

Giới thiệu tổng quan về khóa học



- ✓ Quản lý danh tính và quản lý các tài nguyên trong đám mây (Identity and Governance)
- ✓ Quản trị đám mây Azure (Azure Administrator)
- ✓ Dịch vụ ảo hóa máy chủ Azure (Azure Virtual machines)
- ✓ Hệ thống mạng ảo trong Azure (Virtual Networking & Intersite Connectivity)
- ✓ Dịch vụ cân bằng tải Azure Load balancer
- ✓ Khả năng sẵn sàng và tự động điều chỉnh mở rộng quy mô (High Availability and Scaling)
- ✓ Các dịch vụ điện toán trong Azure: Web Apps và Containers
- ✓ Dịch vụ giám sát & theo dõi hoạt động (Monitoring) các tài nguyên Azure
- ✓ Dịch vụ sao lưu và khôi phục dữ liệu trong Azure (Backup and Recovery)

Tìm hiểu về Azure Resource Manager

Bài học bao gồm

Các nguyên tắc cơ bản về Azure Cloud

**Mô tả dịch vụ quản lý tài nguyên Azure
(Azure Resource Manager)**

Tổng quan về Azure Cloud

Các điểm chính của bài học

Hạ tầng điện toán đám mây(clouds) được tạo ra từ đâu?

Các tài nguyên (Resources)

- ✓ Một đối tượng hoặc thực thể(entities) được quản lý bởi Azure
- ✓ Các máy ảo (Virtual machines), storage accounts, và các hệ thống mạng ảo (Virtual networks)
- ✓ Các tài nguyên (Resources) liên quan đến nhau hoặc phục vụ cho một mục đích chung được nhóm lại thành một "nhóm tài nguyên" (Resource Group)



**Hạ tầng điện toán đám
mây(clouds) được tạo ra từ đâu?**

Các tài nguyên (Resources)

- ✓ Logical container để nhóm các tài nguyên (Resources)
- ✓ Nhóm các tài nguyên dựa trên vòng đời (lifecycle) và bảo mật (security)
- ✓ Có liên quan với một Azure subscription



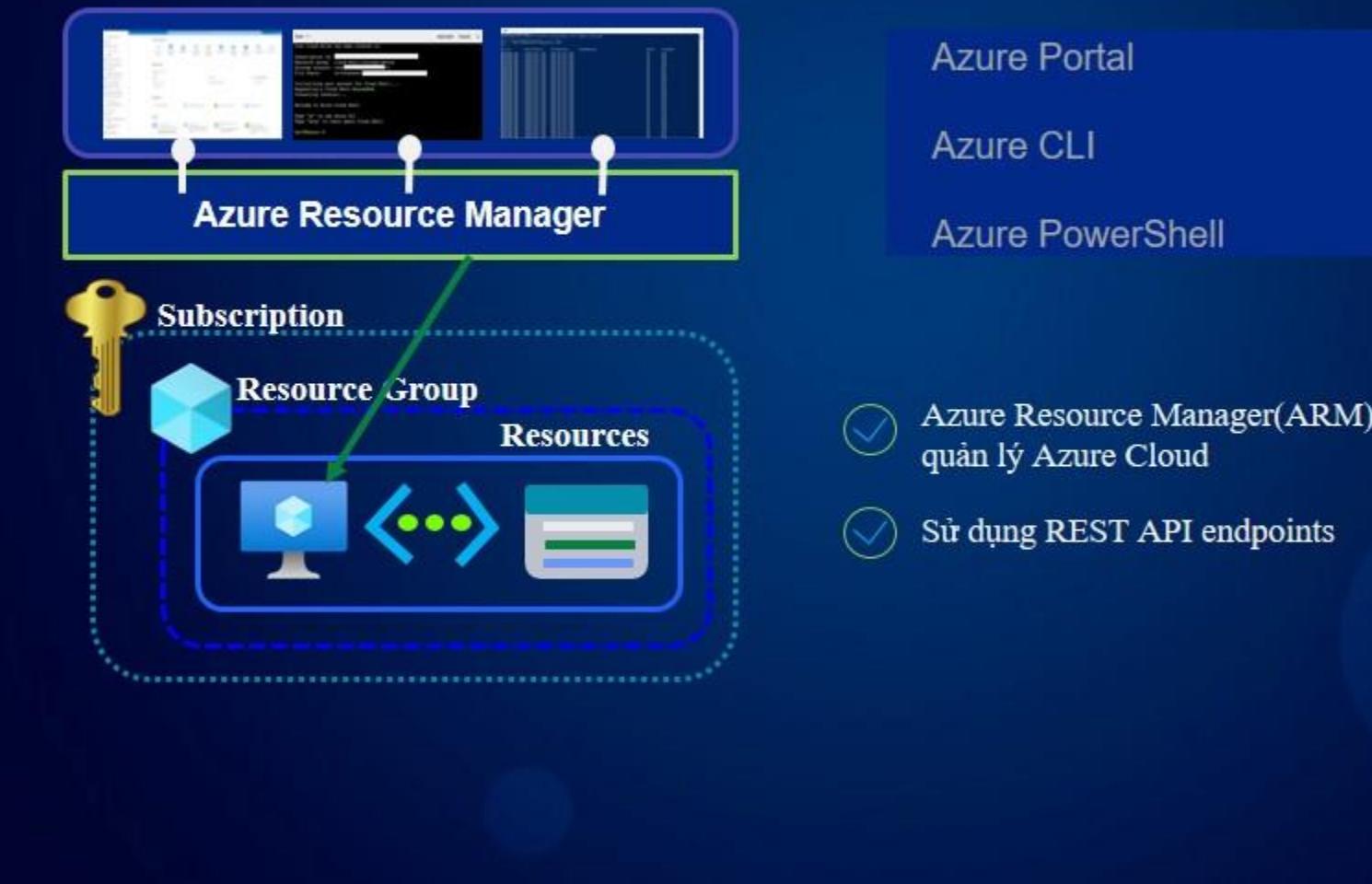
**Hạ tầng điện toán đám
mây(clouds) được tạo ra từ đâu?**

Các tài nguyên (Resources)

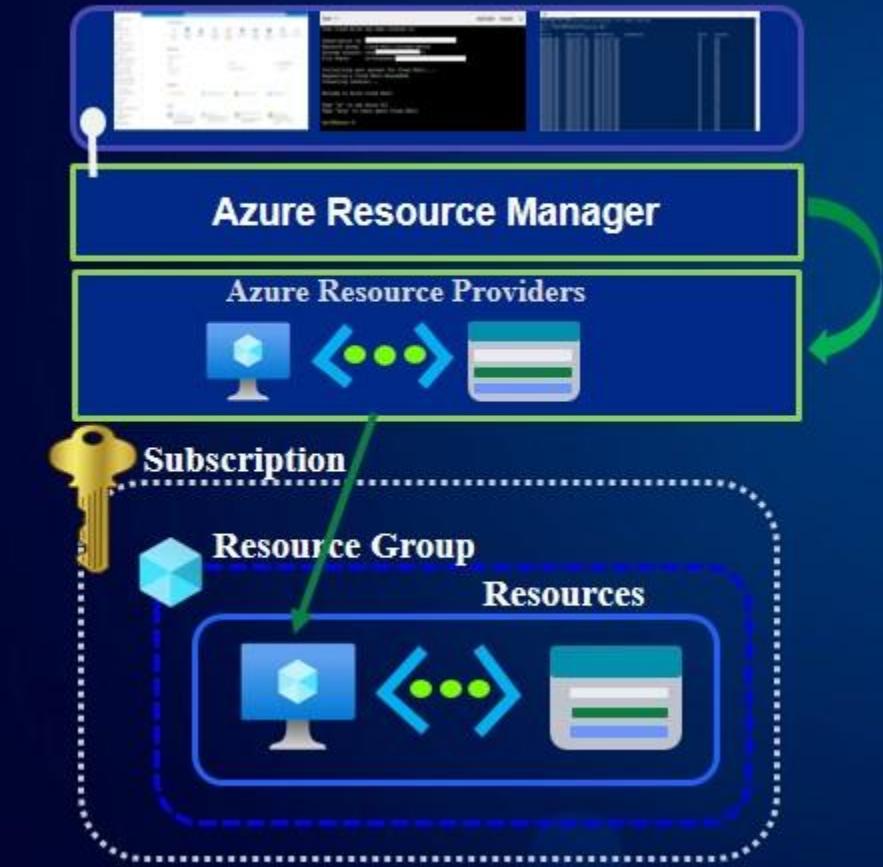
- ✓ Cấu trúc logic nhóm các nhóm tài nguyên và các tài nguyên liên quan với nhau
- ✓ Đơn vị tính phí (billing unit) cho đám mây Azure
- ✓ Kiểm soát bởi Azure Resource Manager(ARM)



Mô tả về Azure Resource Manager

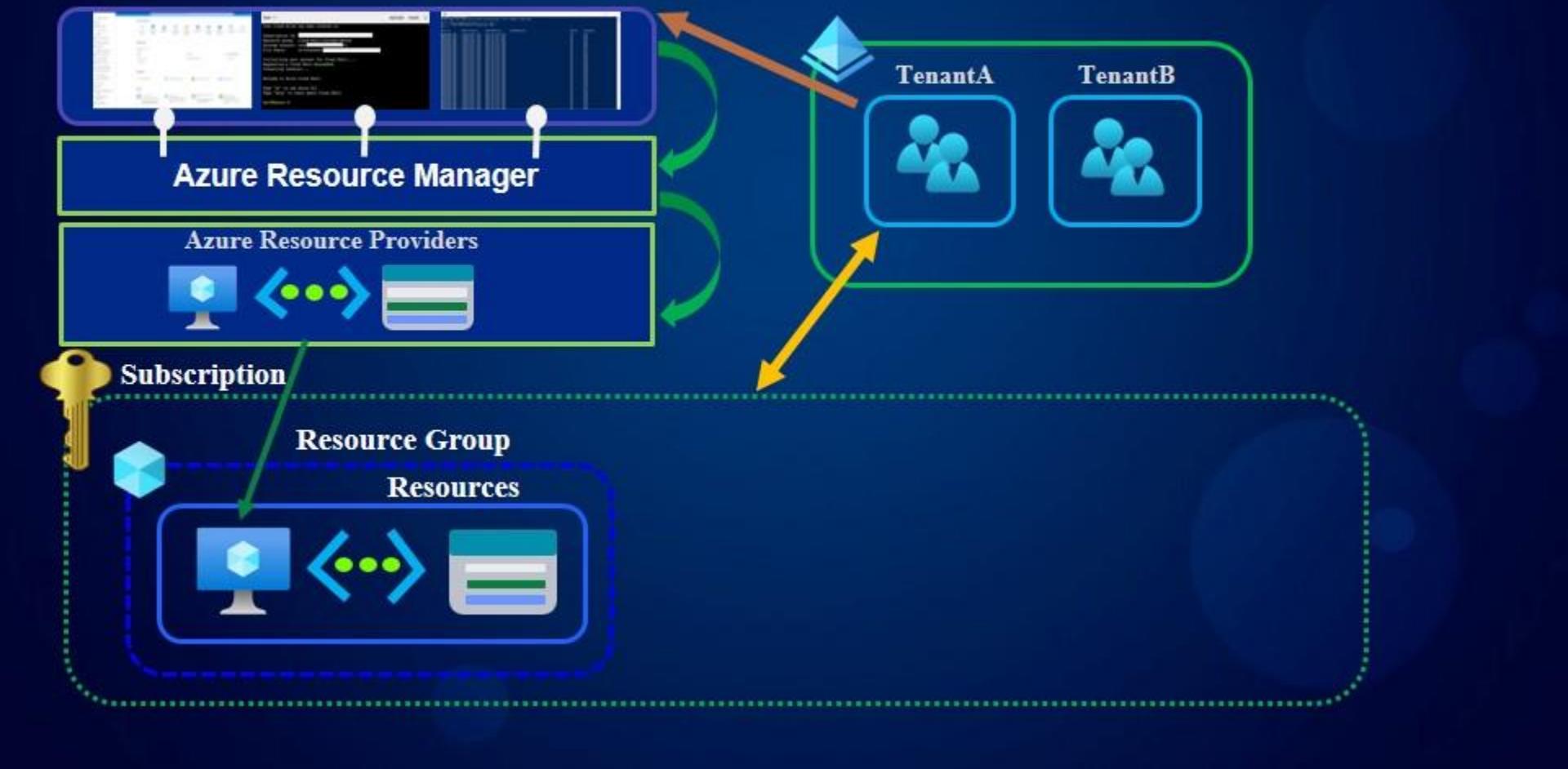


Mô tả về Azure Resource Manager



- ✓ ARM kết nối với resource provider
- ✓ Resource provider hoàn thành yêu cầu(request)

Mô tả về Azure Resource Manager



Các điểm chính của bài học



Một đối tượng hoặc các thực thể(entities) được quản lý bởi Azure, như máy ảo(virtual machines, storage accounts, hệ thống mạng ảo (virtual networks)



Các tài nguyên (Resources) liên quan đến nhau hoặc phục vụ cho một mục đích chung được nhóm lại thành một "nhóm tài nguyên" (Resource Group)



Các nhóm tài nguyên (Resource Group) nằm trong các Thuê bao (subscriptions)



Bạn có thể sử dụng các điểm cuối (endpoints) của REST API để quản lý Azure thông qua Azure Resource Manager(ARM).



Azure Resource Manager(ARM) là một dịch vụ quản lý.



Mỗi một tài nguyên (Resource) trong Azure đều thuộc về một nhà cung cấp tài nguyên (Resource Provider) cụ thể

Sử dụng Azure Portal và Cloud Shell

Bài học bao gồm

Tìm hiểu về Azure Portal

Các thành phần của Azure Portal

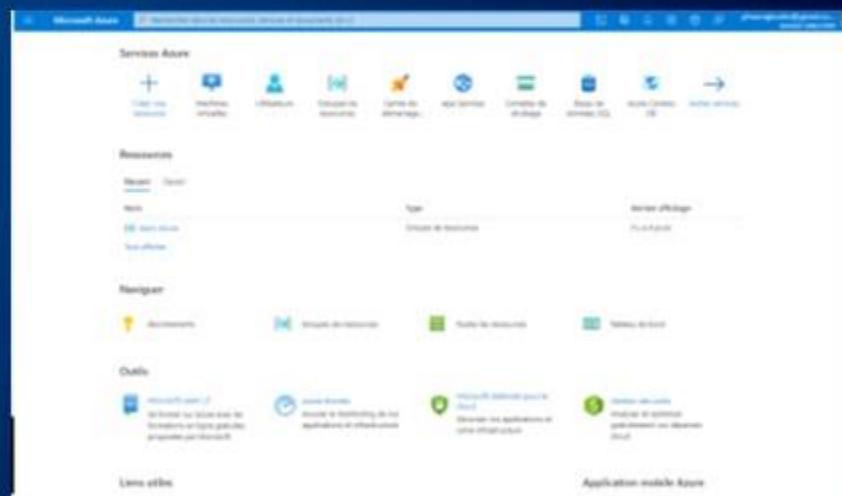
Thực hiện Demo về Azure Portal

Các điểm chính của bài học

Mô tả về Azure Portal

Azure Portal là gì?

- ✓ Web-based portal cho Azure cloud
- ✓ Tạo và quản lý các tài nguyên Azure
- ✓ Sử dụng Cloud Shell



Mô tả về Azure Portal

The screenshot shows the Microsoft Azure Portal interface. At the top, there is a blue header bar with the text "Microsoft Azure" and a search bar labeled "Search resources, services, and docs (G+/-)". On the right side of the header, there are several icons and a user profile area.

The main content area is divided into several sections:

- Azure services:** A row of icons for creating a resource, virtual machines, users, resource groups, quickstart center, app services, storage accounts, SQL databases, Azure Cosmos DB, and more services.
- Resources:** A table showing recent resources. The table has columns for Name, Type, and Last Viewed. One entry is visible: "learn-Azure" (Resource group) last viewed 4 days ago.
- Tools:** A row of icons for Subscriptions, Resource groups, All resources, and Dashboard.

Mô tả về Azure Portal

The screenshot shows the Azure Portal homepage with a dark blue header and sidebar. The header features a search bar labeled "Search resources, services, and docs (G+/-)". The sidebar on the left contains a "FAVORITES" section with a green outline around the "Create a resource" icon, and a list of other services including Home, Dashboard, All services, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Microsoft Defender for Cloud, Cost Management + Billing, and Help + support.

The main content area includes:

- Azure services:** A row of icons for Create a resource, Virtual machines, Users, Resource groups, Quickstart Center, App Services, Storage accounts, SQL databases, Azure Cosmos DB, and More services.
- Resources:** A table showing a single item: "learn-Azure" (Resource group) from 5 days ago.
- Navigate:** Icons for Subscriptions, Resource groups, All resources, and Dashboard.
- Tools:** Icons for Microsoft Learn, Azure Monitor, Microsoft Defender for Cloud, and Cost Management.
- Useful links:** Links to Microsoft Learn, Azure Monitor, Microsoft Defender for Cloud, and Cost Management.
- Azure mobile app:** A link to the Azure mobile application.

Mô tả về Azure Portal

The screenshot shows the Microsoft Azure Portal interface. At the top, there is a blue header bar with the "Microsoft Azure" logo, a search bar containing "Search resources, services, and docs (G+)", and various navigation icons. The main content area is white and organized into several sections:

- Azure services**: A row of icons for creating a resource, Virtual machines, Users, Resource groups, Quickstart Center, App Services, Storage accounts, SQL databases, Azure Cosmos DB, and More services.
- Resources**: A table showing recent resources. The first item is a resource group named "learn-Azure" created 4 days ago.
- Tools**: Icons for Subscriptions, Resource groups, All resources, and Dashboard.

Mô tả về Azure Portal

The screenshot shows the Microsoft Azure Portal interface. At the top, there is a dark blue header bar with the "Microsoft Azure" logo, a search bar containing "Search resources, services, and docs (G+)", and several icons for account management and notifications. Below the header, the main content area has a white background.

Azure services

Icons for various Azure services are displayed:

- Create a resource (+)
- Virtual machines (monitor icon)
- Users (person icon)
- Resource groups (square icon)
- Quickstart Center (rocket icon)
- App Services (globe icon)
- Storage accounts (bar chart icon)
- SQL databases (SQL icon)
- Azure Cosmos DB (globe with lines icon)
- More services (arrow icon)

Resources

Recent resources are listed:

Name	Type	Last Viewed
[?] learn-Azure	Resource group	4 days ago

See all

Tools

Links to other tools:

- Subscriptions (key icon)
- Resource groups (square icon)
- All resources (grid icon)
- Dashboard (dash icon)

Thực hiện Demo về Azure Portal

1

Login vào
Azure Portal

2

Review
Portal

3

Tạo Cloud
Shell

Các điểm chính của bài học



Có thể sử dụng Azure AD để log in vào Azure Portal



Sử dụng Cloud Shell để quản lý Azure



Tạo các tài nguyên Azure (Azure resources)



Quản lý chi phí billing



Quản lý Azure resources



Có thể tạo hỗ trợ (support ticket) với Microsoft Azure

Sử dụng Azure CLI và PowerShell

Bài học bao gồm

Tìm hiểu về Azure CLI và PowerShell

Các hoạt động cơ bản

**Thực hiện Demo sử dụng CLI
và PowerShell**

Các điểm chính của bài học

Mô tả về Azure Portal

Azure CLI là gì?

- Là tiện ích dòng lệnh để quản lý tài nguyên Azure (Azure resources)
- Tạo và quản lý các tài nguyên mà không cần log in vào trong Azure portal.
- Tạo các kịch bản scripts để tự động hóa các công việc

```
Cloud@Azure: ~$ az group create \
> --name $regrp \
> --location $mylocation■
```

Mô tả về Azure Portal

Azure PowerShell là gì?

- Là tập hợp các lệnh ghép ngắn(cmdlets) để quản lý tài nguyên Azure
- Tạo và quản lý các tài nguyên mà không cần log in vào trong Azure portal.
- Tạo các kịch bản scripts để tự động hóa các công việc

```
PS /home/cloud> New-AzResourceGroup `>> -ResourceGroupName $regrp `>> -Location $mylocation
```

Các hoạt động cơ bản

PowerShell

```
New-AzResourceGroup  
    -ResourceGroupName $regrp  
    -Location $mylocation
```

Azure CLI

```
az group create |  
    --name $regrp |  
    --location $mylocation
```



Thực hiện Demo về Azure Portal

1

Login vào
Azure Portal

2

Sử dụng
Cloud Shell

3

Tạo Azure
Resources

Các điểm chính của bài học

Cơ bản về Azure CLI và PowerShell

- ✓ Có thể quản lý các tài nguyên Azure trực tiếp từ máy tính cá nhân của bạn
- ✓ Có thể tạo các kịch bản scripts để tự động hóa trong Azure
- ✓ Không cần phải log in Azure Portal



Sử dụng ARM Templates

Bài học bao gồm

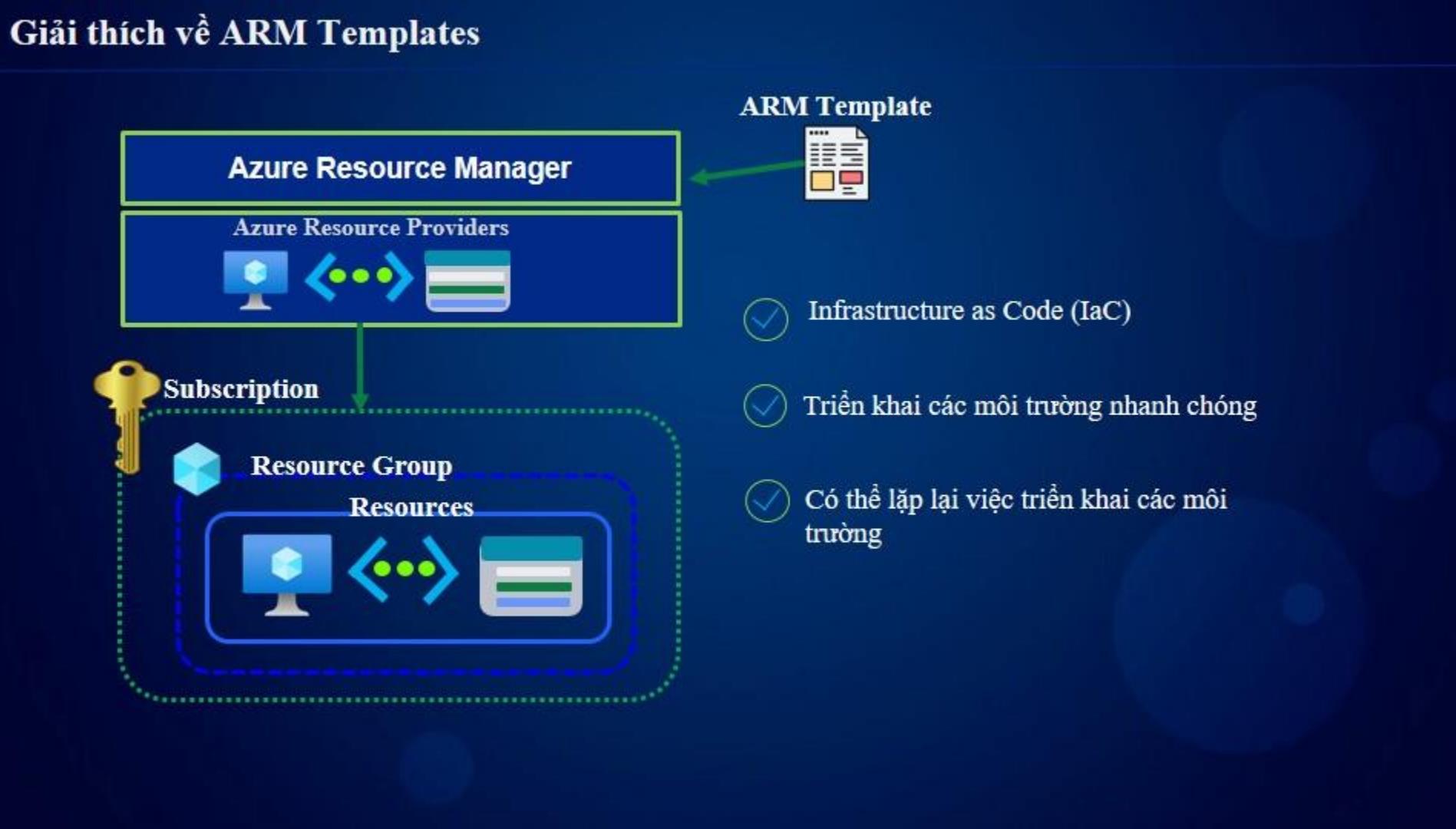
Giải thích về ARM Templates

Các thành phần của ARM Templates

Thực hiện Demo sử dụng ARM Templates

Các điểm chính của bài học

Giải thích về ARM Templates



Các thành phần của ARM Templates



Các thành phần tham số(parameters) và biến(variables) được sử dụng để truyền thông tin cho template.



Các thành phần tài nguyên(resources) được sử dụng để định nghĩa các tài nguyên trong template.



Thành phần outputs được sử dụng để trả về thông tin kết quả từ việc thực thi chạy template

ARM Template



```
ARM Template
{
    "$schema": "https://
schema.management.azure.com

    "contentVersion": "1.0.0.0",
    "parameters": {} ,
    "variables": {} ,
    "resources": {} ,
    "outputs": {} ,
}
```

Thực hiện Demo sử dụng ARM Templates



Các điểm chính của bài học

ARM Template



- ✓ **ARM (Azure Resource Manager) template** là một file có cấu trúc theo **định dạng JSON**
- ✓ Có thể lặp lại việc triển khai các môi trường

```
{  
    "$schema": "https://  
    schema.management.azure.com  
  
    "contentVersion":  
    "1.0.0.0",  
    "parameters": {},  
    "variables": {},  
    "resources": {},  
    "outputs": {}  
}
```

Quản lý Subscriptions

Bài học bao gồm

Mô tả về Subscriptions

Các loại Subscriptions

Subscription Naming Conventions

Các điểm chính của bài học

Mô tả về Subscriptions



Đơn vị tính toán chi phí tổng hợp
của tất cả các tài nguyên (resources)
phía dưới



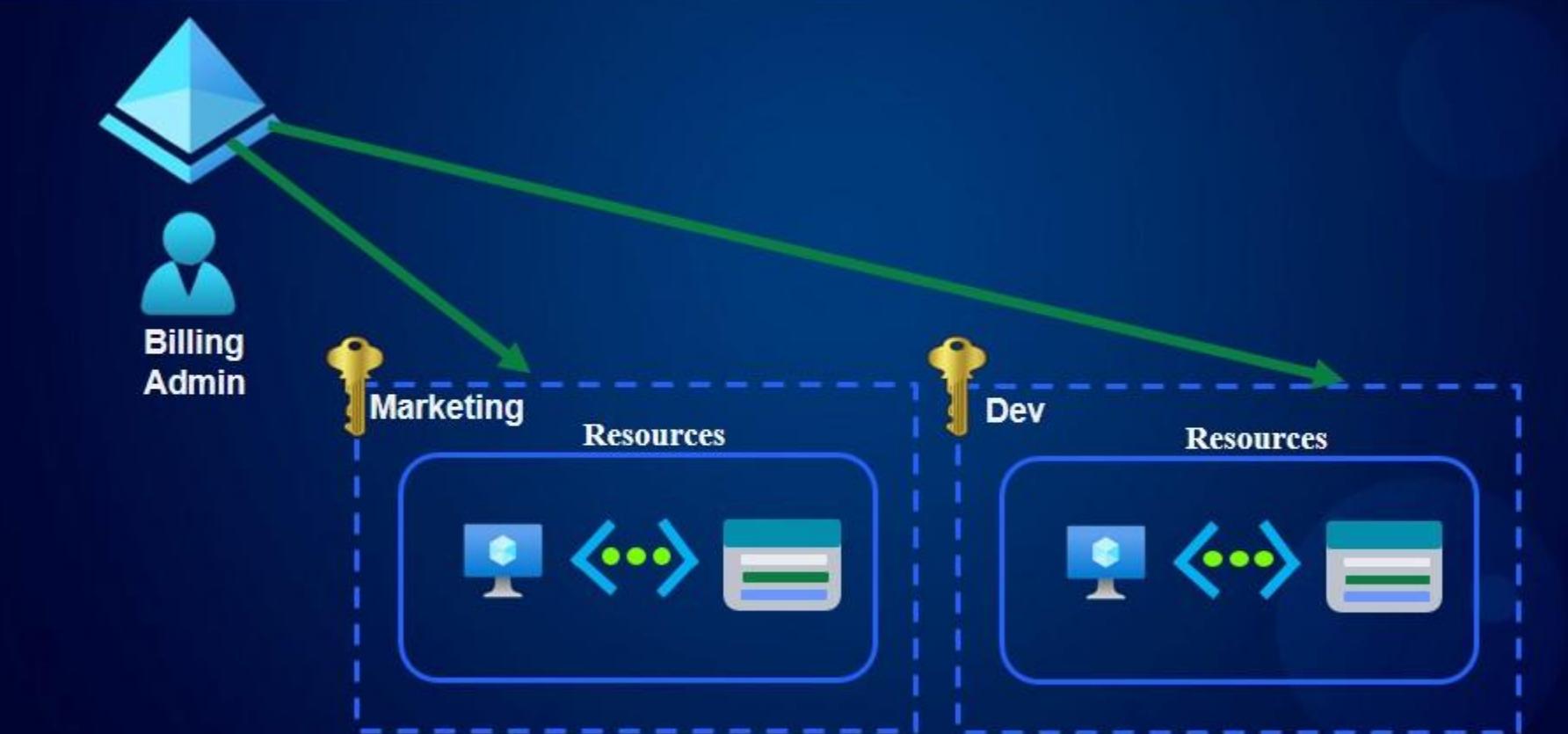
Chứa các nhóm tài nguyên
(resource groups) và các tài nguyên
liên quan



Cấp độ xác định phạm vi áp dụng
các chính sách quản lý và biện pháp bảo mật



Mô tả về Subscriptions



Các loại Subscriptions

Current Offers		
OFFER NAME	OFFER NUMBER	SPENDING LIMIT
Azure Plan	0017G	
Enterprise Agreement Support		
Microsoft Azure EA Sponsorship	0136P	
Pay-As-You-Go	0003P	
Support Plans	0041P, 0042P, 0043P	
Free Trial	0044P	✓
Visual Studio Professional subscribers	0059P	✓
Visual Studio Test Professional subscribers	0060P	✓
MSDN Platforms subscribers	0062P	✓
Visual Studio Enterprise subscribers	0063P	✓
Visual Studio Enterprise (BizSpark) subscribers	0064P	✓
Visual Studio Enterprise (MPN) subscribers	0029P	✓
Pay-As-You-Go Dev/Test	0023P	

Subscription Naming Conventions

Prod/Dev/Staging

1

Các Subscriptions được đặt tên dựa trên ý nghĩa của mỗi môi trường
VD: Như môi trường chạy thật(production), môi trường đang phát triển ứng dụng (development), hoặc môi trường được sử dụng để kiểm tra và thử nghiệm các phiên bản mới của ứng dụng hoặc phần mềm(staging environment) trước khi đưa vào môi trường production

Phòng ban/nhóm

2

Các đăng ký(Subscriptions) được đặt tên dựa trên bộ phận hoặc nhóm mà Subscription dành cho, để sau đó thanh toán chi phí có thể dễ dàng được liên kết với một đơn vị kinh doanh nhất định

3

Region

Subscription được đặt tên dựa trên region của việc kinh doanh sử dụng subscription đó

Prod-Endgineering A-EastUS-2023



Các điểm chính của bài học

Subscriptions



Đơn vị tính toán chi phí tổng hợp
của tất cả các tài nguyên (resources)
phía dưới



Cấp độ xác định phạm vi áp dụng
các chính sách quản lý và biện pháp bảo mật



Chứa các nhóm tài nguyên
(resource groups) và các tài nguyên
liên quan



Chỉ có thể được liên kết với một organization
đuy nhất (Azure AD tenant) tại một thời điểm

Sử dụng Management Groups

Bài học bao gồm

Định nghĩa về Management Groups

Tìm hiểu về phân cấp (Hierarchy)

Phạm vi (Scoping)

Các điểm chính của bài học

Định nghĩa về Management Groups

Quản lý Subscriptions

Tổ chức và quản lý các subscriptions bằng cách Nhóm chúng một cách hợp lý vào trong management groups

- Hệ thống tổ chức phân cấp (Organizational hierarchy)
- Cung cấp một phạm vi khác để thực thi việc quản trị và tuân thủ

Management Group



Định nghĩa về Management Groups

Các quan hệ cha-con (Parent-Child Relationships)

- Root management groups là cấp cao nhất
- Các management groups và subscriptions có thể có một cha duy nhất
- Hỗ trợ sáu cấp độ phân cấp (six levels of hierarchy)

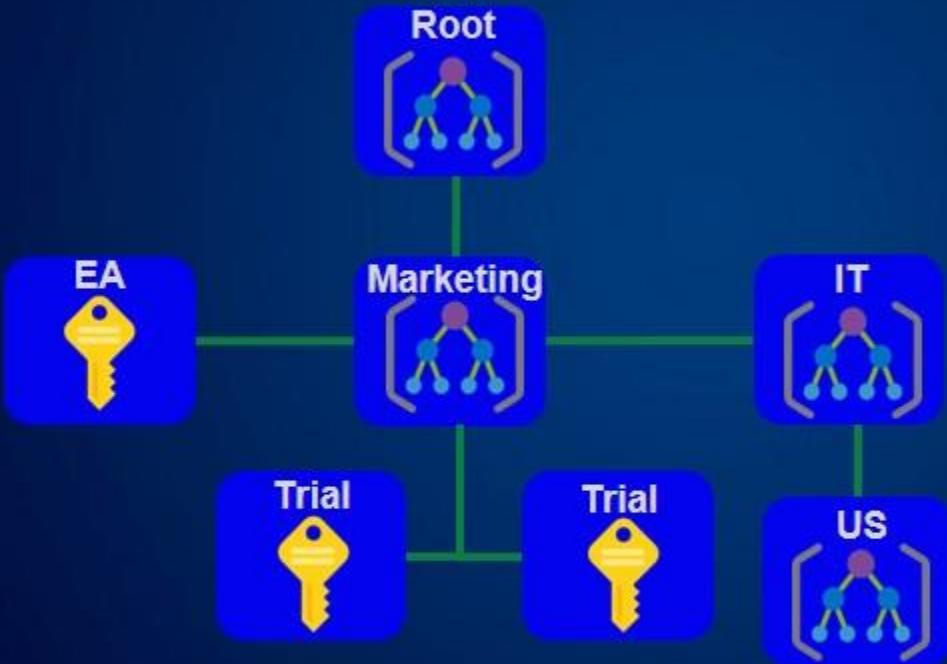
Hỗ trợ tuân thủ (Compliance Support)

- Các chính sách Azure(Azure Policies)
- Azure role-based access control(RBAC)

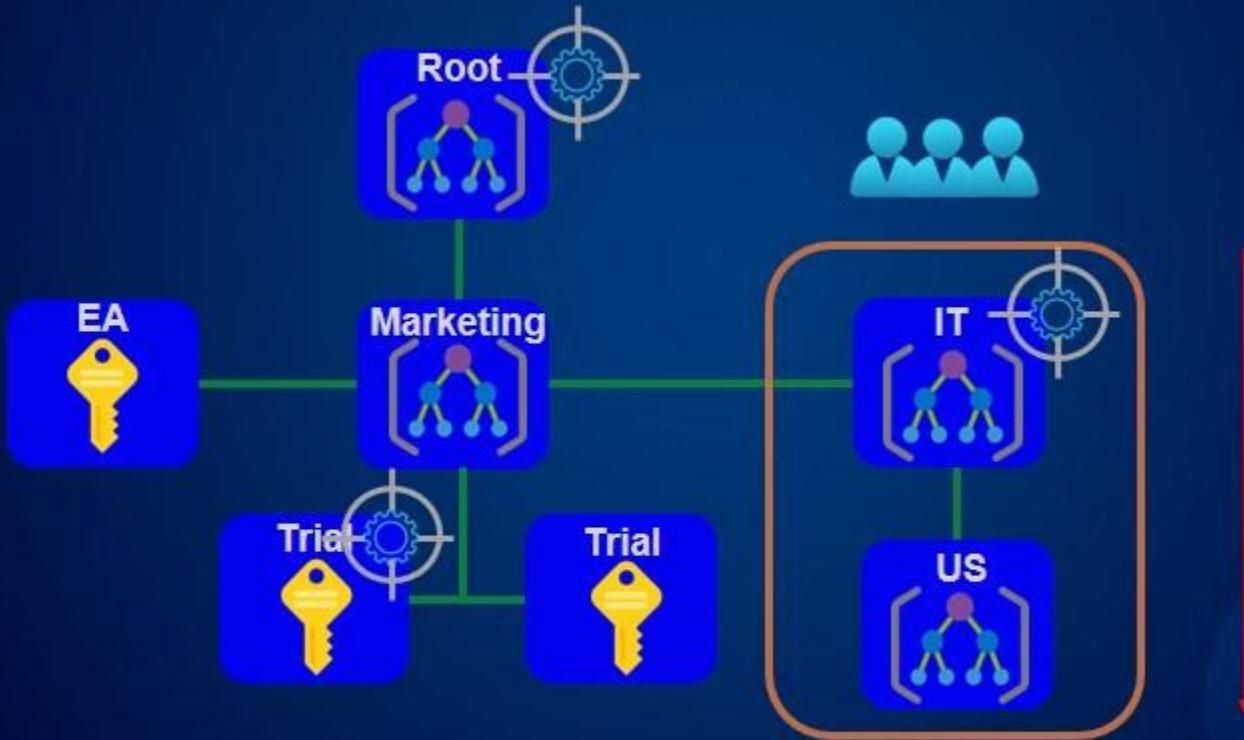
Management Group



Tìm hiểu về phân cấp (Hierarchy)



Phạm vi (Scoping)



Các điểm chính của bài học



- Quyền truy cập vào Root management group là mặc định không được cấp cho tài khoản user thường
- Root management group là không thể chuyển hoặc bị xóa đi
- Azure Role-Based Access Control (RBAC) được hỗ trợ cho management groups
- Global Administrator role phải được cấp cho User quản trị administrator của root group bên trong Azure AD tenant

Tìm hiểu về Azure Policy

Bài học bao gồm

**Định nghĩa về
chính sách Azure (Azure Policy)**

Các thành phần của một policy

Ví dụ về policy

Các điểm chính của bài học

Định nghĩa về chính sách Azure (Azure Policy)

Thực thi Tuân Thủ và kích hoạt Kiểm Tra Giám Sát

Các tổ chức doanh nghiệp cần triển khai khả năng quản trị và tuân thủ cấp doanh nghiệp trong Azure



Hạn chế cấm truy cập vào các tài nguyên(Resources)

- Kiểm soát chi phí
- Hạn chế truy cập vào dịch vụ(service)



Các khu vực được cho phép

- Tuân thủ theo vị trí địa lý

Các thành phần của một policy

Azure Policy



Định nghĩa chính sách

Định nghĩa các tiêu chí đánh giá cho việc tuân thủ và định nghĩa các hành động diễn ra. Kiểm tra hoặc từ chối phải là một sự việc nằm ngoài sự tuân thủ



Áp dụng chính sách

Phạm vi tại nơi mà chúng ta sẽ áp dụng chính sách. Phạm vi này có thể là trong phạm vi một management Group, subscription, resource group, hoặc tài nguyên (resource)



Định nghĩa theo tiêu chí

Một tập hợp các chính sách được điều chỉnh để cùng với nhau để có thể đạt được một mục tiêu tốt nhất (VD: Đảm bảo các máy ảo (VMs) đáp ứng theo các tiêu chuẩn mà chúng ta đặt ra)

Ví dụ về policy

Yêu cầu Tags



Định nghĩa chính sách

Đánh giá xem một VM có đang được tạo
được gắn tag có tên là "Project:abc" hay không.
Nếu VM thiếu tag, thì từ chối tạo tài nguyên



Áp dụng chính sách

Chỉ định áp dụng chính sách trong phạm vi
của resource group nơi mà máy ảo sẽ được tạo ra

Ví dụ về policy



Ví dụ về policy



Các điểm chính của bài học



Định nghĩa chính sách



Áp dụng chính sách



Định nghĩa theo tiêu chí

- **Tạo, quản lý, và thực thi triển khai các chính sách policies**
- **Thi hành các chính sách trên các tài nguyên resources**
- **Kiểm tra việc tuân thủ**
- **Từ chối việc tạo ra các tài nguyên resources, được thực hiện bên ngoài chính sách tuân thủ**

Gắn thẻ các tài nguyên (Resources)

Bài học bao gồm

Mô tả về gắn thẻ cho các tài nguyên

Phân cấp gắn thẻ tài nguyên

Thực hiện Demo gắn thẻ tài nguyên

Các điểm chính của bài học

Mô tả về gắn thẻ cho các tài nguyên

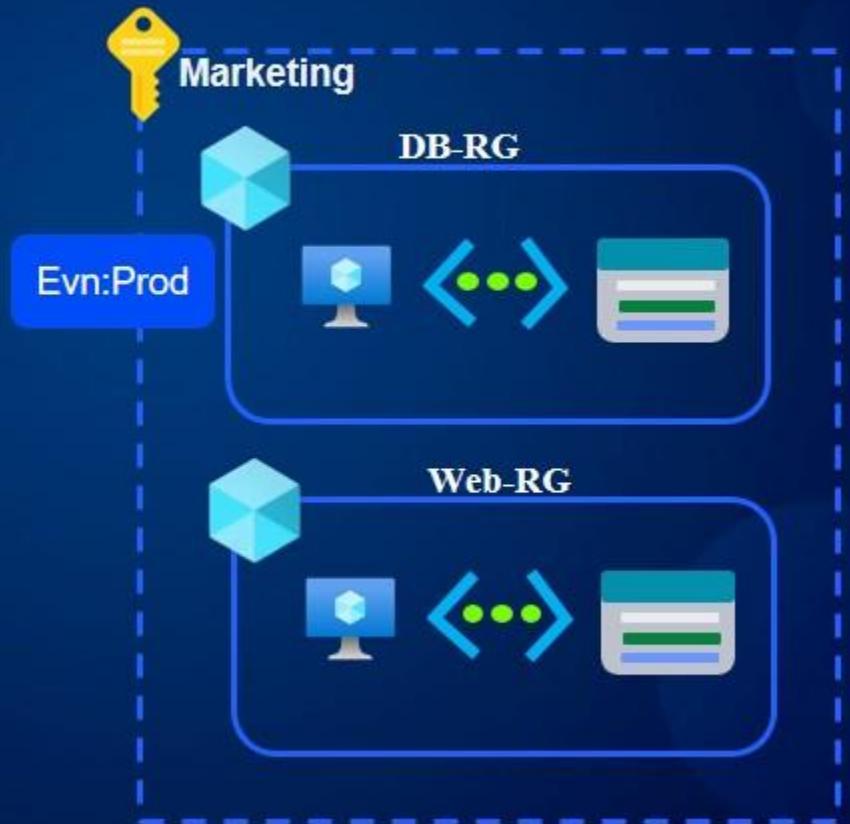
Tags là gì?

Tên: Giá trị

Dept: Marketing

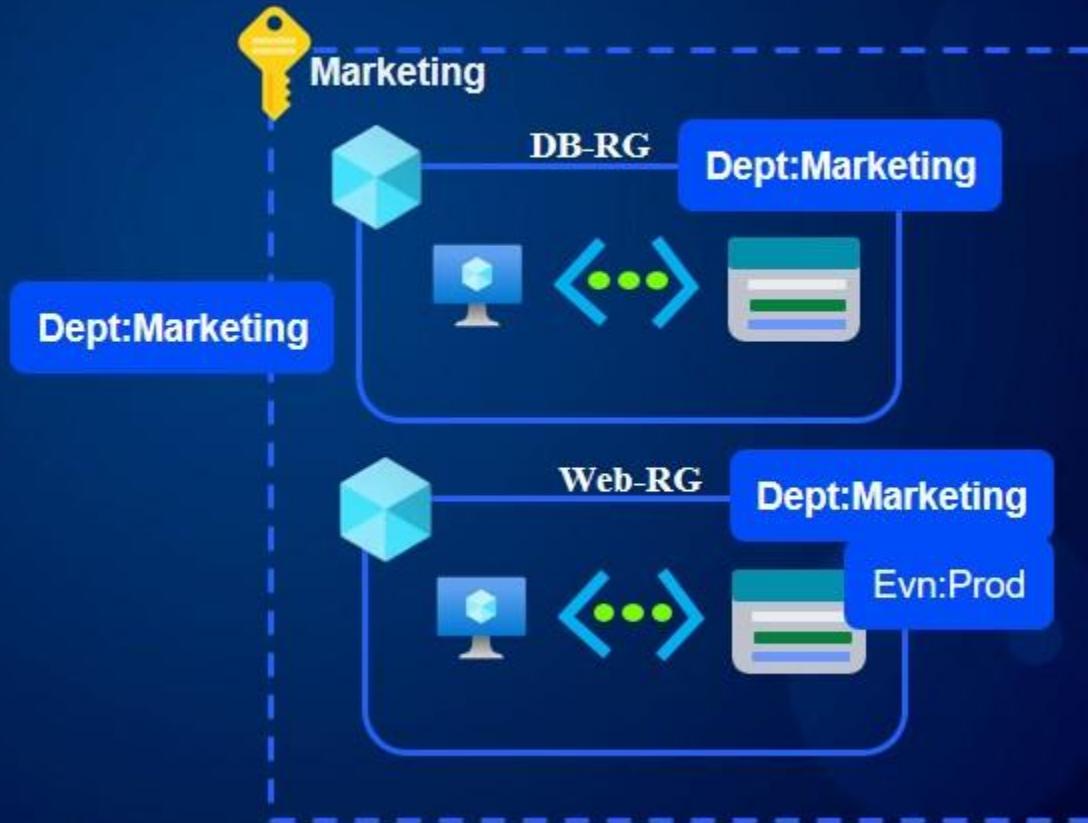
Evn: Prod

- Tên có thể có độ dài tối đa 512 ký tự,
Và giá trị tối đa 256 ký tự
- Tên của các tài nguyên tạo ra trong
Storage accounts có thể được đặt
tối đa lên đến 128 ký tự



Phân cấp gắn thẻ tài nguyên

- Tags không được kế thừa
- Một tài nguyên có thể có đến 50 tags



Thực hiện Demo gắn thẻ tài nguyên

1

Login vào
Azure Portal

2

Xác định
Tag

3

Gắn thẻ tag
cho resource
group

Các điểm chính của bài học



Có thể quản lý các tài nguyên(resources) thông qua tags. Ví dụ, tắt shutdown tất cả các máy ảo VMs sử dụng một tag cụ thể, hoặc các lập trình viên có thể sử dụng một tag cụ thể để cập nhật code trên các máy ảo VMs



Tags là không được thừa kế từ một phạm cao hơn
VD như một resource group.
Mỗi một tài nguyên phải được gắn thẻ tag riêng.
Bạn có thể sử dụng Azure policy để bắt buộc thực hiện việc tagging cho các tài nguyên

Thực hành gắn, xóa, cập nhật Tags cho các tài nguyên trong Azure

Trong tình huống của bài thực hành này, phòng quản lý tài chính của công ty đã liên hệ với bạn, yêu cầu bổ sung thêm phân loại thông tin dựa trên hóa đơn chi phí sử dụng các tài nguyên Azure, thông tin phải bao gồm cả người đã tạo tài nguyên, ngân sách của các bộ phận, phòng ban cụ thể sẽ được sử dụng tài nguyên nếu như các tài nguyên là cần thiết để chạy các ứng dụng hệ thống kinh doanh quan trọng. Và họ cũng yêu cầu bạn đánh dấu phân loại các tài nguyên không sử dụng đến nữa.

- ✓ **Chúng ta cần vào đường link :**

<https://raw.githubusercontent.com/phuongluuho/Azure104/main/lab-1.json>

Để copy nội dung file lab-1.json, sau đó sử dụng ARM Templates.

Để tạo ra một môi trường cho bài thực hành gồm: 01 máy ảo, 01 storage account, 01 card mạng ảo, 01 mạng ảo Virtual network, 1 Public IP, 01 tường lửa network security group



- Gắn thẻ Tags cho Resource Group



- Xóa Tags cho máy ảo VM, và đánh dấu máy ảo này là không cần sử dụng đến nữa, và sẽ xóa máy ảo này đi



- Thay đổi tag cho mạng ảo Virtual Network



- Hoàn thành bài lab



Giai đoạn 1



Giai đoạn 2



Giai đoạn 3



Giai đoạn 4

Khóa(locking) và di chuyển các tài nguyên (Resources)

Bài học bao gồm

Mô tả về khóa tài nguyên(Resource locks)

Các kiểu khóa tài nguyên

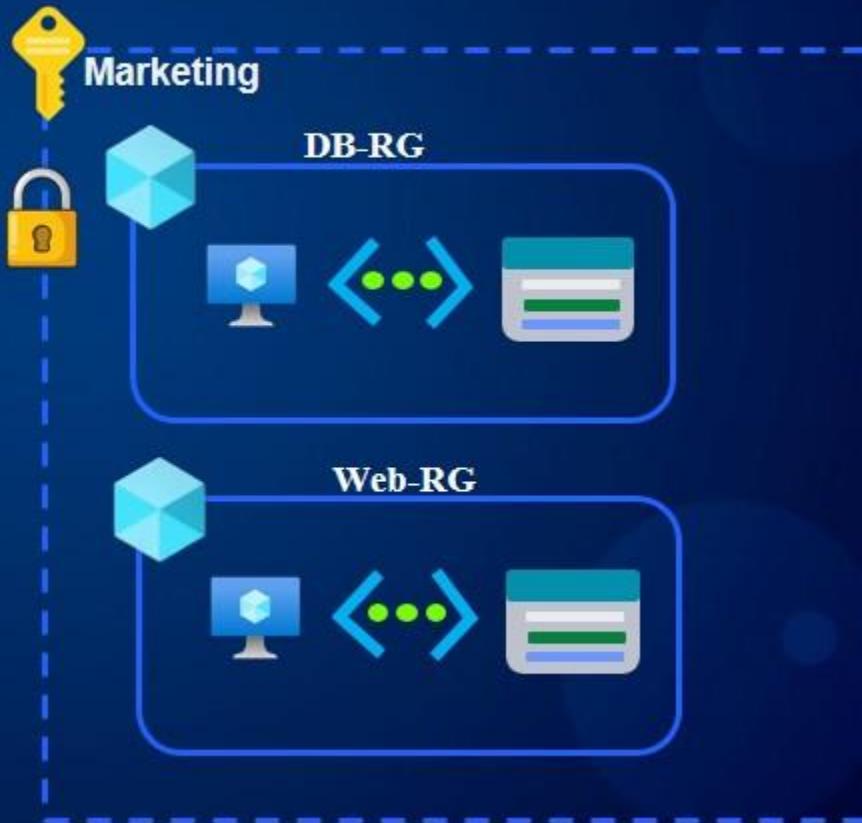
Di chuyển các tài nguyên

**Thực hiện Demo khóa và di chuyển tài
nguyên**

Các điểm chính của bài học

Mô tả về khóa tài nguyên(Resource locks)

- Khóa (locks) cho phép kiểm soát hành động mà người dùng có thể thực hiện trên các tài nguyên
- Bạn có thể khóa subscriptions, resource groups, hoặc các tài nguyên(resources)
- Các hạn chế của khóa áp dụng tới tất cả các người dùng(users) và roles



Các loại khóa tài nguyên

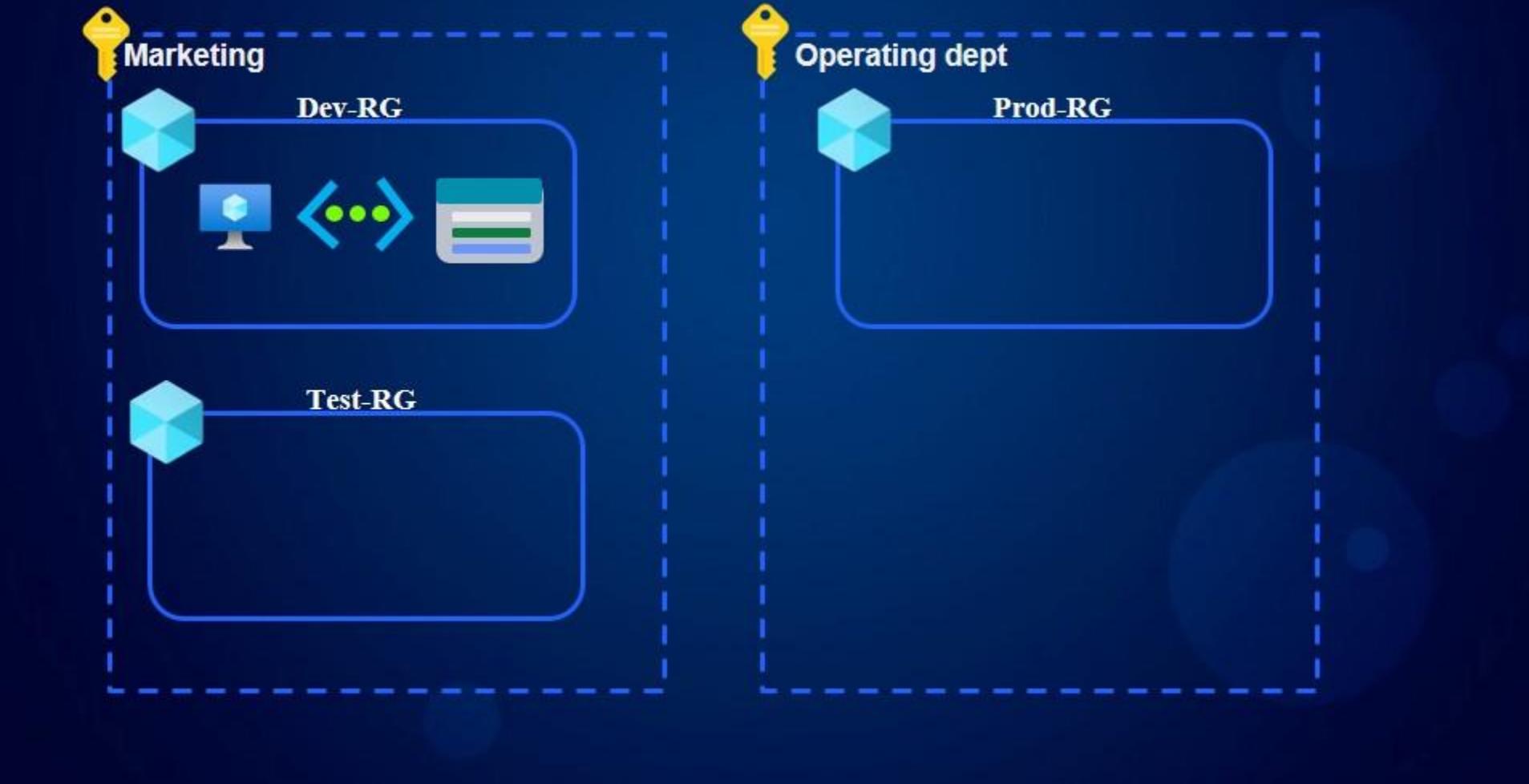
Các loại khóa



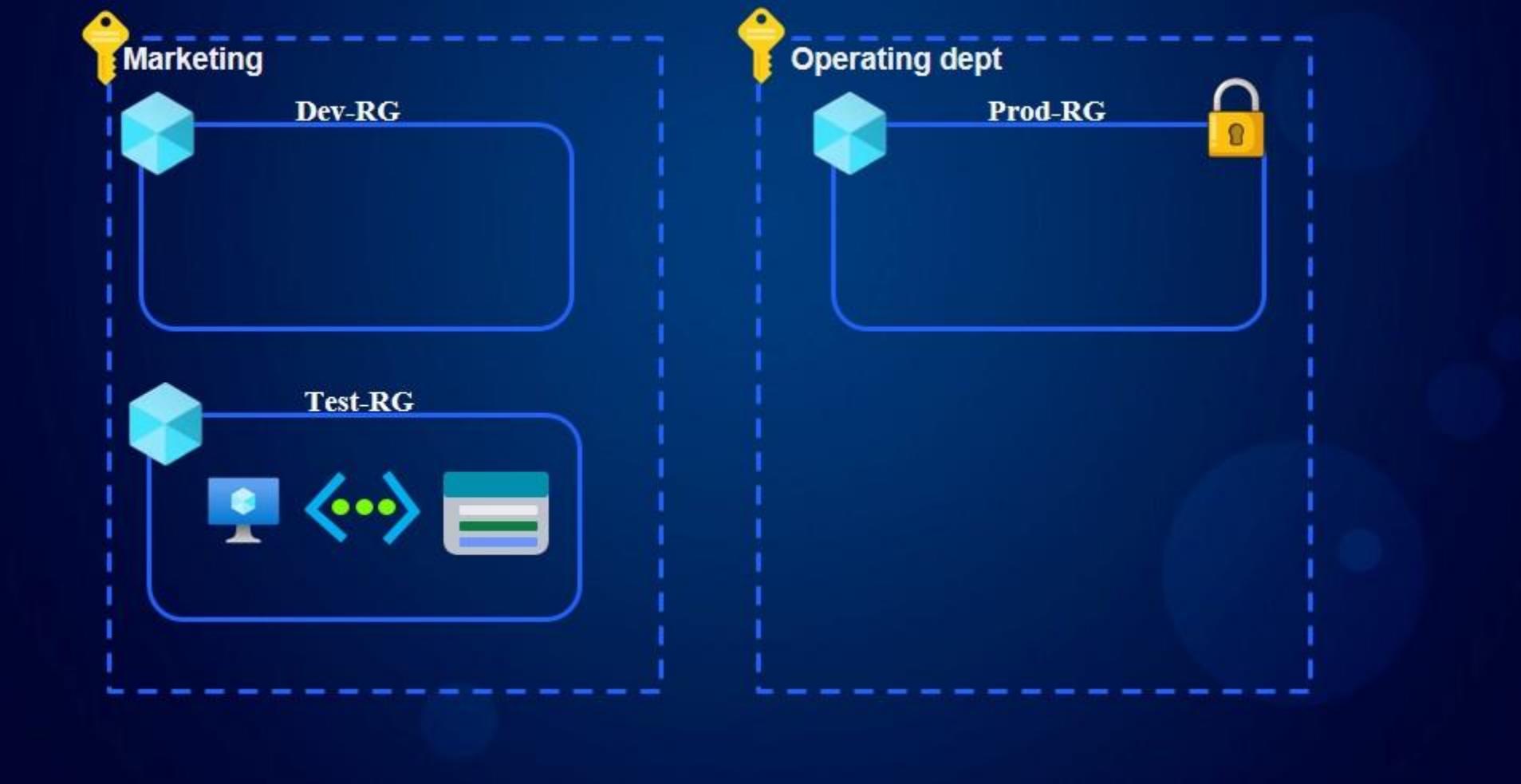
- ReadOnly cho phép người dùng được quyền đọc một tài nguyên, nhưng họ không thể xóa và cập nhật tài nguyên này
- CanNotDelete cho phép người dùng đọc và sửa đổi một tài nguyên, nhưng họ không thể xóa tài nguyên này
- Các khóa(locks) được kế thừa từ phạm vi cha(parent scope)



Di chuyển các tài nguyên



Di chuyển các tài nguyên



Thực hiện Demo

1

Login vào
Azure Portal

2

Tạo máy ảo
VM

3

Cấu hình add
một Delete
Lock

Các điểm chính trong bài học



Các khóa tài nguyên (Resource Locks)



Chỉ đọc
(ReadOnly)



Không thể xóa
(CanNotDelete)

Quản lý chi phí sử dụng tài nguyên Azure

Bài học bao gồm

Những gì tác động đến chi phí sử dụng tài nguyên

Các cách tính toán chi phí tối ưu nhất và các công cụ

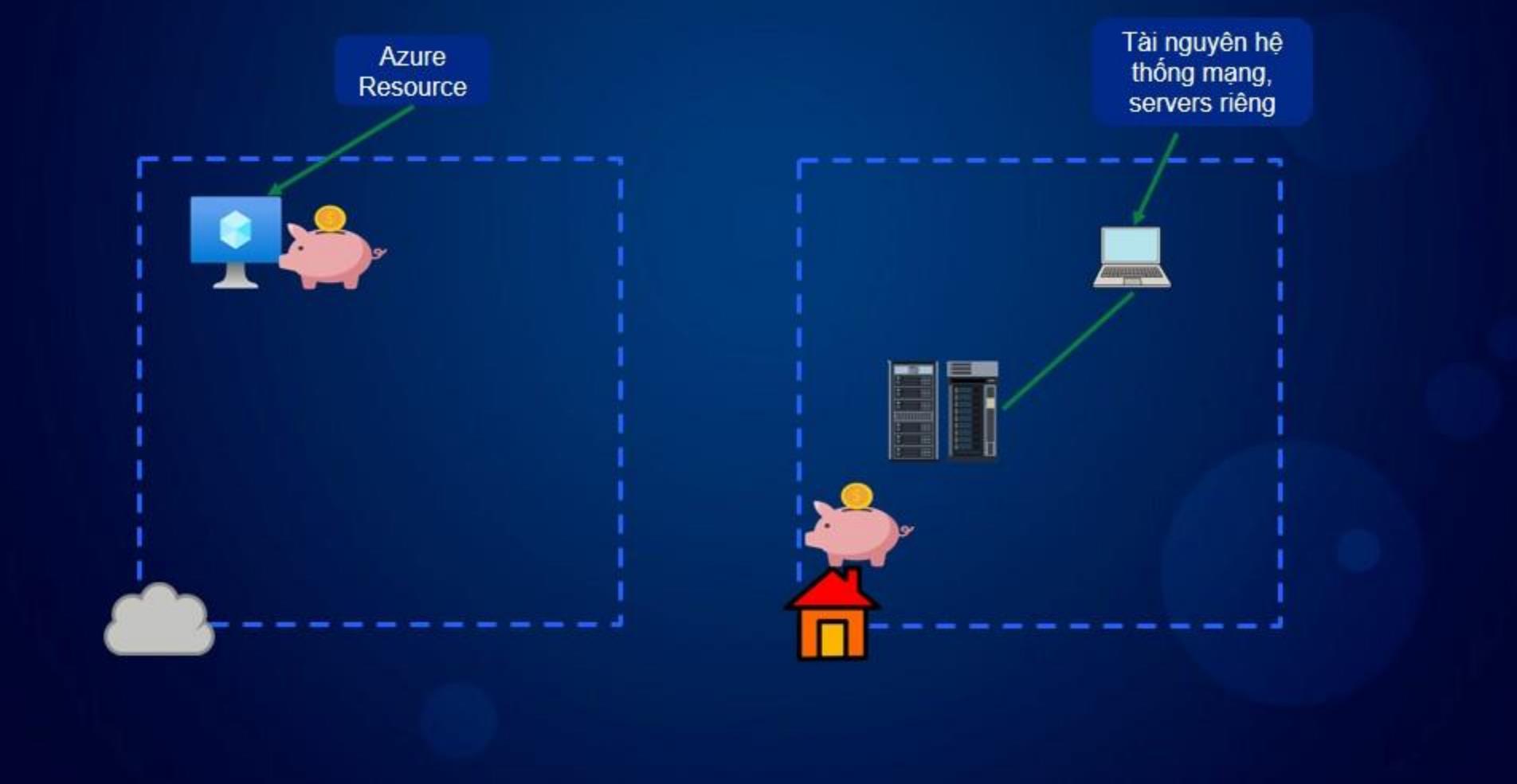
Thực hiện Demo sử dụng quản lý chi phí của Microsoft Cost Management

Thực hiện Demo sử dụng Pricing Calculator

Thực hiện Demo sử dụng TCO Calculator

Các điểm chính của bài học

Những gì tác động đến chi phí sử dụng tài nguyên



Những gì tác động đến chi phí sử dụng tài nguyên

Các loại Subscription

Miễn phí(free), pay-as-you-go,
Enterprise Agreement, và
Cloud Solution Provider(CSP)

Loại tài nguyên

Ví dụ: Storage account Blob
Storage vs. Table storage

Sử dụng các đơn vị tài nguyên

Các tài nguyên như tổng thời gian
sử dụng CPU, network traffic vào/ra,
và dung lượng của ổ đĩa ảo

Sử dụng tài nguyên

Các chi phí sử dụng
Một tài nguyên

Vị trí địa lý

Các chi phí sử dụng
các dịch vụ được tính thay đổi
theo khu vực vùng miền regions

Các cách tính toán chi phí tối ưu nhất và các công cụ

Cách tính toán chi phí tối ưu nhất

- Lựa chọn tài nguyên thích hợp cho trường hợp sử dụng cụ thể
- Hiểu rõ tài nguyên cần, hợp lý cho Công việc(Sizing)
- Dùng cấp các tài nguyên không cần thiết
- Sử dụng các tính năng của đám mây nếu có thể (ví dụ: khả năng mở rộng, tính linh hoạt)
- Lên kế hoạch chi phí trước khi sử dụng tài nguyên

Các công cụ tính toán chi phí



Pricing Calculator

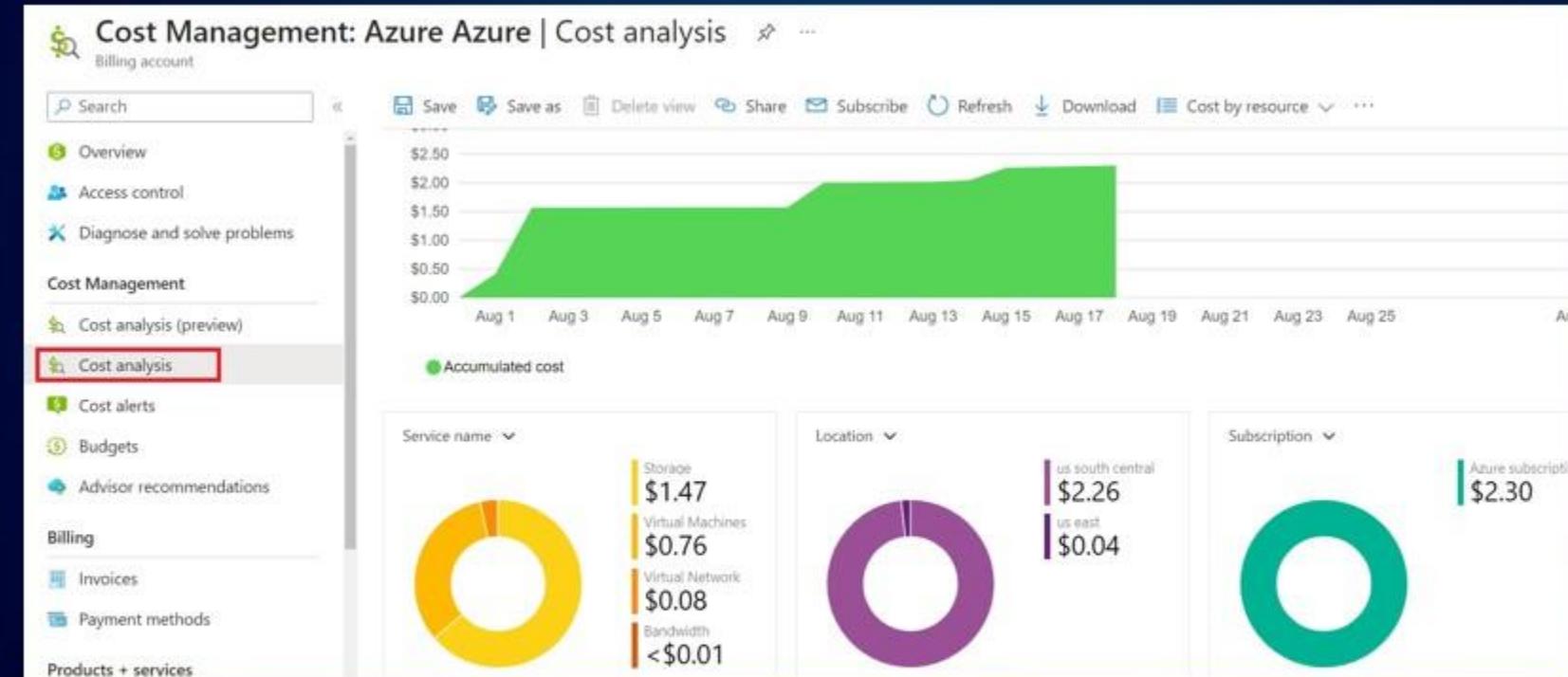


Total Cost of Ownership (TCO)
Calculator



Microsoft Cost Management

Thực hiện Demo sử dụng quản lý chi phí của Microsoft Cost Management



Phân tích chi phí



Tạo ngân sách chi phí

Thực hiện Demo sử dụng Pricing Calculator



**Ước tính chi phí
cho khối lượng
công việc**



**Sửa đổi chi tiết
khối lượng công việc**

Thực hiện Demo sử dụng TCO Calculator

TCO CALCULATOR



VS.



Các điểm chính trong bài học



Pricing Calculator

Ước tính các chi phí sẽ sử dụng các tài nguyên trong Azure



TCO

TCO Calculator

So sánh các chi phí để có thể biết Chi phí có thể tiết kiệm giữa việc sử dụng tài nguyên tại Datacenter và giải pháp Đám mây.



Microsoft Cost Management

Phân tích các chi phí, lọc chi phí, Và tạo ngân sách sử dụng tài nguyên

Xây dựng chiến lược quản trị đám mây với công cụ của Azure

Bài học bao gồm

Định nghĩa về quản trị đám mây

**Lên kế hoạch một chiến lược sử dụng
tài nguyên cloud**

Các dịch vụ quản trị

Các điểm chính của bài học

Định nghĩa về quản trị đám mây



Quản trị Cloud



- Các quy tắc(Rules)
- Các chính sách (Policies)
- Các tiêu chuẩn tuân thủ



- Kiểm soát các tài nguyên
- Bắt buộc thực thi các quy tắc, chính sách và tiêu chuẩn

Lên kế hoạch một chiến lược sử dụng tài nguyên cloud



Định nghĩa

Định nghĩa các công việc cần thiết để quản trị đám mây cho một công ty, tổ chức



Kế hoạch

Lên kế hoạch sử dụng các công cụ nào cần thiết để triển khai việc quản trị



Sẵn sàng áp dụng

Hiểu rõ những công cụ nào sẽ được sử dụng để thực hiện việc quản trị



Áp dụng

Thực hiện việc triển khai quản trị cho công ty(tổ chức) sử dụng một chiến lược quản trị

Các dịch vụ quản trị



Management groups và các Subscriptions

Tổ chức các subscriptions bên trong các cấu trúc phân cấp tài nguyên



Azure RBAC

Cung cấp truy cập vào các tài nguyên tại các phạm vi khác nhau



Các chính sách (Azure policies)

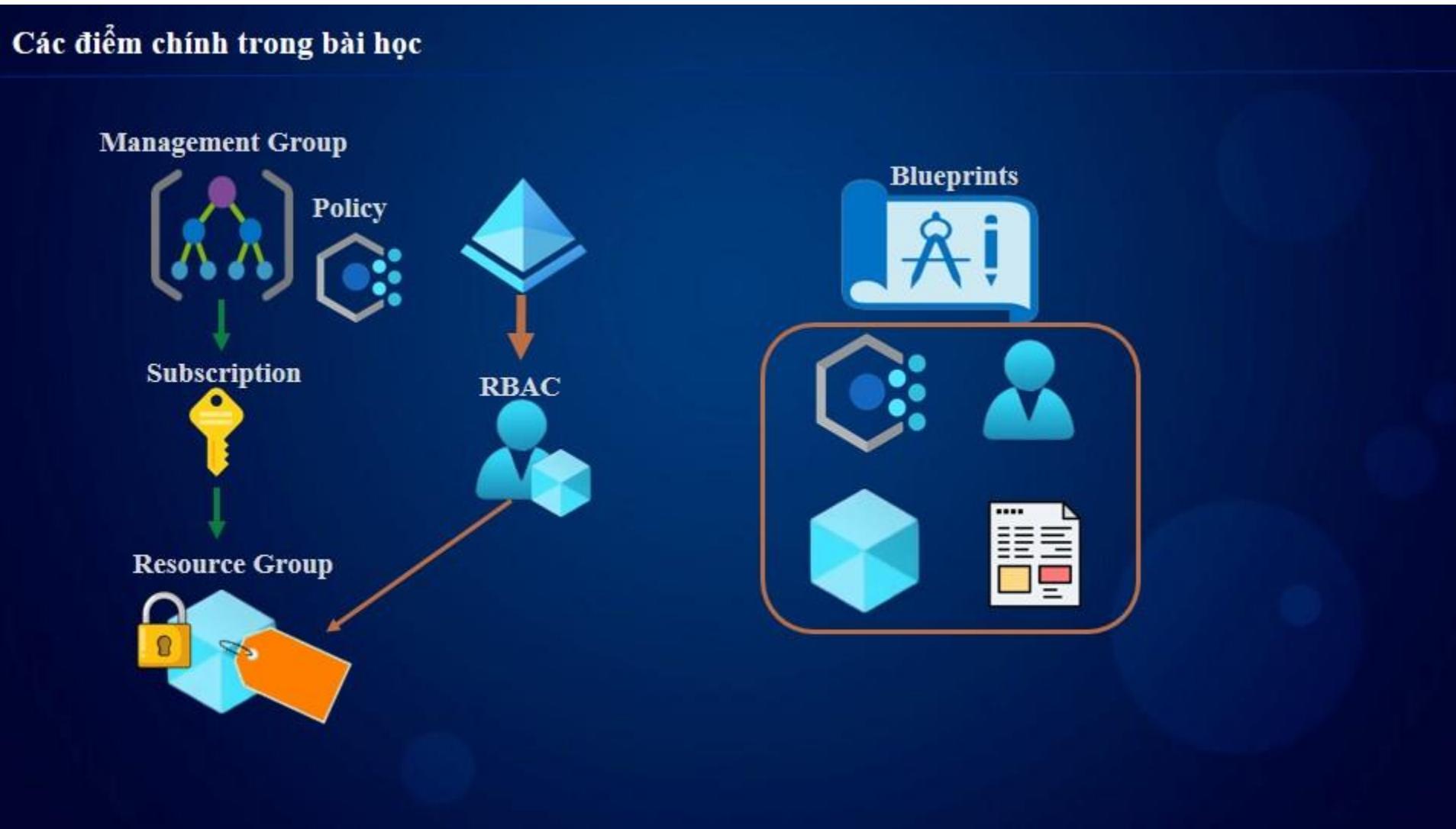
Thực hiện các chính sách để thực thi các tiêu chuẩn



Các khóa(locks) và thẻ tag

Khóa các tài nguyên để ngăn chặn, việc xóa tài nguyên và gắn thẻ tag cho các tài nguyên để phân loại tài nguyên

Các điểm chính trong bài học



Giới thiệu về chương này

Azure Active Directory

Azure Active Directory (AD)

Azure AD

Cơ bản về Identity and Access Management(IAM); Định nghĩa Azure AD, Azure AD tenants; Và kiến trúc Azure AD; So sánh Azure AD và Active Directory; Và tạo và chuyển đổi giữa các tenants.

