Acerca de este documento:

Este documento corresponde a la segunda parte de *preguntas y respuestas* del libro "**ADIT – A**ctive **D**irectory para administradores de **IT**".

Dispone de 40 preguntas sobre temas explicados en el libro.

Realizando este test podrás evaluar el grado de conocimientos adquiridos antes y después de leerlo.

Si no dispones del libro "**ADIT – A**ctive **D**irectory para administradores de **IT**" con este test podrás evaluar si dispones de los conocimientos explicados en el libro antes de comprarlo.

En la penúltima página del documento hallarás todas las respuestas a las preguntas.

Puedes obtener más información acerca del libro "**ADIT – A**ctive **D**irectory para administradores de **IT**" así como otras publicaciones sobre sistemas informáticos, en el blog: http://www.SYSADMIT.com apartados:

Índice y referencias libros: http://www.sysadmit.com/p/vista-previa.html

FAQ libros: http://www.sysadmit.com/p/faq-libros.html

1) Indica que afirmaciones son ciertas sobre la Global Query Block List del DNS Server (marca todas las posibles):

A) Funcionalidad introducida a partir de Windows Server 2003
B) La funcionalidad no puede administrarse desde GUI.
C) Existen ya registros en la lista preconfigurados.
D) Está habilitada por defecto.
E) No está habilitada por defecto.

---

2) DNS Server: Resolución de nombres basada en reenviadores VS sugerencias raíz. Indica que afirmaciones son ciertas (marca todas las posibles).

A) La configuración por defecto es la resolución de nombres basada en reenviadores.
B) Es posible actualizar el fichero de las sugerencias raíz.
C) El fichero de las sugerencias raíz está ubicado en:
`C:\Windows\system32\dns\CACHE.DNS`
D) Son necesarias menos conexiones a DNS Servers en la resolución basada en reenviadores que la resolución basada en sugerencias raíz.
E) En la resolución basada en sugerencias raíz no actúa la caché.

---

3) DNS Server Caché: Indica que afirmaciones son ciertas (marca todas las posibles).

A) La caché del DNS Server no está activada por defecto.
B) El valor de de TTL por defecto de una zona es de: 2h.
C) Los registros dinámicos tienen un TTL de 20 minutos. El valor es distinto al de la zona.
D) Desde el lado cliente: Es posible ver el TTL de un registro con `nslookup` en modo debug.
E) Desde el lado cliente: Es posible ver el TTL de un registro con `ipconfig /displaydns`.

---

4) Indica las herramientas para ver o limpiar la caché del DNS Server. Marca todas las posibles.

A) `dnsmgmt.msc`
B) `dnscmd.exe`
C) Cmd-lets de PowerShell: `Show-DnsServerCache` y `Clear-DnsServerCache`
D) Solo es posible limpiar la caché reiniciando el servicio de DNS Server. No es posible ver la caché en el lado servidor.
E) `ipconfig /flushDNS`

---

5) Los equipos localizan a los DC del dominio utilizando DNS. ¿Qué tipo de registro es consultado que incluye el puerto de LDAP?

A) Tipo A.
B) Tipo CNAME.
C) Tipo SOA.
D) Tipo SRV.
E) Tipo TXT.

---

6) Si detenemos y deshabilitamos el servicio “Cliente DNS” de un equipo añadido al dominio…. Indica que afirmaciones son ciertas (marca todas las posibles).

A) El servicio no puede ser deshabilitado.
B) Conseguimos que no funcione la resolución DNS del equipo.
C) Conseguimos que no actúe la caché cliente, la resolución se realiza igualmente.
D) Conseguimos que no actúe el sufijo DNS principal.
E) Solo encontramos este servicio a partir de Windows 7 y Windows Server 2008 R2.

---

7) Sobre el servicio “Netlogon” de los equipos…. Indica que afirmaciones son ciertas (marca todas las posibles).

A) En equipos que residen en un Workgroup el servicio está en “Manual”.
B) En los DC el servicio está en “Manual”.
C) En los equipos añadidos al dominio el servicio está en “Automático”.
D) En los DC el servicio está en “Automático”.
E) Solo en los DC que disponen de alguno de los cinco roles FSMO el servicio está en “Automático”.

---

8) Sobre el servicio “Netlogon” de los equipos…. Indica que afirmaciones son ciertas (marca todas las posibles).

A) El servicio es necesario para la autenticación en AD tanto en el DC como en el lado cliente.
B) El servicio es necesario para la autenticación en AD solo en el lado cliente.
C) El servicio es necesario para la autenticación en AD solo en el DC.
D) Es posible activar el modo debug del servicio.

