

A **Administración de sistemas operativos**

Consulte nuestra página web: www.sintesis.com
En ella encontrará el catálogo completo y comentado



NO fotocopies el libro

Queda prohibida, salvo excepción prevista en la ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra sin contar con autorización de los titulares de la propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (arts. 270 y sigs. Código Penal). El Centro Español de Derechos Reprográficos (www.cedro.org) vela por el respeto de los citados derechos.

A **Administración de sistemas operativos**

José F. Feria Martínez

ASESOR EDITORIAL:

Juan Carlos Moreno Pérez

© José F. Feria Martínez

© EDITORIAL SÍNTESIS, S. A.
Vallehermoso, 34. 28015 Madrid
Teléfono 91 593 20 98
<http://www.sintesis.com>

ISBN: 978-84-1357-069-3
Depósito Legal: M-3.008-2021

Impreso en España - Printed in Spain

Reservados todos los derechos. Está prohibido, bajo las sanciones penales y el resarcimiento civil previstos en las leyes, reproducir, registrar o transmitir esta publicación, íntegra o parcialmente, por cualquier sistema de recuperación y por cualquier medio, sea mecánico, electrónico, magnético, electroóptico, por fotocopia o por cualquier otro, sin la autorización previa por escrito de Editorial Síntesis, S. A.

Índice

PRESENTACIÓN	11
---------------------------	----

PARTE I **WINDOWS SERVER**

1. ADMINISTRACIÓN BÁSICA DE WINDOWS SERVER	17
Objetivos	17
Mapa conceptual	18
Glosario	18
1.1. Introducción	19
1.2. Características de Windows Server	19
1.3. Primeros pasos tras la instalación	20
1.3.1. Directivas de seguridad local	20
1.3.2. Administración de usuarios y grupos	21
1.3.3. Agregar roles y características básicas	23
1.3.4. Administrador de discos	24
1.3.5. Cuotas de disco	25
1.3.6. Permisos	27
1.4. Arranque y parada	28
1.4.1. Apagar o reiniciar Windows Server desde la consola	28
1.4.2. Apagar o reiniciar Windows Server desde el entorno gráfico	28
1.5. Servicios del sistema	29
1.6. Programador de tareas	29
1.7. Monitorización del sistema	31

1.8. Copias de seguridad	32
1.9. Gestión de procesos	34
1.10. PowerShell	36
1.10.1. Administrar usuarios	36
1.10.2. Administrar procesos desde PowerShell	37
1.10.3. Administrar servicios desde PowerShell	38
Resumen	39
Ejercicios prácticos	40
Actividades de autoevaluación	41
2. DIRECTORIO ACTIVO DE WINDOWS	43
Objetivos	43
Mapa conceptual	44
Glosario	45
2.1. Introducción	45
2.2. Conceptos básicos	46
2.3. Instalación del directorio activo	47
2.3.1. Pasos para la instalación	47
2.4. Administración del Active Directory	49
2.4.1. Creación de usuarios y equipos	49
2.4.2. Sitios y servicios	52
2.4.3. Dominios y confianzas	53
2.5. Seguridad y políticas de grupos	54
2.5.1. Seguridad. Recomendaciones básicas	54
2.5.2. Políticas de grupo	56
2.5.3. Restricciones de inicio de sesión en equipos	59
Resumen	59
Ejercicios prácticos	60
Actividades de autoevaluación	61
3. ADMINISTRACIÓN DE LA RED EN WINDOWS	63
Objetivos	63
Mapa conceptual	64
Glosario	65
3.1. Introducción	65
3.2. Configuración básica de la red	66
3.2.1. Protocolo de control de transmisión/protocolo de internet	66
3.2.2. Nombre de equipo y dominio	66
3.2.3. Enrutamiento	67
3.3. Configuración del protocolo de configuración dinámica de host	68
3.4. Configuración del sistema de nombre de dominio	71
3.4.1. Crear una nueva zona directa o inversa	71
3.4.2. Establecer un reenviador DNS	72
3.4.3. Control de acceso a elementos externos	73
3.5. Escritorio remoto	74
3.5.1. Asegurar el protocolo de escritorio remoto	74
3.5.2. Autenticación a nivel de red	75
3.5.3. Configuración de acceso remoto	75

3.5.4. Agregar usuarios de escritorio remoto	76
3.5.5. Puerta de enlace de escritorio remoto	77
3.5.6. Acceso remoto a Windows desde Linux	77
3.6. Servidor de aplicaciones	78
Resumen	79
Ejercicios prácticos	80
Actividades de autoevaluación	81
4. SERVIDOR DE IMPRESIÓN Y DE ARCHIVOS EN WINDOWS	83
Objetivos	83
Mapa conceptual	84
Glosario	84
4.1. Introducción	85
4.2. Recursos compartidos	85
4.3. Compartición de archivos	86
4.3.1. Compartir carpeta desde el explorador de archivos	86
4.3.2. Compartir una carpeta usando el administrador del servidor	88
4.3.3. Compartir una carpeta a través de Windows PowerShell	89
4.4. Administración de recursos compartidos. Cuotas	89
4.5. Servidor de impresión	91
4.5.1. Grupos de impresoras. Impresoras lógicas	93
4.5.2. Agregar impresora compartida en Linux	95
4.6. Administración de discos	96
Resumen	99
Ejercicios prácticos	100
Actividades de autoevaluación	100

