1. INDICE

1. INDICE 1

2. PRÓLOGO 5

3. PRESENTACIÓN 7

4. COPYRIGHT 8

5. VENTAJAS DEL USO DE GPO 9

6. ENTORNO DE LABORATORIO 10

7. LOCAL GPO 11

7.1. CARACTERÍSTICAS LGPO 11
7.2. EJEMPLO DE LGPO Y MLGPO 12
7.3. ADMINISTRACIÓN DE LGPO CON SCRIPTS 16
7.4. EVITAR LA APLICACIÓN DE LGPO CUANDO HAY GPO DE DOMINIO 17

8. FUNDAMENTOS DE GPO DE DOMINIO 18

8.1. OU VS CONTENEDOR 18
8.2. DEFAULT DOMAIN POLICY (DDP) 19
8.3. DEFAULT DOMAIN CONTROLERS POLICY (DDCP) 19
8.4. ENLACE A GPO VS GPO 20
8.5. GPO DE USUARIO VS GPO DE EQUIPO 21
8.6. CAMBIO DE UBICACIÓN POR DEFECTO DE USUARIOS Y EQUIPOS 23
8.7. NO TODAS LAS GPO SE APLICAN SOBRE TODOS LOS SO 24
8.8. GPO CON REQUISITOS DE NIVEL FUNCIONAL 25
8.9. HERENCIA: LAS GPO SON ACUMULATIVAS 26
8.10. ORDEN DE PROCESADO DE GPO: LA ÚLTIMA GANA 27
8.11. GPO CONTRADICTORIAS AL MISMO NIVEL 29
8.12. BLOQUEAR HERENCIA 30
8.13. VÍNCULO EXIGIDO 31
8.14. DESHABILITAR/HABILITAR VÍNCULO VS DESHABILITAR/HABILITAR GPO 33
8.15. FILTRADO DE SEGURIDAD GPO 34
8.16. LEER SIEMPRE LA AYUDA DE LA GPO. 37
8.17. GPMC SAMPLE SCRIPTS 39
8.18. POWERSHELL SCRIPTS 41
8.19. LAS GPO NO SE APLICAN SOBRE GRUPOS DE SEGURIDAD 43
8.20. DIRECTIVA DE CONTRASEÑAS 44
8.21. DESPLIEGUE DE SCRIPTS CON GPO 47
8.22. BÚSQUEDA DE ÍTEMS 48
8.22.1. MÉTODO1: FILTRADO DESDE LA GPMC 48
8.22.2. MÉTODO2: BÚSQUEDA EN LA WEB 50
8.22.3. MÉTODO3: FICHERO EXCEL 50
8.23. DISPONER DE VERSIÓN IGUAL O SUPERIOR DE DC RESPECTO A LOS CLIENTES. 51
8.23.1. ESCENARIOS POSIBLES (2000-2013) 51

8.23.2. ESCENARIO DC W2008 Y CLIENTES W7 52
8.24. COMENTARIOS EN LAS GPO 52
8.24.1. COMENTARIOS A NIVEL DE GPO 52
8.24.2. COMENTARIOS A NIVEL DE ÍTEM 53
8.25. DERECHOS DE USUARIO VS GPO 54

9. SERVIDOR: ESTRUCTURA, UBICACIÓN FÍSICA, REPLICACIÓN DE LAS GPO 57

9.1. FICHEROS ADM Y ADMX: PLANTILLAS ADMINISTRATIVAS (SERVIDOR) 57
9.2. CARPETA SYSVOL 59
9.3. GPLINK 68
9.4. ¿SOBRE QUE DC ESTAMOS EDITANDO LA GPO? 70
9.5. RÉPLICA DE GPO ENTRE CONTROLADORES DE DOMINIO 72
9.6. FAQ SOBRE LA RÉPLICA DEL SYSVOL 74
9.7. ESTADO DE LA RÉPLICA CON GPMC 75
9.8. GPOTOOL 77

10. CLIENTE: APLICACIÓN DE GPO DE DOMINIO 78

10.1. LECTURA POR DFS 78
10.2. REGISTRY.POL (SERVIDOR) > NTUSER.POL (CLIENTE) > NTUSER.DAT (CLIENTE) 79
10.3. HISTÓRICO DE APLICACIÓN DE GPO 83
10.4. CSE (CLIENT SIDE EXTENSIONS) 83
10.5. FOREGROUND / BACKGROUND REFRESH 85
10.6. FAST LOGON OPTIMIZATION CON GPO 88
10.7. FORZAR EL UPDATE 90
10.8. SLOW LINK 93

