6

Managing Active Directory

In this chapter, we cover the following recipes:

* Installing an AD forest root domain
* Testing an AD installation
* Installing a replica domain controller
* Installing a child domain
* Creating and managing AD users and groups
* Managing AD computers
* Adding/removing users using CSV files
* Creating group policy objects
* Reporting on AD replication
* Reporting on AD computers
* Reporting on AD users

# Introduction

This is the chapter intro blah blah blah

* **One thing:** This allows you to issue
* **Another thing**: This feature does stuff too
* **Etc**: b;aju

## Systems used in this chapter

Each chapter shows the systems Like this:

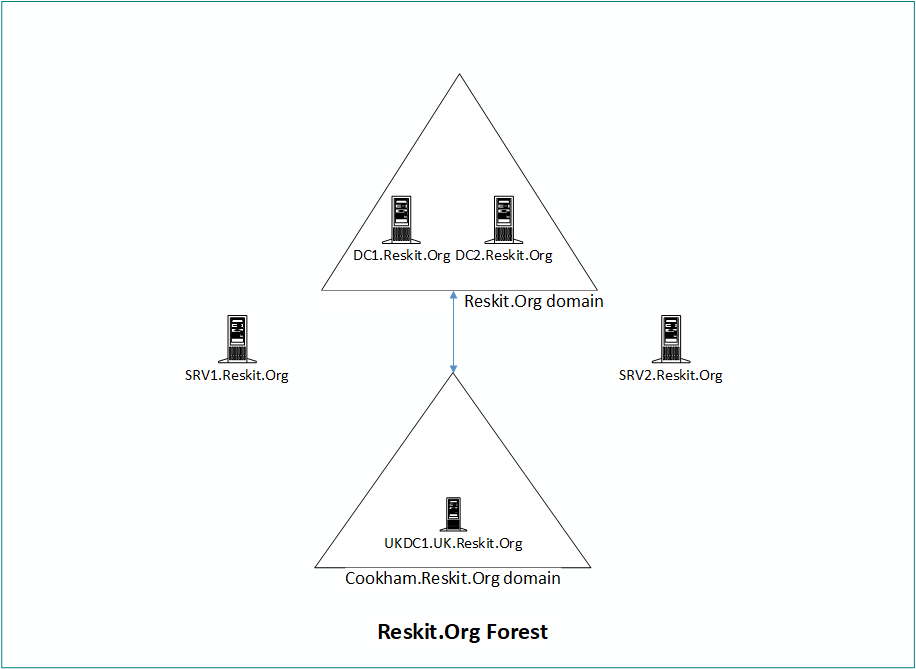


Figure 6.1: Reskit.Org forest diagram

Insert image B42024\_11\_01.png

You can use Hyper-V **virtual machines** (**VMs**) to implement this forest. To build these servers, you can get the build scripts from <https://github.com/doctordns/ReskitBuildScripts>. Each recipe in the chapter sets out the specific servers to use. You build new VMs as you need them.

# Installing an AD forest root domain

You create an AD forest by creating your first domain controller. Installing Active Directory and DNS has always been reasonably straightforward. You can always use the Server Manager GUI, but using PowerShell is also straightforward.

To create a DC, you start with a system running Windows Server. You then add the AD DS Windows feature to the server. Finally, you create your first DC, for example, a single domain controller, DC1.Reskit.Org, for the Reskit.Org domain.

## Getting ready

You run this recipe on DC1, a workgroup server on which you have installed PowerShell 7 and VS Code. You install this server as a workgroup server using the build scripts at https://github.com/doctordns/ReskitBuildScripts.

