

# 1. ÍNDICE

<b>1. ÍNDICE</b>	<b>1</b>
<b>2. PROLOGO</b>	<b>5</b>
<b>3. PRESENTACIÓN</b>	<b>6</b>
<b>4. COPYRIGHT</b>	<b>7</b>
<b>5. INTRODUCCIÓN</b>	<b>8</b>
<b>5.1. POR QUÉ USAR AD: DIAGRAMAS DE MODELO: WORKGROUP Y AD</b>	<b>8</b>
<b>6. ELEMENTOS</b>	<b>10</b>
<b>6.1. ELEMENTOS (1): ESTRUCTURA</b>	<b>10</b>
<b>6.2. ELEMENTOS (2): CONTROLADOR DE DOMINIO</b>	<b>10</b>
<b>6.3. ELEMENTOS (3): DOMINIO, ÁRBOL, BOSQUE</b>	<b>12</b>
6.3.1. CONCEPTOS BASADOS EN EJEMPLOS DE DOMINIO, ÁRBOL, BOSQUE	12
6.3.2. MUNDO REAL: MULTIDOMINIO VS DOMINIO ÚNICO	14
<b>6.4. ELEMENTOS (4): ESQUEMA</b>	<b>15</b>
<b>6.5. ELEMENTOS (5): CATÁLOGO GLOBAL</b>	<b>17</b>
<b>6.6. ELEMENTOS (6): ROLES FSMO</b>	<b>19</b>
6.6.1. DESCRIPCIÓN Y FUNCIONAMIENTO	19
6.6.2. IMPACTO EN CASO DE CAÍDA	24
6.6.3. CONCEPTOS PREVIOS SOBRE TRANSFER Y SEIZE DE ROLES FSMO	25
6.6.4. TRANSFER DE ROLES FSMO VÍA GUI	26
6.6.5. TRANSFER / SEIZE DE ROLES FSMO VÍA CMD	29
<b>6.7. ELEMENTOS (7): NTDS.DIT</b>	<b>30</b>
6.7.1. NTDS.DIT: LOCALIZACIÓN	30
6.7.2. NTDS.DIT: DESCRIPCIÓN DE LOS FICHEROS	32
6.7.3. NTDS.DIT: TAMAÑO DEL FICHERO ENTRE DCs	35
6.7.4. NTDS.DIT: PARTICIONES	35
<b>6.8. ELEMENTOS – (8): DISTINGUISHED NAMES (DN)</b>	<b>37</b>
6.8.1. DN: INTRODUCCIÓN Y NOMENCLATURA	37
6.8.2. DN: LOCALIZACIÓN	39
<b>6.9. ELEMENTOS - (9): SERVICIOS</b>	<b>40</b>
<b>6.10. ELEMENTOS - (10): DDP Y DDCP</b>	<b>42</b>
<b>7. HERRAMIENTAS DE ADMINISTRACIÓN</b>	<b>43</b>
<b>7.1. HERRAMIENTAS GUI</b>	<b>43</b>
7.1.1. USUARIOS Y EQUIPOS DE ACTIVE DIRECTORY (DSA.MSC)	43
7.1.2. CENTRO DE ADMINISTRACIÓN DE ACTIVE DIRECTORY (DSAC.EXE)	50
7.1.3. DOMINIOS Y CONFIANZAS DE ACTIVE DIRECTORY (DOMAIN.MSC)	55
7.1.4. DNS (DNSMGMT.MSC)	56
7.1.5. EDITOR ADSI (ADSIEDIT.MSC)	57
7.1.6. SITIOS Y SERVICIOS DE ACTIVE DIRECTORY (DSSITE.MSC)	58
7.1.7. LDP (LDP.EXE)	59