11. CONCEPTOS AVANZADOS DE GPO DE DOMINIO 96

11.1. VISOR RSOP SERVIDOR (RESULTADOS DE DIRECTIVAS DE GRUPO) 96
11.2. SIMULADOR RSOP SERVIDOR (MODELADO DE DIRECTIVAS DE GRUPO) 100
11.3. VISOR RSOP CLIENTE - RSOP.MSC 101
11.4. VISOR RSOP SERVIDOR/CLIENTE - GPRESULT.EXE 102
11.5. FILTROS WMI 104
11.5.1. HERRAMIENTAS DE DIAGNÓSTICO DE WMI 104
11.5.2. EJEMPLOS DE CONSULTAS WMI CON WMIC Y GET-WMIOBJECT 106
11.5.3. EXPLORADOR REPOSITORIO WMI 108
11.5.4. GPO CON FILTRO WMI - CONFIGURACIÓN 110
11.5.5. GPO CON FILTRO WMI - PRUEBA 112
11.5.6. GPO CON FILTRO WMI - EJEMPLOS DE CONSULTAS WMI 113
11.5.7. GPO CON FILTRO WMI - VENTAJAS Y DESVENTAJAS 114
11.5.8. GPO CON FILTRO WMI – MEDIR TIEMPO DE LA CONSULTA 114
11.5.9. GPO CON FILTRO WMI – ¿DONDE SE GUARDAN LOS FILTROS WMI? 115
11.6. STARTER GPO 116
11.7. MODO LOOPBACK (BUCLE INVERTIDO) 118
11.8. GPO CENTRAL STORE 124
11.8.1. FUNCIONAMIENTO SIN GPO CENTRAL STORE 124
11.8.2. FUNCIONAMIENTO CON GPO CENTRAL STORE 125
11.8.3. VENTAJAS Y DESVENTAJAS DEL GPO CENTRAL STORE 125
11.9. GROUP POLICY SOFTWARE INSTALLATION (GPSI) 126

11.9.1. SOBRE LOS PAQUETES MSI 126
11.9.2. PASOS A SEGUIR (I): SERVIDOR: PUNTO DE DISTRIBUCIÓN 126
11.9.3. PASOS A SEGUIR (II): SERVIDOR: CONFIGURAR GPO 127
11.9.4. ¿COMO DESINSTALAR LA APLICACIÓN INSTALADA CON GPO? 129
11.9.5. INSTALACIÓN DE SOFTWARE CON GPO BAJO SLOW LINK 129
11.9.6. DIAGNÓSTICO BÁSICO 130
11.10. REDIRECCIÓN DE CARPETAS 132
11.11. RESTRICCIÓN DE EJECUCIÓN DE PROGRAMAS 137
11.11.1. RESTRICCIONES CON SRP 137
11.11.2. RESTRICCIÓN SRP BASADA EN HASH 138
11.11.3. RESTRICCIÓN SRP BASADA EN RUTA DE ACCESO 140
11.11.4. REGISTRO RESTRICCIONES SRP 141
11.11.5. COMO SALTARSE LAS RSP DE FORMA GENÉRICA 142

12. GROUP POLICY PREFERENCES 143

12.1. GROUP POLICY SETTINGS (GPS) VS GROUP POLICY PREFERENCES (GPP) 143
12.2. USO DE TECLAS DE FUNCIÓN EN LA EDICIÓN DE GPP 144
12.3. "TATTOING" EN LAS GPP 146
12.4. ESTRUCTURA INTERNA DE LA GPP 150
12.5. OPCIONES COMUNES DE UNA GPP 150
12.6. VARIABLES DE ENTORNO DE UNA GPP 154

13. GPO SOBRE CUALQUIER APLICACIÓN 155

13.1. MAPA CONCEPTUAL 155
13.2. CASO1: EL FABRICANTE PROPORCIONA LA PLANTILLA 155
13.3. CASO2: EL FABRICANTE NO PROPORCIONA LA PLANTILLA 158
13.4. AVERIGUAR LA CLAVE EN EL REGISTRO QUE ACTIVA O DESACTIVA UNA OPCIÓN 158
13.5. DE .REG A GPO - USANDO UNA GPP 160
13.6. DE .REG A GPO - USANDO UNA GPS 161