## How to do it...

1. Installing the AD Domain Services feature and management tools

Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

st

1. Importing the ADDSDeployment module:

Import-Module -Name ADDSDeployment

1. Examining the commands in the ADDSDeployment module

Get-Command -Module ADDSDeployment

1. Creating a secure password for Administrator

$PSSHT = @{

  String      = 'Pa$$w0rd'

  AsPlainText = $true

  Force       = $true

}

$PSS = ConvertTo-SecureString @PSSHT

1. Testing DC forest installation starting on DC1

$FOTHT = @{

  DomainName           = 'Reskit.Org'

  InstallDNS           = $true

  NoRebootOnCompletion = $true

  SafeModeAdministratorPassword = $PSS

  ForestMode           = 'WinThreshold'

  DomainMOde           = 'WinThreshold'

}

Test-ADDSForestInstallation @FOTHT -WarningAction SilentlyContinue

1. Creating forest root DC on DC1

$ADHT = @{

  DomainName                    = 'Reskit.Org'

  SafeModeAdministratorPassword = $PSS

  InstallDNS                    = $true

  DomainMode                    = 'WinThreshold'

  ForestMode                    = 'WinThreshold'

  Force                         = $true

  NoRebootOnCompletion          = $true

  WarningAction                 = 'SilentlyContinue'

}

Install-ADDSForest @ADHT

1. Checking key AD and related services

Get-Service -Name DNS, Netlogon

1. Checking DNS zones

Get-DnsServerZone

1. Restart DC1 to complete promotion

Restart-Computer -Force

## How it works...

In step 1, you install the AD Domain Services feature. This feature enables you to deploy a server as a domain controller. The output of this command looks like this:

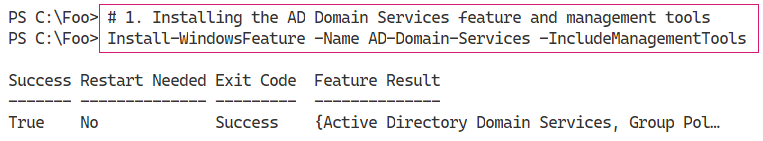


Figure 6.2: Installing the AD DS feature

1. Insert image B42024\_06\_01.png

In step 2, you manually import the ADDSDeployment module. Since PowerShell does not support this module natively, this step loads the module using the Windows PowerShell Compatibility feature. The output of this command looks like this:

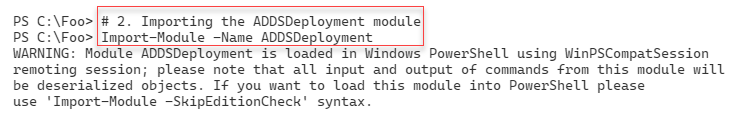


Figure 6.3: Importing the ADDSDeployment module

1. Insert image B42024\_06\_02.png

In step 3, you use the Get-Command cmdlet to discover the commands contained in the ADDSDeployment module, which looks like this:

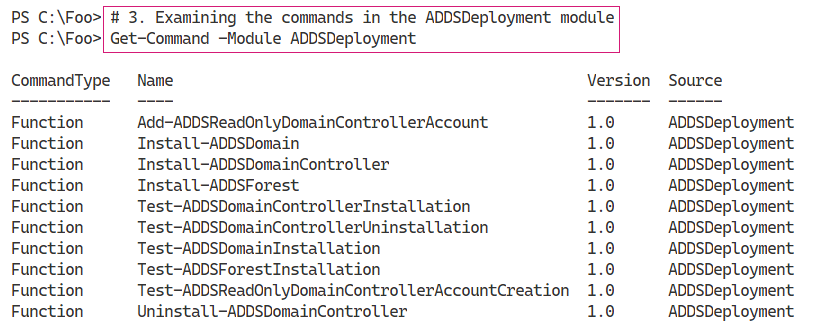


Figure 6.4: Examining commands in the ADDSDeployment module

1. Insert image B42024\_06\_03.png

With step 4, you create a secure string password to use as the Administrator password in the domain you are creating. This step produces no output.