---

9) Necesitamos verificar el canal seguro entre DC y cliente. ¿Cómo lo podemos hacer? Marca todas las posibilidades.

A) `Netdom`
B) cmd-let de PowerShell: `Test-ComputerSecureChannel`
C) Solo puede verificarse revisando el Visor de eventos (`eventvwr.msc`)
D) `fsdpc`
E) `gpresult`

---

10) En AD: El protocolo preferente utilizado en la autenticación es Kerberos a partir de…

A) Windows Server 2000 como DC y clientes Windows 2000 (añadidos al dominio).
B) Windows Server 2000 como DC y clientes Windows XP (añadidos al dominio).
C) Windows Server 2003 como DC y clientes Windows XP (añadidos al dominio).
D) Windows Server 2003 como DC y clientes Windows Vista (añadidos al dominio).
E) Windows Server 2008 como DC y clientes Windows Vista (añadidos al dominio).

---

11)
El servicio Kerberos Key Distribution Center (KDC) está funcionando en…
Indica las afirmaciones que son ciertas (marca todas las posibles):

A) Todos los DC.
B) El DC con el rol de PDCe
C) El DC con el rol de RID Master.
D) En todos los Windows Server sean o no DCs.
E) Todas son falsas.

---

12)
Sobre la cuenta de: KRBTGT
Indica las afirmaciones que son ciertas (marca todas las posibles):

A) Se encuentra disponible a partir de Windows Server 2008.
B) Por defecto está deshabilitada.
C) Por defecto está ubicada en el contenedor Users.
D) Esta cuenta no debería ser borrada.
E) Todas son falsas.

---

13) Sobre la herramienta `SetSPN`:

Indica las afirmaciones que son ciertas (marca todas las posibles):

A) El parámetro –X está incluido solo a partir de Windows Server 2008.
B) El parámetro –X permite ver duplicados.
C) El parámetro –X está incluido solo a partir de Windows Server 2012.
D) El parámetro –X permite exportar y convertir la configuración.
E) El parámetro –X permite crear alias de SPNs.

---

14) Existen varias herramientas para ver el UPN de un usuario…

Indica las afirmaciones que son ciertas (marca todas las posibles):

A) `dsa.msc`
B) Cmd-let de PowerShell: `Get-ADUser`
C) `dsac.exe`
D) `whoami /UPN`
E) Todas son falsas.

---

15) Para que no se rompa el Kerberos: Por defecto el desfase horario entre servidor y cliente puede ser de cómo máximo…

A) Depende del nivel funcional del dominio.
B) Depende del valor de tombstone del dominio.
C) 30 minutos.
D) 20 minutos.
E) 5 minutos.

---

16) Disponemos de un entorno de dominio único con dos DC.
Los equipos añadidos al dominio sincronizarán la hora con…

A) El DC con el rol FSMO de PDCe.

B) Cualquier DC del dominio.

C) El DC o DCs que tengan marcado el catálogo global (GC).

D) Con el servidor NTP externo: time.windows.com a menos que no se cambie manualmente la configuración.

E) Todas son falsas.

---

17) Disponemos de un entorno de dominio único con tres DC.
El mapa de roles FSMO es el siguiente:

```
C:\>netdom query fsmo
Maestro de esquema          DC2.D1.local
Maestro nomencl. dominios   DC1.D1.local
PDC                         DC1.D1.local
Administrador de grupos RID DC2.D1.local
Maestro de infraestructura  DC3.D1.local
El comando se completó correctamente.
```

El DC2 sincronizará la hora con…

A) Con DC1

B) Con un servidor NTP externo.

C) Con la BIOS del sistema.

D) Con DC3

E) Todas son falsas.

---

18) Para eliminar la caché Kerberos en el lado cliente podemos utilizar… (marca todas las posibles).

A) `Net Stop "Cliente de Kerberos" /Y && Net Start "Cliente de Kerberos" /Y`

B) `Klist purge`

C) `ipconfig /kbtclear`

D) `Net Stop "KBTClient" /Y && Net Start "KBTClient" /Y`

E) Ninguna de las anteriores.

---

19) El TimeSkew de un ticket Kerberos indica…:

A) El desfase horario entre un servidor NTP externo configurado con el del equipo.

B) El desfase horario entre el equipo y el DC que le ha dado el ticket.

C) El tiempo de validez del ticket Kerberos.

D) El tiempo que permanecerá en caché el ticket.

E) La hora en que se procederá a renovar el ticket: No necesariamente se generará un ticket nuevo.