14. HERRAMIENTAS DE DIAGNÓSTICO Y REPARACIÓN 165

14.1. CACHED LOGON 165
14.2. VISOR DE EVENTOS DE GPO 169
14.3. LOG GENÉRICO DE APLICACIÓN DE GPO A FICHERO DE TEXTO 170
14.4. LOGS DE APLICACIÓN DE GPP A FICHERO DE TEXTO VÍA GPO 171
14.5. ANALIZADOR DE LOGS 173
14.6. LOGS A FICHERO DE TEXTO GPMC 174
14.7. GPLOGVIEW 174
14.8. DCGPOFIX 176

15. PRINTSERVER - EJEMPLO DE CONFIGURACIÓN DESPLEGADA POR GPO EN EL CLIENTE 177

15.1. INSTALAMOS EL SERVICIO DE SERVIDOR DE IMPRESIÓN 177
15.2. INSTALAMOS UNA IMPRESORA EN EL SERVIDOR 178
15.3. DESPLEGAMOS IMPRESORA USANDO GPO 179
15.4. RESULTADO 182

16. CHECKLIST - DISEÑO DE AD, OU Y GPO 183

16.1. DISEÑO DE AD 183
16.2. DISEÑO DE OU 183
16.3. DISEÑO DE GPO 186
16.4. OPERATIVA DE GPO 191

17. PRÓXIMAS PUBLICACIONES 192

2. PRÓLOGO

¿Quieres aprender a administrar un Exchange de forma correcta?:

<<EX2013ADM – Exchange Server 2013 – Xavier Genestós>>

¿Quieres aprender a administrar un hipervisor con VMWare de forma correcta?

<<Virtualización Corporativa con VMware – Josep Ros>>

Libro del gran Josep Ros con el que aprendí a virtualizar.

¿Quieres aprender Windows Server 2012 utilizando laboratorios?

<<WS2012LABS – Windows Server 2012 – Xavier Genestós>>

¿Qué ocurre con las GPO?

Ahora ya hay respuesta: *<<GPOIT – Group Policy Objects para administradores de IT>>*

Después de formar a muchos administradores de sistemas y ver distintos entornos grandes y pequeños, llego a la conclusión de la necesidad de escribir este libro.

En mis primeras andaduras como técnico de sistemas en varias pymes españolas me tocaba realizar “la ruta” en todos los equipos para cambiar ciertas configuraciones en los equipos.

Era la época de NT 4.0 y algunas redes con Novell Netware 3.12. En pequeñas redes no era problema, pero en redes de más envergadura, era un autentico suplicio: repetir lo mismo tantas veces como equipos hubieran.

Disponía de administración centralizada la configuración de TCP/IP con DHCP, la gestión del antivirus, firewall, correo corporativo con Exchange pero no la configuración de los equipos.

Lo cierto es que con NT 4.0 ya existían las políticas de grupo, pero su función estaba orientada a restringir lo que podía hacer el usuario y lo que no, además existía el problema del tatuaje, por lo que la vuelta atrás era complicada.

Con Windows Server 2000, aparecen las GPO y fueron un salto cualitativo importante: su estructura y forma de despliegue no tenían nada que ver de cómo funcionaba con NT.

El salto definitivo fue la aparición de la GPMC, una consola dedicada para administrar las GPO. Ésta se podía descargar e instalar en cualquier

controlador de dominio con Windows Server 2003 y está integrada en el sistema a partir de Windows Server 2003 R2.

Quizás por injerencias del pasado o bien porque es una tecnología cuyo funcionamiento no se ha sabido explicar de forma clara, en muchas empresas de 20 o 30 equipos no se usa.

En empresas de mayor dimensión: 50, 100, 300, 500 se usa, pero se comenten muchos errores de diseño, estructura y administración que provocan ineficiencias, problemas, etc.

Para remediarlo, la solución es la de siempre: formarse, probar en laboratorio, probar en un entorno de producción pequeño y controlado y así ir creciendo poco a poco.

