

E N T E R P R I S E  
D A D D Y



ACTIVE  
DIRECTORY  
BASICS

EXPLAINING AD TO IT  
PROFESSIONALS

# Contents

<b>Introduction</b> .....	<b>3</b>
<b>Active Directory and its components</b> .....	<b>4</b>
Domain Controllers .....	4
Grouping of Domain Controllers .....	5
Inside the Active Directory database .....	5
Objects .....	6
Containers and objects .....	6
Attributes .....	7
Replication and High Availability .....	7
Intrasite and intersite replication .....	8
Global Catalog servers .....	8
Flexible single-master operations .....	9
Functional levels .....	10
<b>Active Directory and its networking services</b> .....	<b>10</b>
DNS .....	10
DNS Domain Names .....	11
DNS Zones .....	11
DNS Records .....	11
DNS Servers .....	11
DHCP .....	12
DHCP Authorization .....	12
DHCP and Dynamic DNS .....	12
<b>Active Directory in the networking infrastructure</b> .....	<b>13</b>
Device-independent productivity .....	13
Single Sign-On .....	13
Centralized systems management .....	13
Consistent user experience .....	13
Distributed File System for optimized access to files .....	14
<b>Best practices when deploying Active Directory</b> .....	<b>14</b>
<b>Thank You So Much</b> .....	<b>16</b>

# Introduction

Microsoft's Active Directory offers a central way for IT systems administrators to manage user accounts and devices within an IT infrastructure network. Changes in Active Directory can be made by these administrators centrally for consistency across the environment. Through Active Directory, people enjoy benefits such as being able to log onto devices and into applications with the same combination of username and password (and optionally other methods of authentication) and use their settings and files across all devices that are members of Active Directory. Optionally, when a device is lost, defective or stolen, people can remain productive on another Active Directory-managed device.

# Active Directory and its Components

## Domain Controllers

On Microsoft Servers, a domain controller (DC) is a server that responds to security authentication requests (logging in, checking permissions, etc.) within the Windows Server domain.

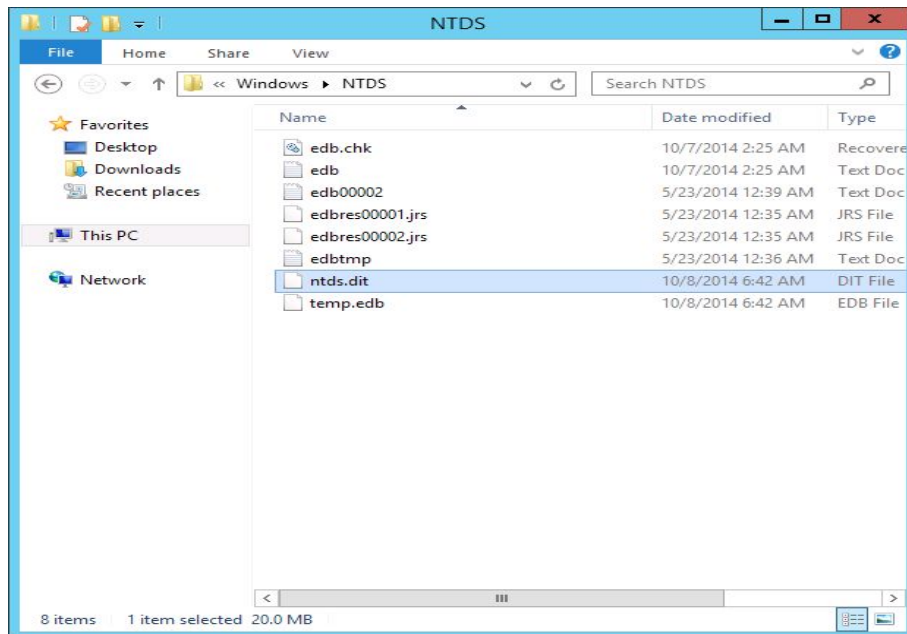
These are Windows Server installations equipped with the Active Directory Domain Services (AD DS) Server Role. Domain Controllers can be physical hosts and virtual machines.

The two most important elements of Domain Controllers are:

### 1. The Active Directory Database

The Active Directory database (ntds.dit) and its supporting files contain the definition of objects and the configuration of objects. Examples of objects are Containers, Organizational Units, user accounts and computer accounts.

