MICROSOFT OFFICIAL COURSE

Module 1

Introducing Active Directory® Domain Services

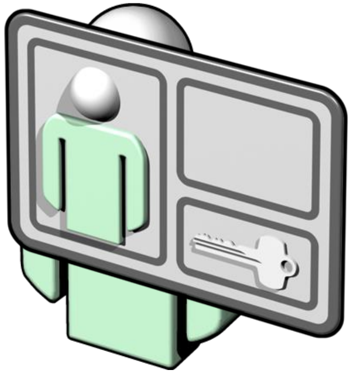
Module Overview

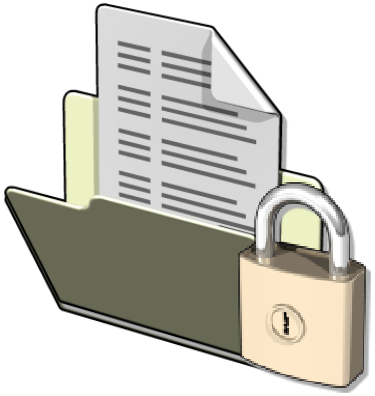
- Overview of Active Directory, Identity, and Access
- Active Directory Components and Concepts
- Install Active Directory Domain Services

Lesson 1: Overview of Active Directory, Identity, and Access

- Information Protection
- Identity and Access
- Authentication and Authorization
- Authentication
- Access Tokens
- Security Descriptors, ACLs, and ACEs
- Authorization
- Stand-Alone (Workgroup) Authentication
- Active Directory Domains: Trusted Identity Store
- Active Directory, Identity, and Access
- Active Directory IDA services

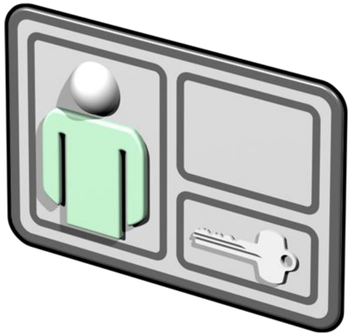
Information Protection



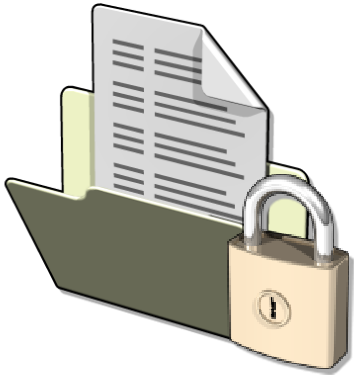


- It’s all about connecting users to the information they require securely
- IDA: Identity and Access
- AAA: Authentication, Authorization, Accounting
- CIA: Confidentiality, Integrity, Availability, and Authenticity

Identity and Access

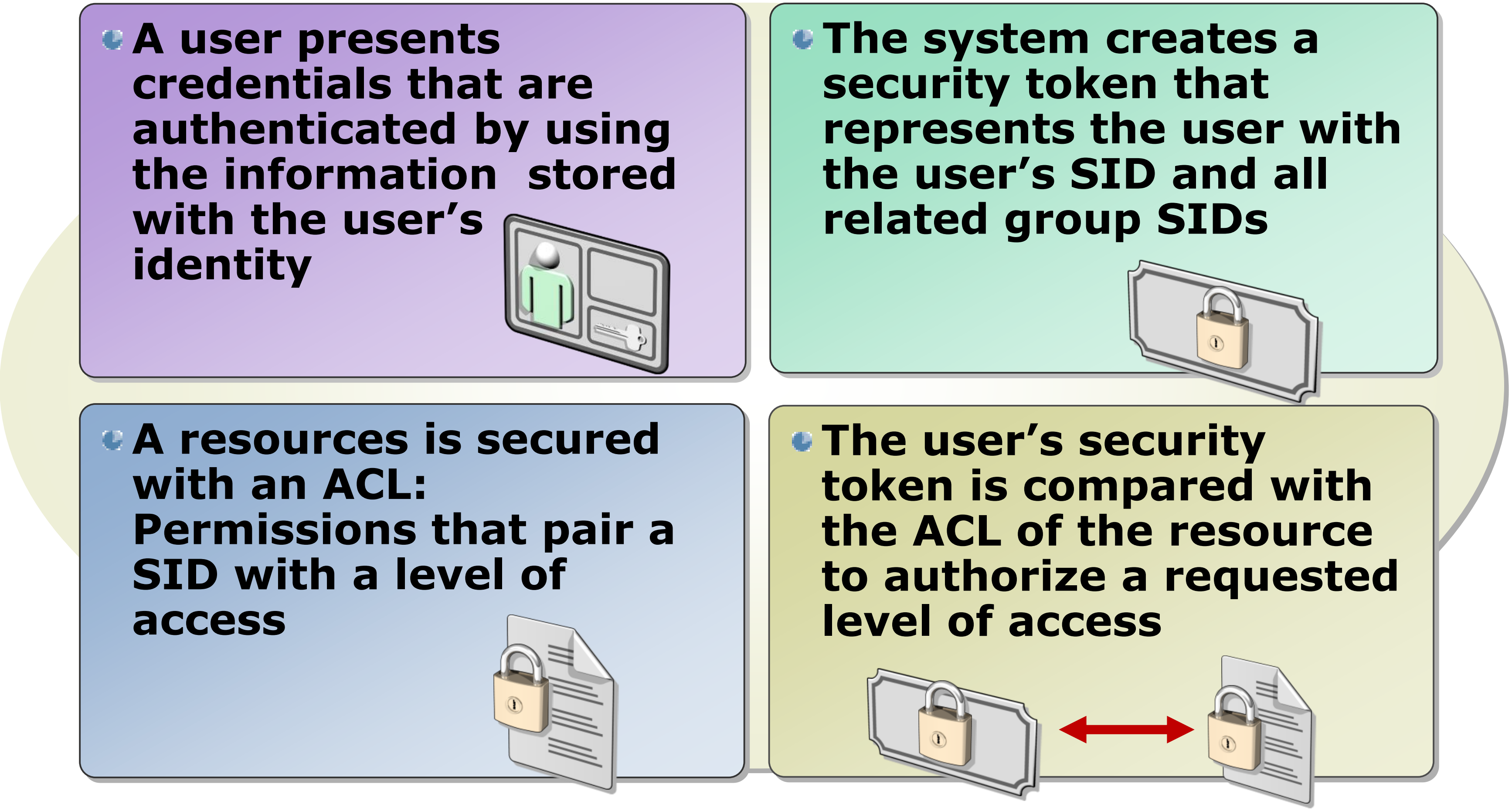


- Identity: User account
- Saved in an identity store (directory database)
- Security principal
- Represented uniquely by the SID



- Resource: Shared Folder
- Secured with a security descriptor
- DACL or “ACL”
- ACEs or “permissions”

Authentication and Authorization



- A user presents credentials that are authenticated by using the information stored with the user's identity

- The system creates a security token that represents the user with the user's SID and all related group SIDs

- A resources is secured with an ACL: Permissions that pair a SID with a level of access

- The user's security token is compared with the ACL of the resource to authorize a requested level of access

Authentication

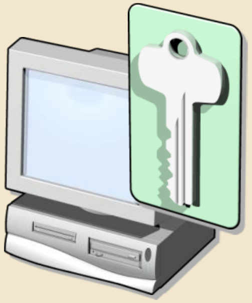
Authentication is the process that verifies a user’s identity

Credentials: At least two components required

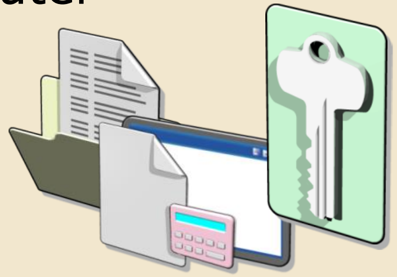
- User name
- Secret, for example, password