Các đơn vị quản trị

Định nghĩa xác thực đa yếu tố(MFA) và self-service password reset(SSPR); Kích hoạt(Enable) MFA; Và Kích hoạt(Enable) SSPR

01

02

03

04

05

Chủ đề Identity (Danh tính)

Azure AD Users

Định nghĩa users, các loại users, các phương pháp tạo users, và kiến trúc; tạo và xóa users; Thực hiện bulk users update; Và mời các tài khoản khách (guest accounts).

Azure AD Groups

Định nghĩa groups, group và các kiểu membership, và role-based access control(RBAC); Tạo và xóa groups động; và cấp quyền truy cập các tài nguyên resources.

Azure AD Join

Định nghĩa Azure AD join, các thiết đặt thiết bị, và điều kiện truy cập; Join Windows 11 vào Azure AD

Các khái niệm về Azure Active Directory

Bài học bao gồm

Cơ bản về Quản lý Danh tính và Quyền truy cập Identity and Access Management(IAM)

Azure AD là gì?

Kiến trúc của Azure AD Tenant

Các tính năng của Azure AD

So sánh Active Directory và Azure AD

Các điểm chính của bài học

Azure Active Directory (AD)



Cá thể

Thực thể chưa được xác thực sẽ
tìm cách xác thực như một danh tính



Danh tính (Identity)

Một hồ sơ nhận dạng được xác thực
bằng cách sử dụng thông tin xác thực



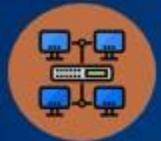
Cấp quyền truy cập

Các hành động được phép/
cấm đối với một danh tính thực hiện
việc truy cập

Azure AD là gì?



Azure Active
Directory
(Azure AD)



Identity and Access Management(IAM)

Dịch vụ quản lý danh tính và quyền truy cập dựa trên đám mây toàn cầu của Azure cung cấp kho lưu trữ danh tính



Tạo các tài nguyên danh tính

Tạo các users và groups



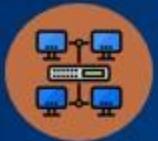
Quản lý bảo mật danh tính

Cho phép xác thực đa yếu tố(MFA), kiểm soát truy cập tài nguyên, và cung cấp việc kiểm soát dựa trên chính sách

Azure AD là gì?



Azure Active
Directory
(Azure AD)



Identity and Access Management(IAM)

Dịch vụ quản lý danh tính và quyền truy cập dựa trên đám mây toàn cầu của Azure cung cấp kho lưu trữ danh tính



Tạo các tài nguyên danh tính

Tạo các users và groups



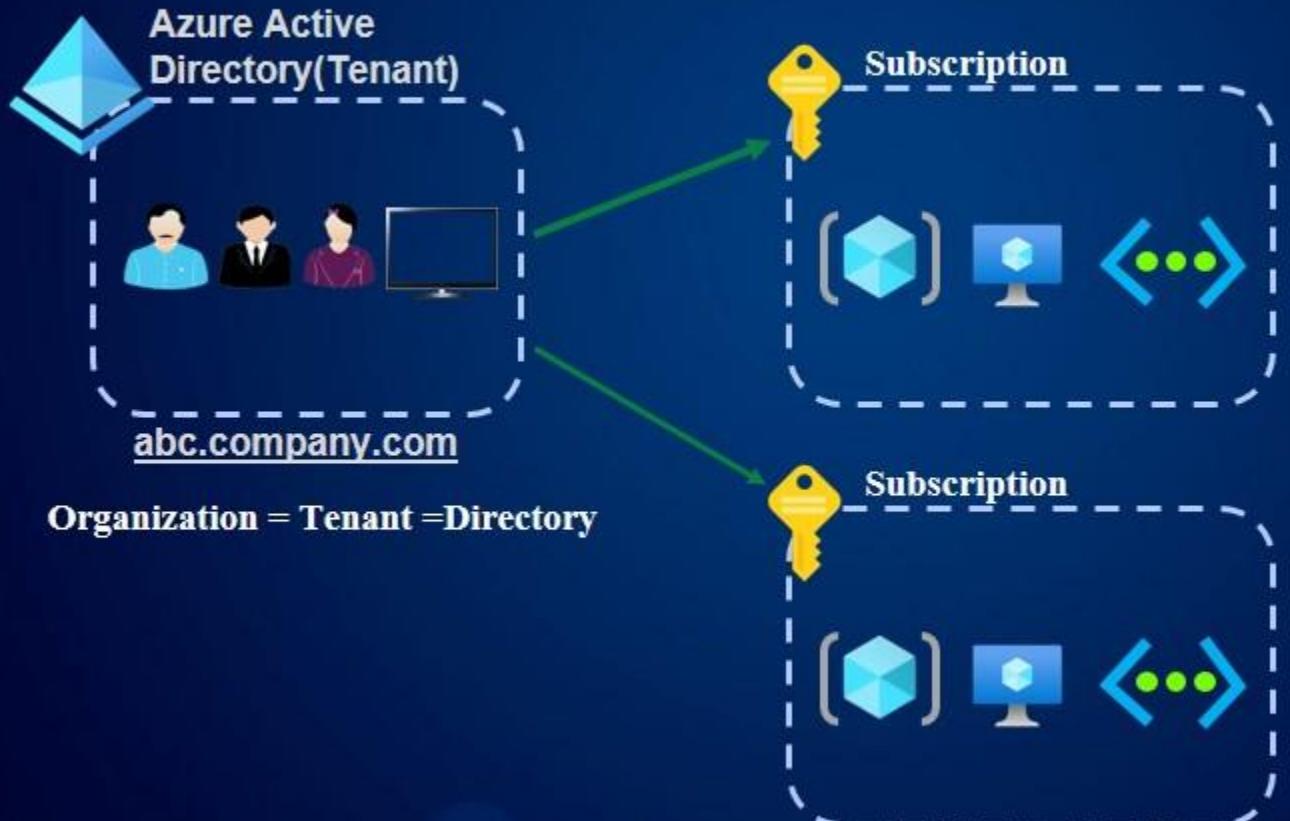
Quản lý bảo mật danh tính

Cho phép xác thực đa yếu tố(MFA), kiểm soát truy cập tài nguyên, và cung cấp việc kiểm soát dựa trên chính sách

Kiến trúc của Azure AD Tenant



Kiến trúc của Azure AD Tenant



Các tính năng của Azure AD



So sánh Active Directory và Azure AD



Active Directory

- ❖ Organizational units(OUs)
- ❖ Group Policy Objects(GPOs)
- ❖ Kerberos, LDAP, NTLM
- ❖ Phân cấp (Hierarchical)
- ❖ Hệ thống mạng lại chỗ (On-Premises)

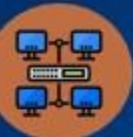
VS.

Azure AD



- ❖ Administrator units
- ❖ SAML, WS-Federation, OAuth
- ❖ Flat directory structure
- ❖ Cloud-based solution
- ❖ Toàn cầu (Global)

Các điểm chính trong bài học



Identity and Access Management(IAM)

Dịch vụ quản lý danh tính và quyền truy cập dựa trên đám mây toàn cầu của Azure cung cấp kho lưu trữ danh tính



Tạo các tài nguyên danh tính



Quản lý bảo mật danh tính

Cho phép xác thực đa yếu tố(MFA), kiểm soát truy cập tài nguyên, và cung cấp việc kiểm soát dựa trên chính sách

Quản lý Tenants

Bài học bao gồm

**Lên kế hoạch cho Organization
của chúng ta**

Thực hiện một Demo: Tạo một Tenant

Các điểm chính của bài học

Thiết kế Tenants

Lên kế hoạch thiết kế cho tenant
Của chúng ta sẽ hỗ trợ việc áp
dụng dễ dàng



Thực hiện Demo

1

Login vào
Azure Portal

2

Lên kế hoạch
Organization

3

Tạo Azure
Active
Directory
Tenant

Các điểm chính trong bài học



Tạo và Quản lý Users

Bài học bao gồm

Mô tả về Users

Các loại Users

Thực hiện một Demo: Tạo User

**Thực hiện một Demo: Quản lý các thuộc tính
của Users**

**Thực hiện một Demo: Sử dụng 1 danh sách users
để tạo nhiều users cùng 1 lúc**

**Thực hiện một Demo: Mời tài các khoản khách
Các điểm chính của bài học**

Mô tả về Users



Mô tả về Users



- Các thành viên(members) có các quyền(permissions) mặc định
- Các identities này là các đối tượng JSON
- Mỗi một user có thể có các role assignments
- Mỗi một user có thể có quyền sở hữu và quản lý tài nguyên

```
{  
    "accountEnabled": true,  
    "department": "Marketing",  
    "displayName": "John doe",  
    "employeeId": 03456789,  
    "givenName": "John",  
    "jobTitle": "Staff",  
    "objectType": "User",  
    "surname": "Doe",  
    "usageLocation": "US",  
    "userPrincipalName":  
        "john@example.onmicrosoft.com",  
    "userType": "Member"  
}
```

Các loại Users



Administrators

Users được cấp quyền
Administrator role



Members

Users thường trong
Azure AD



Khách (Guests)

Users khách (External users)
được mời vào Azure AD tenant

Thực hiện Demo

Các phương pháp trong việc tạo Users

Sử dụng Azure Portal

1

Vào dịch vụ Azure AD > select Users
> New user

Sử dụng Azure CLI

2

#Tạo user
az ad user create

Sử dụng PowerShell

3

#Tạo user
New-AzureADUser

Thực hiện Demo



Tạo/Add một User

Tạo một tài khoản member bên trong Azure AD.



Add nhiều user

Sử dụng một CSV file để add các users vào Azure AD.



Cập nhật(update) các thuộc tính (properties)

Cập nhật các thuộc tính để hiển thị user là nhân viên của phòng Marketing .



Mời một tài khoản khách

Mời một tài khoản khách vào Azure AD.

Các điểm chính trong bài học



Loại User



Administrator, member,
và guests accounts

Role Assignment



Định nghĩa các quyền truy cập
(access permissions)

Đối tượng chủ sở hữu



Apps, devices, groups, và
tài nguyên được sở hữu

Thực hành tạo và xóa Azure AD users trong Azure Portal

Trong tình huống của bài thực hành này, bạn là một senior systems administrator, và bạn phải xử lý một việc là hỗ trợ một số help desk users.

Và bạn sẽ tạo và quản lý các Azure AD users trong Azure Portal.

Và việc này sẽ giúp các users có thể tìm hiểu một số kiến thức cơ bản, vì vậy họ có thể thực hiện role của họ.

- **Bước 1**
Tạo Azure AD Users
- **Bước 2**
Sửa đổi AD Users
- **Bước 3**
Cấm(block), thu hồi quyền truy cập(Revoke)
Azure AD Users
- **Bước 4**
Xóa Azure AD Users

Thực hành tự động hóa tạo và xóa Azure AD users trong Azure Portal

Trong tình huống của bài thực hành này, bạn là một systems administrator, làm việc cho một công ty có nhiều dự án theo thời vụ. Vì vậy có thể cứ hàng tháng, công ty bạn sẽ có một dự án mới và khi có một dự án mới, thì có thể sẽ có một số nhân viên thời vụ tham gia vào dự án. Do đó bạn cần tạo các users cho các nhân viên mới, có thể là 5, 10 hay 15 users, và setup các security groups cho dự án. Hiện tại bạn đang thực hiện việc này bằng phương pháp thủ công. Tuy nhiên trong bài thực hành này bạn sẽ thực hiện việc tự động hóa để tạo ra nhiều users cùng một lúc như là chúng ta làm một môi trường công việc thực tế của một system admin.

- **Bước 1**
Tạo nhiều Users cùng một lúc
- **Bước 2**
Xóa các users cùng một lúc
- **Bước 3**
Tạo group và add users vào group



CSV file

Tạo và Quản lý Groups

Bài học bao gồm

Mô tả về Groups

Các trường hợp áp dụng trong công việc

Thực hiện Demo: Tạo một Group

Thực hiện Demo: Quản lý Group Membership

Các điểm chính của bài học

Mô tả về Groups



Chủ sở hữu(Owner) và Thành viên(Member)

Một owner của một nhóm(group) hoặc một member của một nhóm group



HR Group



Loại Group

Một security group hoặc một Microsoft 365 group



Jose

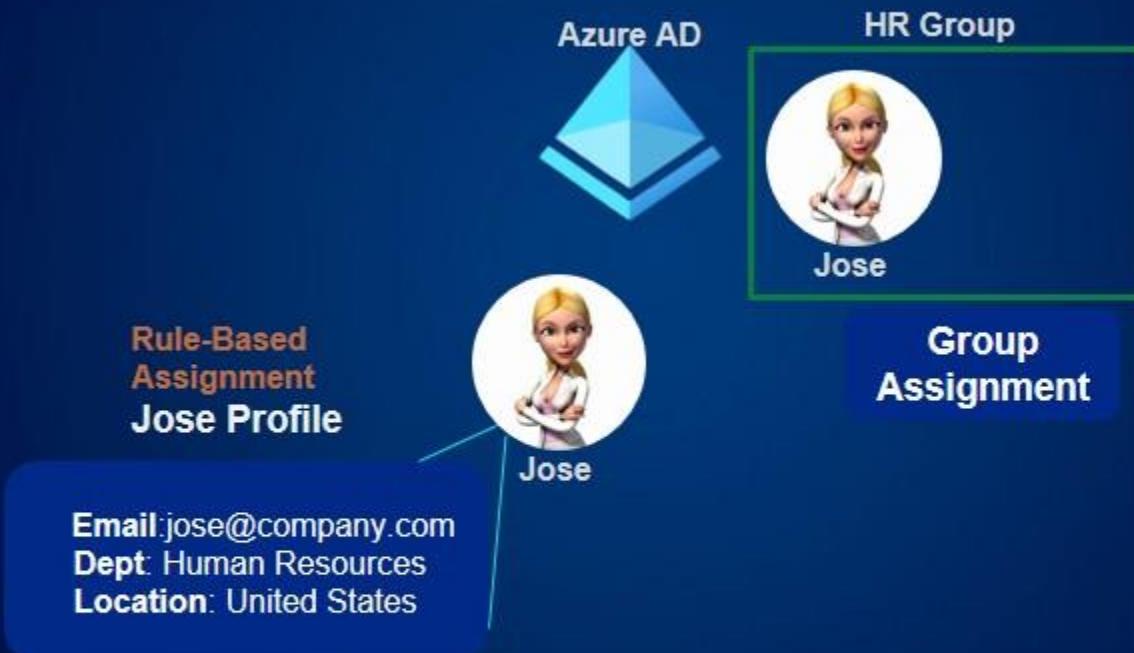
Michael



Loại Membership

Assigned, dynamic user, hoặc dynamic device

Các trường hợp áp dụng trong công việc



Thực hiện Demo

1

Login vào
Azure Portal

2

Tạo Group

Các điểm chính trong bài học

Group Types

Security

Security Group được sử dụng để quản lý quyền truy cập vào các tài nguyên được chia sẻ(shared) cho một nhóm Group của các users

Microsoft 365

Microsoft 365 được sử dụng để cho phép các users truy cập vào các Shared mailbox, calendar, files, VV

Membership Types

Assigned

Users được lựa chọn là một thành viên của một nhóm

Dynamic Users

Membership rules được tạo ra và tự động add các users vào nhóm thông qua các thuộc tính của user

Tạo Administrative Units

Bài học bao gồm

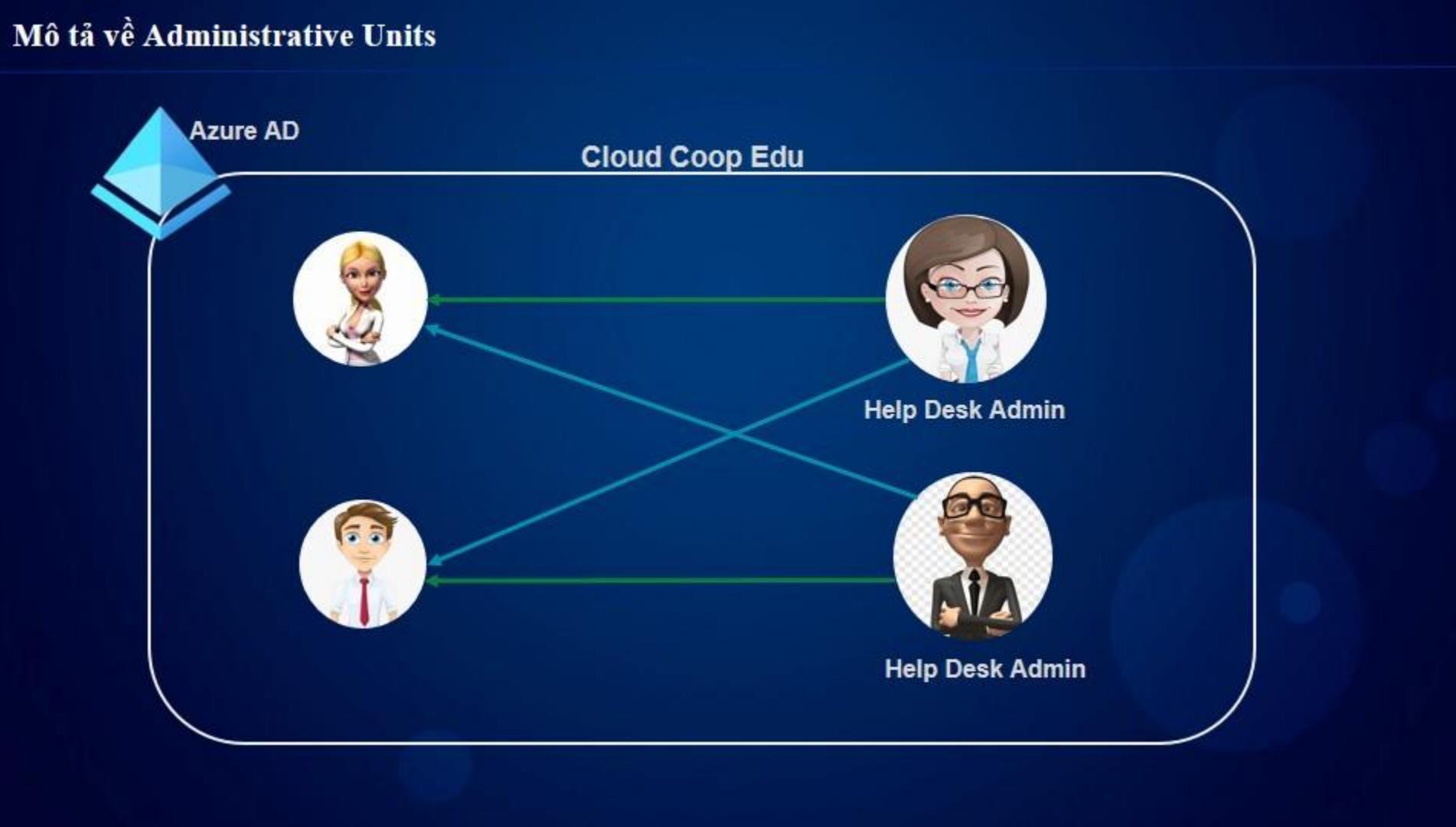
Mô tả về Administrative Units

Các trường hợp áp dụng trong công việc

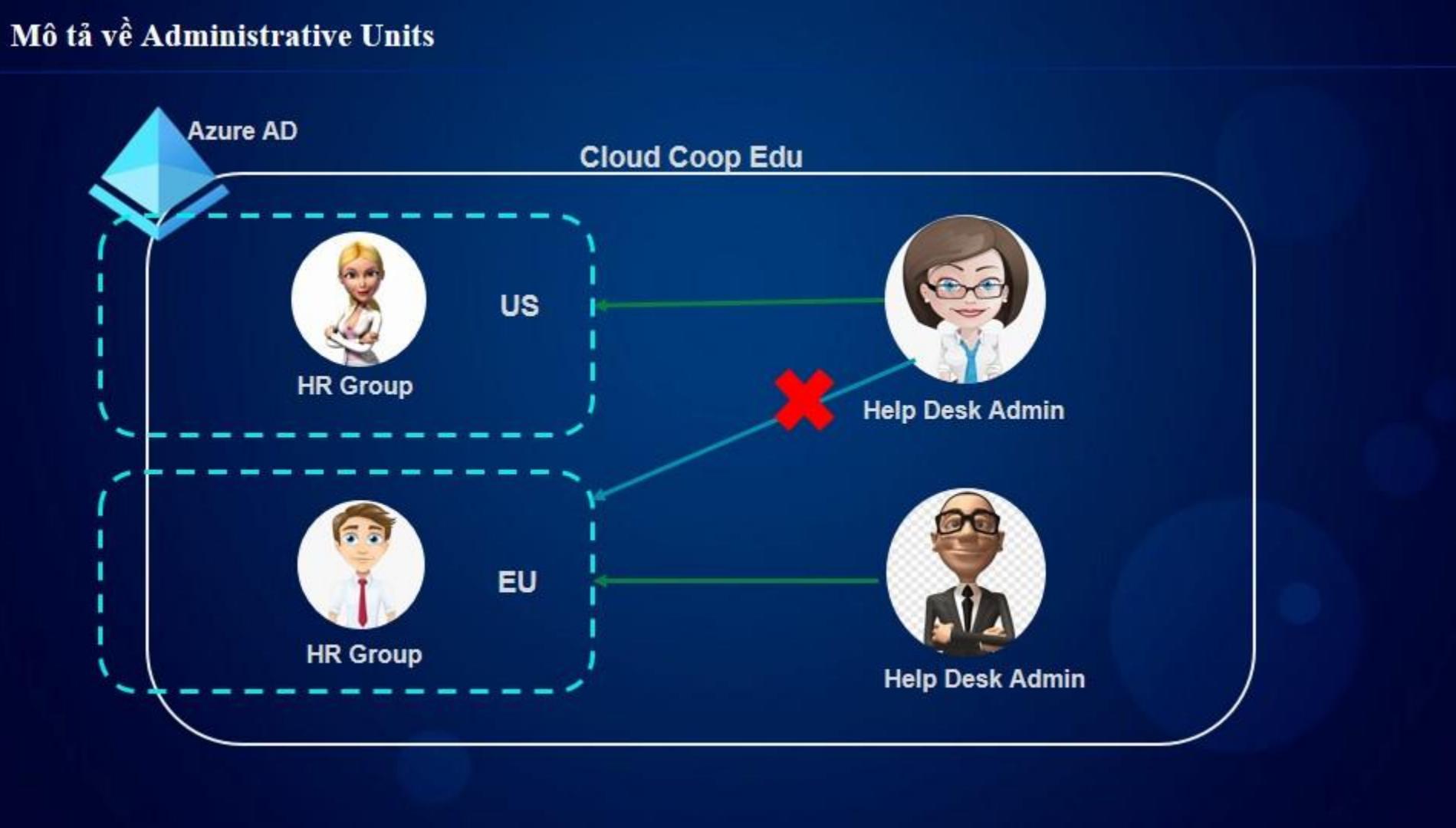
Thực hiện một Demo: Tạo Administrative Units

Các điểm chính của bài học

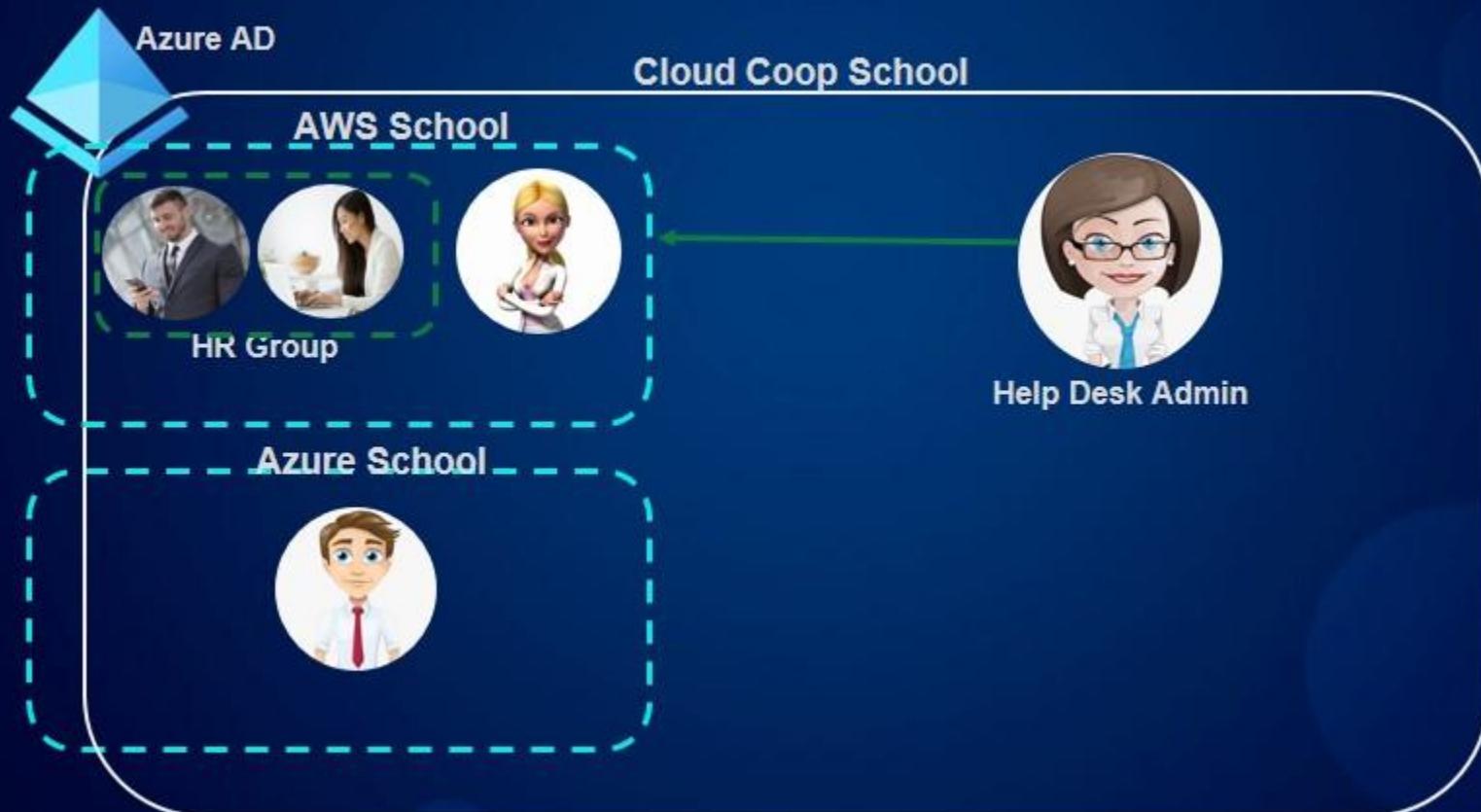
Mô tả về Administrative Units



Mô tả về Administrative Units

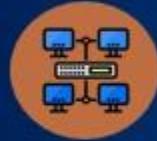


Các trường hợp áp dụng trong công việc



Thực hiện một Demo: Tạo Administrative Units

Lên kế hoạch cho tổ chức organization



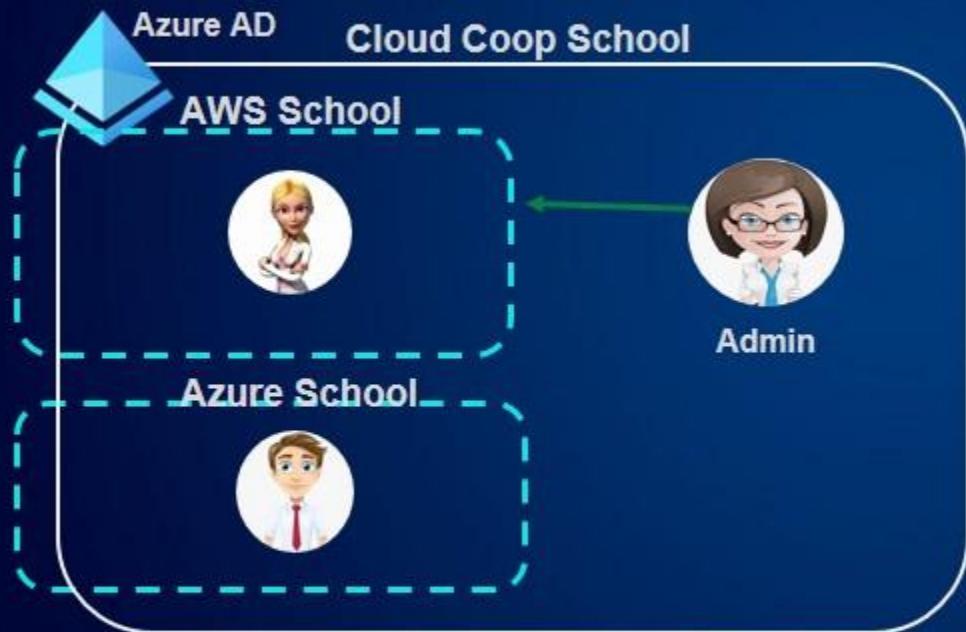
Lên kế hoạch cho organization và đánh giá nhu cầu của tổ chức để xác định giá trị mà administrative units có thể cung cấp để quản lý danh tính, như nhóm(groups) và người dùng(users)

Tạo một Administrative Unit



Tạo một Adminstrative unit để chia organization một cách hợp lý và cho phép xác định phạm vi

Các điểm chính của bài học



Mục đích sử dụng Administrative Units



Là một tài nguyên Azure AD cho việc cung cấp một vùng chứa logic cho các đối tượng Azure AD

Lợi ích trong sử dụng Administrative Units



Cho phép bạn kiểm soát một phạm vi của các users quản trị hệ thống



Các trường hợp sử dụng

Administrative Units dựa trên các vị trí địa lý, các phòng ban, hoặc các tổ chức con(sub organizations) của một tổ chức cha(parent organization)

Thực hành tạo một Group và Add một User vào Azure Active Directory

Trong tình huống của bài thực hành này, công ty của bạn mới thành lập phòng nghiên cứu RD Dept. Và bổ nhiệm bạn sẽ là một trưởng phòng của phòng này và bạn sẽ quản lý các thành viên của phòng. Các thành viên sẽ có các quyền(permissions), license assignments, và các quyền truy cập trong một phạm vi theo role của họ. Một trong các cách hiệu quả nhất để thực hiện việc này là tạo một group trong Azure AD, sau đó bạn có thể áp dụng các phân quyền mà bạn muốn, và cấu hình tự động áp dụng cho các thành viên. Mục tiêu chính của bạn là tạo một nhóm cho phòng RD của bạn và add các thành viên vào group

Các bước thực hiện bài thực hành



Login vào
Azure portal



Vào dịch vụ
Azure AD



Tạo một AAD
Group



Add một User
vào Group

Cấu hình SSPR

Bài học bao gồm

Mô tả về SSPR

Quá trình SSPR

Các phương pháp xác thực(Authentication)

Cân nhắc việc sử dụng SSPR

Thực hiện một Demo: Enable SSPR trong Azure AD

Các điểm chính của bài học

Mô tả về SSPR

Azure AD

Phương pháp đổi mật khẩu(Reset Password) cũ



- Kém hiệu quả
- Tăng chi phí quản trị admin

Mô tả về SSPR



- Cho phép(Enable) users tự thay đổi password
- Tăng hiệu quả công việc
- Giảm các công việc quản trị admin

Quá trình SSPR



Định vị
(Localization)

Xác minh
(Verification)

Xác thực
(Authentication)

Đặt lại mật
khẩu
(Password reset)

Thông báo
(Notification)

Các phương pháp xác thực(Authentication)



Mobile App

Xác thực thông qua ứng dụng. VD:
Microsoft Autheticator application



Mobile App Code

Xác thực thông qua mã thời gian.
VD: Microsoft Autheticator application



Email

Xác thực thông qua Email.
VD: Microsoft gửi mã xác thực
vào một địa chỉ email



Mobile Phone

Xác thực thông qua điện thoại di động,
VD: Gọi điện đến hoặc gửi tin nhắn SMS cung cấp
một mã code



Điện thoại bàn

Xác thực thông qua điện thoại bàn, VD:
tự giúp nhập user và nhấn Phím #



Các câu hỏi bảo mật

Xác thực thông qua việc trả lời các câu hỏi bảo mật

Cân nhắc việc sử dụng SSPR

Ghi nhớ

Cho phép(Enable) và quản lý SSPR thông qua Azure AD Groups

Các phương pháp Được yêu cầu

Một hoặc nhiều các
phương pháp xác thực
được yêu cầu sử dụng
cho SSPR



SSPR cho Admins

Các câu hỏi bảo mật
không được sử dụng
cho admins. Mặc định
admins phải đăng ký
xác thực đa yếu tố
MFA



Đòi hỏi giấy phép (Licences)

Sử dụng SSPR
cần phải có
License như Azure AD
P1 hoặc P2 cho
Business, hoặc
Microsoft 365

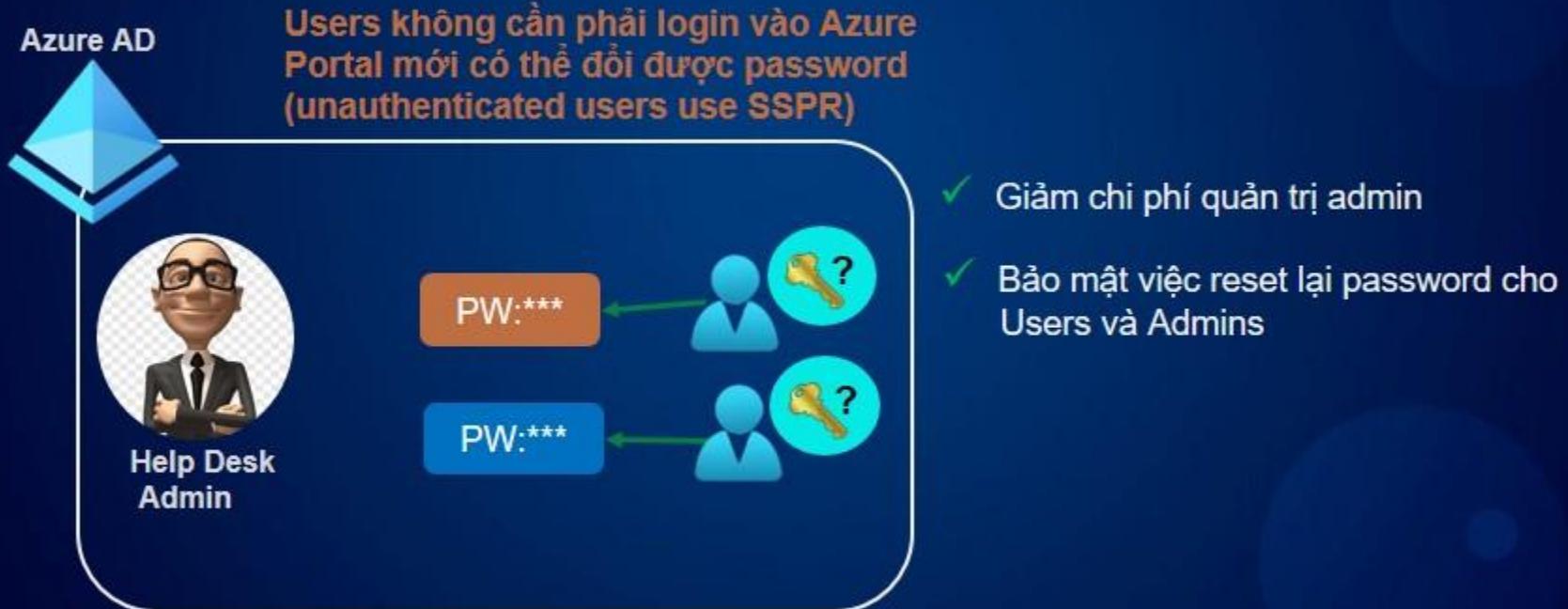


Thực hiện một Demo: Enable SSPR trong Azure AD



Các điểm chính trong bài học

Self-Service Password Reset(SSPR)



Quản lý Azure AD Device

Bài học bao gồm

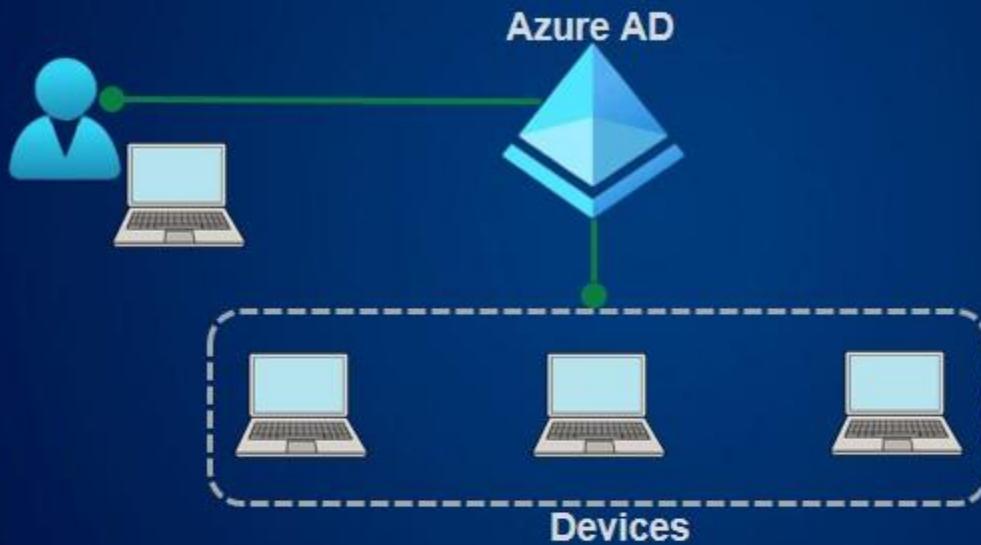
Cơ bản về Device Identity

Các tùy chọn đăng ký device

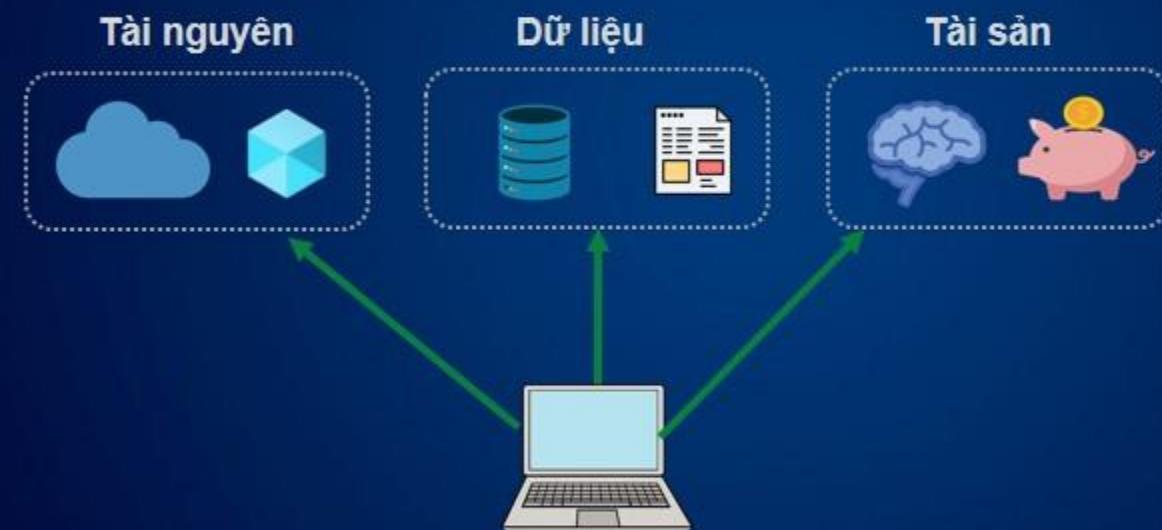
Thực hiện một Demo: Quản lý Devices

Các điểm chính của bài học

Cơ bản về Device Identity



Cơ bản về Device Identity



Các tùy chọn đăng ký device

Cách đăng ký các Thiết Bị(Devices)



Đăng ký Azure AD

Tùy chọn ít hạn chế nhất, cho phép mang theo thiết bị của riêng bạn (BYOD) bằng tài khoản Microsoft hoặc tài khoản cục bộ cá nhân. Hỗ trợ Windows 10, IOS, IpadOS, Android, và macOS.



Azure AD Joined

Thiết bị thuộc quyền sở hữu của tổ chức và truy cập Azure AD thông qua tài khoản công việc. Những danh tính này chỉ tồn tại trên đám mây. Hỗ trợ từ windows 10 và Windows server 2019 trở lên.



Azure AD Hybrid Joined

Giống với Azure AD Joined; Tuy nhiên, những danh tính thiết bị này tồn tại trong môi trường mạng nội bộ và trong đám mây. Hỗ trợ Windows 7, 8.1, 10 và windows server 2008 và các bản thấp hơn.

Thực hiện Demo

1

Login vào
Azure Portal

2

Join và đăng
Ký các
thiết bị

Các điểm chính trong bài học

Device Identity



- ✓ Đơn giản hóa thủ tục cho việc add và quản lý các thiết bị(devices)
- ✓ Cải thiện trải nghiệm của người dùng trên các thiết bị
- ✓ Đăng nhập một lần Single sign-on (SSO) cho mọi thiết bị đã đăng ký(registered) hoặc đã tham gia(joined)

Tìm hiểu về Roles trong Azure

Bài học bao gồm

Mô tả về RBAC

Mô tả về Azure Roles

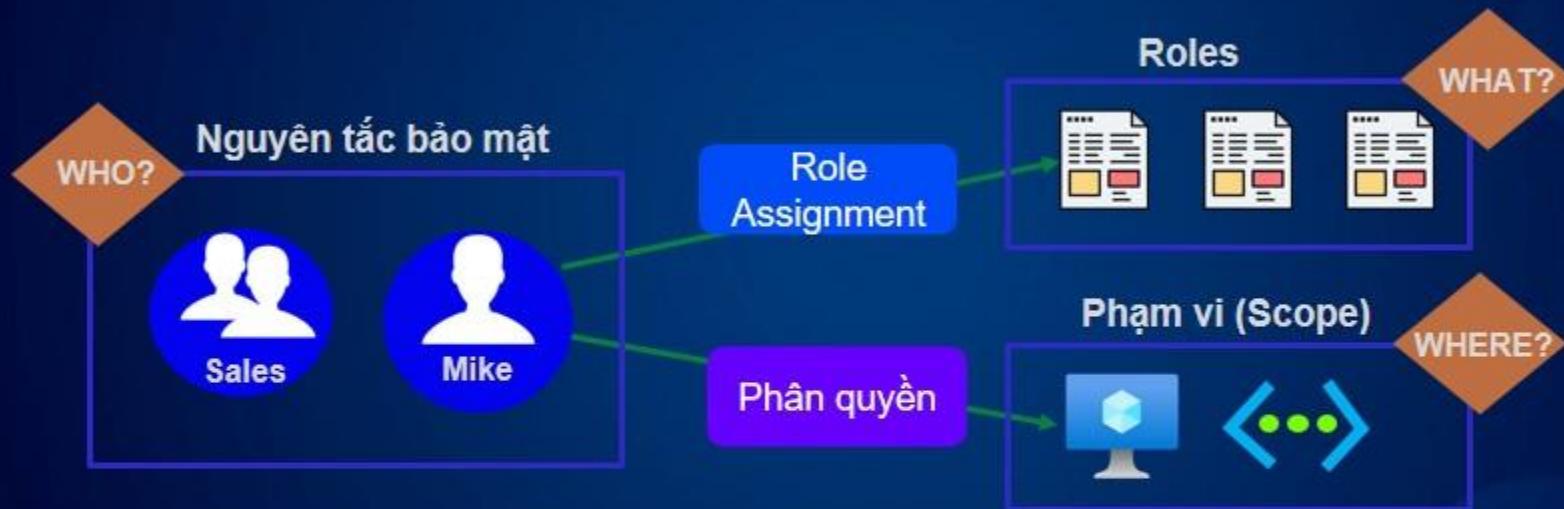
Mô tả về Azure AD Roles

So sánh Azure Roles và Azure AD roles

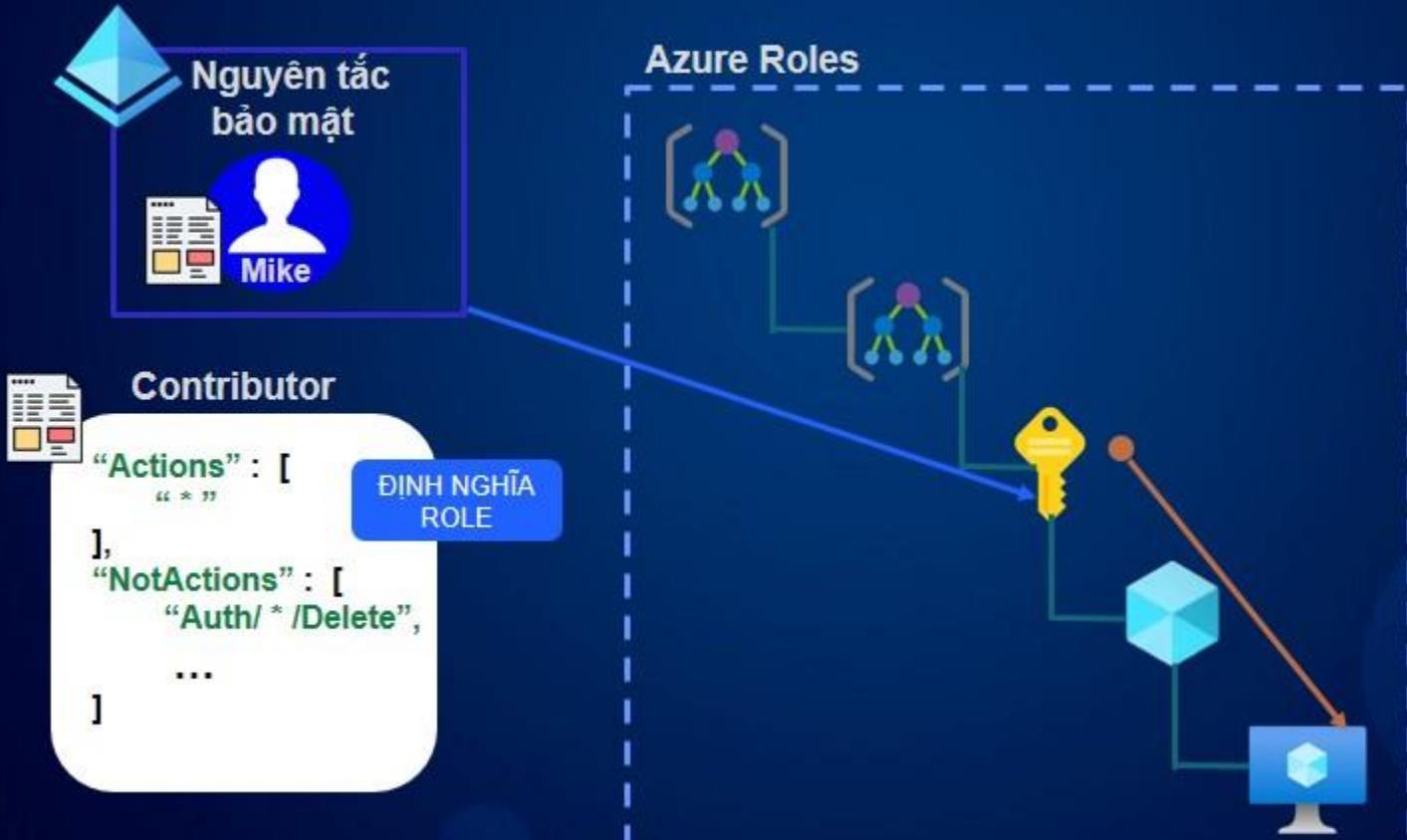
Kiến trúc RBAC

Các điểm chính của bài học

Mô tả về RBAC



Mô tả về Azure Roles



Mô tả về Azure Roles

**Chủ sở hữu
(Owner)**

Mô tả về Azure Roles

Toàn quyền truy cập(Full access) vào các tài nguyên và ủy quyền truy cập

Quyền đọc
(Reader role)

Mô tả về Azure Roles

Toàn quyền truy cập(Full access) vào các tài nguyên và phân quyền truy cập

Contributor role

Chỉ có thể xem các tài nguyên

Mô tả về Azure Roles

Toàn quyền truy cập(Full access) vào các tài nguyên và phân quyền truy cập

Có thể tạo và quản lý các tài nguyên

Chỉ có thể xem các tài nguyên

User Access Administrator role

Mô tả về Azure Roles

Toàn quyền truy cập(Full access) vào các tài nguyên và phân quyền truy cập

Có thể tạo và quản lý các tài nguyên

Chỉ có thể xem các tài nguyên

Có thể phân quyền truy cập vào các tài nguyên

Mô tả về Azure AD Roles



Mô tả về Azure AD Roles

Global Administrator

Mô tả về Azure AD Roles

Có thể quản lý Azure
AD resources

Billing Administrator

Mô tả về Azure AD Roles

Có thể quản lý Azure
AD resources

Có thể thực hiện
các công việc quản lý
hóa đơn chi phí sử
dụng các tài nguyên
Azure

User Administrator

Mô tả về Azure AD Roles

Có thể quản lý Azure
AD resources

Có thể thực hiện
các công việc quản lý
hóa đơn chi phí sử
dụng các tài nguyên
Azure

Có thể quản lý users
và groups

Helpdesk
Administrator

Mô tả về Azure AD Roles

Có thể quản lý Azure
AD resources

Có thể thực hiện
các công việc quản lý
hóa đơn chi phí sử
dụng các tài nguyên
Azure

Có thể quản lý users
và groups

Có thể reset
passwords cho users

So sánh Azure Roles và Azure AD roles

Azure Roles

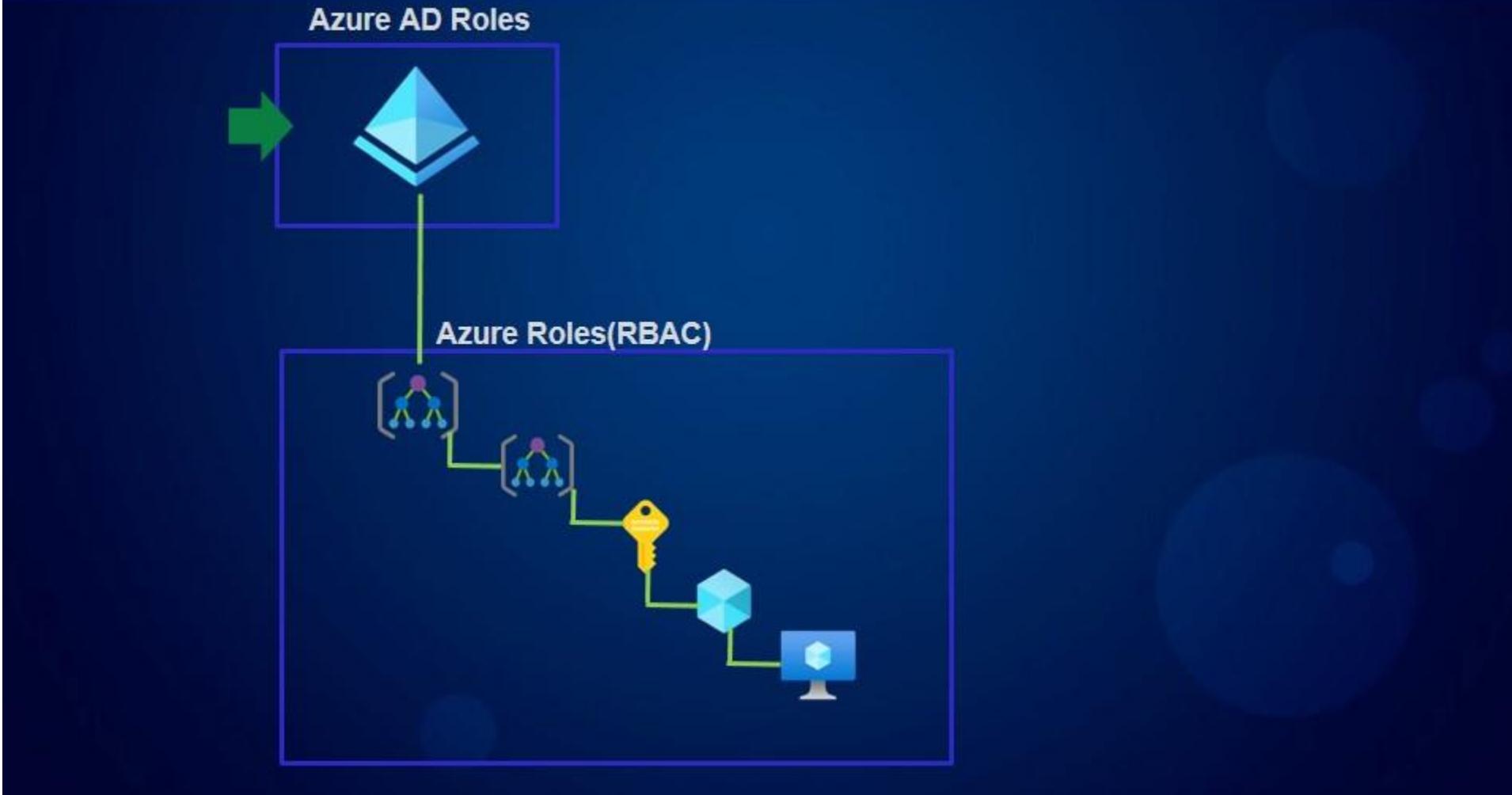
- Quản lý quyền truy cập vào các tài nguyên Azure
- Phạm vi có thể hoạt động tại nhiều cấp độ phạm vi
- Hỗ trợ cho phép tùy chọn roles
- Các roles chính:
 - * Owner
 - * Contributor
 - * Reader
 - * User Access Administrator

Azure AD Roles

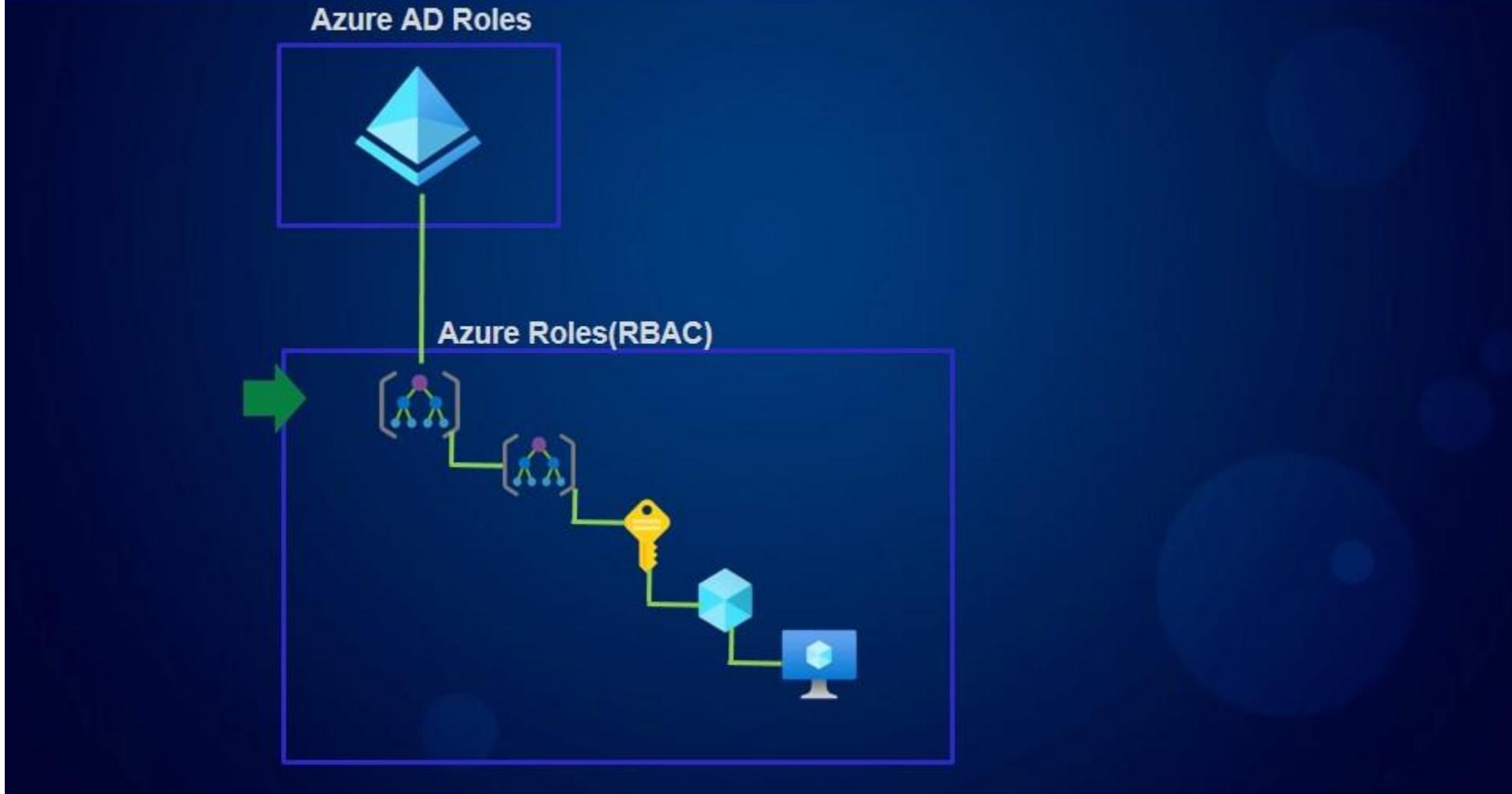
- Quản lý quyền truy cập vào các tài nguyên Azure
- Phạm vi có thể hoạt động tại cấp độ tenant
- Hỗ trợ cho phép tùy chọn roles
- Các roles chính:
 - * Global Administrator
 - * User Administrator
 - * Billing Administrator

Vs.

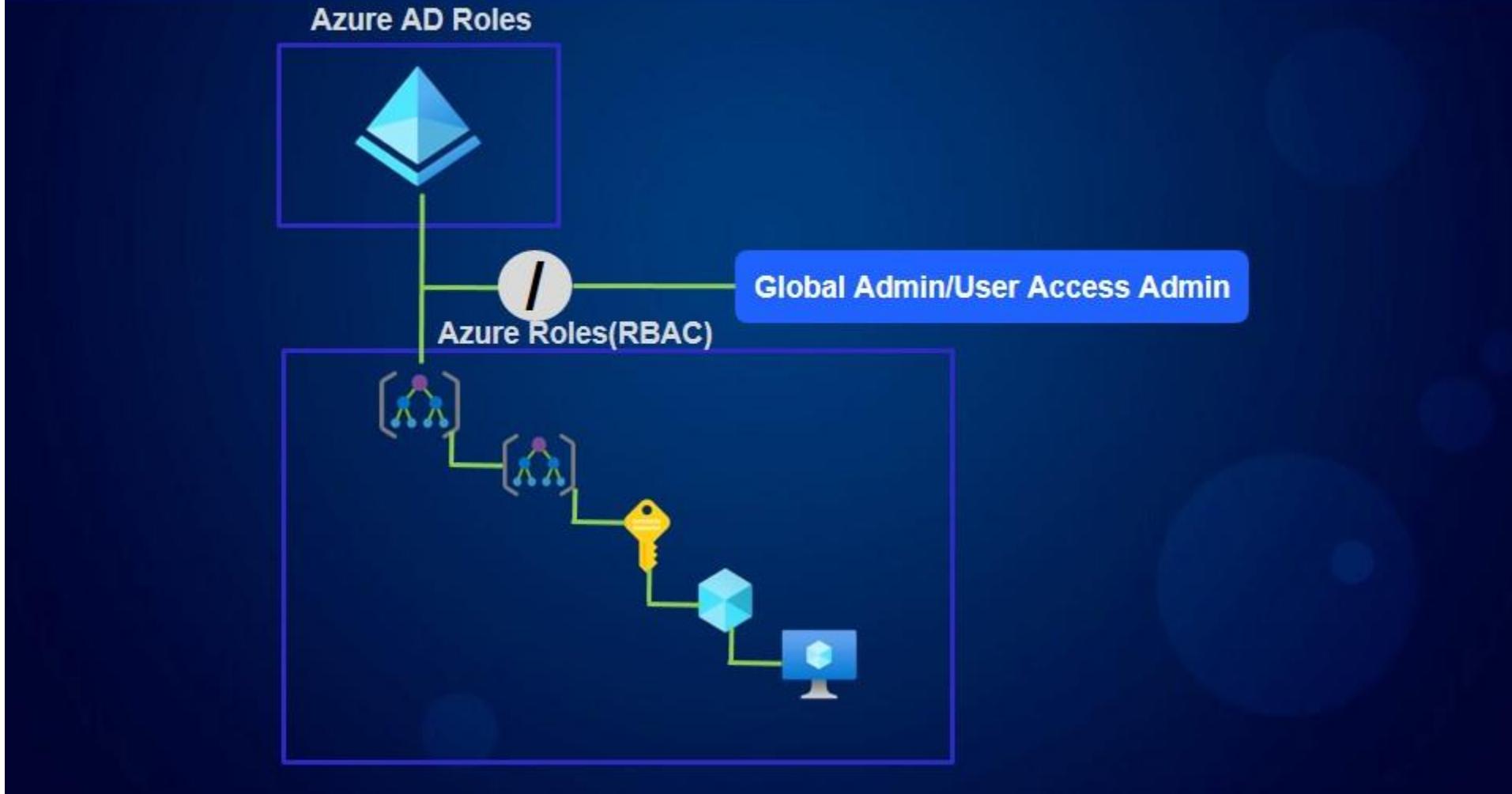
Kiến trúc RBAC



Kiến trúc RBAC



Kiến trúc RBAC



Các điểm chính trong bài học

Azure Roles

- Quản lý quyền truy cập vào các tài nguyên Azure
- Được gọi là Azure RBAC
- Built-in roles
- Roles tùy chọn(Custom roles)
- Phạm vi(Scope) tại management groups, subscriptions, resource groups, và resources

Azure AD Roles

- Quản lý quyền truy cập vào các tài nguyên Azure
- Built-in roles
- Roles tùy chọn(Custom roles)
- Phạm vi(Scope) tại Azure AD tenant

Vs.

Phân quyền truy cập vào các tài nguyên Azure

Bài học bao gồm

Giải thích về Azure RBAC

Tìm hiểu về các định nghĩa Roles

Mô tả về Azure AD Roles

Thuộc tính bổ sung Additive Property

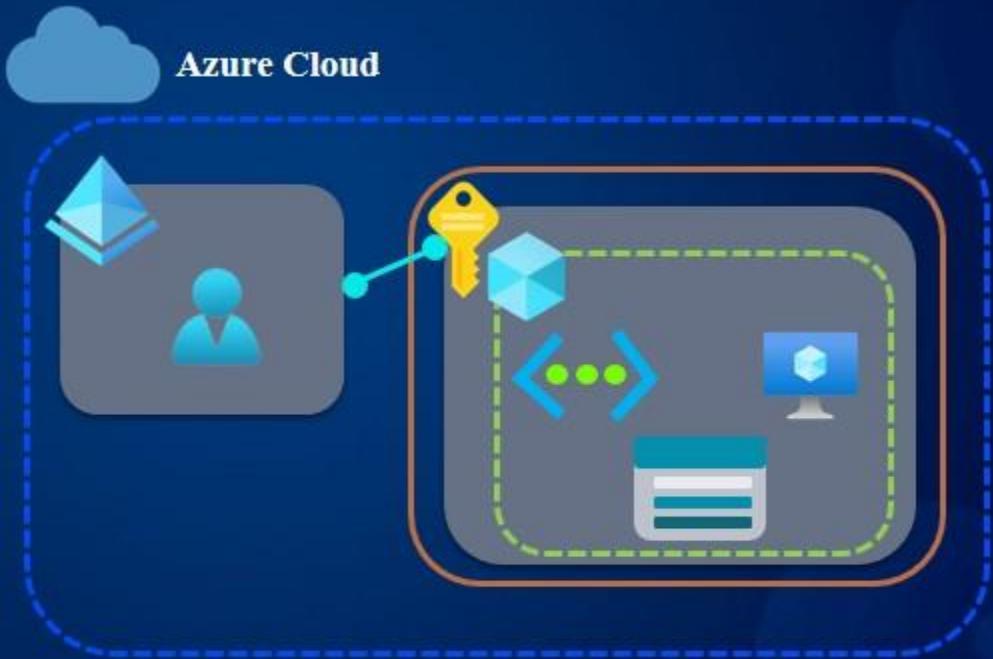
Demo: Cấp quyền truy cập

Các điểm chính của bài học

Giải thích về Azure RBAC

Hệ thống xác thực và quyền truy cập

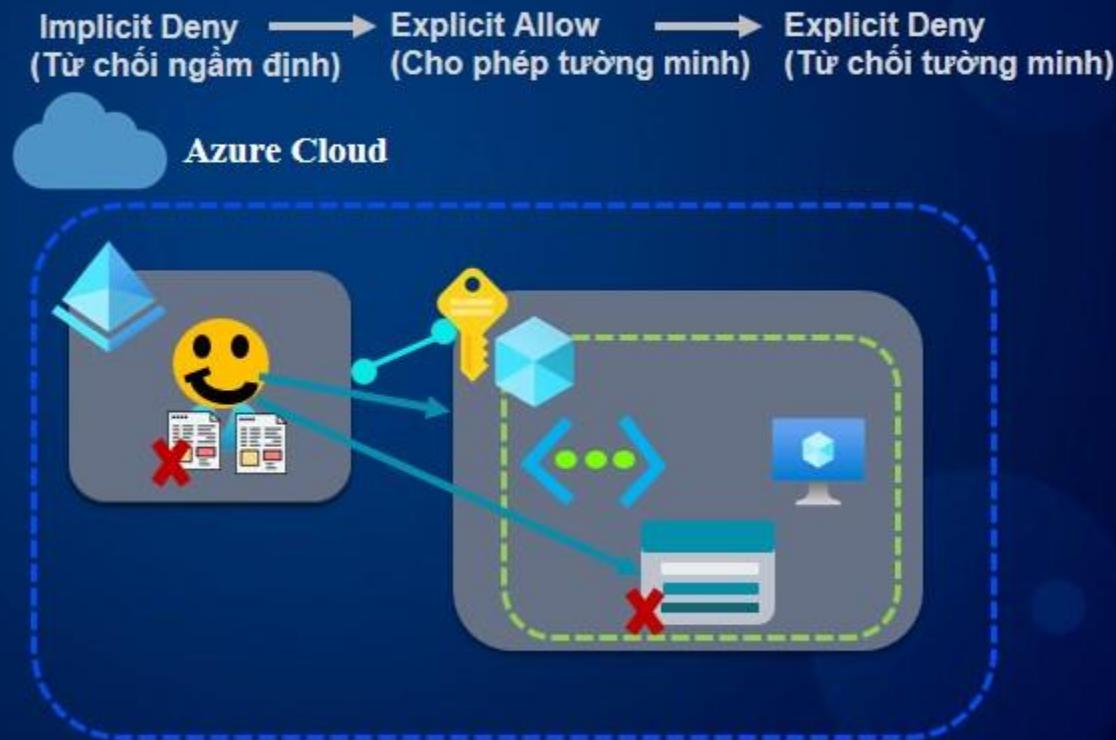
- Nguyên tắc bảo mật (Who?)
- Định nghĩa Role(What?)
- Phạm vi(where?)



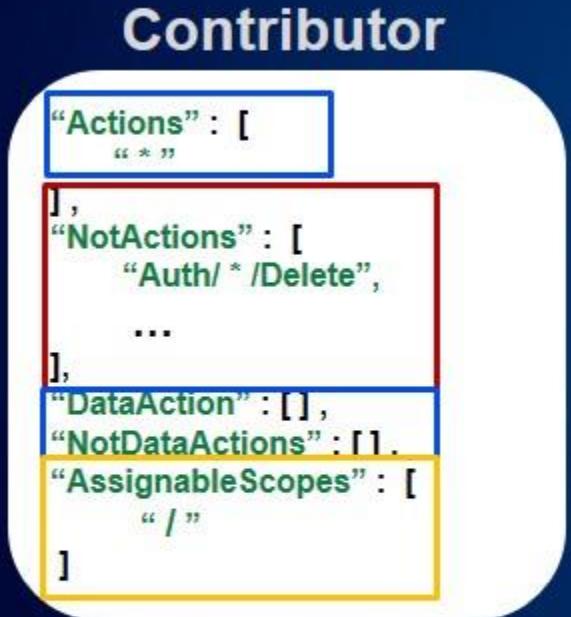
Tìm hiểu về các định nghĩa Roles

Hệ thống xác thực và quyền truy cập

- Nguyên tắc bảo mật (Who?)
- Định nghĩa Role(What?)
- Phạm vi(where?)



Mô tả về Azure AD Roles



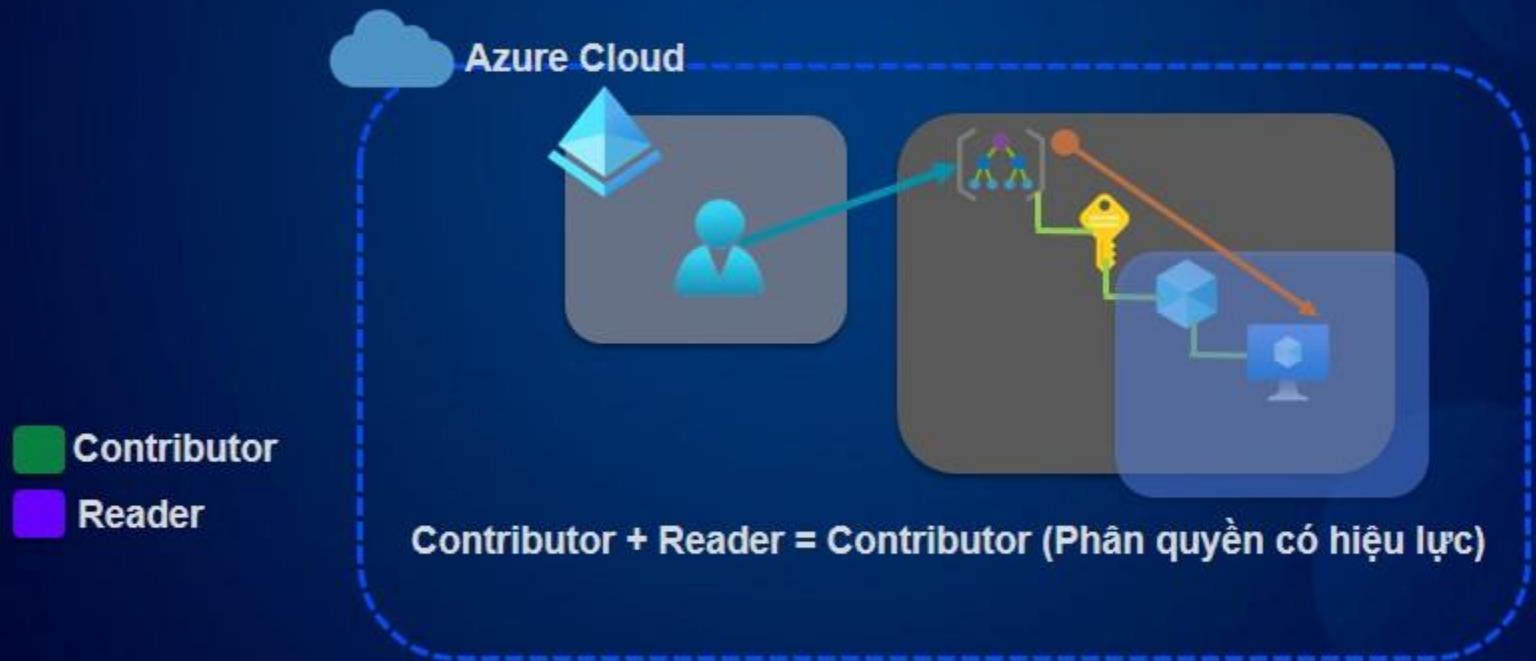
Các hành động

Không được có
các hành động

Các quyền chung

Thuộc tính bổ sung Additive Property

Roles Chồng chéo



Thực hiện Demo

1

Chọn User



Chọn ai(who) cần truy
cập vào tài nguyên Azure

2

Chọn Role



Chọn cấp cho người dùng
role để họ có quyền truy cập

3

Chọn Phạm Vi

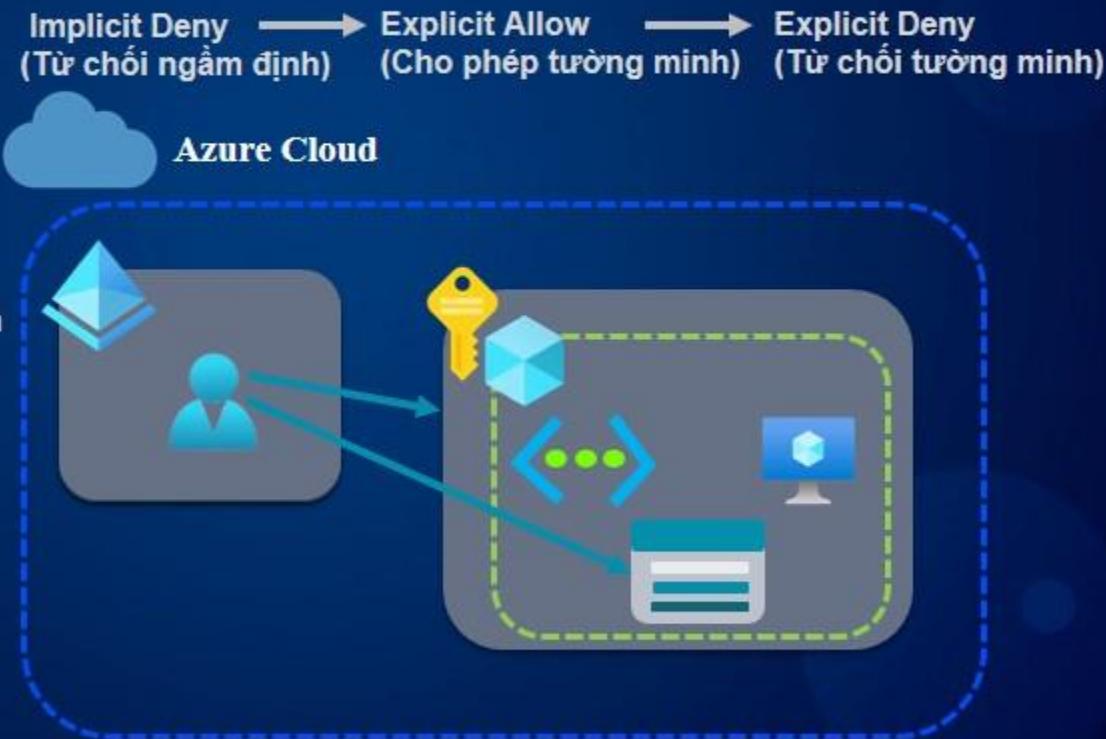


Chọn phạm vi mà user cần
các quyền truy cập.