The screenshot below shows you the Active Directory database (ntds.dit) and its supporting files on the file system of a Domain Controller:



Active Directory basics. Explaining Active Directory to IT professionals

## 2. The Active Directory System Volume

The Active Directory System Volume (SYSVOL) is an SMB-based network share, used to share files with Active Directory members.

There are two different types of domain controllers:

### 1. Read/write Domain Controllers

These Domain Controllers allow changes to their Active Directory databases and System Volumes from Active Directory members and can be used to bring changes to other Domain Controllers.

### 2. Read-only Domain Controllers

Read-only Domain Controllers are Domain Controllers that only allow read-access to their Active Directory databases and System Volumes. Changes are brought in by Read/write Domain Controllers.

## Grouping of Domain Controllers

Domain Controllers are grouped into sites, domains and forests. An Active Directory site, typically, represents a geographical site of high-speed connectivity. You may think of an Active Directory site as a building. Active Directory sites govern replication between Domain Controllers configured in Active Directory sites. By default, authentication traffic from within an Active Directory site is directed to a Domain Controller in that site. A Domain Controller can only be part of one Active Directory site at a time.

Active Directory domains are containers of replication. By default, all Domain Controllers in a domain can receive changes and replicate those changes to all other Domain Controllers in it. Each domain in Active Directory is identified by a Domain Name System (DNS) domain name.

An Active Directory forest is a collection of one or more Active Directory domains that share a common Active Directory schema.

Most Active Directory environments exist with one Active Directory domain in its own Active Directory forest.

## Inside the Active Directory database

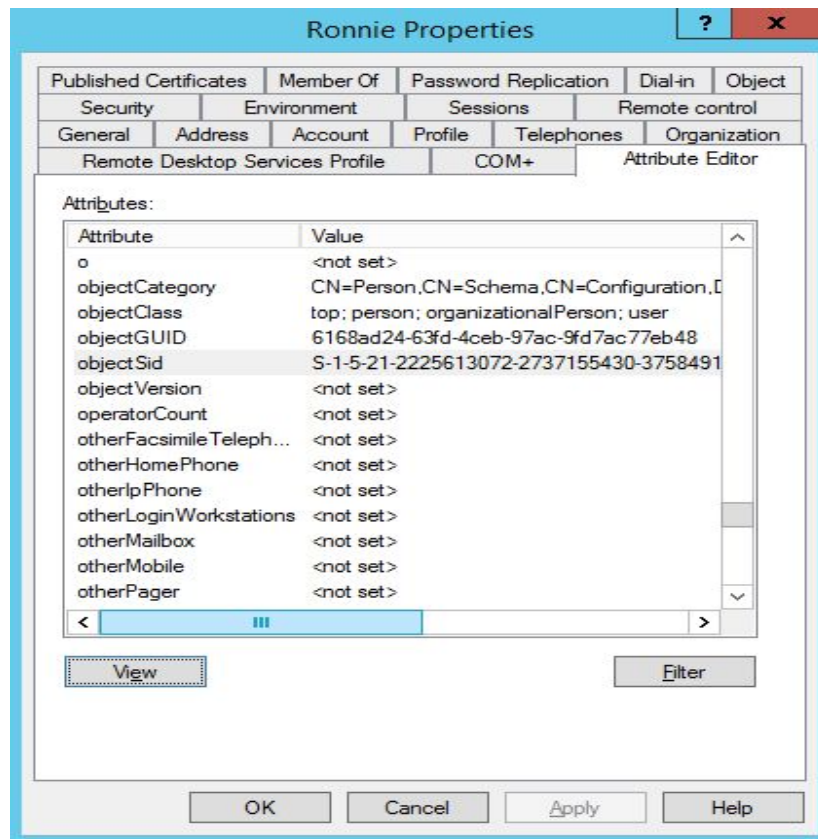
The Active Directory database consists of two types of data:

**The Active Directory schema** Objects are defined in the schema. This way, their behavior and relationships are shaped. For instance, the fact that a user account object can have a last name where a computer object cannot, is defined in the Active Directory schema.

**The Active Directory configuration** The objects themselves and the information in their properties (called attributes) are stored in the configuration part of the Active Directory database.

