

Creating an Active Directory Domain

Active Directory Domain Services (AD DS) and its related services form the foundation for enterprise networks running Microsoft Windows. Together, they act as tools that store information about the identities of users, computers and services; authenticate individual users or computers; and provide a mechanism with which a user or computer can access resources in the enterprise. In this chapter, you will begin your exploration of Windows Server 2008 R2 Active Directory by installing the Active Directory Domain Services role and creating a domain controller in a new Active Directory forest. You will find that Windows Server 2008 R2 continues the evolution of Active Directory by enhancing many of the existing concepts and features with which you are already familiar.

This chapter focuses on the creation of a new Active Directory forest with a single domain in a single domain controller. The practice exercises in this chapter guide you through the creation of a domain named contoso.com that you will use for all other practices in this Course. In later chapters, you will gain experience with other scenarios and the implementation of the other key Active Directory components integrated with AD DS.

Exam objectives in this chapter:

- Configure a forest or a domain.

Before You Begin

To complete the lessons in this chapter, you must have done the following:

- Obtained two computers on which you will install Windows Server 2008 R2. The computers can be physical systems that meet the minimum hardware requirements for Windows Server 2008, found at <http://tinyurl.com/5k7bn2> or <http://tinyurl.com/4evvn9x>. You will need at least 512 MB of RAM, 32 GB of free hard disk space and an x64 processor with a minimum clock speed of 1.4 GHz. Alternately, you can use virtual machines that meet the same requirements.
- Obtained an evaluation version of Windows Server 2008 R2. A 180-day trial evaluation version of Windows Server 2008 R2 with SP1 is available for download at <http://tinyurl.com/5kaojz>.



REAL WORLD

Windows Server 2008 R2 supports only x64 or Itanium 2 processors; it no longer supports the x86 processor architecture. If this system requirement is not met, Windows Server 2008 R2 will not install. This is most important when upgrading pre-existing servers to Windows Server 2008 R2. Pre-existing servers based on the x86 processor architecture must be replaced with hardware based on either the x64 or Itanium 2 processor architecture.

In the most common AD DS installation scenario, the server functions as a domain controller, which maintains a copy of the AD DS database and replicates it with other domain controllers. Domain controllers are the most critical component in an Active Directory infrastructure and should function with as few additional unrelated components installed as possible. This dedicated configuration provides for more stable and reliable domain controllers, because it limits the possibility of other applications or services interfering with the AD DS components running on the domain controller.

In versions of Windows Server prior to Windows Server 2008, server administrators were required to select and configure individual components on a server to ensure that nonessential Windows components were disabled or uninstalled. In Windows Server 2008, key Windows components are broken down into functionally related groups called *roles*. Role-based administration allows an administrator to simply select the role or roles that the server should fulfil. Windows Server 2008 then installs the appropriate Windows components required to provide that role's functionality. You will become more familiar with role-based administration as you proceed through the practice exercises in this Course.

Lesson 1: Installing Active Directory Domain Services

Active Directory Domain Services (AD DS) provides the functionality of an identity and access (IDA) solution for enterprise networks. In this lesson, you learn about AD DS and other Active Directory roles supported by Windows Server 2008. You also explore Server Manager, the tool with which you can configure server roles, and the improved Active Directory Domain Services Installation Wizard. This lesson also reviews key concepts of IDA and Active Directory.

After this lesson, you will be able to:

- ✓ Explain the role of identity and access in an enterprise network.
- ✓ Understand the relationship between Active Directory services.
- ✓ Install the Active Directory Domain Services (AD DS) role and configure a Windows Server 2008 R2 domain controller using the Windows interface.

Estimated lesson time: 60 minutes

Active Directory, Identity and Access

Identity and access (IDA) infrastructure refers to the tools and core technologies used to integrate people, processes and technology in an organisation. An effective IDA infrastructure ensures that the right people have access to the right resources at the right time.

As previously mentioned, Active Directory provides the IDA solution for enterprise networks running Windows. AD DS is the core component of an Active Directory IDA infrastructure. AD DS collects and stores enterprise-wide IDA information in a database called the *Active Directory data store*. The data store contains all pertinent information on all objects that exist within the Active Directory infrastructure. In addition, AD DS acts as a communication and information hub for additional Active Directory services which, together, form a complete IDA infrastructure.