PARTE II GNU/LINUX

5. ADMINISTRACIÓN BÁSICA DE LINUX	105
Objetivos	105
Mapa conceptual	106
Glosario	106
5.1. Introducción	107
5.2. Características de Linux Server	108
5.3. Actualización del sistema	108
5.4. Administración de usuarios	109
5.4.1. Añadir usuarios	110
5.4.2. Modificar usuarios	110
5.4.3. Eliminar usuarios	111
5.4.4. Cambiar contraseñas	111
5.5. Configurar la zona horaria y el idioma	111
5.6. Administración de aplicaciones	113
5.6.1. Apt-get	113
5.6.2. Dpkg	114
5.6.3. Apt	114

5.7. Administrador de discos	115
5.7.1. Fdisk	115
5.7.2. GNU Parted	115
5.7.3. Gparted	116
5.7.4. Discos de GNOME	116
5.8. Monitor de recursos	116
5.9. Permisos	118
5.9.1. Establecer permisos	119
5.9.2. Cambiar propietario y grupo	121
5.10. Gestión y control de procesos	121
5.10.1. Listar procesos	122
5.10.2. Estados de un proceso	122
5.10.3. Prioridades	123
5.10.4. Árbol de procesos	124
5.10.5. Demonios	124
5.10.6. Procesos en primer plano	125
5.10.7. Procesos en segundo plano	125
5.10.8. Cambiar procesos entre primer y segundo plano	126
5.10.9. Mostrar procesos en segundo plano o suspendidos	127
5.10.10. Terminar un proceso	127
5.11. Automatización de tareas	128
5.11.1. Cron	128
5.11.2. Crontab	130
5.11.3. Anacron	131
5.11.4. At	131
5.11.5. Utilidades gráficas	132
Resumen	133
Ejercicios prácticos	134
Actividades de autoevaluación	134
6. ADMINISTRACIÓN DE LA RED EN LINUX	137
Objetivos	137
Mapa conceptual	138
Glosario	138
6.1. Introducción	139
6.2. Configuración del protocolo de configuración dinámica del host	139
6.2.1. Asignar una IP fija a través de protocolo de configuración dinámica del host	142
6.3. Configuración del DNS	142
6.4. Acceso remoto a Linux	143
6.4.1. Secure Shell. Servidor Secure Shell	143
6.4.2. TeamViewer	146
6.4.3. Servidor VNC	146
6.4.4. Remote Desktop Viewer	149
6.5. Seguridad en la red. Iptables	150
6.5.1. Fundamentos de Iptables	150
6.5.2. Instalación de Iptables	151
6.5.3. Definición de reglas	151
6.5.4. Filtrado de paquetes basados en la fuente	152
6.5.5. Eliminación de reglas	152
6.5.6. Cambios persistentes	153

Resumen	154
Ejercicios prácticos	154
Actividades de autoevaluación	155
7. SERVIDOR DE IMPRESIÓN Y DE ARCHIVOS EN LINUX	157
Objetivos	157
Mapa conceptual	158
Glosario	158
7.1. Introducción	159
7.2. Compartir archivos e impresoras	159
7.3. Servidor Samba: Windows y Linux en una misma red	160
7.4. Servidor de archivos. Samba	161
7.4.1. Instalar	161
7.4.2. Configurar	162
7.4.3. Añadir usuarios para acceder a los recursos	163
7.4.4. Asignar permisos a los recursos compartidos	163
7.4.5. Iniciar y detener Samba	164
7.4.6. Compartir una carpeta	164
7.5. CUPS. Servidor de impresión	165
7.6. Samba con soporte para la impresión con CUPS	167
7.7. Agregar impresora compartida en Windows con Samba	168
7.8. Herramientas de línea de comandos para el sistema de impresión CUPS	169
7.8.1. Imprimir	169
7.8.2. Seleccionar la impresora	170
7.8.3. Definir la impresora predeterminada	170
7.8.4. Redirigir la salida estándar de un programa a CUPS	171
7.8.5. Especificar opciones de impresión	171
7.8.6. Cancelar un trabajo	171
7.8.7. Habilitar o deshabilitar una impresora	172
7.9. Administración de discos. Cuotas de espacio	172
7.9.1. Activar cuotas	172
7.9.2. Asignar cuotas de disco	173
7.9.3. Activar y desactivar cuotas de disco	174
Resumen	175
Ejercicios prácticos	176
Actividades de autoevaluación	176
8. LDAP	179
Objetivos	179
Mapa conceptual	180
Glosario	180
8.1. Introducción	181
8.2. El servicio de directorio como infraestructura	181
8.2.1. Gestión centralizada de usuarios	182
8.3. Funcionamiento del protocolo ligero de acceso a directorio	183
8.4. Seguridad en el protocolo ligero de acceso a directorio	184
8.4.1. Política de contraseñas	184
8.4.2. Autorización basada en equipos. El atributo host	185