## Objects

Each object within the Active Directory configuration is identified with a security identifier, the SID. The security identifier consists of two parts: The domain identification part and the relative identifier, relative to the domain. In the screenshot below you can see the properties for the **Ronnie** user object (after the **Advanced Features** were enabled in the View menu of the **Active Directory Users and Computers** management tool).



The Security Identifier for the user object used by Ronnie is S-1-5-21-2225613072-2737155430-3758491199-1128. Its relative identifier is 1128.

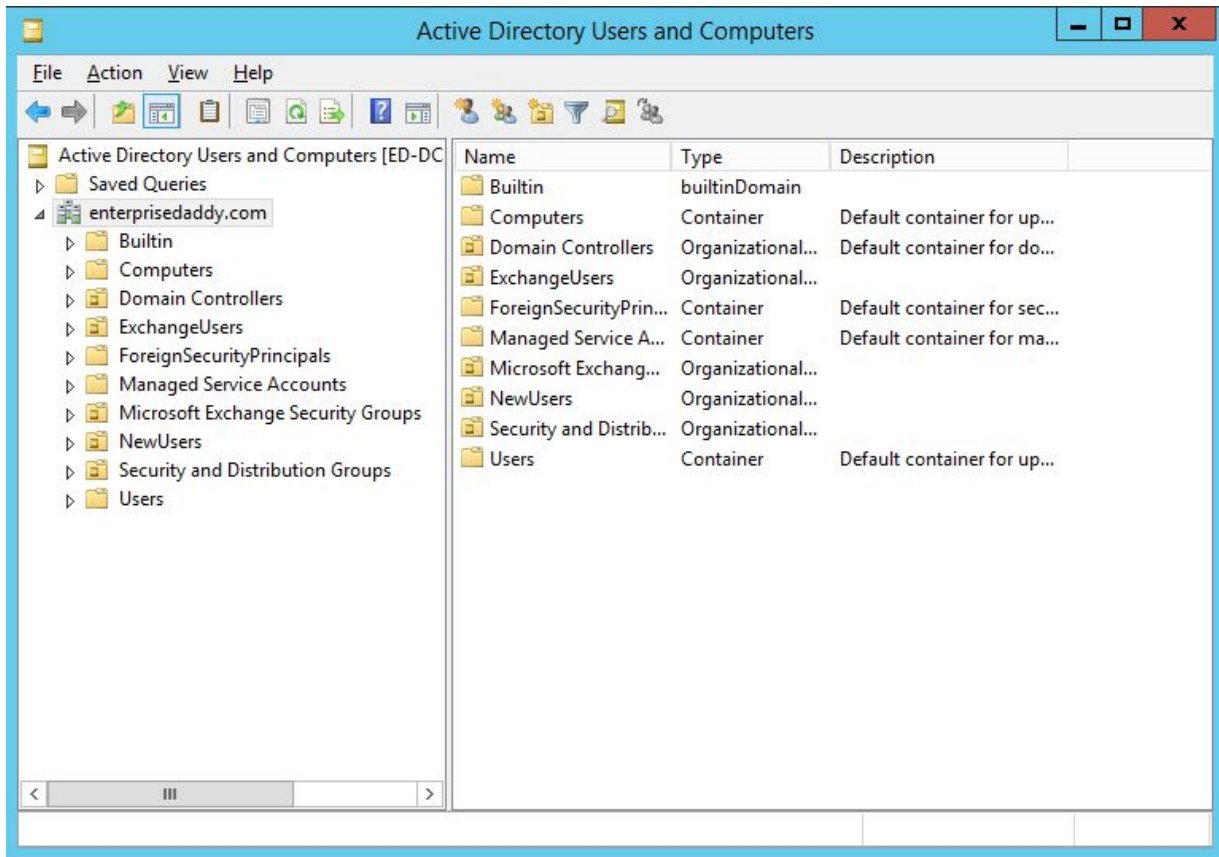
## Containers and objects

Although, strictly speaking, every object is a container in the world of Active Directory, only true container objects have objects under them. Organizational Units (OUs) and Containers (CNs) in the configuration part of the Active Directory database are represented in the Active Directory management tools as folders.