Two types of authentication

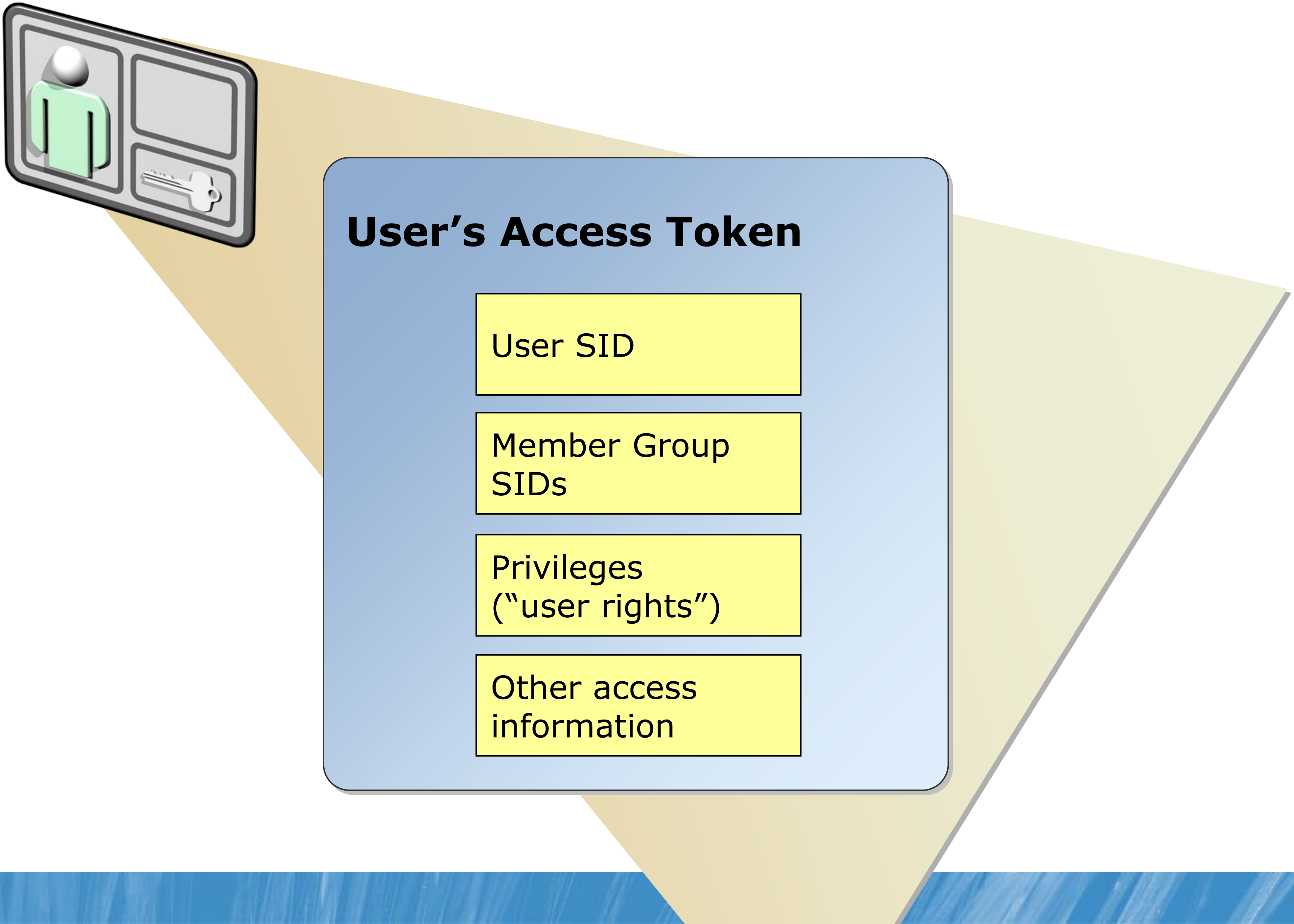
- Local (interactive) Logon–authentication for logon to the local computer



- Remote (network) Logon–authentication for access to resources on another computer



Access Tokens



User's Access Token

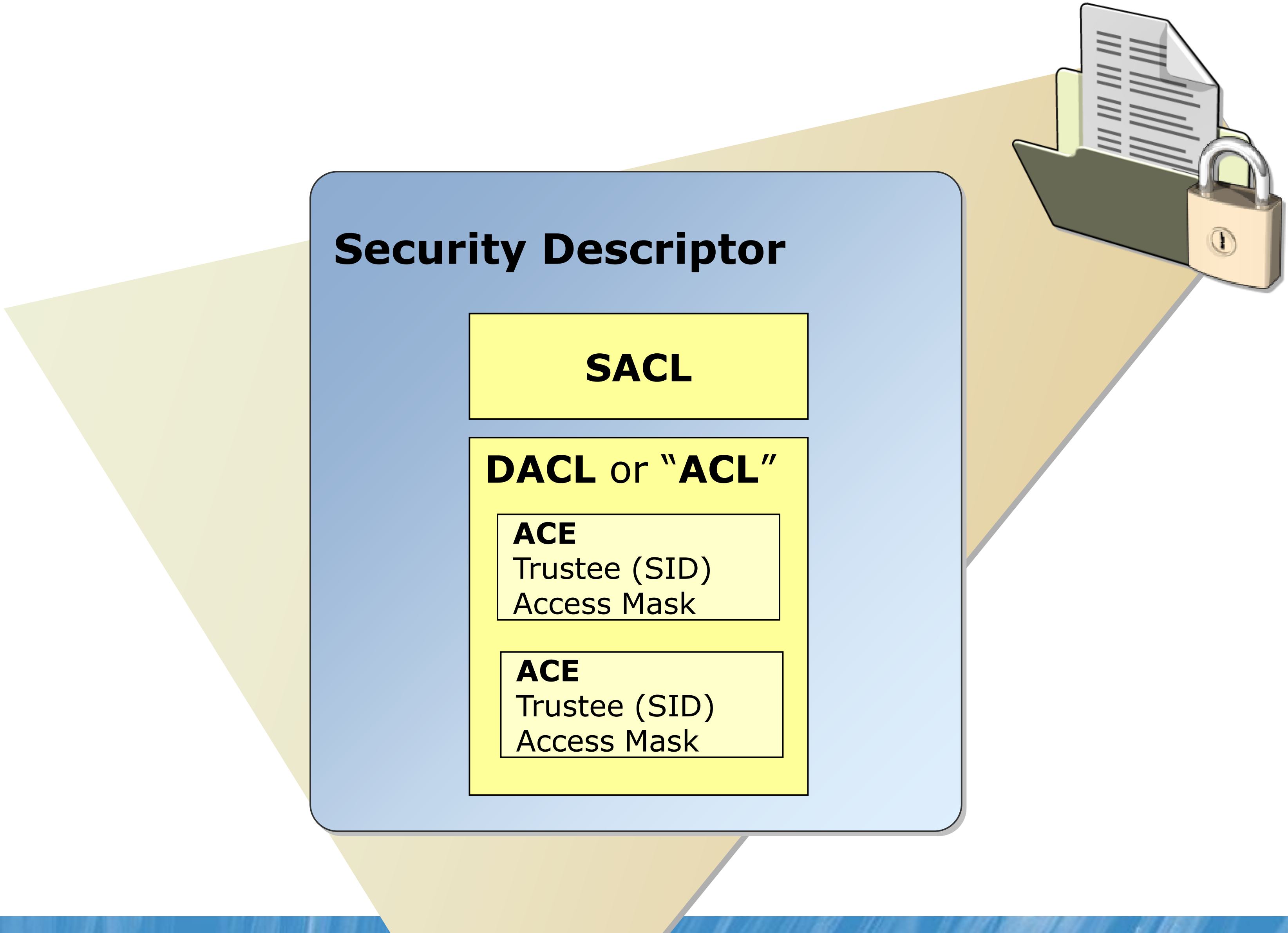
User SID

Member Group SIDs

Privileges ("user rights")

Other access information

Security Descriptors, ACLs and ACEs



Security Descriptor

SACL

DACL or “**ACL**”