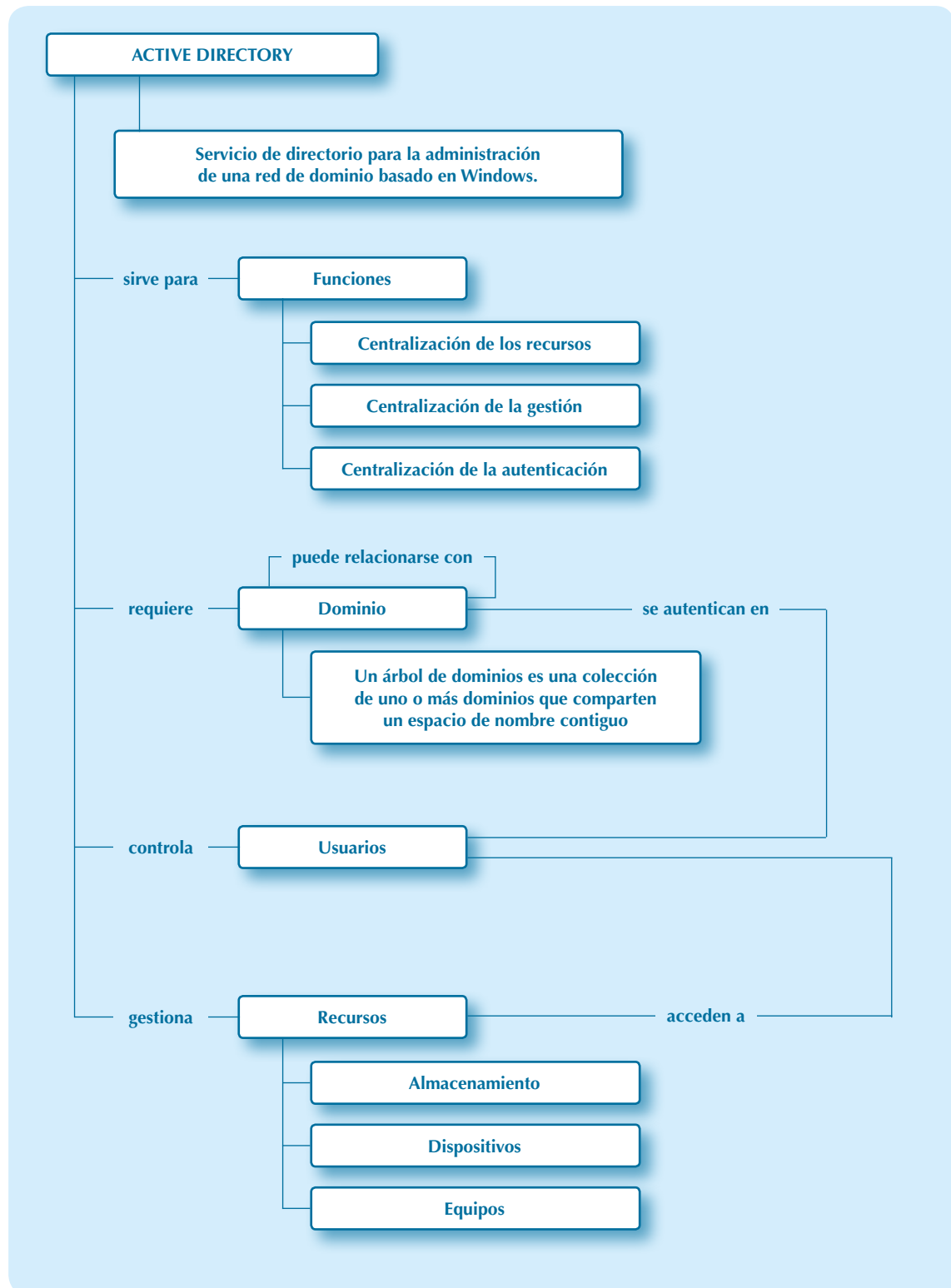
8.5. OpenLDAP	185
8.5.1. Instalar y configurar	185
8.5.2. Llenar la base de datos del protocolo ligero de acceso a directorio	186
8.5.3. Comandos básicos del protocolo ligero de acceso a directorio	187
8.5.4. Política de contraseñas	189
8.6. phpLdapAdmin	192
8.6.1. Instalación	192
8.6.2. Añadir unidades organizativas	193
8.6.3. Añadir grupos	193
8.6.4. Añadir usuarios	194
8.7. LDAP sobre SSL/TLS con OpenLDAP	195
8.7.1. Configuración de la autoridad certificadora	196
8.7.2. Configuración de slapd	197
8.7.3. Configuración de los clientes	197
8.7.4. Comprobar el funcionamiento	198
8.8. Redes heterogéneas	198
Resumen	199
Ejercicios prácticos	200
Actividades de autoevaluación	201
9. PROGRAMACIÓN SHELL SCRIPT LINUX	203
Objetivos	203
Mapa conceptual	204
Glosario	204
9.1. Introducción	204
9.2. Comandos básicos	205
9.3. Entrada y salida	207
9.3.1. Entrada y salida por consola	207
9.3.2. Redirección entrada y salida	207
9.4. Expresiones	209
9.4.1. Comando grep	210
9.4.2. Comando sed	211
9.5. Control de flujo	212
9.5.1. Condición if – then – else – fi	212
9.5.2. Condición case	213
9.5.3. Bucle for	213
9.5.4. Bucle while	214
9.5.5. Bucle until	214
9.6. Funciones	215
9.6.1. Variables locales y globales	216
9.6.2. Valores de retorno	217
9.6.3. Pasar parámetros a funciones	218
Resumen	218
Ejercicios prácticos	219
Actividades de autoevaluación	220

Directorio activo de Windows

Objetivos

- ✓ Instalar y administrar el servicio de directorio e integrarlo en una red.
- ✓ Identificar la función, los elementos y las estructuras lógicas del servicio de directorio.
- ✓ Determinar y crear el esquema del servicio de directorio, personalizándolo e integrándolo el servicio de directorio con otros servicios.
- ✓ Emplear el servicio de directorio como mecanismo de acreditación centralizada de los usuarios en una red.
- ✓ Utilizar herramientas gráficas y comandos para la administración del servicio de directorio.