---

20) Indica que afirmaciones son ciertas sobre el protocolo NTLM y Kerberos. (marca todas las posibles):

A) Podemos ver con el <<Visor de eventos>> (`eventvwr.msc`) si la autenticación de un usuario se ha realizado con NTLM o Kerberos.

B) En la replicación entre DCs siempre se utiliza Kerberos.

C) En la replicación entre DCs siempre se utiliza preferentemente Kerberos y failover a NTLM.

D) Si se accede a un recurso compartido por IP en vez de por nombre el protocolo de autenticación utilizado será: NTLM

E) Para que funcione la autenticación Kerberos de un usuario será necesario que el usuario disponga de un UPN.

---

21) Sobre el grupo de seguridad “Protected Users”…
Indica las afirmaciones que son ciertas (marca todas las posibles):

A) Solo está disponible a partir de Windows Server 2012.

B) Solo está disponible a partir de Windows Server 2012 R2.

C) Los usuarios miembros de este grupo solo podrán utilizar la autenticación Kerberos y no NTLM.

D) Los usuarios miembros de este grupo solo podrán utilizar indistintamente la autenticación Kerberos y NTLM.

E) Solo está disponible a partir de Windows Server 2008 R2.

---

22) Sobre el comando `auditpol.exe`...

Indica las afirmaciones que son ciertas (marca todas las posibles):

A) Puede modificar la directiva de auditoría local.

B) Puede modificar la directiva de auditoría local y de dominio.

C) Solo está disponible a partir de Windows Server 2012.

D) Permite modificar el tipo de autenticación: Kerberos o NTLM.

E) Ninguna de las anteriores.

---

23) Sobre la contraseña DSRM (Directory Services Restore Mode) de los DC:

Indica las afirmaciones que son ciertas (marca todas las posibles):

A) Al iniciar en modo DSRM, los servicios de AD estarán iniciados.

B) Al iniciar en modo DSRM, los servicios de AD estarán detenidos.

C) La contraseña se asigna en el proceso de promoción a DC y puede ser distinta para cada DC.

D) El modo DSRM solo está disponible a partir de Windows Server 2008.

E) En modo DSRM no tendremos disponible la red.

---

24) Podemos cambiar el password de acceso al modo DSRM de un DC con: (Marca todas las posibles)

A) `dsa.msc`

B) `ntdsutil` con AD detenido.

C) `ntdsutil` con AD iniciado.

D) `Net user` con AD iniciado.

E) `dsmod` con AD iniciado.

---

25) Es posible sincronizar el password de una cuenta de AD con el password de DSRM. Podemos realizar el proceso de sincronización de los passwords con:

A) `dsa.msc`

B) `ntdsutil` con AD detenido.

C) `ntdsutil` con AD iniciado.

D) `Net user` con AD iniciado.

E) `dsget` con una pipe a `dsmod` con AD iniciado.

---

26) El valor de Tombstone… (Marca todas las posibles)

A) Es guardado como un atributo dentro de AD.

B) Se genera al promocionar el primer DC y se mantiene el valor aunque despromocionemos y promocionemos un nuevo DC.

C) Se genera al promocionar el primer DC y se actualiza el valor al despromocionar y promocionar un nuevo DC.

D) Podemos ver el valor con `dsquery`.

E) El valor por defecto puede ser 60 o 180 días.

---

27) La papelera de reciclaje de AD requiere…

A) Versión de los DCs: Windows Server 2012 o superior.
B) Nivel funcional del bosque: Windows Server 2008 R2 o superior.
C) Nivel funcional del bosque: Windows Server 2008 o superior.
D) Nivel funcional del bosque: Windows Server 2012 o superior.
E) Versión de los DCs: Windows Server 2003 o superior.

---

28) Para elevar el nivel funcional del dominio es necesario que el DC con el rol FSMO de …. esté disponible.

A) RID Master
B) Domain Naming Master
C) Schema Master
D) PDCe
E) Catálogo Global (GC).

---

29) Marca los sistemas operativos que admiten el nivel funcional: Windows 2000 nativo:

A) Windows Server 2012
B) Windows Server 2008 R2
C) Windows Server 2008
D) Windows Server 2003
E) Windows Server 2000

---

30) Indica a partir de qué nivel funcional de bosque y versión de sistema operativo se permite la inclusión de un RODC en el dominio.

A) SO: Windows Server 2008 / NF: Windows Server 2008
B) SO: Windows Server 2008 / NF: Windows Server 2003
C) SO: Windows Server 2003 / NF: Windows Server 2003
D) SO: Windows Server 2008 R2 / NF: Windows Server 2008
E) SO: Windows Server 2008 R2 / NF: Windows Server 2008 R2

---

31) ¿El nivel funcional puede revertirse en según qué casos?