ACE
Trustee (SID)
Access Mask

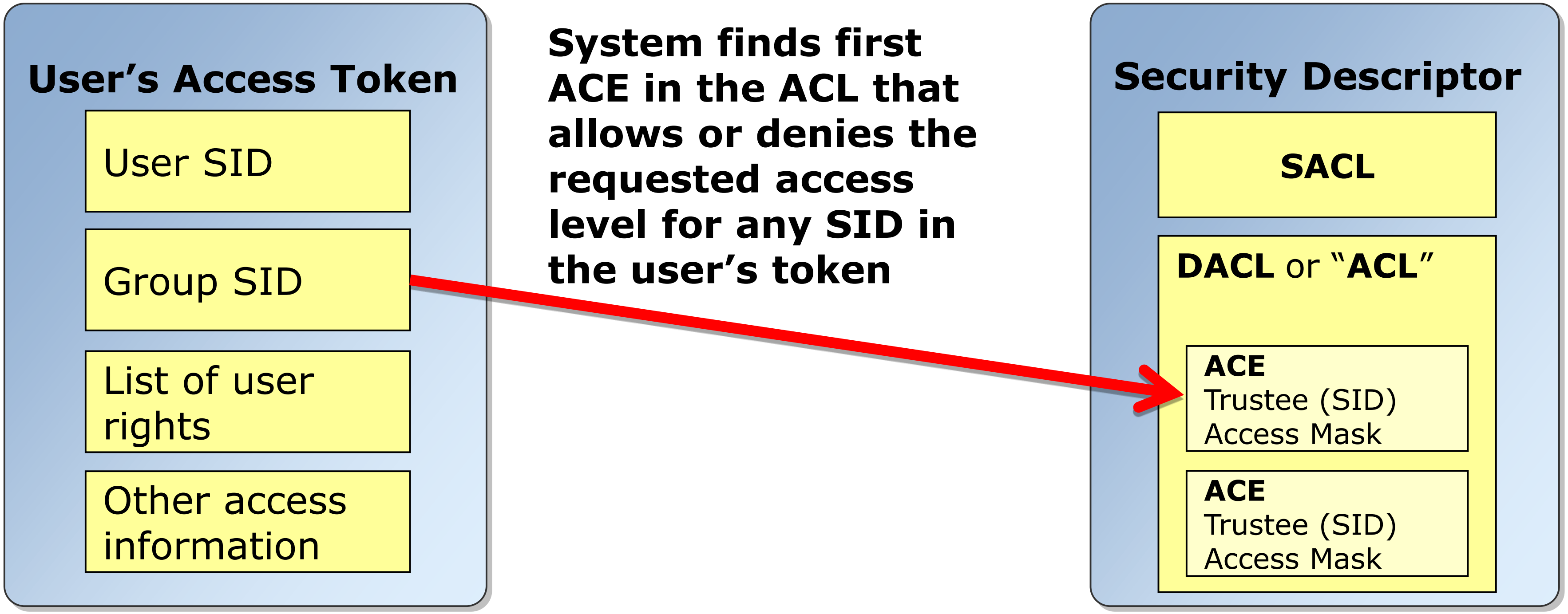
ACE
Trustee (SID)
Access Mask

Authorization

Authorization is the process that determines whether to grant or deny a user a requested level of access to a resource

Three components required for authorization

- Resource
- Access Request
- Security Token



User's Access Token

User SID

Group SID

List of user rights

Other access information

System finds first ACE in the ACL that allows or denies the requested access level for any SID in the user's token

Security Descriptor

SACL

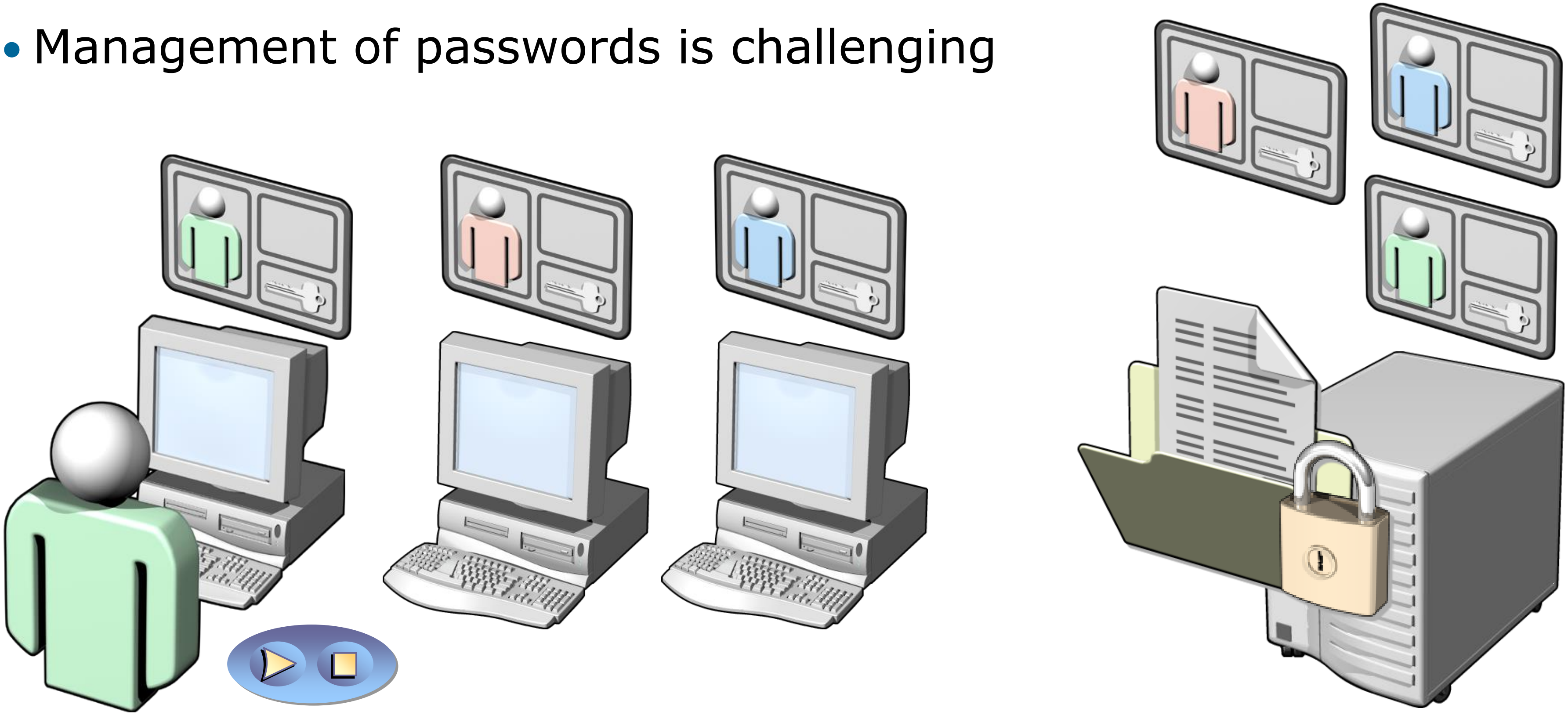
DACL or "**ACL**"