The differences between OUs and CNs is that the first can be used to deploy settings (through Group Policy Objects). The special thing about CNs is that you cannot delete them using standard tooling. Containers that are available in a default Active Directory environment are **Builtin**, **Users** and **Computers**.

Active Directory basics. Explaining Active Directory to IT professionals

In the screenshot of **Active Directory Users and Computers** below, you can see the Organizational Units and Containers for an Active Directory domain based on Windows Server 2012 R2 Domain Controllers:



The **Exchange Users**, **New Users**, **Security and Distribution Groups** and **Domain Controllers** Organizational Units (OUs) are clearly distinguishable from the containers by their icons.

## Attributes

Objects have properties based on the Active Directory schema. These properties are called attributes. Some attributes contain a single value such as the password last set attribute for a user object. Other attributes may contain multiple values such as the members attribute of a group object.

## Replication and High Availability

Active Directory High Availability is not based on Failover Clustering (like Hyper-V) or Log shipping (like Exchange and SQL Server). Instead, Domain Controllers all offer the Active Directory database and System Volume (SYSVOL) to whoever needs the information in it.

## Active Directory basics. Explaining Active Directory to IT professionals

When you deploy at least two Domain Controllers for an Active Directory domain, you'll gain redundancy and High Availability for that Active Directory domain. This requires a mechanism to keep the contents of this database in sync between Domain Controllers. Active Directory uses replication between Domain Controllers to keep things in sync.

Replication synchronizes changes that are made on one Domain Controller with all other Domain Controllers in scope of replication. Data integrity is maintained by tracking changes on each Domain Controller and updating other Domain Controllers systematically. Active Directory replication uses a connection topology that is created automatically by the Knowledge Consistency Checker (KCC) to reduce administrative effort, but can alternatively be modified manually.

### Intrasite and intersite replication

Referring back to the previously mentioned Active Directory sites, two types of replication exist:

#### **Intrasite replication**

Within an Active Directory site, replication is based on pull replication. After being notified of changes, a Domain Controller will ask the Domain Controller with the change what changes it has seen. To reduce network chatter, intrasite replication is setup by default as a two-way ring topology. This avoids Domain Controllers within a site to communicate to each of the other Domain Controllers. Instead, the ring topology allows it to communicate to two of its site siblings.

#### **Intersite replication**

Between Active Directory sites, replication is schedule-based and between bridgehead servers. After the default schedule time-out (15 minutes by default), the bridgehead Domain Controller for a site asks the bridgehead Domain Controller in the other site for the changes it has seen. Bridgehead Domain Controllers then replicate the changes to the Domain Controllers in its site using intrasite replication.

Replication is also where the schema and configuration parts of the Active Directory database come into play. The schema is replicated and used throughout an Active Directory forest, where larger parts of the configuration is only replicated among Domain Controllers of a domain.

### Global Catalog servers

The Active Directory databases of Domain Controllers configured as Global Catalog servers maintain all objects within a forest. These types of Domain Controllers store all attributes for all objects for the domain it is a Domain Controller for, but only the most important attributes for objects in the other domains in the forest. This allows for authorization within the Active Directory forest. For instance: The ability to add a group from another domain in a forest to the access control list of a file share in your domain.



## Flexible single-master operations

When it comes to replication, a couple of bottlenecks can be identified. Since all Domain Controllers are able to commit to the database simultaneously, replication collisions may occur. Therefore, Active Directory replication works with five Flexible Single Master Operations (FSMO) roles:

### **The Primary Domain Controller emulator**

The Domain Controller in the domain with the Primary Domain Controller emulator (PDCe) Flexible Single Master Operations (FSMO) role, is authoritative for the replication of password changes, group policy changes and Distributed File Services (DFS) changes. A Domain Controller will replicate these changes to the PDCe first, which in turn will replicate it to the other Domain Controllers. This way, when a colleague changes the password for a user object in a site across the globe, and I use the new password in my site, the PDCe will be able to tell me that the new password is correct even though the Domain Controller in my site has not received the change yet. The Domain Controller with the PDCe FSMO role also serves as the default time server for all other Domain Controllers in the domain.

### **The RID pool master**

SIDs, and thus RIDs, are used to create new objects. The Domain Controller with the RID pool Flexible Single Master Operations (FSMO) role is responsible for avoiding RID-based object creation collisions. To this purpose, it hands out 500-object RID pools to Domain Controllers within the Active Directory domain. When a Domain Controller depletes its 500-object RID pool, all it has to do is ask for a new pool.