Before you promote a server to be a DC, it’s useful to test to ensure that a promotion would be successful as far as possible. In step 5, you use the Test-ADDSForestInstallation command to check whether you can promote DC1 as a DC in the Reskit.Org domain. The output of this command looks like this:

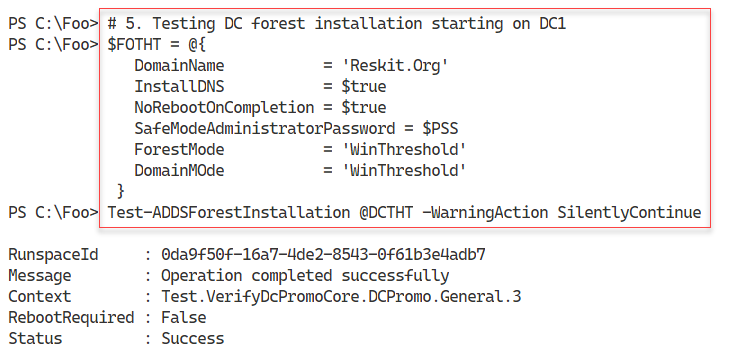


Figure 6.5: Testing DC forest installation

1. Insert image B42024\_06\_04.png

In step 6, you promote DC1 to be the first domain controller in a new domain, Reskit.Org. The output looks like this:

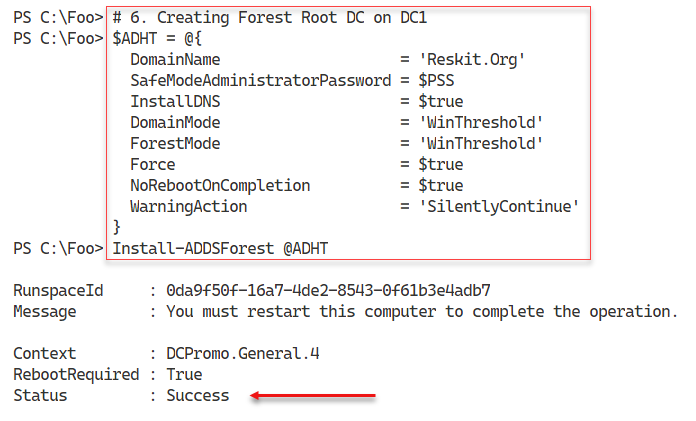


Figure 6.6: Creating a forest root DC on DC1

1. Insert image B42024\_06\_05.png

After the promotion is complete, you can check the critical services required for Active Directory. Checking the Netlogon and DNS services, which you do in step 7, should look like this:

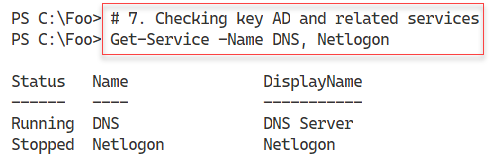


Figure 6.7: Checking the Netlogon and DNS services

1. Insert image B42024\_06\_06.png

When you promoted DC1, you also requested the promotion to install DNS on DC1. In step 8, you check on the zones created by the DC promotion process, which looks like this:

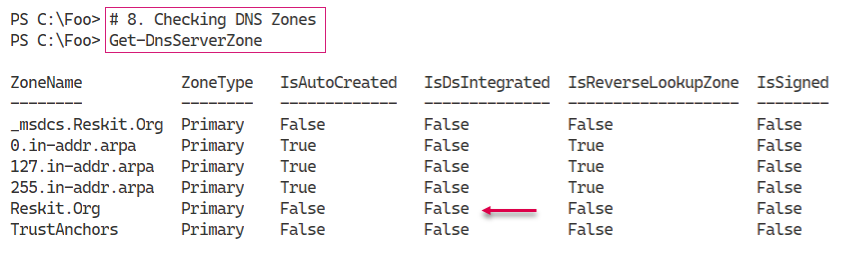


Figure 6.8: Checking DNS zones

1. Insert image B42024\_06\_07.png

You need to reboot DC1 to complete the promotion process, which you do in step 9, generating no actual output.

## There’s more...

The cmdlets that enable you to promote a server to be a DC are not installed on a server system by default. Adding the Active Directory Domain Services Windows feature, in step 1, adds the necessary cmdlets to the system.

In step 6, you install AD and direct that a DNS server should also be installed – and you check for its presence in step 7. In step 8, you view the DNS zones created automatically by the promotion process. You specify the DNS domain name, Reskit.Org, using the DomainName parameter to Install‑ADDSForest. This step creates the DNS domain, but it is, at this point, still a non-AD-integrated zone. Once you reboot the service, this zone should become AD-integrated (and set for secure updates only).

