Active Directory

A diagram of a group diagram

Description automatically generated

I. Khái niệm

+ Là kiến trúc đặc quyền của Microsoft

+ Là một hệ thống được chuẩn hóa với khả năng quản trị tập trung hoàn hảo về người dùng cũng như các nguồn tài nguyên trong một hệ thống mạng

II. Tính năng

+ Centralized Data Store: Lưu trữ dữ liệu tập trung: Dữ liệu được lưu tập trung => dễ truy cập ở mọi thời gian, địa điểm => nâng cao quản trị

+ Scalability: Linh hoạt với nhu cầu: AD cung ứng linh hoạt giải pháp quản trị khác nhau cho từng nhu cầu cụ thể trên nền hạ tầng xác định của các doanh nghiệp

+ Extensibility: Cơ sở dữ liệu mở rộng được

+ Manageability – Khả năng quản trị linh hoạt, dễ dàng: AD tổ chức theo cơ chế của Directory Service dưới mô hình Directory => Nhìn tổng quan

+ Integration with DNS: các service của AD chỉ hoạt động được khi dịch vụ DNS được cài đặt. Nhiệm vụ DNS trong AD: dẫn đường, phân giải các Active Directory Domain Controller trong hệ thống mạng, multi Domain,…

+ Client Configuration Management: cung cấp quản trị các cấu hình phía client

+ Policy-based administration:

+ Replication of information (Sao chép thông tin): AD có khả năng đồng bộ dữ liệu thông tin giữa các domain

+ Flexible, secure authentication and authorization: AD cung cấp nhiều cơ chế authentication: Kerberos, Secure Socket Layer, Transport Layer Security => bảo mật thông tin user khi xác thực truy xuất tài nguyên

+ Security integration:

+ Directory-enable applications and infrastructure

+ Interoperability with other directory services:

* AD được xây dựng trên giao thức directory service chuẩn gồm 2 giao thức: Lightweight Directory Access Protocol (LDAP) và Name Service Provider Interface (NSPI) => tương thích với các dịch vụ khác được xây trên directory service thông qua 2 giao thức này
* LDAP: giao thức directory chuẩn
* NSPI: hộ trợ bởi AD => Đảm bảo, nâng cao tương thích với Directory của Exchange

+ Signed and encrypted LDAP traffic: Là công cụ AD trong window server sẽ tự động xác thực và mã hóa thông tin, dữ liệu truyền tải trên giao thức LDAP => Đảm bảo thông tin được gửi từ nguồn chính thống

**III. Kiến trúc**

1. Active Directory Objects:

A computer icons on a white background

Description automatically generated

\* object đặc biệt container: gồm nhiều object khác

2. Active Directory Schema:

A diagram of a computer class definition

Description automatically generated

\* Trong AD, database lưu trữ là AD Schema, Schema định nghĩa các đối tượng lưu trữ trong AD

+ Schema là một danh sách các định nghĩa xác định các đối tượng (object) và các loại thông tin về đối tượng lưu trữ trong AD

+ Schema cũng được lưu trữ như 1 object

\* Schema được định nghĩa gồm 2 loại đối tượng (object): Schema Class Object và Schema Attribute Objects

- Schema Class: Có chức năng như 1 template cho việc tạo mới các AD. Mỗi Schema Class là 1 tập hợp các thuộc tính của đối tượng (Schema Attribute Object).

+ Khi tạo 1 đối tượng thuộc về 1 loại Schema Class => Schema Attribute lưu trữ các thuộc tính đối tượng đó tương ứng với loại Schema Class của đối tượng.

- Schema Attribute: Định nghĩa các Schema Class tương ứng với nó. Mỗi thuộc tính chỉ được định nghĩa 1 lần trong AD và có thể thuộc nhiều Schema Class theo quan hệ 1 nhiều (1-n)

+ Schema Class + Schema Attribute được đóng gói chung với AD. Schema của AD mở ra một khả năng phát triển mở rộng Schema Class trên các Attribute có sẵn hoặc tạo mới các Attribute Schema.

3. Active Directory Components:

\* Logical Structure:

+ Trong AD, tài nguyên tổ chức theo Logical Structure được ánh xạ thông qua mô hình domains, OUs, trees và forest.

* Domain:

A diagram of a domain

Description automatically generated

+ Cốt lõi của kiến trúc AD

+ Domain lưu trữ thông tin của các đối tượng nằm trong domain đó

+ AD được tạo bởi 1 hoặc nhiều Domain, 1 domain có thể triển khai trên nhiều physical structure

+ Access vào domain được quản trị thông qua Access Control List (ACLs), quyền truy xuất domain trên từng đối tượng

* OUs:

A diagram of a computer network

Description automatically generated

+ Là 1 container được dùng để tổ chức các đối tượng trong 1 domain thành các nhóm quản trị Logical.

+ OUs cung cấp các tác vụ quản trị hệ thống: quản trị user và resources (scope đối tượng nhỏ nhất mà có thể ủy quyền xác thực quản trị)

+ Gồm nhiều đối tượng: user accounts, group, computers cà các OUs khác tạo nên các cây OUs trong cùng một domain

+ Các cây OUs trong 1 domain độc lập với kiến trúc các cây OUs thuộc các domain khác

* Trees:

A diagram of a company's company's company

Description automatically generated

+ Là 1 nhóm các domain được tổ chức theo cấu trúc hình cây với mô hình parent-child ánh xạ từ tổ chức, doanh nghiệp

+ Một domain có 1 hoặc nhiều child domain, 1 child domain chỉ có 1 parent-domain

* Forest:

A diagram of a tree

Description automatically generated

+ Là thuật ngữ định nghĩa 1 mô hình tổ chức của AD

+ 1 forest gồm nhiều domain trees có quan hệ với nhau, các domain trees trong forest độc lập với nhau về tổ chức (quan hệ giữa các domain trees là Trust 2 chiều như các partners với nhau)

+ 1 forest phải đảm bảo các thuộc tính sau:

- Toàn bộ Domain trong forest phải có 1 schema chia sẻ chung

- Các domain trong forest phải có 1 global catalog chia sẻ chung

- Các domain trong forest phải có mối quan hệ trust 2 chiều với nhau

- Các tree trong 1 forest phải có cấu trúc tên (domain name) khác nhau

- Các domain trong forest hoạt động độc lập với nhau, nhưng hoạt động của forest là hoạt động của toàn bộ hệ thống tổ chức doanh nghiệp

\* Physical Structure

+ Site:

- Là thuật ngữ được dùng khi nói về vị trí địa lý của các domain trong hệ thống

- Khi hệ thống các domain được phân tán ở những vị trí địa lý, những nơi khác nhau và có quan hệ với nhau thì những nơi đặt chính các domain này là các site

A diagram of a city

Description automatically generated

- Như hình trên có 3 site: Chicago, St.Louis, Detroit

+ Domain Controller (DC):

* Là 1 máy tính/server chuyên dụng được setup Windows Server và Lưu trữ bản sao của Domain Directory (local domain database)
* 1 domain có thể nhiều domain controller, mỗi domain controller đều có bản sao dữ liệu cho Domain Directory. Domain Controller chịu trách nhiệm chứng thực cho users và chịu trách nhiệm đảm bảo các chính sách bảo mật được thực thi