Mapa conceptual



Glosario

eDirectory (Novell Directory Services). Implementación de Novell utilizada para permitir y controlar el acceso global a todos los recursos de la red.

Kerberos. Arquitectura cliente-servidor que proporciona seguridad a las transacciones en las redes, permitiendo a dos ordenadores en una red insegura demostrar su identidad mutuamente de manera segura.

Microsoft Defender. Programa de seguridad cuyo propósito es prevenir, quitar y poner en cuarentena software espía en Microsoft Windows. Anteriormente se conocía como Windows Defender.

Microsoft Message Queue Server. Implementación de cola de mensajes desarrollada por Microsoft e implementada en sus sistemas operativos Windows Server desde Windows NT 4, Windows 95, Windows Server 2016 y Windows 10.

NetBIOS. Estos nombres son una forma más amigable de identificar computadoras en una red que los números de red.

Parche. Actualizaciones acumulativas para, principalmente, solucionar vulnerabilidades del software.

2.1. Introducción

En un mundo interconectado mediante internet como el actual, muchas empresas con cientos de empleados necesitan acceso a ordenadores conectados a la infraestructura y recursos de la organización para poder realizar su trabajo. El uso de las redes LAN y Active Directory (AD) permite construir una red de ordenadores con garantías de seguridad y limitaciones de acceso a dichos recursos.

El hecho de contar con un entorno de trabajo donde existan cientos de equipos interconectados en una red LAN hace que gestionar y administrar los sistemas operativos en cuanto a usuarios, permisos de acceso, correos, etc., de manera individualizada, sea una tarea ardua y costosa.

La solución viene con la centralización de todas estas tareas de gestión y control en un ordenador o servidor dedicado a la creación de usuarios y asignación de permisos. Es aquí donde AD aporta la capacidad de establecer un único punto de control para toda esa gestión.

2.2. Conceptos básicos

Para un administrador de redes la mejor manera de intercambiar información entre equipos de forma eficiente, es crear un dominio de sistemas, para centralizar la información y la seguridad en uno o varios servidores, facilitando el trabajo del administrador.

Windows Server emplea el concepto de directorio, que consiste en una estructura jerárquica que guarda información sobre objetos en la red implementada como una base de datos.

AD es una herramienta de Microsoft que proporciona el servicio de directorio de una red de Windows Server, que guarda la información de los recursos de la red y permite el acceso de los usuarios y de las aplicaciones a dichos recursos. Es un modelo para organizar, controlar y administrar el acceso a los recursos de la red. Permite gestionar todos los aspectos anteriores sin la necesidad de tener que actuar en cada uno de los equipos que integran la organización.

RECUERDA

- ✓ Cuando un usuario inicia sesión con sus credenciales, es identificado por AD, que verifica dichas credenciales y envía al ordenador la información relativa a dicho usuario. De este modo, el usuario arranca su sistema operativo teniendo acceso a todos sus documentos, imágenes, recursos en línea y demás archivos a los que tenga permitido el acceso.
- ✓ En caso de un problema en el ordenador que se esté utilizando, bastaría con usar otro ordenador de la organización para volver a iniciar sesión con las credenciales y poder seguir trabajando como si del ordenador anteriormente averiado se tratase.

Existe una serie de conceptos que se deben tener muy claros para comprender el funcionamiento de AD:

- a) *Dominio*. Un dominio en AD es un conjunto de ordenadores conectados a una red, que cuentan con un equipo servidor para administrar las cuentas de usuario y credenciales. AD es también un controlador de dominio, ya que podremos crear distintos dominios y gestionar los permisos e interacción en cada uno de ellos. A esta relación entre dominios se le denomina: relación de confianza.
- b) *Confianza*. Es la relación existente entre dos dominios, dos árboles o dos bosques.
- c) *Objeto*. Es el nombre genérico que utilizamos para referirnos a cualquier componente dentro de un directorio. Estos objetos pueden ser de tres tipos:
 - Usuarios: credenciales de acceso a estaciones de trabajo.
 - Recursos: elementos a los que cada usuario podrá acceder según sus permisos, ya sean carpetas compartidas, impresoras, etc.
 - Servicios: funcionalidades a las que cada usuario puede acceder, por ejemplo, el correo electrónico.
- d) *Unidad organizativa*. Es un contenedor de objetos como impresoras, usuarios, grupos etc., organizados mediante subconjuntos, estableciendo así una jerarquía.