Once you complete the verification of a successful AD installation, you reboot the server. After the restart, there are further tests that you should run, as we show in the next recipe, Testing an AD installation.

# Testing an AD installation

In Installing an AD forest root domain, you installed AD on DC1. In that recipe, you installed AD (without rebooting) and tested certain services. After the required reboot (which you completed at the end of the previous recipe), it is useful to check to ensure that your domain is fully up and running and working correctly. In this recipe, you examine core aspects of the AD infrastructure on your first DC.

## Getting ready

You run this recipe on DC1, the first domain controller in the Reskit.Org domain, after you have promoted it to be a DC. You created DC1 as a domain controller in the Reskit.Org domain in Installing an AD forest root domain. Log on as Reskit\Administrator.

## How to do it...

1. Examining AD root **directory service entry** (**DSE**)

Get-ADRootDSE -Server DC1.Reskit.Org

1. Viewing AD forest details

Get-ADForest

1. Viewing AD domain details

Get-ADDomain

1. Checking Netlogon, ADWS, and DNS services

Get-Service NetLogon, ADWS, DNS

1. Getting initial AD users

Get-ADUser -Filter \* |

  Sort-Object -Property Name |

    Format-Table -Property Name, DistinguishedName

1. Getting initial AD groups

Get-ADGroup -Filter \*  |

  Sort-Object -Property Groupscope, Name |

    Format-Table -Property Name, GroupScope

1. Examining Enterprise Admins group membership

Get-ADGroupMember -Identity 'Enterprise Admins'

1. Checking DNS zones on DC1

Get-DnsServerZone -ComputerName DC1

1. Testing domain name DNS resolution

Resolve-DnsName -Name Reskit.Org

## How it works...

After you’ve completed the installation of AD and rebooted, in step 1, you examine the AD DSE, which looks like this:

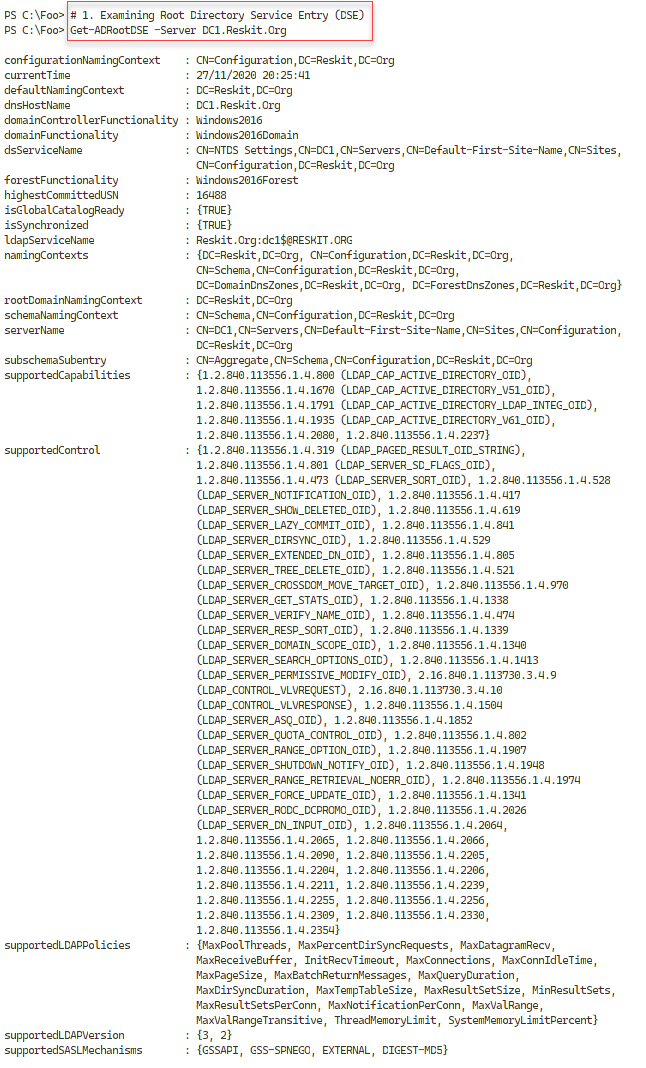


Figure 6.9: Examining the AD Directory Service Entry (DSE)

