DNS WINDOWS

Descargar PDF

En este documento se describen los **comandos PowerShell más habituales para la instalación y configuración del servicio DNS** en Windows Server. No se incluye la configuración mediante la consola gráfica (DNS Manager), aunque es posible realizar todas las tareas desde esa interfaz.

Para direccionar a un equipo en una red interna o en Internet resulta difícil usar solo la IP. Cuando la red crece (o en el caso de Internet) esta tarea se vuelve impracticable. Por eso existe el servicio DNS, que no es más que una base de datos distribuida que permite localizar la IP de cualquier equipo en una red o en Internet mediante un nombre. Este proceso se conoce como resolución directa. También es posible localizar un nombre dado la IP; a esto se le llama resolución inversa.

Un servidor DNS consiste en un conjunto de zonas que contienen archivos utilizados para la resolución directa de nombres y la resolución inversa de IPs.

En las versiones Server de Windows (por ejemplo Windows Server 2019), disponemos de la característica o rol de servidor DNS. A continuación se muestran tablas y comandos habituales para la instalación y configuración básica del servicio DNS mediante PowerShell.

INSTALACIÓN DEL SERVICIO DNS

Los comandos relacionados con la instalación y gestión del rol del servidor DNS son los siguientes:

- `Install-WindowsFeature <rol> [-IncludeManagementTools]`
  Instala la característica o rol especificado. Opcionalmente se puede indicar que se instalen las herramientas de administración.

  Instalar servidor DNS

  Instalación del rol de servidor DNS sin herramientas de administración.

  ```
  PS C:\> Install-WindowsFeature DNS
  Success Restart Needed Exit Code      Feature Result
  ------- -------------- ---------      --------------
  True    No             Success        {Servidor DNS}
  ```

- `Get-WindowsFeature [<rol>]`
  Muestra información de un rol o característica dada; indica si está instalado o no y si está disponible. Si no se pasa ningún parámetro muestra el estado de todos los roles o características de Windows.

  Verificar instalación DNS

  Verificar si el rol de DNS está instalado.

  ```
  PS C:\> Get-WindowsFeature DNS
  Display Name                                            Name                       Install State
  ------------                                            ----                       -------------
  [X] Servidor DNS                                        DNS
  ```

- `Remove-WindowsFeature <rol>`
  Desinstala la característica o rol especificado.

GESTIÓN DE ZONAS

Los comandos para la gestión de zonas DNS son los siguientes:

- `Add-DnsServerPrimaryZone -Name <nombre-zona> -ZoneFile <nombre-archivo-resolución-zona>`
  Añade una zona primaria de resolución directa con un nombre de zona y un archivo de zona dados.

  Crear zona primaria directa

  Crear la zona primaria para el dominio `midominio.dom` con el archivo de zona `midominio.dom.dns`.

  ```
  PS C:\> Add-DnsServerPrimaryZone -Name "midominio.dom" -ZoneFile "midominio.dom.dns"
  ```

- `Add-DnsServerPrimaryZone -NetworkID <ip-red/prefijo-red> -ZoneFile <nombre-archivo-resolución-zona>`
  Añade una zona primaria de resolución inversa para una red y un nombre de archivo de resolución dados.

  Crear zona primaria inversa

  Crear la zona primaria de resolución inversa para la red `192.168.1.0/24`.

  ```
  PS C:\> Add-DnsServerPrimaryZone -NetworkId 192.168.1.0/24 -ZoneFile "1.168.192.in-addr.arpa.dns"
  ```

- `Get-DnsServerZone`
  Muestra todas las zonas existentes en el servidor DNS. También indica si la zona se creó manualmente o automáticamente.

  Mostrar zonas creadas

  Mostrar todas las zonas de resolución creadas.

  ```
  PS C:\> Get-DnsServerZone | Format-Table -AutoSize

   ZoneName                ZoneType IsAutoCreated IsDsIntegrated IsReverseLookupZone IsSigned
   --------                -------- ------------- -------------- ------------------- --------
   0.in-addr.arpa          Primary True           False          True                False
   1.168.192.in-addr.arpa  Primary False          False          True                False
   127.in-addr.arpa        Primary True           False          True                False
   255.in-addr.arpa        Primary True           False          True                False
   midominio.dom           Primary False          False          False               False
  ```

- `Remove-DnsServerZone -Name <nombre-zona>`
  Elimina la zona especificada.

