

## APPLICATION DIRECTORY PARTITIONS

At the beginning of the class you learned that AD DS includes a Data Store of Identity and Management, specifically the Directory Database NTDS.dit. Within that single file are directory partitions.

Each directory partition, also called a naming context, contains objects of a particular scope and purpose. Three major naming contexts are discussed in this training kit:

- **Domain** The Domain naming context (NC) contains all the objects stored in a domain, including users, groups, computers, and Group Policy containers (GPCs).
- **Configuration** The Configuration partition contains objects that represent the logical structure of the forest, including domains, as well as the physical topology, including sites, subnets, and services.
- **Schema** The Schema defines the object classes and their attributes for the entire directory.

Each domain controller maintains a copy, or *replica*, of several naming contexts. The Configuration is replicated to every domain controller in the forest, as is the Schema. The Domain NC for a domain is replicated to all domain controllers within a domain but not to domain controllers in other domains, so each domain controller has at least three replicas: the Domain NC for its domain, the Configuration, and the Schema.

Traditionally, replicas have been complete replicas, containing every attribute of an object, and replicas have been writable on all DCs. Beginning with Windows Server 2008, read-only domain controllers (RODCs) change the picture slightly. An RODC maintains a read-only replica of all objects in the Configuration, Schema, and Domain NCs of its domain. However, certain attributes are not replicated to an RODC—specifically, secrets such as user passwords—unless the password policy of the RODC allows such replication. There are also attributes that are domain and forest secrets that are never replicated to an RODC.

## An Application

partition is a portion of the data store that contains objects required by an application or service that is outside of the core AD DS service. Unlike other partitions, application partitions can be targeted to replicate to specific domain controllers; they are not, by default, replicated to all DCs.

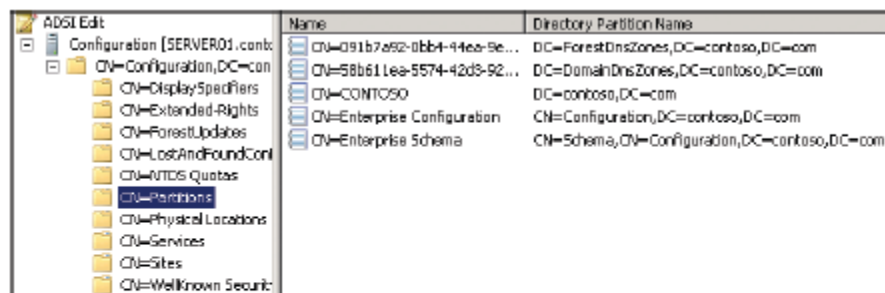
Application directory partitions are designed to support directory-enabled applications and services. They can contain any type of object except security principals such as users, computers, or security groups. Because these partitions are replicated only as needed, application directory partitions provide the benefits of fault tolerance, availability, and performance while optimizing replication traffic.

The easiest way to understand application directory partitions is to examine the application directory partitions maintained by Microsoft DNS Server. When you create an Active Directory–integrated zone, DNS records are replicated between DNS servers by using an application directory partition. The partition and its DNS record objects are not replicated to every domain controller, only to those acting as DNS servers.

To explore the application directory partitions in your forest:

1. Open ADSI Edit.
2. Right-click the root of the snap-in, ADSI Edit, and click Connect To.
3. In the Select A Well Known Naming Context drop-down list, choose Configuration, and then click OK.
4. Expand Configuration and the folder representing the Configuration partition, and then select the Partitions folder, CN=Partitions, in the console tree.

The details pane displays the partitions in your AD DS data store, as shown in Figure 11-9.



Name	Directory Partition Name
CN=091b7a92-0bb4-44ee-9e...	DC=ForestDnsZones,DC=contoso,DC=com
CN=58b611ea-5574-42d3-92...	DC=DomainDnsZones,DC=contoso,DC=com
CN=CONTOSO	DC=contoso,DC=com
CN=Enterprise Configuration	CN=Configuration,DC=contoso,DC=com
CN=Enterprise Schema	CN=Schema,CN=Configuration,DC=contoso,DC=com

FIGURE 11-9 Partitions in the contoso.com forest

Note the two application partitions in Figure 11-9, ForestDnsZones and DomainDnsZones. Most application partitions are created by applications that require them. DNS is one

example, and Telephony Application Programming Interface (TAPI) is another. Members of the Enterprise Admins group can also create application directory partitions manually by using *Ntdsutil.exe*.

An application partition can appear anywhere in the forest namespace that a domain partition can appear. The DNS partitions distinguished names—DC=DomainDnsZones, DC=contoso,DC=com, for example—place the partitions as children of the DC=contoso,DC=com domain partition. An application partition can also be a child of another application partition or a new tree in the forest.

Generally speaking, you use tools specific to the application to manage the application directory partition, its data, and its replication. For example, simply adding an Active Directory-integrated zone to a DNS server automatically configures the domain controller to receive a replica of the DomainDns partition. With tools such as *Ntdsutil.exe* and *Ldp.exe*, you can manage application directory partitions directly.

You should consider application partitions before demoting a domain controller. If a domain controller is hosting an application directory partition, you must evaluate the purpose of the partition, whether it is required by any applications, and whether the domain controller holds the last remaining replica of the partition, in which case, demoting the domain controller would result in permanent loss of all information in the partition. Although the Active Directory Domain Services Installation Wizard prompts you to remove application directory partitions, it is recommended that you manually remove application directory partitions before demoting a domain controller.