Active Directory stores information about users, groups, computers and other identities. An identity is, in the broadest sense, a representation of an object that will perform actions on the enterprise network. For example, a user will open documents from a shared folder on a server. The document will be secured with permissions on an access control list (ACL). Access to the document is managed by the security subsystem of the server, which compares the identity of the user to the identities on the ACL to determine whether the user's request for access will be granted or denied.

Computers, groups, services and other objects also perform actions on the network; they must be represented by identities. Among the information stored about an identity are properties that uniquely identify the object, such as a user name or a security identifier (SID), and the password for the identity. The *identity store* is, therefore, one component of an IDA infrastructure. The Active Directory data store, also known as the *directory*, is an identity store. The directory itself is hosted within a database that is stored on and managed by a domain controller—a server performing the AD DS role. If multiple domain controllers exist within an Active Directory infrastructure, they work together to maintain a copy of the data store on each domain controller. The information within this store allows Active Directory to perform the three main functions of an IDA infrastructure: authentication, access control and auditing.

- **Authentication** A user, computer or other object must first verify its identity to the Active Directory infrastructure before being granted the ability to function as part of the Active Directory domain. This process of verification is typically through an exchange of protected or secret information such as a password or a digital certificate. After the authentication information has been submitted to the Active Directory and verified as valid, the user may proceed as a member of the

domain and perform actions such as requesting access to shared files, submitting a print job to a printer, accessing and reading email, or any number of other actions within the domain.

Kerberos Authentication in an Active Directory Domain

In an Active Directory domain, the Kerberos protocol is used to authenticate identities. When a user or computer logs on to the domain, Kerberos authenticates its credentials and issues a package of information called a *ticket granting ticket* (TGT). Before the user performs a task (such as connecting to a server to request a document), a Kerberos request is sent to a domain controller along with the TGT that identifies the authenticated user. The domain controller issues the user another package of information called a *service ticket* that identifies the authenticated user to the server. The user presents the service ticket to the server, which accepts the service ticket as proof that the user has been authenticated.

These Kerberos transactions result in a single network logon. After the user or computer has initially logged on and has been granted a TGT, the user is authenticated within the entire domain and can be granted service tickets that identify the user to any service. All of this ticket activity is managed by the Kerberos clients and services built into Windows and remains transparent to the user.

- **Access control** The IDA infrastructure is responsible for protecting information and resources by ensuring that access to resources is granted only to the identities that should have it. Access to important resources and confidential information must be managed according to the enterprise policies. Every single object (such as computers, folders, files and printers) within Active Directory has an associated discretionary access control list (DACL). This list contains information regarding the identities that have been granted access to the object and the level of access granted. When a user whose identity has already been authenticated on the domain tries to access a resource, the resource's DACL is checked to determine whether the user's identity is on the list. If the identity exists on the list, the user is allowed to access the resource as specified by the access permissions on the DACL listed for that user.
- **Auditing** Monitoring those activities that occur within the IDA infrastructure is referred to as *auditing*. Auditing allows organisations to monitor events occurring within the IDA infrastructure; these include access to files and folders, where and when users are logging on, changes made to the IDA infrastructure and the general functionality of Active Directory itself. Auditing behaviour is controlled by system access control lists (SACLs). As with the previously mentioned DACL, every object within the IDA infrastructure has a SACL attached to it. The SACL contains a list of identities whose activity on that resource will be audited, as well as the level of auditing that will occur for each identity.

AD DS is not the only component of IDA supported by Windows Server 2008. With the release of Windows Server 2008, Microsoft consolidated several previously separate components into an integrated IDA platform. Active Directory itself now includes five technologies, each of which is identified with a keyword that indicates the purpose of the technology, as shown in Figure 1-1.