GESTIÓN DE REGISTROS DE RECURSOS

Los comandos para la gestión de los registros de recursos en las zonas DNS son los siguientes:

- `Add-DnsServerResourceRecordA -Name <nombre-dns> -ZoneName <zona> -Ipv4Address <ip> [-CreatePtr]`
  Añade un **registro de recurso tipo A** (host address) a una zona directa. Se especifica el nombre DNS corto (no FQDN) y la IP asociada. El parámetro opcional `-CreatePtr` hace que el servidor DNS cree automáticamente el **registro PTR** correspondiente en la zona inversa.

  Añadir registro A

  Añadir registro A `www` para `midominio.dom` con IP `192.168.1.4` y crear automáticamente el registro PTR.

  ```
  PS C:\> Add-DnsServerResourceRecordA -Name www -ZoneName "midominio.dom" -IPv4Address 192.168.1.4 -CreatePtr
  ```

- `Add-DnsServerResourceRecordAAAA -Name <nombre-dns> -ZoneName <nombre-zona> -Ipv6Address <ip> [-CreatePtr]`
  Añade un **registro AAAA** (IPv6) a una zona directa. Opcionalmente crea el PTR en la zona inversa.
- `Add-DnsServerResourceRecordCNAME -Name <nombre-dns> -HostNameAlias <nombre-dns-fqdn> -ZoneName <nombre-zona>`
  Añade un **registro CNAME** (alias). Se especifica el nombre del alias y el FQDN del host canónico.

  Añadir registro CNAME

  Añadir alias `w3` apuntando a `www.midominio.dom`.

  ```
  PS C:\> Add-DnsServerResourceRecordCName -Name w3 -HostNameAlias "www.midominio.dom" -ZoneName "midominio.dom"
  ```

- `Add-DnsServerResourceRecordPtr -Name <ip-parte-host> -ZoneName <zona-inversa> -PtrDomainName <nombre-dns-fqdn>`
  Añade un **registro PTR** en una zona inversa. En PTR se indica la parte host de la IP y el FQDN correspondiente.

- `Add-DnsServerResourceRecordMX -Name <nombre-serv-correo> -MailExchange <nombre-dns-fqdn> -ZoneName <nombre-zona> -Preference <valor>`
  Añade un **registro MX** (Mail Exchanger). `-Preference` indica la prioridad (por defecto 10). `-MailExchange` debe corresponder a un nombre que tenga un registro A.

  Añadir registro MX

  Añadir un servidor de correo `correo` para `midominio.dom` con prioridad 15.

  ```
  PS C:\> Add-DnsServerResourceRecordMX -Name correo -ZoneName "midominio.dom" -MailExchange "correo.midominio.dom"  -Preference 15
  ```

- `Add-DnsServerResourceRecord -Name <nombre> -ZoneName <nombre-zona> -<tipo-registro> [<opción1> ...]`
  Comando general para añadir registros de distintos tipos (NS, TXT, etc.).

  Añadir registro NS

  Añadir otro servidor de nombres `dns2` para `midominio.dom` con IP `192.168.1.5`.

  ```
  PS C:\> Add-DnsServerResourceRecord -Name dns2 -ZoneName "midominio.dom" -NS -NameServer "dns2.midominio.dom"
  ```

- `Get-DnsServerResourceRecord -ZoneName <nombre-zona> [-Name <nombre>] [-RRType <tipo-registro>]`
  Muestra los registros de una zona; se puede filtrar por nombre o tipo.