ACE
Trustee (SID)
Access Mask

ACE
Trustee (SID)
Access Mask

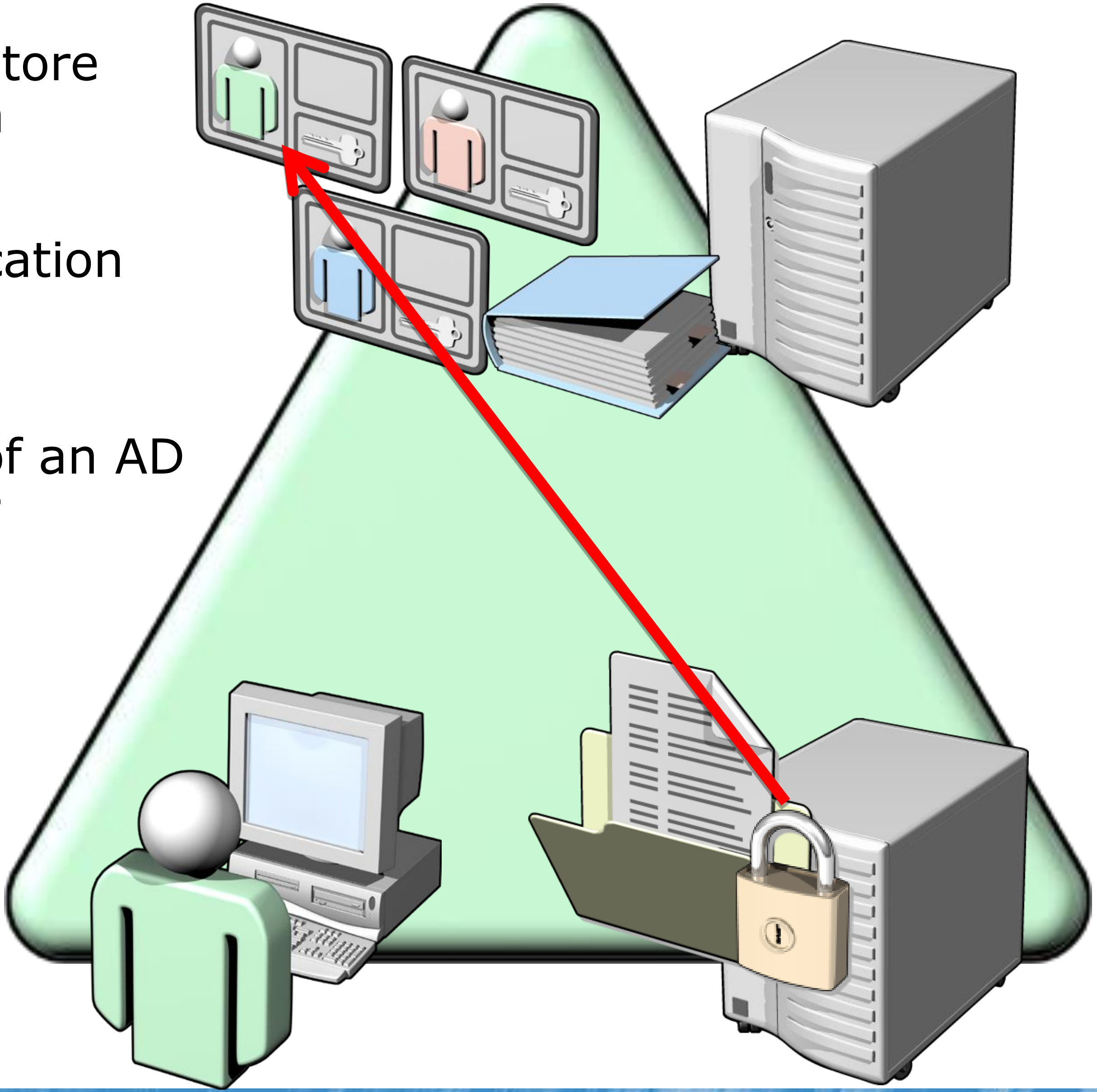
Stand-Alone (Workgroup) Authentication

- The identity store is the SAM database on the Windows system
- No shared identity store
- Multiple user accounts
- Management of passwords is challenging



Active Directory Domains: Trusted Identity Store

- Centralized identity store trusted by all domain members
- Centralized authentication service
- Hosted by a server performing the role of an AD DS domain controller



Active Directory, Identity, and Access

An IDA infrastructure should:

- Store information about users, groups, computers and other identities
- Authenticate an identity
  - Kerberos authentication used in Active Directory provides single sign-on. Users are authenticated only once.
- Control access
- Provide an audit trail

Active Directory IDA Services

Active Directory IDA services :

- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Certificate Services (AD CS)
- Active Directory Rights Management Services (AD RMS)
- Active Directory Federation Services (AD FS)

Lesson 2: Active Directory Components and Concepts

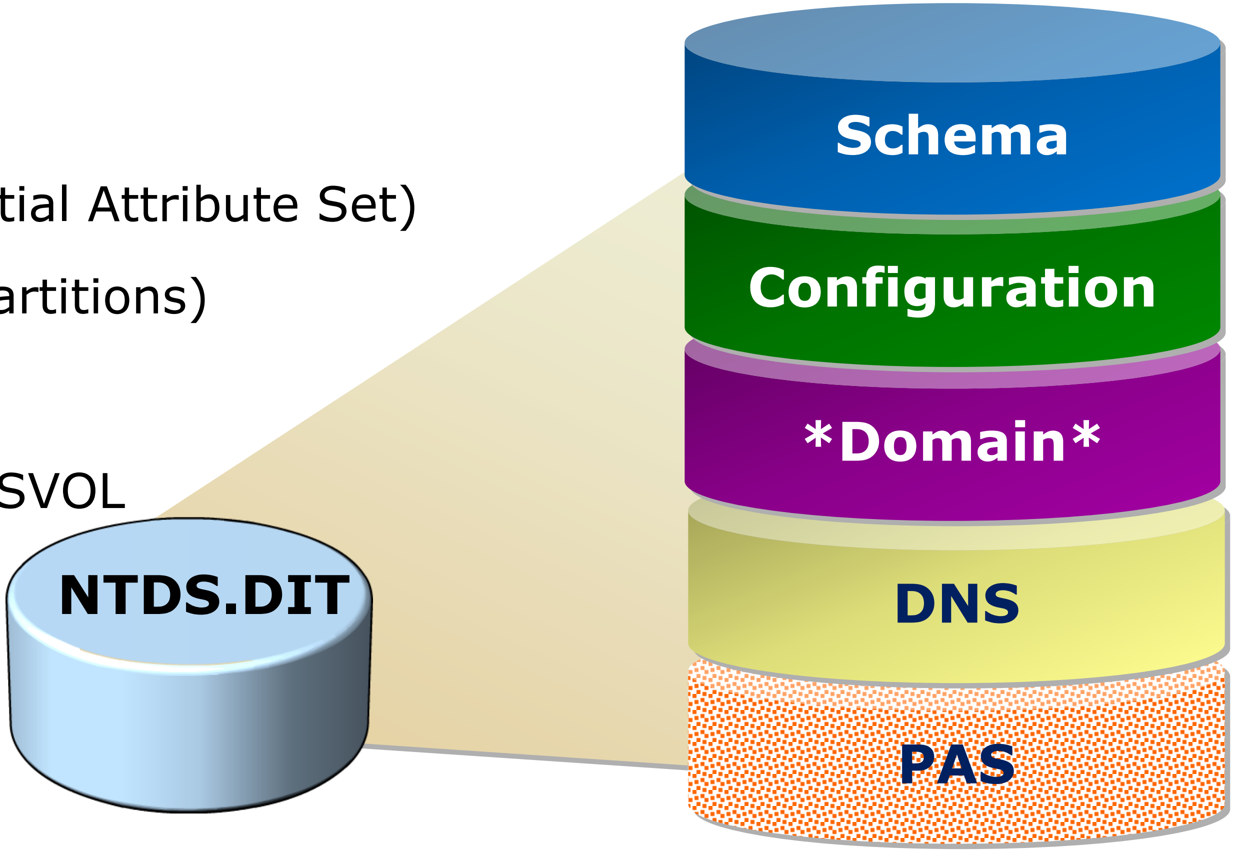
- Active Directory as a Database
- Active Directory Data Store
- Domain Controllers
- Demonstration: Active Directory Schema
- Organizational Units
- Domain
- Forest
- Tree
- Replication
- Sites
- Global Catalog
- Functional Levels
- DNS and Application Partitions
- Trust Relationships

Active Directory as a Database

- Active Directory is a database
  - Each “record” is an object
    - Users, groups, computers, and so on
  - Each “field” is an attribute
    - Logon name, SID, password, description, membership, and so on
  - Identities (security principals or “accounts”)
- Services: Kerberos, DNS, and replication
- Accessing the database
  - Windows tools, user interfaces, and components
  - APIs (.NET, VBScript, Windows PowerShell)
  - LDAP