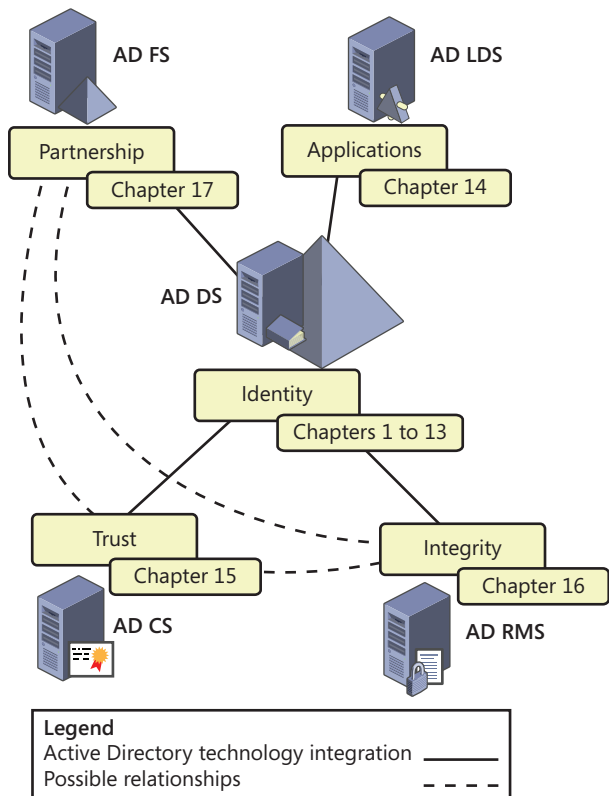


FIGURE 1-1 Integration of the five Active Directory technologies

These five technologies comprise a complete IDA solution:

- Active Directory Domain Services (Identity)** AD DS, as described earlier, is designed to provide a central repository for identity management within an organisation. AD DS provides authentication, authorisation and auditing services on a network and supports object management through Group Policy. AD DS also provides information management and sharing services, enabling users to find any component—file servers, printers, groups, and other users—by searching the directory. Because of this, AD DS is often referred to as a *network operating system directory service*. AD DS is the primary Active Directory technology and should be deployed in every network that runs Windows Server 2008 operating systems. AD DS is covered in Chapters 1 to 13.

MORE INFO AD DS DESIGN

For more details on planning the implementation of AD DS and information regarding AD DS design, see the AD DS Design Guide at <http://tinyurl.com/3ujyju>.

- Active Directory Lightweight Directory Services (Applications)** Essentially a stand-alone version of Active Directory, the Active Directory Lightweight Directory Services (AD LDS) role, formerly known as Active Directory Application Mode (ADAM), provides support for directory-enabled applications. AD LDS is really a subset of AD DS because both are based on the same core code. The AD LDS directory stores and replicates only application-related information. It is commonly used by applications that require a directory store but do not require the information to be replicated as widely as to all domain controllers. AD LDS also enables you to deploy a custom schema to support an application without modifying the schema of AD DS. The AD LDS role is truly lightweight and supports multiple data stores on a single system, so each application can be deployed with its own directory, schema, assigned Lightweight Directory Access Protocol (LDAP) and SSL ports, and application event log. AD LDS does not rely on AD

DS, so it can be used in a stand-alone or workgroup environment. However, in domain environments, AD LDS can use AD DS for the authentication of Windows security principals (users, groups and computers). AD LDS can also be used to provide authentication services in exposed networks such as extranets. Using AD LDS in this situation provides less risk than using AD DS. AD LDS is covered in Chapter 14, 'Active Directory Lightweight Directory Services.'