  Mostrar registros de una zona

  Mostrar todos los registros A de la zona `midominio.dom`.

  ```
  PS C:\> Get-DnsServerResourceRecord -Zonename "midominio.dom" -RRType A | Format-Table -AutoSize
  HostName RecordType Type Timestamp TimeToLive RecordData
  -------- ---------- ---- --------- ---------- ----------
  dhcp     A          1    0         01:00:00   192.168.1.2
  dns      A          1    0         01:00:00   192.168.1.3
  www      A          1    0         01:00:00   192.168.1.4
  ftp      A          1    0         01:00:00   192.168.1.5
  correo   A          1    0         01:00:00   192.168.1.6
  dns2     A          1    0         01:00:00   192.168.1.13
  ```

  Mostrar registros de una zona

  Mostrar todos los registros PTR de la zona inversa `1.168.192.in-addr.arpa`.

  ```
  PS C:\> Get-DnsServerResourceRecord -Zonename "1.168.192.in-addr.arpa" -RRType Ptr | Format-Table -AutoSize
  HostName RecordType Type Timestamp TimeToLive RecordData
  -------- ---------- ---- --------- ---------- ----------
  13       PTR        12   0         01:00:00   dns2.midominio.dom.
  6        PTR        12   0         01:00:00   correo.midominio.dom.
  5        PTR        12   0         01:00:00   ftp.midominio.dom.
  4        PTR        12   0         01:00:00   www.midominio.dom.
  3        PTR        12   0         01:00:00   dns.midominio.dom.
  2        PTR        12   0         01:00:00   dhcp.midominio.dom.
  ```

- `Set-DnsServerResourceRecord -Zonename <nombre-zona> -OldInputObject <$RRantic> -NewInputObject <$RRnou>`
  Modifica un registro de recurso reemplazando el objeto antiguo por uno nuevo. Se usa habitualmente para parámetros del SOA.

  Modificar un registro

  Modificar un registro suponiendo que los valores antiguos están en la variable `$rro` y los valores nuevos en `$rrn`.

```
PS C:\> Set-DnsServerResourceRecord -ZoneName "midominio.dom" -OldInputObject $rro -NewInputObject $rrn
```

- `Remove-DnsServerResourceRecord -ZoneName <nombre-zona> -RRType <tipo-registro> -Name <nombre> [-RecordData <lista-datos-registro>]`
  Elimina uno o varios registros de un tipo dado en una zona. El valor de `-RecordData` depende del tipo de registro.

> **Eliminar un registro**
>
> Eliminar el registro A `ftp` de `midominio.dom`.
>
> ```
> PS C:\> Remove-DnsServerResourceRecord -ZoneName "midominio.dom" -RRType A -Name ftp -RecordData 192.168.1.5
> ```

CONFIGURACIONES AVANZADAS

A continuación se muestran configuraciones avanzadas y casos especiales del servicio DNS en Windows Server.

SERVICIO DNS EN WINDOWS NANO SERVER

Las ediciones Nano Server se usan en máquinas virtuales de Hyper-V y en contenedores Windows. En Nano Server el servicio DNS se instala de forma diferente: se instala el SO y se preconfigura para luego instalar el servicio DNS de forma remota mediante WinRM desde otro equipo.

Comandos relevantes:

- `Enable-WindowsOptionalFeature -Online -FeatureName DNS-Server-Full-Role`
  Desempaqueta/instala el servicio DNS.

> **Instalación DNS en Nano Server**
>
> Instalar/extraer el paquete DNS en una máquina remota (ejemplo de uso con WinRM).
> Tras conectarse a la máquina remota (WinRM), ejecutar el siguiente código:
>
> ```
> [192.168.1.100]: PS C:\> Enable-WindowsOptionalFeature -Online -FeatureName DNS-Server-Full-Role
> ```

- `Import-Module DnsServer`
  Carga el módulo con los comandos de configuración del servicio DNS.
- `Get-Command -Module DnsServer`
  Lista los comandos disponibles del módulo.