1. Insert image B42024\_06\_08.png

In step 2, you use the Get-ADForest command to review further information on the newly created forest, which looks like this:

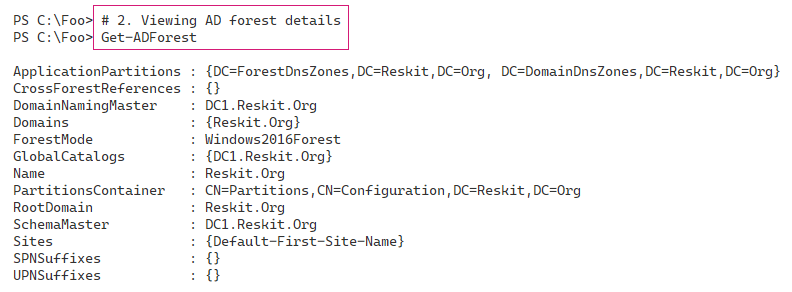


Figure 6.10: Viewing the AD forest details

1. Insert image B42024\_06\_09.png

In step 3, you use Get-ADDomain to return more information about the Reskit.Org domain, which looks like this:



Figure 6.11: Viewing AD domain details

Insert image B42024\_06\_10 .png

The AD services run within the Netlogon Windows service. The ADWS service is a web service used by the PowerShell AD cmdlets to communicate with the AD. AD relies on DNS as a locator service enabling AD clients and DCs to find DCs. All three must be up and running for you to manage AD using PowerShell. In step 4, you check all three services, which looks like this:

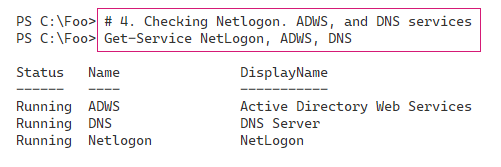


Figure 6.12: Checking the Netlogon, ADWS, and DNS services

Insert image B42024\_06\_11 .png

In Installing an AD forest root domain, you promoted DC1, a Windows server, to be a DC. In doing so, the promotion process creates three domain users: Administrator, Guest, and the krbtgt (Kerberos Ticket-Granting Ticket) user. You should never touch the krbtgt user and should usually leave the Guest user disabled. For added security, you can rename the Administrator user to something less easy to guess and create a new, very low-privilege user with the name Administrator.

In step 5, you examine the users in your newly created AD forest, which looks like this:

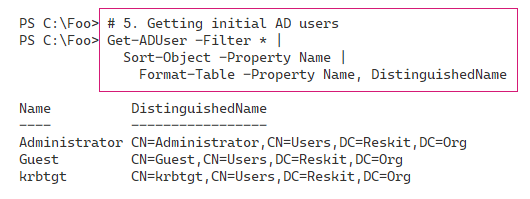


Figure 6.13: Getting initial AD users in the new AD forest

Insert image B42024\_06\_12 .png

The DC promotion process also creates several groups that can be useful. In step 6, you examine the different groups created (and their scope), which looks like this:

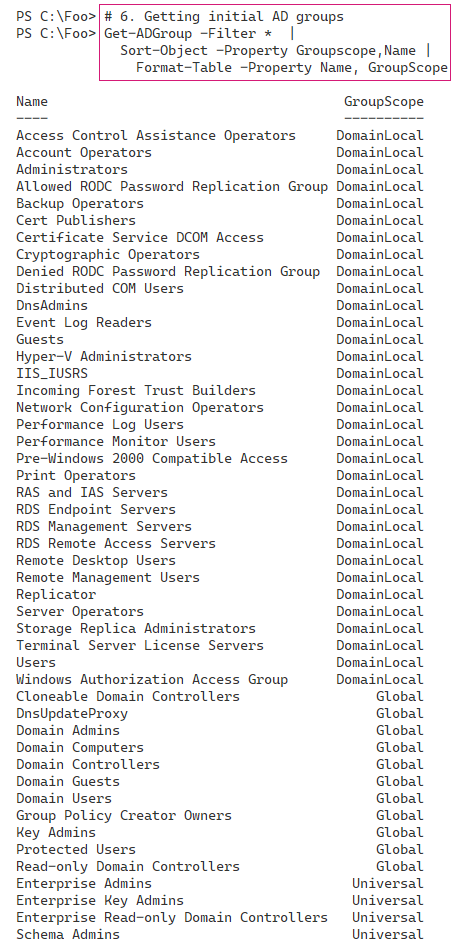


Figure 6.14: Examining initial AD groups and their scope

Insert image B42024\_06\_13 .png

The Enterprise Admins group is one with very high privilege. Members of this group can perform just about any operation across the domain – stop/start services, modify the AD, and access any file or folder on the domain or any domain-joined system. In step 7, you examine the initial members of this high-privilege group, which looks like this:

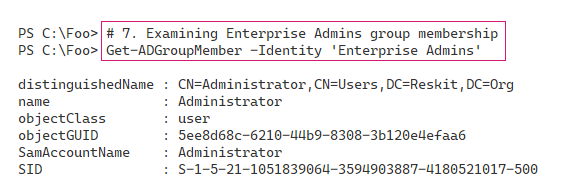


Figure 6.15: Examining Enterprise Admins group membership

Insert image B42024\_06\_14 .png

AD relies on DNS to enable an AD client or AD DC to find DCs. When you install a DC, you can also install the DNS service at the same time. When you install a DC with DNS, the AD promotion process creates several DNS zones in your newly created DNS service. In step 8, you examine the DNS zones created on DC1, which looks like this:

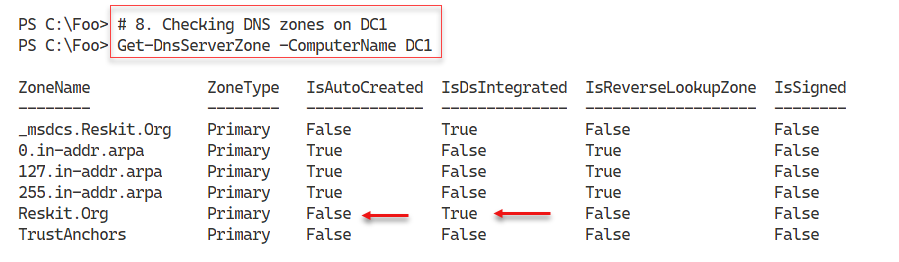


Figure 6.16: Checking the DNS zones created on DC1

Insert image B42024\_06\_15 .png

Another good test of your newly promoted DC is to ensure you can resolve the DNS name of your new domain (Reskit.Org). In step 9, you use the Resolve-DnsName to check, which looks like this:

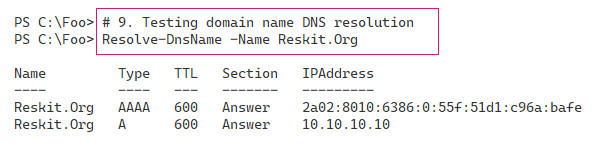


Figure 6.17: Testing domain name DNS resolution

Insert image B42024\_06\_16 .png

## There’s more…

In step 1, you viewed the DSE for your domain. The AD implements a **Lightweight Directory Access Protocol** (**LDAP**) directory service for domain activities. The DSE is a component of LDAP directories and contains information about your directory structure. The DSE is available without requiring authentication and contains much information about your AD forest. That information could help an attacker; thus, best practice is never to expose an AD DC to the Internet if you can help it. For a more detailed look at the root DSE, see https://docs.microsoft.com/windows/win32/adschema/rootdse.

The ADWS service, which you investigate in step 4, implements a web service. The AD commands use this web service to get information from and make changes to your AD. If this service is not running, AD commands do not work. You should always check to ensure the service has started before proceeding to use the AD cmdlets.

In step 6, you saw the groups created by the promotion process. These groups have permissions associated and thus are useful. Before adding users to these groups, consider reviewing the group and determining (and possibly changing) the permissions and rights assigned to these groups.