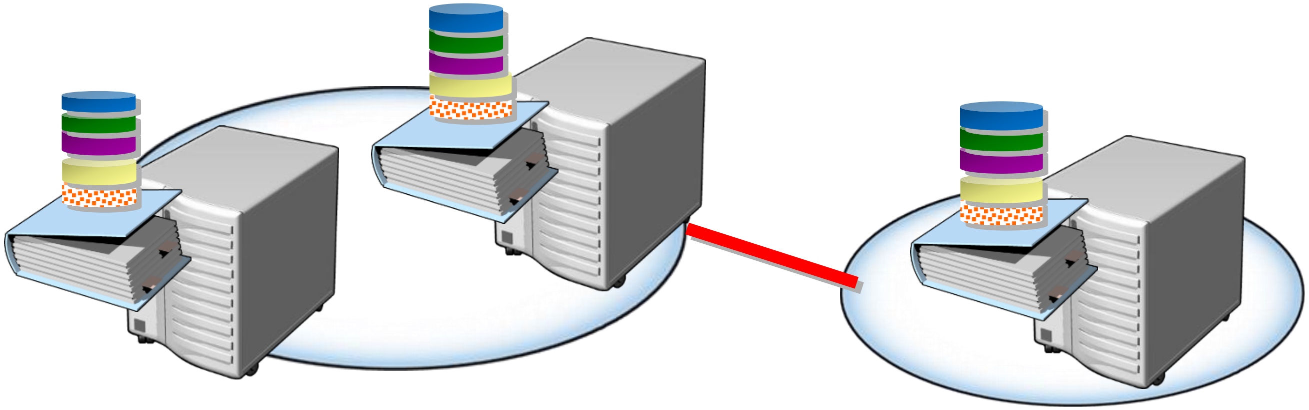
Active Directory Data Store

- %systemroot%\NTDS\ntds.dit
- Logical partitions
  - Domain naming context
  - Schema
  - Configuration
  - Global catalog (Partial Attribute Set)
  - DNS (application partitions)
- SYSVOL
  - %systemroot%\SYSVOL
  - Logon scripts
  - Policies



Domain Controllers

- Servers that perform the AD DS role
  - Host the Active Directory database (NTDS.DIT) and SYSVOL
    - Replicated between domain controllers
  - Kerberos KDC service: Performs authentication
  - Other Active Directory services
- Best practices
  - Availability: At least two in a domain
  - Security: Server Core and RODCs



Demonstration: Active Directory Schema

In this demonstration, you will see

- How the Schema acts as a blueprint for Active Directory by exploring the following Attributes and Object classes:

  Attributes

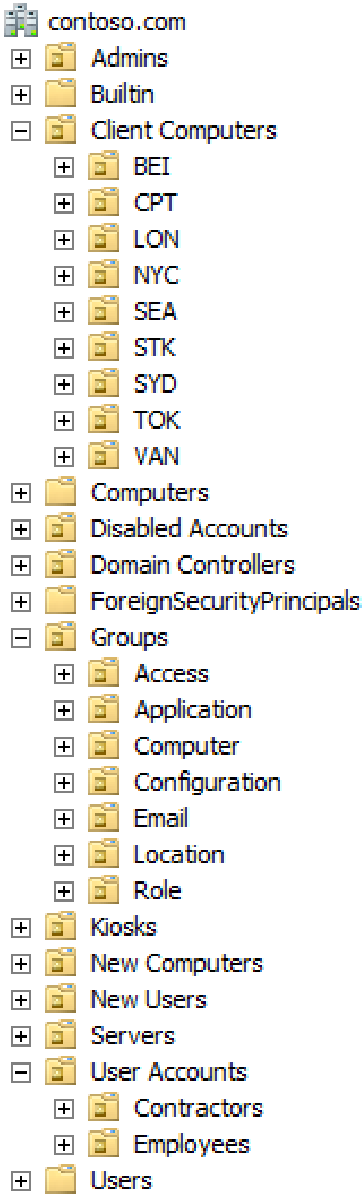
    - objectSID
    - sAMAccountName
    - unicodePwd
    - member
    - Description

  Classes

    - User
    - Group

Organizational Units

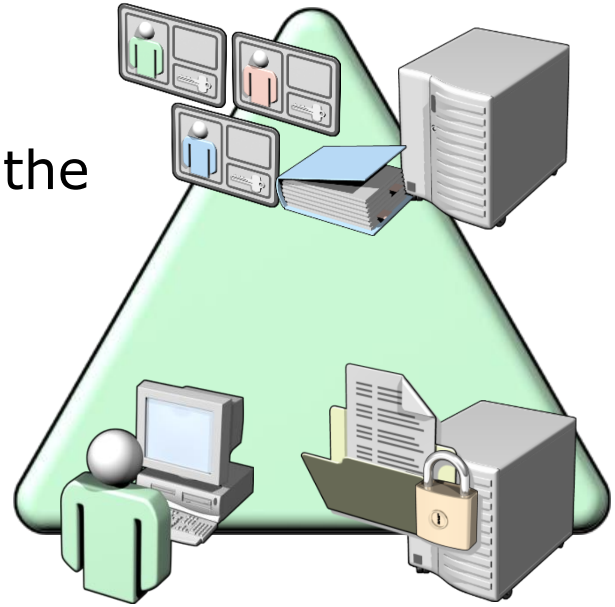
- Objects
  - Users
  - Computers
- Organizational Units
  - Containers that can be used to group objects within a domain
  - Create OUs to:
    - Delegate administrative permissions
    - Apply Group Policy



- contoso.com
  - Admins
  - Builtin
  - Client Computers
    - BEI
    - CPT
    - LON
    - NYC
    - SEA
    - STK
    - SYD
    - TOK
    - VAN
  - Computers
  - Disabled Accounts
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Groups
    - Access
    - Application
    - Computer
    - Configuration
    - Email
    - Location
    - Role
  - Kiosks
  - New Computers
  - New Users
  - Servers
  - User Accounts
    - Contractors
    - Employees
  - Users

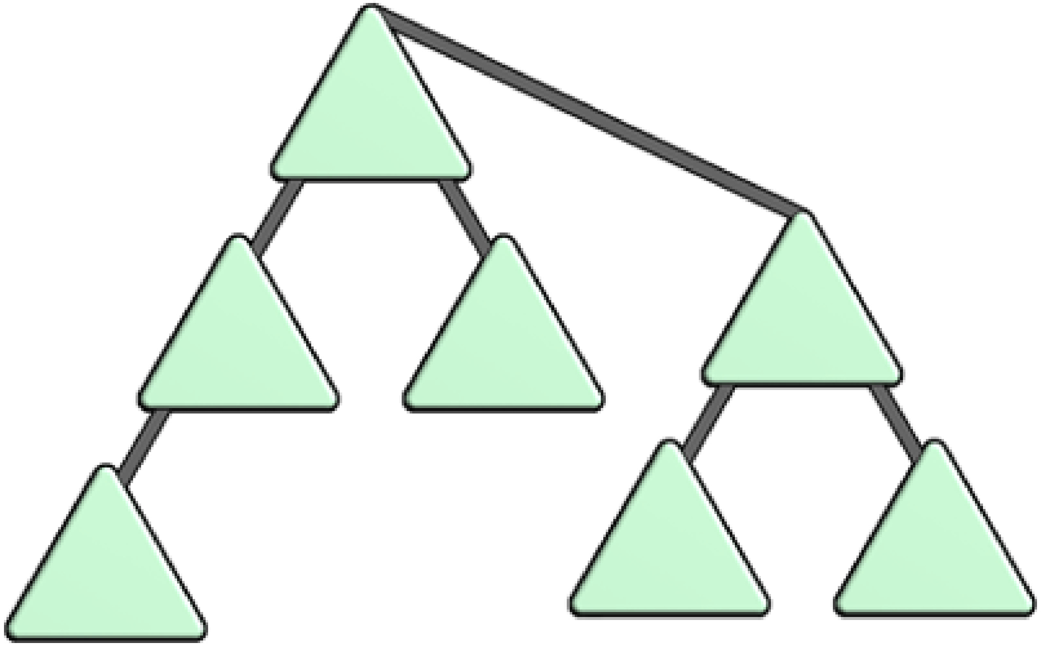
Domain

- Requires one or more domain controllers
- All domain controllers replicate the Domain naming context (Domain NC)
  - The domain is the context within which Users, Groups, Computers, and so on are created
  - “Replication boundary”
- Trusted identity source: Any domain controller can authenticate any logon in the domain
- The domain is the *maximum* scope (boundary) for certain administrative policies
  - Password
  - Lockout



