hoạt động như thế nào?

Trong Azure, mỗi máy ảo (VM) cần ít nhất 1 network interface để kết nối với mạng. Dưới đây là các nguyên tắc quan trọng mà bạn cần nắm:

- Mỗi VM bắt buộc phải có ít nhất 1 network interface (có thể có nhiều hơn).

- Network interface này phải cùng location và subscription với VM.

- Network interface cũng phải được kết nối đến một Virtual Network (VNet) trong cùng location/subscription.

- Azure hỗ trợ gán IP tĩnh hoặc IP động, cả private và public IP cho network interface.

- Chi phí băng thông được tính dựa trên lưu lượng ra ngoài (egress).

- Tổng băng thông được cấp cho VM là tổng tất cả lưu lượng egress qua các interface gắn vào VM đó.

Ví dụ thực tế:

VM WebServer1 có 2 interface: 1 interface private gán IP động trong VNet 10.10.0.0/24, 1 interface public có IP tĩnh để người dùng truy cập. Azure sẽ tính băng thông outbound của cả 2 interface này khi tính chi phí.

Kết luận

Việc hiểu rõ về IP riêng (RFC 1918) và cách hoạt động của network interface trong Azure là bước khởi đầu không thể thiếu nếu bạn đang học MCSA/Azure, triển khai hạ tầng trên cloud, hoặc chuẩn bị thi các chứng chỉ như AZ-104, AZ-700.

Hãy dành thời gian vẽ sơ đồ mạng VNet của bạn, chia subnet thông minh và lên kế hoạch cấp phát IP theo chuẩn RFC 1918. Đây chính là nền tảng cho mọi dịch vụ mạng sau này như: Load Balancer, NSG, VPN Gateway, Peering...

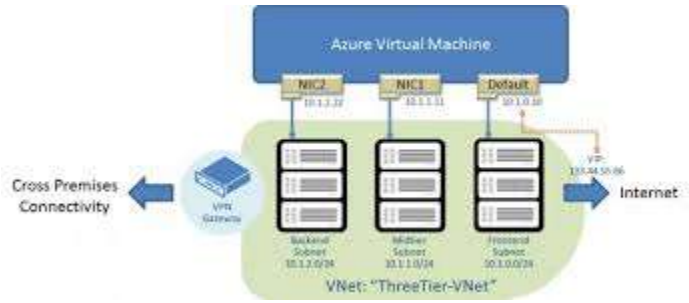
#AzureNetworking #RFC1918 #VirtualNetwork #AzureVM #VNProCloud #MCSA #AZ104 #AZ700

Hiểu Về Network Interface trong Azure VM – Kiến Thức Mỗi Kỹ Sư Cloud Phải Biết!

Trong hành trình làm việc với Azure, việc hiểu rõ cách thức kết nối mạng cho các máy ảo (VM) là điều bắt buộc nếu bạn muốn triển khai hạ tầng cloud đúng chuẩn và tối ưu. Một thành phần then chốt trong kết nối này chính là network interface (giao diện mạng). Vậy nó hoạt động như thế nào? Có giới hạn hay yêu cầu gì không? Bài viết dưới đây sẽ giải thích rõ cho bạn.

Network Interface là gì?

Trong Azure, network interface (NIC) là cầu nối giữa Virtual Machine (VM) và Virtual Network (VNet). Đây chính là nơi bạn gắn IP, routing, NSG (Network Security Group), và nhiều cấu hình mạng khác.



Những Điều Bạn Cần Nắm Rõ:

- - Mỗi VM bắt buộc phải có ít nhất một network interface. – Một máy ảo có thể có nhiều NIC, ví dụ trong các tình huống như cần kết nối vào nhiều subnet hoặc dùng cho tường lửa.
- - Mỗi network interface phải nằm cùng location và subscription với VM. – Điều này đảm bảo tính nhất quán và khả năng kết nối nội bộ giữa các thành phần.
- - Network interface cũng phải nằm trong một Virtual Network cùng location và subscription. – Nếu bạn có nhiều vùng (region) hoặc nhiều subscription, hãy lưu ý rằng bạn không thể "kéo dây" từ nơi này qua nơi khác nếu không có các giải pháp kết nối liên vùng.
- - Azure cung cấp địa chỉ IP tĩnh (static) hoặc động (dynamic), cả dạng private lẫn public. – Tuỳ theo nhu cầu mà bạn chọn IP dạng nào, ví dụ dịch vụ nội bộ dùng IP private tĩnh, còn Web Server có thể dùng IP public tĩnh.

- - Băng thông được tính theo chiều ra (egress) – không tính inbound! – Ví dụ: nếu bạn tải file từ VM lên Internet hoặc các region khác thì sẽ bị tính phí, còn tải về từ Internet thì không tính.
- - Băng thông gán cho VM là tổng egress của tất cả các NIC. – Nếu VM có nhiều NIC, Azure sẽ cộng tất cả lượng dữ liệu outbound của từng NIC để tính toán giới hạn băng thông.