<b>7.2. HERRAMIENTAS CMD</b>	<b>62</b>
7.2.1. COMANDOS DS	62
7.2.2. CSVDE (CSVDE.EXE)	64
7.2.3. LDIFDE (LDIFDE.EXE)	65
7.2.4. NETDOM (NETDOM.EXE)	66
7.2.5. DNSCMD (DNSCMD.EXE)	67
7.2.6. NLTEST (NLTEST.EXE)	68
7.2.7. HERRAMIENTAS POWERSHELL	69
<b>7.3. HERRAMIENTAS DE TERCEROS WINDOWS</b>	<b>72</b>
7.3.1. ADEXPLORER	72
7.3.2. ADMODIFY	74
7.3.3. ADFIND	76
7.3.4. QUEST ACTIVE ROLES MANAGEMENT SHELL FOR ACTIVE DIRECTORY	77
<b>7.4. HERRAMIENTAS DE TERCEROS LINUX</b>	<b>79</b>
7.4.1. LDAP UTILS	79
<b>8. DNS - SERVIDOR</b>	<b>80</b>
<b>8.1. DNS AD FAQ.</b>	<b>80</b>
<b>8.2. CARACTERÍSTICAS ESPECIALES DEL DNS SERVER DE AD</b>	<b>84</b>
8.2.1. ALMACÉN DE LA ZONA EN AD	84
8.2.2. BACKUP Y RESTORE	86
8.2.3. DNS DINÁMICO (DDNS)	87
8.2.4. GLOBAL QUERY BLOCK LIST	88
<b>8.3. REENVIADORES VS SUGERENCIAS RAÍZ</b>	<b>90</b>
8.3.1. RESOLUCIÓN DE NOMBRES BASADA EN SUGERENCIAS RAÍZ	90
8.3.2. RESOLUCIÓN DE NOMBRES BASADA EN REENVIADORES	93
<b>8.4. CACHÉ DNS SERVER</b>	<b>95</b>
8.4.1. TTL	95
8.4.2. VER Y LIMPIAR LA CACHÉ	97
<b>8.5. DNS LOGS</b>	<b>100</b>
<b>9. DNS - CLIENTE</b>	<b>102</b>
<b>9.1. LOCALIZACIÓN DE LOS DC</b>	<b>102</b>
<b>9.2. SUFIJO DNS PRINCIPAL</b>	<b>103</b>
<b>9.3. REGISTRO DNS DE LA DIRECCIÓN IP</b>	<b>105</b>
<b>9.4. CACHÉ DNS</b>	<b>106</b>
<b>9.5. GPO CLIENTE DNS</b>	<b>108</b>
<b>10. AUTENTICACIÓN</b>	<b>108</b>
<b>10.1. SERVICIO NETLOGON</b>	<b>108</b>
10.1.1. NETLOGON: ESTADO Y MODO DEBUG	108
10.1.2. NETLOGON: CANAL SEGURO	110
<b>10.2. KERBEROS</b>	<b>113</b>
<b>10.3. NTLM</b>	<b>121</b>
<b>10.4. KERBEROS Y NTLM</b>	<b>124</b>
10.4.1. KERBEROS Y NTLM: ¿CUÁNDO DE USA CADA UNO?	124
10.4.2. KERBEROS Y NTLM: PROTECTED USERS	126
<b>10.5. TIPOS DE LOGIN</b>	<b>127</b>
<b>10.6. AUDITORIA DE LOGINS</b>	<b>129</b>

