Program: MCA & IBCA

Course Code: MCAS9250

Course Name: N/w Mgt. & System Adm.

Semester: Vth & IX

Windows Domain

- A Domain is a specific NAME given to a LAN that includes one or more Domain Controllers (Servers).
- The advantage is that you have a dedicated server to log/track all users and shares via Active Directory and you can also use this server for other things such as a SQL server and/or SBS etc...
- Advantages of Domain One location for all user accounts, groups and computers. Passwords are same for all computers. Easier and quicker to maintain. Scales easier if you add more users and computers. Very high Security in sharing and personal settings

Windows Domain

- Disadvantages of Domain Requires a windows server. Complex to set up.

- The disadvantage to this is the cost and maintenance required to keep this configuration running.

Domain-Based Networks

- Domain-based networks are vastly more complex to setup for the average user in the short-term, partly due to the more highly technical-nature inherent to server role promotion, but may ultimately save in administrative time over the long-run if the users manage to learn how to make more effective use of Active Directory's robust management features.
- Domain Networks can be created and managed by promoting any Workgroup Server to the role of a Domain Controller or Primary Domain Controller (PDC).
- Servers designated as Primary Domain Controllers contain a more thorough and complex set of security and administrative properties which the simplified Workgroup Server does not have.

Domain-Based Networks

- Each Domain must have at least one designated PDC Server within its Forest for centralized user account management through the AD.
- Domains share a hierarchal directory of databases, security policies, and common security relationships with other sub-Domains. A PDC provides access to a centralized user account and workgroup account policy as maintained by the Domain Administrator predominantly from the AD Server itself.
- Domains use a hierarchy of parent-child relationships within a Domain Forest, AD Domains are generally recommended and most effectively used by larger organizations where collaborative computing between numerous workgroups must span multiple departmental servers with common sets of relational security policies in place.

Domains and Workgroups

- Domains and workgroups are logical groups of computers that are created for the purposes of administration and resource access. A Windows NT 4 system can be configured as either a member of a workgroup or a member of a domain.
- Workgroups are used in small networks of usually not more than 10 computers. In a workgroup scenario, a dedicated, or centralized, network server is nonexistent, and each system in the workgroup can offer services to and use services from other systems in the workgroup.
- Security in a workgroup model is handled by each system; that is, each computer has its own list of users who can access the system.

Domains and Workgroups

- There is no centralized database of user accounts, which results in a situation that can lead to a variety of administrative headaches.
- For example, changing user passwords and making sure that they are changed on each system in the workgroup can be an administrative nightmare.
- Domains are very different from workgroups.
- In a Windows environment, a domain model is a network model that uses a centralized approach to resource management, meaning that computers within the domain can access data and network services from a central location.

Domains and Workgroups

- A Windows NT server that is configured in the domain model can be set up to perform three roles on the network:
- **Primary domain controller (PDC)**-The PDC is the main server and is responsible for the majority of server-related tasks on the network, including authentication and managing the network user account information. A Windows NT domain can have only a single PDC, and every effort should be made to ensure that it is running at all times.
- **Backup domain controller (BDC)**-As a company grows, its reliance on a single server can create a problem. A single server represents a single point of failure and in many cases, cannot handle the workload for an entire network.