- e) *Árbol*. Es un conjunto de dominios, los cuales dependen de una raíz común y están organizados en una determinada jerarquía, también llamada DNS común. Esta estructura permite identificar unos dominios de otros. Por ejemplo, el dominio instituto.es y ciclo.instituto.es pertenecen al mismo árbol de dominio; pero, sin embargo, instituto.es y aulas.es no pertenecen al mismo árbol.
- f) *Bosque*. Un bosque es la suma de todos los dominios existentes contenidos en él.

2.3. Instalación del directorio activo

Para usar AD se necesita cumplir una serie de requisitos. El primero de ellos es disponer de un sistema operativo Windows Server en sus versiones 2000, 2003, 2008, 2016 o 2019.

También necesitaremos una dirección IP fija y un protocolo TCP/IP instalado. Por último, es necesario disponer de un servidor DNS y un sistema de archivos compatible con Windows, por ejemplo, NTFS.

2.3.1. Pasos para la instalación

1. Lo primero será acceder al *Administrador del servidor* para dar de alta los roles necesarios y seleccionar la instalación basada en características o en roles. Una vez seleccionado el servidor, en la lista de role, marcar *Servicios de dominio de Active Directory*.
2. Al hacerlo, nos solicitará añadir las características necesarias de los servicios de dominio de AD.
3. Una vez finalizada la instalación, en el *Administrador del servidor* aparece, en la barra superior, un triángulo de advertencia, indicando que se han instalado los servicios de AD, pero hay que configurar el servidor.

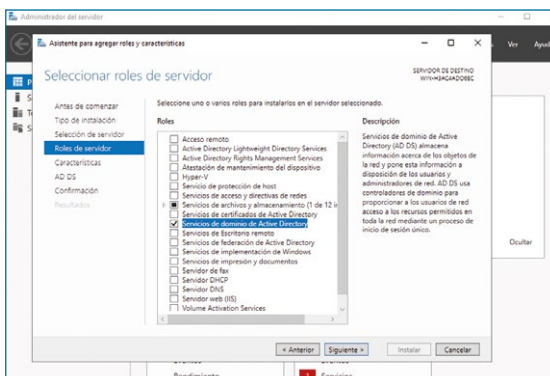


Figura 2.1
Instalación de AD.

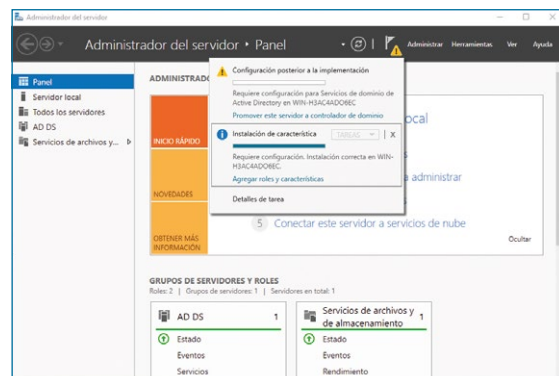


Figura 2.2
Aviso del administrador del servidor tras la instalación.

4. A continuación, se debe promover el servidor a controlador de dominio, para iniciar el asistente de configuración. Al ser el primer servidor del dominio, árbol, bosque...,

seleccionar *Agregar un nuevo bosque* y, en el nombre del dominio raíz (bosque y árbol), escribir el nombre de dominio que se quiera asignar, por ejemplo: *priServer.local*.

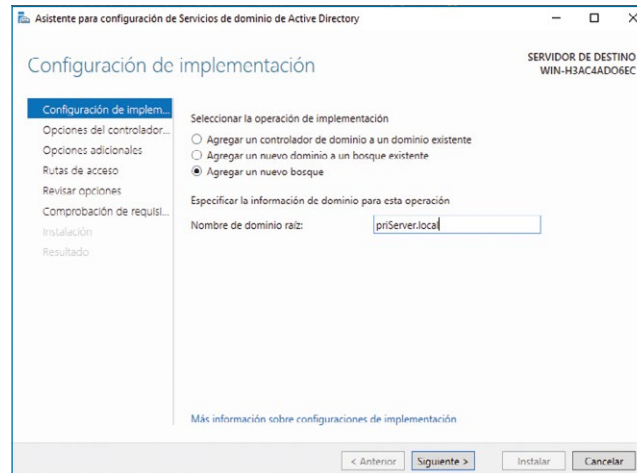


Figura 2.3
Configuración del dominio.

5. Verificar el nombre NetBIOS del dominio. Se debe tener en cuenta que el máximo de caracteres es 15. No conviene que el nombre del dominio y NetBIOS sean diferentes (algunas aplicaciones de red pueden dar conflictos).
6. Seleccionar la ubicación de los archivos del AD:
 - Base de datos.
 - Archivos de registro.
 - Carpeta SYSVOL (políticas de seguridad, scripts, distribución de software).
7. Tras mostrar un informe de requisitos y acciones que tomará el sistema, hacer clic en el botón *Instalar*.
8. El sistema se reiniciará por sí solo, tras lo cual, se puede observar cómo el inicio de sesión ya se realiza en el dominio, y no de manera local.