<b>11. DSRM</b>	<b>133</b>
11.1. DSRM – (1): UTILIDAD	133
11.2. DSRM – (2): ACCESO AL MODO DSRM	133
11.3. DSRM – (3): RESET DEL PASSWORD	135
11.4. DSRM – (4): SINCRONIZACIÓN DEL PASSWORD CON UNA CUENTA DE DOMINIO	136
<b>12. TOMBSTONE</b>	<b>137</b>
12.1. TOMBSTONE: DEFINICIÓN Y VALOR	137
12.2. TOMBSTONE: RECUPERACIÓN DE OBJETOS	139
12.3. TOMBSTONE: EFECTOS	140
<b>13. NIVELES FUNCIONALES</b>	<b>141</b>
13.1. UTILIZACIÓN	141
13.2. CONCEPTOS	141
13.3. EJEMPLO DE FUNCIONAMIENTO	143
13.4. FUNCIONALIDADES MÁS RELEVANTES SEGÚN NIVEL FUNCIONAL	144
13.5. HERRAMIENTAS GUI CLÁSICAS: ELEVAR EL NIVEL FUNCIONAL	146
13.6. HERRAMIENTA GUI NUEVA: ELEVAR EL NIVEL FUNCIONAL	147
13.6.1. POWERSHELL: REVERSIÓN DEL NIVEL FUNCIONAL	148
<b>14. RÉPLICA ENTRE DCS</b>	<b>149</b>
14.1. MODELO DE LA RÉPLICA	149
14.2. DIAGRAMA Y ELEMENTOS DE FUNCIONAMIENTO	151
14.3. RÉPLICA: DETALLE DE ATRIBUTOS REPLICADOS	152
14.4. RÉPLICA: HERRAMIENTA DE ADMINISTRACIÓN GUI: DSSITE.MSC	154
14.5. RÉPLICA: HERRAMIENTA DE ADMINISTRACIÓN GUI: AD REPLICATION TOOL	155
14.5.1. REPLICA: HERRAMIENTA DE ADMINISTRACIÓN CMD: REPADMIN	155
14.6. REPLICA: HERRAMIENTAS DE ADMINISTRACIÓN POWERSHELL	159
<b>15. HERRAMIENTAS DE DIAGNOSTICO</b>	<b>160</b>
15.1. DCDIAG	160
15.2. SNAPSHOTS DE AD	164
15.3. BPA	166
15.4. PERFMON	168
<b>16. BACKUP Y RESTORE</b>	<b>170</b>
16.1. VSS	170
16.2. MÉTODO TRADICIONAL: REALIZAR BACKUP	172
16.3. MÉTODO TRADICIONAL: REALIZAR RESTORE	173
16.3.1. TIPOS DE RESTORE	173
16.3.2. PROCEDIMIENTO PARA UN RESTORE AUTORITATIVO:	174
16.3.3. PROCEDIMIENTO PARA UN RESTORE NO-AUTORITATIVO:	177
16.4. BACKUP Y RESTORE DE AD EN ENTORNO VIRTUALIZADO	177
16.4.1. INTRODUCCIÓN	177

16.4.2. EL PROBLEMA: USN ROLLBACK _____	178
16.4.3. LA SOLUCIÓN: VM GENERATION ID _____	179
16.4.4. FAQ: VM GENERATION ID _____	183

**17. LIMPIEZA DE UN DC DE AD **185****

<b>17.1. ESCENARIO Y NECESIDAD DE LIMPIEZA _____</b>	<b>185</b>
<b>17.2. LIMPIEZA AUTOMÁTICA DE UN DC _____</b>	<b>187</b>
<b>17.3. VERIFICACIÓN DE LA LIMPIEZA _____</b>	<b>190</b>
<b>17.4. LIMPIEZA MANUAL DE UN DC _____</b>	<b>191</b>

**18. PRÓXIMAS PUBLICACIONES **197****

## 2. PROLOGO

Con el transcurso de los años, desde su primera versión con Windows Server 2000, Active Directory se ha convertido en un estándar en los servicios de directorio y administración de sistemas.

Si examinamos la documentación que existe sobre este servicio, la primera conclusión a la que llegaremos es que es un servicio pensado para grandes corporaciones.

También nos daremos cuenta de su gran complejidad.

Como conclusión de ambas afirmaciones, entendemos rápidamente que formarse en Active Directory es una apuesta de pasado, presente y futuro.

Sin embargo deberemos realizar un proceso de adaptación de conocimientos y procedimientos según la estructura que queramos diseñar y mantener.