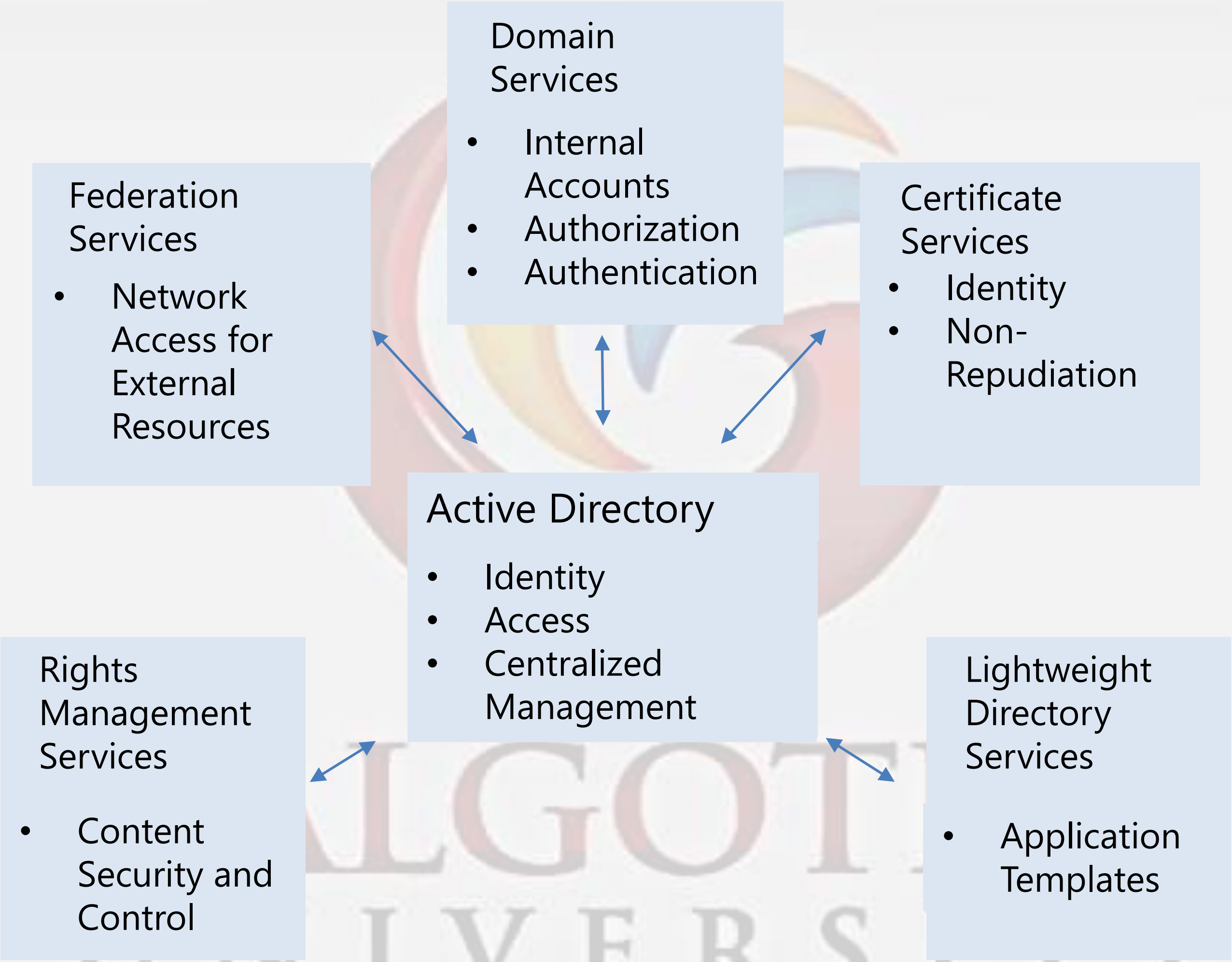
Domains and Workgroups

- That is where a BDC comes in. The BDC holds a second copy of the information that is stored on the PDC, including the database of user accounts and other important network information.
- **Member server-**The member server does not take part in domain authentication and does not hold a copy of the user account database. Member servers provide file, print, and application services.

MS Active Directory

- **Active Directory (AD) is a directory service that Microsoft** developed for windows domain networks.
- It is an object-oriented, hierarchical, distributed directory services database system.
- That provide central database about hardware, software and human resources of entire network.
- A server running Active Directory Domain Services (ADDS) is called a domain controller.
- It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.

MS Active Directory



Domain Services

- Internal Accounts
- Authorization
- Authentication

Federation Services

- Network Access for External Resources

Certificate Services

- Identity
- Non-Repudiation

Active Directory

- Identity
- Access
- Centralized Management

Rights Management Services

- Content Security and Control

Lightweight Directory Services

- Application Templates

Windows Active Directory (AD)

- You host it, on-premises / Cloud
- You manage the infrastructure and the data
- Services:
  - AD Directory Services (AD DS)
    - Kerberos authentication
    - NTLM authentication
  - AD Lightweight Directory Services (AD LDS)
  - AD Federation Services (AD FS)
  - AD Certificate Services (AD CS)
  - AD Rights Management Services (AD RMS)

Windows Azure Active Directory (WAAD)

- Microsoft hosts it in their datacenters
- Microsoft manages the infrastructure
- You manage the data
- Services:
    - Directory Services
        - Federated authentication
            - WS-Federation
            - SAML-P
            - Oauth 2.0
            - More to come...
    - Access Control Services (ACS)

X500 Directory Access Protocol

- **X.500** is a series of computer networking standards covering electronic directory services. The X.500 series was developed by ITU-T, formerly known as CCITT, and first approved in 1988.
- The primary concept of X.500 is that there is a single Directory Information Tree (DIT), a hierarchical, organization of entries which are distributed across one or more servers, called Directory System Agents (DSA).
- An entry consists of a set of attributes, each attribute with one or more values.

X500 Directory Access Protocol

- X.500 Directory Service is a standard way to develop an electronic directory of people in an organization so that it can be part of a global directory available to anyone in the world with Internet access.
- Such a directory is sometimes called a global White Pages directory. The idea is to be able to look up people in a user-friendly way by name, department, or organization.
- Many enterprises and institutions have created an X.500 directory. Because these directories are organized as part of a single global directory, you can search for hundreds of thousands of people from a single place on the World Wide Web.

X500 Directory Access Protocol

- The X.500 directory is organized under a common "root" directory in a "tree" hierarchy of: country, organization, organizational unit, and person.
- An entry at each of these levels must have certain attributes; some can have optional ones established locally.
- Each organization can implement a directory in its own way as long as it adheres to the basic schema or plan.
- The distributed global directory works through a registration process and one or more central places that manage many directories.

SUMMARY

- Windows Domain
- Domain Based Networks
- MS Active Directory
- Windows Active Directory (WAD)
- Windows Azure Active Directory(WAAD)
- X500 Directory Access Protocol

Thank You