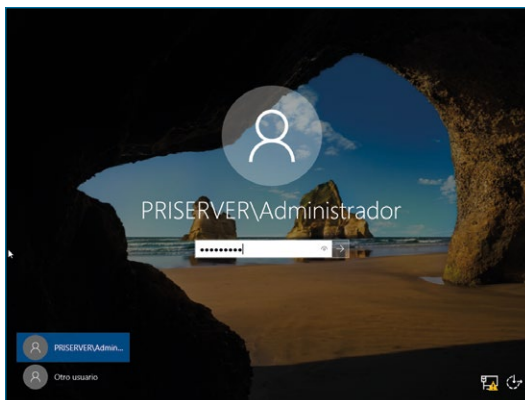


Figura 2.4
Inicio de sesión en el dominio.

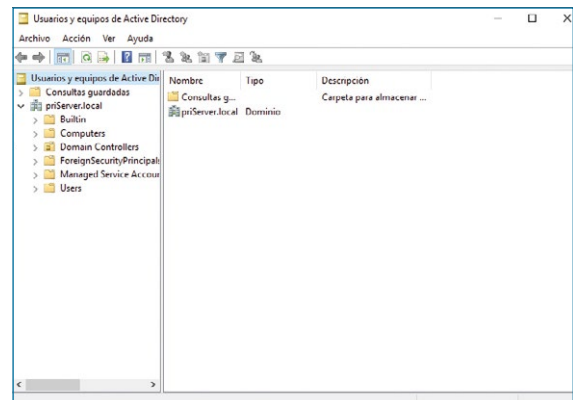


Figura 2.5
Usuarios y equipos de AD.

9. Al iniciar el *Administrador del servidor*, en la barra lateral izquierda y en el menú de herramientas aparecen nuevas opciones: *Servicios de certificados de Active Directory (AD CS)*, *DNS, Dominios y confianzas de Active Directory*, *Editor ADSI*, *Sitios y servicios de Active Directory*, *Usuarios y equipos de Active Directory*.
10. La herramienta más utilizada en el AD es *Usuarios y equipos de Active Directory*. En ella se gestionan los usuarios, los grupos de seguridad y los equipos que pertenecen al AD.

2.4. Administración del Active Directory

2.4.1. Creación de usuarios y equipos

En un servidor se requieren muchas tareas de administración relacionadas con redes, seguridad, protocolos e interfaces. Pese a toda esta complicada gestión, existen tareas simples, pero esenciales, en el servidor para que todo funcione correctamente. La gestión de usuarios y grupos es un claro ejemplo de sencillez. Lógicamente, sin un usuario no se podrá acceder al servidor o al dominio desde un equipo cliente, y, si ese usuario no pertenece a un grupo, será mucho más costosa la gestión de permisos.

No se puede crear un grupo o un usuario sin razón alguna. Por eso, se debe tener clara cuál será la función de ese usuario y qué tipo de grupo se va a crear. Para ello, Windows Server ofrece los siguientes tipos de usuario:

- Estándar, con acceso a las funciones del servidor a las que se le haya otorgado permisos.
- Administrador, con control total en el dominio, perteneciendo al grupo de administradores.

A) Creación de usuarios

Para crear una cuenta de equipo, debemos volver a la herramienta *Usuarios y equipos de Active Directory*, bien desde el menú *Herramientas del Administrador del Servidor*.

Es recomendable crear unidades organizativas (OU) para gestionar y facilitar el trabajo en áreas, dentro de las cuales se irán añadiendo los respectivos usuarios que se necesiten. La creación de OU es tan sencilla como hacer clic con el botón derecho del ratón sobre el dominio y seleccionar la opción *Nuevo* → *Unidad organizativa*.

Para añadir un usuario en dicha unidad organizativa, se accede a esta, se hace clic con el botón derecho en algún lugar libre y se selecciona la opción *Nuevo* → *Usuario*.

Tras rellenar el formulario correspondiente, se debe asignar una contraseña y establecer las siguientes opciones, las cuales son recomendadas para garantizar la máxima seguridad.



Otra opción para añadir un nuevo usuario es a través del menú *Acción* → *Nuevo* → *Usuario*.

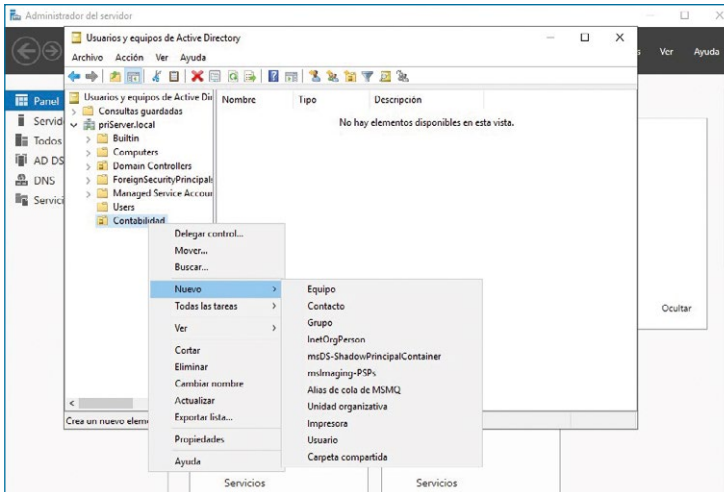


Figura 2.6
Añadir usuarios en AD.