Các điểm chính của bài học

Hệ thống xác thực và quyền truy cập

- ✓ Cung cấp cho các danh tính quyền truy cập vào các tài nguyên Azure
- ✓ Roles là tập hợp của các quyền
- ✓ Có một hệ thống phân cấp phạm vi



Bài học bao gồm

Mô tả các Roles tùy chỉnh

Tạo các định nghĩa Role

Demo: Tạo Roles tùy chỉnh

Các điểm chính của bài học

Mô tả về Azure AD Roles

Virtual Machine Contributor

- Định nghĩa role tùy chỉnh
- Không có Built-in role đáp ứng được các yêu cầu
- User Access Administrator hoặc Owner role(chủ sở hữu) cho tài khoản

```
“Actions” : [  
    “Compute/virtualMachine/* ”  
],  
“NotActions” : [],  
“DataAction” : [],  
“NotDataActions” : [],  
“AssignableScopes” : [  
    “/”  
]
```

Mô tả về Azure AD Roles

Virtual Machine Contributor

- Định nghĩa role tùy chỉnh
- Không có Built-in role đáp ứng được các yêu cầu
- User Access Administrator hoặc Owner role(chủ sở hữu) cho tài khoản

```
“Actions” : [  
    “Compute/virtualMachine/* ”  
],  
“NotActions” : [],  
“DataAction” : [],  
“NotDataActions” : [],  
“AssignableScopes” : [  
    “/”  
]
```

Tạo các định nghĩa Role

Custom Role

```
“Actions” : [  
    “Compute/*/read”,  
    “Compute/virtualMachines/  
        restart/action”  
],
```

```
“NotActions” : [],  
“DataAction” : [],  
“NotDataActions” : [],  
“AssignableScopes” : [  
    “/”  
]
```

Tạo các định nghĩa Role

Custom Role

```
“Actions” : [  
    “Compute/*/read”,  
    “Compute/virtualMachines/  
        restart/action”
```

```
],  
“NotActions” : [],  
“DataAction” : [],  
“NotDataActions” : [],  
“AssignableScopes” : [  
    “/”  
]
```

Tạo các định nghĩa Role

Custom Role

```
“Actions” : [  
    “Compute/*/read”,  
    “Compute/virtualMachines/  
    restart/action”]  
,  
“NotActions” : [],  
“DataAction” : [],  
“NotDataActions” : [],  
“AssignableScopes” : [  
    “/”  
]
```

Tạo các định nghĩa Role

Custom Role

```
“Actions” : [  
    “Compute/*/read”,  
    “Compute/virtualMachines/  
    restart/action”]  
,  
“NotActions” : [],  
“DataActions” : [],  
“NotDataActions” : [],  
“AssignableScopes” : [  
    “/”  
]
```

Mô tả về Azure AD Roles

Custom Role

```
“Actions” : [  
    “ Compute/*/read ”,  
    “ Compute/virtualMachines/  
        restart/action”  
],  
“NotActions” : [],  
“DataAction” : [],  
“NotDataActions” : [],  
“AssignableScopes” : [  
    “ / ”  
]
```

Thực hiện Demo

1

Tạo một Role tùy chỉnh



Định nghĩa một role trong JSON.

2

Cấp Role



Gán một role tùy chỉnh cho một user

3

Kiểm tra Role Assignment



Kiểm tra role assignment của user

Các điểm chính của bài học

Custom Roles

- Cung cấp cho các danh tính(identities) quyền truy cập vào các tài nguyên Azure
- Roles là tập hợp của các quyền
- Phạm vi phân cấp cho role assignments
- Định nghĩa role tùy chọn
- Không có một built-in roles nào có thể đáp ứng được với các nhu cầu của chúng ta
- User Access Administrator hoặc chủ sở hữu Owner role cho tài khoản

Tìm hiểu về Storage Accounts

Bài học bao gồm

Mô tả về Storage Accounts

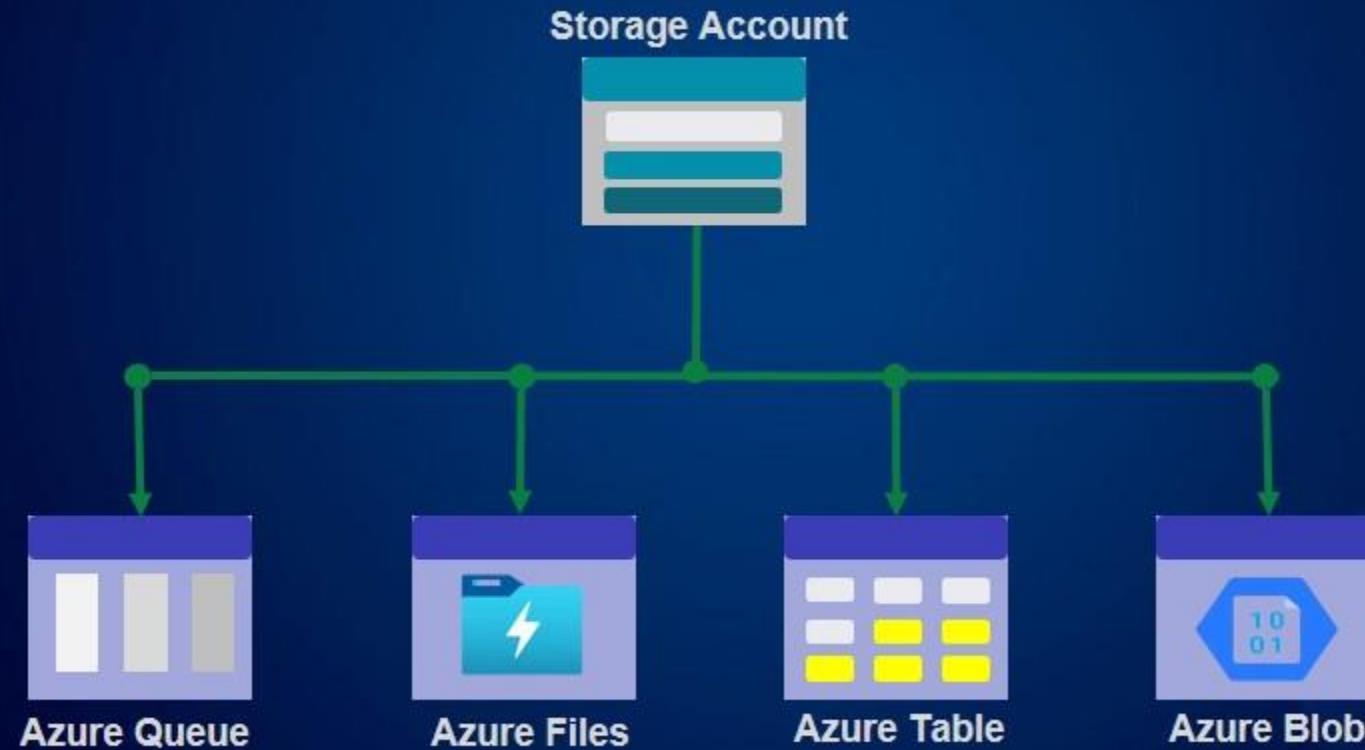
Các thành phần của Storage Accounts

Tìm hiểu về Azure Storage Redundancy

Demo: Tạo Storage Accounts

Các điểm chính của bài học

Mô tả về Storage Accounts



Mô tả về Storage Accounts

Azure Queue

Lưu trữ các thông điệp (Message) cho Microservices



Storage Account



Azure Table

Dịch vụ lưu trữ dữ liệu phi cấu trúc(No Sql), không yêu cầu CSDL quan hệ như SQL



Azure Files

Dịch vụ lưu trữ và chia sẻ files trong đám mây



Azure Blob

Lưu trữ dữ liệu lớn, bao gồm nhiều loại dữ liệu Media



Các thành phần của Storage Accounts

Loại tài khoản

Xác định các chức năng và các chi phí sử dụng dịch vụ

01

Cấp độ hiệu xuất

Xác định các cấp độ hiệu xuất

02



Tạo bản sao dữ liệu (Replication)

Xác định cơ sở hạ tầng dự phòng

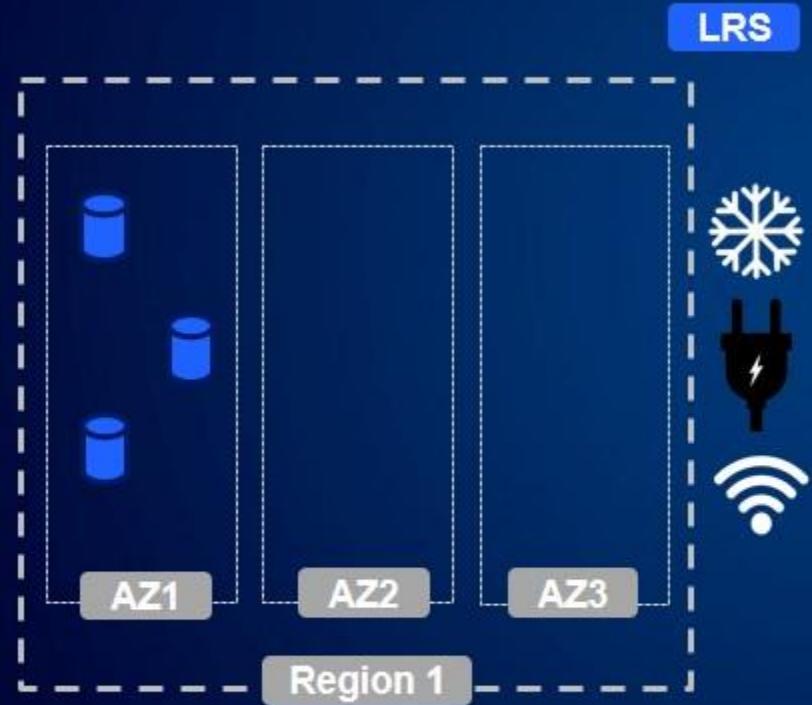
03

Cấp độ truy cập

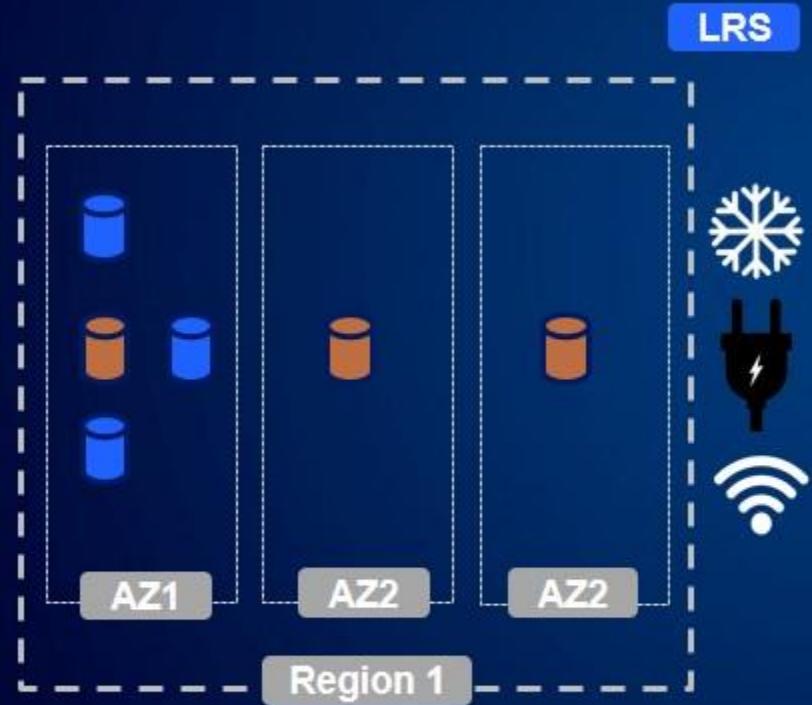
Xác định các cấp độ truy cập và các chi phí sử dụng dữ liệu

04

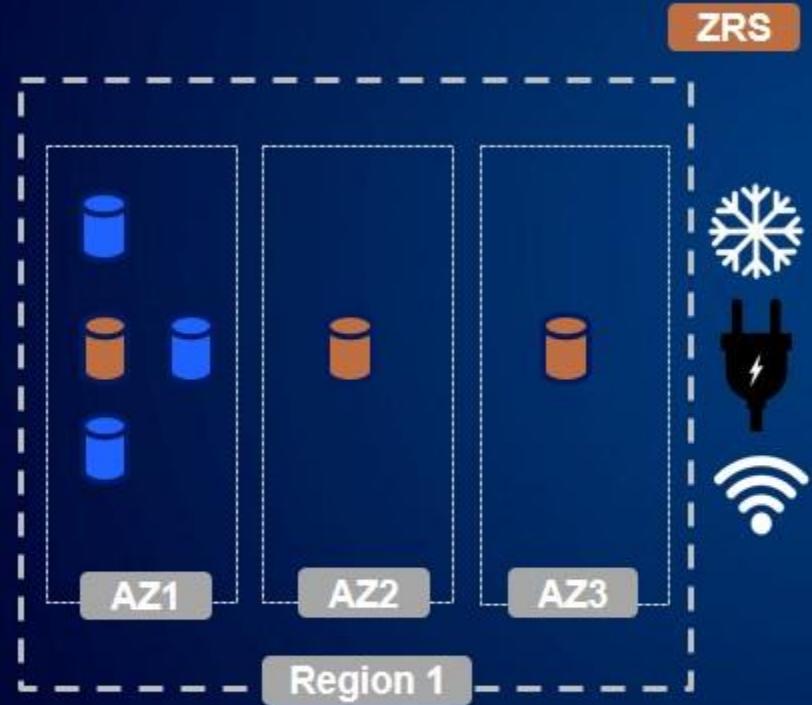
Tìm hiểu về Azure Storage Redundancy



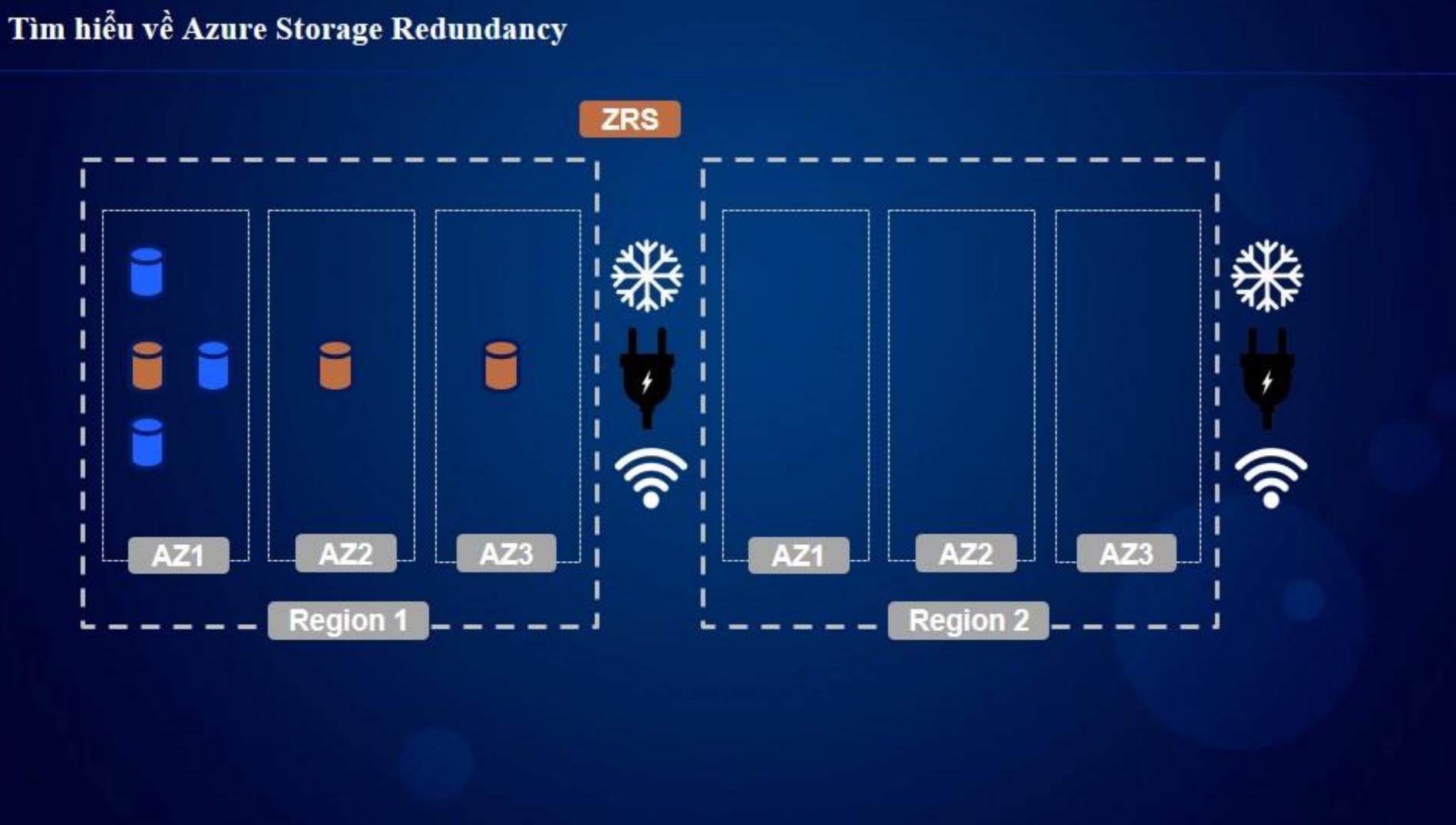
Tìm hiểu về Azure Storage Redundancy



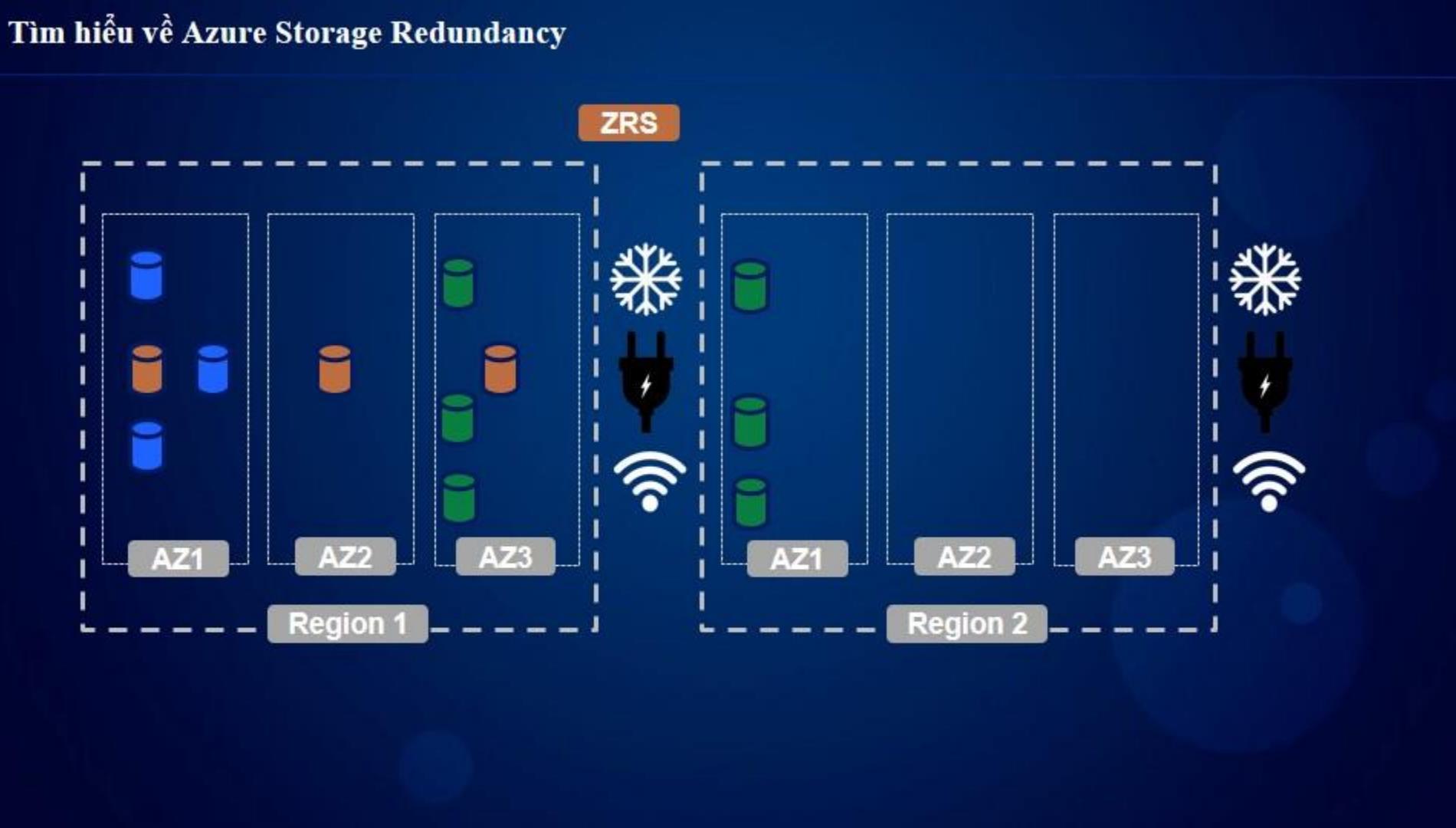
Tìm hiểu về Azure Storage Redundancy



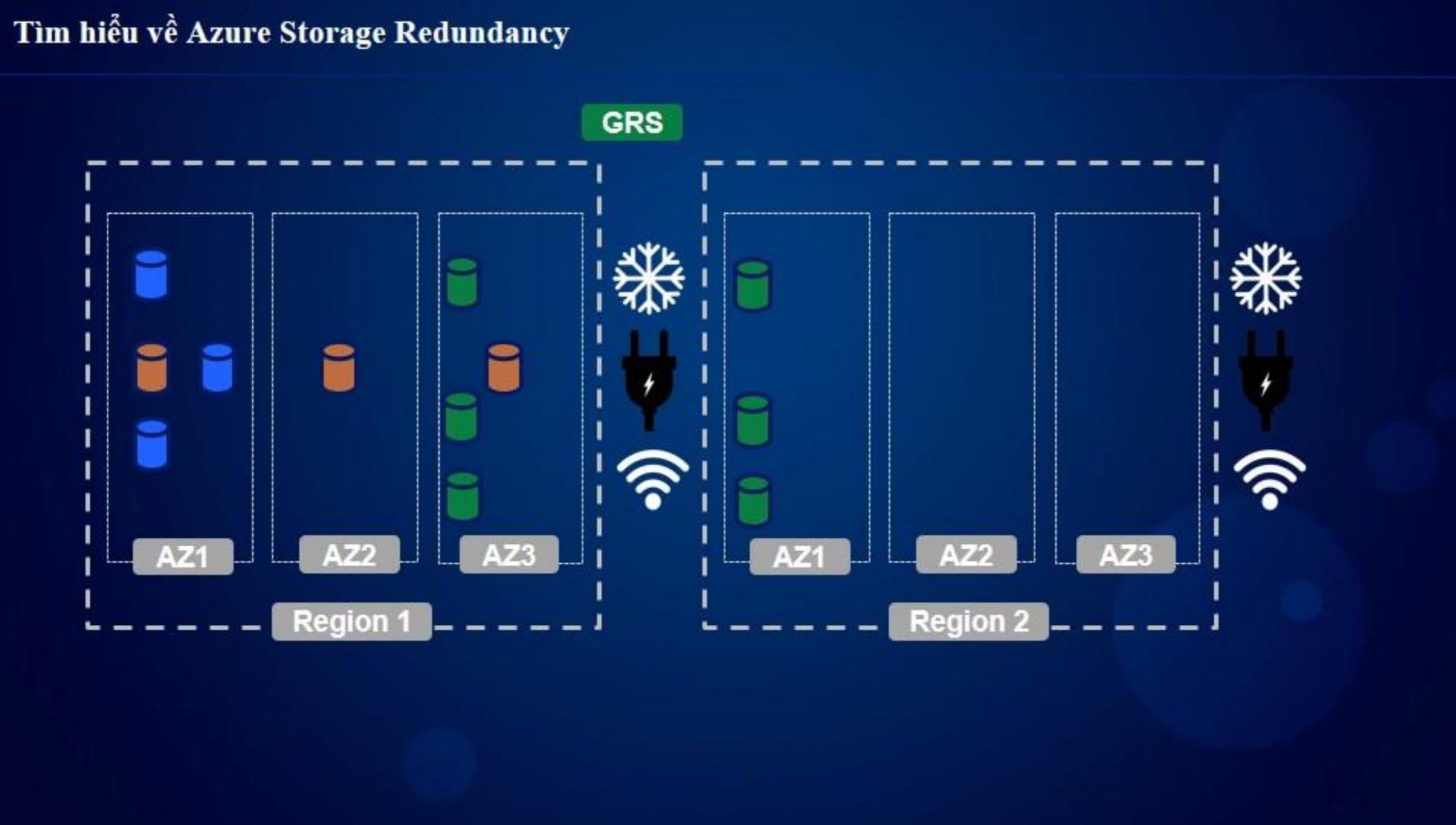
Tìm hiểu về Azure Storage Redundancy



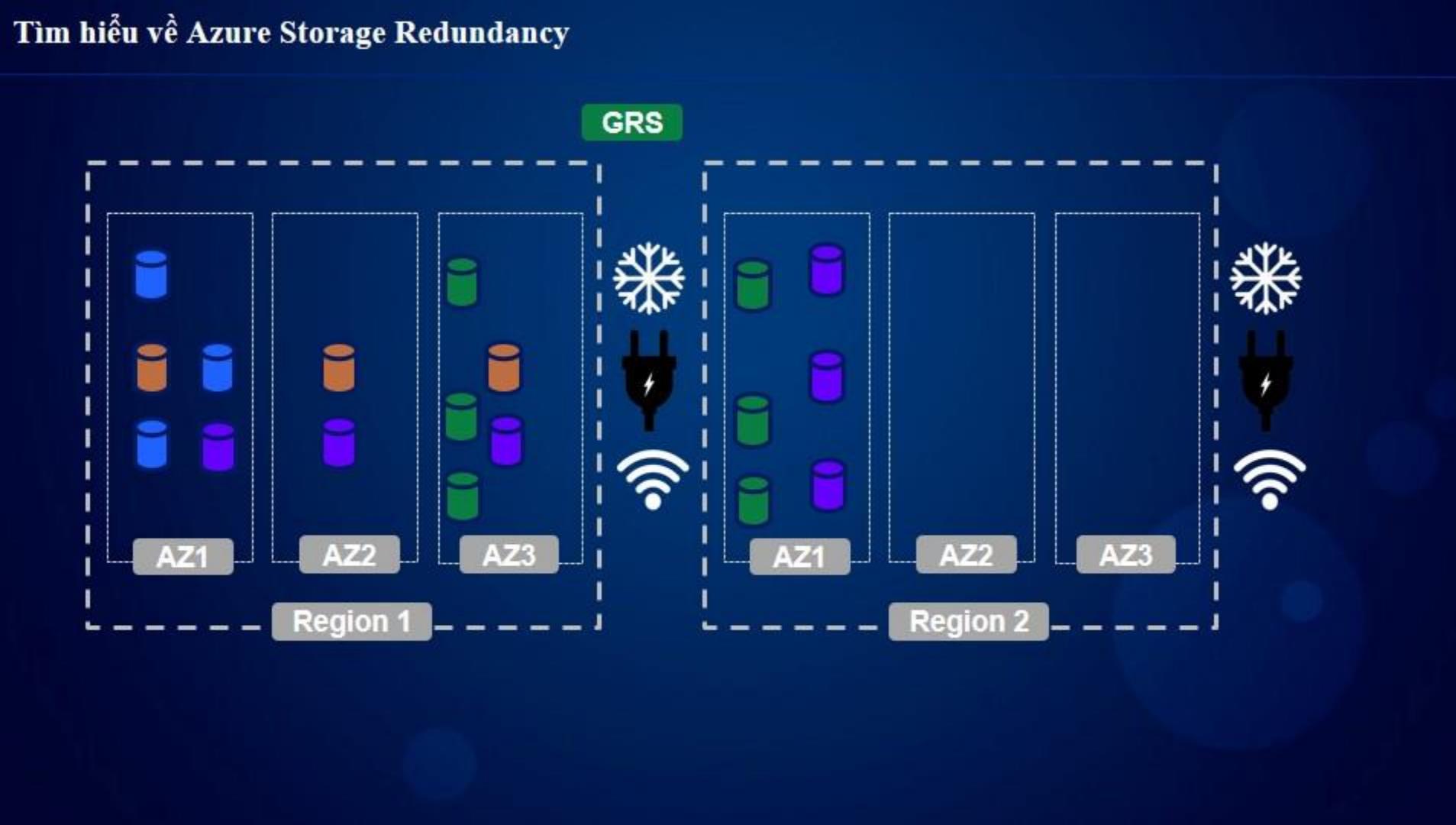
Tìm hiểu về Azure Storage Redundancy



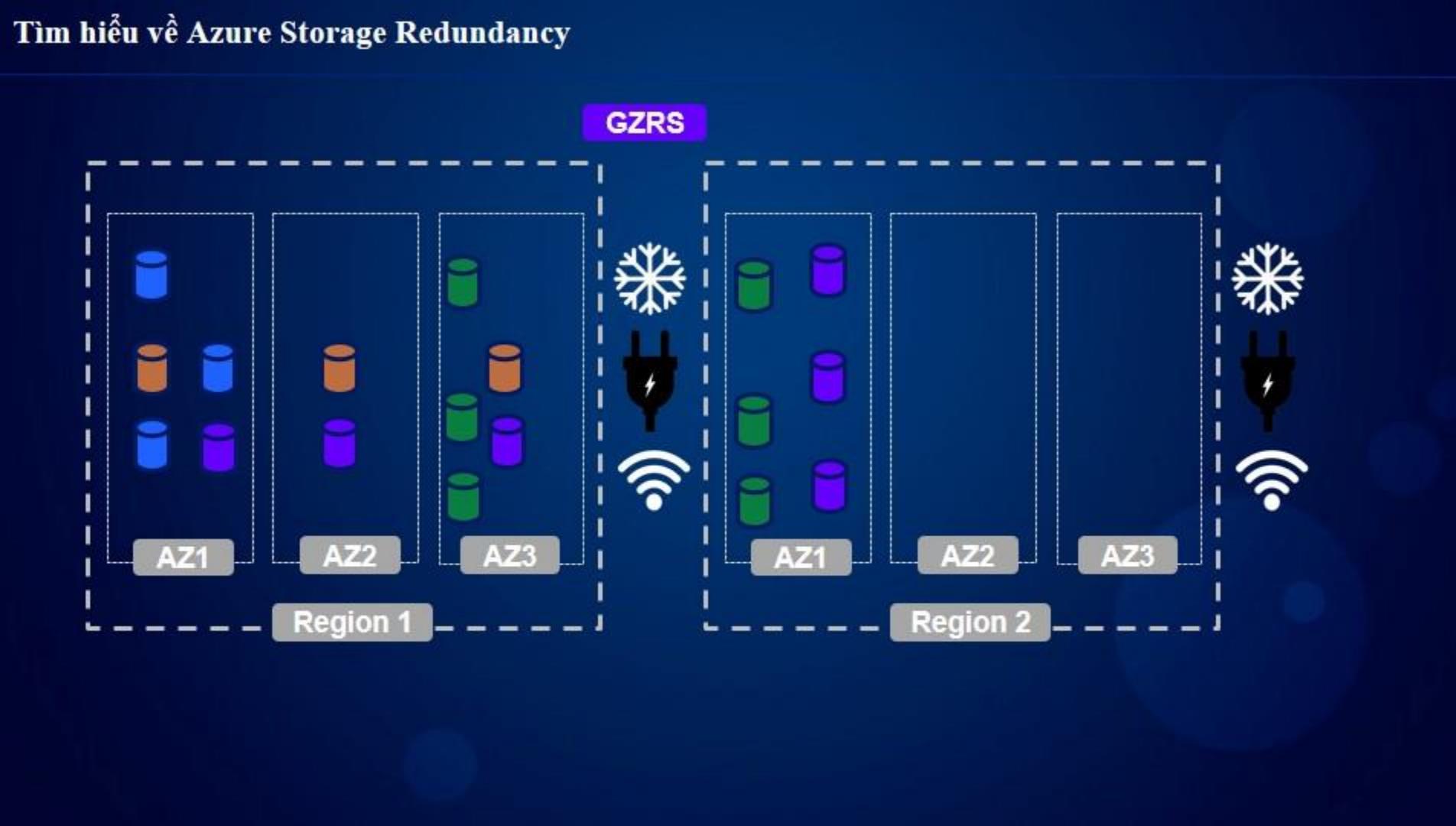
Tìm hiểu về Azure Storage Redundancy



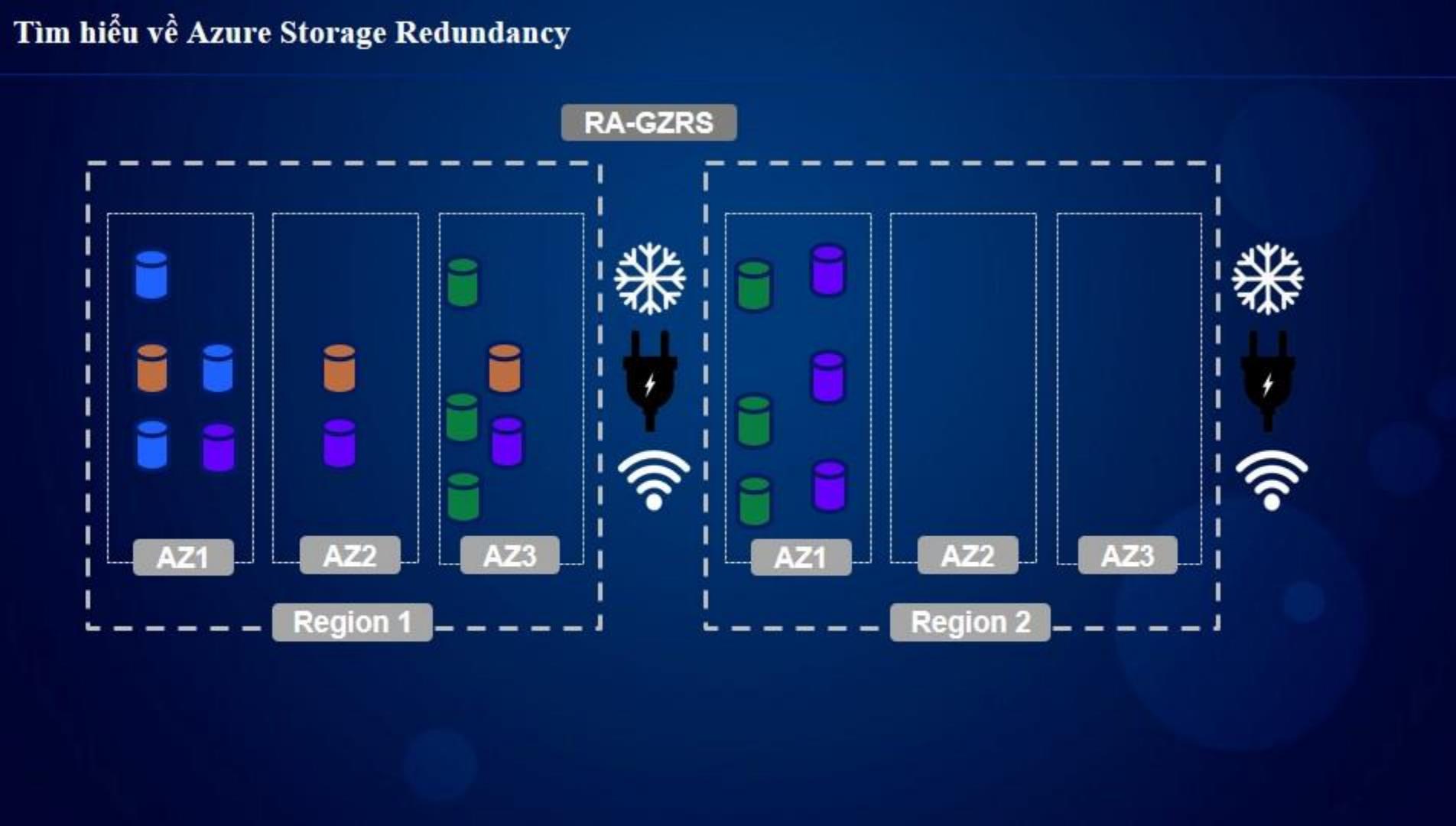
Tìm hiểu về Azure Storage Redundancy



Tìm hiểu về Azure Storage Redundancy



Tìm hiểu về Azure Storage Redundancy



Thực hiện Demo

1

Log In vào Azure Portal



Sử dụng tài khoản Azure
của bạn

2

Tạo Storage Account



Định nghĩa triển khai

3

Kiểm tra Storage



Kiểm tra các tài nguyên
trong Account

Các điểm chính của bài học

Loại tài khoản(Account Type)	General purpose v1 General purpose v2	Hỗ trợ các phiên bản cũ cho các loại dịch vụ lưu trữ dữ liệu như blobs, files, queues, và tables Được đề xuất cho blobs, files, queues, và tables
Cấp độ hiệu xuất (performance Tier)	Blob storage Standard Premium	Legacy blob-specific accounts Default storage performance tier High-performance storage tier
Sao lưu dữ liệu (Replication)	Lưu trữ dự phòng cục bộ (locally redundant storage(LRS)) Lưu trữ dự phòng theo địa lý (Geo-redundant storage(GRS)) Lưu trữ dự phòng theo khu vực địa lý (Geo-Zonal redundant storage(GZRS)) Lưu trữ dự phòng theo khu vực địa lý-chỉ đọc (Read-Access Geo-Redundant Storage (RA-GRS))	Ba bàn lưu trữ trong một khu vực vật lý bên trong một Region Bốn bàn lưu trữ trong các vùng sẵn sàng(AZ) bên trong 1 region LRS trong một Region chính và một Region thứ hai ZRS trong một Region chính và một Region thứ hai
Cấp độ truy cập (Access Tier)	Hot Cold Archive	Thường xuyên truy cập dữ liệu ít, thỉnh thoảng truy cập dữ liệu Cho Backup dữ liệu nhưng rất ít có nhu cầu truy cập dữ liệu

Các khái niệm về Azure Blob Storage

Bài học bao gồm

Mô tả về Azure Blog Storage

Các thành phần của kiến trúc blog

Các loại Blogs

Các cấp độ truy cập Container

Demo: Cấu hình Blob Storage

Các điểm chính của bài học

Mô tả về Azure Blob Storage

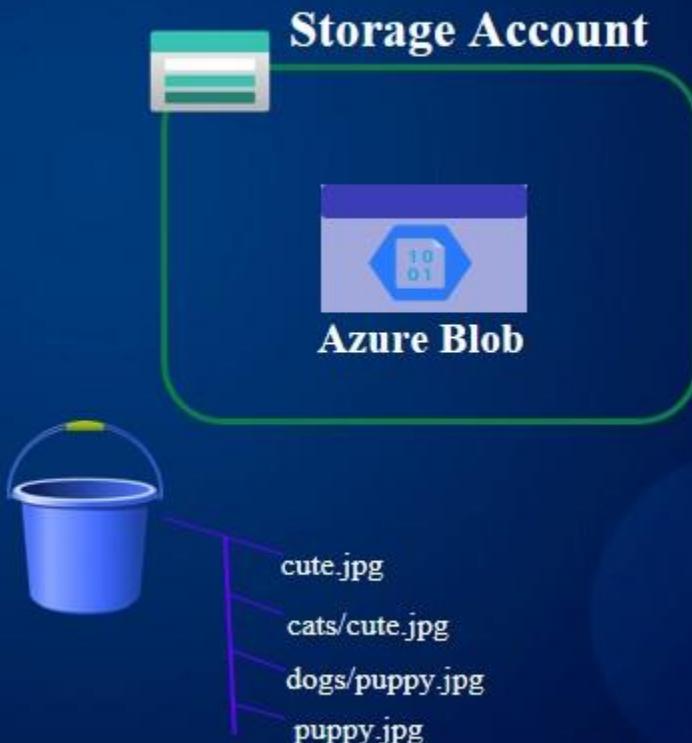
Blob Storage

Azure Blob là một dịch vụ con hoặc một tài nguyên con của Azure Storage(storage account).

Blob lưu trữ dữ liệu dựa trên đối tượng(object storage), và có thể dễ dàng truy cập từ HTTP/REST

Blob cho phép lưu trữ các loại dữ liệu như:

- Hình ảnh và video files
- Text files
- Log files
- VHD(virtual hard disk) files



Các thành phần của kiến trúc blog



Blob Service

Một dịch vụ con của storage accounts.



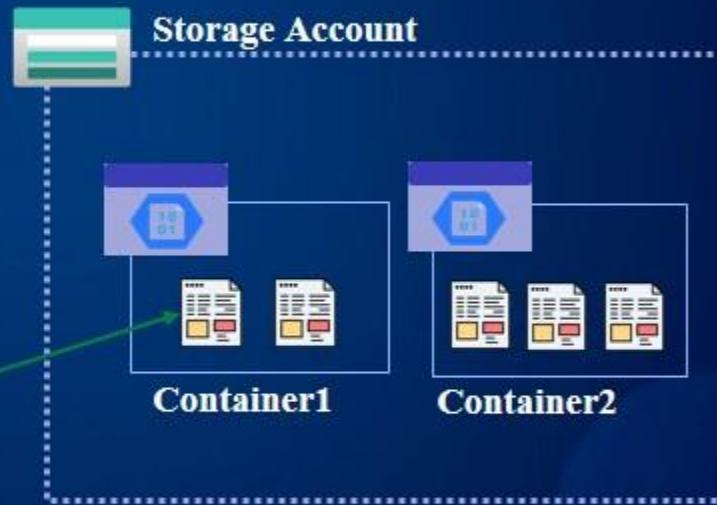
Blob Container

Container nơi mà chúng ta lưu trữ các blobs của chúng ta



Blobs

Chúng ta lưu trữ dữ liệu trong các Containers của chúng ta



Các loại Blogs



Block Blobs

Lưu trữ các file hình ảnh hoặc Videos. Phù hợp cho các tác vụ truyền dữ liệu liên tục (streaming).



Append Blob

Log files.



Page Blobs

Virtual machine disks.

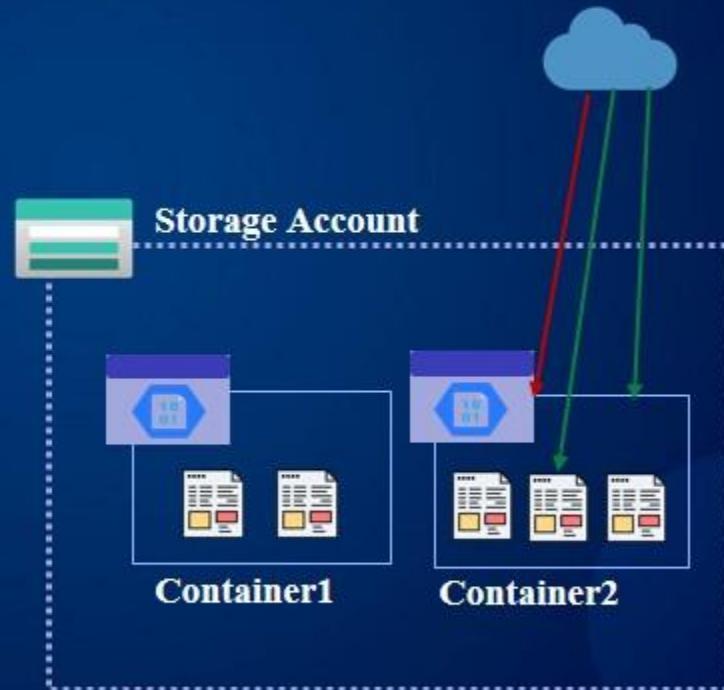
Các cấp độ truy cập Container

Kiểm soát truy cập (Access Control)

Mặc định, cho phép quyền truy cập public vào cấp độ storage account

Các cấp độ truy cập container (Container Access Level)

- **Quyền truy cập riêng tư-Private** (không cho phép người dùng ẩn danh(anonymous) có quyền truy cập)
- **Blob** (Cho phép người dùng ẩn danh (anonymous) có quyền truy cập vào blob)
- **Container** (Cho phép người dùng ẩn danh (anonymous) có quyền truy cập vào container và blobs)



Thực hiện Demo

1

Log In vào Azure Portal



Sử dụng tài khoản Azure của bạn

2

Tạo Blob Container



Upload files vào blobs

3

Kiểm tra Cấp Độ Truy Cập



Kiểm tra các cấp độ truy cập container

Các điểm chính của bài học

- ✓ Đối tượng lưu trữ
(Object Storage)
- ✓ Blob Container
- ✓ Cấu Trúc File Phẳng
(Flat-File Structure)



Cấu hình Blob Object Replication

Bài học bao gồm

Mô tả về Object Replication

Các khái niệm về Object Replication

**Các lợi ích trong việc triển khai
Object Replication**

Demo: Cấu hình Object Replication

Các điểm chính của bài học

Mô tả về Object Replication

Object Replication

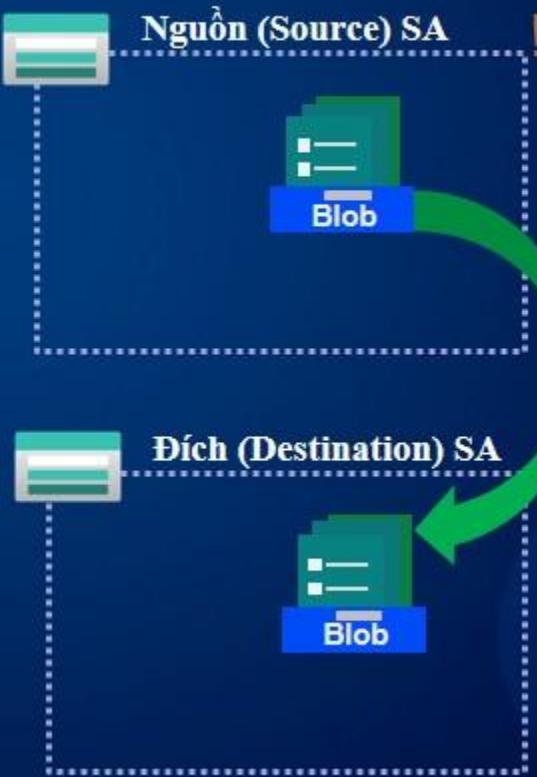
Object replication là quá trình sao chép(copy) không đồng bộ các dữ liệu như block blobs hoặc các đối tượng lưu trữ khác, giữa các storage accounts.

- Yêu cầu cần có Storage account nguồn và storage account đích
- Yêu cầu cần có versioning(tạo phiên bản) và change feed.

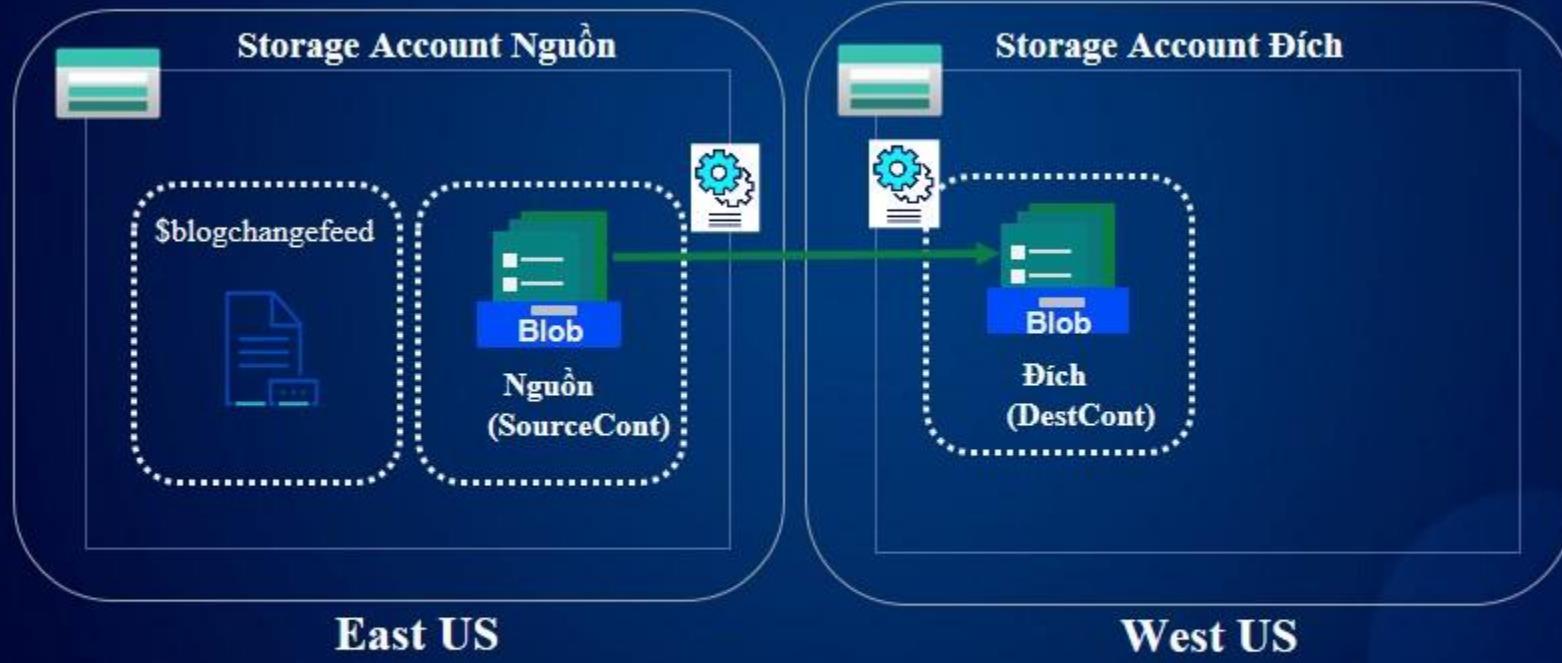
Change Feed: Là tính năng cho phép bạn theo dõi và nhận thông tin về các sự kiện thay đổi trong dữ liệu lưu trữ, bao gồm việc thêm, sửa đổi hoặc xóa các files và thư mục

- Hỗ trợ sao chép (replicate) dữ liệu từ một tenant này sang một tenant khác

Ghi chú: block blob có thể là các đối tượng dữ liệu lớn



Các khái niệm về Object Replication



Các lợi ích trong việc triển khai Object Replication



Giảm tối đa độ trễ (Latency)

Giảm độ trễ cho các yêu cầu đọc dữ liệu(read requests)



Gia tăng hiệu xuất

Xử lý các block blogs trong các regions khác nhau



Phân phối dữ liệu

Xử lý và phân tích dữ liệu tại một vị trí(location) cụ thể, và sau đó sao chép (replicate) dữ liệu này đến các khu vực (regions) khác.



Tối ưu hóa chi phí

Chuyển các dữ liệu đã sao chép vào cấp độ lưu trữ dữ liệu (Archive tier), việc này làm giảm các chi phí

Thực hiện Demo

1

Log In vào Azure Portal



Sử dụng tài khoản Azure của bạn

2

Tạo Storage Accounts



Tạo storage account nguồn và đích

3

Cấu hình Replication



Setup và kiểm tra Blob object replication

Các điểm chính của bài học



Versioning

Tính năng Versioning phải bật(enabled) trong cả hai storage account nguồn và đích



Change Feed

Tính năng Change feed phải được bật trong Storage Account nguồn. Và Azure Storage theo dõi sự kiện thay đổi trên luồng dữ liệu gọi là "\$blobchangefeed" để cung cấp thông tin và tư vấn về quá trình sao chép hoặc đồng bộ dữ liệu.



Giữa Subscription và Azure AD

Object replication được hỗ trợ giữa các subscriptions và Azure AD tenants.



Chính sách Replication

Một storage account chỉ có thể là một storage account nguồn cho tối đa hai storage account đích. Và mỗi chính sách (policy) chỉ hỗ trợ một cặp kết nối (pairing) duy nhất bằng cách sử dụng một ID chính sách (policy ID) cụ thể

Cấu hình quản lý vòng đời Blob (Lifecycle Management)

Bài học bao gồm

Mô tả về quản lý vòng đời

Các khái niệm về quản lý vòng đời

Demo: Cấu hình Lifecycle Management

Các điểm chính của bài học

Mô tả về quản lý vòng đời

Quản lý vòng đời (Lifecycle Management)

Dịch vụ Azure Blob Storage cho phép tự động hóa các hoạt động quản lý vòng đời của blobs

Tự động hóa quản lý vòng đời blob



Dễ dàng quản lý các vòng đời blob từ việc thường xuyên sử dụng tới việc lưu trữ hoặc xóa dữ liệu

Di chuyển tới các tầng truy cập(Access Tiers)



Chuyển đổi các blobs giữa các tầng truy cập để đáp ứng nhu cầu truy cập và sử dụng

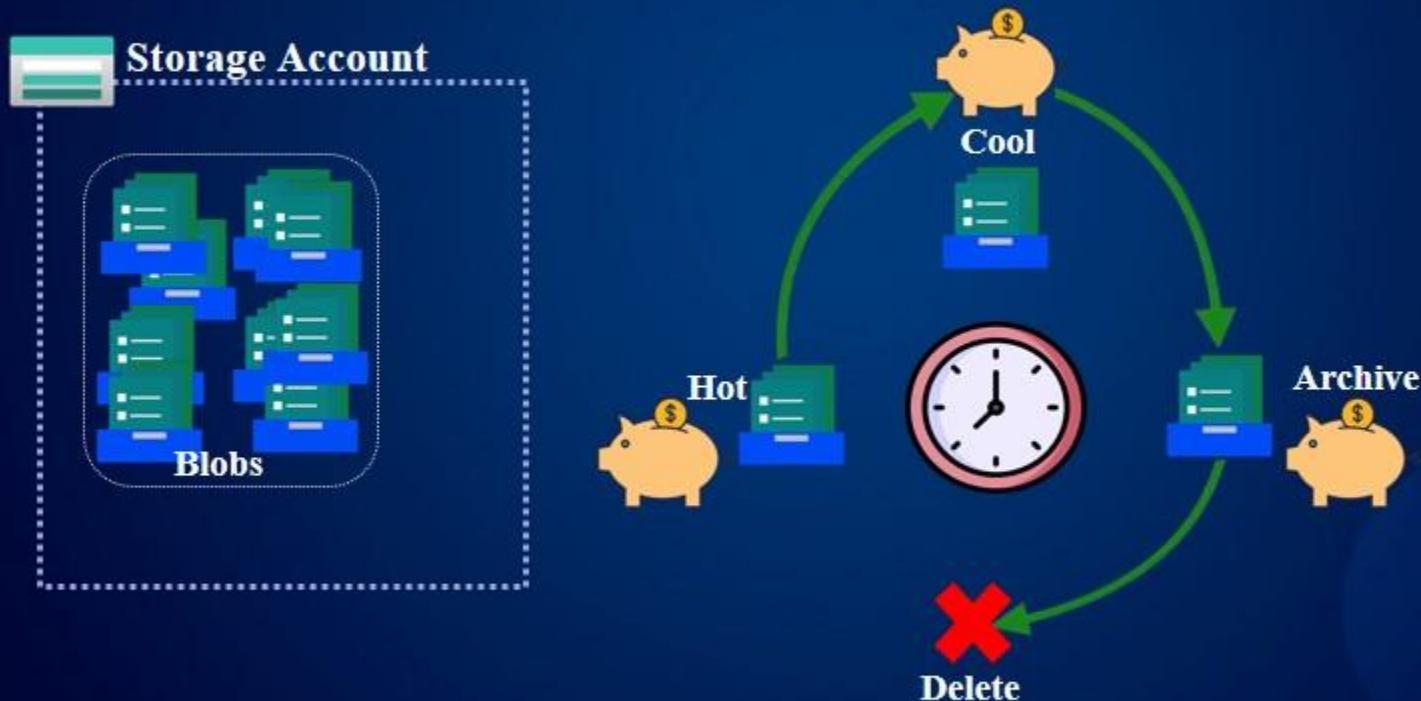
Tối ưu hóa chi phí



Tiết kiệm chi phí bằng cách giảm công việc quản trị admin và phân cấp các blobs dựa trên các nhu cầu sử dụng



Các khái niệm về quản lý vòng đời



Thực hiện Demo

1

Log In vào
Azure Portal



Sử dụng tài khoản
Azure của bạn

2

Tạo Storage
Accounts



Tạo một storage account

3

Cấu hình
Lifecycle
Management



Setup các hoạt động
vòng đời để di
chuyển Blobs

Các điểm chính của bài học



Storage Accounts

Hỗ trợ GPv2 storage accounts và Blob storage accounts



Loại(Types) và loại subtypes blobs

Hỗ trợ block và append blobs và hỗ trợ Subtypes, như base blobs, snapshots và versions.



Lọc (Filtering)

Có thể sử dụng tiền tố (prefix) hoặc kết hợp chỉ mục của blob(blob index) để lọc các đối tượng blob dựa trên quy tắc quản lý vòng đời

Thực hành tạo quy tắc(rule) quản lý vòng đời, để tự động xóa dữ liệu đã hết thời hạn sử dụng trong Azure Blob Storage

Trong tình huống của bài thực hành này, bạn là system admin quản trị website cho một cửa hàng trực tuyến. Vào kỳ nghỉ lễ đang tới gần, vì vậy bạn cần đưa các hình ảnh của các mặt hàng mà cửa hàng có theo nhu cầu của kỳ nghỉ lễ mà người tiêu dùng họ sẽ mua nhiều lên website. Để ứng dụng web có thể truy xuất các hình ảnh thì bạn cần upload các files ảnh này vào Azure storage. Tuy nhiên sau kỳ nghỉ lễ, bạn không muốn giữ lại các ảnh này do tốn kém chi phí lưu trữ dữ liệu. Do đó bạn sẽ phải thực hiện việc tự động hóa xóa các file ảnh trong vòng 30 ngày

Các bước thực hiện bài thực hành



Login vào
Azure portal



Upload các
files ảnh vào
Blob Storage



Tạo quy tắc(rules)
cho việc tự động
xóa các files ảnh



Hoàn thành bài
Thực hành

Cấu hình Azure Files

Bài học bao gồm

Mô tả về Azure Files

Các khái niệm về Azure Files

Các tùy chọn kết nối

Demo: Làm việc tương tác với Azure files

Các điểm chính của bài học

Mô tả về Azure Files

Azure Files

Azure Files là một dịch vụ con/tài nguyên con(sub-service/sub-resource) của Azure Storage(storage accounts).

Azure Files là một dịch vụ quản lý chia sẻ(file share)

Các tính năng của Azure Files:

- Kết nối SMB/NFS
- Hỗ trợ các hệ điều hành Windows, Linux, và MacOS
- Mở rộng với tính năng Azure File Sync
- Cấu trúc file theo kiểu truyền thống



Các khái niệm về Azure Files

Dịch vụ File (File Service)



Azure Files Service là một dịch vụ con của Azure Storage Accounts



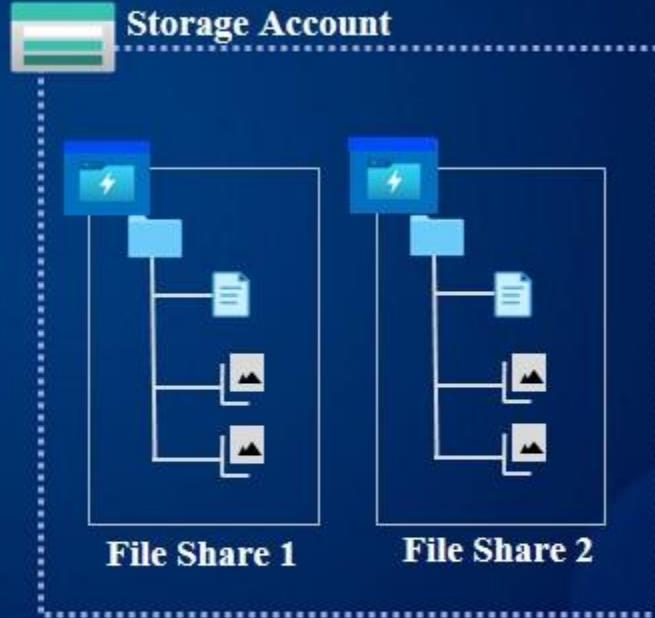
Chia sẻ File (File Share)

Cấu trúc file, chúng ta có thể kết nối vào như trong dịch vụ chia sẻ file nội bộ



Files và thư mục (Folders)

Files và Folders tồn tại bên trong File Share



Các tùy chọn kết nối

Kết nối không an toàn

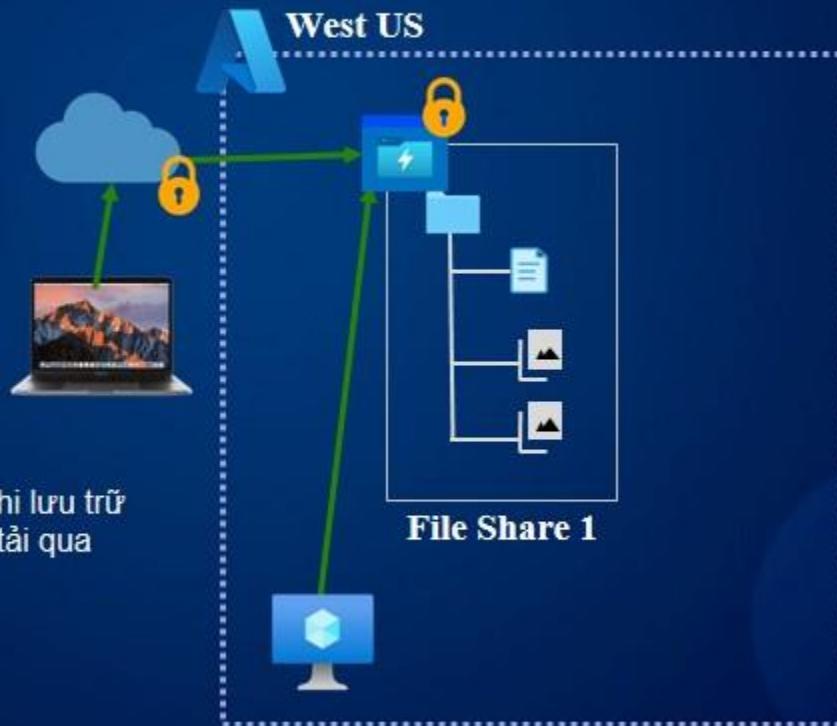
REST, SMB 2.1, và SMB 3.0

Kết nối an toàn

REST và SMB 3.0

Bảo mật

Dữ liệu mặc định được mã hóa khi lưu trữ
và cũng được mã hóa khi truyền tải qua
giao thức HTTPS và
SMB (Server Message Block)



Thực hiện Demo

1

Log In vào
Azure Portal



Sử dụng tài khoản
Azure của bạn

2

Tạo Storage
Accounts



Tạo một storage account

3

Tạo một
Azure File Share



Tạo vào truy cập vào
Azure file share

Các điểm chính của bài học

Quản lý chia sẻ File



Sử dụng storage account redundancy và bảo mật security

Hệ điều hành

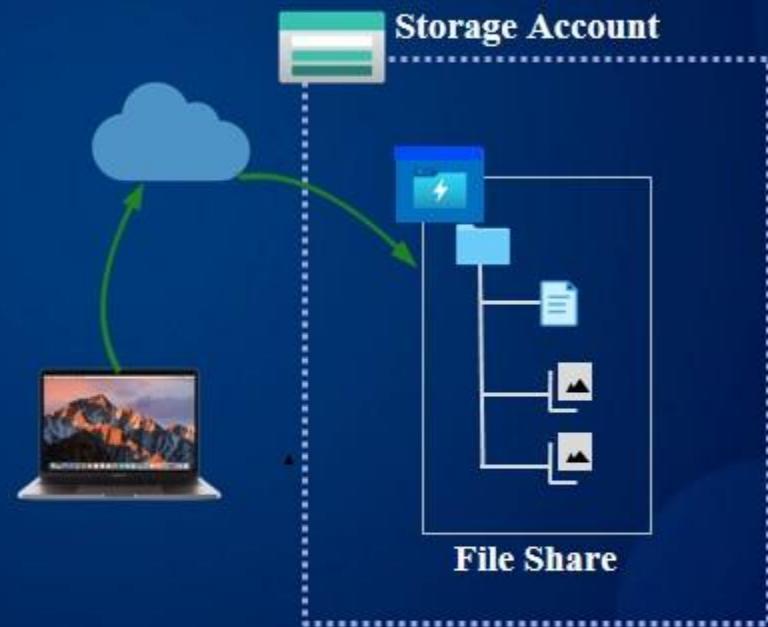


Hỗ trợ hệ điều hành Windows, Linux, và MacOS

File Share Quota



Kích cỡ mặc định 5 TB



Cấu hình Azure File Sync

Bài học bao gồm

Mô tả về Azure File Sync

Các thành phần của Azure File Sync

File Sync Cloud Tiering

Demo: Cấu hình Azure File Sync

Các điểm chính của bài học

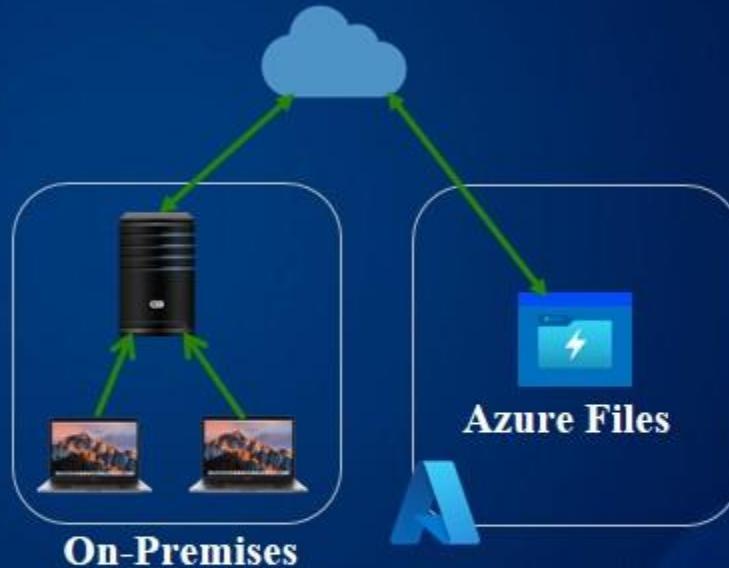
Mô tả về Azure File Sync

Azure File Sync

Azure File Sync là một phần mở rộng của Azure Files, cho phép bạn có thể mở rộng khả năng của máy chủ tại hệ thống mạng nội bộ hoặc Data Center(On-premises) của bạn.

Các tính năng:

- Bộ đệm(cache) cục bộ cho các files thường xuyên được truy cập
- Hỗ trợ từ HĐH Windows 2012 trở lên
- SMB, NFS, và FTPS
- Yêu cầu cài đặt File Sync Agent



Các thành phần của Azure File Sync



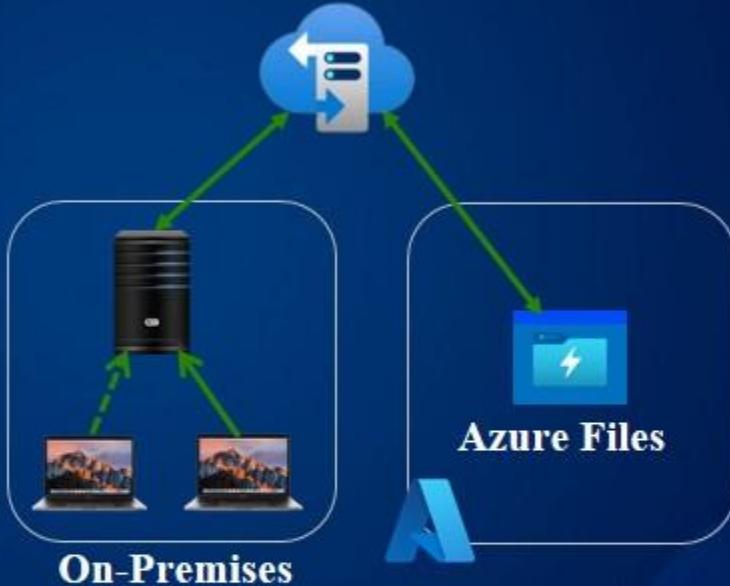
Dịch vụ đồng bộ dữ liệu
Tài nguyên Azure cấp độ cao



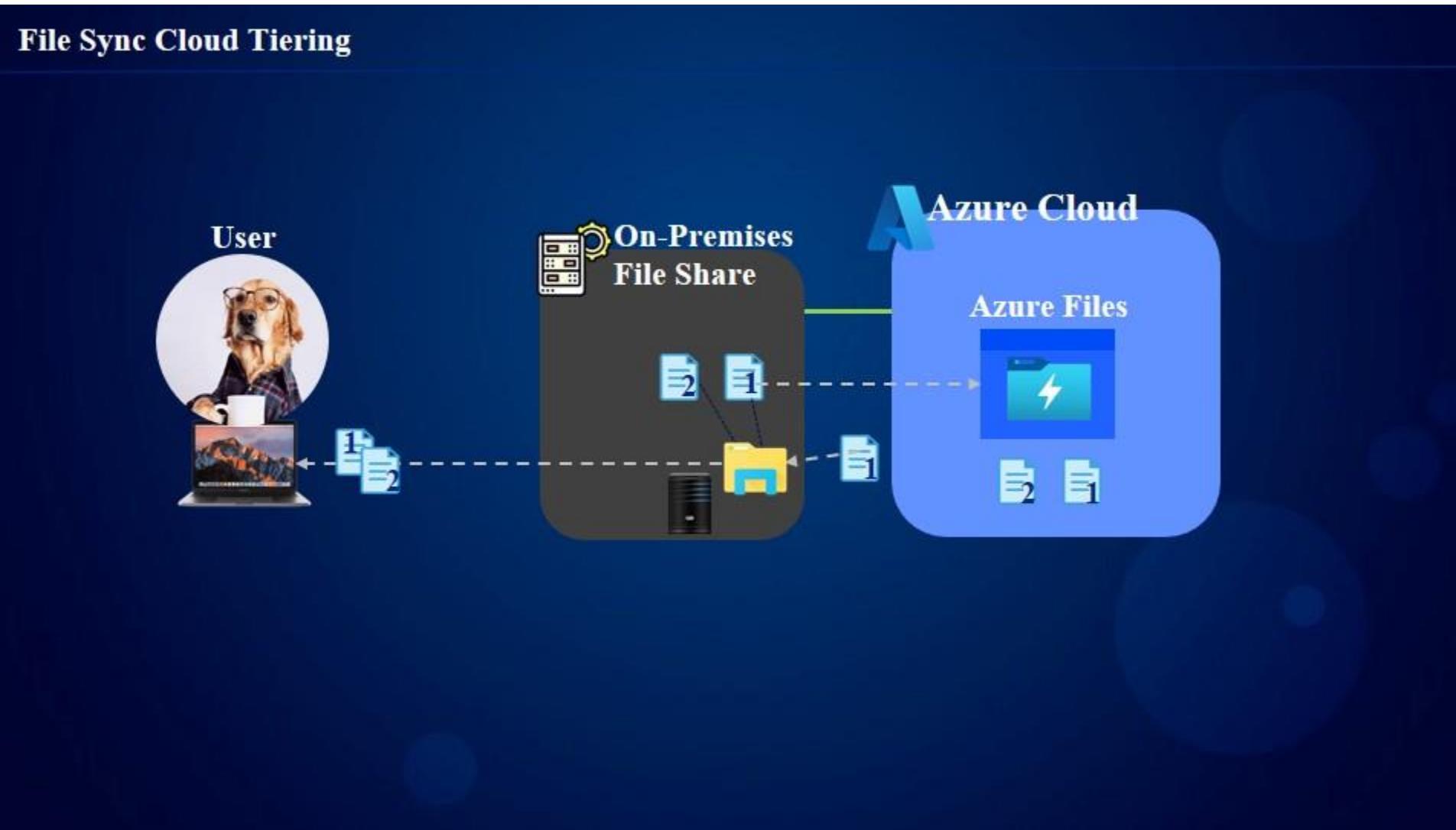
Điểm cuối đám mây
Azure file share được sử dụng trong đồng bộ file(File Sync)



Đăng ký máy chủ
Tạo sự tin cậy(trusted) các file servers



File Sync Cloud Tiering



Các điểm chính của bài học

Mở rộng On-Premises File Share

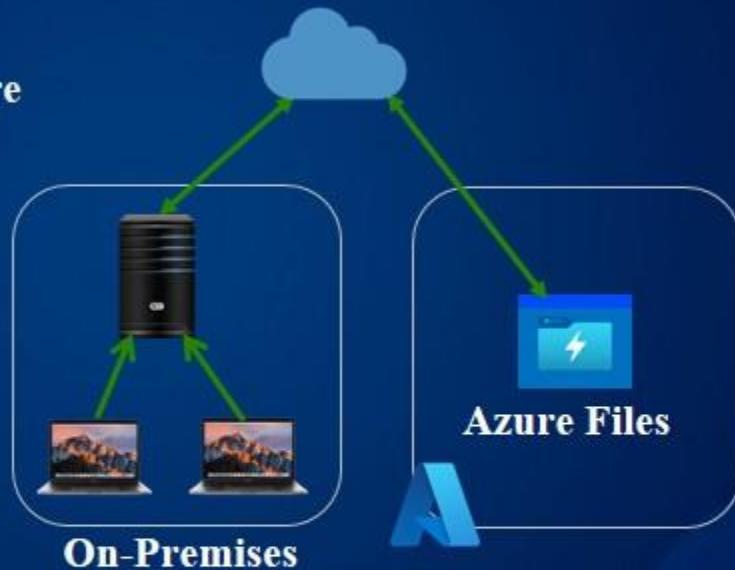
Tăng dung lượng lưu trữ thông qua các tầng lưu trữ dữ liệu đám mây

Chỉ hỗ trợ Windows

Hỗ trợ từ Windows 2012 trở lên

Yêu cầu File Sync Agent

Cần download Azure File Sync agent vào Local file server



Thực hành tạo và khôi phục (Restore) File Share Snapshots trong Azure

Trong tình huống của bài thực hành này, công ty của bạn cần đảm bảo các bản sao lưu dữ liệu(backups) phải luôn được sẵn sàng cho tất cả các file shares. Phiên bản File (File verioning) cũng rất quan trọng, bởi vì các nhân viên thường sửa đổi các files trong dịch vụ chia sẻ dữ liệu file share. Để kiểm tra các chức năng của Azure file share, bạn được giao nhiệm vụ tạo một snapshot của một file share và khôi phục nó trong windows file server



Quản lý quyền truy cập vào Storage Account

Bài học bao gồm

Các tùy chọn truy cập của Storage Account

Public Endpoints

**Demo: Tìm hiểu về các quyền truy cập
mạng(network access) trong Storage Account**

Các điểm chính của bài học

Các tùy chọn truy cập của Storage Account



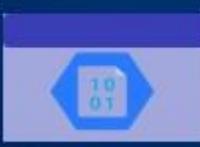
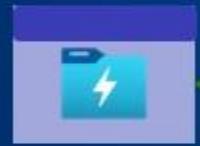
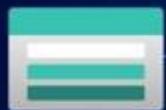
Mặc định tất cả các dịch vụ là được công khai(public) sử dụng Service public endpoint URL.