### **The infrastructure master**

The Domain Controller with the Infrastructure Master Flexible Single Master Operations (FSMO) role is responsible for updating references from objects in its domain to objects in other domains. The infrastructure master compares its data with that of the previously mentioned Global Catalog servers. Domain Controllers configured as Global Catalog servers receive regular updates for objects in all domains through replication, so the Global Catalog data will always be up to date. If the infrastructure master finds data that is out of date, it requests the updated data from a global catalog. The infrastructure master then replicates that updated data to the other Domain Controllers in the domain.

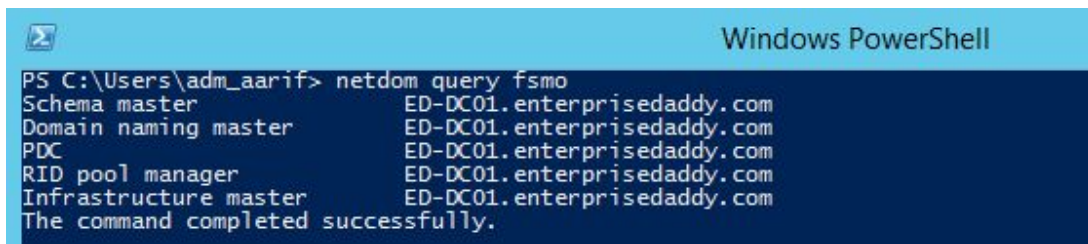
### **The schema master**

The Domain Controller with the Schema Master Flexible Single Master Operations (FSMO) role is responsible for the integrity of the Active Directory schema. Since schema changes impact all objects on all Domain Controllers within an Active Directory forest, changes to the Active Directory schema occur on the Domain Controller with the Schema Master Flexible Single Master Operations (FSMO) role and replicated from there.

### The domain naming master

The second forest-wide Flexible Single Master Operations (FSMO) role is the Domain Naming Master role. The Domain Controller holding this role is authoritative for the Active Directory domains within an Active Directory forest. When you add or remove a domain to a forest, the change originates from the Domain Controller holding the Schema Master Flexible Single Master Operations (FSMO) and replicates from there.

Using the **netdom query fsmo** command, you can quickly find out the Domain Controllers holding the Flexible Single Master Operations (FSMO) roles in an Active Directory environment:



```
Windows PowerShell
PS C:\Users\adm_aarif> netdom query fsmo
Schema master           ED-DC01.enterprisedaddy.com
Domain naming master    ED-DC01.enterprisedaddy.com
PDC                     ED-DC01.enterprisedaddy.com
RID pool manager        ED-DC01.enterprisedaddy.com
Infrastructure master   ED-DC01.enterprisedaddy.com
The command completed successfully.
```

## Functional levels

Active Directory domains and forests are configured with a functional level. These levels govern the minimum Windows Server Operating System (OS) version for Domain Controllers. Raising these levels unlock new functionality.

When you raise the Active Directory Domain Functional Level (DFL), you remove the ability to run and promote Windows Servers below that version in the Active Directory domain. You can only upgrade when all Domain Controllers with earlier Windows Server versions are removed from the domain or upgraded.

After all Active Directory domains in an Active Directory forest have their Domain Functional Level (DFL) raised to a certain version, you can raise the Active Directory Forest Functional Level (FFL) for the forest.

## Active Directory and its networking services

### DNS

Active Directory relies heavily on the Domain Naming System (DNS). First of all, each Active Directory domain is represented by a DNS domain name. Within an Active Directory forest, multiple domains may share a common

Active Directory basics. Explaining Active Directory to IT professionals

DNS name tree or have separate DNS domain names. Secondly, Active Directory-joined devices use DNS to locate Active Directory services like Domain Controllers.

You might already know a lot about DNS since it is commonly used on the internet. It is used to find the IPv4 and IPv6 addresses to websites you want to visit. In relation to Active Directory, there's a little more to it:

## DNS Domain Names

The Domain Naming System (DNS) is a hierarchical naming system. Its highest level is the root. Beneath the root you'll find top level domains (TLDs), like .com, .net and .org. Then, there's the domain name portion, which can be registered: EnterpriseDaddy.com is a registered domain name for the company named Enterprise Daddy.