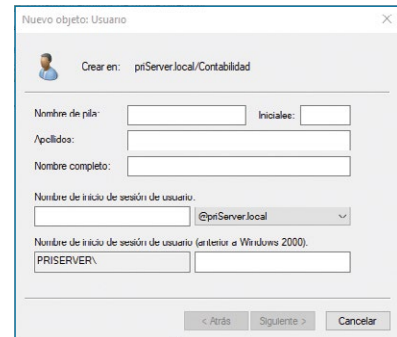


Figura 2.7
Formulario de nuevo usuario.

Actividad propuesta 2.1



Añade un nuevo usuario al dominio y comprueba que puede acceder al sistema, autenticándose en el dominio.

B) Creación de grupos

Para crear un grupo, lo haremos en la OU Contabilidad, haciendo clic con el botón derecho en ella y seleccionamos *Nuevo* → *Grupo*. En el asistente se especifica el nombre, el ámbito y el tipo de grupo (si es para listas de correo, seleccionaremos *Distribución*; y, si es para conceder permisos, *Seguridad*).

RECUERDA

- ✓ Para el mismo usuario, usando Windows PowerShell, la sintaxis es muy simple, en este caso se debe ejecutar el siguiente comando:

```
dsadd user "CN=contal,OU=Contabilidad,DC=prIServer,DC=local"
```

Los tipos de ámbitos son:

- *Dominio local*. Solo para el servidor local.
- *Global*. Para todos los equipos y servidores en el dominio.
- *Universal*. Tanto para conexiones locales como externas.

Para añadir un usuario a un grupo, existen dos posibilidades. La primera es acceder a las propiedades del grupo y en la pestaña *Miembros agregar los usuarios*. El segundo método es a través de las propiedades del usuario, accediendo a la pestaña *Miembro de*, y allí se comprueban los grupos en los que está actualmente, a la vez que se pueden agregar o quitar grupos.

Figura 2.8
Formulario para nuevo grupo.

Figura 2.9
Añadir usuarios a un grupo ya creado.



Actividad propuesta 2.2

Crema un nuevo grupo llamado “Empleados” y añade el usuario creado anteriormente a dicho grupo.

C) Creación de equipos

La administración de equipos se parece bastante a la administración de cuentas de usuario.

En la ventana *Usuarios y equipos de Active Directory*, en el panel de la izquierda, seleccionamos el contenedor que nos interese. En este caso, utilizaremos el contenedor *Equipos* (es recomendable mantener las cuentas de equipo en una OU separada de las cuentas de usuario).

RECUERDA

- ✓ Del mismo modo que con los usuarios, para crear un grupo usando Windows PowerShell, se usa el siguiente comando:

```
dsadd group "cn=Conta, ou=Contabilidad,dc=priServer,dc=local"
```

Es posible establecer diferentes opciones en el mismo comando agregando los siguientes parámetros:

- `secgrp [yes | no]`. Especifica si el grupo es de seguridad (yes) o de distribución (no).
- `scope [l | g | u]`. Especifica el ámbito del grupo: l para dominio local, g para global o u para universal.
- `samid Nombre`. Especifica el `sAMAccountName` (Identificador exclusivo predeterminado en Microsoft Active Directory) del grupo. Si no lo especificamos, el nombre del grupo será el especificado en el DN del grupo (*Distinguished Name* compuesto por el CN, *Common Name* o nombre del objeto, seguido de la unidad organizativa que contiene el objeto y del nombre del dominio).

- desc descripción. Establece la descripción del grupo
- members MemberDN. Añade miembros al nuevo grupo. Los miembros se especifican mediante sus DN y separados por espacios.
- memberof GroupDN. Hace que el nuevo grupo que estamos creando sea miembro de uno o mas grupos existentes. Los grupos también se especifican mediante su DN y separados por espacios.

Como por ejemplo:

```
dsadd group "cn=desarrollo,dc=priServer,dc=local" -samid desarrollo
        -secgrp yes -scope g -desc "Grupo Global de desarrollo"
```

En el menú *Contexto* que aparece tras hacer clic con el botón derecho del ratón, se elige *Nuevo* → *Equipo*.

En la ventana *Nuevo objeto: Equipo*, se rellena el nombre de la cuenta de equipo que se está creando (el nombre de equipo es la única información obligatoria). Por defecto, el administrador es el único que podría unir a este equipo al dominio, aunque es posible definir otro usuario o grupo para ello.

Figura 2.10
Formulario para nuevo equipo.

Actividad propuesta 2.3



Añade un nuevo equipo al dominio denominado "Prueba".

2.4.2. Sitios y servicios

En una red física, un sitio representa un conjunto de equipos conectados mediante una línea de alta velocidad, como una red de área local. En AD, los sitios representan la estructura física, o topología, de la red. Es importante distinguir entre sitios y dominios. Los sitios representan la estructura física de la red, mientras que los dominios representan la estructura lógica de la organización.

En sitios y servicios de AD, se pueden administrar los siguientes objetos:

- Sitios.
- Subredes.
- Servidores.
- Configuración NTDS.
- Conexiones.
- Vínculos a sitios.
- Transportes entre sitios IP y SMTP.

Los sitios facilitan varias actividades, entre las que se pueden incluir:

- a) *Replicación*. Se replica la información de directorio.
- b) *Autenticación*. Al iniciar sesión en un dominio, primero solicita la autenticación a un controlador de dominio del sitio local, garantizando que se usen los controladores de dominio más cercanos, reduciendo la latencia y el tráfico en las conexiones de red.
- c) *Ubicación de servicio*. Servicios como AD CS, Exchange Server y Message Queue Server, usan los servicios de dominio de Active Directory (AD DS) para almacenar objetos que pueden usar la información de la subred y el sitio, permitiendo encontrar los proveedores de servicio más cercanos de una forma más sencilla.