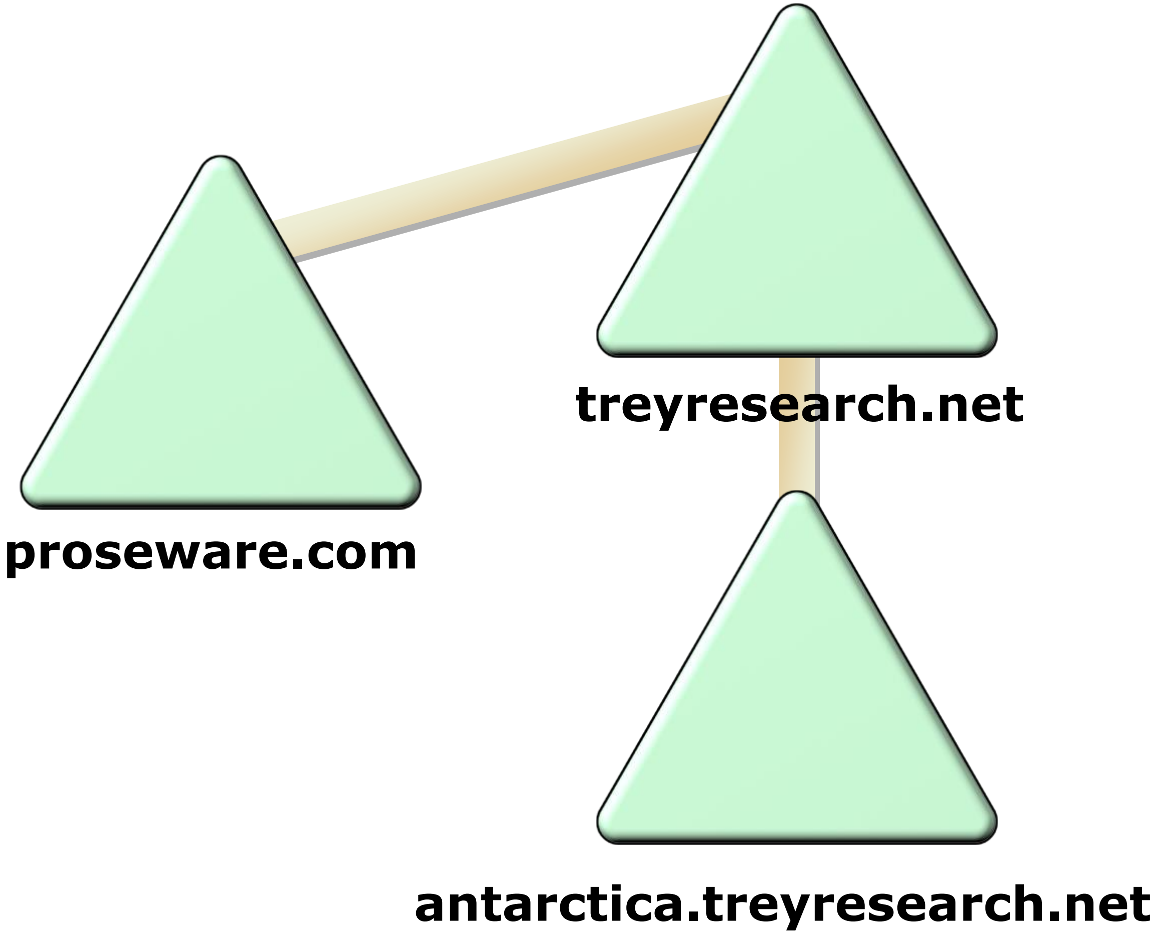
Forest

- A collection of one or more Active Directory domain trees
- First domain is the *forest root domain*
- Single configuration and schema replicated to all domain controllers in the forest
- A security and replication boundary



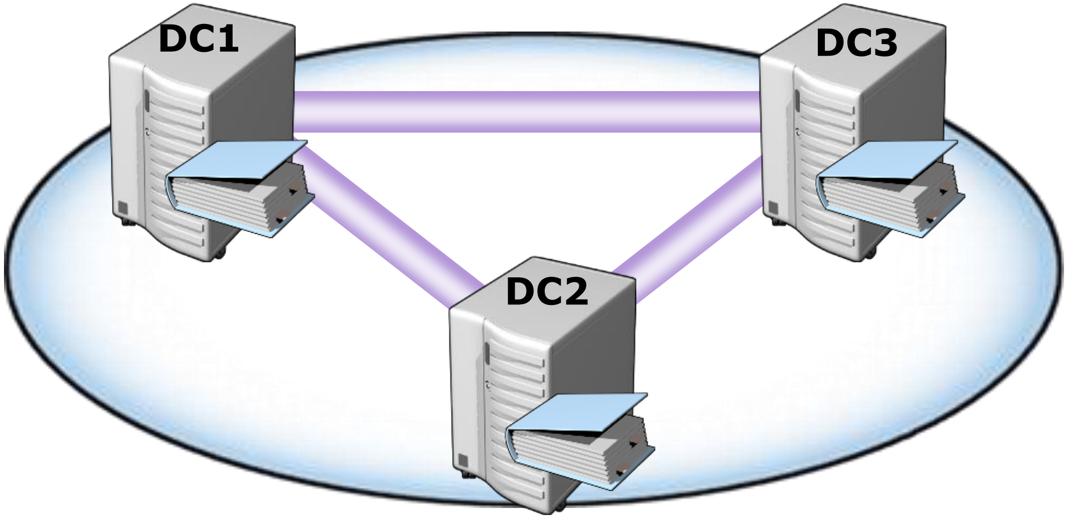
Tree

- One or more domains in a single instance of AD DS that share *contiguous DNS namespace*