REENVIADORES Y ZONAS DE REENVÍO

Un servidor DNS puede actuar de forma híbrida, realizando tanto resoluciones recursivas como autoritativas. Se puede configurar para reenviar peticiones a otros servidores si el nombre solicitado no está en sus zonas autoritativas. Los **reenviadores (forwarders)** se pueden definir a **nivel de servidor** o a **nivel de zona** (zonas de reenviamiento condicional).

Los comandos relevantes son:

- `Add-DnsServerForwarder -IPAddress <ip>`
  Añade un servidor DNS público/privado a la lista de reenviadores a nivel de servidor.

> **Forwarders a nivel de servidor**
>
> Añadir el reenviador público de Google `8.8.8.8`.
>
> ```
> PS C:\> Add-DnsServerForwarder -IPAddress 8.8.8.8
> ```

- `Get-DnsServerForwarder`
  Muestra los reenviadores definidos (a nivel de servidor).

- `Remove-DnsServerForwarder -IPAddress <ip>`
  Elimina el reenviador indicado (a nivel de servidor).
- `Add-DnsServerConditionalForwarderZone -Name <nombre-zona> -MasterServers <lista-ip>`
  Añade una zona de reenvío condicional que reenvía consultas para un dominio a servidores específicos.

Forwarding condicional

Añadir una zona de reenvío condicional para `otrodominio.dom` cuyo servidor que conoce ese dominio es `192.168.2.252`.

```
PS C:> Add-DnsServerConditionalForwarderZone -Name otrodominio.dom -MasterServers 192.168.2.252 -Passthru
ZoneName          ZoneType  IsAutoCreated IsDsIntegrated IsReverseLookupZone IsSigned
--------          --------  ------------  -------------- ------------------- --------
otrodominio.dom   Forwarder False         False          False
```

El parámetro `-Passthru` hace que se muestre información adicional sobre la zona creada.

Forwarding condicional

Añadir una zona de reenvío condicional inversa para la red `192.168.2.0/24`.

```
PS C:\> Add-DnsServerConditionalForwarderZone -Name 2.168.192.in-addr.arpa -MasterServers 192.168.2.252 -Passthru
ZoneName               ZoneType  IsAutoCreated IsDsIntegrated   IsReverseLookupZone   IsSigned
--------               --------  ------------  --------------   -------------------   --------
2.168.192.in-addr.arpa Forwarder False         False            True
```

Las zonas de reenviamiento se eliminan con el mismo comando que se utiliza para eliminar cualquier zona (`Remove-DnsServerZone -Name <zona>`).

CONFIGURACIÓN DE REGISTROS NS Y SOA

Al crear una zona automáticamente se crean los registros NS y SOA con valores por defecto en la sección `RecordData`. Es habitual modificar algunos de esos valores (por ejemplo servidor primario, responsable, intervalos de refresh/retry/expire). El proceso general para modificar estos campos es:

1. Cargar en una variable el objeto del registro que queremos modificar.
2. Clonar/copiar ese objeto en otra variable.
3. Modificar los valores en la nueva variable.
4. Actualizar el registro con el cmdlet `Set-DnsServerResourceRecord`.

Modificar registro NS

Cambiar el nombre del servidor DNS en el registro NS de `midominio.dom`.

```
# Paso 1: obtener registro de recurso NS
PS C:\> $RRnsOld = Get-DnsServerResourceRecord -ZoneName "midominio.dom" -RRType Ns

# Paso 2: clonar registro
PS C:\> $RRnsNew = [ciminstance]::new($RRnsOld)
# (en Windows 2019+ se puede usar Clone)
PS C:\> $RRnsNew = $RRnsOld.Clone()

# Paso 3: modificar nombre del servidor al RecordData
PS C:\> $RRnsNew.RecordData.NameServer = "dns.midominio.dom"

# Paso 4: actualizar registro NS
PS C:\> Set-DnsServerResourceRecord -ZoneName "midominio.dom" -OldInputObject $RRnsOld -NewInputObject $RRnsNew
```