Ví Dụ Thực Tế

Bạn có một máy ảo chạy firewall, có 2 NIC:
- NIC 1 kết nối vào subnet nội bộ (trust)
- NIC 2 kết nối ra ngoài (untrust)

Nếu tổng băng thông outbound (từ cả hai NIC) vượt quá giới hạn mà VM SKU cho phép, bạn cần nâng cấp SKU hoặc điều chỉnh kiến trúc.

Ghi Nhớ

- - Không có NIC = VM không thể giao tiếp mạng!
- - Gắn nhiều NIC nhưng chỉ tối ưu khi bạn thực sự cần chia luồng lưu lượng.
- - Luôn kiểm tra limit băng thông cho từng loại VM SKU trong Azure VM documentation.

#MCSA #Azure #VnPro #AzureNetworking #CloudInfrastructure #AzureVM #VirtualNetwork #NetworkInterface #CloudTraining #AWS #MicrosoftAzure #LearnAzure

Azure Networking – Sự thật ít ai biết về băng thông mạng Azure

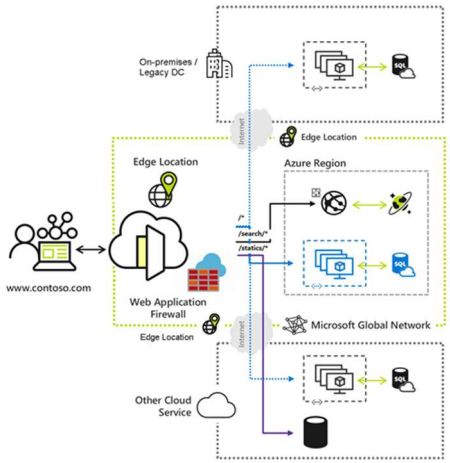
Khi triển khai hạ tầng mạng trên Azure, nhiều kỹ sư thường cho rằng có thể "tăng tốc" băng thông bằng cách thêm card mạng, bật Accelerated Networking hay thay đổi giao thức. Tuy nhiên, bạn sẽ rất ngạc nhiên khi biết rằng băng thông mạng mong đợi (Expected Network Throughput) thực chất không bị ảnh hưởng bởi các yếu tố sau:

- Số lượng Network Interface (NIC): Việc thêm nhiều NIC vào một VM không có nghĩa là bạn sẽ được cộng dồn băng thông.

- Accelerated Networking: Tính năng này giúp giảm độ trễ và tăng hiệu năng xử lý gói tin, nhưng không thay đổi giới hạn throughput mặc định của VM.

- Điểm đến của lưu lượng mạng (Traffic Destination): Dù bạn gửi dữ liệu ra Internet, nội vùng VNet hay qua peering thì băng thông vẫn phụ thuộc vào SKU của VM.

- Giao thức truyền tải (Protocol): Dùng TCP hay UDP cũng không ảnh hưởng đến mức băng thông Azure đã định sẵn cho VM.



Vậy yếu tố nào thực sự quyết định băng thông mạng Azure VM?

Câu trả lời nằm ở kích cỡ (SKU) của máy ảo Azure. Mỗi SKU định nghĩa rõ mức băng thông tối đa cho inbound và outbound traffic. Ví dụ:
- D2s_v3 có throughput khoảng 1.5 Gbps
- D8s_v3 có thể lên đến 4 Gbps
- Một số VM dòng E, F, hoặc những VM chuyên về network như Dd_v5 có thể đạt từ 10–30 Gbps nếu hỗ trợ

Bạn có thể kiểm tra chi tiết trong tài liệu Microsoft: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-machine-network-throughput

Lưu ý dành cho anh em kỹ sư:

- Đừng nhầm Accelerated Networking với việc tăng băng thông, nó chỉ giúp tăng hiệu năng xử lý bằng cách offload cho NIC vật lý (SR-IOV).

- Khi cần nâng throughput, hãy scale VM SKU lên dòng cao hơn thay vì thêm nhiều NIC hoặc "tối ưu" cấu hình không liên quan.

- Trong thiết kế hệ thống có sử dụng Azure Firewall, Load Balancer hoặc VPN Gateway, cũng cần cân nhắc kỹ throughput để tránh nghẽn cổ chai.

Kết luận dành cho cộng đồng:

Hiểu đúng về giới hạn throughput trên Azure không chỉ giúp bạn tránh sai lầm trong thiết kế mà còn tối ưu chi phí và hiệu năng thực tế. Nếu bạn đang xây dựng hạ tầng Hybrid, cần transfer data lớn giữa các region hoặc về on-prem, hãy ưu tiên chọn đúng VM SKU thay vì hy vọng "tăng tốc bằng mẹo".

Hãy chia sẻ bài viết này nếu bạn thấy hữu ích cho anh em kỹ sư hệ thống, Azure, MCSA!