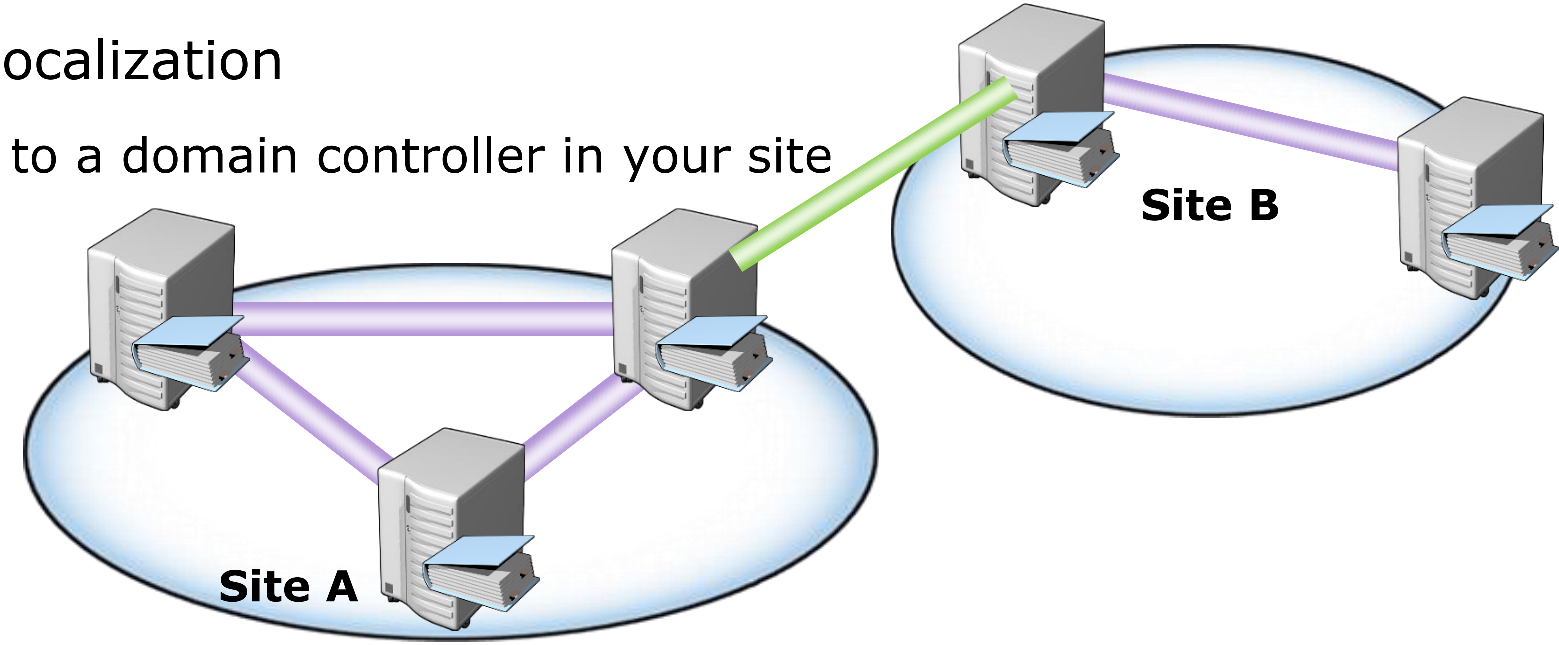
Replication

- Multimaster replication
  - Objects and attributes in the database
  - Contents of SYSVOL are replicated
- Several components work to create an efficient and robust replication topology and to replicate granular changes to AD
- The Configuration partition of the database stores information about sites, network topology, and replication



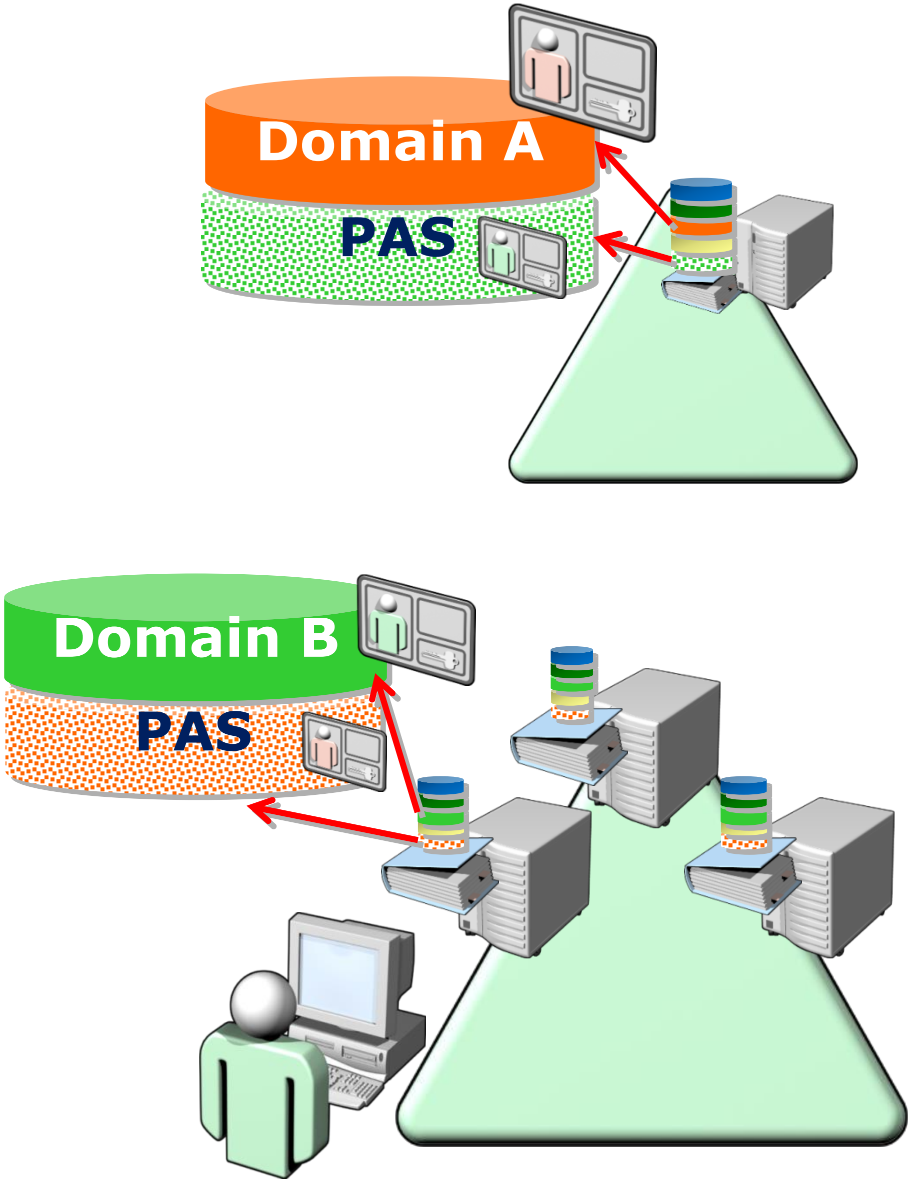
Sites

- An Active Directory object that represents a well-connected portion of your network
  - Associated with subnet objects representing IP subnets
- Intrasite vs. intersite replication
  - Replication within a site occurs very quickly (15–45 seconds)
  - Replication between sites can be managed
- Service localization
  - Log on to a domain controller in your site



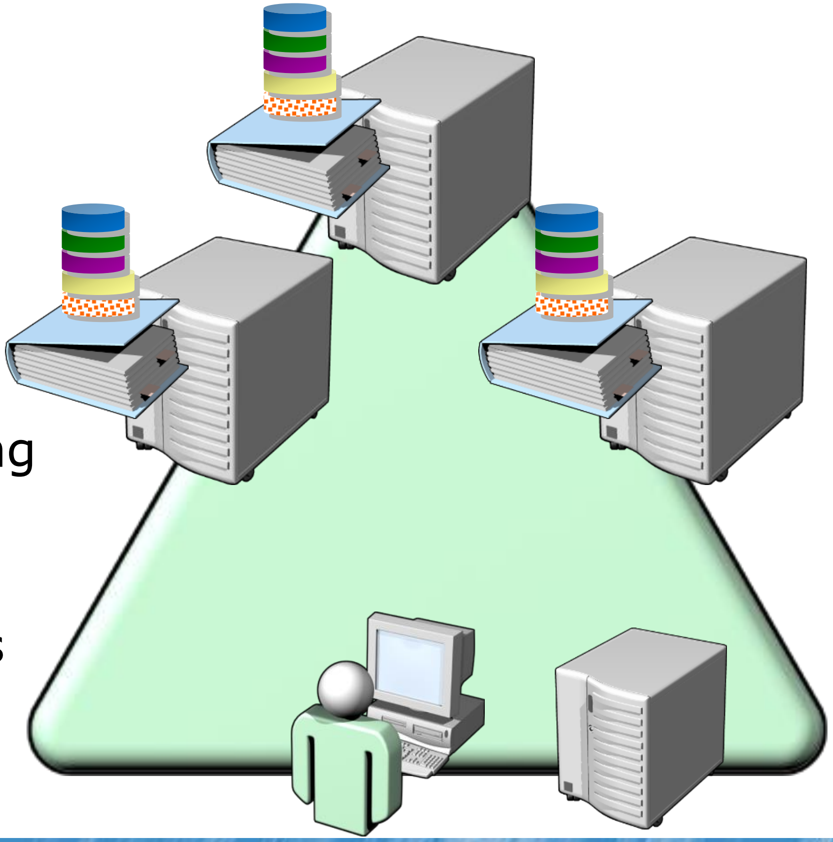
Global Catalog

- Partial Attribute Set or Global Catalog
- Contains every object in every domain in the forest
- Contains only selected attributes
- A type of index
- Can be searched from any domain
- Very important for many applications