Modificar registro SOA

Modificar el registro SOA de la zona de resolución directa del dominio `midominio.dom` de manera que el servidor se llame `dns`, las incidencias de funcionamiento del servicio DNS se envíen al usuario de correo del dominio `admin`. También se tiene que configurar para

que se hagan transferencias de zona cada dia, que se reintente conectar cada 4 horas y que las zonas secundarias consideren que la zona ha caducado despues de 7 dias sin actualizarse.

```
# Paso 1: obtener registro de recurso SOA
PS C:\> $RRsoaOld = Get-DnsServerResourceRecord -ZoneName "midominio.dom" -RRType Soa

# Paso 2: clonar registro
PS C:\> $RRsoaNew = [ciminstance]::new($RRsoaOld)

# Paso 3: modificar valores del RecordData
PS C:\> $RRsoaNew.RecordData.PrimaryServer = "dns.midominio.dom"
PS C:\> $RRsoaNew.RecordData.ResponsiblePerson = "admin.midominio.dom"
PS C:\> $RRsoaNew.RecordData.RefreshInterval = New-TimeSpan -Days 1
PS C:\> $RRsoaNew.RecordData.RetryDelay = New-TimeSpan -Hours 4
PS C:\> $RRsoaNew.RecordData.ExpireLimit = New-TimeSpan -Days 7

# Paso 4: actualizar registro SOA
PS C:\> Set-DnsServerResourceRecord -ZoneName "midominio.dom" -OldInputObject $RRsoaOld -NewInputObject $RRsoaNew
```

SUBDOMINIOS Y DELEGACIONES DE ZONAS

Un servidor autoritativo de un dominio puede delegar la resolución de nombres de uno de sus subdominios a otro servidor DNS. Esto se consigue añadiendo una delegación de zona (registro de delegación) que apunta al servidor DNS del subdominio (normalmente un par: un NS y un registro A **glue**) en el servidor del dominio padre.

En Windows Server no es necesario crear manualmente los registros glue; se indica la delegación usando el comando apropiado y el servidor se encarga de crear lo necesario (si procede). Los servidores DNS del subdominio deben estar configurados correctamente.

Comandos:

- `Add-DnsServerZoneDelegation -Name <zona-dominio> -ChildZoneName <zona-subdominio> -NameServer <fqdn-dns-subdominio> -IPAddress <ip-dns-subdominio>`
  Delegar la administración de un subdominio en el servidor DNS especificado por su FQDN e IP.

  Delegación de subdominios

  Delegar `grupo1.midominio.dom` y `grupo2.midominio.dom`. Los servidores DNS de los subdominios son `dnsG1.grupo1.midominio.dom` (IP `192.168.1.23`) y `dnsG2.grupo2.midominio.dom` (IP `192.168.1.33`).

  ```
  PS C:\> Add-DnsServerZoneDelegation -Name "midominio.dom" `
  -ChildZoneName "grupo1" `
  -NameServer "dnsG1.grupo1.midominio.dom" `
  -IPAddress 192.168.1.23

  PS C:\> Add-DnsServerZoneDelegation -Name "midominio.dom" `
  -ChildZoneName "grupo2" `
  -NameServer "dnsG2.grupo2.midominio.dom" `
  -IPAddress 192.168.1.33
  ```

- `Get-DnsServerZoneDelegation -Name <nombre-zona>`
  Mostrar delegaciones definidas para una zona.

  Mostrar delegaciones

  Mostrar las delegaciones definidas en la zona `midominio.dom`.

  ```
  PS C:\> Get-DnsServerZoneDelegation -Name "midominio.dom" | Format-Table -AutoSize
  ZoneName          ChildZoneName          NameServer                IPAddress
  --------          -------------          ----------                ---------
  midominio.dom     grupo1.midominio.dom   dnsG1.grupo1.midominio.dom  192.168.1.23
  midominio.dom     grupo2.midominio.dom   dnsG2.grupo2.midominio.dom  192.168.1.33
  ```

- `Remove-DnsServerZoneDelegation -Name <zona-dominio> -ChildZoneName <zona-subdominio>`
  Eliminar una delegación de subdominio.