Quyền truy cập vào Storage Account
Có thể bị giới hạn cho phép trong
các mạng ảo, dải địa chỉ IP thông qua
tường lửa (firewall) của Storage Account
, và qua các nguyên cụ thể

Cho phép truy cập bằng địa chỉ private IP
cho các tài nguyên trong một
mạng ảo(virtual network) liên quan

Public Endpoints

Storage
Account



Internet



`https://<accountName>.<subservice>.core.windows.net/<resourceName>`

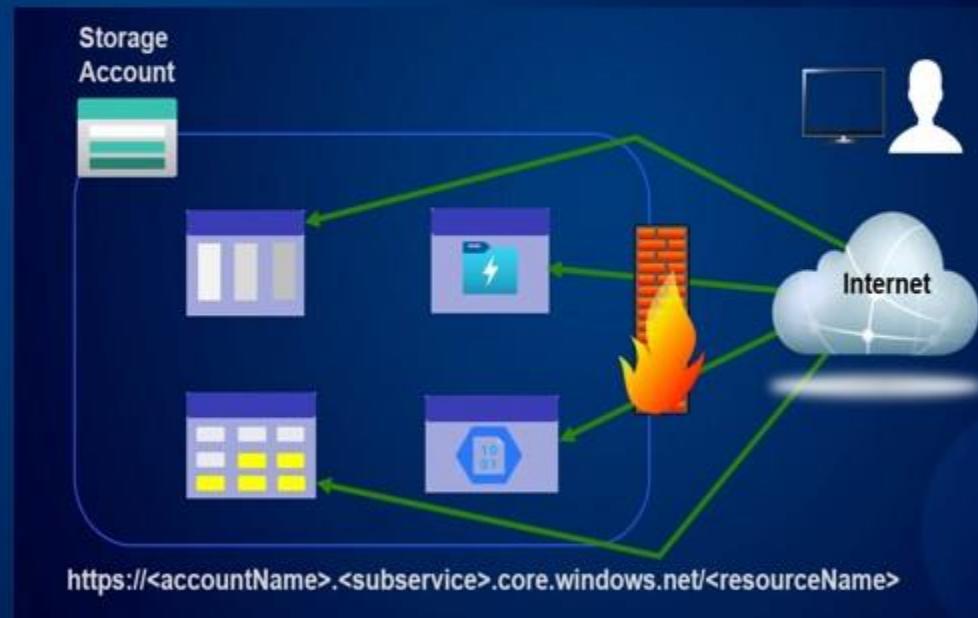
Các điểm chính của bài học

Cung cấp chức năng cấu hình quyền truy cập mạng (network access)

Mỗi một dịch vụ con có một
điểm cuối(endpoint)

Endpoints:

- Public endpoint
- Giới hạn truy cập
(Restricted access)
- Private endpoint



Bảo mật Storage Account

Bài học bao gồm

Về mã hóa dữ liệu Azure Storage

Xác thực truy cập trong Azure Storage

**Demo: Tìm hiểu về bảo mật
trong Storage Account**

Các điểm chính của bài học

Về mã hóa dữ liệu Azure Storage

Bảo mật dữ liệu

- Mặc định, tất cả các dữ liệu được lưu trữ (dữ liệu trong trạng thái nghỉ) trong các dịch vụ Azure Storage được bảo mật sử dụng dịch vụ mã hóa dữ liệu (Storage Service Encryption (SSE))
- Tất cả các dữ liệu trong trạng thái được truyền tải qua mạng có thể được bảo mật sử dụng giao thức bảo mật dữ liệu khi nó được truyền tải qua mạng là transport-level security (HTTPS).



Xác thực truy cập trong Azure Storage



Access keys

Azure-generated keys cung cấp quyền truy cập vào tầng quản lý và dữ liệu của một giải pháp lưu trữ dữ liệu Azure



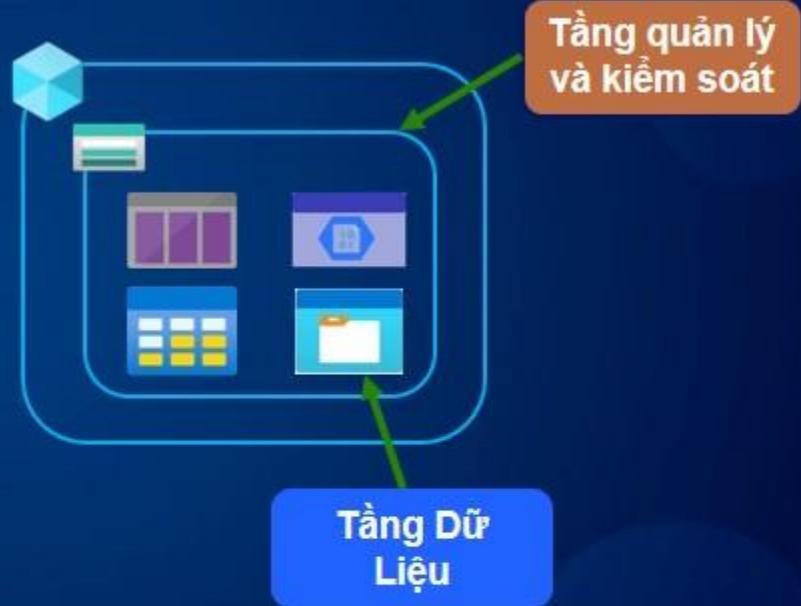
Shared Access Signature(SAS)

Một chữ ký truy cập(access signature), được tạo ra từ khóa truy cập(access keys), nó cung cấp quyền truy cập vào một cấp độ tài khoản hoặc một cấp độ dịch vụ



Azure AD Authentication

Sử dụng Azure role-based access control(RBAC) và các danh tính của Azure Active Directory(AD) để quản lý và cấp quyền xác thực truy cập (thay vì sử dụng access keys)



Các điểm chính của bài học

- ✓ Access keys
- ✓ Shared Access Signature(SAS)
- ✓ Azure AD Authentication



Thực hành sử dụng SAS URI để giới hạn quyền truy cập vào Azure Storage Account

Trong bài thực hành này, bạn sẽ tạo một SAS token cho việc truy cập vào một Azure Storage Account và kiểm tra(test) việc truy cập vào các tài nguyên từ một PC windows client.



Sử dụng Azure Jobs

Bài học bao gồm

Mô tả về Azure Jobs

So sánh Importing và Exporting Jobs

Các điểm chính của bài học

Mô tả về Azure Jobs



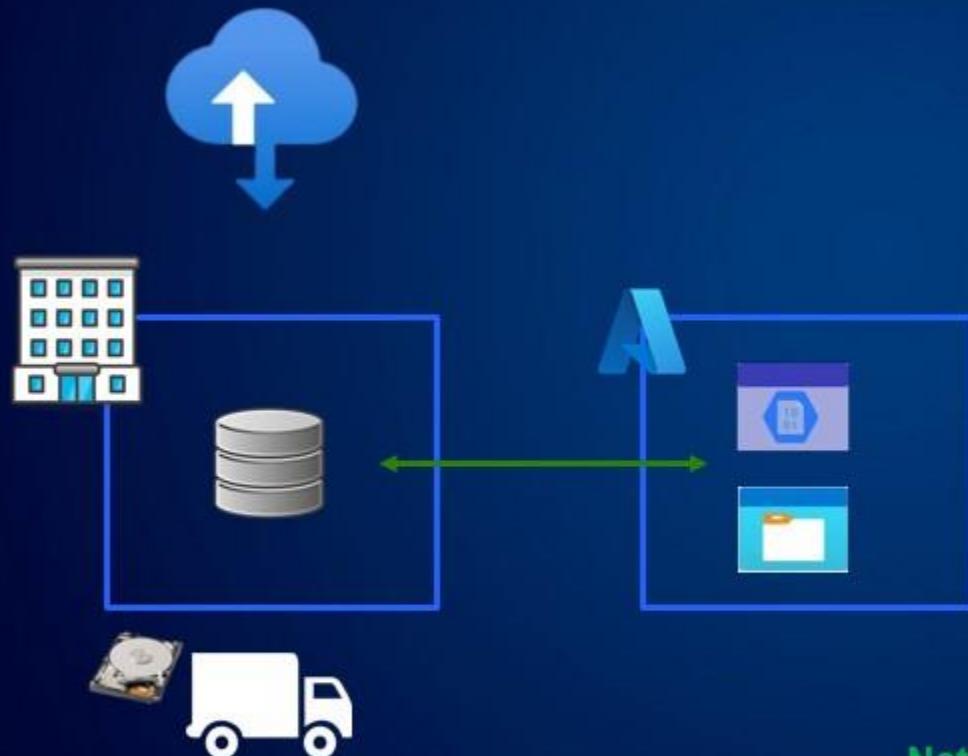
Azure Jobs

Di chuyển một lượng lớn dữ liệu
giữa hệ thống mạng nội bộ hoặc
data Center(on-premises) của bạn
và Azure Storage

- Di chuyển dữ liệu tới/từ Blob service
- Di chuyển tới Files service
- Vận chuyển dữ liệu tới data centers
của Azure
- Hỗ trợ các loại ổ cứng:

SATA
HDD
SSD

So sánh Importing và Exporting Jobs

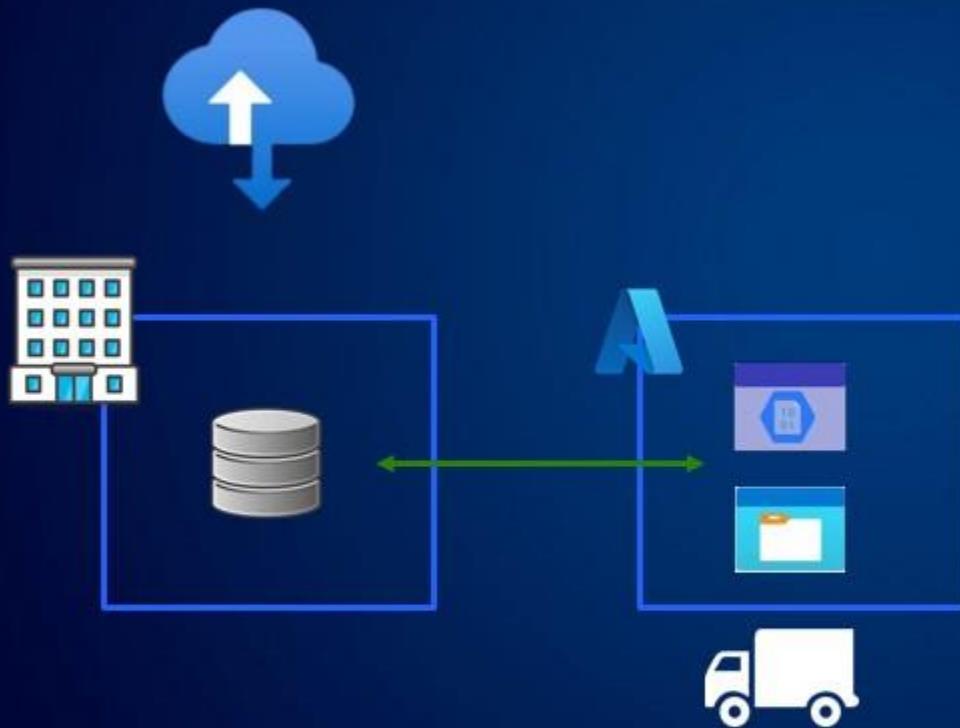


Azure Import Jobs

1. Chuẩn bị các ổ cứng disks (WAImportExport)
2. Tạo job
3. Ship các ổ cứng

Note: Công cụ WAImportExport là một công cụ được thiết kế để copy dữ liệu tới và từ Azure Blob Storage, và Azure Files

So sánh Importing và Exporting Jobs



Azure Import Jobs

1. Chuẩn bị các ổ cứng disks (WAImportExport)
2. Tạo job
3. Ship các ổ cứng
4. Kiểm tra trạng thái job
5. Nhận lại các ổ cứng
6. Kiểm tra dữ liệu trong Azure Storage

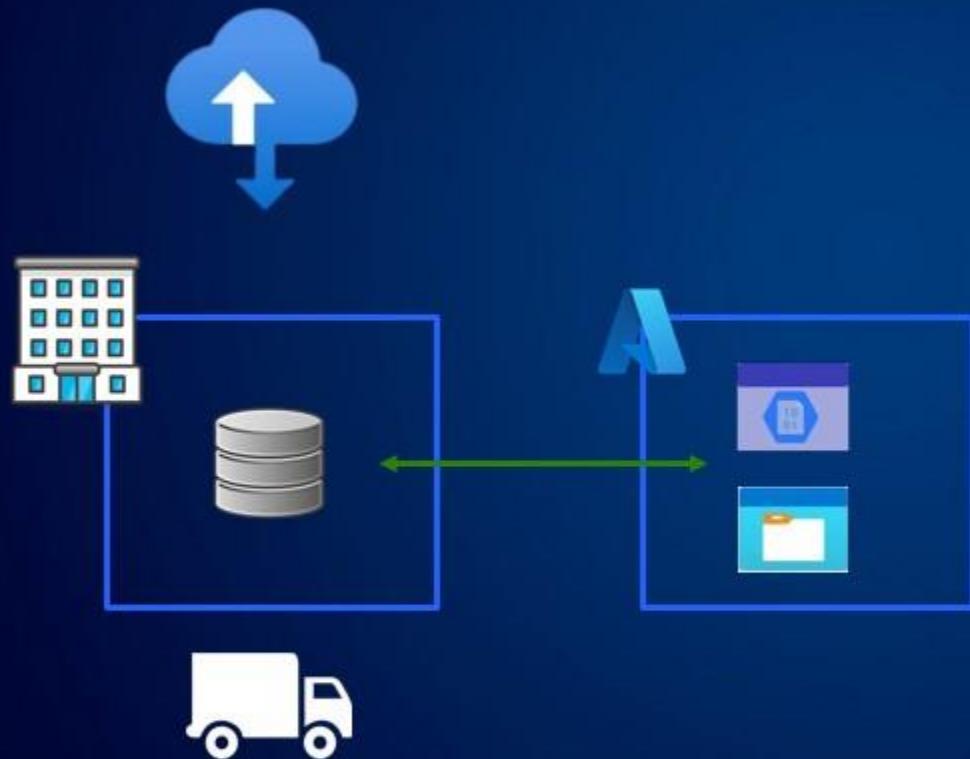
So sánh Importing và Exporting Jobs



Azure Export Jobs

1. Tạo job
2. Ship các ổ cứng(WAImportExport)

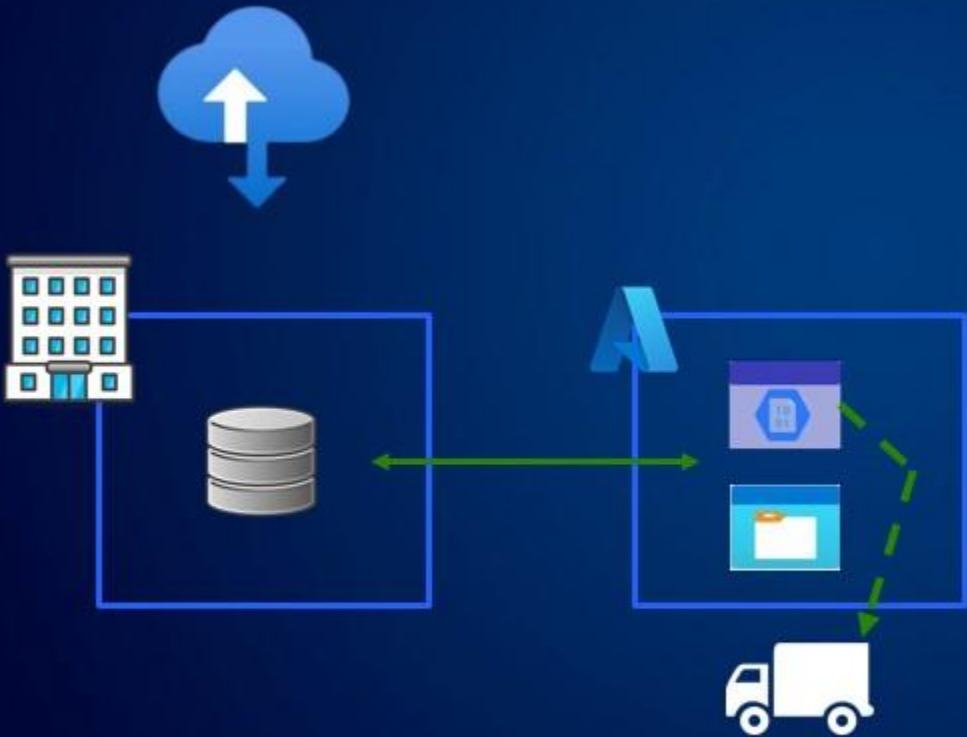
So sánh Importing và Exporting Jobs



Azure Export Jobs

1. Tạo job
2. Ship các ổ cứng(WAImportExport)

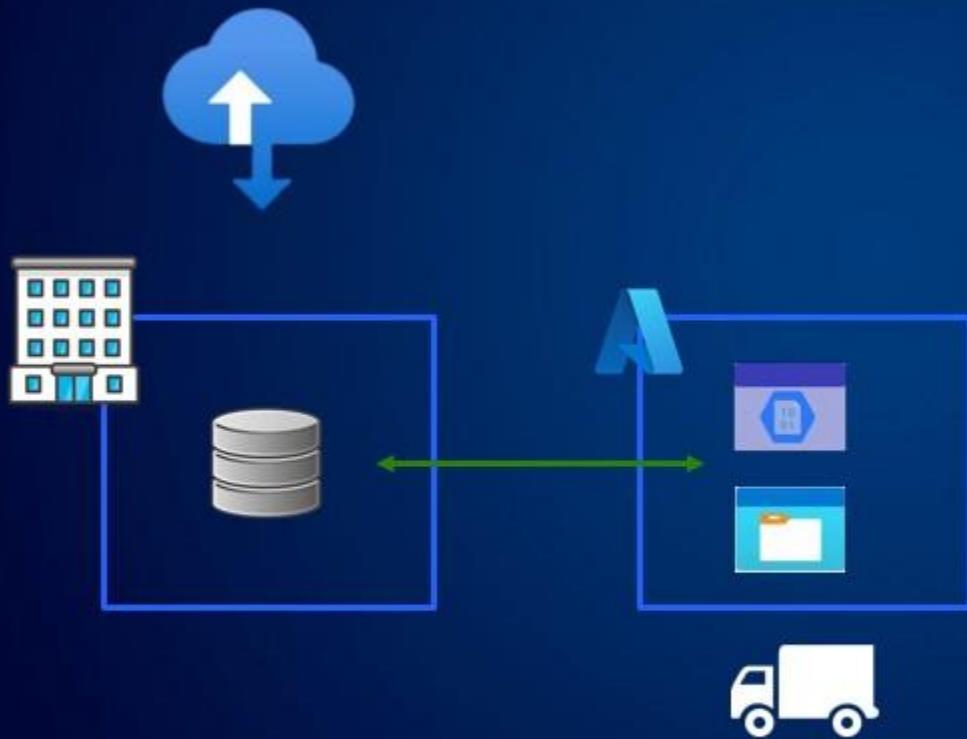
So sánh Importing và Exporting Jobs



Azure Export Jobs

1. Tạo job
2. Ship các ổ cứng(WAImportExport)
3. Kiểm tra trạng thái job
4. Nhận lại các ổ cứng và mở khóa các ổ cứng

So sánh Importing và Exporting Jobs



Azure Export Jobs

1. Tạo job
2. Ship các ổ cứng(WAImportExport)
3. Kiểm tra trạng thái job
4. Nhận lại các ổ cứng và mở khóa các ổ cứng

Các điểm chính của bài học

Import jobs



Gửi một lượng lớn dữ liệu tới Azure Cloud khi mà băng thông mạng (network bandwidth) không đủ đáp ứng việc di chuyển dữ liệu lên đám mây

Export jobs



Nhận một lượng lớn dữ liệu từ Azure Cloud khi mà băng thông mạng (network bandwidth) không đủ đáp ứng việc di chuyển dữ liệu từ đám mây vào bên trong mạng nội bộ hoặc data center của chúng ta

WAImportExport CLI Tool



Sử dụng các ổ cứng(disks) cho việc copy dữ liệu, chúng ta cần ước tính số ổ cứng mà chúng ta cần cho việc di chuyển dữ liệu

Chỉ hỗ trợ các thiết bị chạy hệ điều hành windows



Azure Blob và Files



Sử dụng các công cụ làm việc với Azure Storage

Bài học bao gồm

Mô tả về các công cụ

**Sử dụng các công cụ làm việc
với Azure Storage**

Các điểm chính của bài học

Mô tả về các công cụ



Storage Explorer

Công cụ đồ họa(GUI) được sử dụng để làm việc và tương tác với các storage accounts. Hỗ trợ & chạy trên Hệ điều hành Windows, Linux, và MacOS



AzCopy

Công cụ dòng lệnh (command-line) được sử dụng để làm việc và tương tác với các storage accounts. Hỗ trợ & chạy trên hệ điều hành Windows, Linux, và MacOS

Các điểm chính của bài học



Storage Explorer

- Quản lý Storage Account
- Sử dụng Azure Active Directory(AD) hoặc Shared Access Signature(SAS)
- Cung cấp giao diện đồ họa
- Sử dụng AzCopy bên trong, để thực hiện các hoạt động liên quan đến sao chép dữ liệu và tương tác với các tài nguyên lưu trữ trong Azure

vs



Azcopy

- Quản lý Storage Account
- Sử dụng Azure Active Directory(AD) hoặc Shared Access Signature(SAS)
- Có thể sử dụng AzCopy để thực hiện việc tự động hóa và tạo các kịch bản (scripts)

Các khái niệm về mạng ảo (Virtual Network)

Bài học bao gồm

Mô tả hệ thống mạng

**So sánh hệ thống mạng truyền thống
và hệ thống mạng ảo**

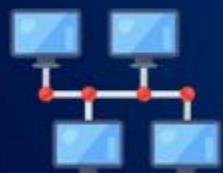
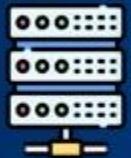
Mô tả hệ thống mạng ảo(Virtual Network)

Các điểm chính của bài học

Mô tả hệ thống mạng



Hệ thống mạng nội bộ LAN truyền thống
(On-Premises Network)

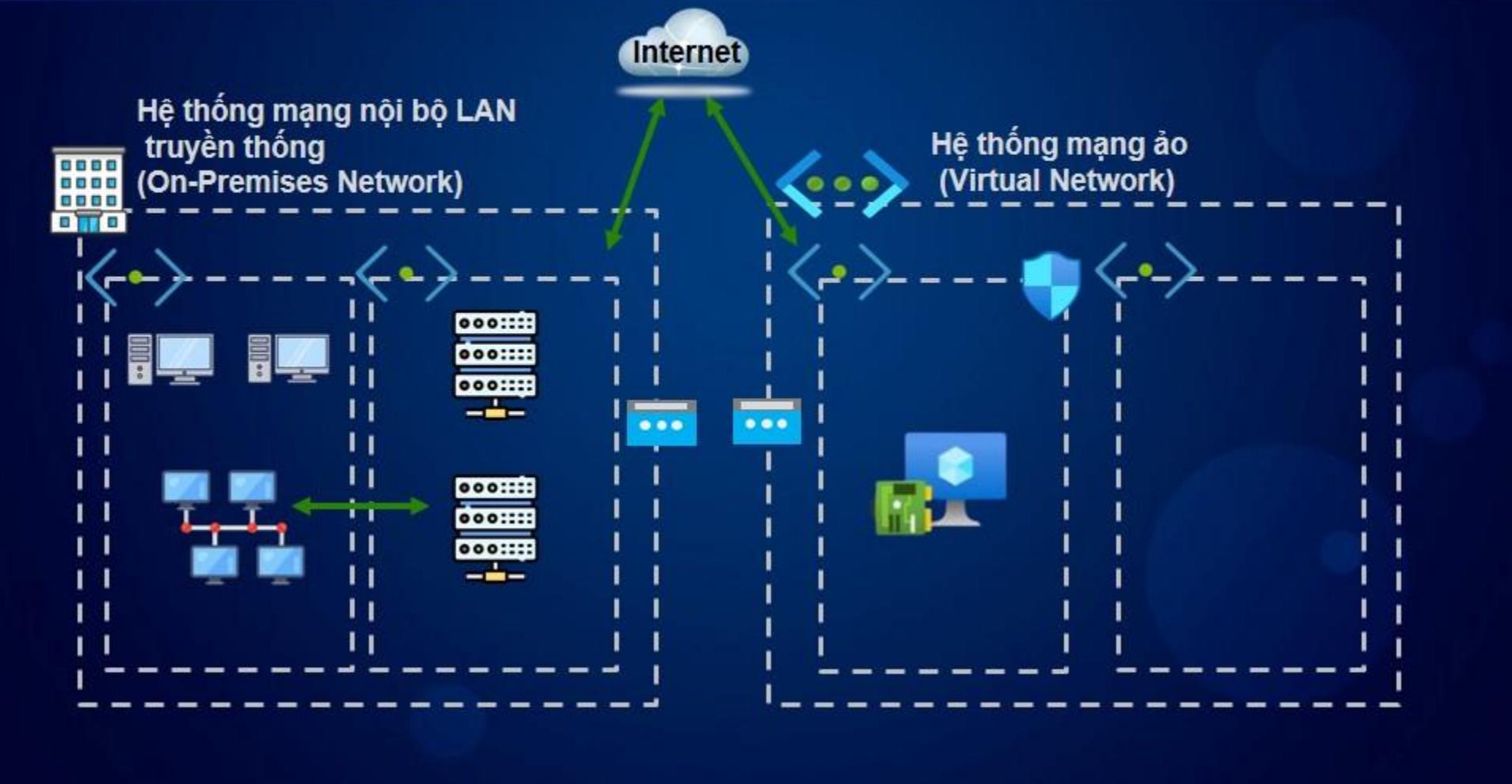


Mục đích của một hệ thống mạng (Network)

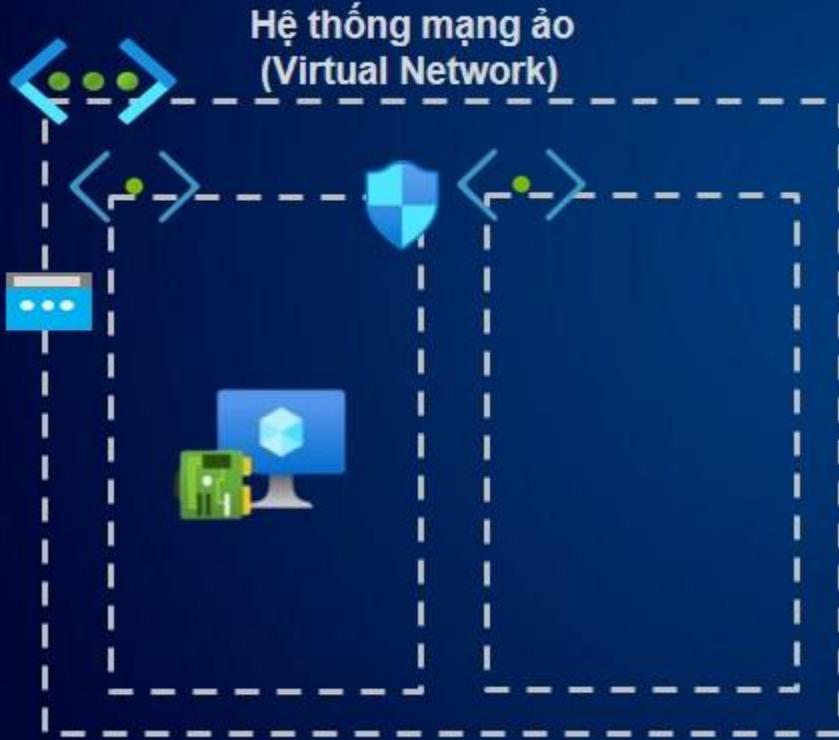
Một hệ thống mạng cho phép bạn có một mạng riêng biệt nơi mà các tài nguyên có thể giao tiếp với nhau và với các mạng bên ngoài

- Người dùng (Users) truy cập vào các file servers
- Dịch vụ chia sẻ máy in(Printer sharing)
- Web servers
- App server truy cập database servers và kết nối internet

So sánh hệ thống mạng truyền thống và hệ thống mạng ảo



Mô tả hệ thống mạng ảo(Virtual Network)



1

Hệ thống mạng riêng biệt

Virtual Networks (Vnets) là các mạng độc lập, riêng biệt trong đám mây Azure

2

Truy cập mạng riêng (Private Network Access)

Cung cấp kết nối, truy cập nội bộ giữa các máy ảo (VMs) hoặc app service

3

Tích hợp hệ thống mạng (Network Integration)

Cho phép kết nối, truy cập giữa các mạng ảo Vnets và các mạng nội bộ hoặc Data Center của công ty(on-prem networks), và các thiết bị cho truy cập từ xa của người dùng.

Các thành phần của hệ thống mạng ảo(Virtual Network)



Dải địa chỉ IP

Dải địa chỉ IP nội bộ cho mỗi một hệ thống mạng ảo. Cấp các địa chỉ cho các tài nguyên.

VNet

Trong hệ thống mạng ảo trong Azure là nơi mà các tài nguyên Azure như máy ảo(VM) được triển khai.

Mạng con(subnet)

Chia một mạng ảo ra thành các mạng con nhỏ hơn (sub-networks) nơi mà các tài nguyên sẽ tồn tại ở trong đó.

Các điểm chính của bài học

Mục đích của một hệ thống mạng (Network)

Một hệ thống mạng cho phép bạn có một mạng riêng biệt nơi mà các tài nguyên có thể giao tiếp với nhau và với các mạng bên ngoài



Hệ thống mạng riêng biệt

Virtual Networks (Vnets) là các mạng độc lập, riêng biệt trong đám mây Azure



Truy cập mạng riêng (Private Network Access)

Cung cấp kết nối, truy cập nội bộ giữa các máy ảo (VMs) hoặc app service



Tích hợp hệ thống mạng (Network Integration)

Cho phép kết nối, truy cập giữa các mạng ảo Vnets và các mạng nội bộ hoặc Data Center của công ty (on-prem networks), và các thiết bị cho việc truy cập từ xa của người dùng.

Tạo hệ thống mạng ảo

Virtual Networks

Bài học bao gồm

Thiết kế một hệ thống mạng

Các tính năng của hệ thống mạng ảo(VNet)

Demo: Tạo một VNet

Các điểm chính của bài học

Thiết kế một hệ thống mạng



Định nghĩa IP CIDR

Lựa chọn một Classless Inter-Domain Routing (CIDR) notation cho phép linh hoạt và dễ dàng mở rộng khi bạn cần thêm địa chỉ IP hoặc các subnets trong hệ thống mạng



Các yêu cầu phân chia các mạng con subnets

Xác định một giải pháp mạng về cách phân đoạn(segment) cho hệ thống mạng để đáp ứng nhu cầu cụ thể của bạn. **Ví dụ:** Phân đoạn mạng theo các lớp (tiers) cho kiến trúc hệ thống mạng.



Các kết nối mạng cần thiết

Xác định loại kết nối cần thiết như: Internet, tài nguyên tới tài nguyên, tài nguyên tới dịch vụ, VV.



Các tính năng của hệ thống mạng ảo(VNet)

Mạng con(subnet)

Azure Vnet sử dụng các mạng con(subnets) để chia các dải địa chỉ IP. Dải địa chỉ IP có thể sử dụng từ x.x.x.0-3 đến x.x.x.255

Mạng riêng nội bộ (Private Networking)

Azure Vnet hỗ trợ dịch vụ DHCP, để cấp các IP nội bộ(private IP) cho các tài nguyên

Mạng public internet (Public Networking)

Azure Vnet hỗ trợ public IP(IPv4 và IPv6) để các tài nguyên có thể có kết nối public internet

Peering

Azure Vnet hỗ trợ kết nối peering giữa các Azure Vnets

Network Gateway

Azure Vnet sử dụng các gateway subnets để tạo các kết nối VPN

Network Gateway

Azure Vnets giúp việc giám sát (monitoring) trở nên dễ dàng. Bạn có thể xem các logs, theo dõi tình trạng kết nối và xem một biểu đồ mô tả cấu trúc mạng ảo (topology) của mạng đó.



Demo: Tạo một VNet



Các điểm chính của bài học



Kết nối mạng mặc định

Mặc định, là mạng ảo cho phép các lưu lượng truy cập mạng nội bộ (infra-network traffic) và lưu lượng mạng đi ra ngoài internet

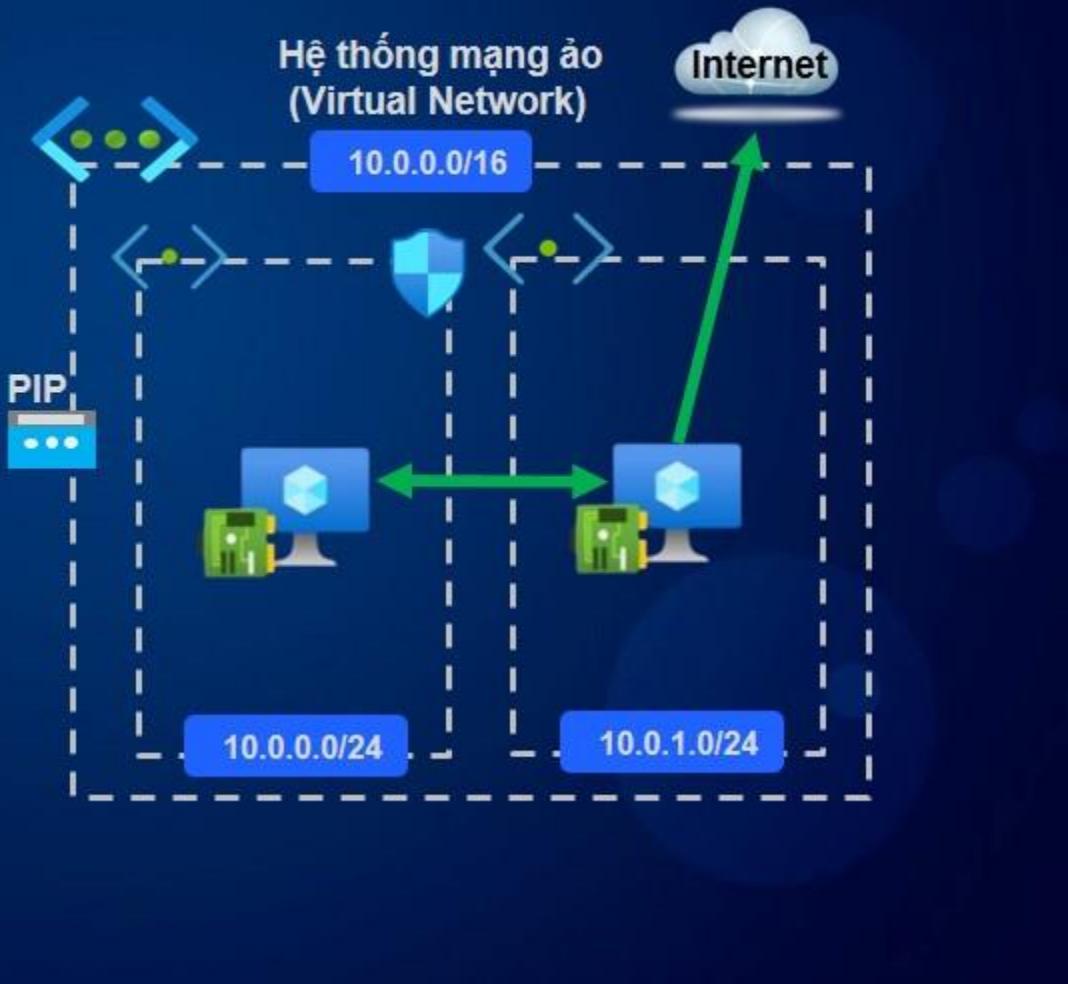


khuyến nghị sử dụng địa chỉ IP private theo tiêu chuẩn RFC 1918. Theo RFC 1918 thì các phạm vi địa chỉ IP private, bao gồm một số dải IP: 10.0.0.0/8, 172.16.0.0/12 và 192.168.0.0/16. Một VNet hoặc subnet cho phép có size từ /29 (cho mạng nhỏ) đến /8 (cho mạng lớn)



IP dành riêng(Reserved IPs)

Azure dành riêng để sử dụng các địa chỉ IP là X.X.X.0-3 và X.X.X.255



Thực hành tạo các Subnets trong Azure

Trong tình huống của bài thực hành này, công ty của bạn cần cấm(block) kết nối truy cập giữa 2 máy ảo VMs. Hai máy ảo này được đặt trong cùng một mạng con subnet. Vậy chúng ta cần phải di chuyển một máy ảo sang một mạng con subnet khác, và cấm kết nối truy cập giữa hai máy ảo sử dụng một tường lửa network security group.



Tạo một mạng ảo, và
tạo 02 máy ảo



Tạo một Subnet mới,
và tường lửa NSG và
rules cho tường lửa mới



Di chuyển VM tới
Subnet mới



Hoàn thành
bài lab



Giai đoạn 1



Giai đoạn 2



Giai đoạn 3



Giai đoạn 4

Triển khai các tài nguyên mạng

Bài học bao gồm

Địa chỉ IP

Các loại địa chỉ IPs

Public IP SKUs

Cấu hình card mạng ảo(NIC IP Configurations)

Demo: Tạo các tài nguyên mạng

Các điểm chính của bài học

Địa chỉ IP

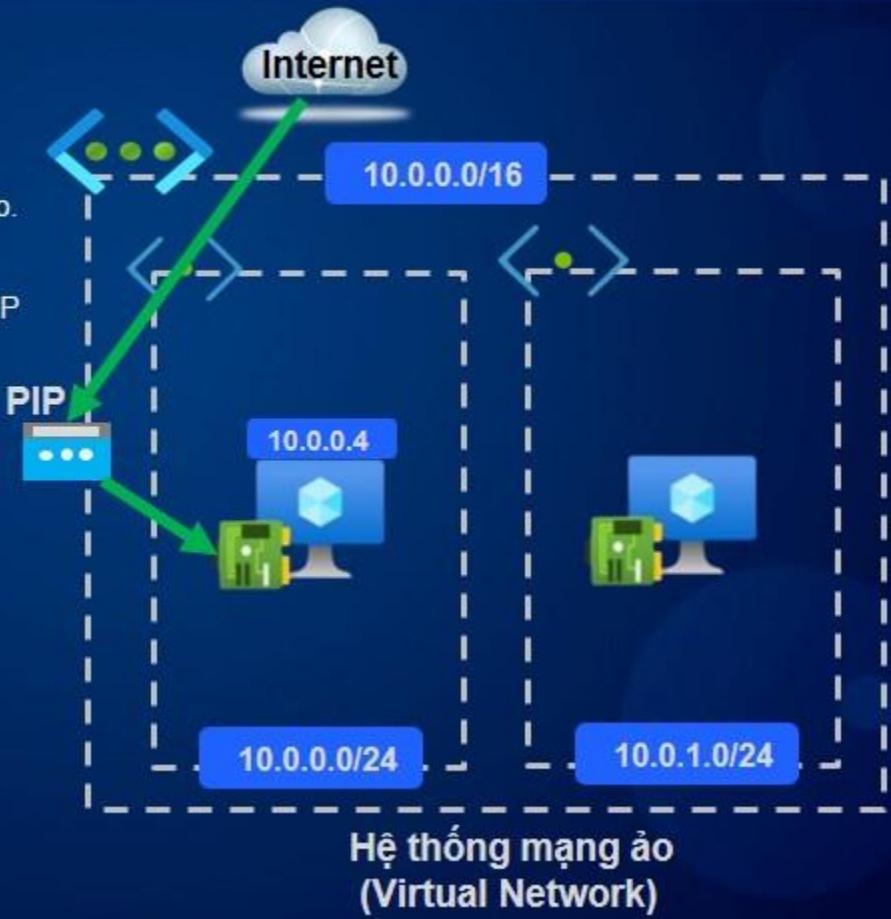
Kết nối trong mạng nội bộ

Có thể sử dụng Vnets để cung cấp các kết nối truy cập giữa các tài nguyên bên trong mạng ảo.

Có thể sử dụng Vnets để cung cấp các public IP cho các tài nguyên bên trong mạng ảo.

Lập kế hoạch IP CIDR

Lập kế hoạch sao cho không có sự trùng lặp dải địa chỉ IP, giúp cho việc tích hợp hệ thống mạng một cách hiệu quả mà không gặp vấn đề xung đột địa chỉ IP



Các loại địa chỉ IP

Private IPs

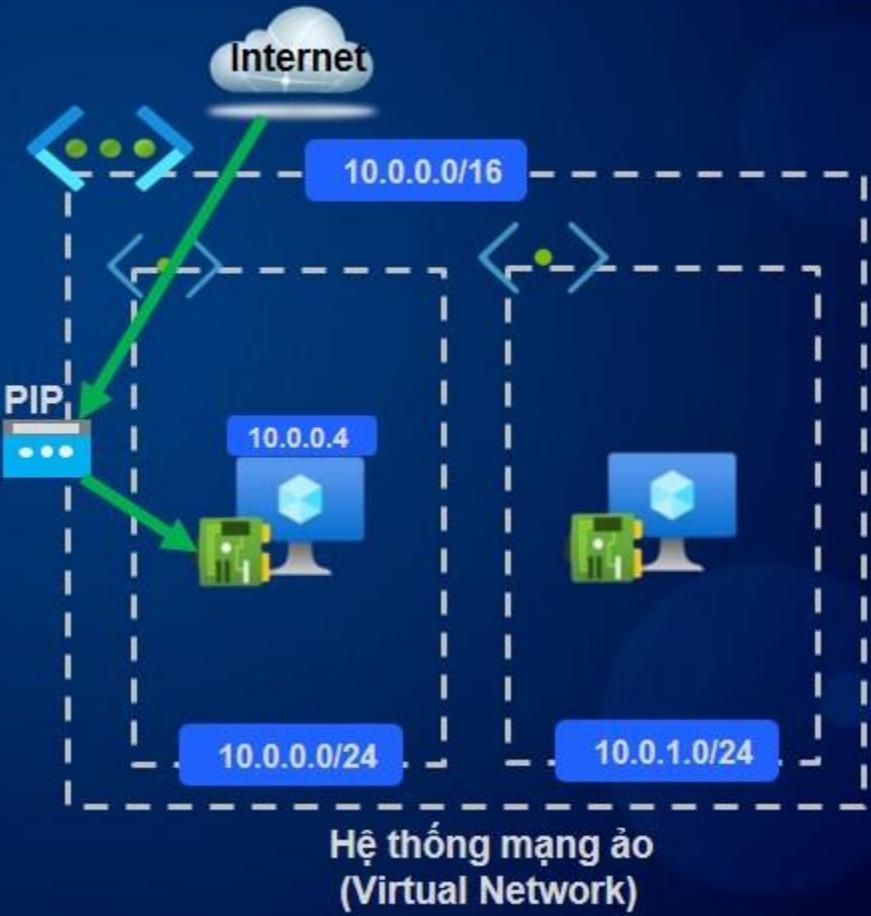


Cấp các địa chỉ IP động và tĩnh cho phép kết nối truy cập giữa các tài nguyên bên trong hệ thống mạng ảo



Public IPs

Cấp các địa chỉ IP cho phép kết nối truy cập từ ngoài internet vào một tài nguyên



Public IP SKUs

Basic SKU

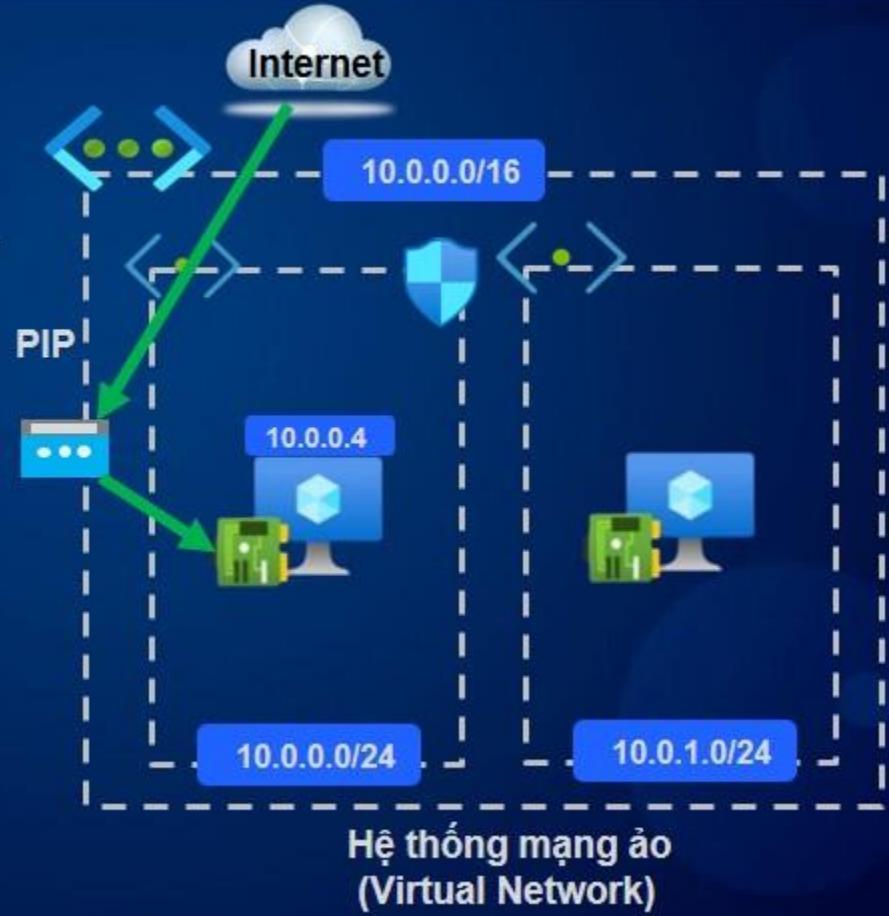


Là một dạng cơ bản của Public IP, có thể được cấp địa chỉ IP tĩnh hoặc động, mặc định có thể truy cập từ ngoài internet sử dụng Public IP này. Nhưng cần sử dụng các quy tắc NSG để kiểm soát lưu lượng traffic, và không hỗ trợ triển khai trên nhiều vùng Availability Zone.

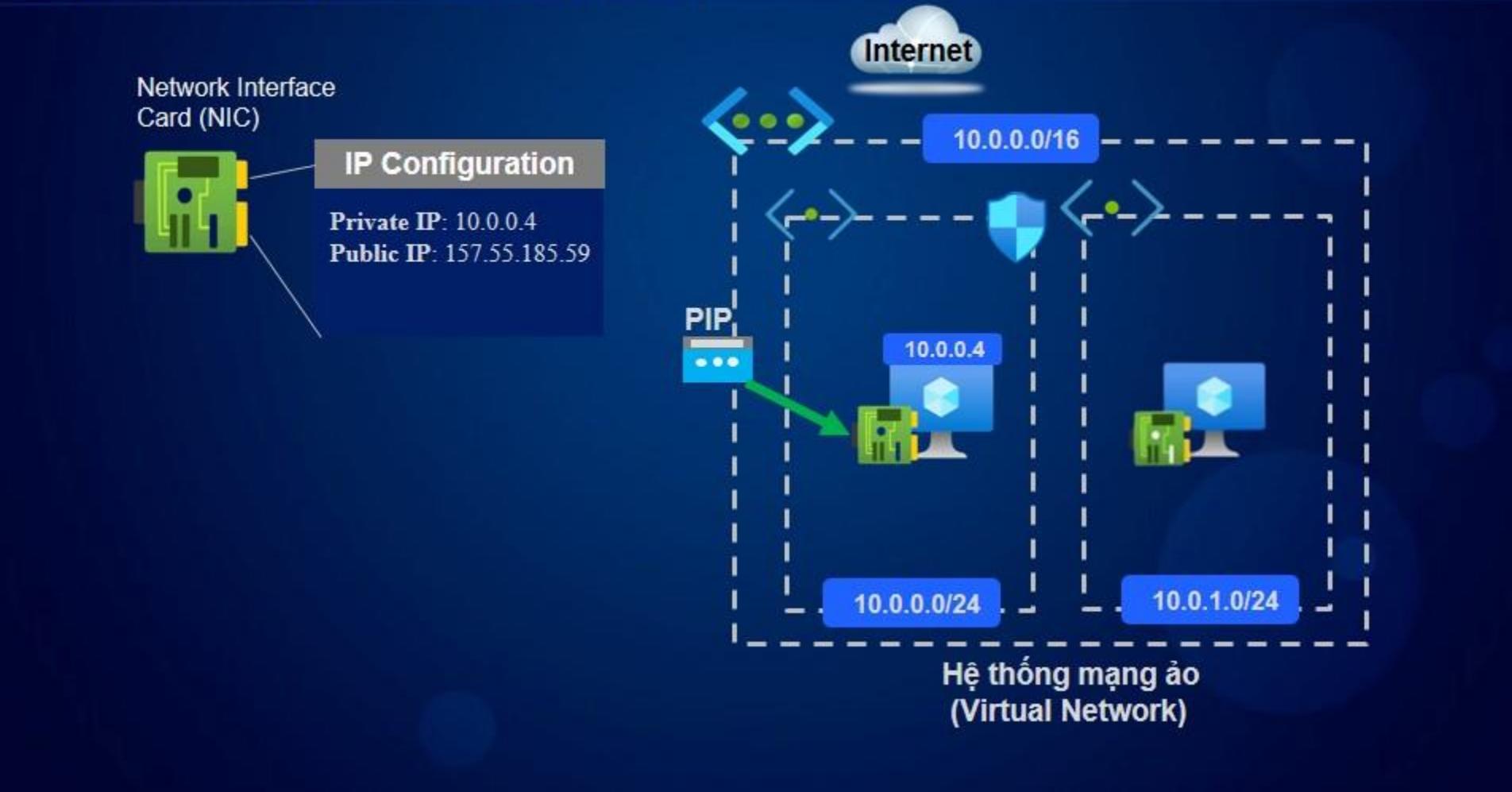


Standard SKU

Được cấp địa chỉ Public IP tĩnh, mặc định có thể cho phép truy cập từ ngoài internet và yêu cầu cần có NSG để cho phép kiểm soát lưu lượng traffic. Hỗ trợ triển khai trên nhiều vùng availability zone



Cấu hình card mạng ảo(NIC IP Configurations)



Các điểm chính của bài học

Network Interface
Card (NIC)



IP Configuration

Private IP: 10.0.0.4
Public IP: 157.55.185.59

Private IPs



Cấp các địa chỉ IP động và tĩnh cho phép kết nối truy cập giữa các tài nguyên bên trong hệ thống mạng ảo



Public IPs

Cấp các địa chỉ IP cho phép kết nối truy cập từ ngoài internet vào một tài nguyên

Hai loại Public IP SKUs:

- Basic
- Standard

Định tuyến(Routing) hệ thống mạng ảo

Bài học bao gồm

**Mô tả về định tuyến(routing) hệ thống
mạng ảo**

Các loại định tuyến

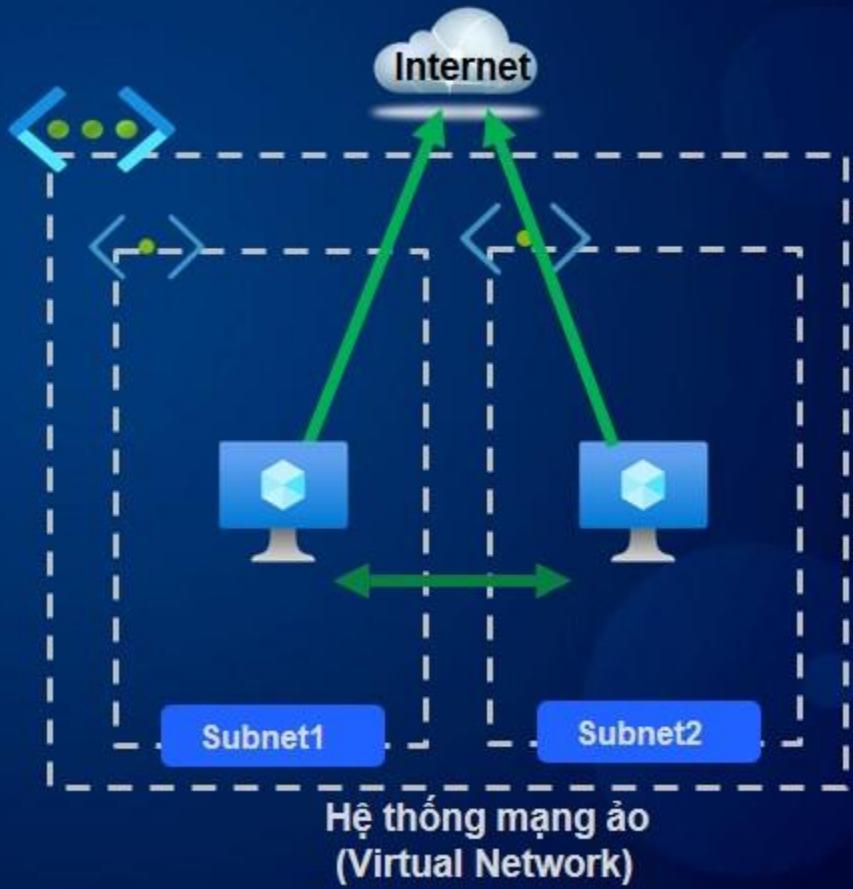
Demo: Routing hệ thống mạng ảo

Các điểm chính của bài học

Mô tả về định tuyến(routing) hệ thống mạng ảo

- Các định tuyến (Routes) = Các tuyến đường(Paths) mà dữ liệu sẽ đi qua để đến đích
- Các định tuyến là các tuyến đường mà traffic mạng có thể đi qua.

Ví dụ: Một định tuyến(route) cho phép các máy ảo (VMs) có thể truy cập ra ngoài(outbound) internet.



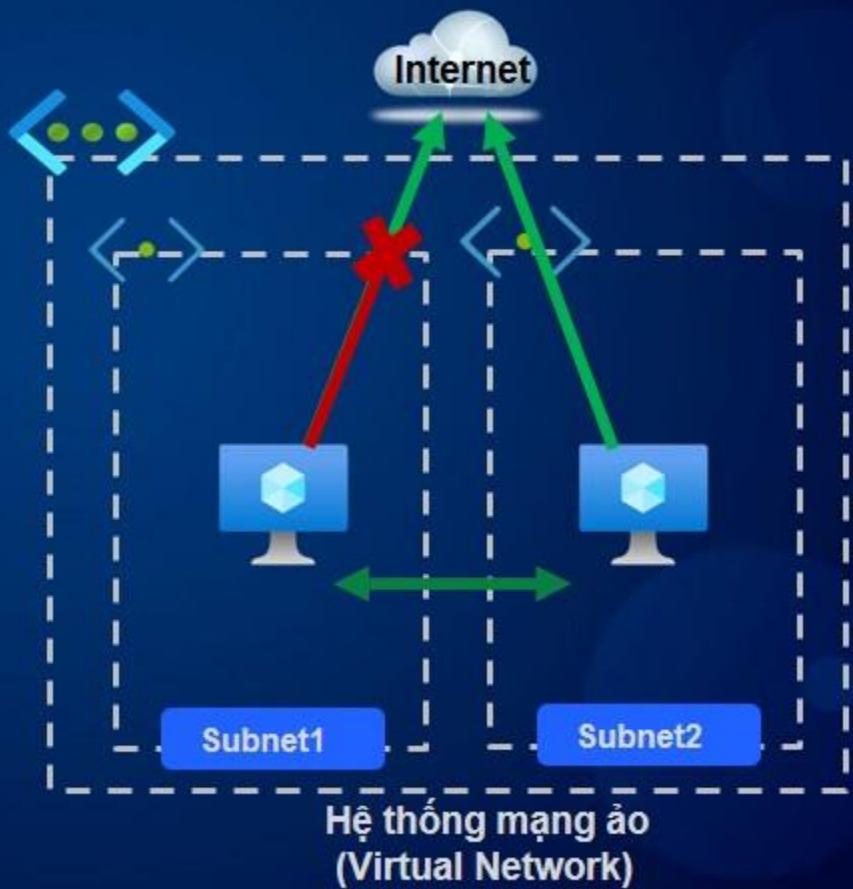
Các loại định tuyến

- **Định tuyến hệ thống (System Routes)**

Các định tuyến mặc định(Default routes) được Azure tạo ra cho các mạng ảo, và không thể sửa đổi các định tuyến này.

- **Định tuyến do người dùng tạo ra (Custom Routes)**

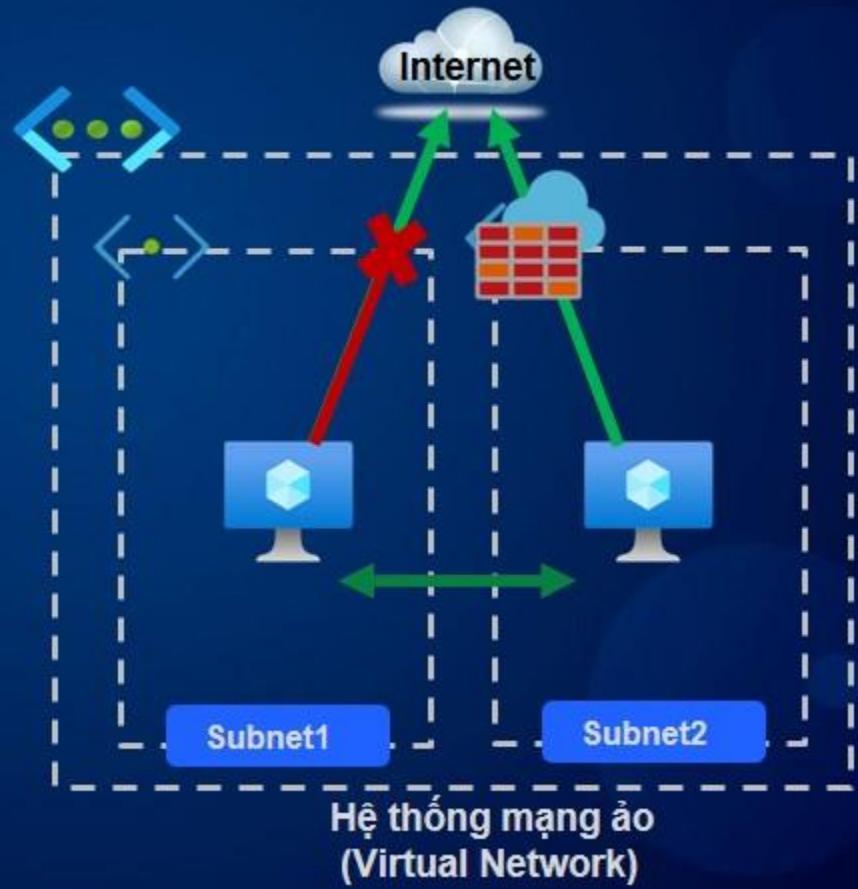
Người dùng định các định tuyến hoặc Border gateway protocol(BGP), và chúng ghi đè lên định tuyến hệ thống (system routes)



Tình huống trong bài Demo

- Người dùng định nghĩa định tuyến (User-Defined Route)
- Các định tuyến được tạo ra bởi người dùng sẽ được ưu tiên hơn tất cả các định tuyến khác được tạo ra tự động hoặc thông qua các cấu hình mặc định.

Ví dụ: Có thể tạo ra một định tuyến ghi đè lên các định tuyến ra ngoài internet, để các luồng truy cập mạng (network traffic) không đi đến Internet, mà thay vào đó có thể đi đến không có gì hoặc đi đến một thiết bị ảo như tường lửa Azure Firewall.



Các điểm chính của bài học

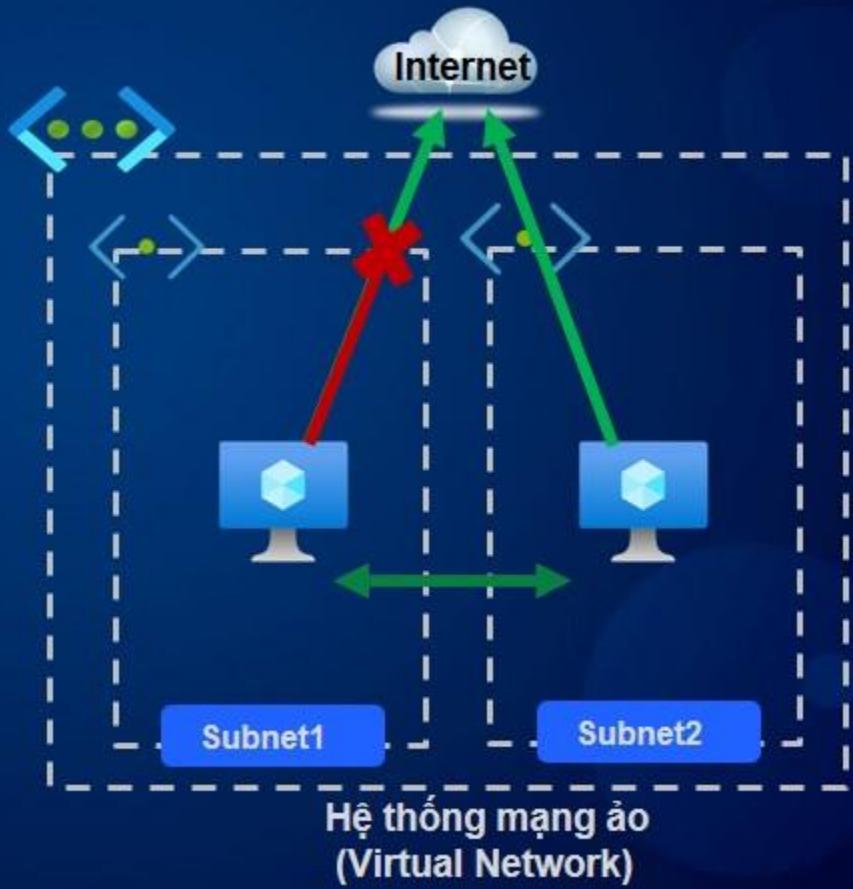
- **Định tuyến hệ thống (System Routes)**

Các định tuyến mặc định(Default routes) được Azure tạo ra cho các mạng ảo, và không thể sửa đổi các định tuyến này.

- **Định tuyến do người dùng tạo ra (Custom Routes)**

Người dùng định các định tuyến hoặc Border gateway protocol(BGP), và chúng ghi đè lên định tuyến hệ thống (system routes)

Custom > BGP >System



Network Security Groups

Bài học bao gồm

Định nghĩa NSGs

Mô tả kiến trúc NSGs

Demo: Thực hiện cấu hình NSGs

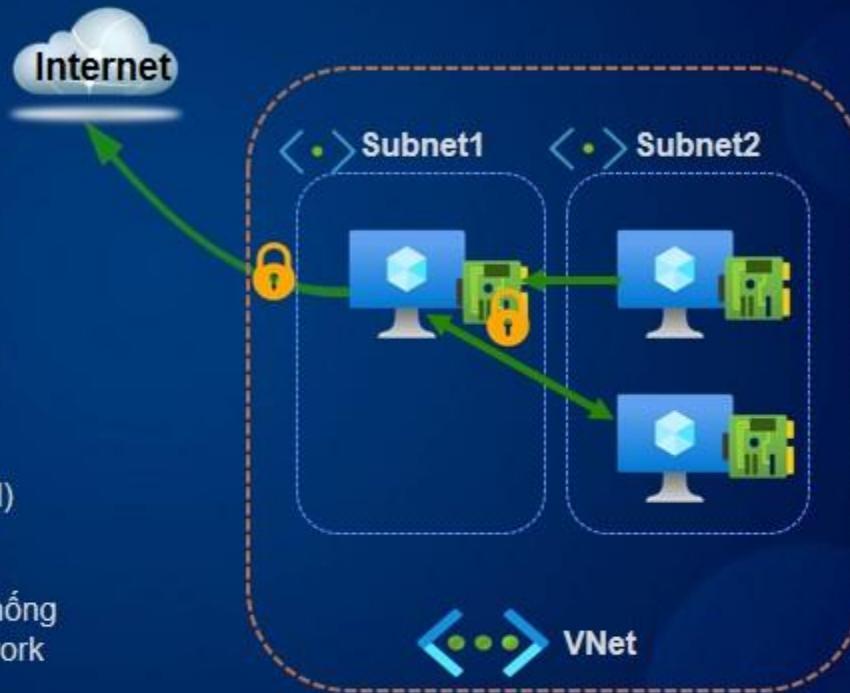
Các điểm chính của bài học

Định nghĩa NSGs

NSGs kiểm soát các luồng truy cập mạng traffic

Một Network Security Group (NSG) kiểm soát các luồng truy cập đi vào và đi ra cho một mạng ảo (Virtual Network) trong Azure. Chúng ta có thể thực hiện việc cấu hình NSGs như sau:

- Tạo quy tắc(rules) định nghĩa cho phép(allowed) /cấm(denied)
- Kiểm soát bảo mật(security) tại các cấp độ hệ thống mạng con(subnet) hoặc card mạng ảo NIC network



Định nghĩa NSGs



Filter Traffic

Xác định traffic nào sẽ được cho phép hoặc từ chối đi vào (inbound) và đi ra (outbound)



Rules

Đánh giá các quy tắc mặc định (default rules) và quy tắc của người dùng định nghĩa(user-defined rules) tạo ra



Priority

Chỉ định mức độ ưu tiên để sắp xếp thứ tự ưu tiên của các quy tắc(rules). Số càng thấp độ ưu tiên càng cao

Priority ↑	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓
▼ Inbound Security Rules				
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer
65500	DenyAllInBound	Any	Any	Any
▼ Outbound Security Rules				
65000	AllowVnetOutBound	Any	Any	VirtualNetwork
65001	AllowInternetOutBound	Any	Any	Any
65500	DenyAllOutBound	Any	Any	Any

Định nghĩa NSGs



Liên kết

không có ảnh hưởng gì nếu nó không được liên kết (associated) với một subnet hoặc một card mạng ảo (NIC).