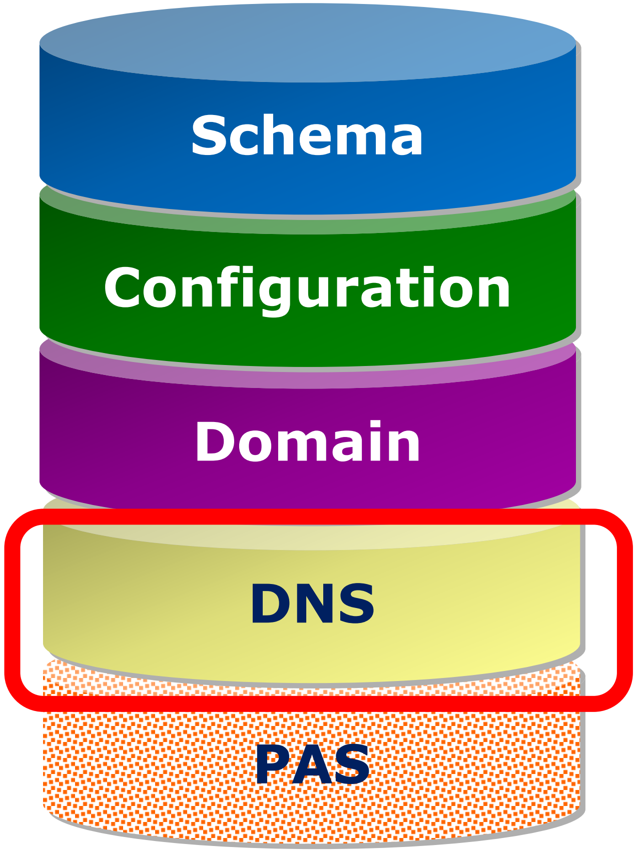
Functional Levels

- Domain functional levels
- Forest functional levels
- New functionality requires that domain controllers are running a particular version of Windows
  - Windows 2000
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2
- Cannot raise functional level while domain controllers are running previous Windows versions
- Cannot add domain controllers running previous Windows versions after raising functional level



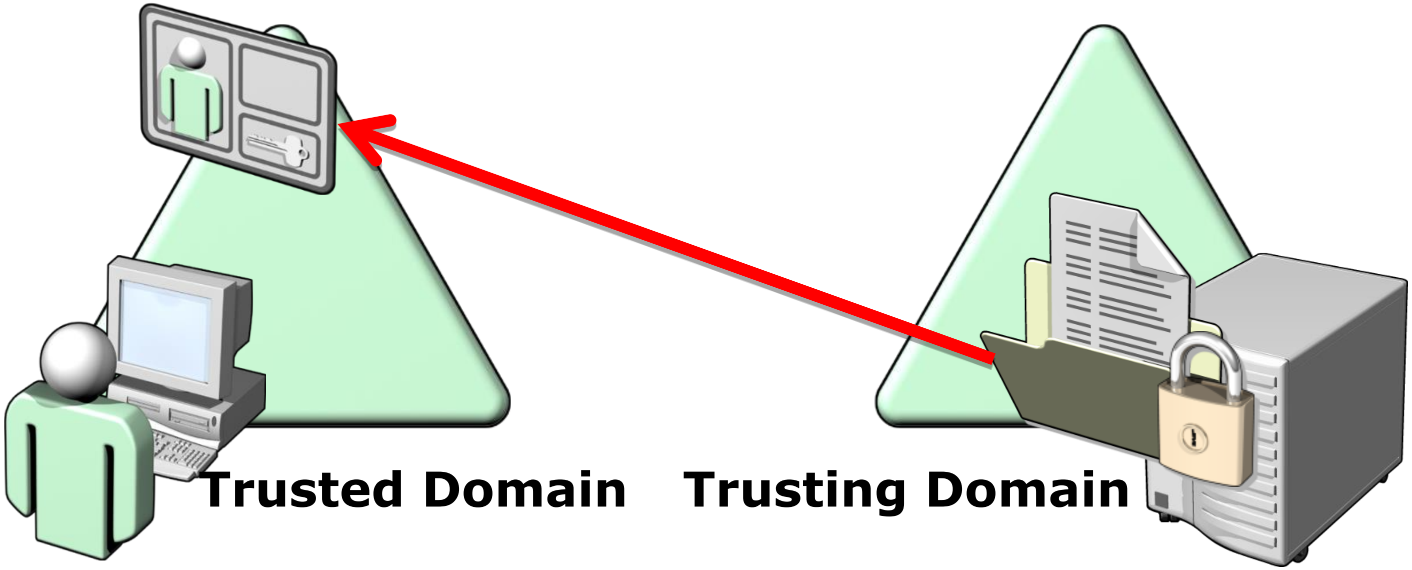
DNS and Application Partitions

- Active Directory and DNS are closely integrated
- One-to-one relationship between the DNS domain name and the logical domain unit of Active Directory
- Complete reliance on DNS to locate computers and services in the domain
- A domain controller acting as a DNS server can store the zone data in Active Directory itself—in an *application partition*



Trust Relationships

- Extends concept of trusted identity store to another domain
- Trusting domain (with the resource) trusts the identity store and authentication services of the trusted domain
- A trusted user can authenticate to, and be given access to resources in, the trusting domain
- Within a forest, each domain trusts all other domains
- Trust relationships can be established with external domains

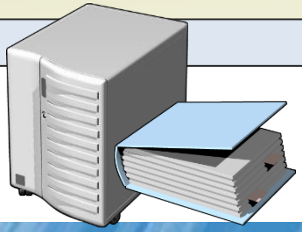


Lesson 3: Install Active Directory Domain Services

- Install and Configure a Domain Controller
- Prepare to Create a New Forest with Windows Server 2008 R2

Install and Configure a Domain Controller

1. Install the Active Directory Domain Services role by using the Server Manager
2. Run the Active Directory Domain Services Installation Wizard
3. Choose the deployment configuration
4. Select the additional domain controller features
5. Select the location for the database, log files, and SYSVOL folder
6. Configure the Directory Services Restore Mode Administrator Password



Prepare to Create a New Forest with Windows Server 2008 R2

- Domain’s DNS name (contoso.com)
- Domain’s NetBIOS name (contoso)
- Whether the new forest will need to support domain controllers running previous versions of Windows (affects choice of functional level)
- Details about how DNS will be implemented to support AD DS
  - Default: Creating domain controller adds DNS Server role as well
- IP configuration for the domain controller
  - IPv4 and, optionally, IPv6
- User name and password of an account in the server’s Administrators group. Account must have a password.
- Location for data store (ntds.dit) and SYSVOL
  - Default: %systemroot% (c:\windows)

Lab: Install an AD DS Domain Controller to Create a Single Domain Forest

- Exercise 1: Perform Post-Installation Configuration Tasks
- Exercise 2: Install a New Windows Server 2008 Forest with the Windows Interface
- Exercise 3: Raise Domain and Forest Functional Levels

Logon information

Virtual machine	6425C-NYC-SVR-D
Logon user name	Administrator
Password	Pa$$w0rd

Estimated time: 30 minutes

Lab Scenario

You have been hired to improve identity and access at Contoso, Ltd. The company currently has one server in a workgroup configuration. Employees connect to the server from their personal client computers. In anticipation of near-term growth, you need to improve the manageability and security of the company’s resources. You decide to implement an AD DS domain and forest by promoting the server to a domain controller. You have just finished installing Windows Server 2008 R2 from the installation DVD.

Lab Review

- What can you do with the Initial Configuration Tasks console?
- What must you do before starting the dcpromo wizard?
- Which tool is used to raise the domain functional level?

Module Review and Takeaways

- Review Questions
- Common Issues Related to AD DS Installation
- Best Practices Related to AD DS Installation
- Tools