When an Active Directory domain is created, a DNS domain name must be specified.

Microsoft's best practice is to register a domain name on the internet and use that, or an internal sub-domain beneath it, as the Active Directory DNS domain name. This provides the best interoperability and connectivity to the outside world.

## DNS Zones

For each of the hierarchical layers in the Domain Naming System (DNS), two corresponding DNS zone types exist:

### Forward Lookup Zones

DNS Forward Lookup Zones contain information on DNS records that allow you to convert a DNS name to IPv4 and IPv6 addresses.

### Reverse Lookup Zones

DNS Reverse Lookup Zones perform the reverse job of Forward Lookup Zones. It allows for DNS clients to get a DNS name for a specific IPv4 or IPv6 address.

## DNS Records

DNS Zones contain DNS Records. In DNS Forward Lookup Zones, A and AAAA records contain information on the IPv4 and IPv6 addresses associated to certain hostnames, like www.DNS Forward Lookup Zones used by Active Directory typically contain a lot of SRV records to point to IPv4 and IPv6 addresses for Active Directory functionality like Domain Controllers configured as Global Catalog servers.

In DNS Reverse Lookup Zones, PTR records contain DNS names for certain IPv4 and IPv6 addresses.

## DNS Servers

The Domain Naming System (DNS) is offered through DNS Servers. These are the servers that are queried by domain-joined devices. While you can use stand-alone DNS Servers, Active Directory offers Active Directory integration for DNS. This way, Domain Controllers double as DNS Servers and the information in the DNS zones

## Active Directory basics. Explaining Active Directory to IT professionals

are replicated between them in the same way the Active Directory configuration is replicated. This offers some benefits:

On traditional DNS Servers, changes can only be made on Primary DNS Servers. Changes are then transferred to Secondary DNS Servers. Information in Active Directory-integrated DNS Zones can be modified on each of the Domain Controllers acting as DNS Servers.

On traditional DNS Servers, changes in DNS Zones are transferred by transferring the entire DNS Zones. Information in Active Directory-integrated DNS Zones is replicated on a per-record basis, vastly reducing the amount of network traffic and time required for DNS updates.

## DHCP

Although the Dynamic Host Configuration Protocol (DHCP) is not a requirement for Active Directory, it is commonly used in Active Directory environments for its flexibility.

Through the Dynamic Host Configuration Protocol (DHCP), devices on a network can automatically configure their IPv4 and IPv6 addressing information by negotiating this information with DHCP Servers.

DHCP is used extensively in environments with and without Active Directory. Your Internet Service Provider (ISP) uses it to configure your router without Active Directory. However, using DHCP within an environment with Active Directory offers several benefits:

### DHCP Authorization

In an Active Directory environment, domain-joined devices acting as DHCP servers need to be authorized in Active Directory. Without this authorization, DHCP will not offer addressing information. This is helpful to protect against devices that offer addressing information that point devices to other routers and DNS Servers than your DHCP Servers.

### DHCP and Dynamic DNS

Authorized DHCP Servers offer automatic registration and updating of DNS records within Active Directory-integrated DNS Zones, both Forward Lookup Zones and Reverse Lookup Zones. This way, information in DNS is kept up to date without administrative effort.

# Active Directory in the networking infrastructure

## Device-independent productivity

Every colleague with a user account in Active Directory is able to sign into every domain-joined device with the credentials and authentication methods associated with that user account. Of course, servers are not considered standard devices and administrators can further limit the scope of devices for colleagues.

When a device is lost, defective or stolen, people can simply sign into another Active Directory-managed device and be productive on it.

## Single Sign-On

Once signed into a domain-joined device with an Active Directory user account, colleagues benefit from Single Sign-On (SSO) into Active Directory-integrated applications, files and services.

When a colleague signs into a device, their credentials are sent to the Local Security Authority Subsystem Service (lsass.exe). This service is responsible for providing the Single Sign-On experience for the colleague. LSASS hosts a number of plug-ins representing the protocols that Windows supports including NTLM authentication, Digest authentication and Kerberos. Credentials are presented to each of these plugins, producing one-way hashes and tickets in the memory space of LSASS, which would remain there for the duration of the user session. During this session, the colleague benefits of Single Sign-On to all Active Directory-integrated applications, files and services.