Thứ tự ưu tiên

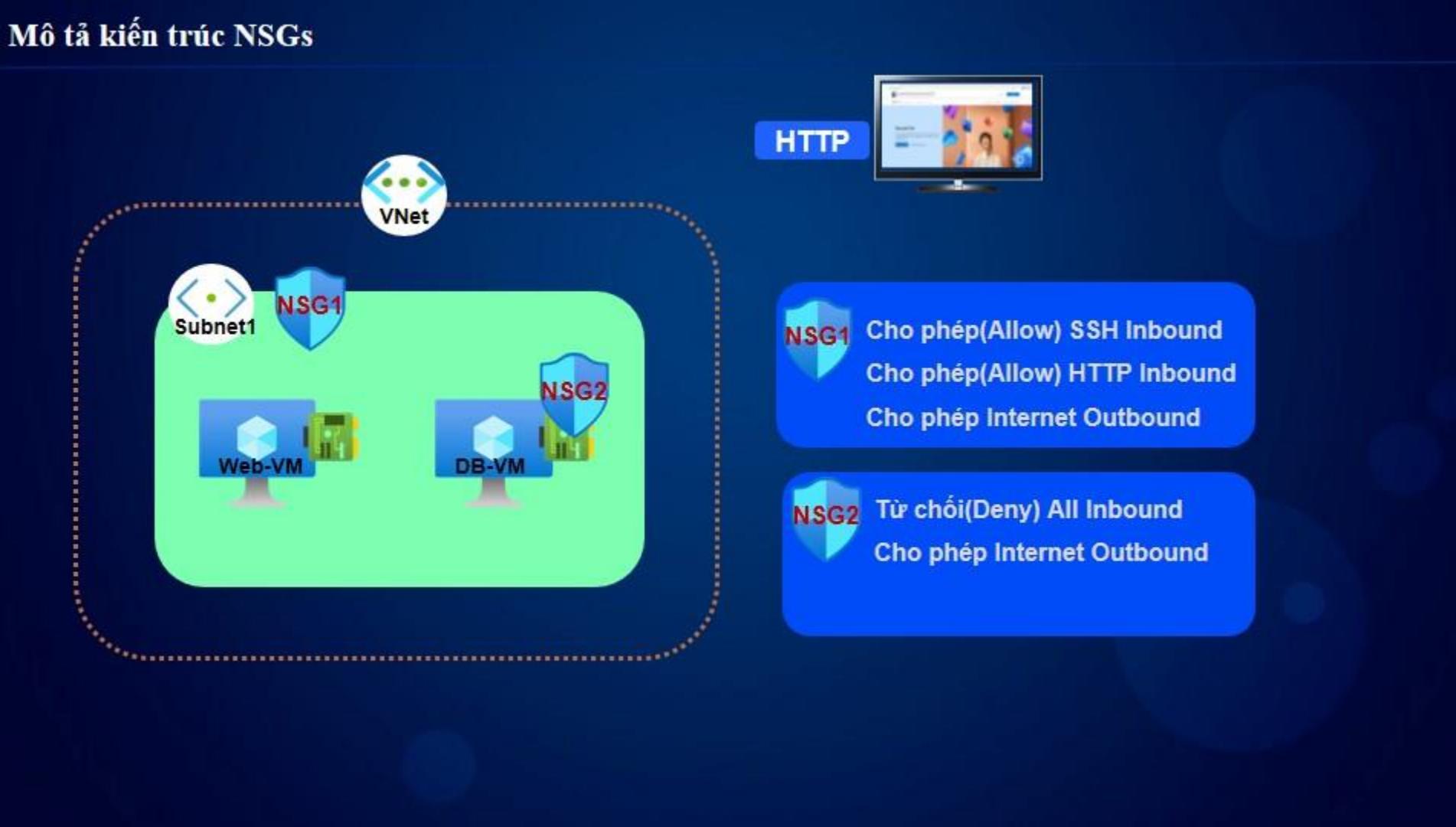
Các quy tắc (rules) trong NSGs được xử lý theo thứ tự từ trên xuống dưới trong danh sách. Khi một quy tắc được khớp (matched) với traffic, thì không có quy tắc nào khác được đọc (read)



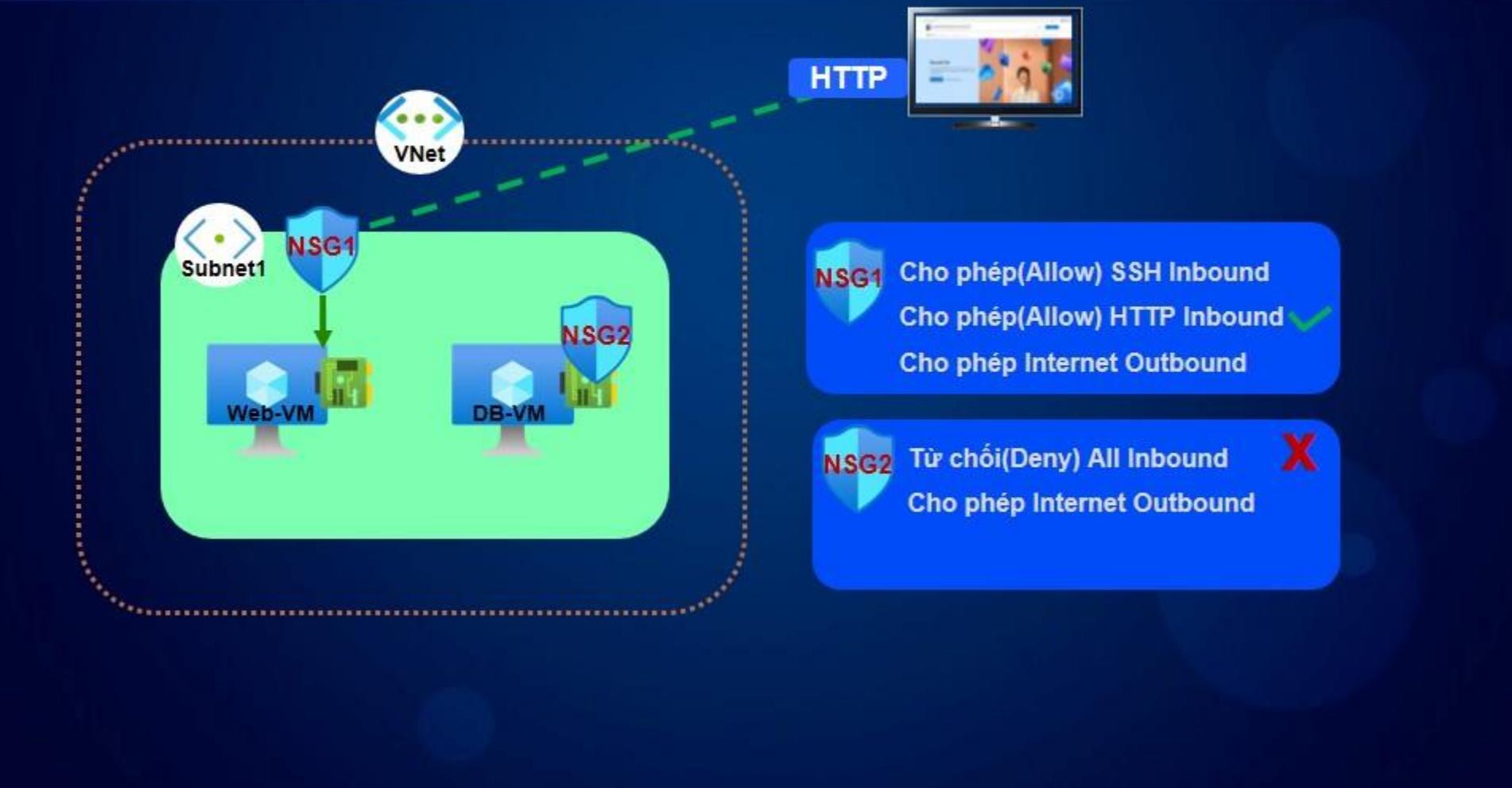
Định nghĩa NSGs

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
✓ Inbound Security Rules						
100 Allow_ssh 22 TCP Any Any Allow						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
✓ Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

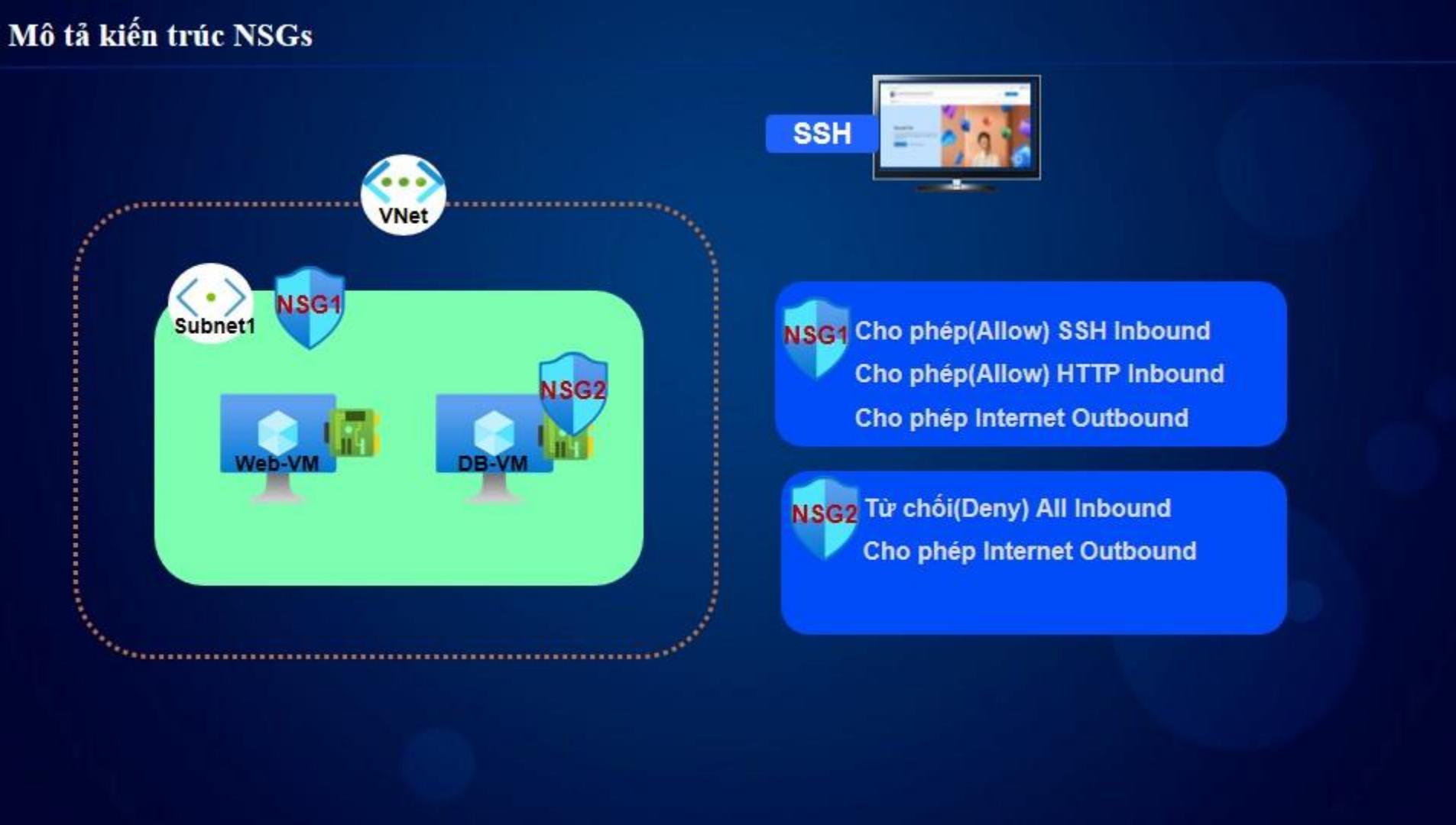
Mô tả kiến trúc NSGs



Mô tả kiến trúc NSGs



Mô tả kiến trúc NSGs



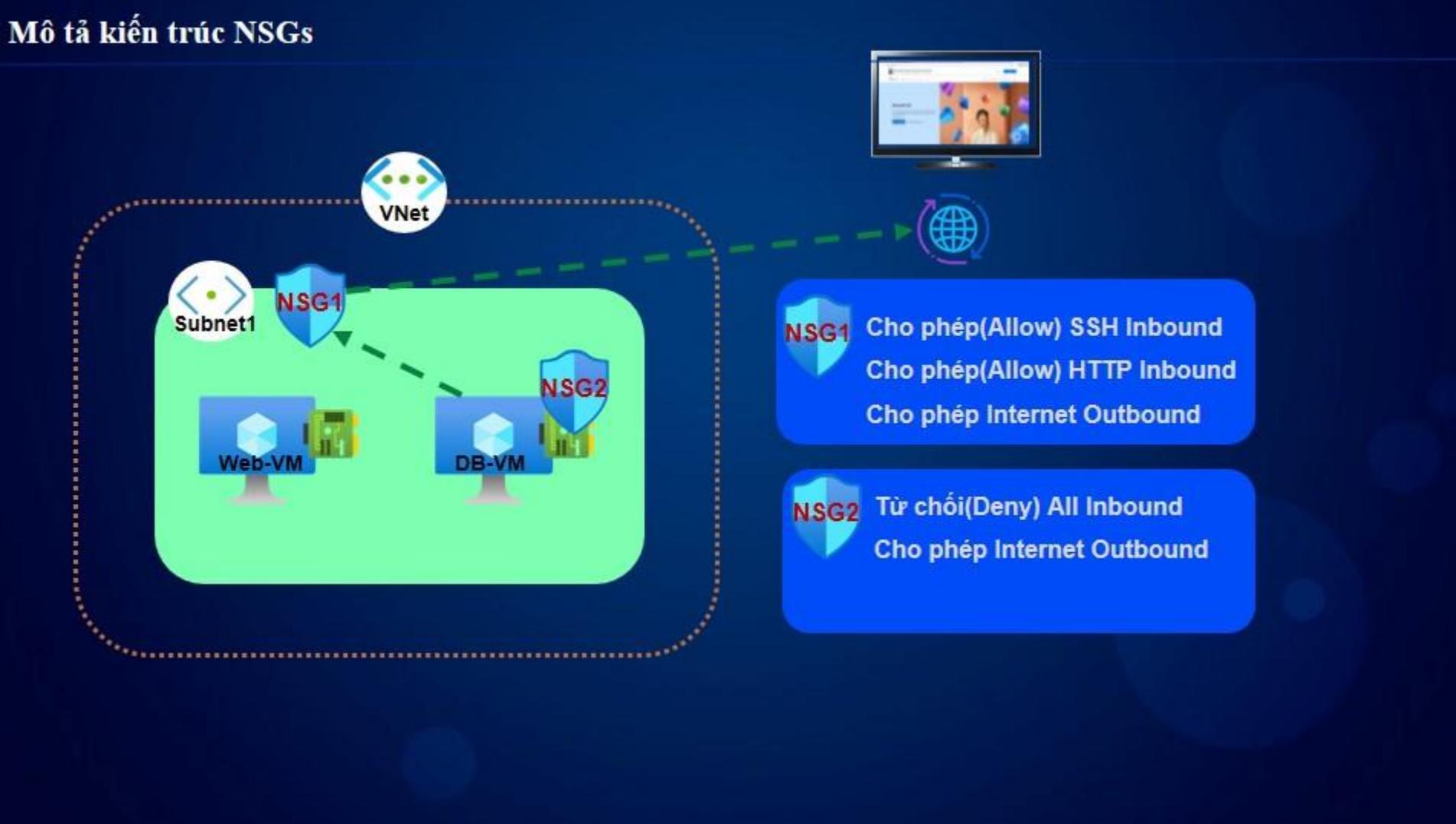
Mô tả kiến trúc NSGs



Mô tả kiến trúc NSGs



Mô tả kiến trúc NSGs



Các điểm chính của bài học

Network Security Groups kiểm soát Traffic

1 Lọc traffic

Cho phép(allow) hoặc từ chối(deny) sử dụng các quy tắc(rules) được định nghĩa bởi các thuộc tính như độ ưu tiên(priority), cổng(port), Giao thức(protocol), nguồn(source), đích đến(destination), và hành động(action).

2 Liên kết (Association)

NSG có thể được liên kết với các mạng con subnets hoặc các card mạng ảo của các máy ảo VM. Và nếu khi chúng bị hủy bỏ liên kết(unassociated), chúng không có ảnh hưởng đến việc kiểm soát traffic.

3 Quy tắc(Rules)

Không thể xóa các quy tắc mặc định , và người dùng có thể định nghĩa tạo ra các quy tắc.

4

Cách quy tắc trong Network Security Groups (NSGs) được áp dụng theo hướng traffic.

Traffic từ bên ngoài vào (Inbound):

Khi có một gói tin từ bên ngoài vào mạng con (subnet), các quy tắc Inbound của mạng con (subnet) sẽ được kiểm tra đầu tiên. Sau đó, nếu gói tin chuyển tiếp đến card mạng (NIC) của máy ảo, các quy tắc Inbound của card mạng sẽ được áp dụng.

Traffic từ bên trong ra ngoài (Outbound):

Ngược lại, khi có một gói tin từ bên trong mạng con (subnet) ra ngoài, các quy tắc Outbound của card mạng (NIC) sẽ được kiểm tra đầu tiên. Sau đó, nếu gói tin đi tiếp ra khỏi mạng con, các quy tắc Outbound của mạng con sẽ được áp dụng.

Thực hành tạo một Application Security Group Cho hai Web Servers trong Azure

Trong tình huống của bài thực hành này, công ty của bạn đã chuẩn bị hai web servers và họ muốn cung cấp dịch vụ web cho người dùng từ ngoài internet. Cả hai servers này đã được cài đặt dịch vụ IIS, nhưng cả hai servers này chưa được mở cổng 80(HTTP) hoặc cổng 443(HTTS) để cho phép người dùng truy cập từ ngoài internet vào. Bạn được giao công việc tạo một application security group và liên kết nó với một network security group để mở hai cổng này, cho phép 2 servers có thể truy cập được từ ngoài internet.

- ✓ **Chúng ta cần vào đường link :**

<https://raw.githubusercontent.com/phuongluuho/Azure104/main/LabnsgWebSRV.json>
để copy nội dung file LabnsgWebSRV.json

- **Sau đó sử dụng ARM Templates để tạo ra một môi trường cho bài thực hành gồm:**
02 máy ảo windows webservers, 01 storage account,
02 card mạng ảo, 01 mạng ảo Virtual network,
02 Public IP, 01 tường lửa network security group



Tạo một Application
Security Group



Tạo một rule mới cho
Network Security Group



Kiểm tra kết nối truy
cập từ ngoài internet
vào 2 webservers



Hoàn thành
bài lab



Giai đoạn 1



Giai đoạn 2



Giai đoạn 3



Giai đoạn 4

Sử dụng Azure DNS

Bài học bao gồm

Mô tả Azure DNS

Mô tả Record Sets

Mô tả Alias Records

Demo: Thực hiện cấu hình Azure DNS

Các điểm chính của bài học

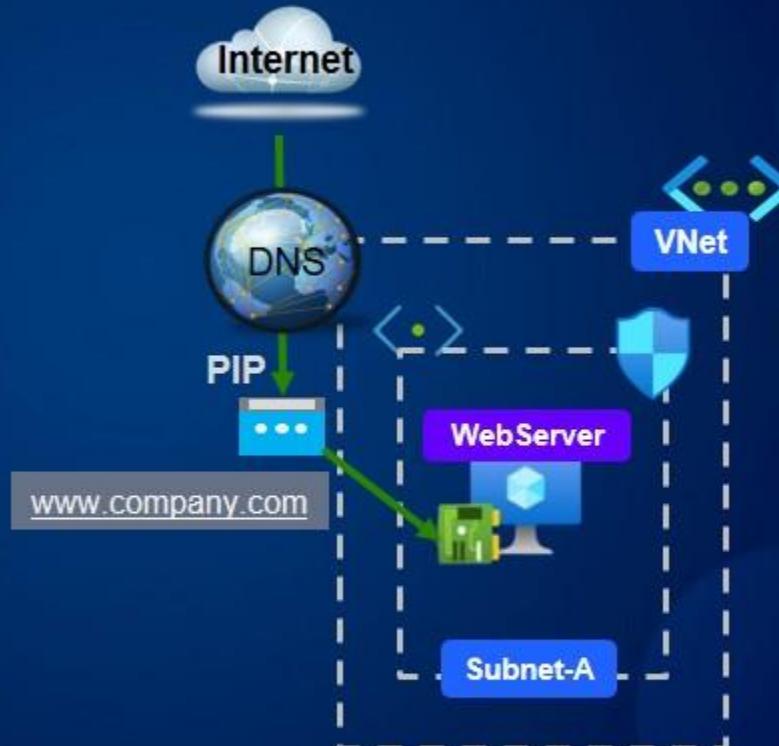
Mô tả Azure DNS

Azure DNS

Một Domain Name System (DNS) dịch vụ hosting cung cấp dịch vụ phân giải tên miền.

Có thể sử dụng:

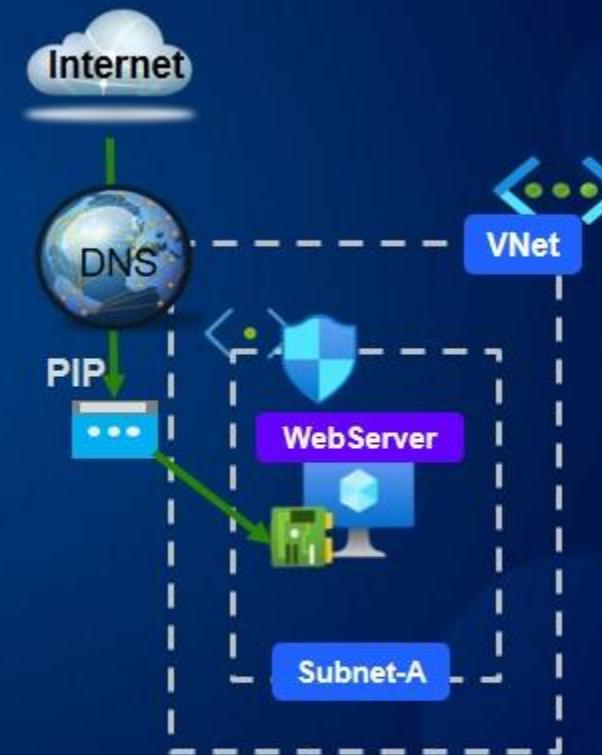
- Records/record sets
- Hỗ trợ A, AAAA, CNAME, TXT, MX, PTR, SRV, và SOA
- Private/public zones



Mô tả Record Sets

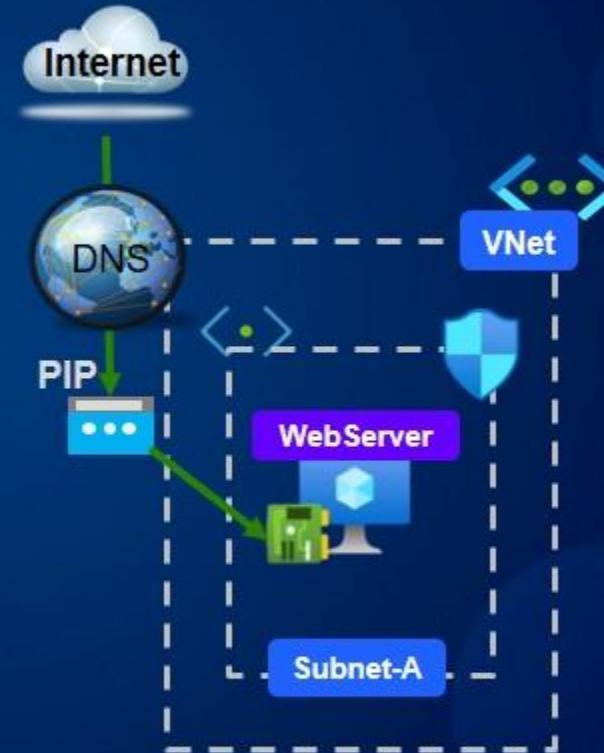
Record		
Name	Type	Value
www.company.com	A	Public IP

Record Set		
Name	Type	Value
www.company.com	A	Public IP 1
www.company.com	A	Public IP 2



Mô tả Record Alias Records

Alias Record		
Name	Type	Value
www.company.com	A	Target_Resource



Các điểm chính của bài học

Các tính năng của Azure DNS:

- Role-Based Access Control (RBAC)
- Nhật ký Activity logs
- Khóa tài nguyên (Resource Locking)
- Private DNS Zone
- Alias Records



Sử dụng tường lửa Azure Firewall

Bài học bao gồm

Mô tả về Azure Firewall

Các tính năng của Azure Firewall

Các bước triển khai Azure Firewall

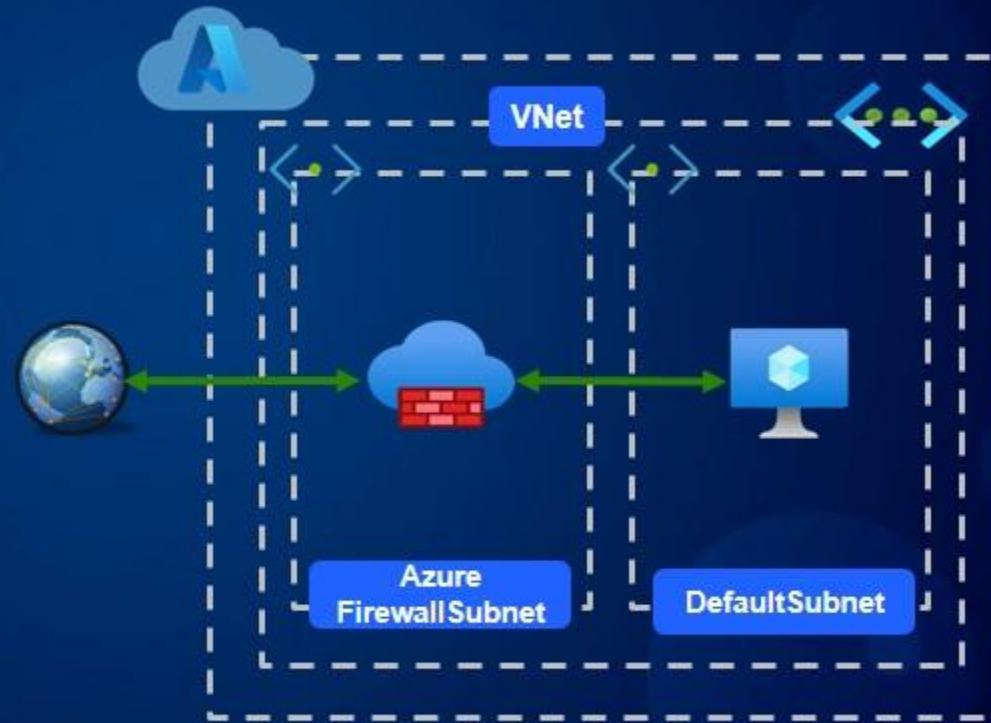
Demo: Cấu hình Azure Firewall

Các điểm chính của bài học

Mô tả Azure Firewall

Azure Firewall

- Sử dụng Platform as a service (PaaS) Azure Firewall để lọc các traffic
- Hỗ trợ Fully qualified domain name (FQDN)



Các tính năng của Azure Firewall

DNAT và SNAT

Cấu hình các quy tắc outbound/inbound NAT rules cho các hệ thống mạng ảo Vnets của bạn

01

Các quy tắc mạng (Network rules)

Cấu hình lớp network (layer 4) rules cho traffic nào được phép

02

Các quy tắc ứng dụng (App rules)

Cấu hình các quy tắc cho việc lọc các websites được truy cập từ hệ thống mạng ảo của bạn

03

Giám sát (Monitoring)

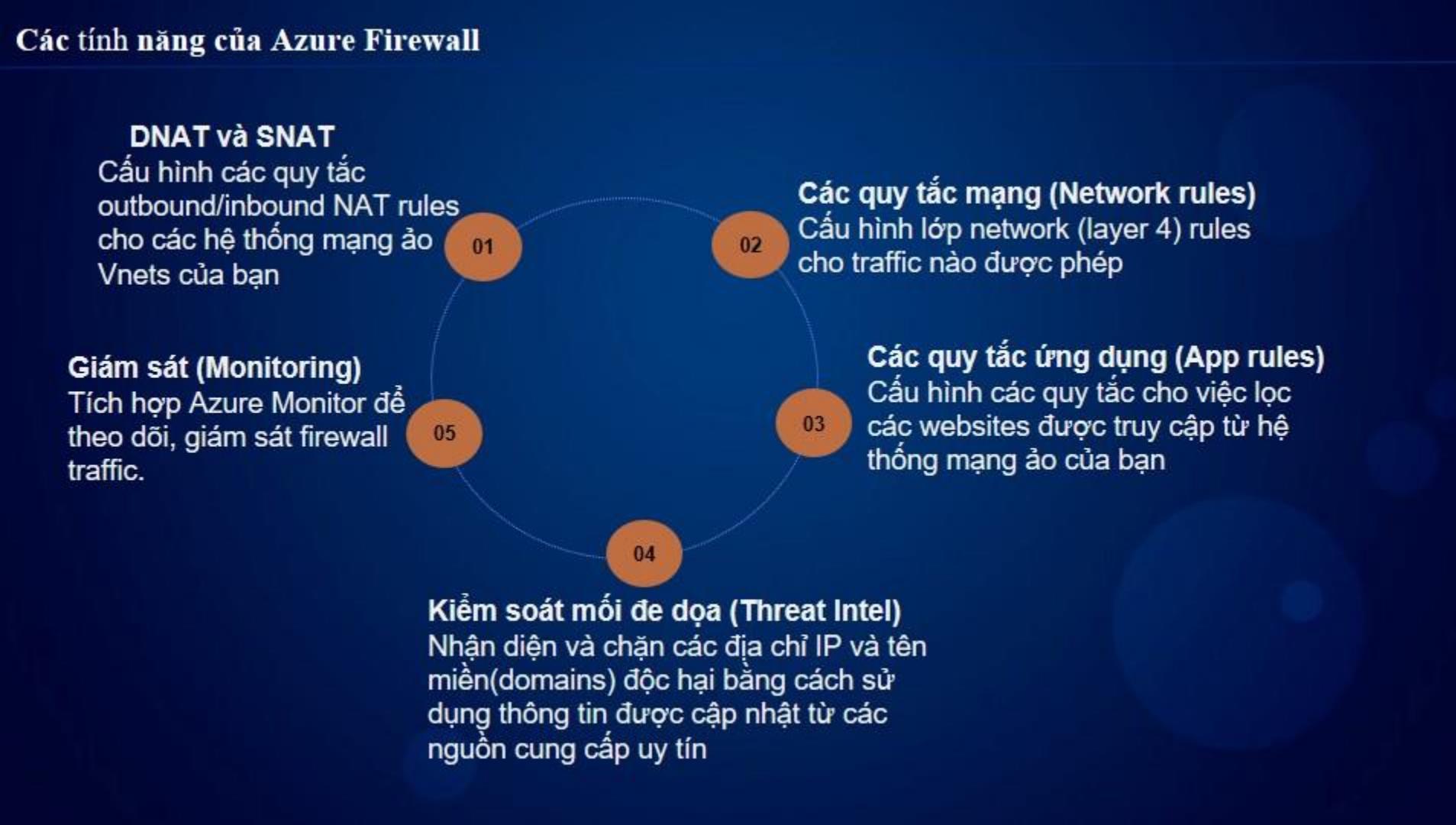
Tích hợp Azure Monitor để theo dõi, giám sát firewall traffic.

05

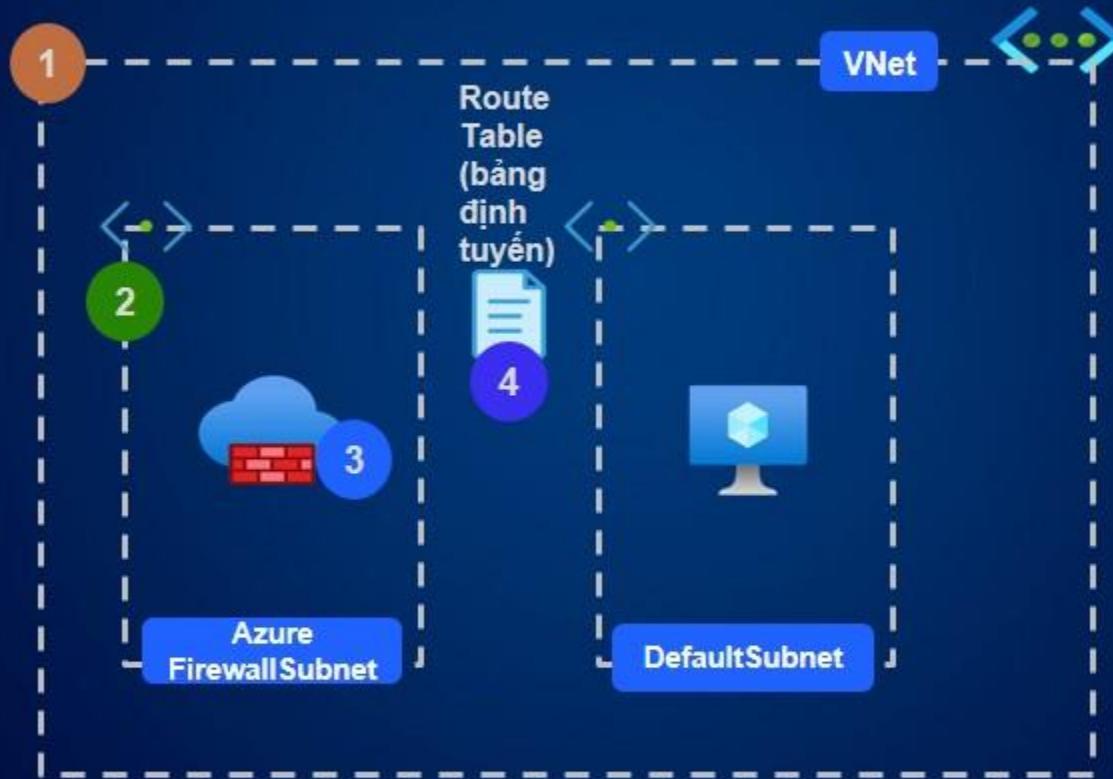
04

Kiểm soát mối đe dọa (Threat Intel)

Nhận diện và chặn các địa chỉ IP và tên miền(domains) độc hại bằng cách sử dụng thông tin được cập nhật từ các nguồn cung cấp uy tín

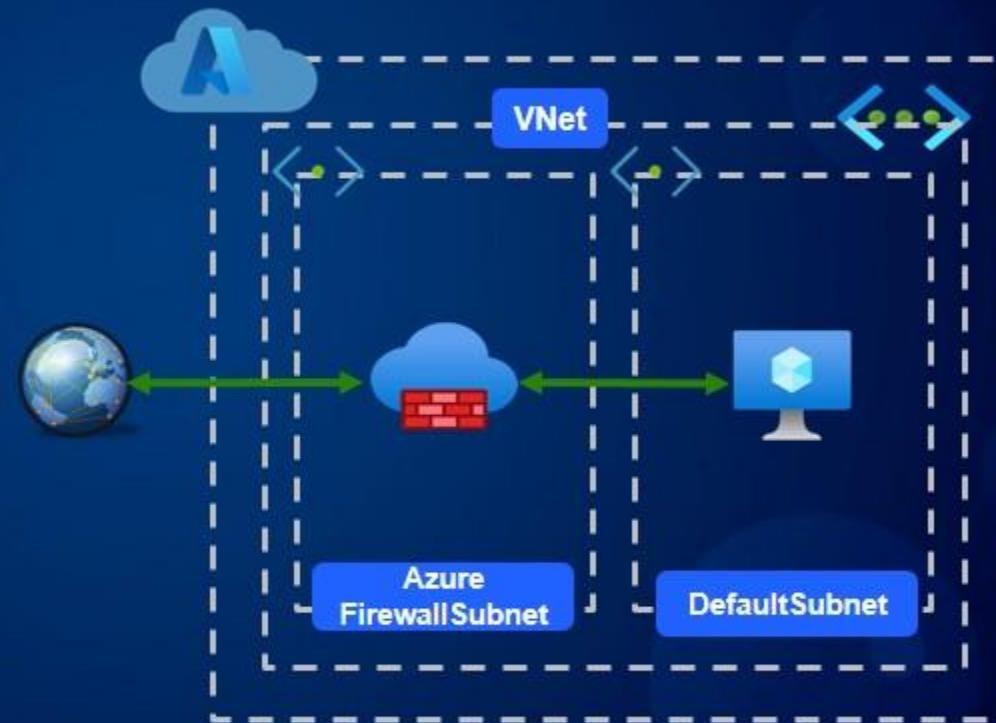


Các bước triển khai Azure Firewall



Các điểm chính của bài học

- Nat rules**
- Network rules**
- Application rules**



Thực hành tạo một tường lửa (Azure Firewall) và áp dụng nó cho mạng ảo Vnet trong Azure

Trong tình huống của bài thực hành này, công ty của bạn cần hạn chế các traffic của server truy cập ra bên ngoài. Họ muốn bạn ngăn chặn người dùng users truy cập vào các loại domain vd: <https://microsoft.com> , và họ không muốn cho phép server truy cập ra ngoài qua cổng 53. Vậy bạn cần có một giải pháp cho việc như sau:

- Giúp công ty của bạn tạo ra một tường lửa Azure Firewall, sau đó kết nối và áp dụng nó trong hệ thống mạng ảo Vnet, và đáp ứng với các yêu cầu trong việc hạn chế các traffic truy cập từ server.
- Cho phép mở cổng 3389 RDP, để người dùng có thể truy cập remote desktop vào server từ ngoài internet
- Users chỉ có thể truy cập vào www.microsoft.com từ bên trong server
- Chỉ cho phép mở cổng 53 cho 8.8.8.8, 8.8.4.4 (Google DNS Servers), để server có thể sử dụng các DNS Servers này.



Tạo một máy ảo, một subnet cho tường lửa,và một tường lửa Azure Firewall



Tạo một bảng định tuyến (route table)



Cấu hình tường lửa
Và kiểm tra việc kết nối bên trong máy ảo



Hoàn thành bài lab



Giai đoạn 1



Giai đoạn 2



Giai đoạn 3



Giai đoạn 4

Sử dụng Service Endpoints

Bài học bao gồm

Truy cập các dịch vụ PaaS

Mô tả về Service Endpoints

Các đặc điểm của Service Endpoint

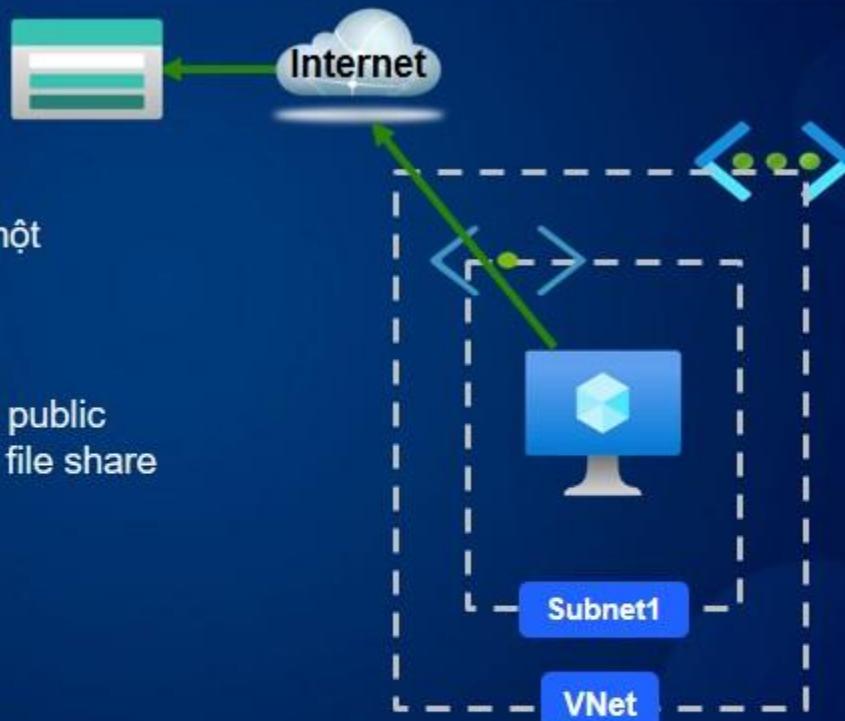
Demo: Cấu hình một Service Endpoints

Các điểm chính của bài học

Truy cập các dịch vụ PaaS

Kết nối Platform as a Service (PaaS)

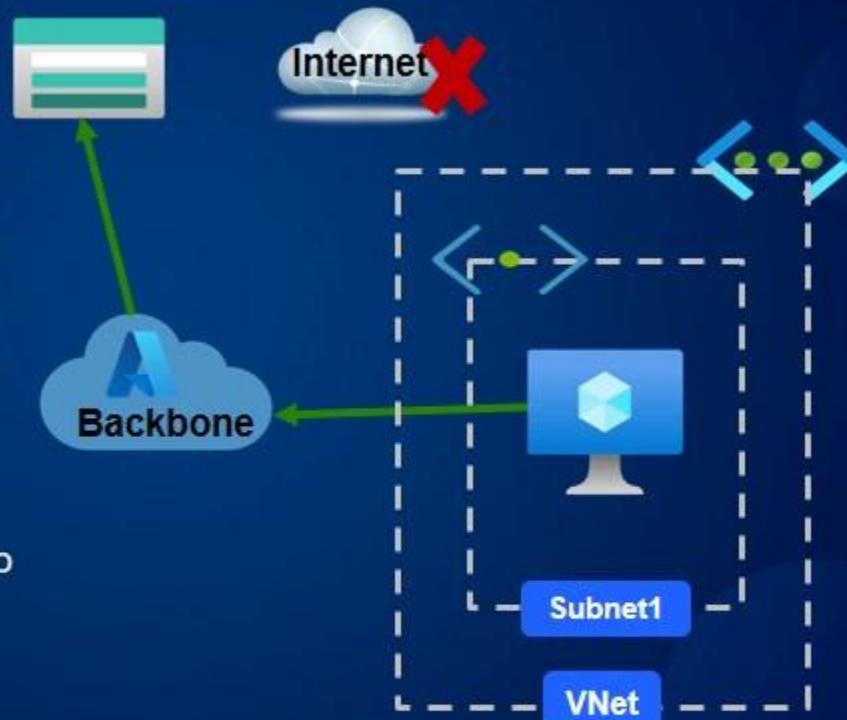
- ✓ Mặc định, các dịch vụ Microsoft có một public endpoint.
- ✓ **Ví dụ:** Một máy ảo VM sử dụng một public Endpoint để truy cập vào một Azure file share trong một storage account



Mô tả về Service Endpoints

Service Endpoint

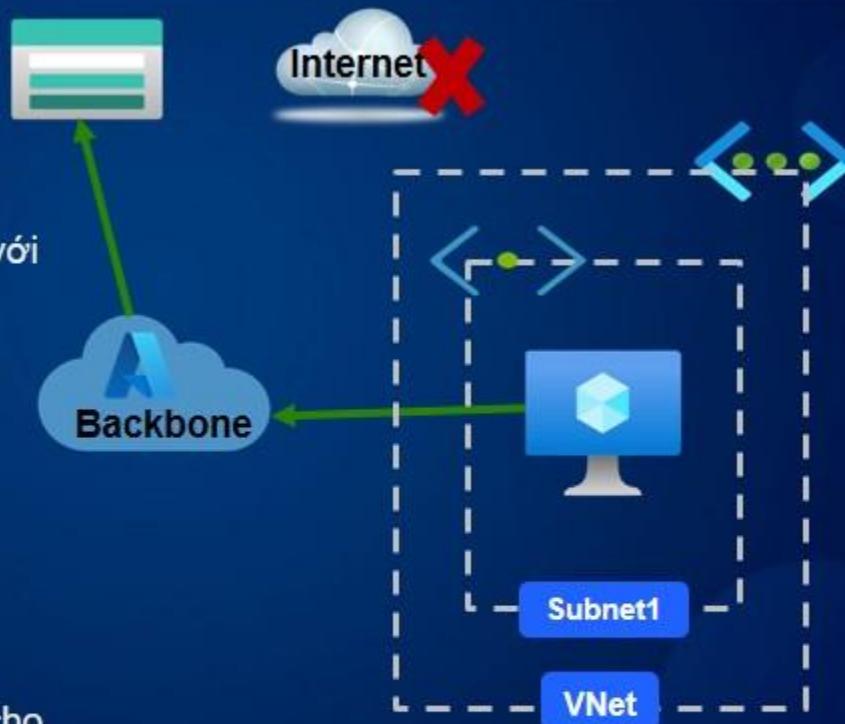
-  Sử dụng service endpoints, bạn có thể cung cấp một kết nối nội bộ vào một dịch vụ từ bên trong một mạng ảo Vnet
-  **Ví dụ:** Một máy ảo VM sẽ sử dụng một service endpoint để truy cập vào một Azure file share trong một storage account



Các đặc điểm của Service Endpoints

Service Endpoint

- Cho phép mỗi một subnet kết nối với service endpoint
- Không hỗ trợ tất cả các dịch vụ
- Hỗ trợ các dịch vụ tại các region
- Không sử dụng một private IP cho việc kết nối các dịch vụ
- Tùy chọn tường lửa trong storage account có thể tăng tính bảo mật cho việc kết nối

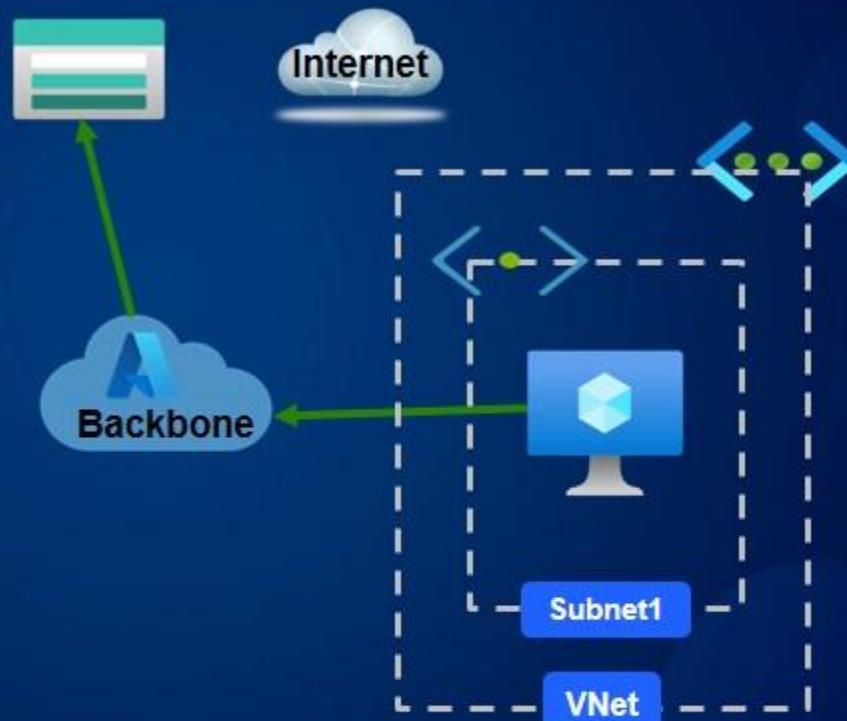


Các điểm chính của bài học

Service Endpoint

Chúng ta có thể sử dụng một service endpoint để cho phép các subnets trong các mạng ảo có thể kết nối nội bộ vào các dịch vụ Azure.

- Giảm thiểu việc bị tấn công mạng
- Cho phép sử dụng NSG rules
- Định tuyến nâng cao



Sử dụng Private Endpoints

Bài học bao gồm

Mô tả về Private Endpoints

Các môi trường Hybrid Network

Demo: Cấu hình một Private Endpoint

Các điểm chính của bài học

Mô tả về Private Endpoints

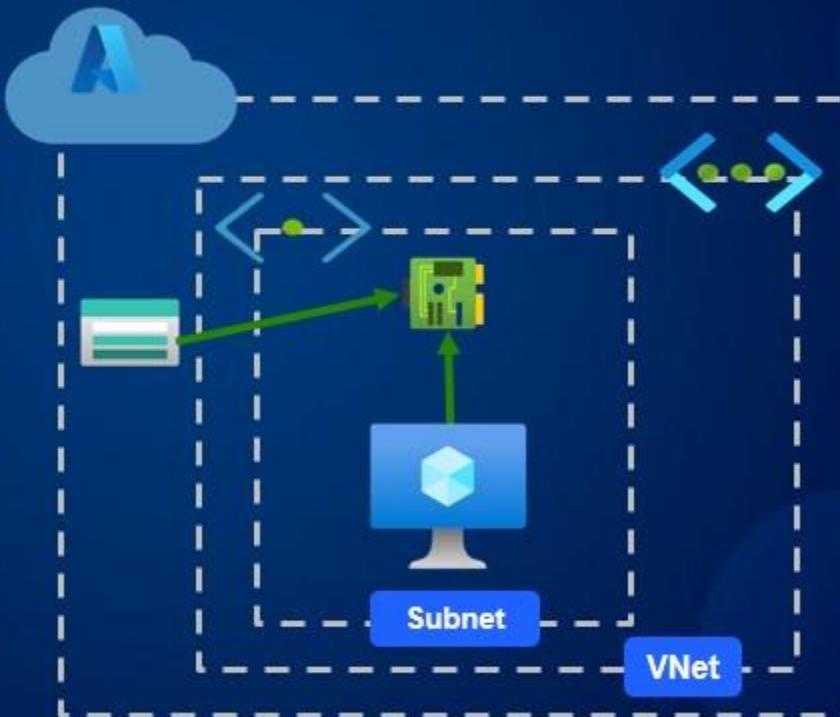
Private Endpoint

Sử dụng Azure Private Link, bạn có thể truy cập đến các dịch vụ giống như bạn đang truy cập vào các tài nguyên bên trong hệ thống mạng nội bộ của bạn, và một private IP thì giống với một private endpoint

Các trường hợp nên sử dụng kết nối private endpoint :

Các dịch vụ Azure (Azure services)

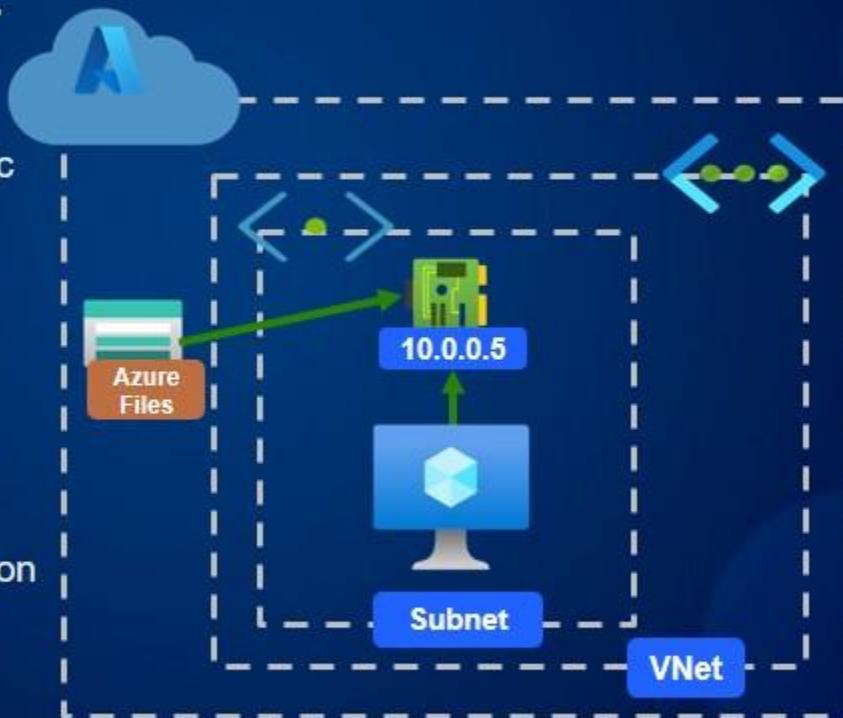
Các dịch vụ của khách hàng/đối tác



Các điểm chính của bài học

Một Private Endpoint cung cấp:

- Một private IP cho việc kết nối vào các dịch vụ Azure
- Kết nối vào các dịch vụ Azure (Azure services)
- Kết nối tới các dịch vụ của khách hàng/đối tác
- Kết nối trực tiếp vào một tài nguyên con (sub-resource) của một dịch vụ Azure ánh xạ(mapping)



Cấu hình Azure Vnet Peering

Bài học bao gồm

Mô tả về Vnet Peering

Các lợi ích của Vnet Peering

Demo: Cấu hình Vnet Peerings

Các điểm chính của bài học

Mô tả về Vnet Peering

Kết nối mạng



Kết nối mạng mặc định

Mặc định các traffic outbound trong mạng nội bộ được cho phép đi ra ngoài Internet. Các mạng ảo mặc định là được cô lập với bên ngoài.



Vnet Peering

Là một cầu nối giữa các mạng ảo, cho phép các mạng ảo kết nối, nói chuyện với nhau như trong cùng một hệ thống mạng nội bộ



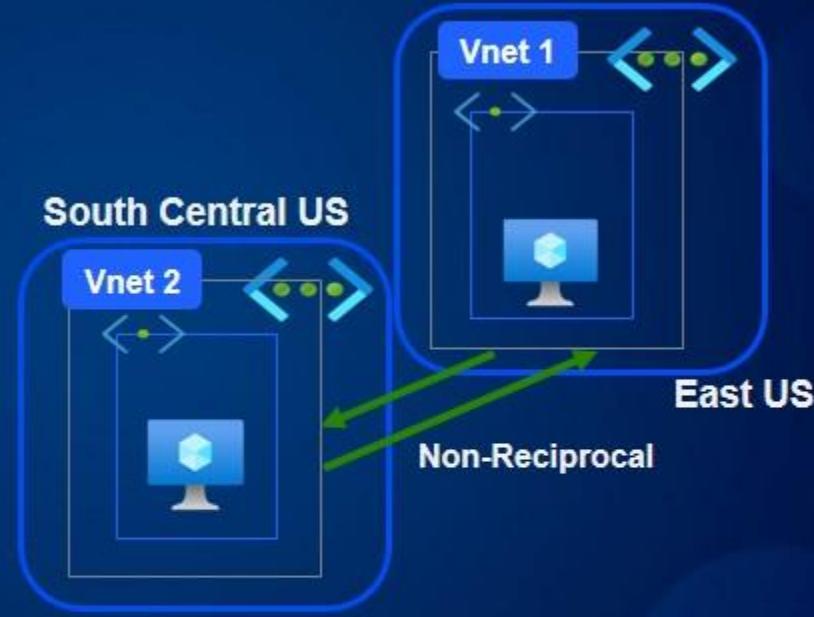
Mô tả về Vnet Peering

Non-Reciprocal

- Việc thiết lập kết nối peering giữa hai mạng ảo cần phải được thực hiện tại cả hai mạng ảo.

Kết nối toàn cầu (Global Connectivity)

- Kết nối Peerings có thể là cùng region hoặc tại các region khác nhau (Global)



Mô tả về Vnet Peering

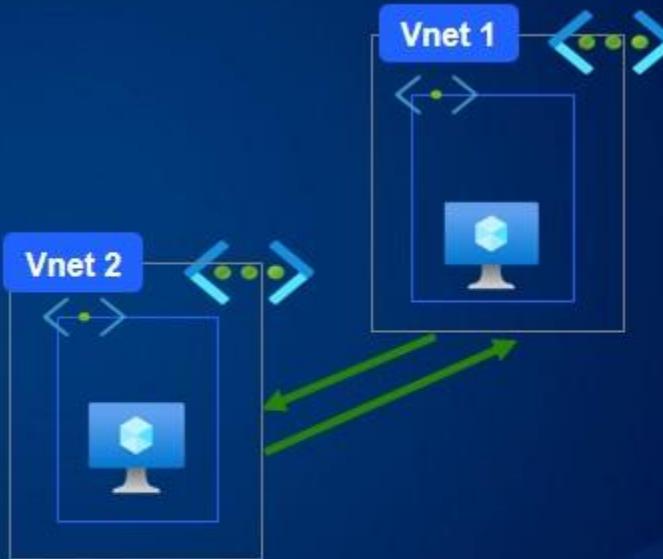


Các lợi ích của Vnet Peering



Các lợi ích

- Độ trễ thấp (Low-latency), kết nối băng thông cao (high-bandwidth)
- khả năng kết nối và trao đổi dữ liệu giữa các mạng ảo khác nhau
- Dữ liệu của các mạng ảo khác nhau, được truyền giữa:
- Các Subscriptions
- AAD tenants qua Azure roles
- Azure regions



Các điểm chính của bài học

Các loại Peering

- Mạng ảo (Virtual network) peering
- Toàn cầu (Global virtual network) peering

Tính chuyên tiếp - Bắc cầu (Transitivity)

- Các kết nối Peering là không có tính bắc cầu (non-transitive)

Các lợi ích

- Độ trễ thấp (Low-latency), kết nối băng thông cao (high-bandwidth)
- khả năng kết nối và trao đổi dữ liệu giữa các mạng ảo khác nhau
- Dữ liệu của các mạng ảo khác nhau, được truyền giữa các Subscriptions, AAD tenants qua Azure roles, Azure regions

Reciprocity

- Các kết nối Peering là không có sự tương hỗ

Triển khai VPNs

Bài học bao gồm

So sánh VPN Gateways và Vnet Peering

Các khả năng của VPN Gateways

Các loại định tuyến và VPN Gateway SKUs

So sánh Active-Active và Active-Passive

Demo: Cấu hình VPN Gateway

So sánh VPN Gateways và Vnet Peering

VPN Gateway



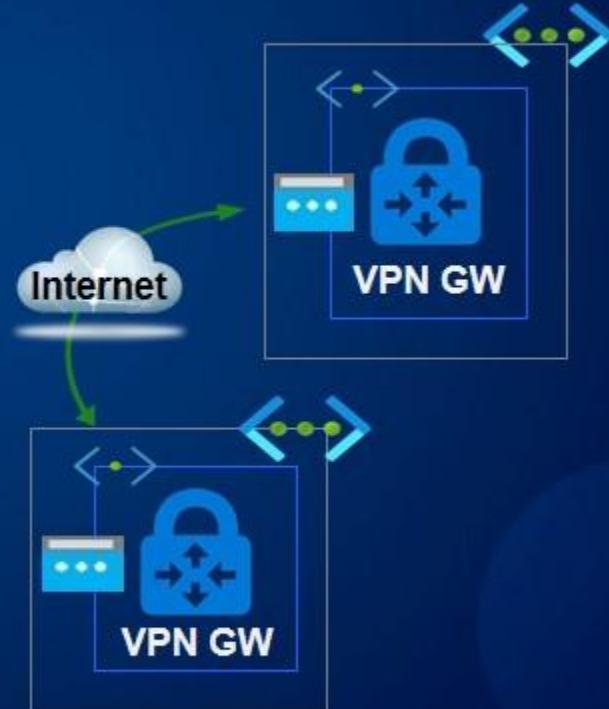
So sánh VPN Gateways và Vnet Peering

VPN Gateway

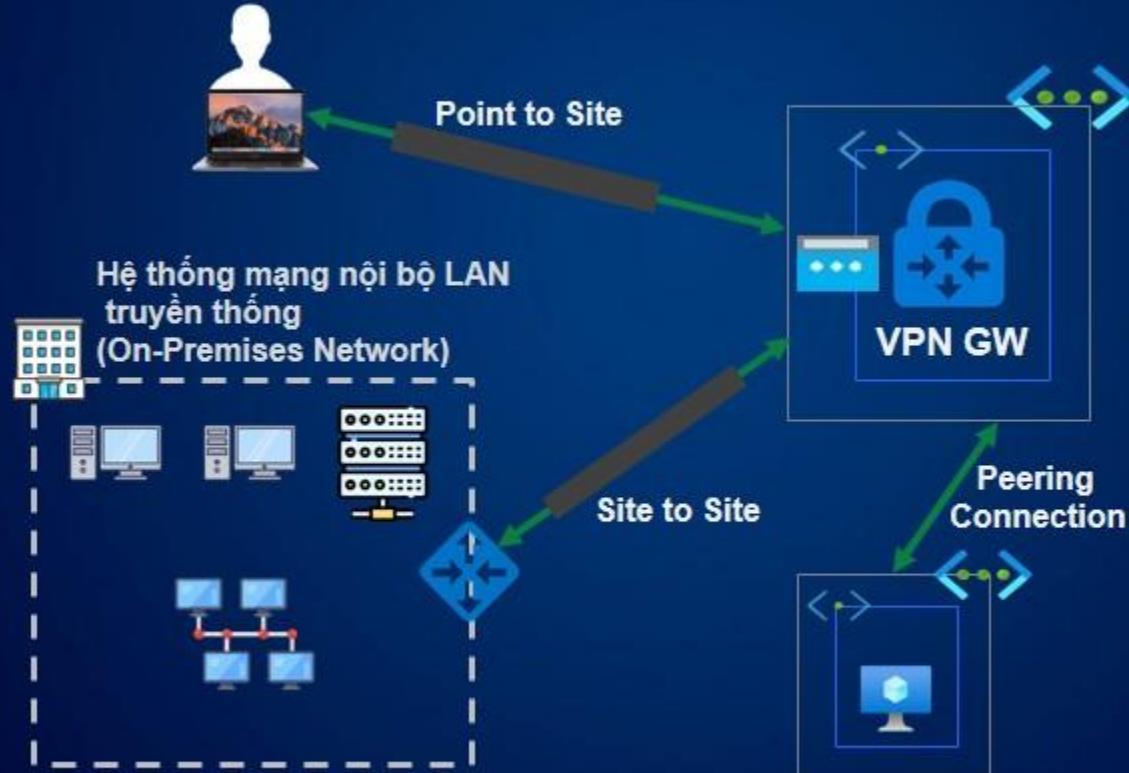
Thiết lập kết nối giữa các Vnets,
Giống như Vnet peering

Các thành phần:

- Vnet gateway cho VPN gateway
- Gateway subnet
- Public IP cho Vnet gateway
- IP sec tunnel cho mã hóa dữ liệu



Các khả năng của VPN Gateways



Các loại định tuyến (routing)

Dựa trên chính sách (Policy-Based)

- ❖ Định tuyến tĩnh thông qua các quy định chính sách
- ❖ Ké thừa các thiết bị VPN on-premises
- ❖ Chỉ hỗ trợ IKEv1
- ❖ Chỉ hỗ trợ Basic SKU

Dựa trên định tuyến (Route-Based)

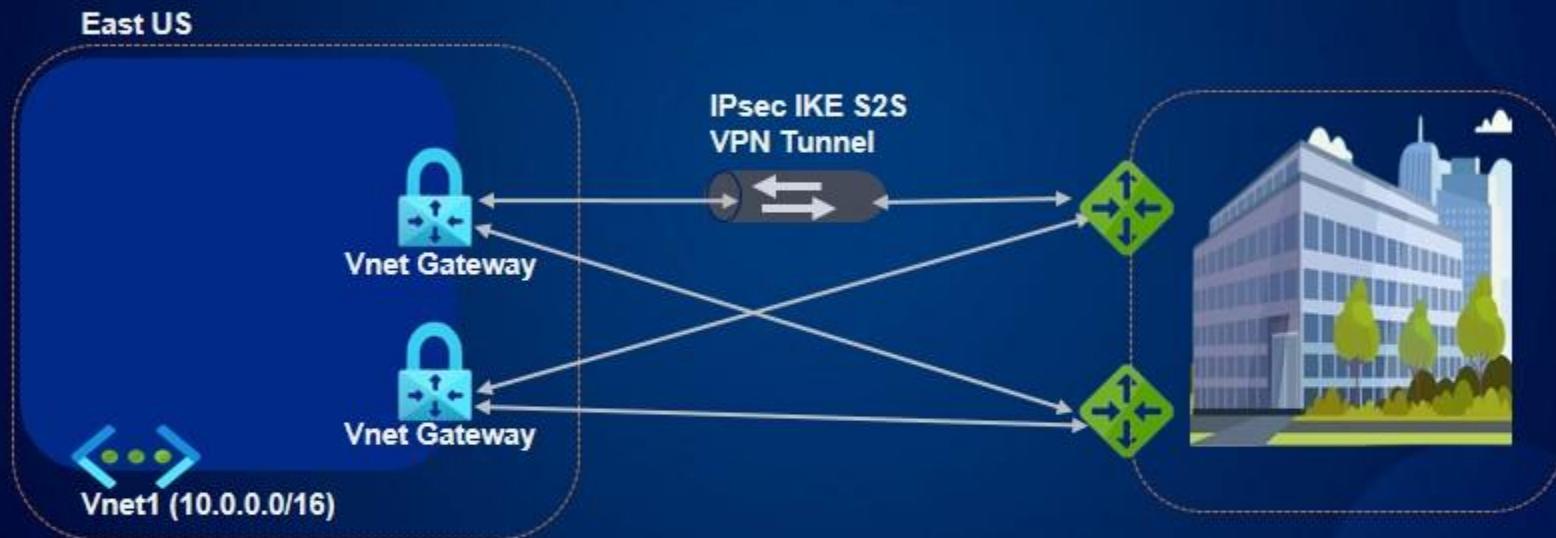
- ❖ Định tuyến tĩnh và định tuyến động
- ❖ Khả năng thích nghi với thay đổi trong cấu trúc mạng
- ❖ Có thể tồn tại cùng với ExpressRoute
- ❖ Hỗ trợ IKEv2

VPN Gateway SKUs

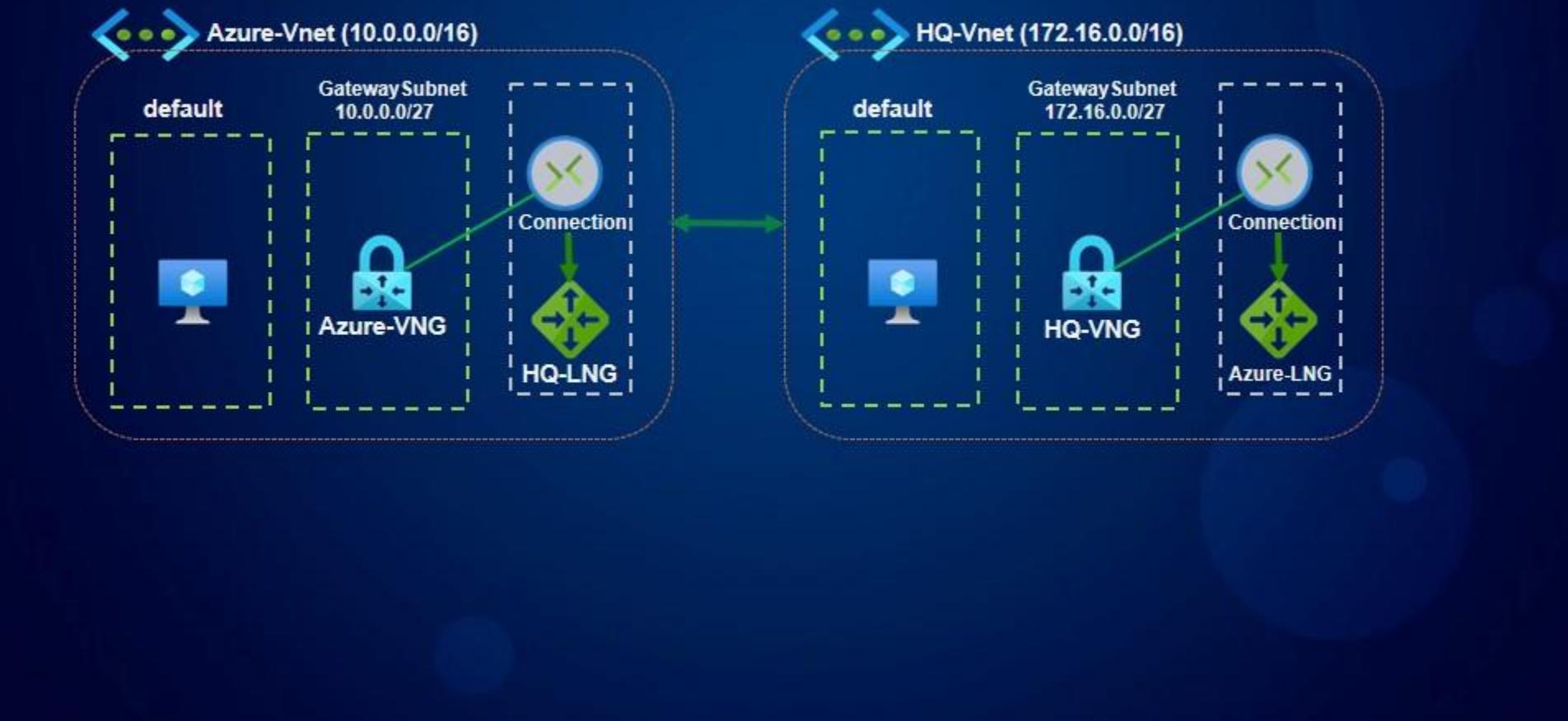
SKU	Site-to-Site Tunnels	Throughput (Thông lượng)	BGP Support
Basic	Max: 10	100 Mbps	Không hỗ trợ
VpnGw1AZ	Max: 30	650 Mbps	Hỗ trợ
VpnGw2AZ	Max: 30	1 Gbps	Hỗ trợ
VpnGw3AZ	Max: 30	1.25 Gbps	Hỗ trợ

Ghi chú: VPN gateway cơ bản (Basic VPN gateway) chỉ nên được sử dụng trong môi trường thử nghiệm và phát triển (dev/test workloads). Nó không hỗ trợ chuyển đổi giữa các loại SKU (tính năng khác nhau) mà thay vào đó yêu cầu phải triển khai lại VPN gateway để thay đổi cấu hình hoặc tính năng.

So sánh Active-Active và Active-Passive



Demo: Cấu hình Vnet Gateway



Triển khai VPNs-Demo

Các điểm chính của bài học

Azure	On-Premises	Azure
Tạo Vnets và Subnets Xác định DNS Server	Tạo Gateway Subnet Tạo VPN Gateway	Tạo Local Network Gateway Cấu hình Thiết bị VPN Tạo kết nối VPN (VPN Connection)

- Vnet to Vnet
- Site to Site
- Point to Site
- IPsec tunnel for encryption

Cấu hình ExpressRoute

Bài học bao gồm

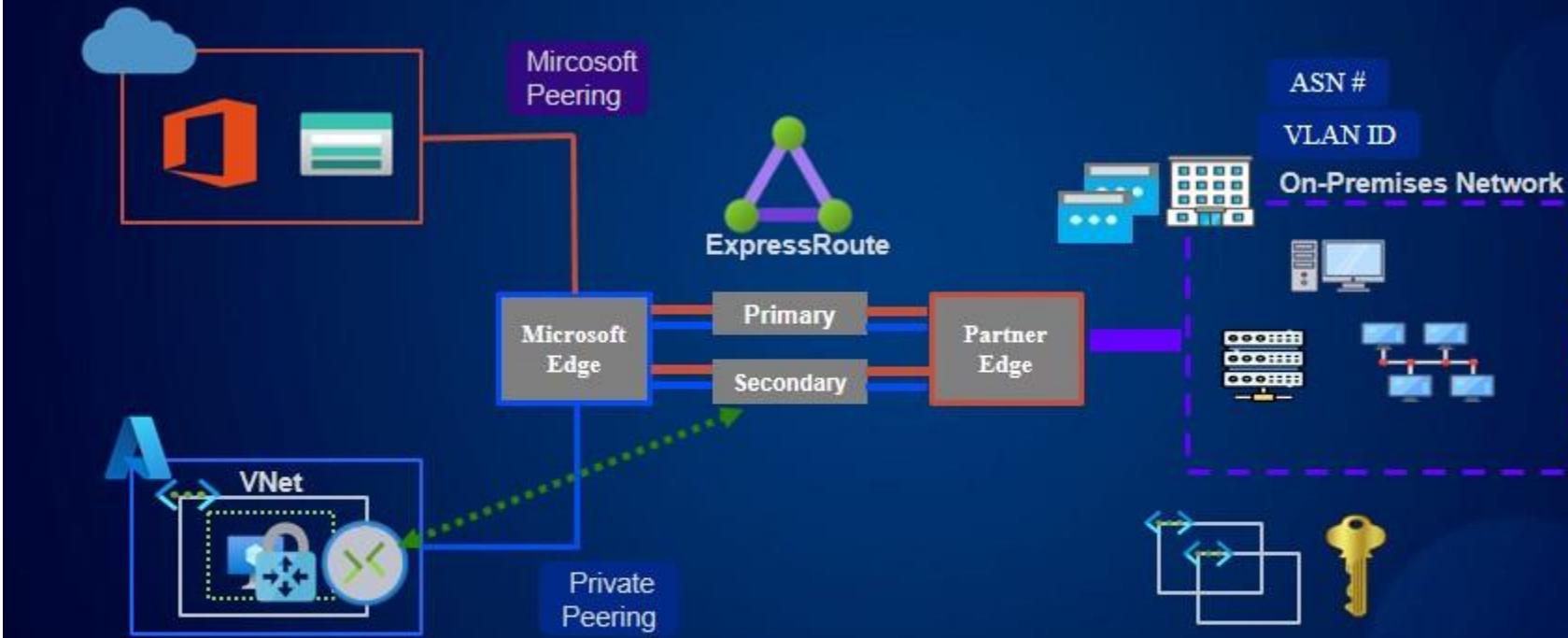
Mô tả ExpressRoute

Các bước thực hiện tạo một ExpressRoute

Demo: Cấu hình ExpressRoute

Các điểm chính của bài học

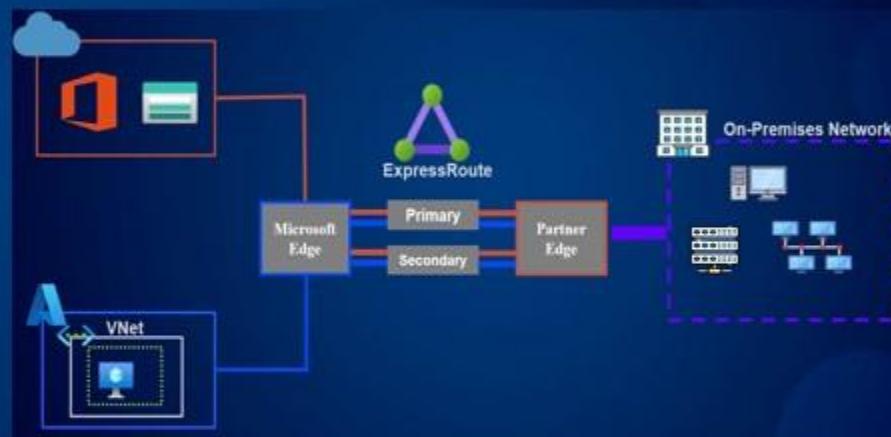
Mô tả ExpressRoute



Các bước thực hiện tạo một ExpressRoute

Tạo một ExpressRoute

- 1 **Tạo ExpressRoute Circuit**
- 2 **Cung cấp service Key cho nhà cung cấp dịch vụ (Provider)**
- 3 **Tạo cấu hình Peering**
Ghi chú: Bước này sẽ là một phần của bước 2 nếu nhà cung cấp cho phép kết nối Layer 3 thay vì layer 2.
- 4 **Tạo Virtual Network Gateway**
Loại gateway (gateway type) phải là ExpressRoute và nó phải được triển khai bên trong một gateway subnet



Các điểm chính của bài học



Azure ExpressRoute

- ✓ Kết nối dành riêng đường mạng vật lý
(Dedicated Physical Connection)
- ✓ Built-in Redundancy
(kết nối mạng dự phòng được tích hợp sẵn)
- ✓ Kết nối tới Microsoft
- ✓ Kết nối qua private peering
- ✓ Định tuyến động BGP
- ✓ Băng thông 50 Mbps – 10 Gbps

Triển khai Virtual WAN

Bài học bao gồm

Mô tả Virtual WAN

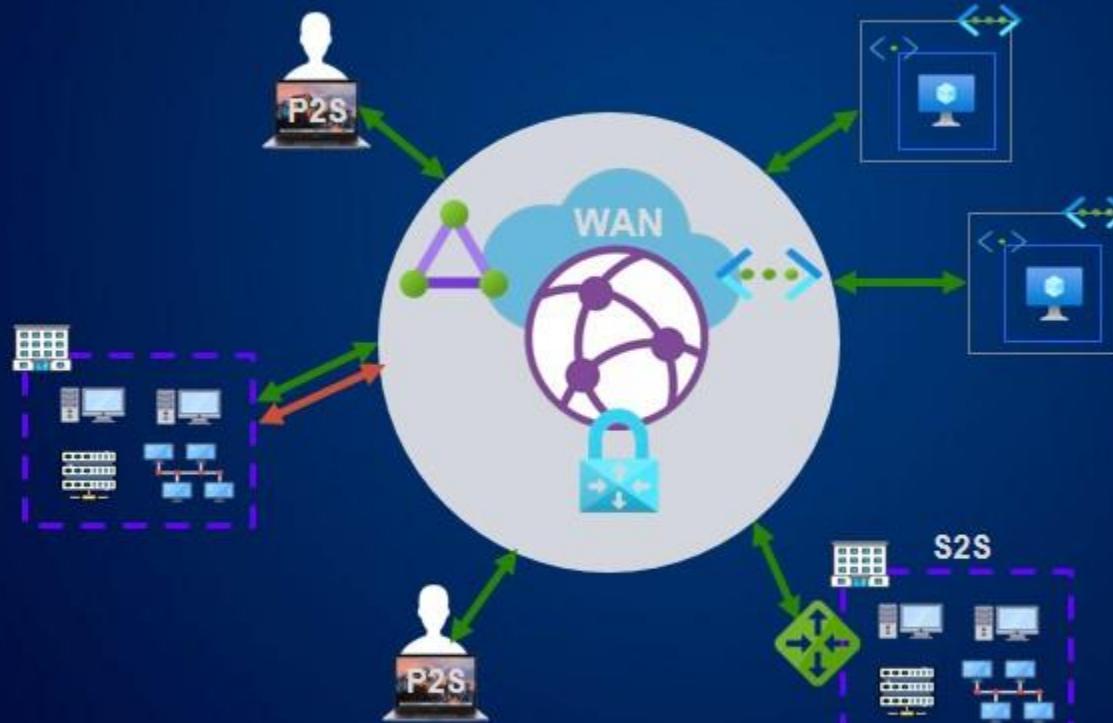
Kết nối Hub-to-Hub

Virtual WAN SKUs

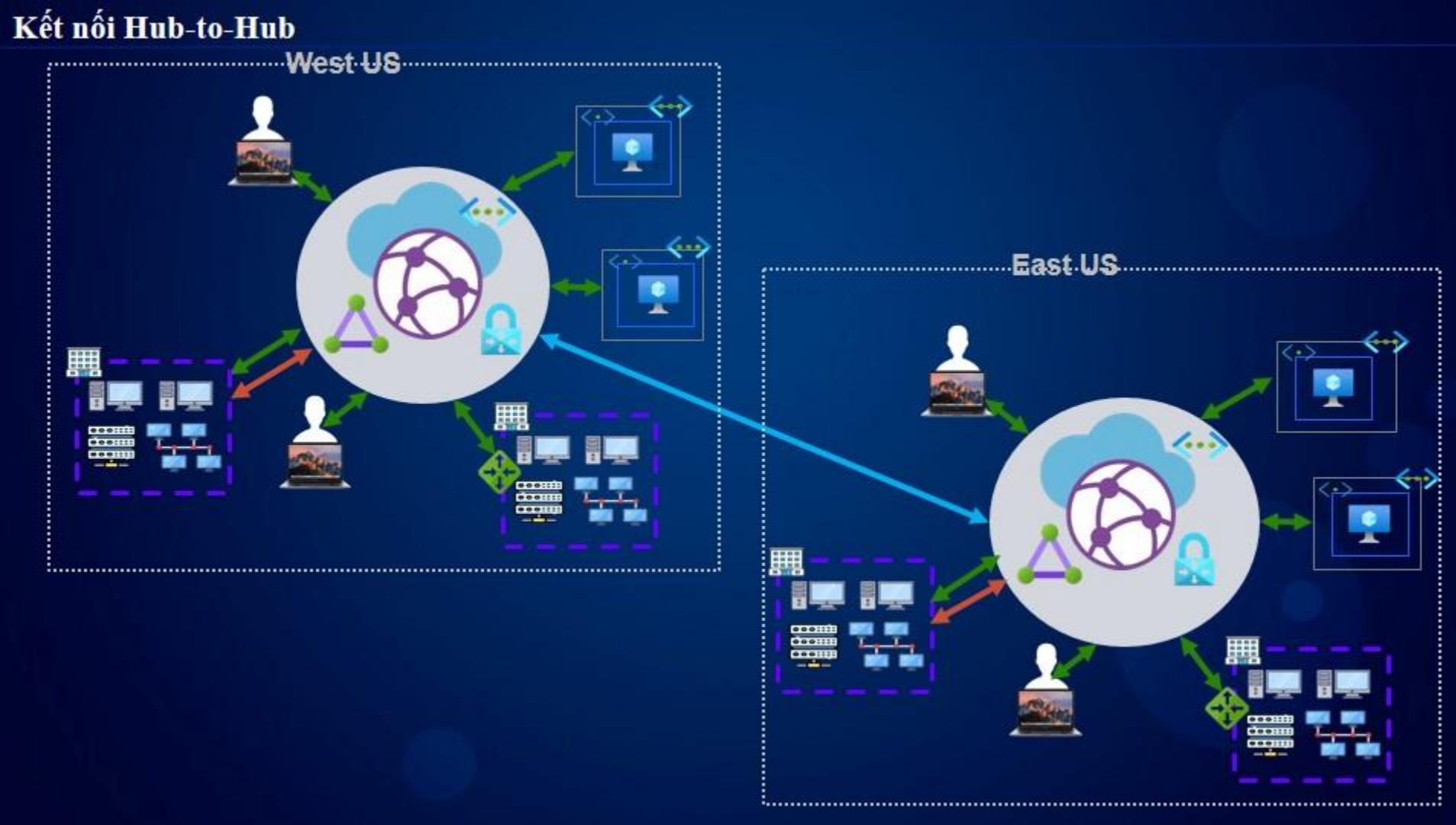
Demo: Tạo một Virtual WAN

Các điểm chính của bài học

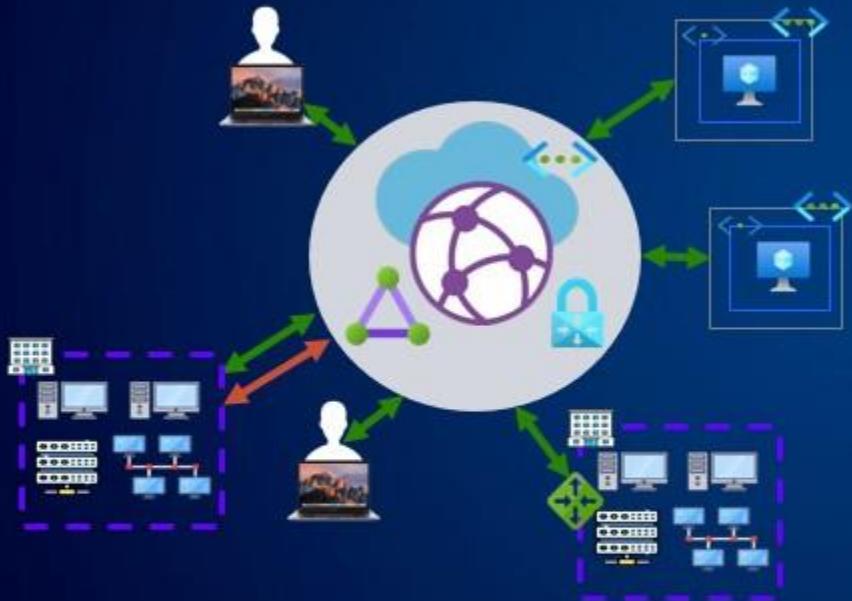
Mô tả Virtual WAN



Kết nối Hub-to-Hub



Virtual WAN SKUs



Basic

- Không hỗ trợ kết nối peering bắc cầu
- Chỉ cho phép kết nối S2S VPN
- Hỗ trợ nâng cấp lên Standard



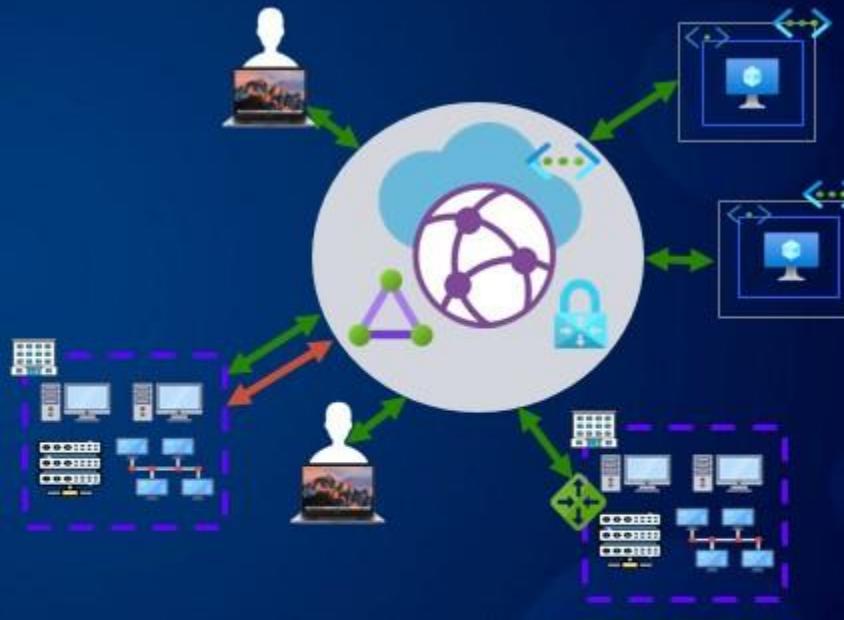
Standard

- Được hỗ trợ kết nối peering bắc cầu
- Cho phép các kết nối: S2S VPN, P2S VPN, ExpressRoute, và Vnet to Vnet

Các điểm chính của bài học

Azure Virtual WAN

- ✓ Kết nối các hệ thống mạng sử dụng kiến trúc hub-spoke
- ✓ Basic và Standard SKUs
- ✓ Kết nối S2S và P2S VPN gateways, global reach ExpressRoute, và Vnets
- ✓ Bảo mật với Azure Firewall và Firewall Manager
- ✓ Any-to-any connectivity
- ✓ Connections propagated to managed routes
- ✓ Đơn giản hóa việc triển khai và quản lý mạng ảo



Thực hành tạo một cấu trúc mạng Hub-Spoke trong Azure

Trong tình huống của bài thực hành này, công ty của bạn có nhiều dịch vụ. VD như: DNS, AD, File services, internal apps, Intrusion Detection System(Hệ thống Phát hiện xâm nhập), VV... Để giúp giảm thiểu việc phải quản trị các dịch vụ này theo phương pháp phân tán. Phòng IT sẽ tập trung tất cả các dịch vụ vào một trung tâm hub, để giúp cho việc quản trị tập trung các dịch vụ. Vậy bạn sẽ cần thực hiện setup công nghệ hub-spoke, tạo một hub Vnet và cấu hình kết nối một spoke Vnet trong Azure.