Los controladores de dominio se ubican en sitios según el lugar donde se necesitan los datos de dominio.

2.4.3. Dominios y confianzas

Una relación de confianza es un vínculo que se establece entre dos dominios diferentes y permite que los usuarios de un dominio sean autenticados por un controlador de otro dominio y tener acceso a sus recursos compartidos, con la confianza de que el otro dominio autenticará las cuentas de sus propios usuarios.

Otra ventaja de tener una relación de confianza es poder administrar de manera centralizada diversos dominios a la vez.

Existen cuatro tipos de relaciones disponibles: confianza externa, confianza de dominios, confianza de bosques y confianza de acceso directo.

- *Confianza externa*. Cuando los recursos están ubicados en un bosque diferente de AD. Una relación de confianza externa siempre es “no transitiva”.
- *Confianza de dominios*. Se crea cuando la relación es entre un bosque de AD y un directorio Kerberos que no sea Windows, como, por ejemplo, *eDirectory*.
- *Confianza de bosques*. Permite compartir recursos entre diversos bosques. Son relaciones transitivas y pueden ser unidireccionales o bidireccionales.
- *Confianza de acceso directo*. Mejora el tiempo de inicio de sesión de los usuarios. Este tipo de confianza siempre es transitiva y puede ser unidireccional o bidireccional.

El primer paso previo y fundamental es verificar la conectividad entre ambos dominios para que sean capaces de reconocerse en la red. Es necesario que los DNS estén correctamente configurados, de forma que el dominio en Windows Server pueda resolver los nombres del otro dominio. Para ello, se deben establecer los reenviadores condicionales correspondientes en ambos dominios.

Una vez comprobado que ambos dominios son visibles entre sí, se puede establecer la relación de confianza.

1. Acceder a *Dominios y confianzas de Active Directory*.
2. Seleccionar *Propiedades* del menú contextual del servidor y acceder a la pestaña *Confianzas* para crear una nueva confianza. (Es posible que existan relaciones ya creadas en el caso de tener subdominios, ya que estas se crean automáticamente cuando se crea un subdominio).
3. En el asistente, indicar el nombre del dominio con el que se quiere establecer la confianza (nombre NetBIOS o nombre DNS).

4. A continuación, establecer el tipo de confianza.
5. Establecer la dirección de la confianza, ya sea bidireccional, unidireccional de entrada o unidireccional de salida.

Una *Confianza de bosque* permite que los usuarios de cualquiera de los dominios en ambos bosques puedan autenticarse en los dominios del otro bosque.



TOMA NOTA

Una relación bidireccional son dos relaciones unidireccionales donde el dominio A confía en el dominio B, y el dominio B confía en el dominio A.

Normalmente, se requieren dos pasos para crear una relación de confianza. En el primero, un dominio debe asignar permisos de acceso a un segundo. A continuación, el segundo dominio se debe configurar para tener acceso al primero. Dado que la relación de confianza aún no se ha establecido, estos dos pasos los deben realizar administradores distintos. Existen otras formas de establecer las relaciones de confianza.

Una de ellas solo requiere que se cree una cuenta de usuario idéntica con privilegios administrativos en ambos dominios. Esta puede ser una opción útil para los administradores de red que usan contraseñas idénticas para todas las cuentas administrativas o que, al menos, las conocen y las pueden modificar mientras establecen la relación de confianza.



TEN EN CUENTA

La creación de cuentas duplicadas en dominios distintos anula la finalidad de tener una sola cuenta para toda la red, ya que los cambios efectuados en una cuenta deben realizarse también en el otro dominio.

2.5. Seguridad y políticas de grupos

2.5.1. Seguridad. Recomendaciones básicas

Un sistema informático debe ser mantenido y administrado periódicamente para evitar problemas de seguridad. Para ello, las siguientes recomendaciones deben ser adoptadas para asegurar unas mínimas garantías, tanto de seguridad como de continuidad del servicio.

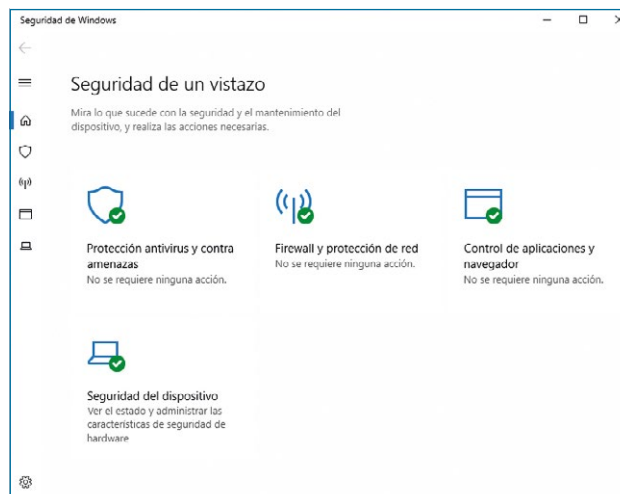


Figura 2.11
Seguridad de Windows.