TỔNG KẾT KIẾN THỨC ACTIVE DIRECTORY (AD)

1. Offline Domain Join

Offline Domain Join là kỹ thuật thêm máy tính vào domain mà không cần kết nối trực tiếp với Domain Controller. Thường được dùng trong các tình huống máy client ở xa, không thể liên lạc trực tiếp với DC khi khởi động lần đầu.

2. Không xóa máy tính khỏi domain

Việc xóa trực tiếp máy tính khỏi domain có thể gây mất thông tin quan trọng như GPO link, quyền truy cập tài nguyên, hoặc làm rối cấu trúc OU. Thay vào đó, nên disable hoặc di chuyển vào OU 'Retired' để quản lý tốt hơn.

3. Thêm máy tính vào domain

Có thể thực hiện bằng giao diện GUI hoặc dòng lệnh như `netdom join`. Quá trình yêu cầu thông tin domain, tài khoản có quyền join và sẽ khởi động lại máy sau khi join thành công.

4. Tổ chức tài khoản AD

Tài khoản nên được phân loại theo OU như theo phòng ban, chức năng. Việc tổ chức hợp lý giúp áp dụng GPO chính xác, phân quyền dễ dàng và dễ kiểm soát bảo mật.

5. Special Identities trong Windows

Special Identities là các nhóm hệ thống như Authenticated Users, Everyone, INTERACTIVE... Không thể chỉnh sửa thành viên, nhưng rất quan trọng trong phân quyền GPO, File Share, và các quyền truy cập hệ thống.

6. Container Computers trong AD

Container mặc định chứa các đối tượng máy tính khi join domain mà không được chỉ định OU cụ thể. Có thể dùng lệnh `redircmp` để chuyển hướng máy tính mới vào OU tùy chỉnh thay vì container mặc định.

7. Join Domain thủ công

Người quản trị có thể join domain bằng tay qua `System Properties` hoặc dùng lệnh `netdom`. Cần xác thực bởi user có quyền join domain (thường là Domain Admin hoặc người được ủy quyền).

8. Tích hợp DNS trong AD

Active Directory yêu cầu DNS để phân giải tên dịch vụ như _ldap._tcp.dc._msdcs.domain. DNS có thể tích hợp với AD để tự động tạo các bản ghi SRV khi tạo thêm DC hoặc domain.

9. OU – Organizational Units

OU giúp tổ chức đối tượng như user, computer theo logic quản trị. GPO được áp dụng ở OU giúp chia nhỏ phạm vi ảnh hưởng. Không nên lạm dụng OU lồng nhau quá sâu vì khó quản lý kế thừa GPO.

10. Group Policy Object (GPO)

GPO giúp quản lý chính sách hệ thống: cài đặt phần mềm, policy bảo mật, script đăng nhập... GPO được áp vào Site, Domain hoặc OU và có thể kế thừa hoặc bị chặn (block inheritance).

11. Replication trong AD

Active Directory dùng mô hình replication đa chủ (multi-master). Các DC đồng bộ thông tin thông qua các liên kết replication, thường mỗi 15 phút/lần trong cùng site. Có thể kiểm tra bằng lệnh `repadmin /replsummary`.

12. Domain Controller là gì

DC là máy chủ lưu trữ AD DS, chịu trách nhiệm xác thực user, quản lý thông tin domain. Trong tổ chức nên có ít nhất 2 DC để đảm bảo dự phòng và cân bằng tải.

13. Cấu trúc logical & physical của AD

Logical gồm: Forest, Domain, OU. Physical gồm: Site, Subnet và replication link. Cấu trúc logic phục vụ quản trị, trong khi cấu trúc vật lý phục vụ hiệu năng và replication.

14. Account Management trong AD

Gồm tạo, đổi mật khẩu, disable, di chuyển user. Có thể dùng giao diện ADUC hoặc lệnh PowerShell (`New-ADUser`, `Set-ADUser`, `Move-ADObject`...) để thao tác hàng loạt.