## Centralized systems management

Using Group Policy Objects (GPOs), administrators can govern settings on domain-joined devices. Administrators can centrally configure settings for applications and services, and also settings that govern how Windows looks and feels.

In addition to the functionality offered by Group Policy Objects (GPOs), Group Policy Preferences (GPPs) can be used to replace legacy startup, shutdown, logon and logoff scripts.

## Consistent user experience

User profiles, Home folders and Folder redirection can be used to synchronize files and settings between devices and file servers. This way, all these settings are backed up automatically on the file server and thus

Active Directory basics. Explaining Active Directory to IT professionals

protected against data loss on the device level. Also, on any new domain-joined device a colleague logs on, these files and settings are automatically synced back from the file server, offering a consistent user experience.

## Distributed File System for optimized access to files

The Distributed File System (DFS) File Server Role Service can be used in conjunction with Active Directory sites to synchronize files and folders between file servers located in different Active Directory sites and pointing domain-joined devices to the file server located in their Active Directory site.

The System Volume (SYSVOL) file share on Domain Controllers is the most prominent example of the Distributed File System (DFS) model, exposing the data in it to domain-joined devices efficiently, based on Active Directory sites.

## Best practices when deploying Active Directory

With Active Directory entrenched in every major aspect of networking infrastructures, there's an urgency to deploy Active Directory and Domain Controllers correctly. Below is my list of pointers to achieve this:

- Intend to create at least two (equal) Domain Controllers per domain.
- Intend to implement Role Separation. By all means do not misuse a Domain Controller as an Exchange Server or SQL Server, unless it's a Windows Small Business Server.
- Properly dimension the server in terms of hardware and software. Use RAID and separate spindles for storage of Active Directory-related data when possible. Use the [Infrastructure Planning and Design \(IPD\) Guide](#) for Active Directory to this purpose.
- Use hardware and software still covered by the producers (extended) guarantee, support, and/or life cycle policy for the period in which you need to rely on the Domain Controller. Additionally, I strongly recommend Windows Server 2012 as the Operating System for newly deployed Domain Controllers.
- When the server is a virtual machine, have the correct procedures in place. Always run sysprep.exe when working with Windows Server templates.
- Before you install Windows Server, run the Memory Diagnostics from the Windows Server DVD. Possible memory corruption issues show early this way and this will minimize issues further on in the lifetime of the server.
- Document the passwords for the DSRM accounts on each of your Domain Controllers on the password list for your organization. You will need these passwords in disaster recovery scenarios.

## Active Directory basics. Explaining Active Directory to IT professionals

- Implement Information Security measures (anti-malware and UPS client software) according to the best practices of the manufacturer for Domain Controllers. Make exclusions for the Active Directory database and supporting files.
- To promote Domain Controllers, use answer files. Write them, get them checked, signed off and then use them. Include them in your documentation after you've used them since the passwords will be stripped by the server after usage.
- After promotion, check dcpromo.log, dcpromoui.log and event viewer for issues.
- Run Windows Update after promotion. You will only be offered Active Directory-specific updates after promoting a Windows Server installation to a Domain Controller.
- Configure system state backups to run periodically. Don't forget to configure regular separate backups of GPOs and Starter GPOs through the Group Policy Management Console since these won't be as easy to recover granularly.
- Run the Active Directory Best Practices Analyzer regularly.

## Thank You So Much!

I hope you've enjoyed this eBook as much as I loved writing it for you. I can't thank you enough for your continued support of Enterprise Daddy Blog and everything I do. I appreciate each and every one of you for taking time out of your day or evening to read this, and if you have an extra second, **I would love to hear what you think about it.** Please leave a comment at <http://www.enterpisedaddy.com/ebook>, or if you'd rather reach me in private, don't hesitate to shoot me an email. I read each and every single comment and email, so don't be afraid to say hi! Lastly, if you haven't already, you can follow me on Twitter (@adilarif001), and join in on the conversations going on right now on my [Facebook Fan Page](#)

Cheers,

Adil Arif

[adilarif@enterpisedaddy.com](mailto:adilarif@enterpisedaddy.com)