A) No, no es reversible.
B) Con cmd-lets de PowerShell a partir de Windows Server 2012.
C) Con cmd-lets de PowerShell a partir de Windows Server 2012 R2.
D) Con cmd-lets de PowerShell a partir de Windows Server 2008.
E) Con cmd-lets de PowerShell a partir de Windows Server 2008 R2.

---

32) Sobre la réplica de AD. Indica que afirmaciones son ciertas:

A) Cualquier DC puede lanzar réplicas de cambios sobre los demás.
B) Los DC que no dispongan de ninguno de los cinco roles FSMO no podrán lanzar réplicas de cambios sobre los demás.
C) Es imprescindible el DNS para que funcionen las réplicas.
D) Existe un failover de DNS a IP en caso de que no funcione correctamente el DNS.
E) Es necesario el servicio RPC/IP para que funcionen las réplicas.

---

33) Sobre la réplica de AD: Cuando un usuario cambia el password:
Indica que afirmaciones son ciertas:

A) Solo se replican los atributos que han cambiado al resto de DCs.
B) Se replica el objeto con todos sus atributos, hayan cambiado o no.
C) Por defecto, el cambio es replicado dentro de 1h al resto de DCs.
D) En este caso no se utiliza Kerberos para cifrar la réplica.
E) El DC con el rol de Domain Naming Master tiene que autorizar la réplica.

---

34) Indica con que herramientas es posible forzar una replicación entre DCs.

A) Active Directory Replication Status Tool
B) `repadmin`
C) Sitios y servicios de Active Directory (`dssite.msc`)
D) PowerShell (`sync-adobject`)
E) `dsa.msc`

---

35) Si ejecutamos `dcdiag /Q` sobre un DC:

A) Modo Quick: Va más rápido.
B) Solo muestra los errores.
C) El parámetro no es correcto.
D) Realiza un test de solo el DNS.
E) Ninguna de las anteriores.

---

36) Los snapshots de AD se realizan con la herramienta `ntdsutil` y se enlazan a una IP y un puerto con la herramienta: `dsamain`.
Indica que afirmaciones son ciertas sobre los snapshots de AD:

A) Permiten retroceder el estado actual de AD a un snapshot realizado.
B) La funcionalidad está disponible a partir de Windows Server 2008.
C) Podemos conectar `dsa.msc` al snapshot, pero en modo solo lectura.
D) Podemos modificar objetos del snapshot que hemos montado.
E) Es necesario el nivel funcional de dominio Windows Server 2012 o superior.

---

37) Indica las herramientas con las que podemos encontrar los clientes de AD que consumen más CPU de un DC.

A) `dcdiag`
B) `perfmon`
C) `klist`
D) `replmon`
E) PowerShell: `GetADDS-Status`

---

38) Podemos ver la fecha y hora del último backup de AD ejecutando… (Marca todas las posibles).

A) PowerShell: `GetADDS-Status`
B) `dcdiag`
C) No es posible saberlo.
D) `netbackup`
E) `Repadmin /showbackup *`

---

39) Cual es el primer síntoma que padecerá nuestro AD si sufre un USN-Rollback:

A) Los DC se reinician constantemente.
B) Los DC siempre entran en modo DSRM.
C) Los DC dejan de replicar.
D) Los servicios de AD no se inician.
E) El DNS Server no inicia.

---

40) Una vez sufrimos un USN-Rollback. ¿Que estaremos obligados a hacer?
Marca solo una respuesta.

A) Limpieza manual de AD del DC.
B) Añadir un DC nuevo.
C) Reparar las réplicas con `repadmin`.
D) Configurar un DNS alternativo.
E) Renombrar el fichero `ntds.dit` con los servicios de AD detenidos.

Respuestas			
1	B,C,D	26	A,B,D,E
2	B,C	27	B
3	C,D	28	D
4	A,B,C	29	B,C,D,E
5	D	30	B
6	C	31	E
7	A,C,D	32	A,C,E
8	A,D	33	A
9	A,B	34	B,C,D
10	A	35	B
11	A	36	B,C
12	B,C,D	37	B
13	A,B	38	E
14	A,B,C,D	39	C
15	E	40	A
16	B		
17	A		
18	B		
19	B		
20	A,B,D,E		
21	B,C		
22	A		
23	B,C		
24	C		
25	C		

Calcula tu resultado del 1 al 10:

Resultado: (Número de respuestas OK * 10) / 40

- Ejemplo de 28 respuestas OK:

  Resultado: (28 * 10) / 40 = 7

- Ejemplo de 23 respuestas OK:

  Resultado: (23 * 10) / 40 = 5,75