Al cabo de los años de impartir formación, me he dado cuenta de varios hechos:

- Existe mucha documentación orientada al diseño de grandes infraestructuras para multinacionales: difícil de trasladar a empresas de menor dimensión.
- Existe documentación básica sobre la administración de Active Directory, sin embargo, esta se queda en la superficie y se limita a describir los procedimientos básicos.
- Existen conceptos muy importantes que no encontramos explicados de forma clara, práctica y sencilla.
- También encontramos documentación donde se mezclan otros temas junto con Active Directory y muchos conceptos importantes quedan diluidos.

El objetivo de este libro es trabajar con Active Directory y profundizar en todos aquellos temas importantes sin perder de vista que su implementación, administración y mantenimiento se realizará no necesariamente en entornos de grandes corporaciones.

Este libro cuenta con la ventaja de que temas relacionados con Active Directory como GPO (*GPOIT – Group Policy Objects para administradores de IT*), permisos (*WFS – Windows File Server*) o laboratorios paso a paso (*WS2012LABS – Windows Server 2012*) ya quedan explicados en libros anteriores.

De esta forma disponemos de todo un libro para poder explicar ampliamente, con profundidad temas prácticos y fundamentales sobre este servicio.

## 3. PRESENTACIÓN

*¿Cuál es el objetivo del libro?*

El objetivo de esta publicación es formar al lector para diseñar, implementar y administrar de forma práctica Active Directory basado en tecnología Windows Server, construyendo una infraestructura sólida, robusta y fiable.

*¿Cuál es la estructura del libro?*

El libro está estructurado en varios módulos donde se abordan todos aquellos temas imprescindibles para la correcta administración de servicios relacionados con Active Directory.

Veremos módulos orientados a fundamentos, herramientas, administración, mantenimiento y diseño de Active Directory.

*¿Sobre el autor?*

El autor es un administrador de sistemas de entornos Microsoft, GNU/Linux, VMware, etc con más de 10 años de experiencia en el sector.

Además es formador de tecnología Windows Server, Exchange, etc desde 2006.

*¿Cuál es el enfoque del libro?*

ES:

- Libro de trabajo, en formato A4, de cómoda lectura.
- Fundamentalmente práctico, claro y conciso.
- Laboratorios y escenarios propuestos de fácil despliegue.
- Orientado a la posterior implementación en una red pequeña, mediana o grande.

NO ES:

- En este primer volumen, no se recogen todas las funcionalidades del producto.
- No está orientado a la certificación oficial, pero sí encontrarás contenido para complementar ciertos temas de la certificación.

## 4. COPYRIGHT

ADIT – Active Directory para administradores de IT

ISBN 978-1-326-01175-8

© 2014 - Xavier Genestós Gil

Reservados todos los derechos. Esta publicación está protegida por las leyes de propiedad intelectual.

No se permite distribuir ni parcialmente, ni totalmente, la publicación a través de cualquier medio, soporte, sin autorización expresa del autor.

Todas las marcas, nombres propios, que aparecen en el libro son marcas registradas de sus respectivos propietarios, siendo su utilización realizada exclusivamente a modo de referencia.

El autor del libro no se hace responsable de los problemas que pueda causar en su infraestructura, siendo responsabilidad de los administradores de sistemas realizar las copias de seguridad, planes de contingencia y laboratorio de pruebas previo antes de aplicar cualquier cambio en los servidores de producción.