SERVIDORES SECUNDARIOS Y TRANSFERENCIAS DE ZONA

El servicio DNS debe proveer alta disponibilidad; esto se logra mediante réplicas (servidores secundarios) por zona. Las zonas primarias (maestras) y secundarias (esclavas) deben mantenerse sincronizadas. Las transferencias de zona pueden ser completas o incrementales. Los atributos numéricos del `RecordData` del SOA configuran cuándo y cómo se hacen las transferencias (SerialNumber, RefreshInterval, RetryDelay, ExpireLimit, MinimumTTL).

Los atributos son:

- `SerialNumber`: número de serie de la zona. La zona primaria y secundaria tienen que tener el mismo número de serie. Si el número de serie de la zona primaria es mayor que el de la secundaria, entonces se producirá una transferencia de zona cuando corresponda para actualizar la secundaria.
- `RefreshInterval`: intervalo entre comprobaciones de cambios por parte de la secundaria. Por defecto el valor se expresa en segundos (como todos los campos que expresen tiempos). Con el sufijo *m* el tiempo se expresa en minutos, con *h* en horas y con el sufijo *d* en días.
- `RetryDelay`: tiempo de reintento si falla la transferencia.
- `ExpireLimit`: tiempo tras el cual la secundaria considera que la zona ha caducado si no ha podido actualizarse y por lo tanto deja de responder a consultas.
- `MinimumTTL`: TTL mínimo para respuestas negativas en caché; es decir, el tiempo que un cliente debe esperar antes de volver a consultar por un nombre que no existe.

Para forzar una transferencia incremental o completa se incrementa el `SerialNumber` en la zona primaria (y opcionalmente se configuran notificaciones a secundarias).

Comandos relevantes para configurar zonas secundarias y transferencias de zona:

- `Set-DnsServerPrimaryZone -Name "<zona>" -Notify NotifyServers -NotifyServers <ips> -SecondaryServers <ips> -SecureSecondaries TransferToSecureServers`
  Configurar el servidor primario para que notifique a los servidores secundarios especificados cuando haya cambios en la zona. El parámetro `-SecureSecondaries` indica que solo se permiten transferencias a servidores seguros (autenticados).

  Configurar notificaciones y transferencias de zona

  Configurar el servidor primario de la zona midominio.dom para que notifique los cambios de la base de datos de resolución de la zona al servidor secundario de ip `192.168.1.13`. Configurar también el servidor primario de la zona de resolución inversa correspondiente a la red `192.168.1.0/24`.

  ```
  PS C:\> Set-DnsServerPrimaryZone -Name "midominio.dom" `
  -Notify NotifyServers -NotifyServers 192.168.1.13 `
  -SecondaryServers 192.168.1.13 -SecureSecondaries TransferToSecureServers

  PS C:\> Set-DnsServerPrimaryZone -Name "1.168.192.in-addr.arpa" `
  -Notify NotifyServers -NotifyServers 192.168.1.13 `
  -SecondaryServers 192.168.1.13 -SecureSecondaries TransferToSecureServers
  ```

- `Add-DnsServerSecondaryZone -Name <nombre-zona> -ZoneFile <archivo-resolución-zona> -MasterServers <lista-dns-primarios>`
  Añadir una zona secundaria de resolución directa.

  Crear zonas secundarias directas

  Crear la zona secundaria para el dominio `midominio.dom`.

  ```
  PS C:\> Add-DnsServerSecondaryZone -Name "midominio.dom" `
  -ZoneFile "midominio.dom.dns" `
  -MasterServers 192.168.1.3
  ```

- `Add-DnsServerSecondaryZone -NetworkId <red> -ZoneFile <archivo> -MasterServers <lista-dns-primarios>`
  Añadir una zona secundaria de resolución inversa.

  Crear zonas secundarias inversas

  Crear la zona secundaria de resolución inversa para la red `192.168.1.0/24`.

```
PS C:\> Add-DnsServerSecondaryZone -NetworkId 192.168.1.0/24 `
-ZoneFile "1.168.192.in-addr.arpa.dns" `
-MasterServers 192.168.1.3
```