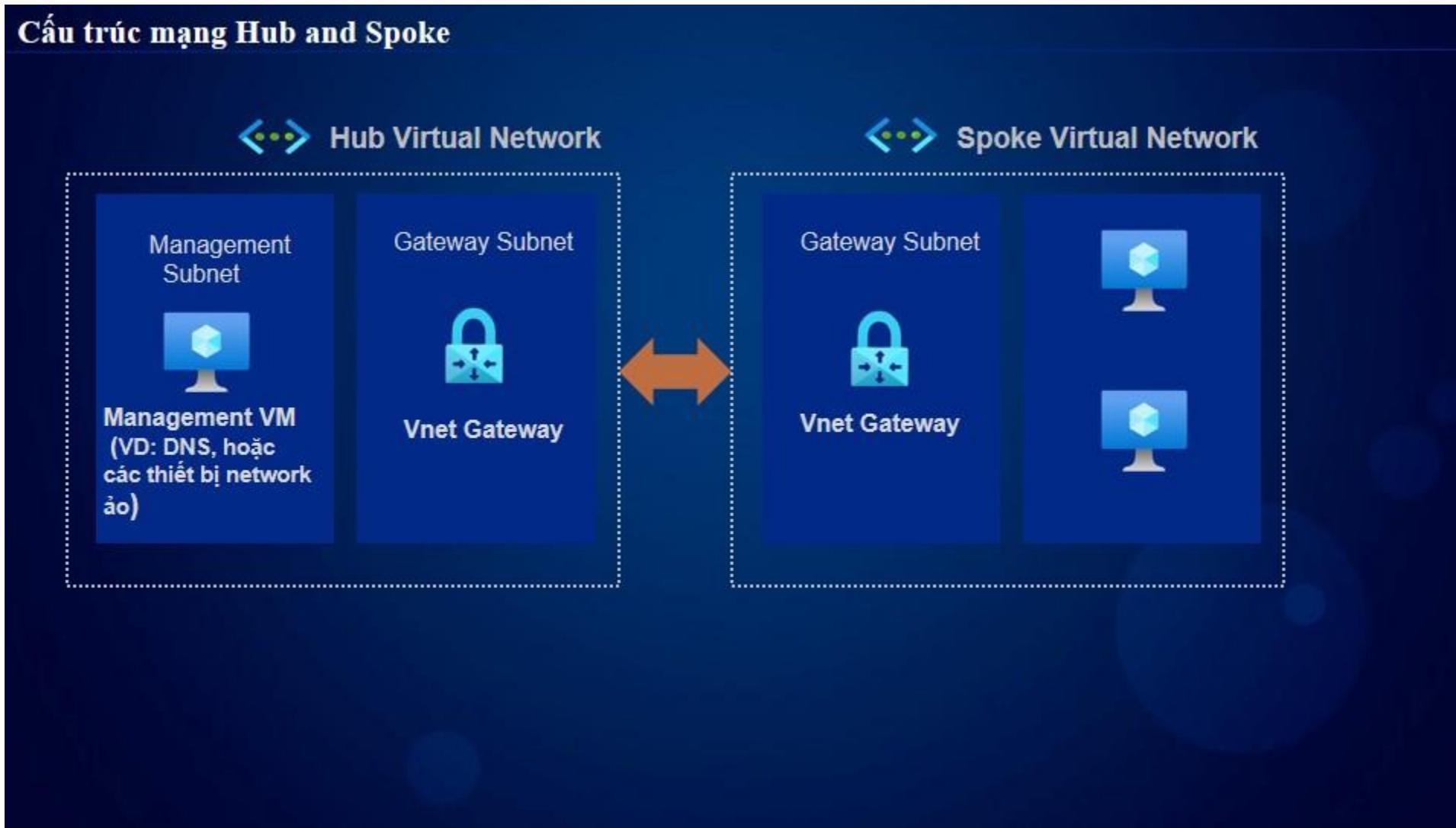
- ✓ Chúng ta cần vào đường link :

<https://raw.githubusercontent.com/phuongluuho/Azure104/main/Template-Hub-Spoke.json>

Để copy nội dung file Template-Hub-Spoke.json, sau đó sử dụng ARM Templates.

Để tạo ra một môi trường cho bài thực hành gồm: 02 mạng ảo Virtual network, 02 Public IP, 02 Virtual network gateway

Cấu trúc mạng Hub and Spoke





Tạo 02 máy ảo VMs
trong 02 Vnets. Cấu
hình hai Network
Gateways



Add hai Connections
giữa các Vnets



Kiểm tra việc kết nối
bên trong 02 máy ảo



Hoàn thành
bài lab



Giai đoạn 1



Giai đoạn 2



Giai đoạn 3



Giai đoạn 4

Tạo và quản lý các máy ảo VMs

Azure Virtual Machine là gì?

- ✓ Là tài nguyên đám mây computing có khả năng mở rộng, và là cơ sở hạ tầng dưới dạng dịch vụ (IaaS).
- ✓ Bao gồm CPU, bộ nhớ(memory), bộ lưu trữ dữ liệu (storage), và các tài nguyên mạng
- ✓ Có thể sử dụng Azure Portal, Azure CLI, và PowerShell để tạo máy ảo VM



Định nghĩa máy ảo (Virtual Machines)



Các thành phần lõi



CPU và Memory

Định nghĩa cấu hình của máy ảo (VM).
Lựa chọn cấu hình máy ảo tùy theo
trường hợp sử dụng.



Networking

Các mạng ảo (Vnets), các mạng con (subnets),
Card mạng ảo (NIC), địa chỉ Public IP (PIP),
Và tường lửa Network Security Group (NSG)



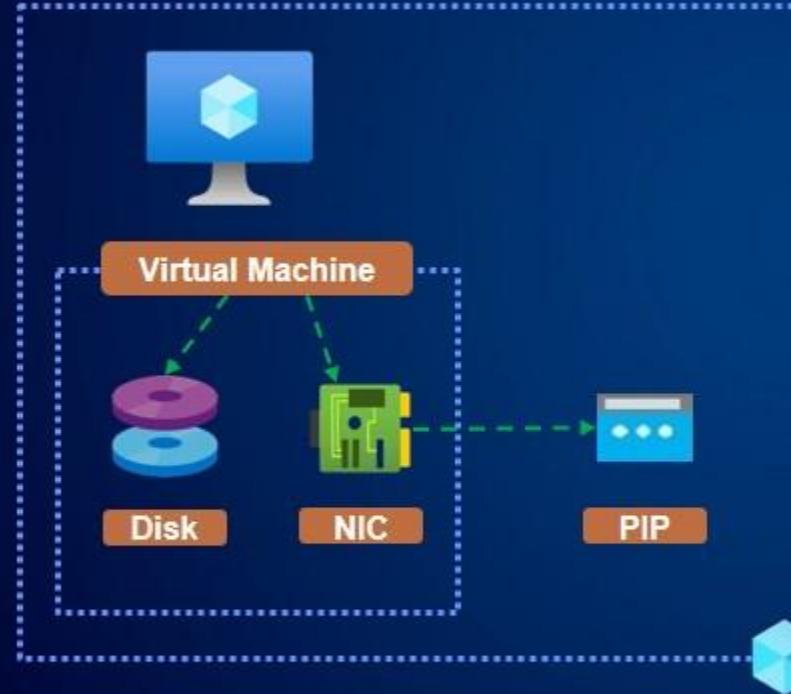
Bộ lưu trữ dữ liệu

Ổ ảo (Azure Disk), bao gồm ổ đĩa ảo
cho hệ điều hành (OS Disk), Ổ tạm
(temporary disk), và ổ lưu trữ dữ
liệu (data disk)

Virtual Machine Family Type

Loại máy ảo (VM)	Mô tả
General Purpose	CPU và bộ nhớ (memory) có hiệu suất cân bằng , thường sử dụng cho môi trường testing, phát triển ứng dụng, hoặc cho các VM có khối lượng công việc vừa và nhỏ.
Compute Optimized	CPU và bộ nhớ (memory) có hiệu suất cao. Thường được sử dụng cho các Web servers, thiết bị mạng, app servers, servers chạy các công việc tự động(batch processing) có lượng truy cập traffic vừa phải.
Memory Optimized	CPU và bộ nhớ (memory) có hiệu suất cao. Hoạt động tốt cho các CSDL quan hệ, Caching, và đặc biệt là trong việc thực hiện các phân tích dựa trên bộ nhớ (memory analytics)
Storage Optimized	Có thông lượng disk và I/O cao, được sử dụng cho Big Data, SQL, NoSQL, và data warehousing. đặc biệt hoạt động tốt cho các cơ sở dữ liệu Online Transactional Processing (OLTP). OLTP là loại cơ sở dữ liệu chủ yếu sử dụng để thực hiện các giao dịch trực tuyến và xử lý dữ liệu giao dịch thường xuyên
GPU	Được chuyên biệt hóa để xử lý các công việc đòi hỏi sử dụng đồ họa mạnh và chỉnh sửa video, cũng như huấn luyện trí tuệ nhân tạo (AI) và học sâu (deep learning).
HPC	Được tối ưu hóa để cung cấp tốc độ và hiệu suất tính toán cao nhất. Là loại máy ảo mạnh mẽ nhất, thích hợp cho các công việc tính toán đòi hỏi quy mô lớn và phức tạp như địa vật lý quy mô lớn, và các lĩnh vực toán học/công nghệ khoa học tiên tiến.

Các thuộc tính của máy ảo VM



Name: AppVM01

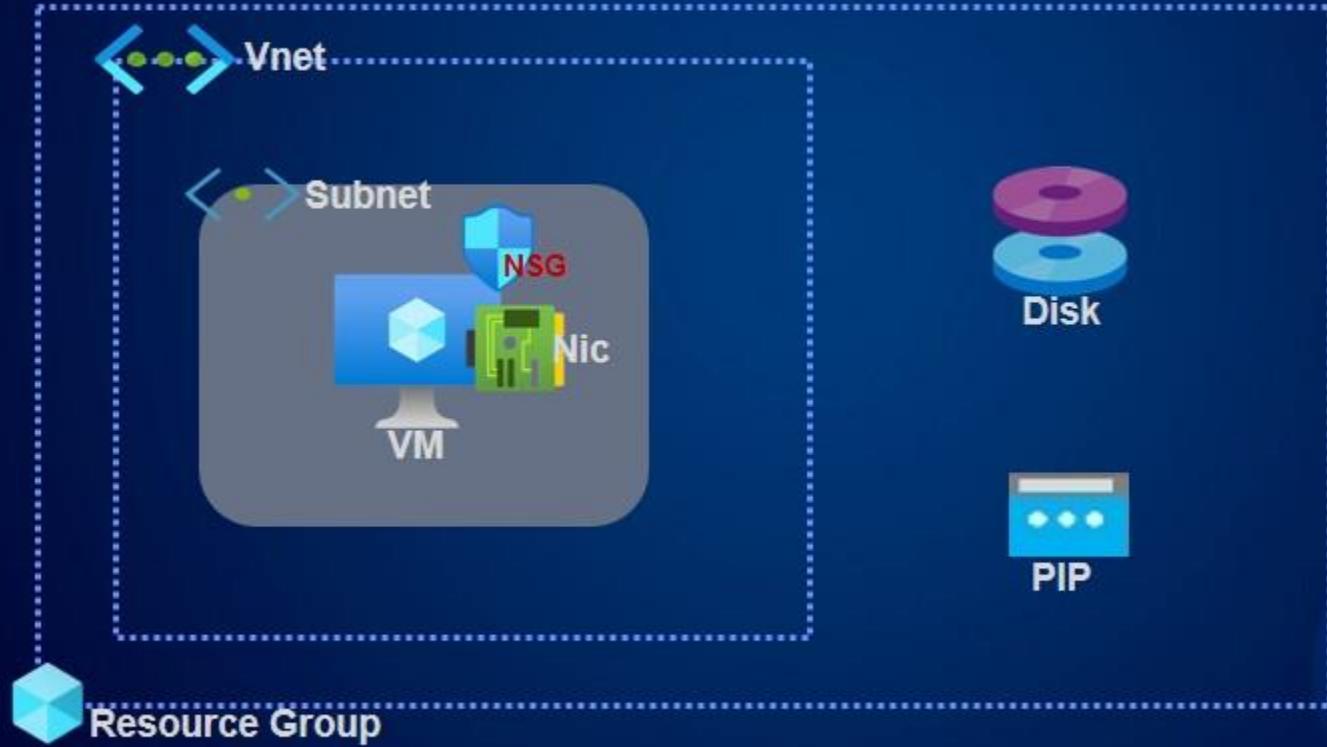
Region: South Central US

Size: Standard_B1s

Image: Linux/Windows

Tạo và quản lý các máy ảo VMs-Phần 2

Kiến trúc máy ảo VM



Thực hiện một Demo



Tạo một Linux VM

Sử dụng Azure Portal, Azure CLI, và PowerShell trong Cloud Shell



Cấu hình các Disks

Add một data disk cho VM



Cấu hình Networking

Chọn/tạo một Vnet, subnet, NIC, PIP, và NSG



Cài đặt một Webserver

Cài đặt Nginx sử dụng custom data



Cấu hình mở cổng NSG cho HTTP

Quản lý các quy tắc (rules) cho máy ảo

Các trường hợp sử dụng

1

Linux/Windows Compute

Triển khai máy các máy ảo
Linux/Windows sử dụng
Azure VM's IaaS model

2

Di chuyển tài nguyên

Di chuyển các tài nguyên lên
Azure. Ví dụ di chuyển(Migrate)
Web servers lên Azure VMs

3

Các giải pháp Cloud Computing

Azure VM Workloads với các
cấu hình cụ thể có thể cung cấp
các giải pháp với tính sẵn sàng cao
(high availability), tính chịu lỗi,
khả năng mở rộng, và tính linh hoạt

Exam Tips

CPU/Memory



Định nghĩa tài nguyên
CPU và Memory

Networking



VMs sử dụng Vnets, Nics,
Và NSG để định nghĩa kết
nối mạng

Lưu trữ (Storage)



VMs sử dụng Azure Disks
Để lưu trữ OS, và các dữ liệu
tạm, và dữ liệu lưu trữ liên tục

Có thể quản lý bảo mật cho
VMs bằng cách mở các cổng
trong một NSG
(Network Security Group)

Quản lý Azure VM Disks

Virtual Hard Disks là gì?

Virtual Hard Disks (VHDs)

Là một file nằm trong một ổ cứng (Hard disk).

Các máy ảo (VMs) sử dụng VHDs để lưu trữ OS, các ứng dụng (apps), và dữ liệu (data). VHDs sử dụng cơ sở hạ tầng lưu trữ cơ bản của Microsoft. Các VHDs được lưu trữ dưới dạng page blobs trong dịch vụ blob.



Mục đích của các VHDs



OS Disk

- Mặc định với các máy ảo (VM)
- Lưu trữ hệ điều hành (OS)
- Thường được đăng ký giống như một ổ SATA
- Được đặt tên là ổ C cho Windows và được mount "/" cho các hệ thống Unix-Linux
- Có dung lượng lớn nhất là 4,095 GiB



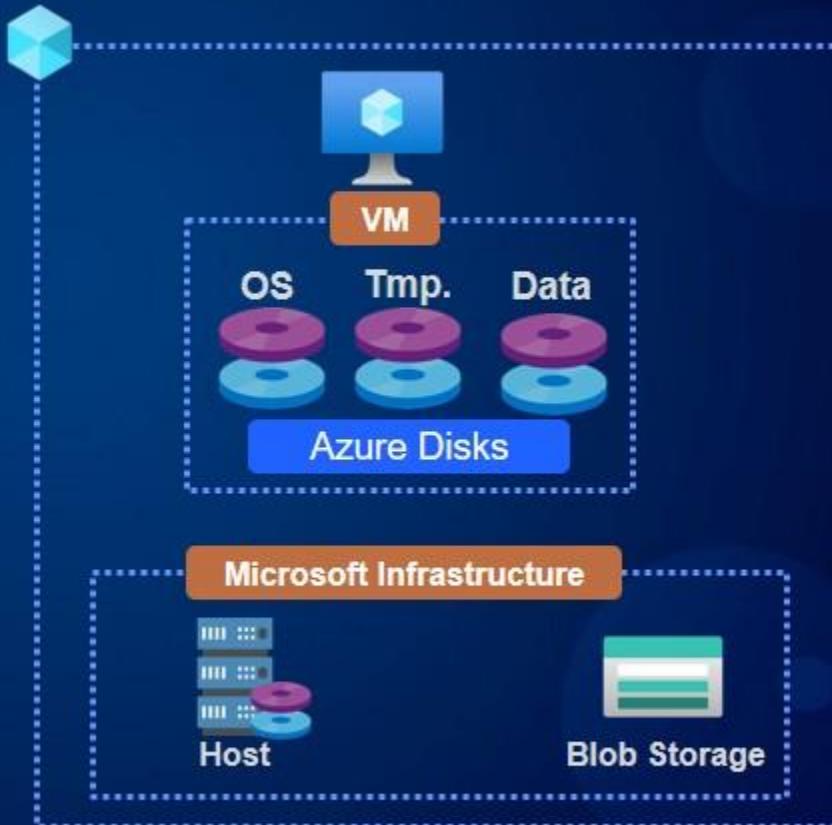
Ổ tạm (Temporary Disk)

- Mặc định với các máy ảo (VM)
- Lưu trữ các dữ liệu tạm thời như page và các swap files
- Là một ổ đĩa tạm thời tầng của Microsoft được cung cấp cho máy ảo, dựa trên cơ sở hạ tầng trong quá trình chạy máy ảo



Ổ chứa dữ liệu (Data Disk)

- Là ổ được gắn thêm vào một máy ảo (VM)
- Được sử dụng để lưu trữ các dữ liệu như files, CSDL (Databases)
- Được đăng ký giống như một ổ SCSI
- Có dung lượng lớn nhất là 32,767 GiB



Unmanaged VS. Managed Disks

Unmanaged

- Không phải là một tài nguyên được quản lý bởi Azure Resource Manager (ARM).
- Tự tạo và quản lý các tài khoản lưu trữ storage accounts.
- Không được đảm bảo tính sẵn sàng

Managed

- Là một tài nguyên được quản lý bởi Azure Resource Manager (ARM)
- Azure-managed storage accounts
- Được hỗ trợ tính sẵn sàng (HA)
- Role-Based Access Control (RBAC)
- Hỗ trợ Snapshot
- Hỗ trợ Backup

VS.

Các loại Disk chính

Disk Type	Trường hợp sử dụng
Ultra Disk (SSD)	Được thiết kế để xử lý các công việc có yêu cầu về I/O (Input/Output) cực cao như các công việc thuộc top tier Online Transactional Processing (OLTP), là các công việc đòi hỏi các xử lý giao dịch cực lớn.
Premium (SSD)	Sử dụng cho môi trường chạy thật và cung cấp dịch vụ cho người dùng (Production)
Standard (SSD)	Sử dụng cho các Webservers, các ứng dụng có mức độ truy cập bình thường, và môi trường dev/test.
Standard (HDD)	Chỉ dành cho Backup, không sử dụng cho việc chạy ứng dụng

Ghi chú: Hiệu xuất Disk là được giới hạn cho các VM Sizes cụ thể

Mã hóa Disks

Mã hóa dữ liệu tại trạng thái nghỉ trên disk storage cho bảo mật đa lớp

1 Storage Service Encryption (SSE)

- Mã hóa của các ổ cứng vật lý trong Data Center
- Được tích hợp vào nền tảng hệ thống Azure

2 Azure Disk Encryption (ADE)

- Tùy chọn mã hóa của ổ VHDs
- Đảm bảo một disk chỉ có máy ảo, là chủ sở hữu của disk này mới có quyền được truy cập vào disk
- Sử dụng các công cụ mã hóa OS tools như BitLocker và DM-Crypt



Thực hiện một Demo



Add một Data Disk cho một VM

Sử dụng Azure Portal để add một Data Disk



Bật (Enable) Azure Disk Encryption (Mã hóa)

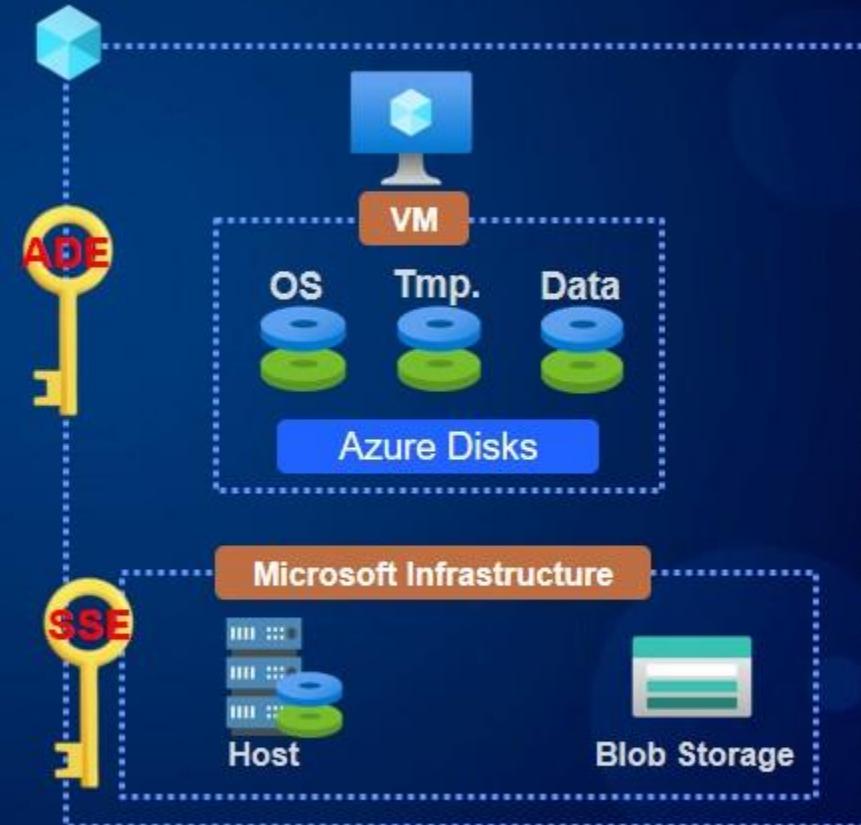
Tạo một key Vault, tạo một key, và Chọn các tùy chọn encryption



Xác nhận Encryption

Sử dụng PowerShell để xác nhận Encryption.

Exam Tips



Thực hành add Data Disk cho một VM trong Azure

Trong tình huống của bài thực hành này, công ty của bạn cần xóa một máy ảo (VM) và giữ lại dữ liệu trong máy ảo đó. Bạn cần phải có một giải pháp tốt nhất để attach ổ ảo này vào một máy ảo (VM) khác, và cần đảm bảo hệ điều hành có thể truy cập vào ổ ảo này.

- ✓ **Chúng ta cần vào đường link :**

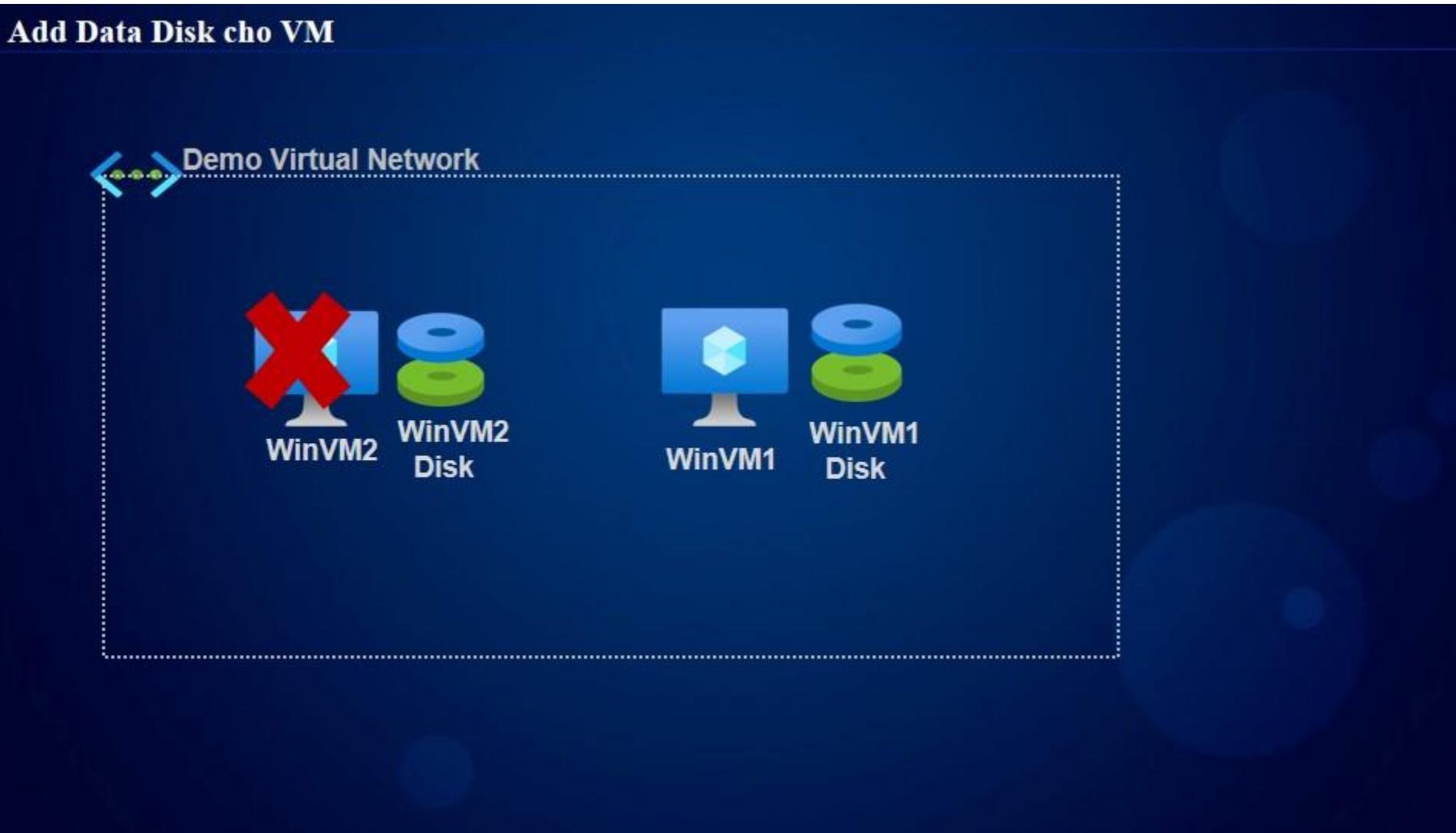
<https://raw.githubusercontent.com/phuongluuho/Azure104/main/Add-Datadisk.json>

Để copy nội dung file Add-Datadisk.json, sau đó sử dụng ARM Templates.

Để tạo ra một môi trường cho bài thực hành gồm:

02 máy ảo, 02 mạng ảo Virtual network, 02 Public IP, 02 disks, 02 cards mạng ảo

Add Data Disk cho VM



Cấu hình tính sẵn sàng cao(HA) và tự động mở rộng quy mô (Scale Sets) máy ảoVM

Mạng toàn cầu và sẵn sàng cao (HA)



Mạng toàn cầu và sẵn sàng cao (HA)



Mạng toàn cầu và sẵn sàng cao (HA)

Region: East US



Virtual Machine Availability Sets

Mục đích của tập hợp các máy ảo
có tính sẵn sàng cao



- Bảo vệ các máy ảo dự phòng
- Bảo vệ chống lại các sự cố xảy ra ở cấp độ máy chủ vật lý (Host).
- Ngăn chặn việc dừng hoạt động của hệ thống do các công việc bảo dưỡng hoặc bảo trì

Virtual Machine Availability Sets



Fault Domain (FD)

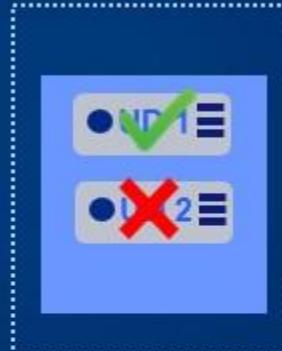
Sự cố máy chủ vật lý mức cơ bản, như: Mất điện hay mất kết nối mạng.
(Max FD:3)



Update Domain (UD)

Nhóm logic của cơ sở hạ tầng cho việc bảo trì/cập nhật.
(Max UD:20)

FD 1



FD 2



Availability Sets

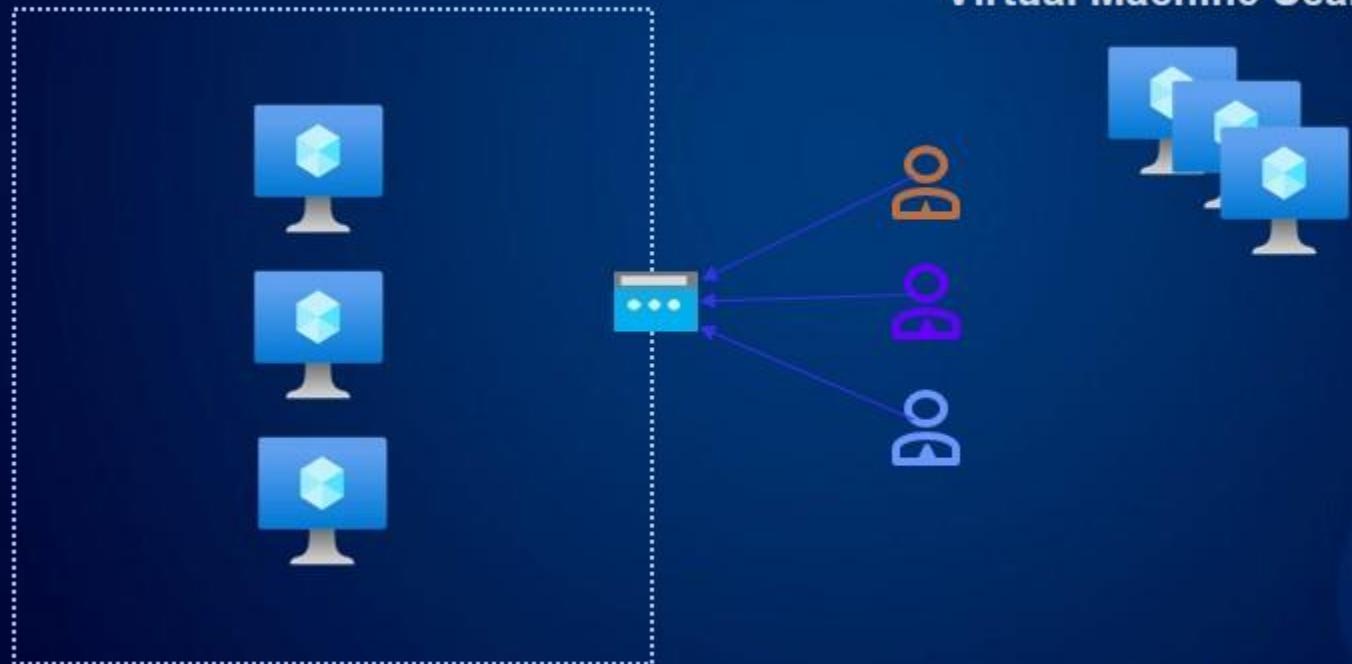


Cấu hình tính sẵn sàng cao (HA) và tự động mở rộng quy mô (Scale Sets) máy ảo VM

Phần 2

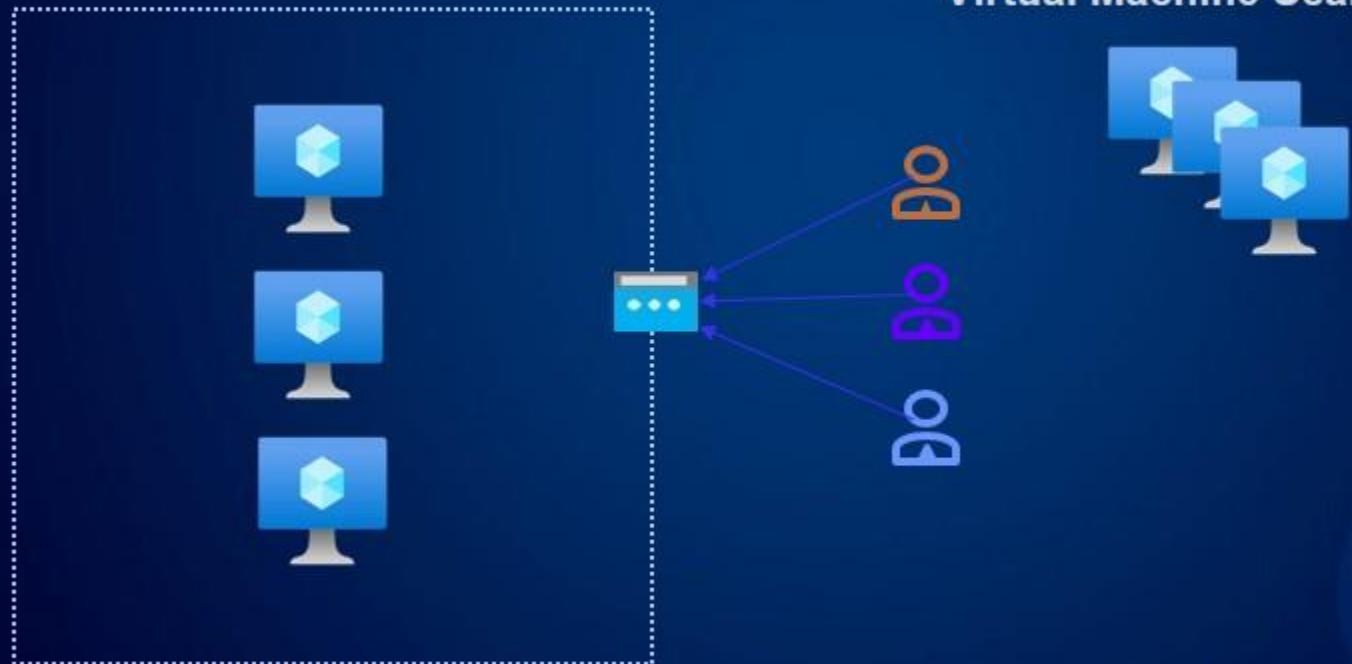
Autoscaling Operations

Virtual Machine Scale Sets



Autoscaling Operations

Virtual Machine Scale Sets



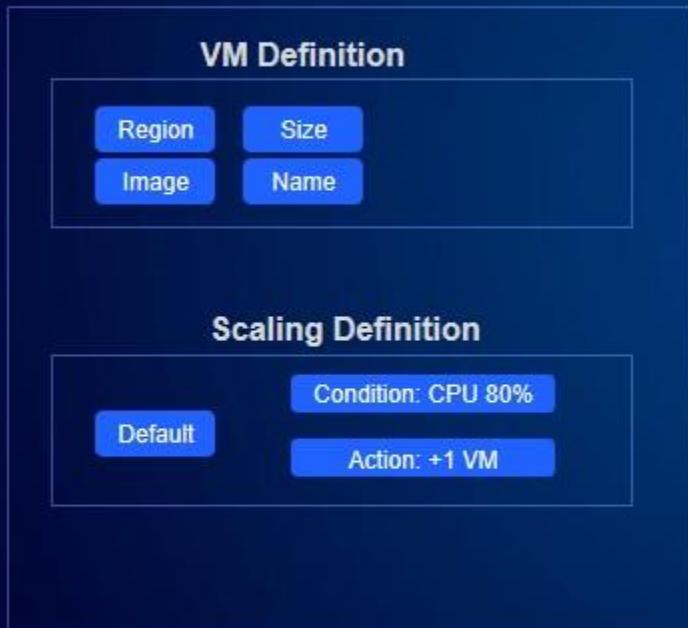
Tại sao chúng ta sử dụng Scale Sets

Mục đích của Virtual Machine Scale Sets

- ✓ Cấu hình đơn giản và dễ dàng
- ✓ Tiết kiệm chi phí bằng cách điều chỉnh việc sử dụng theo nhu cầu
- ✓ Tự động điều chỉnh để đáp ứng nhu cầu traffic



Các thành phần của Virtual Machine Scale Sets



Các thành phần của Scale Set



Định nghĩa cho máy ảo (VM Definition)

Định nghĩa VM size, OS, NICs, storage, etc.



Định nghĩa cho Autoscaling (Autoscaling Definition)

Định nghĩa các hành động của Autoscaling, scaling in (tự động giảm quy mô)/ scaling out (tăng quy mô) dựa trên việc đáp ứng điều kiện (Ví dụ nếu sử dụng CPU > 80% thì sau đó tăng thêm 1 máy ảo VM).



Scale-In Policy (Chính sách giảm quy mô)

Xoá các máy ảo theo mức độ ưu tiên khi thực hiện các hoạt động giảm quy mô (scaling-in).

Exam Tips



Sẵn sàng cao (High Availability)

Thiết kế các giải pháp có tính sẵn sàng cao sử dụng triển khai, trên nhiều zones khác nhau trong một region của Azure.



Availability sets

Được sử dụng để bảo vệ máy ảo (VMs) dự phòng bằng cách ngăn chặn các sự cố và cập nhật có thể gây ra gián đoạn dịch vụ. Việc này được thực hiện bằng cách nhóm các máy ảo logic vào các "domain" khác nhau trong một "availability set".



Virtual machine scale sets

Là một dịch vụ của Azure giúp tự động điều chỉnh quy mô (auto scale) của các máy ảo để đáp ứng yêu cầu về traffic, và giảm chi phí sử dụng tài nguyên bằng cách giảm số lượng VMs khi nhu cầu traffic mạng giảm xuống.

Thực hành sử dụng PowerShell để thay đổi (Resize) Cấu hình máy ảo (VM) trong một Availability Set

Trong tình huống của bài thực hành này, phòng quản lý tài chính trong công ty có giải trình với bạn về chi phí sử dụng các máy ảo (VMs) đã vượt quá ngân sách chi tiêu. Vì vậy bạn cần phải tìm một giải pháp để dễ dàng giảm chi phí Azure VMs trong Subscription của bạn. Qua cân nhắc các giải pháp, bạn lựa chọn việc sử dụng PowerShell để kiểm tra các máy ảo có mức sử dụng CPU thấp nhất và thay đổi cấu hình(size) của các máy ảo này xuống mức có cấu hình thấp hơn, giúp bạn giảm chi phí sử dụng Azure VMs.

- ✓ Chúng ta cần vào đường link :

<https://raw.githubusercontent.com/phuongluuho/Azure104/main/resize-VM.json>

Để copy nội dung file resize-VM.json, sau đó sử dụng ARM Templates.

Để tạo ra một môi trường cho bài thực hành gồm:

02 máy ảo (VMs), Mạng ảo Virtual network and Load Balancer, Public IP, và Availability Set



Vào PowerShell
trong Cloud Shell



Lấy VM CPU
Metrics



Thay đổi kích cỡ
cấu hình máy ảo VMs
Trong Availability Set



Hoàn thành
bài lab



Giai đoạn 1



Giai đoạn 2



Giai đoạn 3



Giai đoạn 4

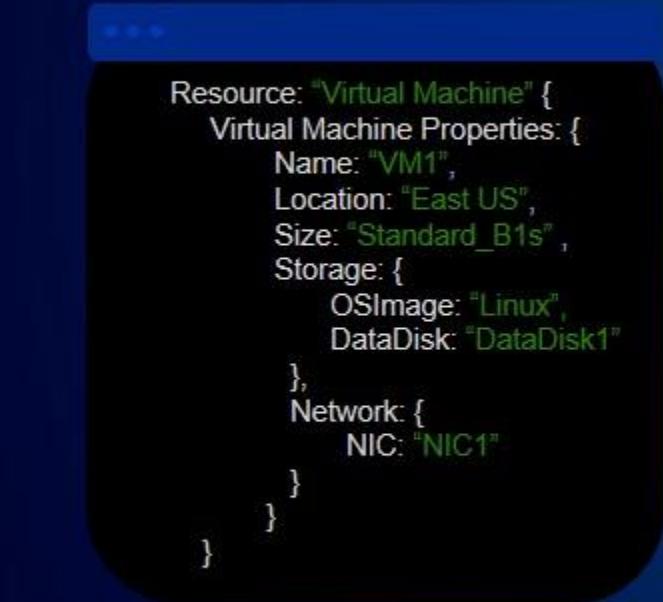
Tự động hóa triển khai máy ảo (VMs)

Tại sao cần phải tự động hóa triển khai máy ảo (VMs)



- ✓ Vá lỗi (Patch)/Cập nhật (update) hệ điều hành (OS)
- ✓ Tự động hóa cài đặt phần mềm/ứng dụng (VD: Apache2 web server)
- ✓ Tự động hóa cấu hình hệ thống, (ứng dụng/phần mềm)

Azure Resource Manager (ARM) Templates



```
Resource: "Virtual Machine" {
    Virtual Machine Properties: {
        Name: "VM1",
        Location: "East US",
        Size: "Standard_B1s",
        Storage: {
            OSImage: "Linux",
            DataDisk: "DataDisk1"
        },
        Network: {
            NIC: "NIC1"
        }
    }
}
```

1

Cơ sở hạ tầng dưới dạng code -Infrastructure as Code (IaC)

Có thể lưu trữ định nghĩa của hạ tầng và cấu hình trong các files văn bản, quản lý mã nguồn của chúng, và triển khai chúng tự động trong định dạng JSON

2

Deployment Consistency (Tính nhất quán trong triển khai)

Quản lý việc triển khai các tài nguyên một cách đồng đều và nhất quán, bằng cách sử dụng các phương pháp triển khai phần mềm/ứng dụng

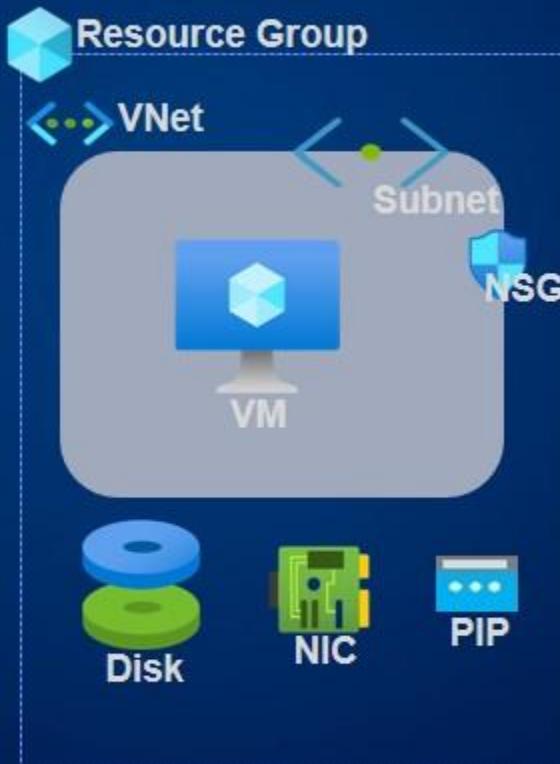
3

Tự động hóa (Automation)

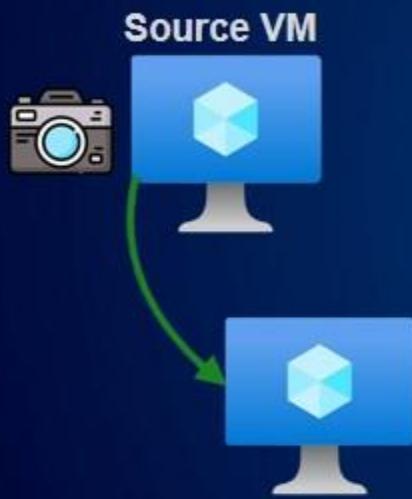
Sử dụng tự động hóa để thực hiện triển khai tài nguyên một cách tự động, và cung cấp một cách tiếp cận theo mô-đun đối với triển khai tài nguyên.

Tại sao cần phải tự động hóa triển khai máy ảo (VMs)

```
Resource: "Virtual Machine" {  
    Virtual Machine Properties: {  
        Name: "VM1",  
        Location: "East US",  
        Size: "Standard_B1s",  
        Storage: {  
            OSImage: "Linux",  
            DataDisk: "DataDisk1"  
        },  
        Network: {  
            NIC: "NIC1"  
        }  
    }  
}
```



Virtual Hard Disk (VHD) Templates



Chuẩn bị máy ảo (VMs)

Thực hiện cài đặt, cập nhật và cấu hình các phần mềm/trung dụng cần thiết



Tạo ra máy ảo (VMs)

Có thể tạo ra một bản image OS , cho việc triển khai để tạo ra các máy ảo khác, sử dụng Sysprep (Windows), hoặc Agent deprovision (Linux)

Thực hiện Demo



Triển khai máy ảo (VMs) sử dụng ARM Template

Sử dụng một ARM template, triển khai một máy ảo Linux VM và sửa đổi các thuộc tính quy tắc (rule) của NSG



Tạo ra máy ảo (VMs)

Tạo ra một image là một máy ảo Linux VM như VHD Template



Triển khai một máy ảo (VM) từ Custom template

Sử dụng image đã tạo ra, để triển khai một Linux VM

Exam Tips



ARM Templates

Triển khai VMs nhanh chóng và quản lý hạ tầng sử dụng kiểm soát sự thay đổi sử dụng cơ sở hạ tầng dưới dạng code (IaC)



VHD template

Tạo một bản golden image của máy ảo VMs để dễ dàng triển khai các máy ảo (VMs), cùng với các ứng dụng/phần mềm và các cấu hình hệ thống



Tự động hóa quản trị hệ thống

Quản lý việc triển khai các máy ảo sử dụng custom data và quản lý máy ảo VM sử dụng extension scripts.

Thực hành sử dụng Cloud Init Deployment cài đặt NGINX cho Linux VM

Trong tình huống của bài thực hành này, sẽ có một yêu cầu bạn cài đặt NGINX cho một máy ảo Linux VM mới sử dụng phương pháp tự động hóa. Vậy thay vì bạn cài đặt NGINX cho máy ảo sử dụng phương pháp thủ công, bạn có thể sử dụng cloud-init để cài đặt NGINX trong triển khai Linux VM.

Các bước trong bài thực hành này như sau:

Sử dụng PowerShell để Snapshot một Azure VM Disk

Trong tình huống của bài thực hành này, công ty của bạn có một quy định là cần phải giữ lại tất cả các bản sao lưu backups trong một thời gian nhất định, để đảm bảo dữ liệu có thể khôi phục nếu cần thiết. Sếp của bạn đã yêu cầu bạn tạo một snapshot của một disk trong Azure, và đảm bảo là bạn có thể truy cập vào nó. vậy bạn sẽ tạo một snapshot của một VM disk và chuyển nó tới một storage account.

✓ Chúng ta cần vào đường link :

<https://raw.githubusercontent.com/phuongluuho/Azure104/main/template-Snapshot-disk.json>

Để copy nội dung file template-Snapshot-disk.json, sau đó sử dụng ARM Templates.

Để tạo ra một môi trường cho bài thực hành gồm:

01 máy ảo (VMs), mạng ảo Virtual network và 01 Storage Account

Thực hành sử dụng một Custom Images cho một máy ảo (VM) Scale Set trong Azure

Trong tình huống của bài thực hành này, công ty của bạn có một custom Linux VM mà họ muốn triển khai lại cho một virtual machine scale set, để giảm lượng công việc trong triển khai môi trường của máy ảo (VM) . Bạn phải tìm một cách tối ưu nhất trong việc tái triển khai VM này mà không cần phải cài đặt và cấu hình máy ảo VM một cách thủ công.

✓ **Chúng ta cần vào đường link :**

<https://raw.githubusercontent.com/phuongluuho/Azure104/main/template-Custom-Images.json>

Để copy nội dung file template-Custom-Images.json, sau đó sử dụng ARM Templates.

Để tạo ra một môi trường cho bài thực hành gồm:

01 máy ảo (VMs), 01 mạng ảo Virtual network và 01 ổ ảo, 01 card mạng ảo, 01 Public IP.



Xác nhận VM sử
dụng để làm một
Image



Tạo một Image từ
máy ảo VM



Sử dụng Image này
để tạo một Scale Set



Hoàn thành
bài lab



Giai đoạn 1



Giai đoạn 2



Giai đoạn 3



Giai đoạn 4

Quản lý các cập nhật (Updates) của máy ảo (VMs)

Bài học bao gồm

Mô tả quản lý cập nhật (Update Management)

Các thành phần của Update Management

Demo: Bật (Enabling) Update Management

Các điểm chính của bài học

Mô tả quản lý cập nhật (Update Management)



Update Management

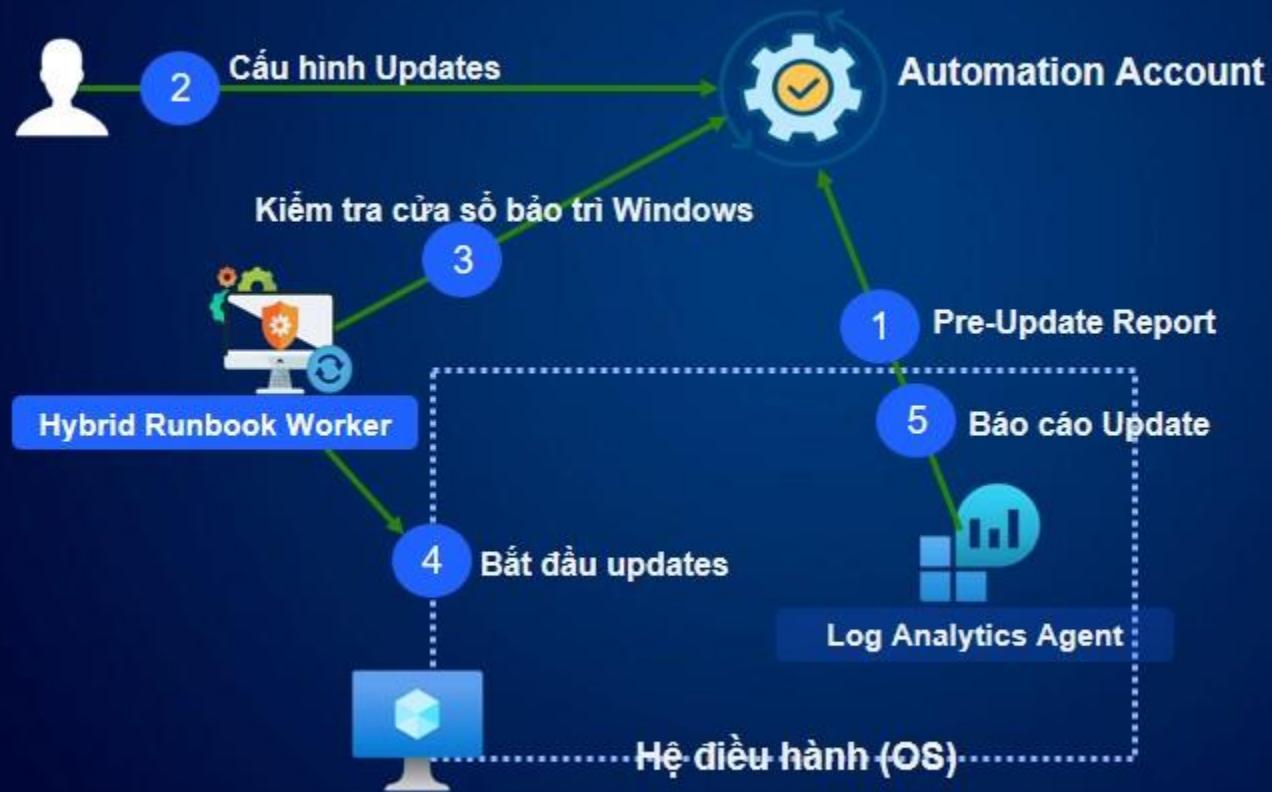
Quản lý các cập nhật (updates) hệ thống và các bản vá lỗi (patches) cho Azure Cloud và On-premises.

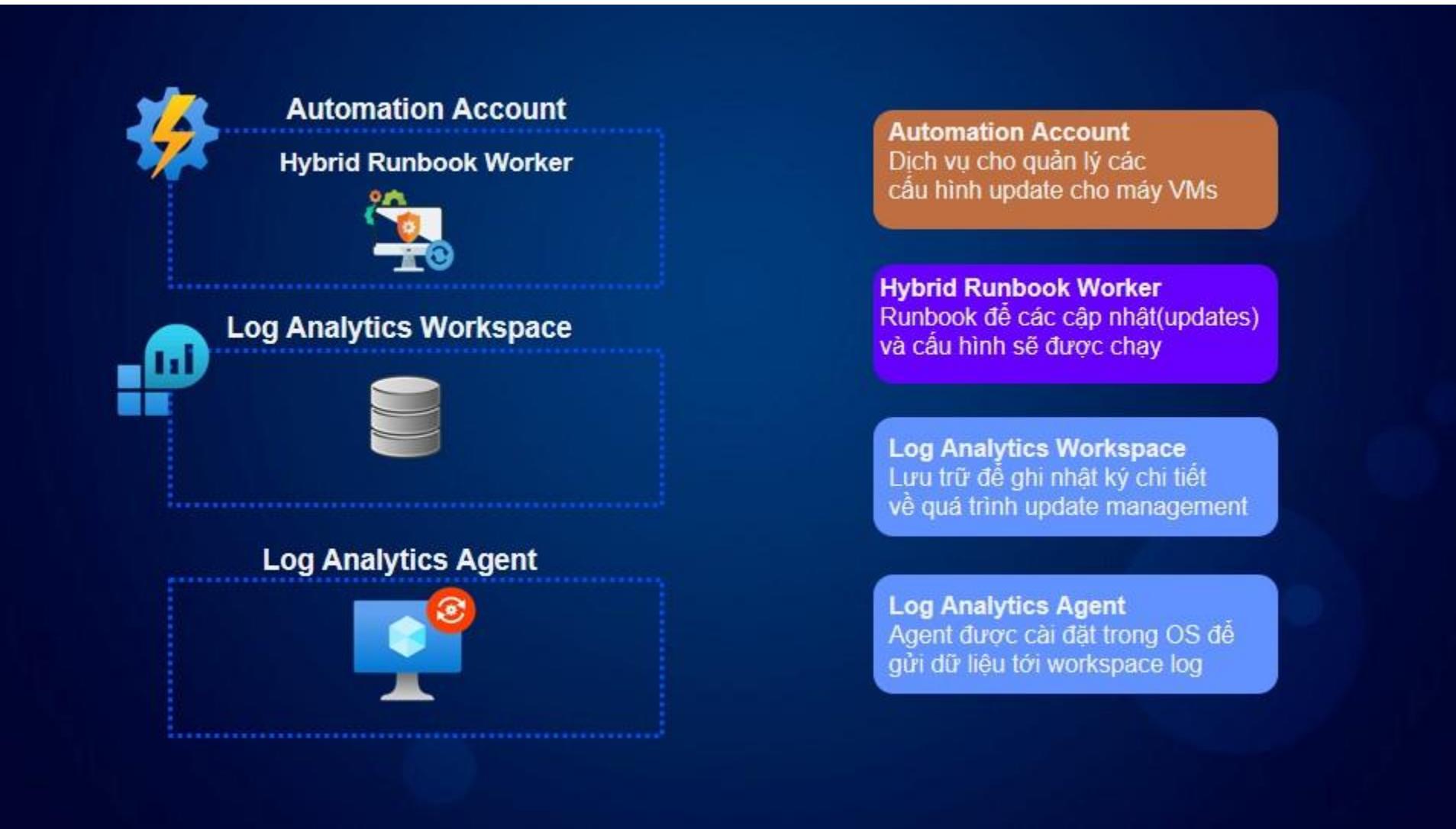
- Hỗ trợ Linux và Windows VMs

Cung cấp các khả năng thiết đặt cho:

- Lập lịch
- Quét (Scanning) kiểm tra sự tuân thủ
- Tạo báo cáo (Reporting)

Các thành phần của Update Management





Tự động hóa cấu hình máy ảo (VMs)

Bài học bao gồm

**Mô tả tự động hóa cấu hình
(Configuration Automation)**

Mô tả PowerShell DSC

Trường hợp sử dụng

Các điểm chính của bài học

Mô tả tự động hóa cấu hình (Configuration Automation)

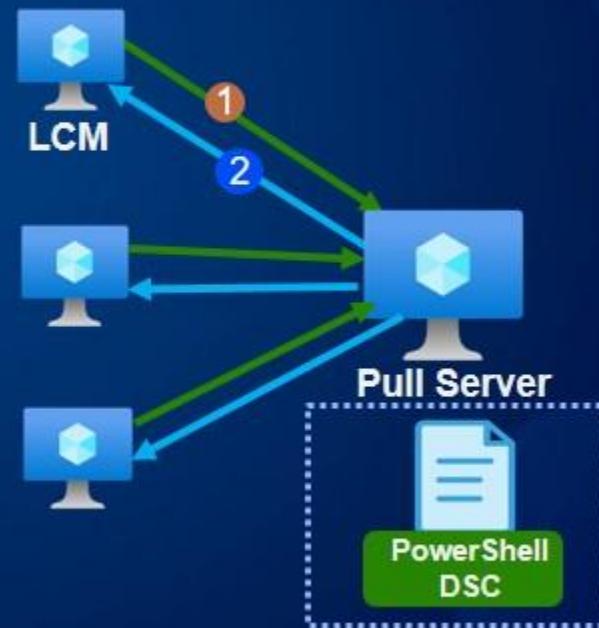
Tự động hóa cấu hình (Configuration Automation)

Quản lý tự động hóa cấu hình của các máy ảo (VMs)

Sử dụng một Automation account và PowerShell

Desired State Configuration (DSC).

- Hỗ trợ Linux và Windows VMs
- Pull server đã được tích hợp sẵn (Built-in pull server)
- PowerShell DSC sử dụng cú pháp mô tả trạng thái mong muốn



Mô tả tự động hóa cấu hình (Configuration Automation)

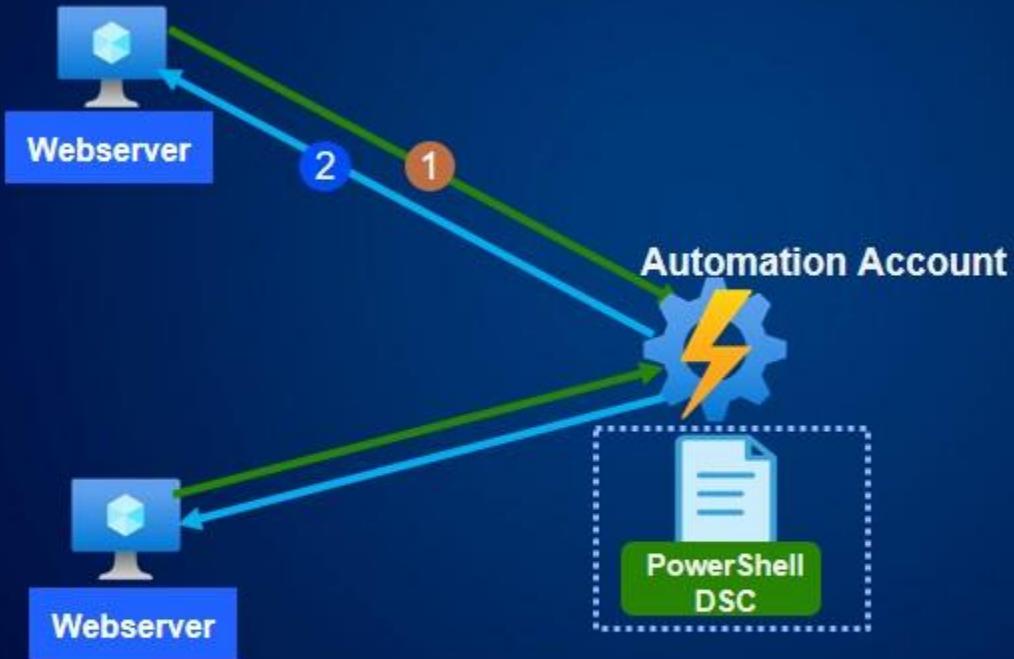


Mô tả PowerShell DSC



```
Configuration MyDscConfiguration {  
    Node "localhost" {  
        WindowsFeature MyFeatureInstance {  
            Ensure = 'Present'  
            Name = 'Web-Server'  
        }  
    }  
}
```

Trường hợp sử dụng



Các điểm chính của bài học

Automation Account

Dịch vụ quản lý cấu hình cập nhật (updates) cho máy ảo (VMs)

PowerShell DSC

Các tập lệnh PowerShell khai báo trạng thái mong muốn của máy ảo

Local Configuration Manager

Gửi trạng thái cấu hình hiện tại tới pull server cho việc đánh giá

Sử dụng Azure Bastion

Bài học bao gồm

Azure Bastion là gì?

Kiến trúc của Azure Bastion

Demo: Thực hiện Azure Bastion

Các điểm chính của bài học

Azure Bastion là gì?

Azure Bastion là gì?

Fully-managed PaaS



Kết nối RDP/SSH



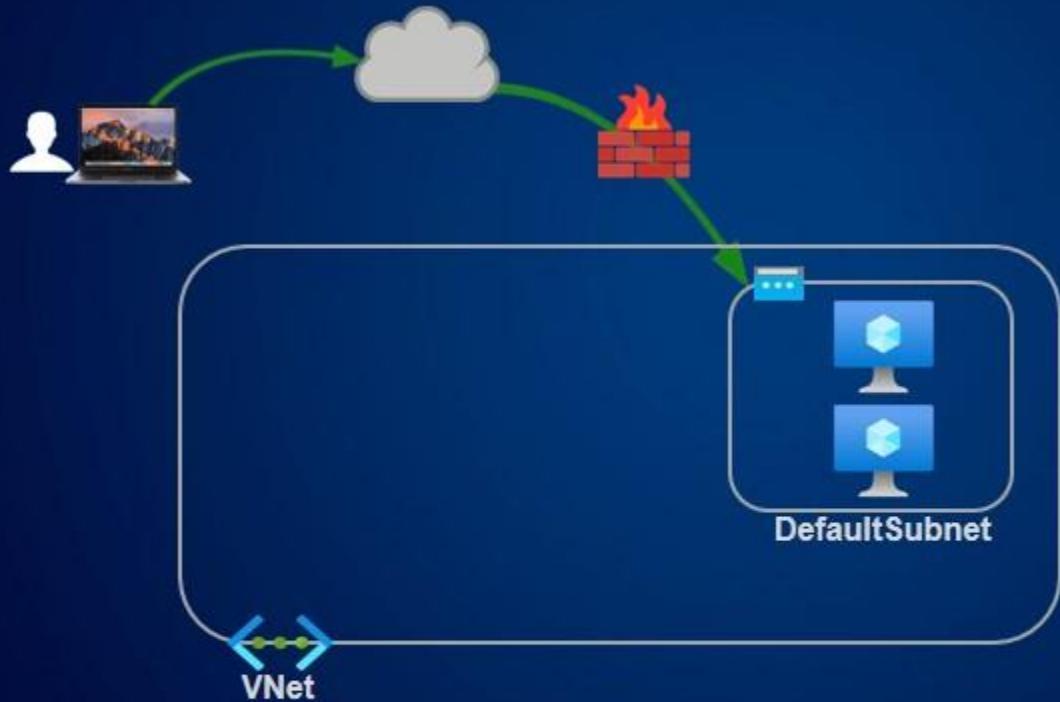
Không cần Public IP



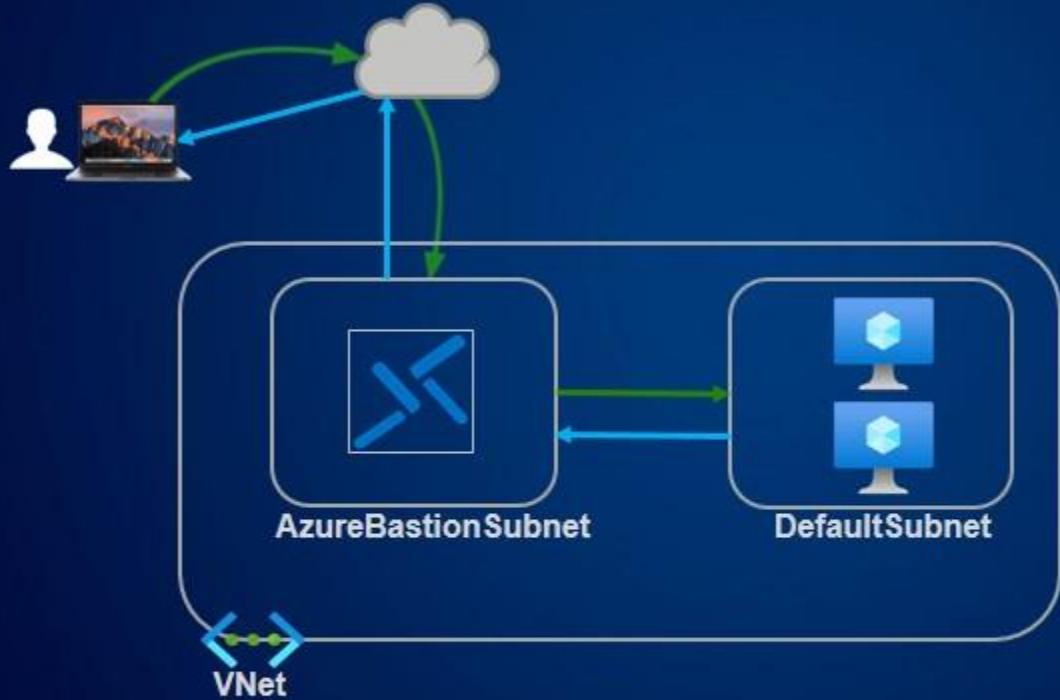
Các tính năng

- ❖ Kết nối RDP/SSH qua SSL/TLS
- ❖ Được triển khai trong mỗi một virtual network
- ❖ Kết nối tới tất cả các máy ảo (VMs) trong Vnet
- ❖ Hỗ trợ trình duyệt HTML5
- ❖ Không cần dùng Public IPs
- ❖ Chỉ hỗ trợ IPv4
- ❖ Được quản lý bảo mật

Kiến trúc của Azure Bastion



Kiến trúc của Azure Bastion



Các điểm chính của bài học



Private Traffic

Traffic từ Bastion tới đích là máy ảo (VM) là ở bên trong Vnets (Bao gồm trường hợp các VNets đã được kết nối với nhau thông qua VNet peering).



Tăng cường bảo mật

Không cần phải có NSGs bởi vì bastion đã được tăng cường bảo mật bên trong mạng nội bộ.



Tích hợp dịch vụ

Bastion tích hợp với Azure Firewall.



Concurrent Connections

Tổng số kết nối tối đa là 25 với RDP và 50 với SSH traffic.



Audit Logs

Bật (enable) tính năng ghi log (diagnostics) để theo dõi các kết nối đến và từ bastion để kiểm tra và xác minh các hoạt động.



Đổi hỏi Role

Yêu cầu cấp quyền Reader role cho Bastion, VM, và NIC để có thể sử dụng Bastion.

Thực hành truy cập vào một máy ảo Windows (VM) qua SSL không sử dụng Public IP, sử dụng Azure Bastion

Trong tình huống của bài thực hành này. Tại công ty của bạn, Security Engineers đã chặn cổng 3389 trên tường lửa và thiết lập quy định là tất cả các máy ảo Windows không được truy cập từ bên ngoài internet. Để đăng nhập vào máy ảo Windows, bạn cần đưa ra giải pháp sử dụng Azure Bastion để login vào các máy ảo (VMs) Azure.