## 5. INTRODUCCIÓN

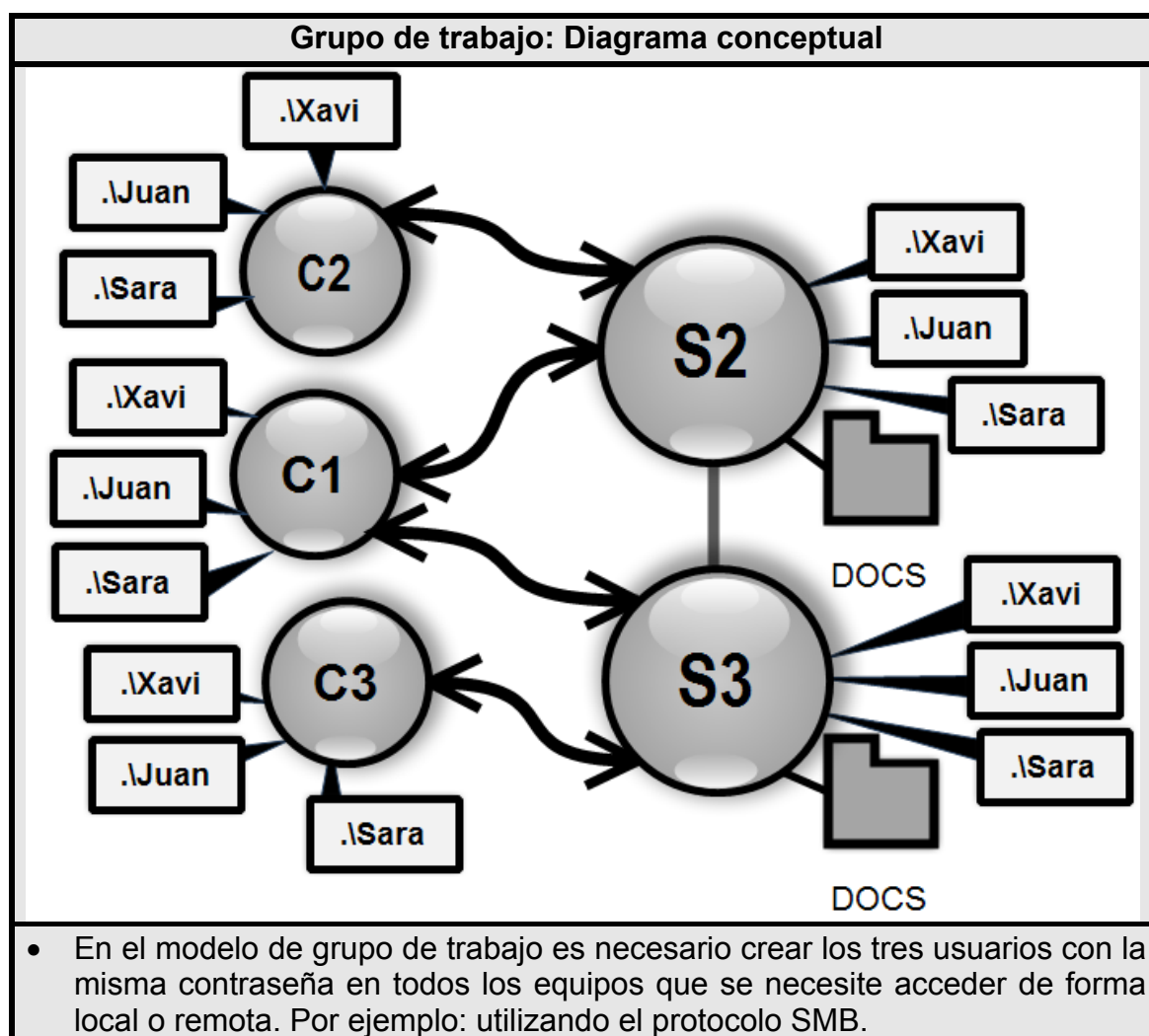
### 5.1. POR QUÉ USAR AD: DIAGRAMAS DE MODELO: WORKGROUP Y AD

Una de las principales ventajas del uso de Active Directory (AD) es la autenticación centralizada de los usuarios.

Para entender esta funcionalidad basta con comparar el modelo de AD de dominio con el modelo de un grupo de trabajo (workgroup).

Imaginemos que disponemos de tres equipos (C1, C2 y C3) y tres usuarios (Xavi, Juan y Sara) que necesitan acceder desde cualquier equipo a dos servidores de ficheros (S1 y S2).

Veamos como sería el diagrama conceptual según los dos modelos:





Puedes adquirir este libro en la editorial LULU:

<http://www.lulu.com/shop/search.ep?contributorId=1107000>

Como continuación de estos libros sobre administración de sistemas IT, dispones del blog:

<http://www.sysadmit.com>

# **SYSADMIT**

---