- **Active Directory Certificate Services (Trust)** Organisations can use Active Directory Certificate Services (AD CS) to set up a certificate authority (CA) for issuing digital certificates as part of a public key infrastructure (PKI) that binds the identity of a person, device or service to a corresponding private key. Certificates can be used to authenticate users and computers; provide Web-based authentication; support smart card authentication; and to support applications, including secure wireless networks, virtual private networks (VPNs), Internet Protocol security (IPSec), Encrypting File System (EFS), digital signatures and more. AD CS provides an efficient and secure way to issue and manage certificates. You can use AD CS to provide these services to external communities. If you do so, AD CS should be linked with an external, renowned CA that will prove to others you are who you say you are. AD CS is designed to create trust in an untrustworthy world; as such, it must rely on proven processes to certify that each person or computer that obtains a certificate has been thoroughly verified and approved. In internal networks, AD CS can integrate with AD DS to provision users and computers automatically with certificates. AD CS is covered in Chapter 15, 'Active Directory Certificate Services and Public Key Infrastructures.'
- **Active Directory Rights Management Services (Integrity)** Although a server running Windows can prevent or allow access to a document based on the document's DACL, there have been few ways to control what happens to the document and its content after a user has opened it. Active Directory Rights Management Services (AD RMS) is an information-protection technology that enables you to implement persistent usage policy templates that define allowed and disallowed use whether online or offline, inside or outside the firewall. For example, you could configure a template that allows users to read a document but not to print or copy its contents. By doing so, you can ensure the integrity of the data you generate, protect intellectual property and control who can do what with the documents your organisation produces. AD RMS requires an Active Directory domain with domain controllers running Windows 2000 Server with Service Pack 3 (SP3) or later; IIS, a database server such as Microsoft SQL Server 2008; the AD RMS client (which can be downloaded from the Microsoft Download Center and is included by default in Windows Vista, Windows 7, and Windows Server 2008); and an RMS-enabled browser or application such as Microsoft Internet Explorer, Microsoft Office, Microsoft Word, Microsoft Outlook or Microsoft PowerPoint. AD RMS can rely on AD CS to embed certificates within documents as well as in AD DS to manage access rights. AD RMS is covered in Chapter 16, 'Active Directory Rights Management Services.'
- **Active Directory Federation Services (Partnership)** Active Directory Federation Services (AD FS) enables an organisation to extend IDA across multiple platforms (including both Windows and non-Windows environments) and to project identity and access rights across security boundaries to trusted partners. In a federated environment, each organisation maintains and manages its own identities; however, each organisation can also securely project and accept identities from other organisations. Users are authenticated in one network but can access resources in another—a process known as *single sign-on* (SSO). AD FS supports partnerships because it allows different organisations to share access to extranet applications while relying on their own internal AD DS structures to provide the actual authentication process. To do so, AD FS extends your internal AD DS structure to the external world through common Transmission Control Protocol/Internet Protocol

(TCP/IP) ports such as 80 (HTTP) and 443 (Secure HTTP, or HTTPS). It normally resides in the perimeter network. AD FS can rely on AD CS to create trusted servers and on AD RMS to provide external protection for intellectual property. AD FS is covered in Chapter 17, 'Active Directory Federation Services.'

Together, the Active Directory roles provide an integrated IDA solution. AD DS or AD LDS provides foundational directory services in both domain and stand-alone implementations. AD CS provides trusted credentials in the form of PKI digital certificates. AD RMS protects the integrity of information contained in documents. Additionally, AD FS supports partnerships by eliminating the need for federated environments to create multiple, separate identities for a single security principal.

Beyond Identity and Access

Active Directory delivers more than just an IDA solution, however; it also provides the mechanisms to support, manage, and configure resources in distributed network environments.

A set of rules, the *schema*, defines the classes of objects and attributes that can be contained in the directory. The fact that Active Directory has user objects that include a user name and password, for example, is because the schema defines the *user* object class, the two attributes and the association between the object class and attributes.

Policy-based administration eases the management burden of even the largest, most complex networks by providing a single point at which to configure settings that are then deployed to multiple systems. You will learn about such policies, including Group Policy, audit policies, and fine-grained password policies in Chapter 6, 'Implementing a Group Policy Infrastructure'; Chapter 7, 'Managing Enterprise Security and Configuration with Group Policy Settings'; and Chapter 8, 'Improving the Security of Authentication in an AD DS Domain.'

Replication services distribute directory data across a network. This includes both the data store itself as well as data required to implement policies and configuration, including logon scripts. In Chapter 8; Chapter 11, 'Managing Sites and Active Directory Replication'; and Chapter 10, 'Administering Domain Controllers,' you will learn about Active Directory replication. There is even a separate partition of the data store named *configuration* that maintains information about network configuration, topology and services.

Several components and technologies enable you to query Active Directory and locate objects in the data store. A partition of the data store called the *global catalog* (also known as the *partial attribute set*) contains information about every object in the directory; it is a type of index that can be used to locate objects in it. Programmatic interfaces, such as Active Directory Services Interface (ADSI), and protocols such as LDAP can be used to read and manipulate the data store.

The Active Directory data store can also be used to support applications and services not directly related to AD DS. Within the database, application partitions can store data to support applications that require replicated data. The domain name system (DNS) service on a server running Windows Server 2008 can store its information in a database called an *Active Directory integrated zone*, which is maintained as an application partition in AD DS and replicated using Active Directory replication services.

Components of an Active Directory Infrastructure

The first 13 chapters of this Course focus on the installation, configuration and management of AD DS. AD DS provides the foundation for IDA in, and management of, an enterprise network. It is worthwhile to spend a few moments reviewing the components of an Active Directory infrastructure.