Tạo máy ảo Windows
VM, và tạo Azure
Bastion Subnet



Tạo một dịch vụ
Azure Bastion



Truy cập vào
Windows VMs



Hoàn thành
bài lab



Giai đoạn 1



Giai đoạn 2



Giai đoạn 3



Giai đoạn 4

Thực hành cấu hình managed identity cho một máy ảo VM để truy cập vào Azure storage Account không cần Access key

Dịch vụ Managed identities cho các tài nguyên Azure cung cấp cho các dịch vụ Azure với một danh tính (identity) được quản lý tự động trong Microsoft Azure AD. Bạn có thể sử dụng danh tính này để xác thực (authentication) đến tất cả các dịch vụ mà được hỗ trợ xác thực Microsoft Azure AD mà không cần phải chứa thông tin xác thực (Credentials) trong code của bạn. Việc này giúp tăng cường tính bảo mật và loại bỏ việc cần phải quản lý và giữ bí mật trong code ứng dụng của bạn.

Trong bài thực hành này, sẽ của bạn yêu cầu bạn tạo một máy ảo Linux VM cho bộ phận phát triển (DEV), và muốn máy ảo này có quyền truy cập vào một Azure Storage Account mà không cần phải sử dụng Access key để đảm bảo việc bảo mật. Và bạn đã tìm ra một giải pháp là cấu hình sử dụng Managed Identity cho máy ảo này.



Cấu hình managed identity cho VM, để cấp quyền truy cập vào Storage Account



Setup Azure CLI cho VM



Chạy các lệnh Azure CLI bên trong VM để kiểm tra xem, có thể truy cập vào một container trong Storage Account không cần Access Key.



Hoàn thành bài lab



Giai đoạn 1



Giai đoạn 2



Giai đoạn 3



Giai đoạn 4

Giới thiệu về cân bằng tải Azure Load Balancer

Bài học bao gồm

Mô tả về Azure Load Balancer

**So sánh hệ thống mạng truyền thống vs.
Azure Load Balancer**

Các thành phần của một Azure Load Balancer

Demo: Tạo một Load Balancer

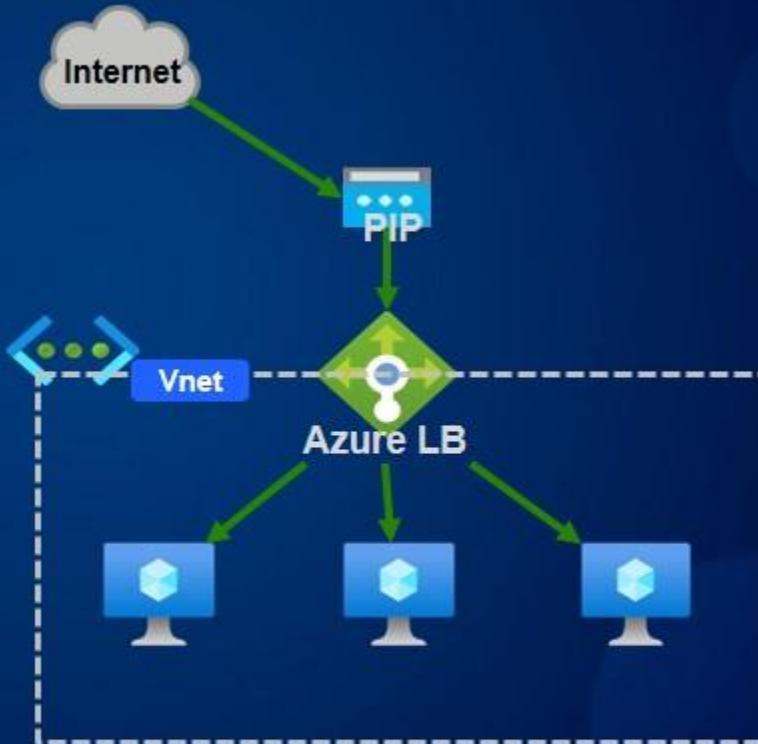
Các điểm chính của bài học

Mô tả về Azure Load Balancer

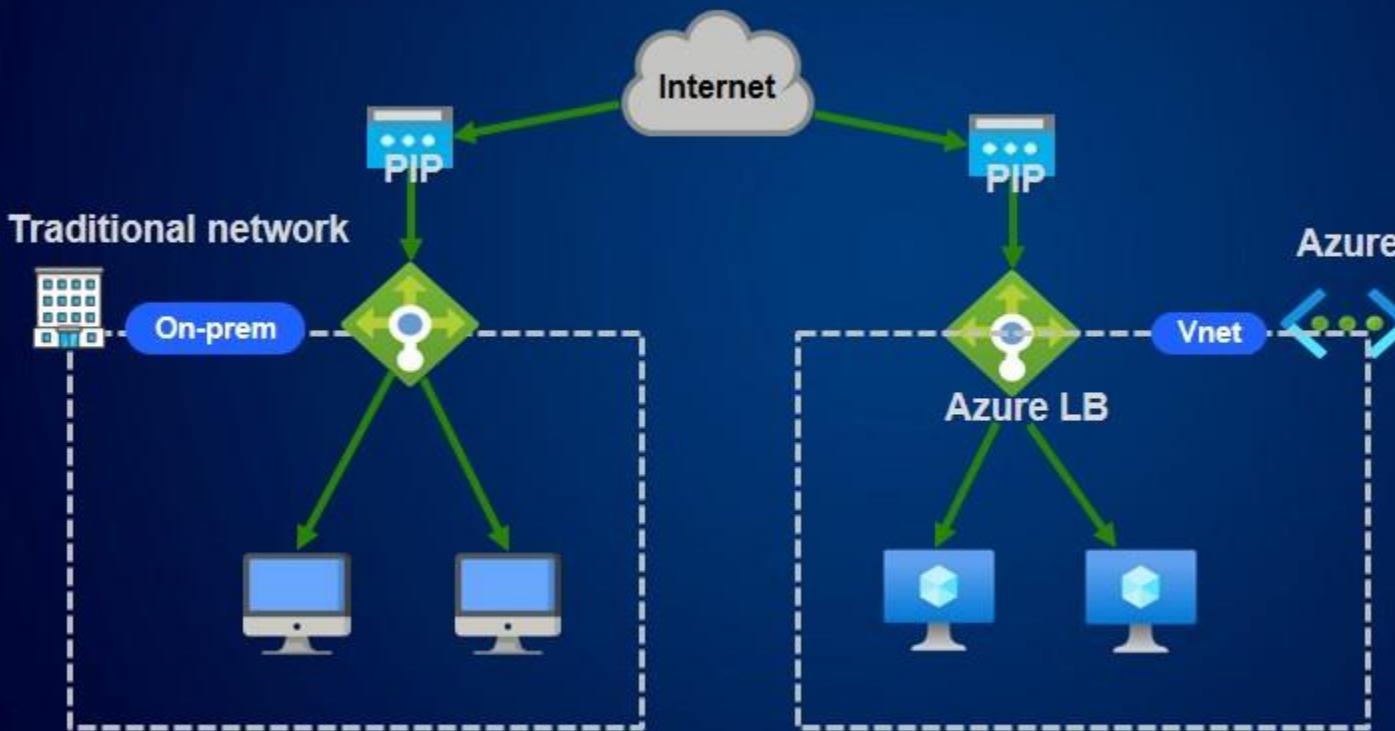
Azure Load Balancer (LB)

Azure Load Balancer là một giải pháp mạng được thiết kế để phân phối traffic mạng đồng đều giữa các máy chủ hoặc máy ảo trong hạ tầng phía sau (backend compute).

- Layer 4 load balancing (TCP/UDP)
- Tính sẵn sàng cao (High Availability)
- Các tài nguyên backend phải có tính dự phòng
- Các máy ảo (VMs) và VMSS



So sánh hệ thống mạng truyền thống vs. Azure Load Balancer



Các thành phần của một Azure Load Balancer

Frontend IP

10.0.0.0

Private hoặc public endpoint được sử dụng để truy cập vào giải pháp cân bằng tải(load balancing solution)



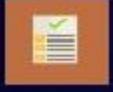
Backend Pool

Giải pháp tính toán (compute solution) cơ bản cho cân bằng tải (load balancer)



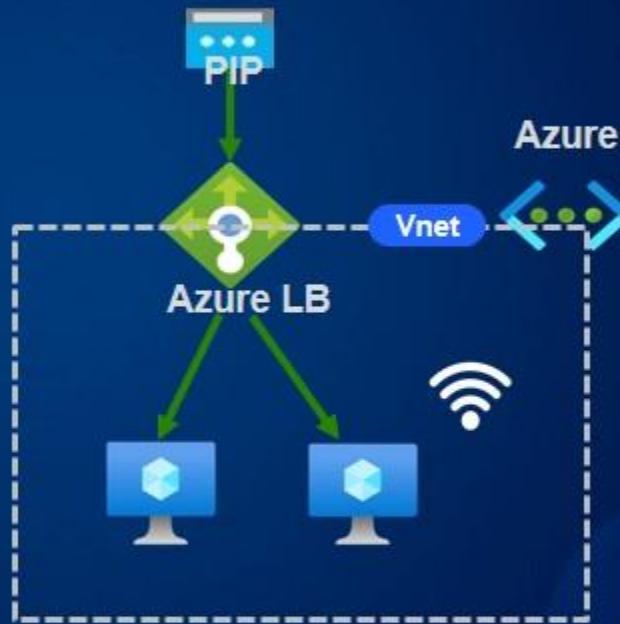
Health Probe

Một cơ chế kiểm tra định kỳ sức khỏe của backend pool để xác định các node (máy chủ hoặc máy ảo) nào đang sẵn sàng phục vụ



Rules (quy tắc)

Cân bằng tải (load balancing) hoặc các quy tắc NAT được cấu hình để cho phép truy cập vào (inbound)/ra (outbound)



Các điểm chính của bài học

Load Balacing

Cân bằng tải traffic truy cập giữa các giải pháp truy cập từ ngoài (external) và truy cập trong nội bộ (internal).

01

02

03

04

Health Probing

Health check ports cho các nodes(các máy ảo) trong backend pool.

SNAT

Port forward outbound traffic từ các nodes trong backend pool.

DNAT

Port forward inbound traffic tới các nodes trong backend pool.

Thực hành sử dụng Azure CLI để tạo một Standard Load Balancer

Trong tình huống của bài thực hành này. Công ty của bạn có một ứng dụng bị quá tải. Trong các thời điểm lượng truy cập từ người dùng tăng đột biến , ứng dụng sẽ không có phản hồi. Bạn phải triển khai một hệ thống cân bằng tải, bằng cách tạo thêm 02 servers và một standard load blancer, để giải cứu ứng dụng khỏi sự cố và cải thiện thời gian phản hồi.

✓ **Chúng ta cần vào đường link :**

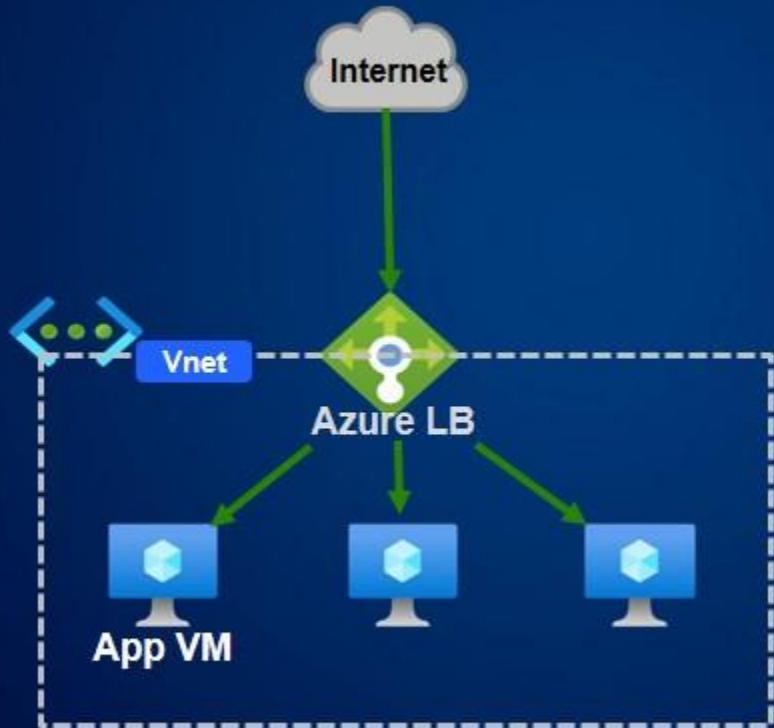
<https://raw.githubusercontent.com/phuongluuho/Azure104/main/template-Azure-LoadBalancer.json>

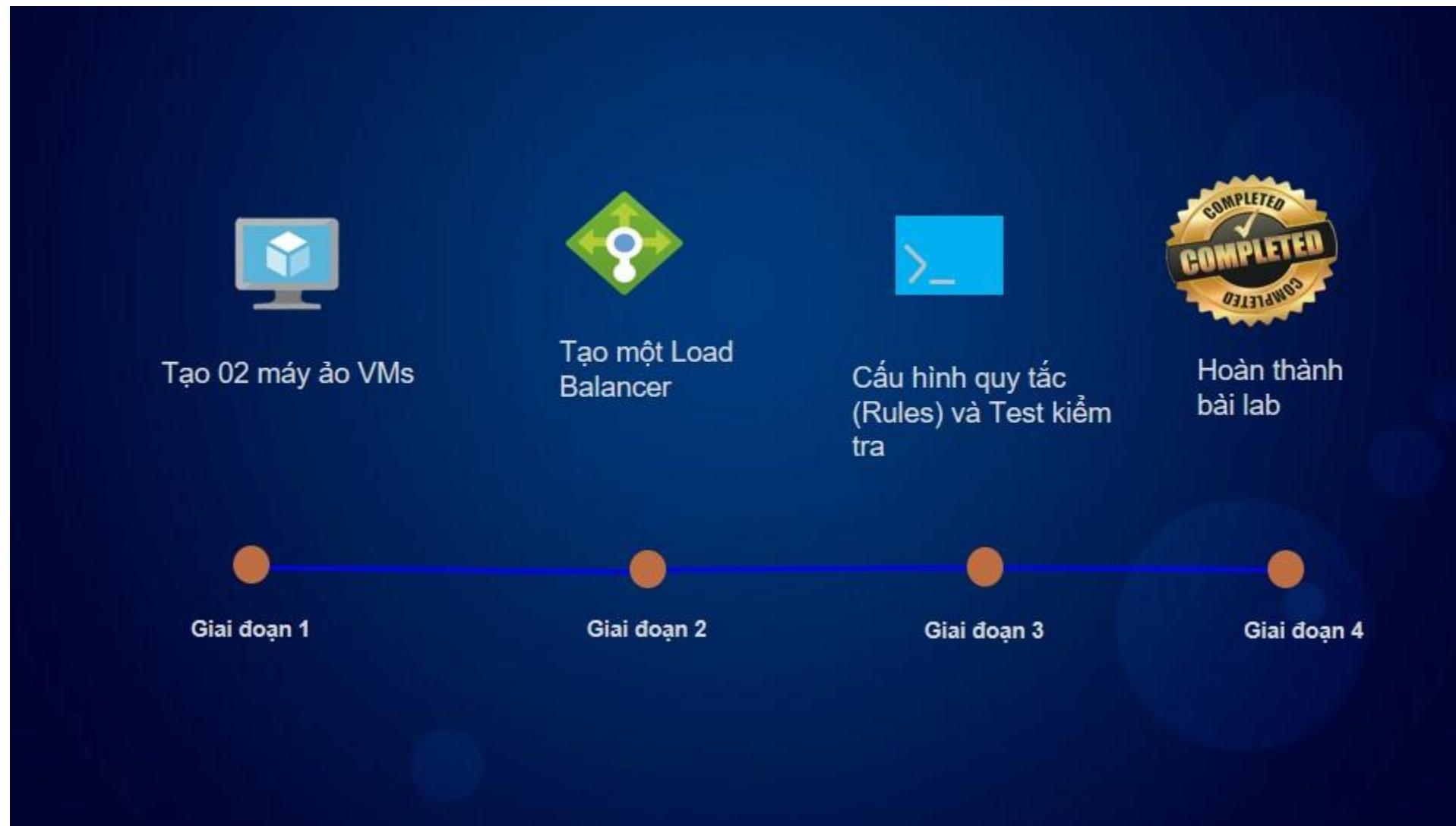
Để copy nội dung file template-Azure-LoadBalancer.json, sau đó sử dụng ARM Templates.

Để tạo ra một môi trường cho bài thực hành gồm:

01 máy ảo (VMs), 01 mạng ảo Virtual network và 01 NSG, 01 card mạng ảo, 01 Public IP.

Azure Load Balancer





Sử dụng Azure Application Gateway

Bài học bao gồm

Mô tả về Azure Application Gateway

**So sánh Azure Load Balancer vs.
Azure Application Gateway**

Các thành phần của một Application Gateway

Demo: Tạo một Application Gateway

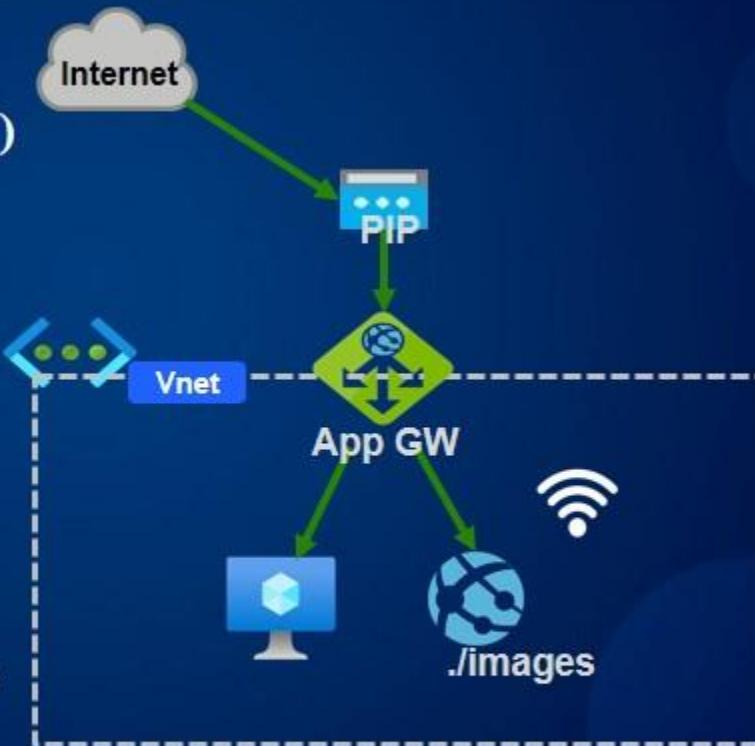
Các điểm chính của bài học

Mô tả về Azure Application Gateway

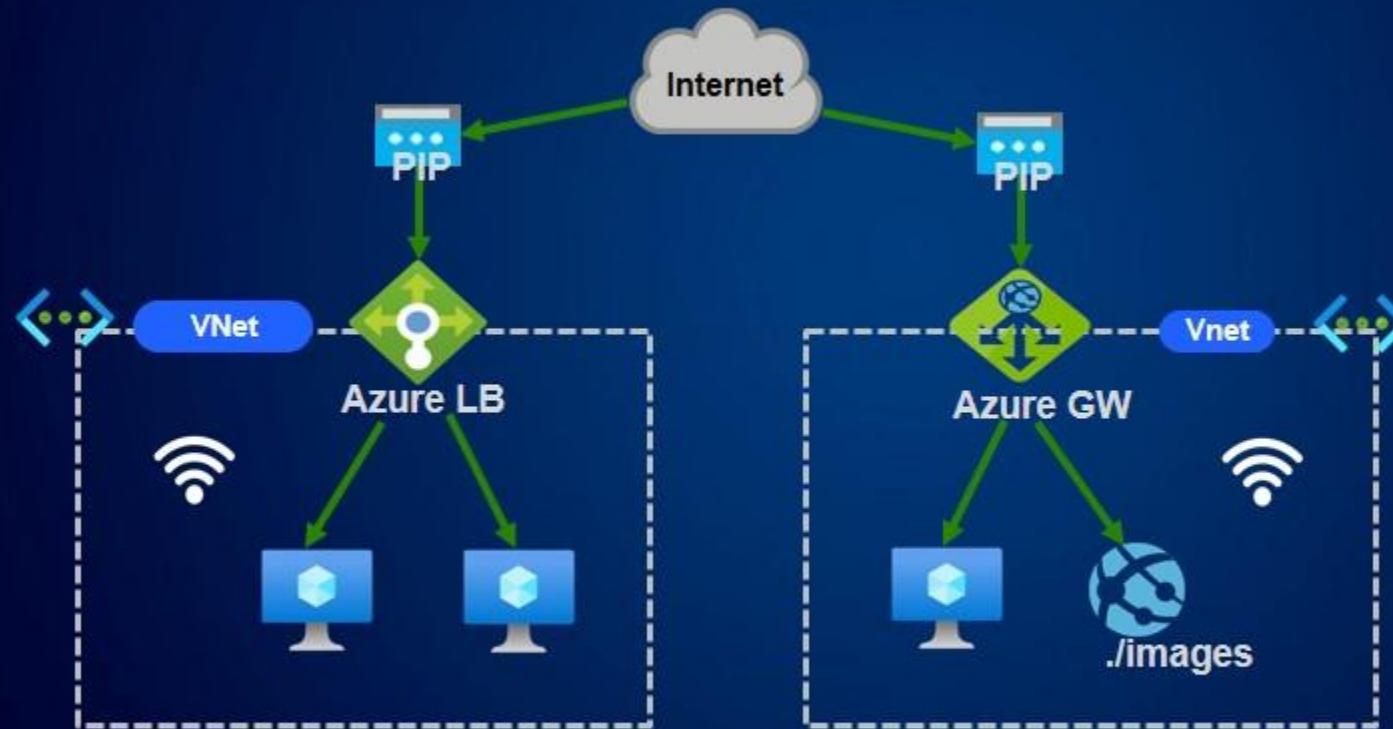
Azure Application Gateway (App GW)

Azure Application Gateway là một dịch vụ Networking cho cân bằng tải giữa backend compute.

- Layer 7 load balancing (HTTP/HTTPS)
- Định tuyến dựa trên đường dẫn URL (URL path-based Routing)
- Các tài nguyên backend phải được dự phòng
- Các máy ảo (VMs) và VMSS, App services



So sánh Azure Load Balancer vs. Azure Application Gateway



Các thành phần của một Application Gateway

Frontend IP

10.0.0.0
Private hoặc public endpoint được sử dụng để truy cập vào giải pháp cân bằng tải (load balancing solution).

Backend Pool

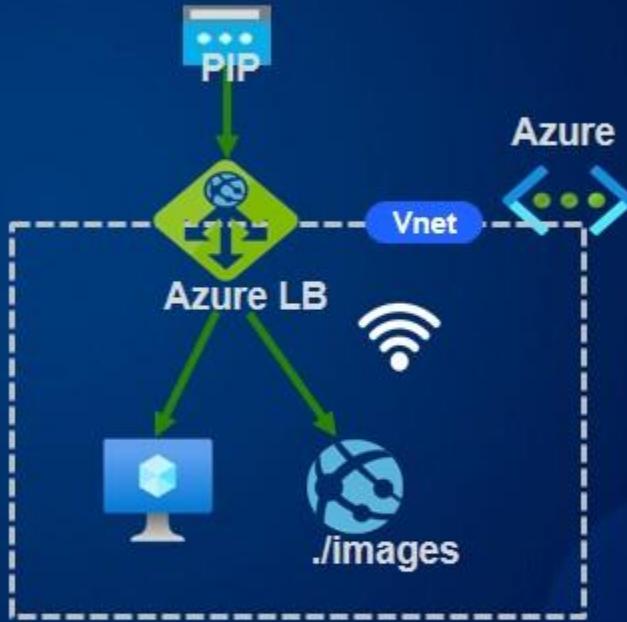
Giải pháp tính toán (compute solution) cơ bản cho cân bằng tải (load balancer.)

Listener

Cổng (Port), giao thức (protocol), và các cấu hình chứng chỉ (certificate configurations).

Rules (quy tắc)

Các quy tắc cân bằng tải (Load balancing rules), HTTP settings, và health probe.



Các điểm chính của bài học

Load Balancing

Cân bằng tải traffic giữa các backend pools sử dụng HTTP/HTTPS.

Tăng giảm quy mô (Autoscaling)

Tăng quy mô (Scale up) / Giảm quy mô (Scale down) các backend pools cho application gateway.

SSL Termination

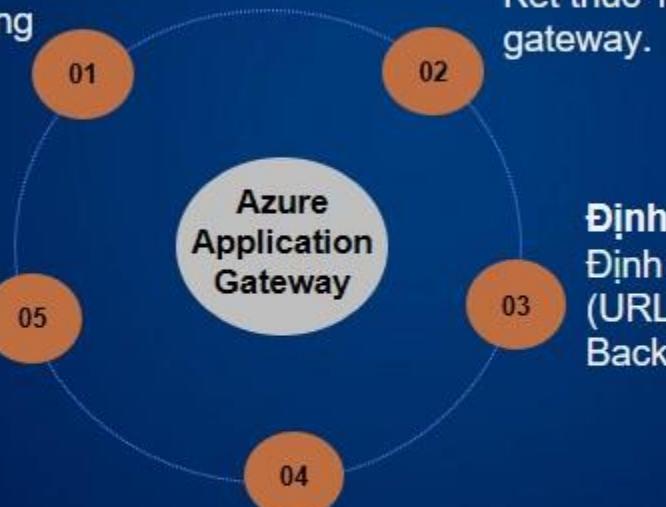
Kết thúc TLS/SSL tại application gateway.

Định tuyến URL (URL Routing)

Định tuyến dựa trên đường dẫn (URL path-based routing) giữa các Backend pools.

Bảo mật (Security)

Web Application Firewall làm tường lửa bảo mật cho giải pháp cân bằng tải.



Cấu hình một Application Load Balancer và VM Scale Set tự động điều chỉnh quy mô VMs trong Azure

- Cấu hình một Virtual Machine Scale Set (VMSS) để host một static website
- Cấu hình một Azure Application Gateway để cân bằng tải và là một gateway trung tâm cho phép người dùng (users) có thể truy cập vào static website.
- Cấu hình autoscale để đảm bảo việc tự động tăng (scale out)/giảm quy mô (scale in) theo nhu cầu truy cập của người dùng vào static website.

✓ **Chúng ta cần vào đường link :**

<https://raw.githubusercontent.com/phuongluuho/Azure104/main/Template-nw-nsg.json>

Để copy nội dung file Template-nw-nsg.json, sau đó sử dụng ARM Templates.

Để tạo ra một môi trường cho bài thực hành gồm:

01 mạng ảo Virtual network và 01 NSG, 01 Storage Account.

Kiến trúc cân bằng tải của Application Gateway

Virtual Machine Scale Set

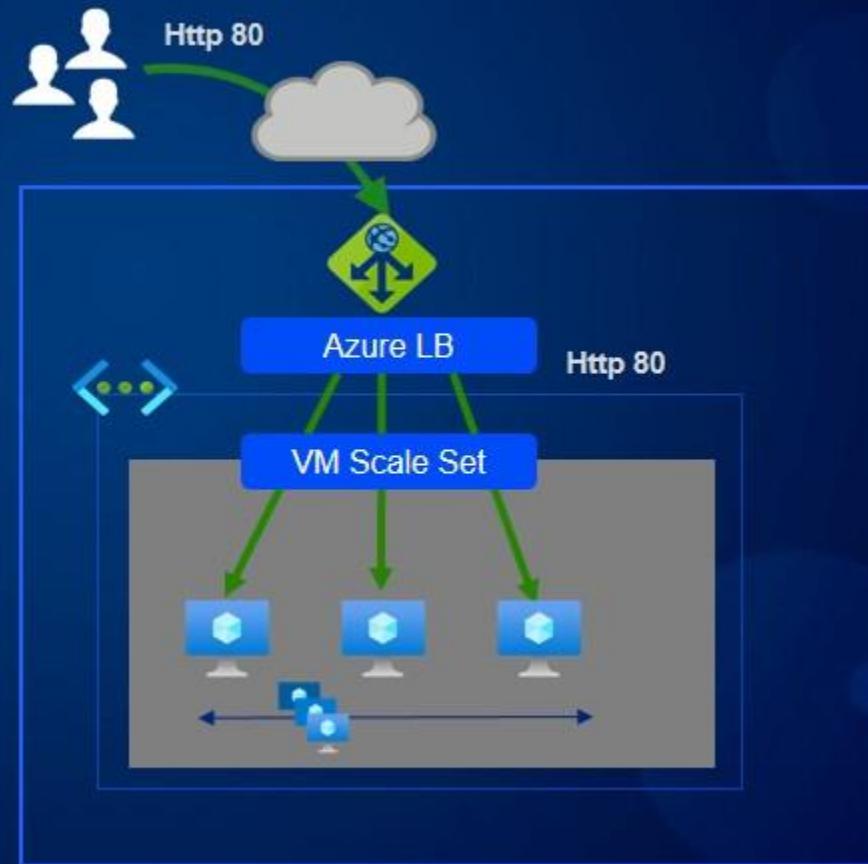
Một tập hợp gồm nhiều máy ảo VMs cung cấp cùng một dịch vụ và được build từ cùng một image.

Autoscale Rules (quy tắc tự động điều chỉnh quy mô)

Rules (quy tắc) tăng giảm số lượng máy ảo (VMs) bên trong một VMSS, theo nhu cầu từ người dùng (users).

Azure Application Gateway LB

Đóng vai trò trung tâm cân bằng tải cho static website. Nó sử dụng backend pool & routing rule để cân bằng tải các traffic truy cập vào các máy ảo VMs healthy back-end.

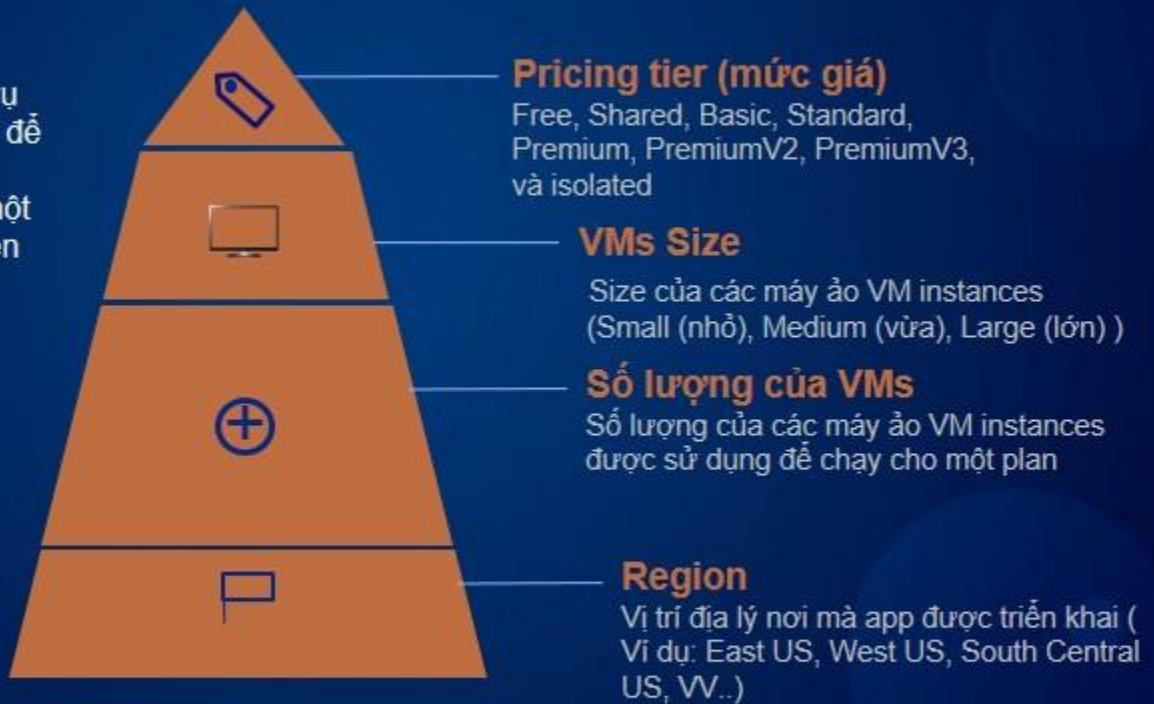


Tạo một App Service Plan

App Service Plan là gì?

App Service Plan

Một "App Service Plan" là một dịch vụ trong Microsoft Azure được sử dụng để định nghĩa và quản lý các tài nguyên điện toán (compute resources) mà một ứng dụng web (web app) sẽ chạy trên đó.



Các loại App Service Compute

Pricing tier (mức giá) của một gói dịch vụ App Service plan xác định các tính năng bạn nhận được và số tiền bạn phải trả. Có ba loại điện toán lõi (core compute) cho các gói dịch vụ.



Shared

Chạy các ứng dụng (apps) trên cùng một VM với các ứng dụng khác, bao gồm cả các ứng dụng của các khách hàng khác.
(Không thể mở rộng quy mô (scale out) vì là mô hình điện toán được chia sẻ (shared compute))



Dedicated

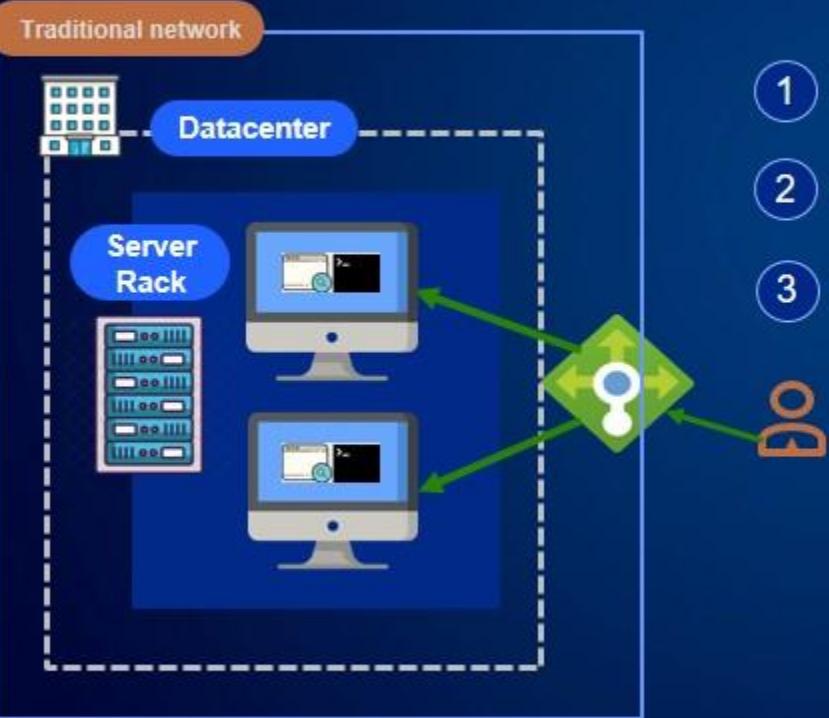
Chỉ chạy các ứng dụng sử dụng cùng một app service plan trên một máy ảo chuyên dụng (dedicated VM).
(Mô hình điện toán biệt lập (isolated compute).)



Isolated

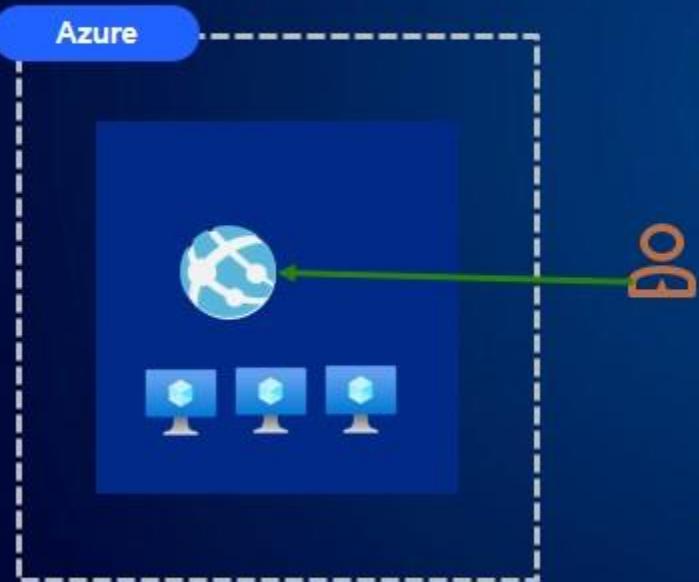
Chạy các ứng dụng sử dụng các máy ảo chuyên dụng (dedicated VMs) và các mạng ảo chuyên dụng (dedicated Vnets).
(Mô hình điện toán biệt lập (isolated compute) và networking.)

So sánh hệ thống truyền thống vs. App service



- 1 Quản lý và quản trị máy chủ và hạ tầng mạng
- 2 Quản lý update vá lỗi (patching) và bảo mật
- 3 Quản lý hệ thống cân bằng tải (load balancing)

So sánh hệ thống truyền thống vs. App service



- 1 Được Azure quản lý hạ tầng
- 2 Tính sẵn sàng cao (High availability)
- 3 Tính linh hoạt, khả năng mở rộng quy mô hệ thống (Scalability)

Các điểm chính của bài học

1 App service Plans

Một plan định nghĩa các tài nguyên điện toán và các tính năng có sẵn cho một web app.

2 Các tài nguyên điện toán của App service Plans

Mức giá (Pricing tier), cấu hình size của các máy ảo (VM instances), số lượng của các máy ảo, và region.

3 Các loại điện toán App service Plans Types

Được chia sẻ (Shared), chuyên dụng (Dedicated), và biệt lập (isolated). Mỗi một loại cung cấp một cấp độ khác nhau của điện toán biệt lập, mạng biệt lập, và các tính năng như mở rộng quy mô (scaling).

4 App service Plans và Web Apps

Cung cấp một Platform as a Service (PaaS) để cấu hình và host các ứng dụng, mà chúng ta không phải quản lý hệ thống hạ tầng mạng và máy chủ. Chúng ta chỉ cần quản lý các cấu hình cụ thể và code của chúng ta.

Tạo Web Apps

Các tính năng của Web App



Được quản lý cơ sở hạ tầng

Không cần phải update các bản vá lỗi, bảo trì, cấu hình & cài đặt các thành phần bên trong cơ sở hạ tầng với Platform as a Service (PaaS).



Tính sẵn sàng cao (Highly Available)

Azure App Service chạy các ứng dụng (apps) trên nhiều nodes để cung cấp tính sẵn sàng cao.



Tự động điều chỉnh quy mô

(Autoscaling In/Out)

các khả năng điều chỉnh quy mô giống với Azure Scale Sets, để đảm bảo chúng ta có thể đáp ứng các đòi hỏi traffic truy cập mạng cho ứng dụng của chúng ta.



Tập trung vào việc phát triển

Việc phát triển code ứng dụng là ưu tiên hàng đầu trong quá trình triển khai web app service deployments.



Deployment Slots

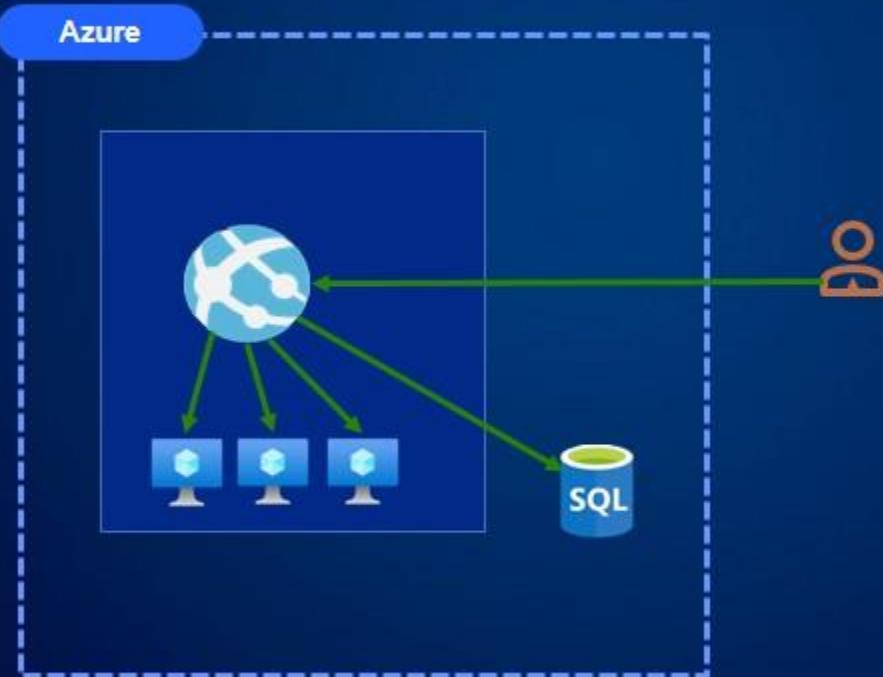
CI/CD DevOps cung cấp các tính năng như các môi trường triển khai(staging slots) cho việc triển khai, ví dụ như môi trường triển khai sản phẩm (production slot) và môi trường triển khai thử nghiệm (staging slot).



Azure Service Integration

App Service tích hợp một số dịch vụ của Azure, như Azure AD như là một nhà cung cấp danh tính (identity provider) hoặc các mạng ảo (Vnets) để kết nối App Service với các tài nguyên bên trong một mạng ảo.

Kiến trúc Web App



Tạo Web Apps- phần 2

Các điểm chính của bài học

1 Application Runtime

Host một ứng dụng sử dụng một runtime cụ thể được chọn như là một phần của quá trình cung cấp môi trường thực thi cho web app

2 Public Accessibility

Mặc định Web Apps cho phép truy cập Public và chúng ta có thể sử dụng Domain được cấp để truy cập vào Web apps

3 Các công cụ publish ứng dụng

Sử dụng các công cụ như Azure DevOps, GitHub, Zip file, SCM, VV.. Để publish code ứng dụng vào web apps

4 Hỗ trợ database

Sử dụng connection string để kết nối database của chúng ta với web app.

Các cấu hình (configurations) của Web Apps

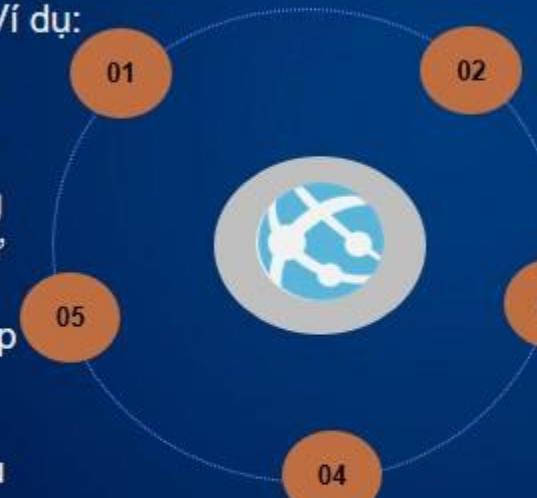
Các tùy chọn cấu hình Web Apps

Custom Domain

Cấp một domain tùy chọn để sử dụng cho web app, Ví dụ: www.company.com

Backup

Backup web apps sử dụng các bản sao lưu lưu trữ dữ liệu đầy đủ (full archival backup) hoặc các bản chụp sao lưu gia tăng (incremental snapshots). Và lưu trữ các bản sao lưu vào dịch vụ Blob Storage trong một storage account



Scaling

Cấu hình định nghĩa các tùy chọn điều chỉnh quy mô (scaling options) để scale up/scale out các tài nguyên điện toán cho web apps

Triển khai (Deployment)

Triển khai các ứng dụng sử dụng các chiến lược DevOps, như sử dụng các môi trường triển khai (deployment slots) cho một môi trường chạy thử nghiệm (staging slot) và một môi trường chạy thật (production slot).

Network

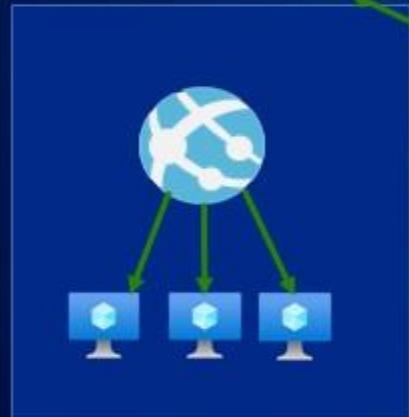
Quản lý các tùy chọn network và thực hiện các việc tích hợp VD như kết nối Web apps với Vnets, CDN, VV.

Web App Custom Domain

Azure

www.company.com

<app-name>.azurewebsites.net



DNS Zone

Type	Host	Value
A	@	<IP>
TXT	@	<verification_code>

Do

Web App Custom Domain

Azure

www.company.com

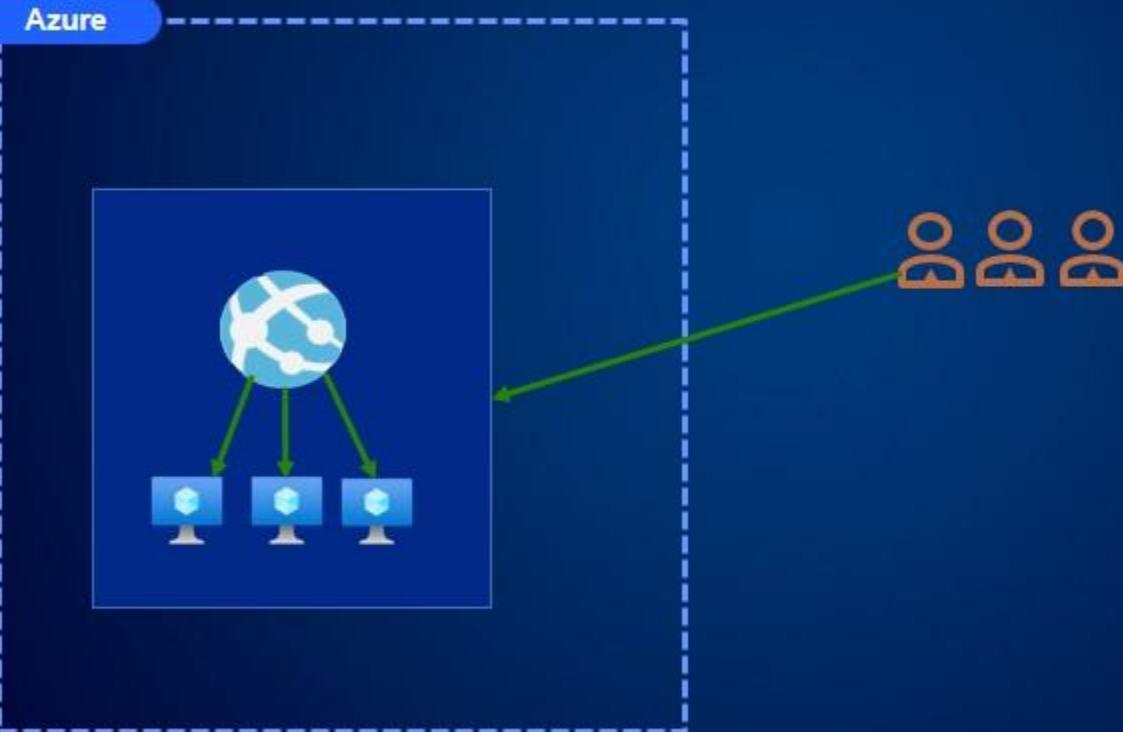


DNS Zone

Type	Host	Value
A	@	<IP>
TXT	@	<verification_code>

Do

Web App Scaling



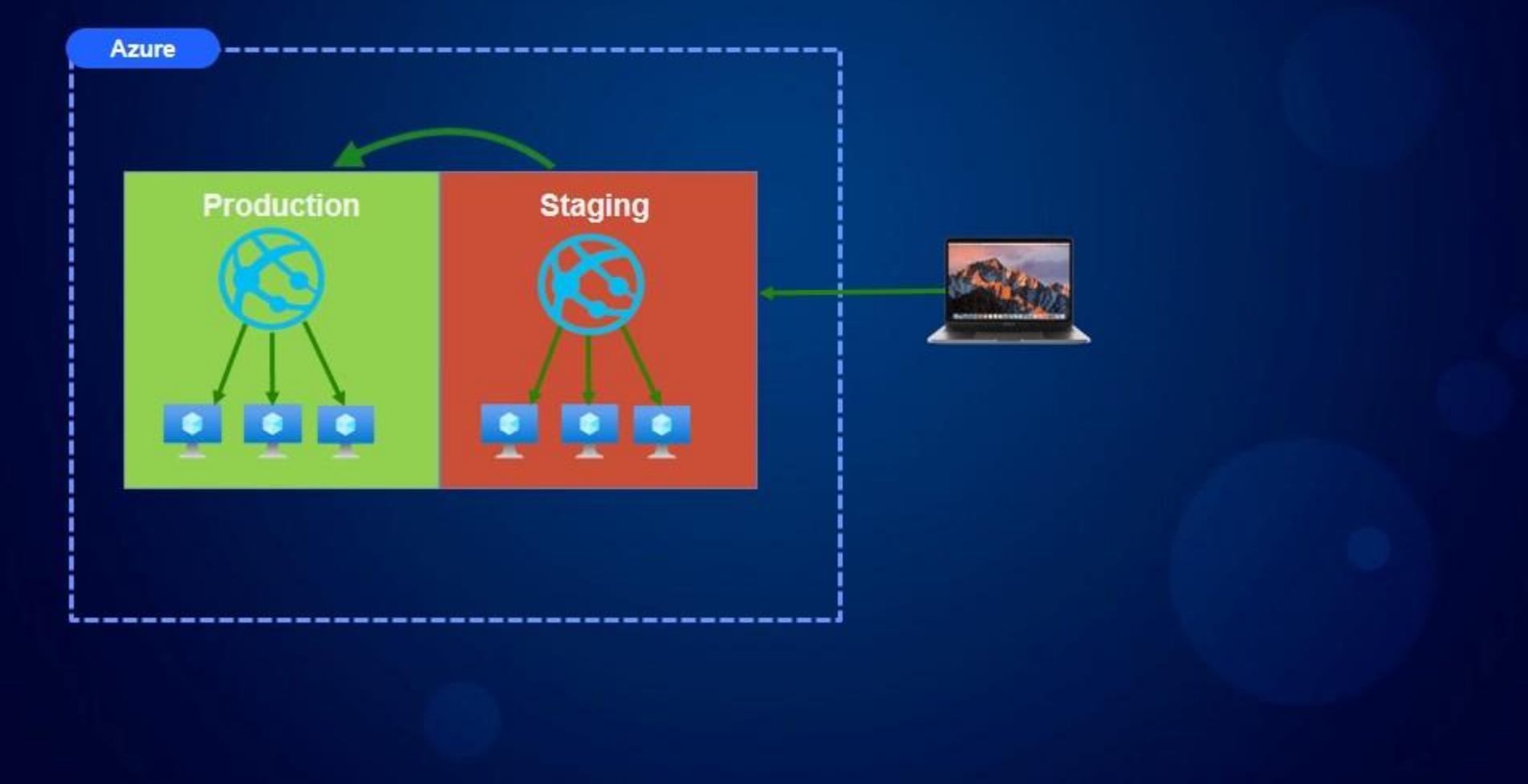
Web App Scaling

Azure

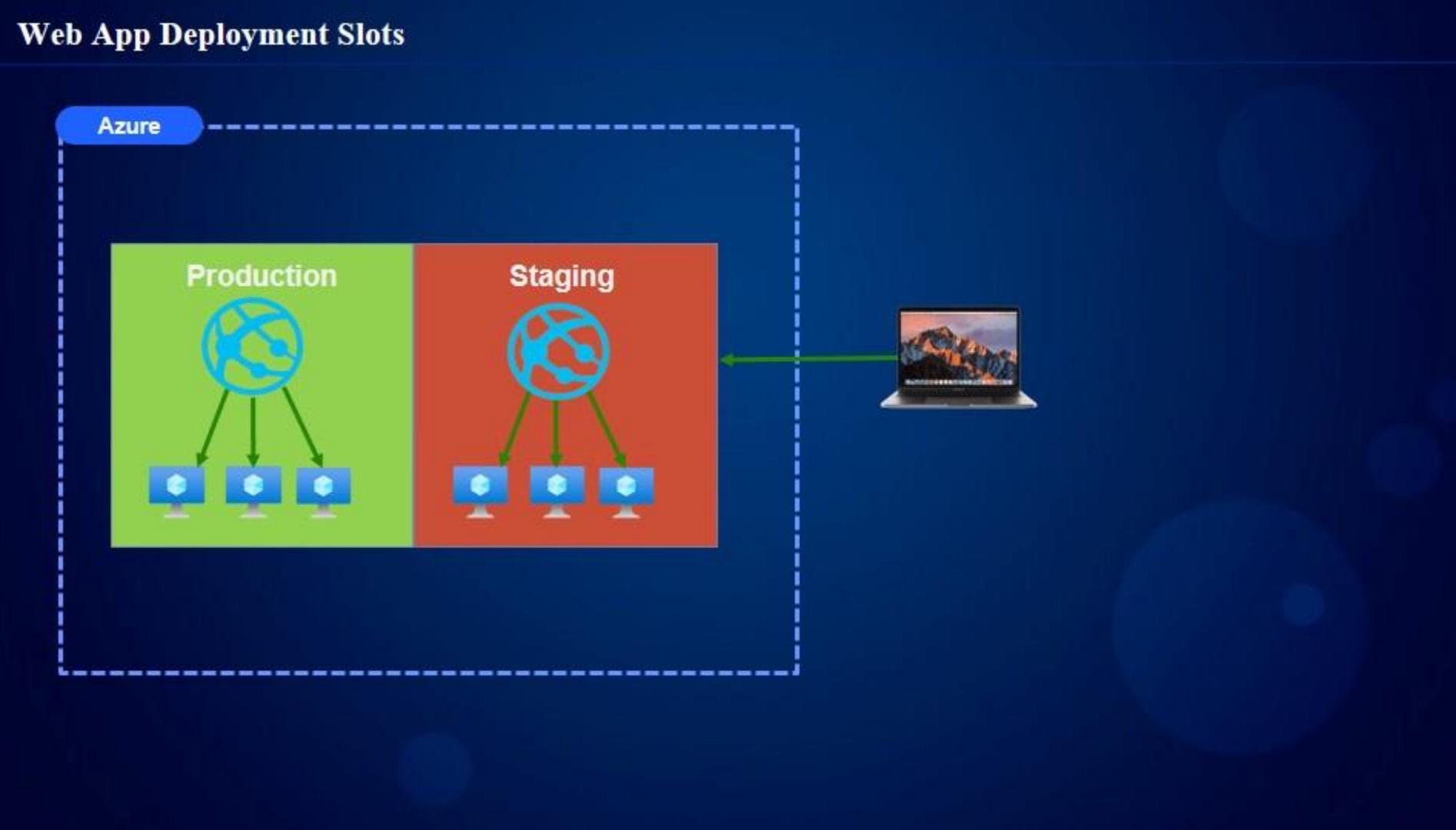


- 1 Scale up Compute
- 2 Scale out Compute

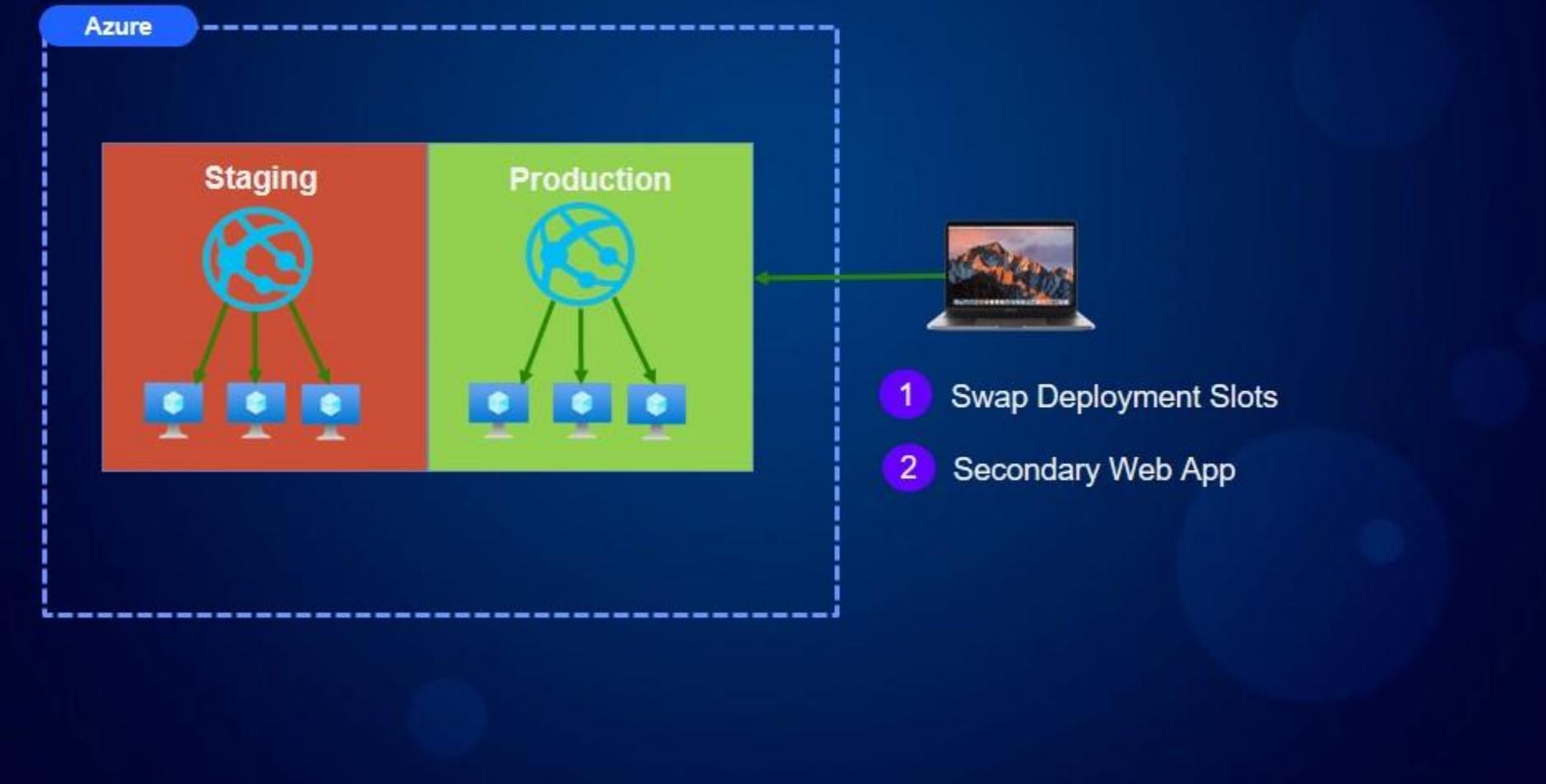
Web App Deployment Slots



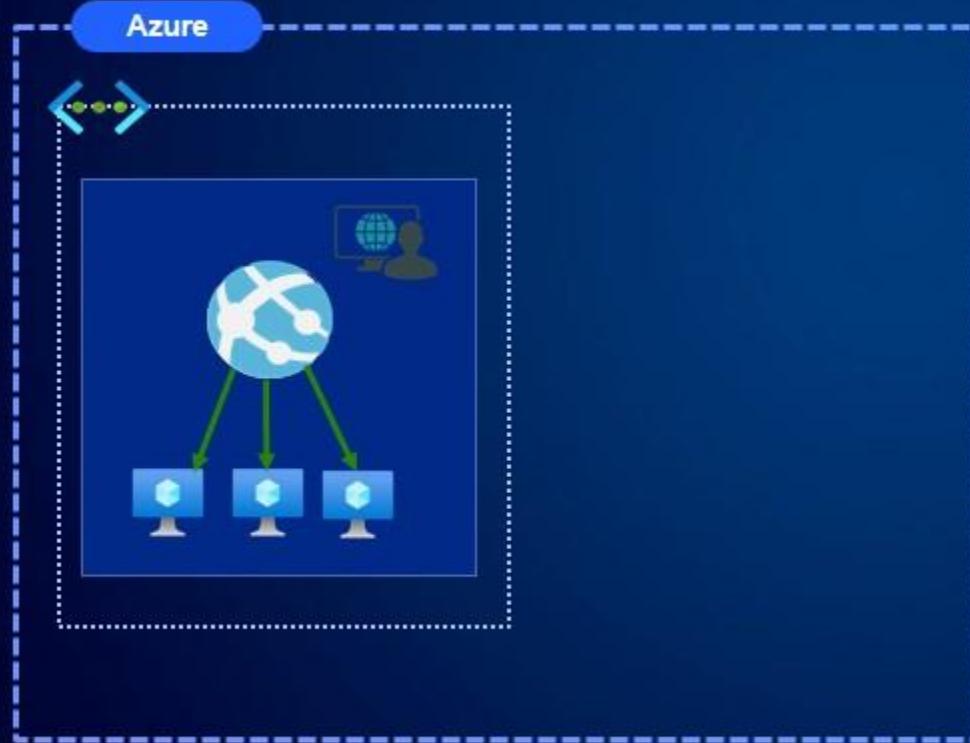
Web App Deployment Slots



Web App Deployment Slots

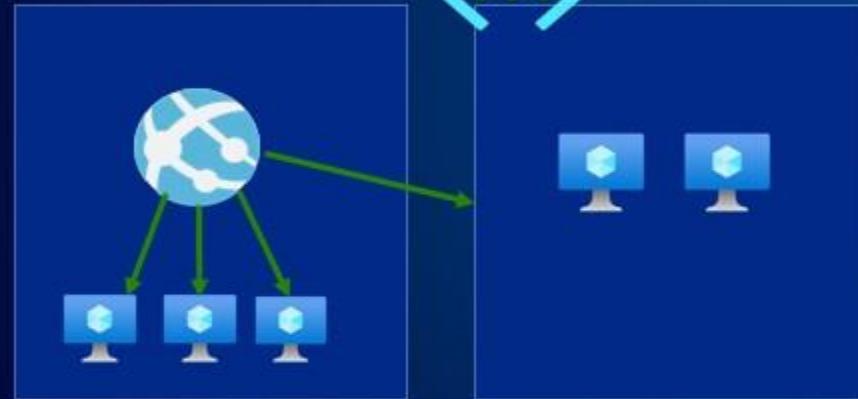


Web App Network Settings



Web App Network Settings

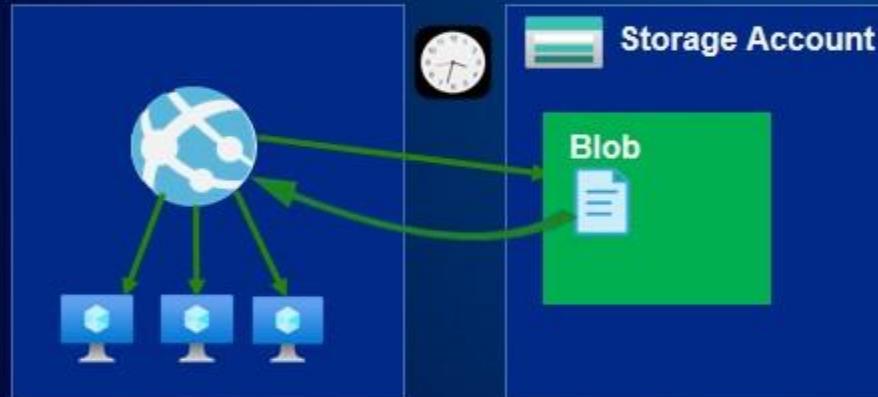
Azure



- 1 Isolated Only
- 2 Vnet integration

Web App Backup

Azure



Full Backup Snapshot



- 1 App Configuration
- 2 File Content
- 3 Database Connection

Các điểm chính của bài học



Scaling

Bị giới hạn bởi mức giá (pricing tier) và loại điện toán (compute type).



Deployment

Được sử dụng cho các môi trường chạy các ứng dụng cho một hoán đổi (swap).



Network

Web App mặc định được public, và có thể được triển khai bên trong hoặc được tích hợp với một Vnet.



Backup

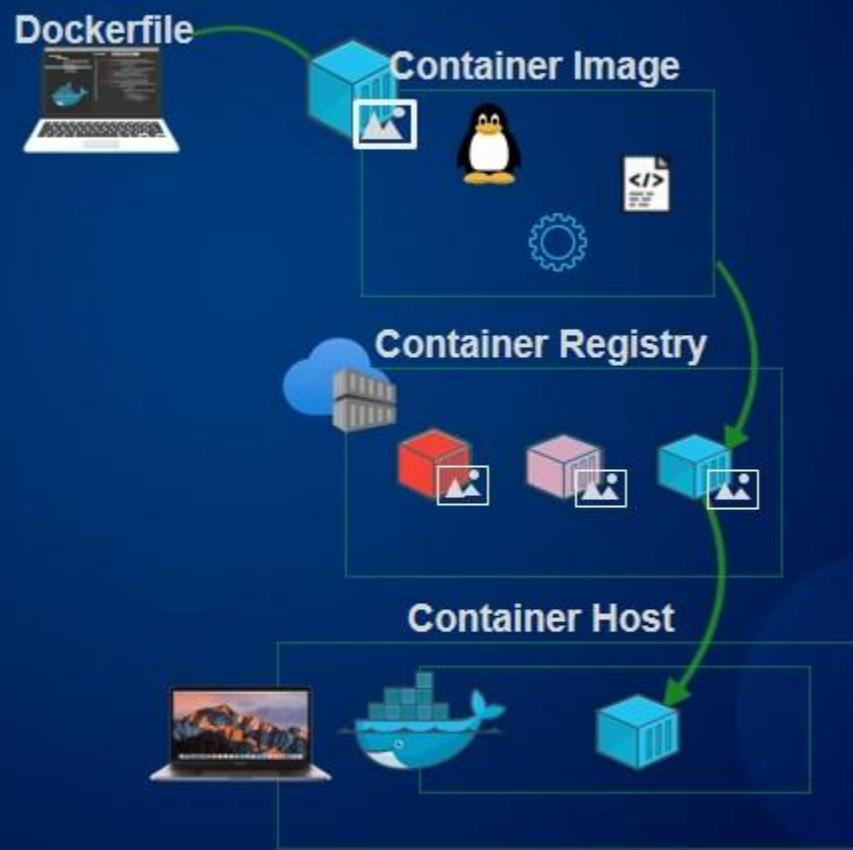
Blob backups cho app configs, file content, và database connections.

Mô tả về Containers trong Azure

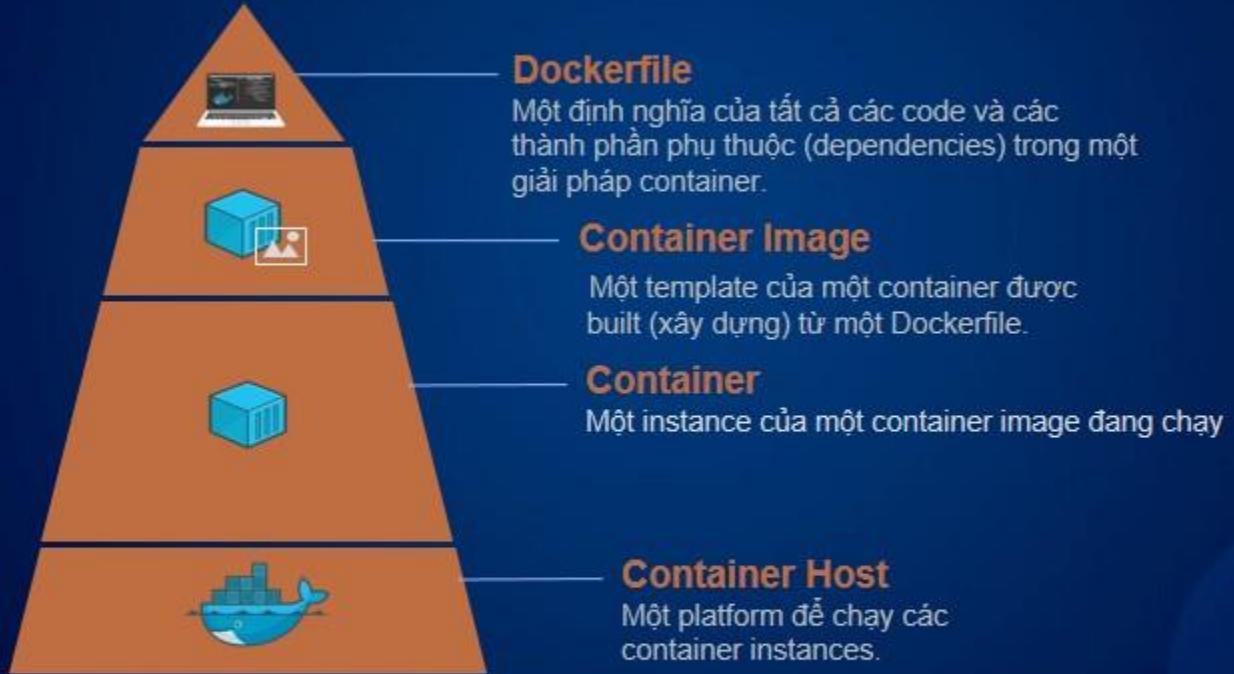
Containers là gì?

Container

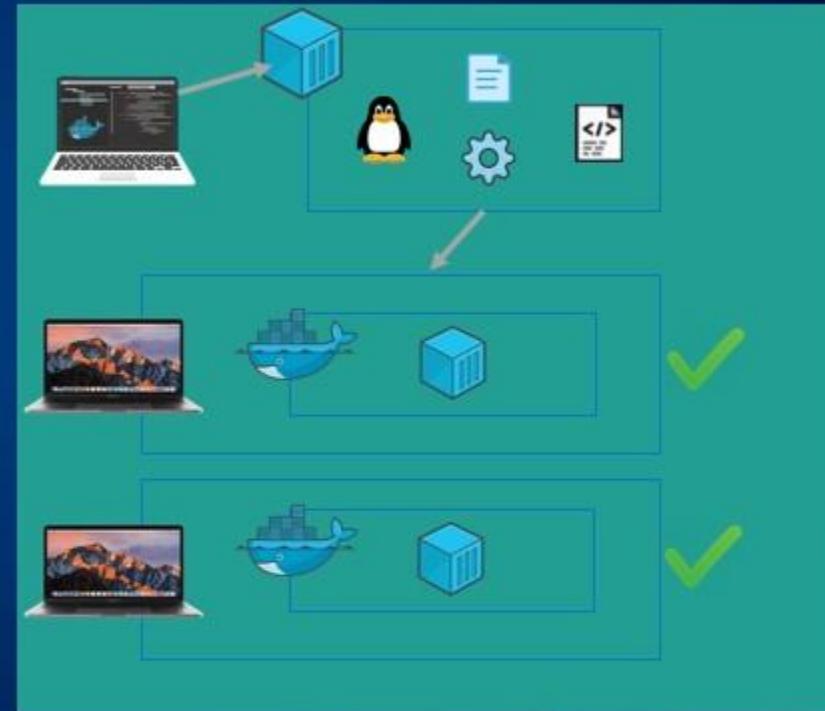
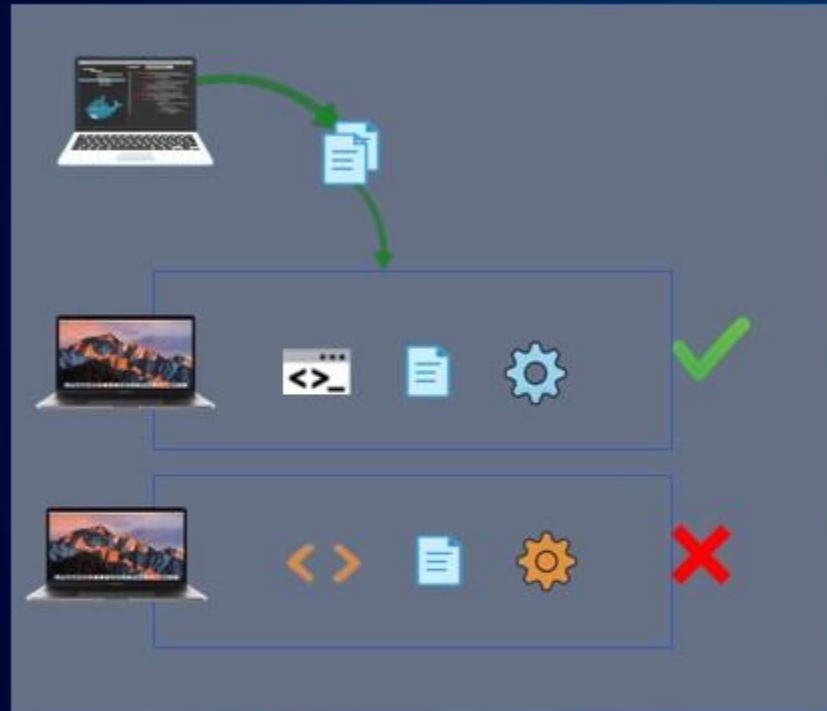
Một container là một đơn vị đóng gói (a unit of software). Nó bao gồm code, các thành phần phụ thuộc (dependencies), và cấu hình (configurations). Containers mang lại tính di động và đồng nhất, cho phép chúng ta dễ dàng triển khai và chạy ứng dụng trên nhiều loại môi trường khác nhau.



Containers là gì?



Các khái niệm về Container Development



Thực hiện một Demo



Tạo một Container

Tạo các containers tuân theo một quy trình giống nhau, bất kể chúng được triển khai trong môi trường nào.



Tạo một Container Registry

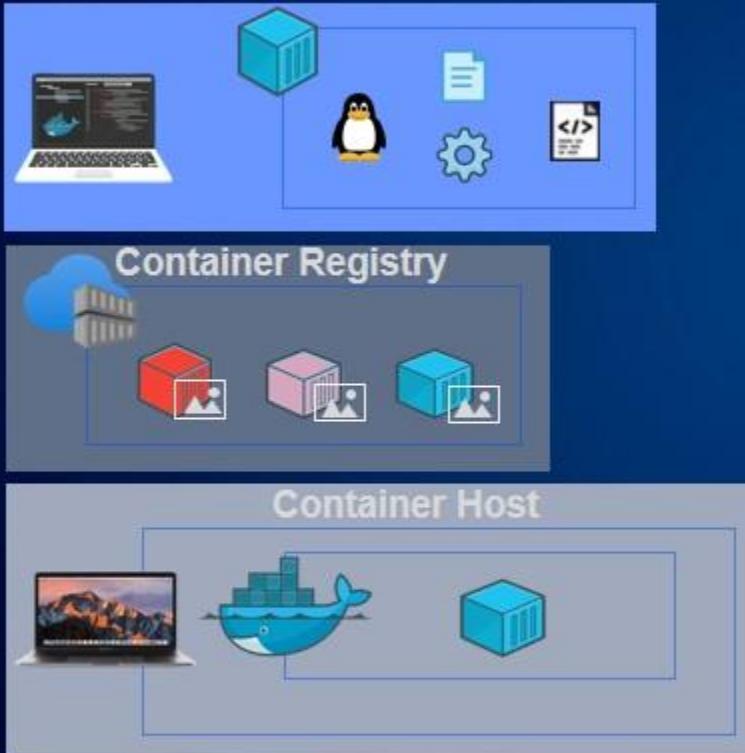
Tạo một Azure Container Registry , nó sẽ hoạt động như là một repository (kho lưu trữ)



Push (Đưa) Container vào Registry

Push container image vào Azure Container Registry, nó là một repository của Container images.