Veremos que con el transcurso del tiempo, los recursos dedicados a la administración de sistemas de IT crecen, mientras que los dedicados a helpdesk descienden. Evidentemente no en la misma proporción. Además, contra más grande sea nuestra infraestructura más aumenta la rentabilidad de la inversión en formarse y usar GPO.

En un presente y futuro donde se dibujan mejoras en la eficiencia, productividad y aprovechar los recursos al máximo, las GPO encajan a la perfección: primero porque no suponen un sobrecoste en cuanto a licenciamiento ni recursos en los servidores, ya que están integradas en nuestros controladores de dominio y segundo porque gracias a éstas podremos estandarizar, automatizar, etc.

También hay servicios, como WSUS, servidor de impresión, etc que se despliegan en los clientes con GPO.

Si echamos un vistazo al presente o futuro, veremos entornos VDI donde un buen uso de las GPO mejorará el rendimiento de nuestra infraestructura traduciéndose en un ahorro de costes.

Las GPO son el pasado, presente y futuro. Si ya las estamos usando, es posible que no estemos utilizando toda su potencia y funcionalidades. Si no las estamos usando, estamos realizando tareas de forma manual cuando podríamos automatizarlas y estandarizarlas.

Mi intención con este libro es formar al administrador de sistemas sobre el uso correcto de las GPO en entornos de Active Directory y mejorar su infraestructura para hacerla mas sólida, estable y robusta.

Veréis que se trata de un libro fundamentalmente práctico, orientado al entorno empresarial que va al grano. Se explica el concepto y se realiza un pequeño laboratorio para mostrar su funcionamiento.

También encontraremos explicaciones sobre qué es o no recomendable y los posibles problemas que puede ocasionarnos.

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 un sistema de directivas de grupo (GPO) basado en la tecnología Microsoft 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 los servicios de GPO.

Cada concepto está explicado con un pequeño laboratorio para ver de forma práctica su funcionamiento.

¿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 y Exchange 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:

- No está orientado a la certificación oficial, pero sí encontrarás contenido para complementar ciertos temas de la certificación.

4. COPYRIGHT

GPOIT - Group Policy Objects para administradores de IT

REV-B

ISBN 978-1-291-47370-4

5. VENTAJAS DEL USO DE GPO

Los administradores de sistemas tienden a pensar que el uso de GPO (Group Policy Objects) va dirigido exclusivamente a restringir el uso de componentes o configuraciones al usuario, de forma que si el usuario no puede tocar, el usuario no puede romper.

Esta afirmación es cierta, pero las ventajas y usos de GPO van mucho más allá.

Tecnología asentada: Nacen con Windows Server 2000, es una tecnología probada con muchos años de funcionamiento.

Las grandes corporaciones lo usan: Esto es garantía de continuidad, soporte y documentación para la solución de problemas.

Configuración centralizada: No será necesario conectar a los equipos para cambiar la configuración de estos, podremos administrar de forma centralizada desde una consola única: GPMC (Group Policy Management Console)

Configuraciones documentadas: Dispondremos de documentación de todas las configuraciones realizadas por GPO en la GPMC, pudiendo ver qué elementos han sido configurados y por tanto difieren de la configuración por defecto.

Automatizar: Ahorro de tiempo y menos errores humanos: Si no usamos GPO y realizamos cambios de configuración a mano en muchos equipos, es probable que en alguno de ellos nos equivoquemos.

Estandarizar: Disponer de grupos de usuarios o equipos con la misma configuración. Esto facilita el diagnostico de errores ya que disponemos de configuraciones iguales.

Mejora del rendimiento y uso de recursos en Terminal Server o VDI: Imaginemos por ejemplo el impacto de realizar una exclusión en la indexación del servicio de “Windows Search” en un Terminal Server o en escritorios virtuales de X usuarios.

6. ENTORNO DE LABORATORIO

Para efectuar las pruebas de laboratorio descritas en este libro necesitaremos implementar el siguiente escenario:

- Dos controladores de domino del mismo dominio.
- Un equipo cliente, añadido al dominio.

Todos los laboratorios y pruebas mostradas en este libro están realizadas sobre dos controladores de dominio Windows Server 2012 y un cliente Windows 7, sin embargo los conceptos y las funcionalidades son trasladables a versiones anteriores de sistema operativo.

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