Các điểm chính của bài học



Development

Tạo và build một container để chúng ta có thể dễ dàng đóng gói ứng dụng và push container image để chạy nó trên cloud và các môi trường khác nhau.

Registry

Quản lý một container registry (repository) của một container images trong một nơi duy nhất,. VD: Azure Container Registry (ACR) .

Host

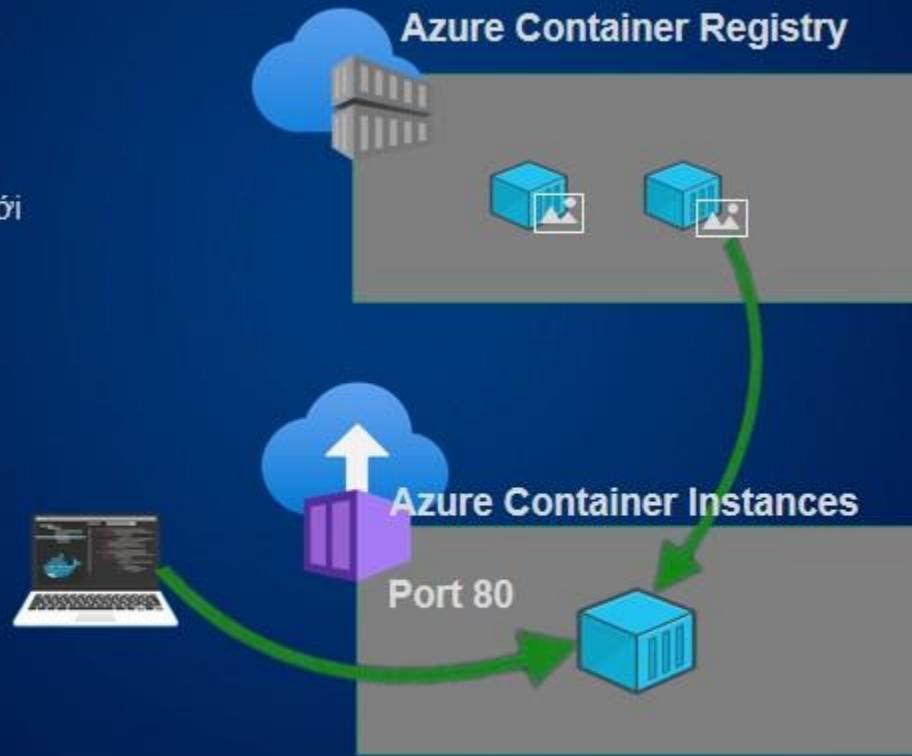
Host một container image như một instance của một container trong một hosting service.
VD: Azure container instances (ACI)

Sử dụng Azure Container Instances cho Containers

Mô tả về Azure Container Instances

Azure Container Instances (ACI)

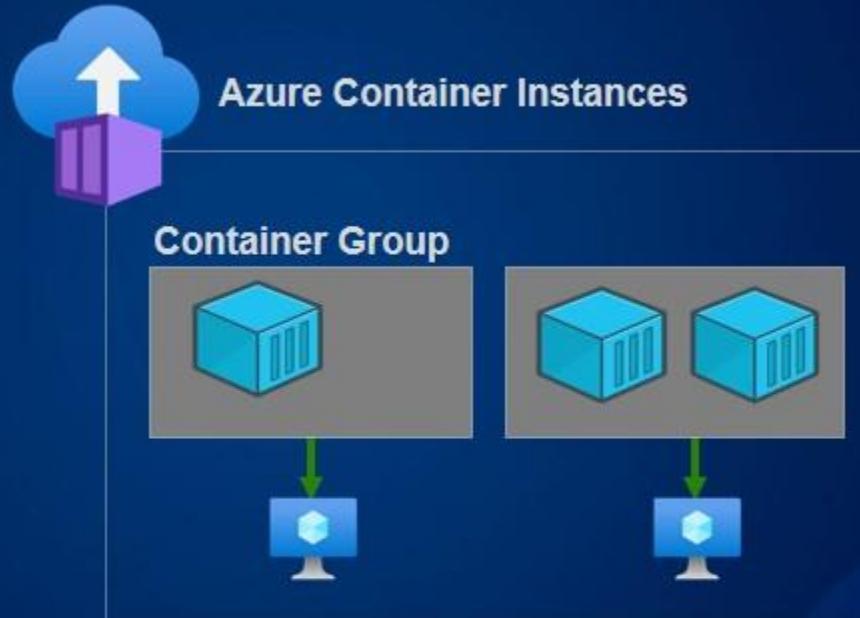
Azure Container Instances là một container hosting service, giống với Docker.



Mô tả về Azure Container Instances

Định nghĩa Container Groups

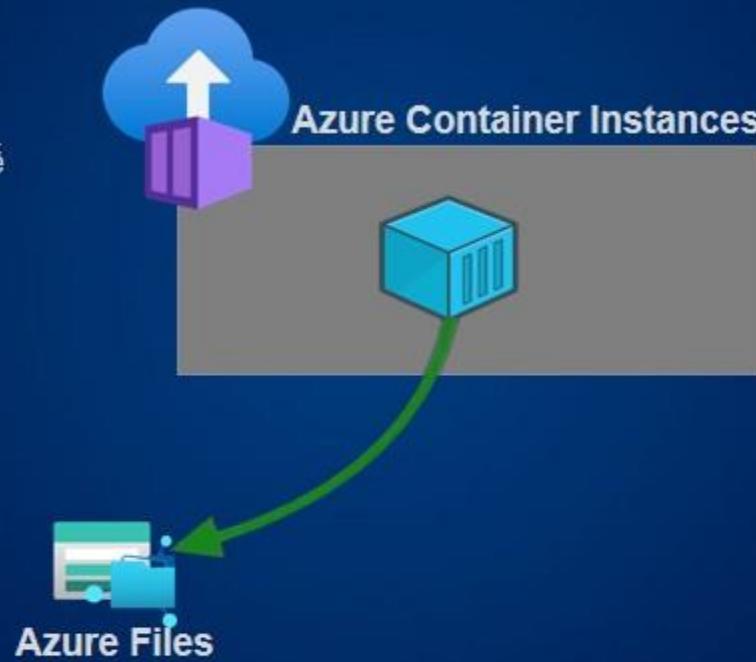
Là một tập hợp gồm các Containers, cùng chia sẻ một vòng đời, các tài nguyên, local networking và storage.



Mô tả về Azure Container Instances

Container Storage

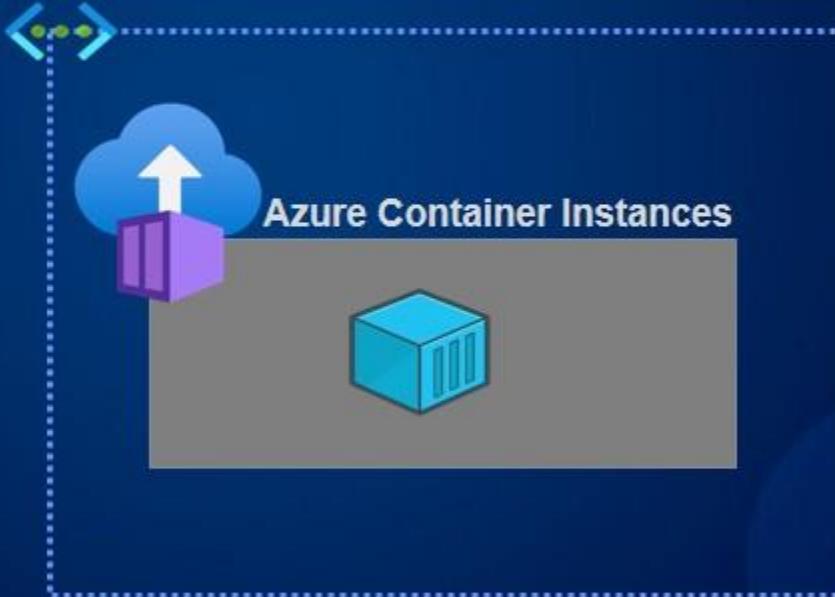
Có thể sử dụng Azure file share để lưu trữ dữ liệu cho containers.



Mô tả về Azure Container Instances

Container Networking

Có thể triển khai các containers trong private hoặc public network.



Mô tả về Azure Container Instances

Container Networking

Có thể triển khai các containers trong private hoặc public network.



Thực hiện một Demo



Tạo một Container Group

Tạo một container group sử dụng một image trong Azure Container Registry (ACR).



Triển khai một giải pháp Multi-Container

Sử dụng một JSON file để tạo một multi-container container group, chạy được nhiều containers.



Update Container Group

Update container group với một FQDN.

Các điểm chính của bài học



**Scaling (Điều chỉnh quy mô)/
Sizing (điều chỉnh cấu hình)**
Không có các tùy chọn tự động
Scaling, cần triển khai lại một
container group. Và chúng ta cần định
nghĩa CPU, memory và GPU.

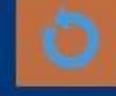


Container Groups
Một top-level tài nguyên trong
ACI. Một tập hợp gồm các containers
trong một host machine và chia sẻ
cùng một vòng đời và các tài nguyên.



Storage

Có thể gắn (mount) một storage volume
cho một container để lưu trữ dữ liệu cho
container này một cách liên tục.
VD: một Azure file share trong Azure Files.



Restart Policy (chính sách khởi động lại)

Sử dụng Restart Policy cho các containers :
Always, Never, và OnFailure.

Sử dụng Azure ACR Tasks để build và chạy một Container

Sếp của bạn muốn bạn chạy ứng dụng trong một container, nhưng do bạn không cài đặt Docker desktop trong máy tính của bạn. Tuy nhiên bạn đã học về Azure ACR tasks và cách build container trong Azure Cloud Shell và bạn quyết định thử thực hiện cách này. Vậy mục tiêu của bạn là sẽ tạo một container registry mới và sử dụng ACR tasks để build, push, và chạy container trong Azure.



Tạo một Container Registry mới



Tạo một Dockerfile



Build và chạy Container



Hoàn thành bài lab



Giai đoạn 1



Giai đoạn 2



Giai đoạn 3



Giai đoạn 4

Thực hành tạo Web App từ Docker Container trong Azure

Công ty của bạn muốn bạn triển khai một ứng dụng. Ứng dụng này được tối ưu hóa và chạy trong container, và bạn được bàn giao một Dockerfile. Công ty cũng yêu cầu tất cả các images phải được lưu trong Azure Container Registry. Và bạn đã tìm được một giải pháp tốt nhất, đó là host container trong Azure App Service.



Tạo một Container Registry mới



Tạo một image và Push vào ACR



Tạo một Web App từ Container Image



Hoàn thành bài lab



Giai đoạn 1



Giai đoạn 2



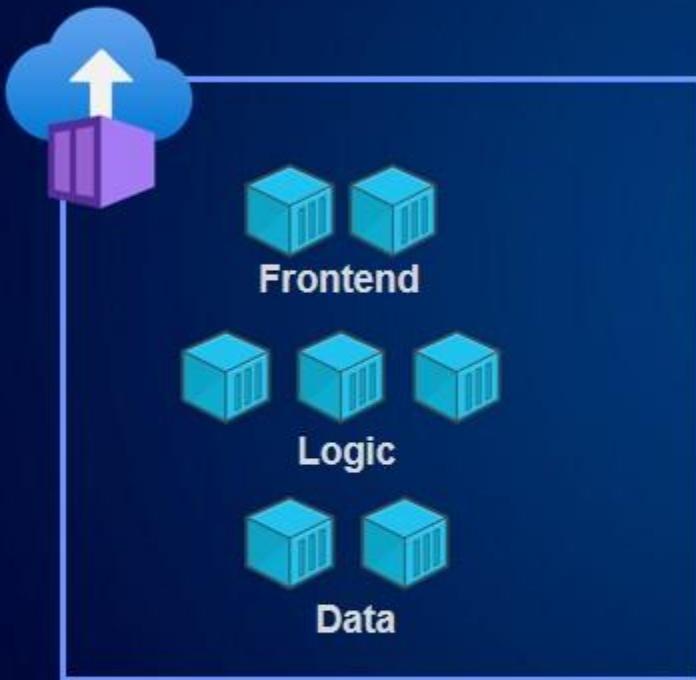
Giai đoạn 3



Giai đoạn 4

Sử dụng dịch vụ Azure Kubernetes

Traditional Azure Container Instances (ACI) Solution



Các giới hạn của ACI

➤ **Khả năng điều chỉnh quy mô (Scalability)**

Phải triển khai lại nếu có nhu cầu mở rộng quy mô (Scale up) một container group.

➤ **Quản lý**

Việc triển khai quản lý, điều phối các giải pháp container group có nhiều containers sẽ rất khó khăn và phức tạp, nếu không có một lớp quản lý điều phối (orchestration layer).

Các lợi ích của Kubernetes

- **Khả năng điều chỉnh quy mô (Scalability)**

Có thể dễ dàng điều chỉnh quy mô các containers để đáp ứng nhu cầu công việc.

- **Quản lý**

Cung cấp một lớp quản lý điều phối (orchestration layer) cho các clusters

Note: Cluster là một tập hợp có nhiều nodes.



Các lợi ích của Kubernetes

➤ AKS là gì?

Dịch vụ Azure Kubernetes (AKS) là một serverless platform cho Kubernetes. Nó cung cấp khả năng điều chỉnh quy mô (scalable) cho các giải pháp container.

Note: Serverless computing là một mô hình thực thi điện toán đám mây trong đó nhà cung cấp dịch vụ đám mây phân bổ tài nguyên điện toán theo yêu cầu. Bảo trì và vận hành các máy chủ cho khách hàng.

➤ Tại sao chúng ta sử dụng AKS?

AKS loại bỏ việc quản lý của một Kubernetes cluster bằng cách quản lý hầu hết việc triển khai và vận hành điều phối (orchestration).

Notes: Pod là đơn vị cơ bản và nhỏ nhất trong Kubernetes. Một pod có thể chứa một hoặc nhiều containers chia sẻ cùng một địa chỉ IP, lưu trữ dữ liệu (storage) và các tài nguyên khác như CPU, RAM.

	Kubernetes	AKS
Auto scaling Pods và Clusters		✓
Danh tính (Identity) và quản lý quyền truy cập Azure AD Integration		✓
Storage Volume (Lưu trữ dữ liệu) Azure Storage		✓
Networking Vnets, NSGs, và network policies		✓

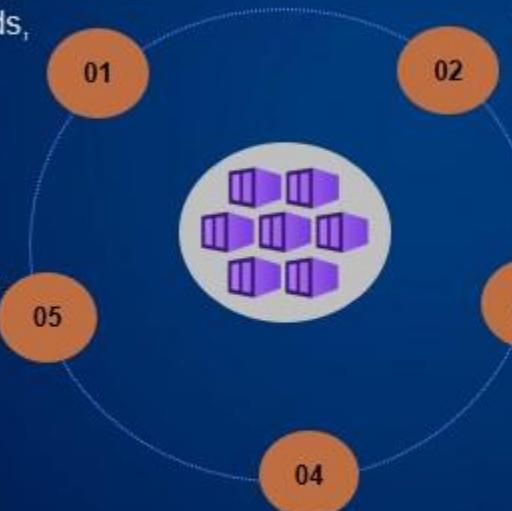
Các tính năng của dịch vụ Azure Kubernetes

Quản lý

Autoscaling cho các clusters và Horizontal scaling (tăng quy mô theo chiều ngang) cho các pods, Và Kubernetes verioning và upgrades.

Registry

Lưu trữ các container images trong Azure Container Registry, Docker Hub, hoặc các kho lưu trữ khác public/private repos. Hỗ trợ Docker images.



Danh tính (Identity)

Sử dụng Azure identity objects và Role-Based Access Control(RBAC) để cấp quyền truy cập vào AKS cluster. Cấp một identity cho một cluster để quản lý các tài nguyên.

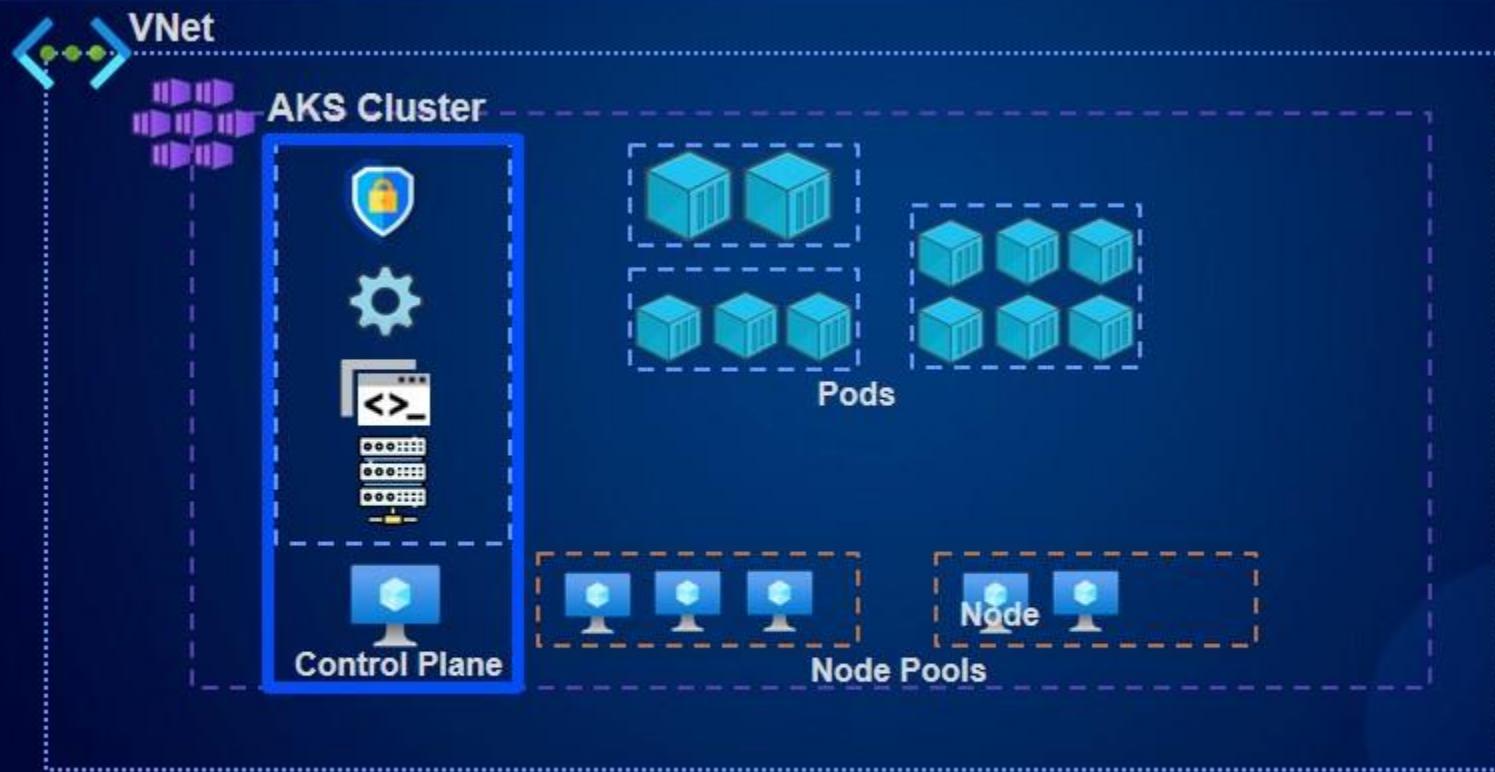
Networking

Tích hợp kết nối Vnet thông qua kubenet hoặc Container Network Interface (CNI). Định tuyến HTTP app. Sử dụng các quy tắc mạng (network policies) để quản lý traffic.

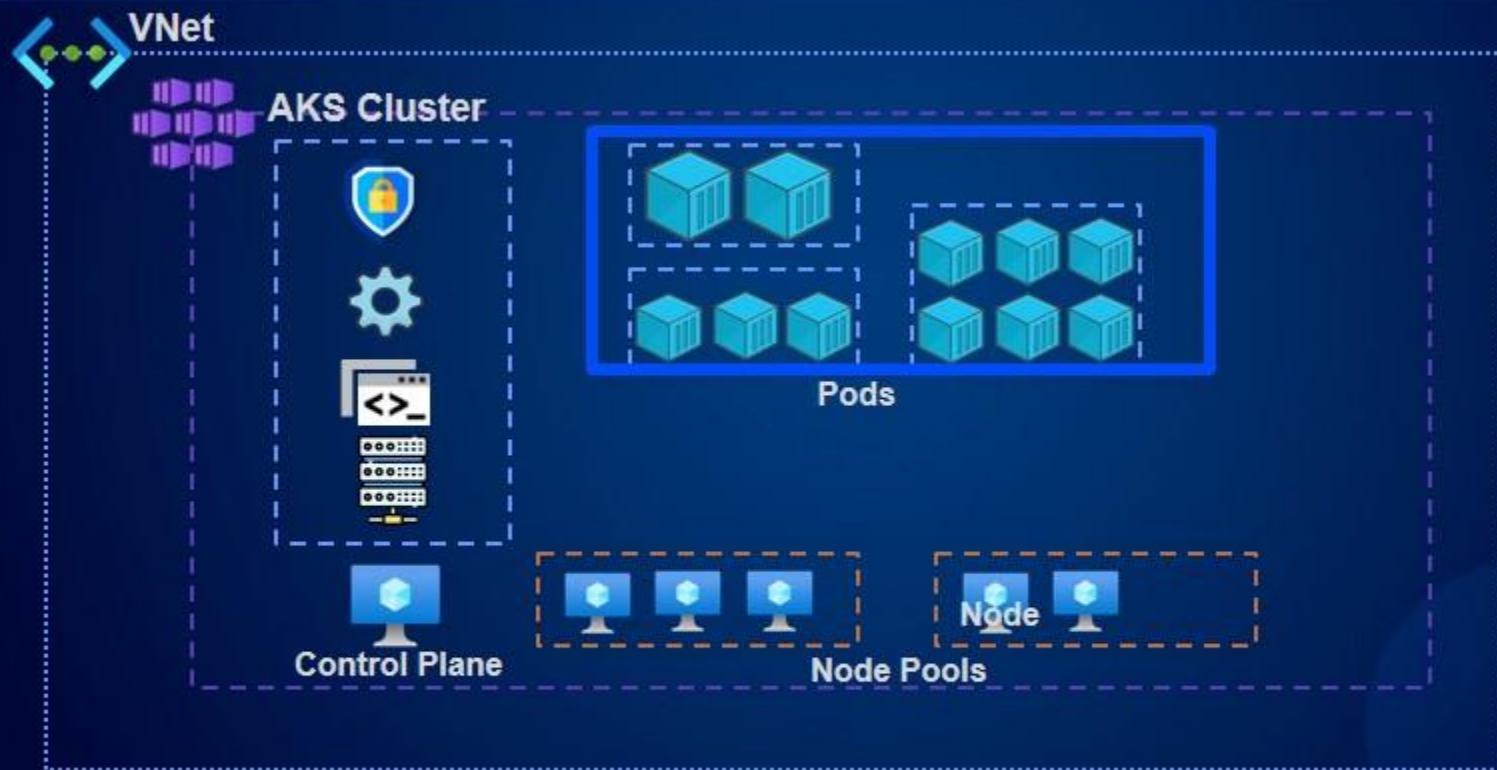
Lưu trữ dữ liệu (Storage)

Thực hiện triển khai các storage volumes cho việc lưu trữ dữ liệu, có thể là tĩnh (static) hoặc động (dynamic)

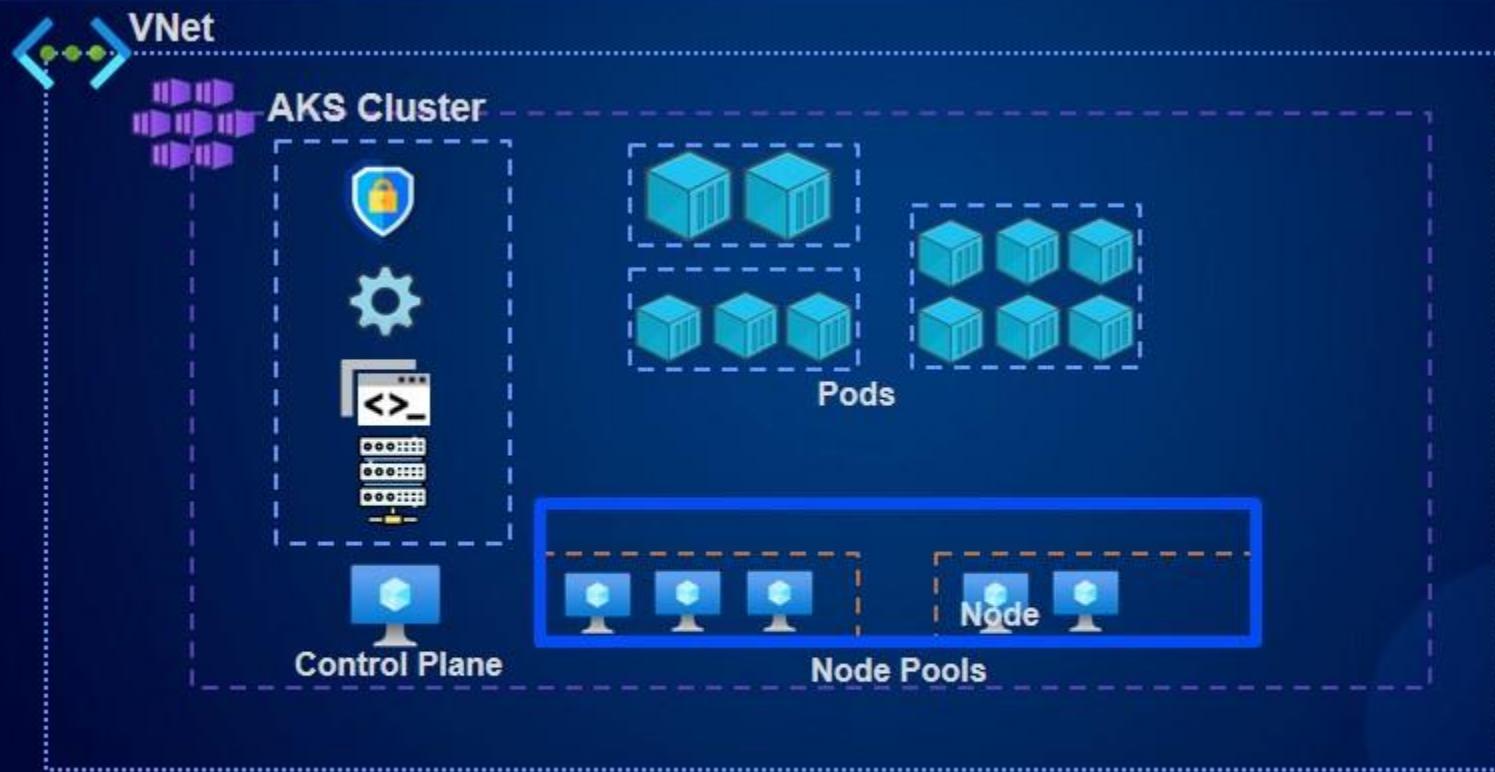
Kiến trúc của dịch vụ Azure Kubernetes



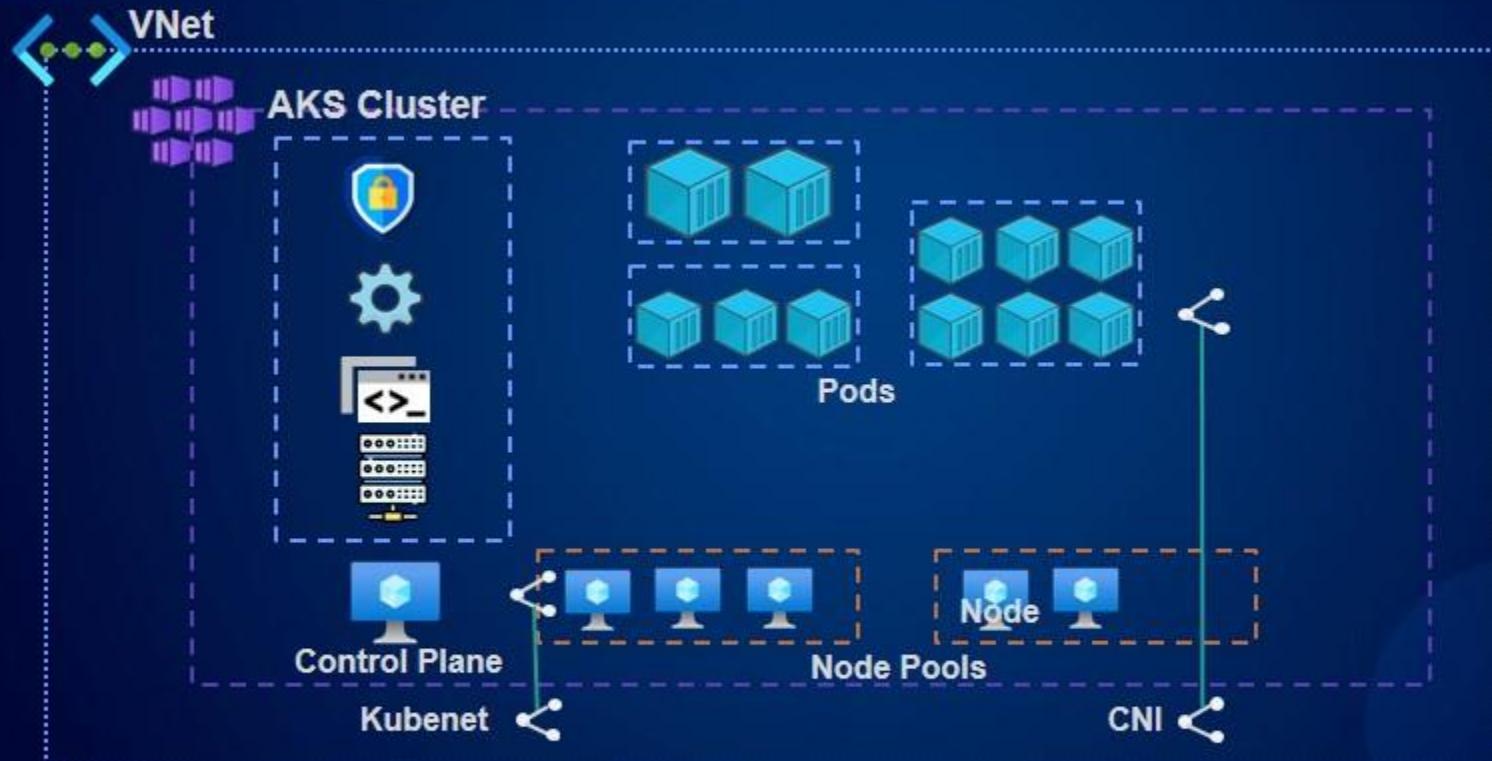
Kiến trúc của dịch vụ Azure Kubernetes



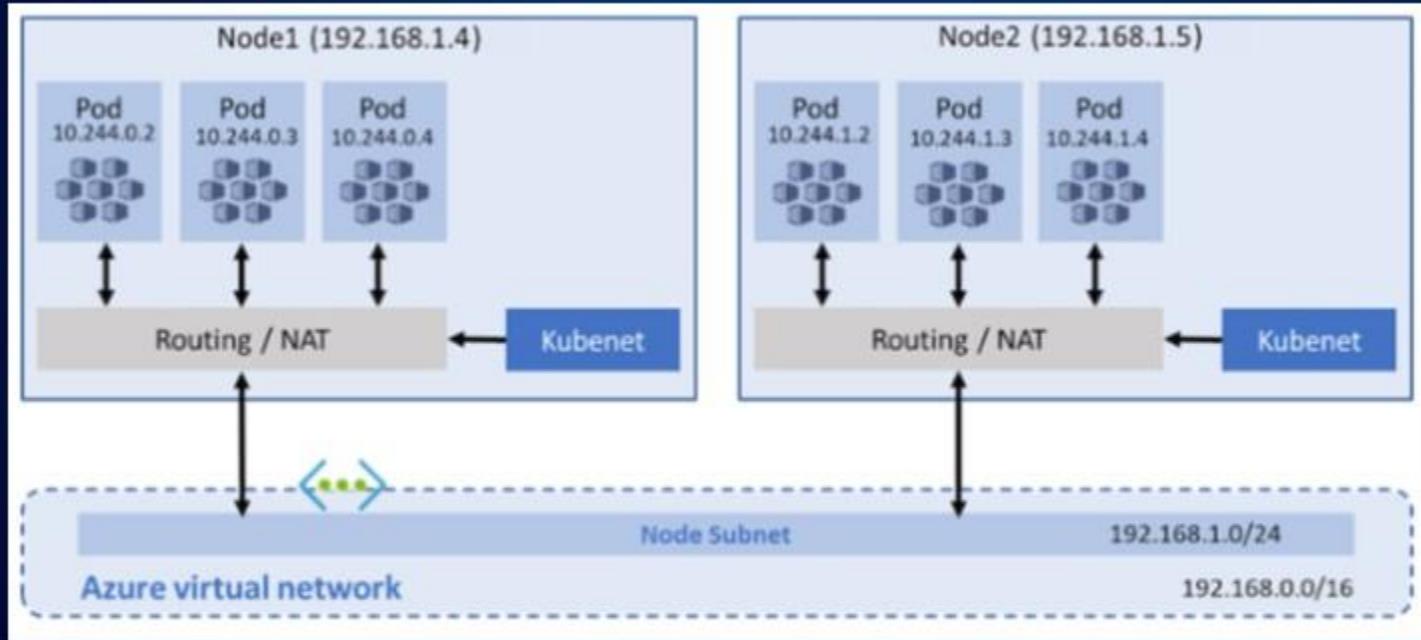
Kiến trúc của dịch vụ Azure Kubernetes



Kiến trúc của dịch vụ Azure Kubernetes



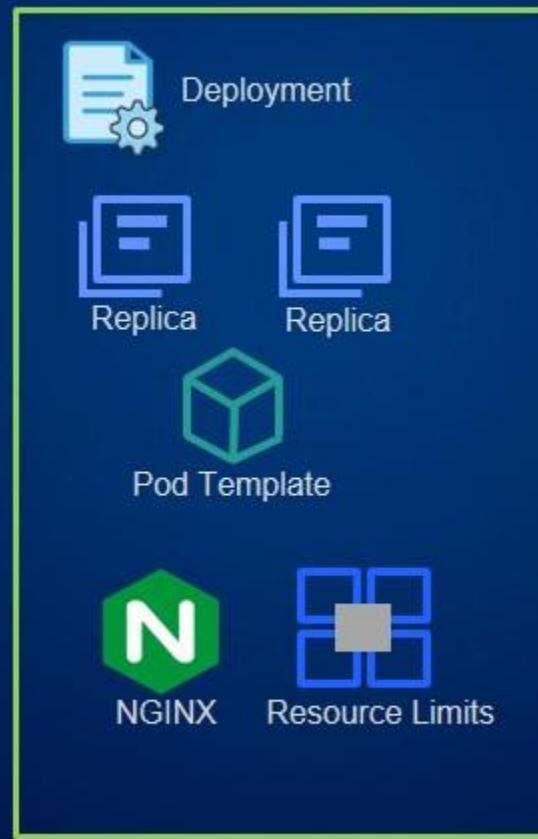
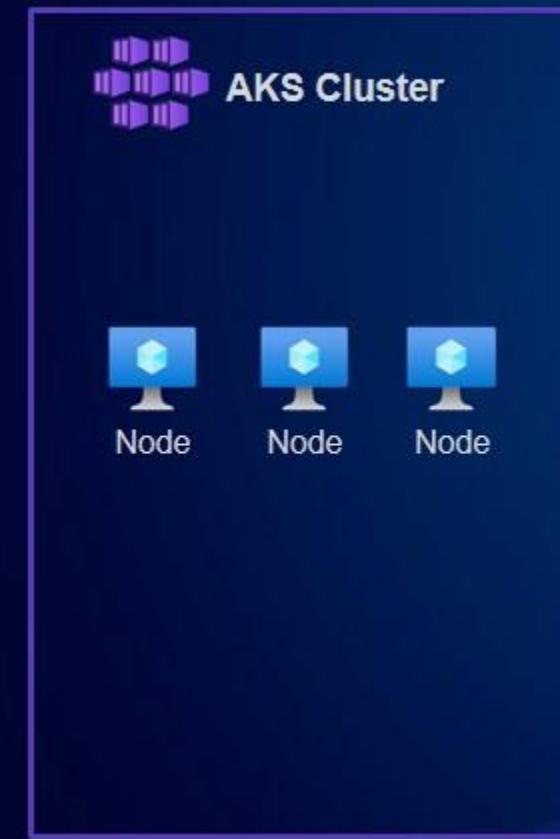
Kiến trúc của dịch vụ Azure Kubernetes



Thực hành triển khai và truy cập vào một ứng dụng trong một AKS Clusters

Trong bài thực hành này, chúng ta sẽ sử dụng Azure Command Line Interface (CLI) để tạo một AKS Cluster. Sau đó chúng ta sẽ sử dụng lệnh kubectl để triển khai một ứng dụng vào Cluster này, và cuối cùng chúng ta add thêm một dịch vụ kubernetes, để có thể truy cập vào ứng dụng từ ngoài internet.

Triển khai và truy cập vào một ứng dụng trong một AKS Clusters



Sử dụng Azure Monitor

Bài học bao gồm

Mô tả về Azure Monitor

Metrics (chỉ số) vs. Logs

Giải thích về Monitoring (giám sát)

Demo: Phân tích Metrics

Các điểm chính của bài học

Mô tả về Azure Monitor

Full-Stack Monitoring (Hệ thống giám sát toàn diện)

Cung cấp khả năng giám sát toàn diện từ đầu đến cuối cho các ứng dụng và cơ sở hạ tầng.

Thu thập và lưu trữ các metrics(chỉ số) và logs từ các tài nguyên được giám sát (Monitored resources)

- Monitor các tài nguyên Azure
- Monitor các tài nguyên on-premises
- Monitor platform services
- Monitor application code



Metrics (chỉ số) vs. Logs

Metrics

- Dữ liệu ngắn, dựa trên thời gian
- Được cập nhật thường xuyên
- Gần với thời gian thật
- Cảnh báo (alert) dựa trên các giá trị số liệu
- Trực quan thông qua Metrics Explorer

Logs

- Dữ liệu dài, dựa trên sự kiện
- Được cập nhật không liên tục
- Dạng tự do và/hoặc có cấu trúc
- Được lưu trữ trong Log Analytics Workspace
- Truy vấn bằng ngôn ngữ Kusto

vs

Giải thích về Monitoring (giám sát)



Các điểm chính của bài học

Metrics	Metrics được thu thập cho mỗi một tài nguyên. Làm thế nào để sử dụng metrics? <ul style="list-style-type: none">• Xem metrics trong Metrics Explorer• Truy vấn, lọc và phân tích trong Log Analytics• Cảnh báo (Alert) và thực hiện các hành động xử lý (take action)• Xuất (Export) và lưu trữ (Archive)
Logs	Mặc định logs không được thu thập trong Azure Làm thế nào để sử dụng logs? <ul style="list-style-type: none">• Truy vấn logs trong Log Analytics• Lưu trữ (Archive) logs• Chuyển (stream) logs tới bên thứ ba (third party)
Diagnostic Settings	Định nghĩa cách và nơi mà metrics và logs sẽ được lưu trữ cho mỗi một tài nguyên <ul style="list-style-type: none">• OS-level data• App-level data

Setup Alerts (cảnh báo) và Actions (hành động xử lý)

Bài học bao gồm

Mô tả về Azure Monitor Alerts

Action Group

Demo: Tạo một Alert

Các điểm chính của bài học

Mô tả về Azure Monitor Alerts

Azure Monitor Alerting

Các cảnh báo được kích hoạt dựa trên các signals (tín hiệu), các signals này sẽ nhắc bạn thực hiện các hành động chủ động (proactive actions) và giúp tự động hóa việc Monitoring (theo dõi) và chẩn đoán (diagnostics)



Singnal Types (Các loại tín hiệu)
Metric, activity (hoạt động), và log signals



Action Group (Nhóm hành động xử lý)
Các hành động xử lý (actions) sẽ diễn ra
khi một cảnh báo đã được kích hoạt.

! Alerts

Resource
(Tài nguyên)



Condition
(Điều kiện)

Signals

Logic

Actions



Action
Group

Action Group



Các điểm chính của bài học



Cấu hình Azure Monitors Logs

Bài học bao gồm

Mô tả về Azure Monitor Logs

Các thành phần của Log Analytics

Demo: Cấu hình Log Analytics

Các điểm chính của bài học

Mô tả về Azure Monitor Logs



Log Analytics

Một dịch vụ tổng hợp dữ liệu log trong một nơi duy nhất, nơi dữ liệu có thể được phân tích, được trực quan hóa, và được truy vấn.



Internal Data(Dữ liệu bên trong)

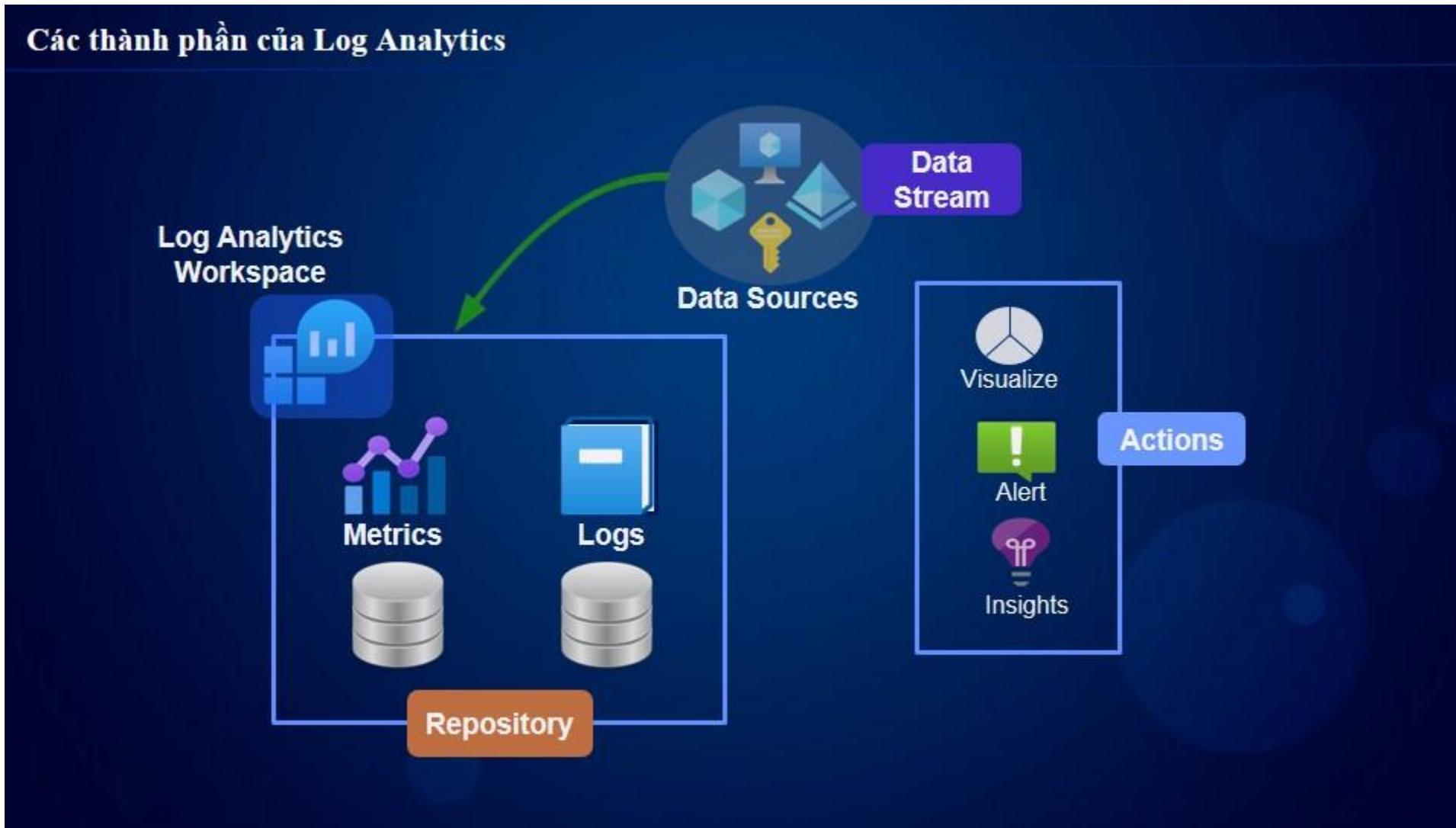
Các tài nguyên Azure, Azure AD tenant, và các subscriptions, và các tài nguyên on-premises.



External Data(Dữ liệu bên ngoài)

Các tài nguyên On-premises trong các hybrid environments (các môi trường lai)

Các thành phần của Log Analytics



Các điểm chính của bài học



Azure Monitor Logs

Internal Data(Dữ liệu bên trong)
Các tài nguyên Azure, Azure AD tenant, và các subscriptions, và các tài nguyên on-premises.

Log Analytics Agent

Một extension được cài đặt vào các tài nguyên để cho phép tập hợp dữ liệu từ xa vào workspace.

Tìm hiểu về Monitors Insights

Bài học bao gồm

Mô tả về Insights

VM và Network Insights

Container và Application Insights

Các điểm chính của bài học

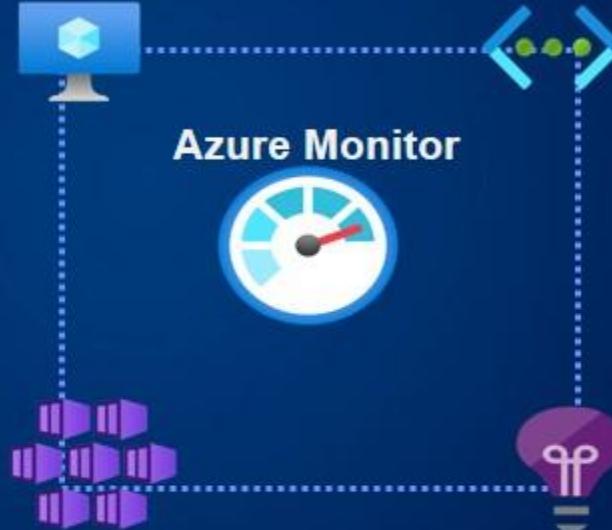
Mô tả về Insights

Service Monitoring

Các tính năng giám sát dành riêng cho dịch vụ được tích hợp trong Azure Monitor.

Bao gồm:

- VM insights
- Network Insights
- Container Insights
- Application Insights



VM và Network Insights



VM Insights

Dịch vụ monitoring cụ thể dành riêng cho các máy ảo VMs và Virtual machine scale sets (VMSS).

- Yêu cầu cần có Log Analytics workspace
- Yêu cầu cần có Log Analytics Agent (Được cài đặt khi được kết nối connected)
- Còn được gọi là Azure Monitor cho máy ảo

Network Insights

Dịch vụ monitoring cụ thể dành riêng cho các mạng ảo (Virtual network).

- Không cần phải cài đặt agent
- Làm việc song song với Network Watcher nếu được bật (enabled)
- Còn được gọi là Azure Monitor cho Networks

Container và Application Insights



Container Insights

Dịch vụ monitoring cụ thể dành riêng cho các containers hoặc AKS clusters.

- Yêu cầu cần có Log Analytics workspace
- Yêu cầu cần có Log Analytics Agent

Application Insights

Dịch vụ monitoring cụ thể dành riêng cho application code.

- App insights resource
- Instrumentation of App Code

Các điểm chính của bài học



VM Insights

Dịch vụ monitoring cụ thể dành riêng cho các máy ảo VMs và Virtual machine scale sets (VMSS).



Network Insights

Dịch vụ monitoring cụ thể dành riêng cho các mạng ảo (Virtual network).



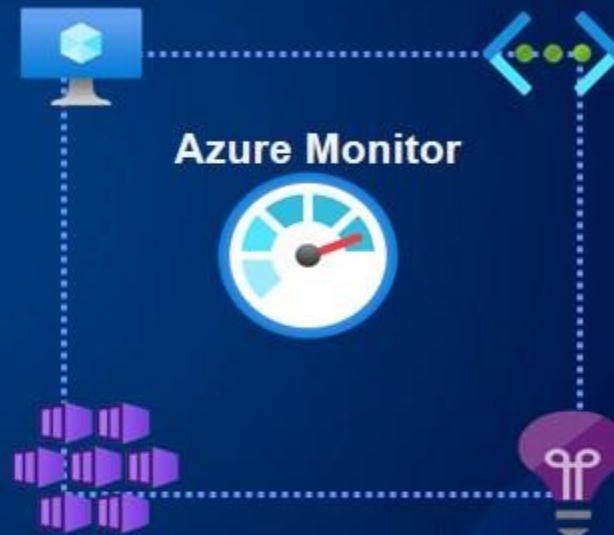
Container Insights

Dịch vụ monitoring cụ thể dành riêng cho các containers hoặc AKS clusters.



Application Insights

Dịch vụ monitoring cụ thể dành riêng cho application code.



Cấu hình Application Insights

Bài học bao gồm

Mô tả về Application Insights

Các tính năng của Application Insights

Kiến trúc các thành phần của Application Insights

Các điểm chính của bài học

Mô tả về Application Insights

Application Insights

Một giải pháp Monitoring toàn diện (full-stack) cho developers có thể sử dụng để monitor các applications.

- Hỗ trợ hỗ trợ cho nhiều loại ứng dụng khác nhau với App Insights
- Kho lưu trữ (Repository) cho events và metrics data
- Dữ liệu liên quan đến hiệu suất, lỗi, và các sự kiện khác từ ứng dụng được chuyển đến và lưu trữ trong một Application Insight resource



Các tính năng của Application Insights

Metrics

Live Metrics Stream cho metrics gần với thời gian thực và công cụ Metrics Explorer cho phép xem, phân tích các metrics thay đổi như thế nào theo thời gian.

Usage Analytics

Phân tích các user metrics từ client-side events (các sự kiện phía khách) như tương tác của người dùng user

Alerts

Việc cảnh báo (Alerting) dựa trên dữ liệu chỉ số (metrics) hoặc dữ liệu sự kiện (events) để thông báo cho các quản trị ứng dụng về các vấn đề có thể xảy ra hoặc đã xảy ra trong hệ thống.

Profiler

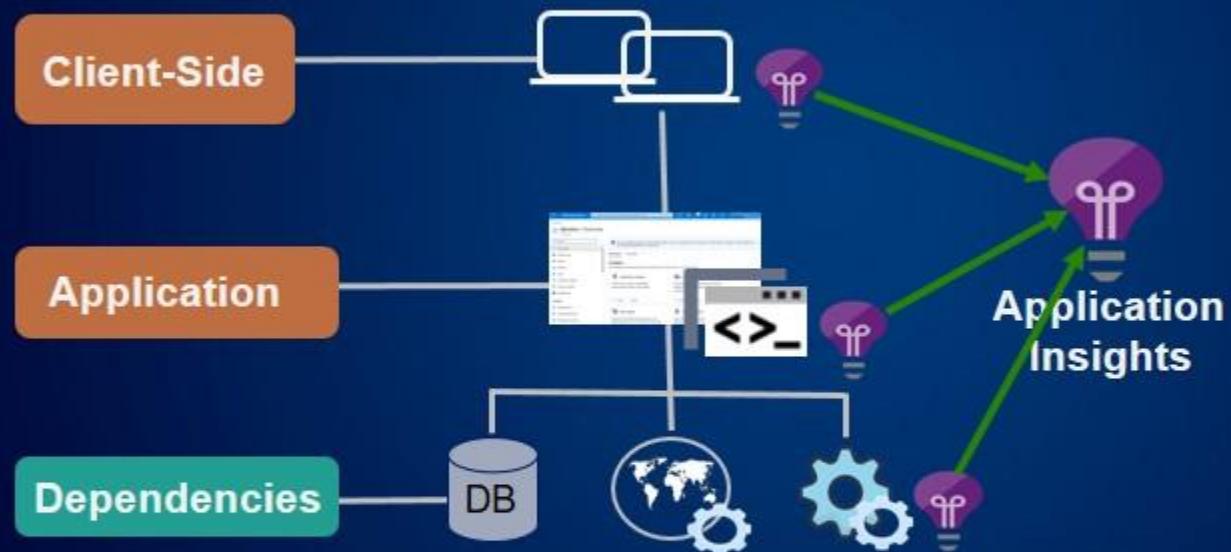
Xác định cách phân phối các yêu cầu (requests), như các thành phần trang(page) và hiệu suất (performance) của chúng



Application Map

Một bản đồ tổng quan về cấu trúc liên kết của các ứng dụng (applications) và các thành phần phụ thuộc (dependencies), được sử dụng để nhận biết các vấn đề phụ thuộc như các nút thắt cổ chai (bottlenecks) trong hệ thống.

Kiến trúc các thành phần của Application Insights



Các điểm chính của bài học



Runtime Instrumentation

Việc triển khai công cụ monitoring vào ứng dụng mà không đòi hỏi sự can thiệp trực tiếp vào code của ứng dụng thông qua việc thêm các gói (packages) hoặc source code.



Build-Time Instrumentation

Là quá trình triển khai công cụ monitoring vào ứng dụng đòi hỏi cần có sự can thiệp vào code của ứng dụng thông qua việc sử dụng một SDK (Software Development Kit) và triển khai các gói (packages) cho Application Insights trong quá trình build ứng dụng.



Instrumentation Key

"Instrumentation Key" được sử dụng để triển khai công cụ monitoring trong các ứng dụng. Được lưu trữ trong Application Insights Resource.



Sử dụng Network Watcher

Bài học bao gồm

Mô tả về Azure Network Watcher

Demo: Sử dụng Network Watcher

Các điểm chính của bài học

Mô tả về Azure Network Watcher

Azure Network Watcher

Azure Network Watcher là một dịch vụ bao gồm các công cụ mạng (Networking Tools) cho việc giám sát (monitoring) và chẩn đoán (diagnostics).

- Tổng quan về các cấu trúc mạng
- Giám sát (monitor) kết nối mạng trong Azure
- Giám sát (monitor) kết nối mạng trong các mạng lai (hybrid networks)
- Xử lý khắc phục (Troubleshoot) các sự cố kết nối
- Giải pháp xử lý khắc phục các sự cố kết nối cho mạng lai (hybrid network)
- Có thể bật Enable Network Watcher cho mỗi một region bên trong một subscription



Các điểm chính của bài học

10.0.0.0

Topology (Cấu trúc liên kết mạng)

Xem một biểu đồ của các tài nguyên trong một mạng ảo Vnet.



Connection Monitor

Giám sát (Monitor) kết nối giữa các tài nguyên Azure trong hệ thống mạng



Network Performance Monitor

Giám sát (Monitor) hiệu xuất mạng và tình trạng kết nối giữa các tài nguyên, data centers, và/hoặc ExpressRoute từ một vị trí trung tâm

10.0.0.0

IP Flow Verify

Kiểm thử (test) allowed inbound hoặc denied outbound traffic cho các VMs



Next Hop

Xác định các traffic mạng đi từ VM tới điểm đến (DEST)



Effective Security Rules

Xác định các quy tắc security hiệu quả cho một card mạng (NIC)



Packet Capture

Bắt các gói tin (packets) đến và/hoặc từ một VM cho việc phân tích xử lý lỗi mạng

Tìm hiểu
Khắc Phục Thảm Họa
(Disaster Recovery)

Bài học bao gồm

Mô tả về khắc phục thảm họa

RPO vs. RTO

Các phương pháp khắc phục thảm họa

Mô tả về khắc phục thảm họa

Khắc phục thảm họa (Disaster Recovery) là gì?

Là quá trình (process) trong phục hồi từ một sự cố hay thảm họa, VD như data center mất điện. Mọi doanh nghiệp đều cần duy trì hoạt động kinh doanh liên tục và kế hoạch khắc phục thảm họa (BCDR).

- Đánh giá các rủi ro
- Khôi phục sau thảm họa
- Định nghĩa và chọn các phương pháp triển khai các kỹ thuật sao lưu (backup) dữ liệu
- Kiểm thử test khắc phục thảm họa



RPO vs. RTO



Các điểm chính của bài học

Các Phương Pháp Khắc phục thảm họa (Disaster Recovery Methods)

Backup

Một bản copy backup các dữ liệu quan trọng

Cold Site

Cần chuẩn bị trước một bản copy backup của hệ thống cơ sở hạ tầng quan trọng của công ty

Hot Site

Cần chuẩn bị trước một hệ thống copy backup của hệ thống cơ sở hạ tầng quan trọng của công ty, hệ thống này phải luôn phải sẵn sàng hoán đổi cho hệ thống đang chạy, là môi trường production khi có sự cố xảy ra

Cấu hình Azure Backup

Bài học bao gồm

Mô tả về Azure Backup

Các thành phần của Azure Backup

Demo: Sử dụng Azure Backup

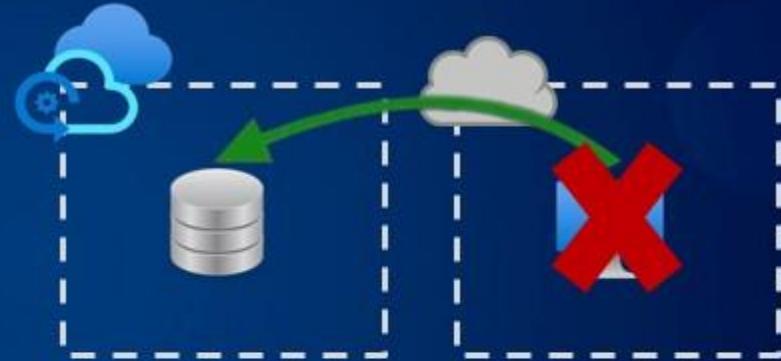
Các điểm chính của bài học

Mô tả về Azure Backup

Backup là một dịch vụ (Service) trong Azure

Azure Backup là một dịch vụ được quản lý bởi Azure, sử dụng cho việc sao lưu và khôi phục dữ liệu.

Yêu cầu cần có một Azure Recovery Services vault.



Mô tả về Azure Backup

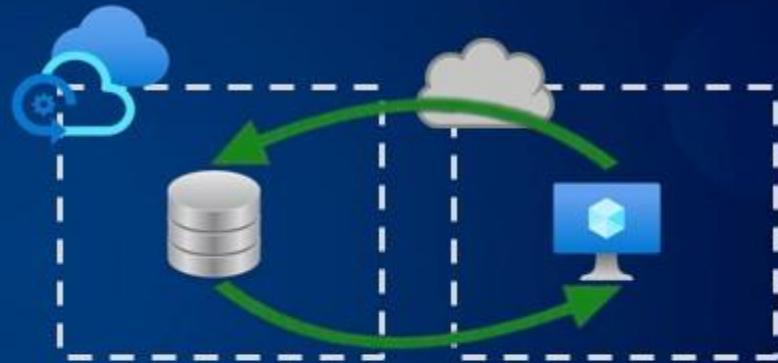
Backup là một dịch vụ (Service) trong Azure

Azure Backup là một dịch vụ được quản lý bởi Azure, sử dụng cho việc sao lưu và khôi phục dữ liệu.

Yêu cầu cần có một Azure Recovery Services vault.

Hỗ trợ việc backup dữ liệu cho:

- Azure virtual machines
- On-premises machines
- SQL Server workloads
- SAP HANA workloads



Các thành phần của Azure Backup



Các điểm chính của bài học

Hỗ trợ việc backup dữ liệu cho:

- Azure virtual machines
- On-premises machines
- SQL Server workloads
- SAP HANA workloads

Recovery Services Vault

Dịch vụ quản lý lưu trữ cho tất cả các backup data

Azure Backup

Dịch vụ backup được quản lý trên đám mây để cấu hình tần suất (frequency) và lưu giữ (retention) backup data.

Thực hành khôi phục (restore) File Share từ Azure Backup tới một Storage Account

- Trong bài thực hành này, công ty của bạn cần khôi phục một số dữ liệu từ một file share, và họ không muốn ghi đè lên các dữ liệu data hiện có.
- Bạn được giao công việc là copy dữ liệu tới một storage account khác, và sử dụng storage account này như là nơi để khôi phục dữ liệu.
- Bạn sử dụng một Recovery Services Vault để khôi phục dữ liệu tới một storage account khác.

✓ **Chúng ta cần vào đường link :**

https://raw.githubusercontent.com/phuongluuho/Azure104/main/deployment_restorefileshare.json
Sau đó sử dụng ARM Templates.

• **Để tạo ra một môi trường cho bài thực hành gồm:**

01 máy ảo (VMs), 01 Storage account & File Share, 01 Recovery Services vaults ,
01 mạng ảo Virtual network và 01 NSG, 01 card mạng ảo, 01 Public IP.



Tạo một Storage Account mới



Tạo một Backup cho các files trong File Share của Storage Account từ Recovery Services vault



Thực hiện việc khôi phục dữ liệu



Hoàn thành bài lab



Giai đoạn 1



Giai đoạn 2



Giai đoạn 3



Giai đoạn 4

Azure Site Recovery

Bài học bao gồm

Mô tả về Azure Site Recovery

Các thành phần của Azure Site Recovery

Demo: Cấu hình Site-to-Site Recovery

Các điểm chính của bài học

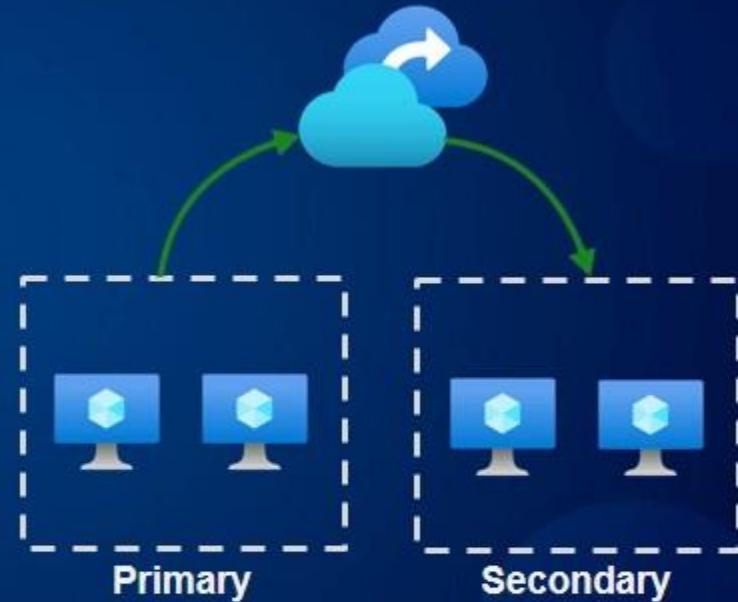
Mô tả về Azure Site Recovery

Giải pháp Khắc Phục Thảm Họa (Disaster Recovery Solution)

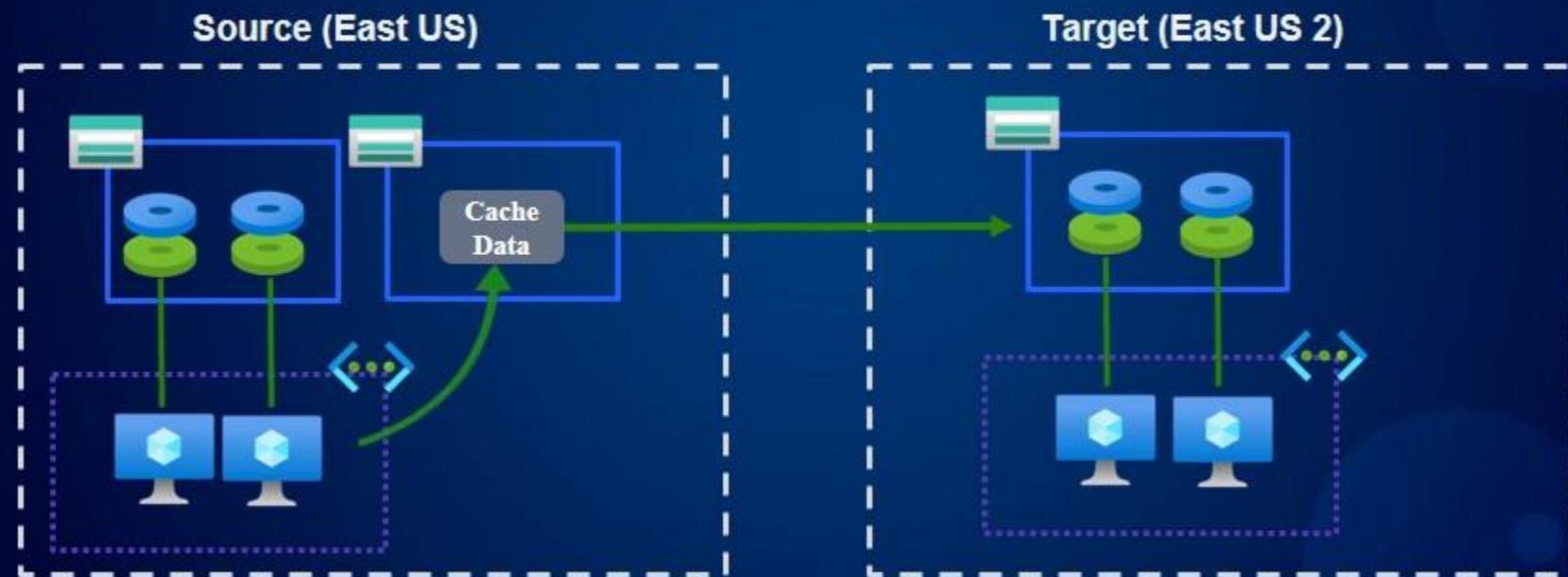
Azure Site Recovery service cung cấp một giải pháp cho tự động hóa việc khắc phục thảm họa.

Yêu cầu cần có một Azure Recovery Services vault.

- Giữa các zone (Cross-zone)
- Giữa các region (Cross-region)



Các thành phần của Azure Site Recovery



Các điểm chính của bài học



Replicated Items

Sử dụng Azure Site Recovery để sao chép hay đồng bộ (replication) máy ảo VMs Site-to-Site



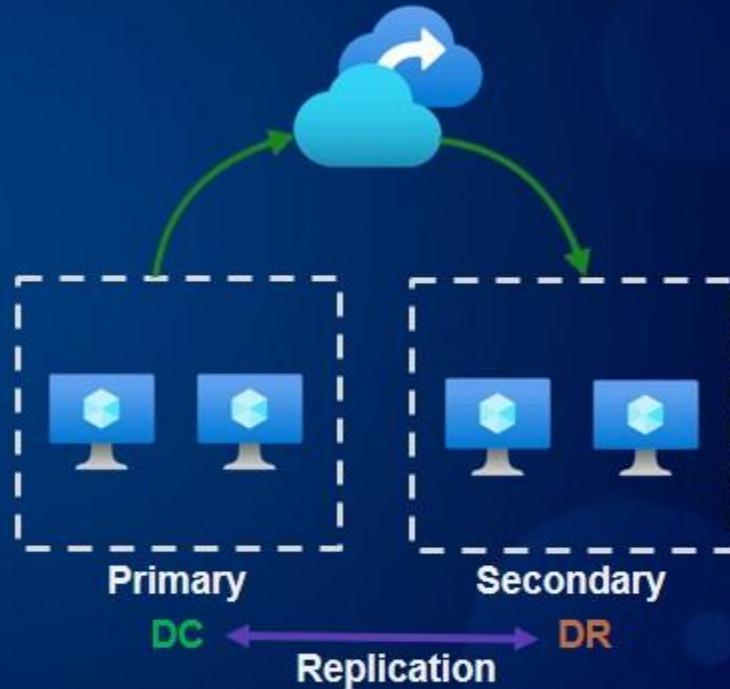
Replication policy

Khả năng điều chỉnh tần suất(Frequency) đồng bộ hóa sao chép của các snapshots của máy ảo, và cấu hình trong bao lâu snapshots sẽ được giữ lại trước khi bị xóa. Có thể lựa chọn giữ lại dữ liệu một cách nhất quán cùng với trạng thái của ứng dụng, hoặc theo trạng thái của các snapshots cho đến khi xảy ra sự cố thảm họa



Recovery Plan

Tự động hóa và chạy các sự kiện test failover, một công cụ giúp tổ chức xây dựng kịch bản phục hồi sau thảm họa.



Backup Reports

Bài học bao gồm

Mô tả về Backup Reports

Các thành phần của Backup Reports

Demo: Cấu hình Backup Reports

Các điểm chính của bài học

Mô tả về Backup Reports

Backup Reports

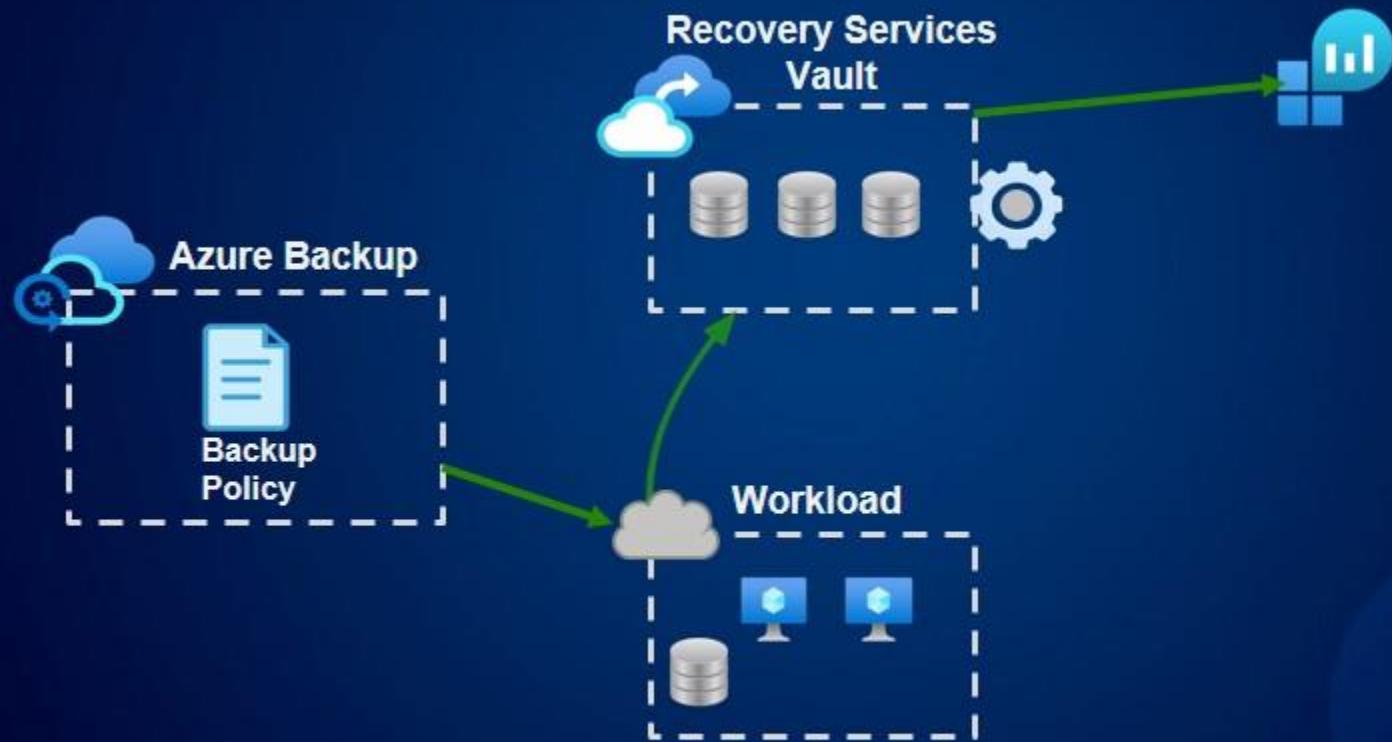
Cung cấp thông tin chi tiết về các bản hoạt động của Azure Backup và các thông tin chi tiết đó có thể được sử dụng để có các thông tin cho các mục đích công việc như:

- Các dự báo về tình trạng sử dụng dung lượng lưu trữ của các bản backups
- Kiểm tra và đánh giá các sự kiện (events) liên quan đến việc backup và khôi phục (restore) dữ liệu

Sử dụng Log Analytics như là một logging Service để lưu trữ các logs.



Các thành phần của Azure Backup



Các thành phần của Azure Backup

- Xem backup policies
- Xem backup jobs
- Xem backup items
- Xem Backup Summary



Cách tham gia thi chứng chỉ AZ 104

- **Hình thức thi:**

- **Offline:** Đến trực tiếp trung tâm khảo thí của Pearson VUE tại TP Hà Nội hay Sài Gòn
 - * Lệ phí thi tại Việt Nam khoảng 80\$, tại Hoa Kỳ khoảng 165\$
 - * Bạn nên hỏi các bạn nhân viên tại trung tâm khảo thí Pearson VUE để hỏi mua Voucher do có thể được giảm giá lên đến 50%, hoặc có thể cho phép thi lại miễn phí lần 2 trong trường hợp bạn thi trượt lần đầu.
 - Ngoài ra nếu bạn là sinh viên cũng sẽ có thể được giảm giá thi.
- **Online:** Thi online tại nhà trên chính máy tính của bạn lệ phí khoảng 165\$, và bạn cần đăng ký thi trước 24h. Các bạn có thể click vào đường Link trong phần tài nguyên để đăng ký thi.
- Sau khi các bạn làm bài thi xong thì sẽ thấy kết quả thi hiện lên trên màn hình, ngay sau khi nhấn nút Submit.

Azure Roadmap

