Replicación de PDC's y SLAPD

Sergio González González
Instituto Politécnico de Bragrança, Portugal

sergio.gonzalez@hispalinux.es

Jonatan Grandmontagne García
Instituto Politécnico de Bragrança, Portugal

jon@alunos.ipb.pt

Breve explicación sobre como se hace la replicación en los servidores PDC de MS Windows y Samba (http://www.samba.org/), así como en openLDAP (http://www.openldap.org/).

1. Introducción

Antes de proceder a la explicación de las partes que componen este documento, vamos a dar una serie de definiciones previas:

- *PDC (Primary Domain Controller)*: un PDC es un servidor capaz de responder a las peticiones de autentificación de las máquinas pertenecientes a un dominio determinado.
- *BDC (Backup Domain Controller)*: un BDC es un servidor secundario.

  Un BDC es recomendable en los siguientes casos:

  - En redes donde exista un PDC y este normalmente esté muy ocupado. El BDC en este caso recibirá algunas peticiones de autentificación, quitando de esta forma trabajo al PDC.
  - En redes remotas la existencia de un BDC es deseable para reducir el tráfico y añadir estabilidad a las operaciones.

2. Replicación de BDCs bajo MS Windows

En esta sección vamos a ver la sincronización de la base de datos de un Dominio de MS Windows por los distintos controladores de dominio, así como la replicación de los datos importantes.

El servicio de replicación proporciona los mecanismos para copiar dicha información a cada BDC de la red.

Periódicamente, el servidor PDC de MS Windows sincroniza la base de datos de cuentas de dominio con cada BDC de la red. Este sólo envía aquellos datos que han cambiado, reduciendo así el tráfico de red. La sincronización es necesaria para mantener la base de datos de las cuentas de dominio consistente, esto permite a cada BDC validar las peticiones de autentificación de los usuarios.

Existe un tiempo de espera hasta que las modificaciones realizadas en la base de datos de las cuentas del dominio se propaguen a los servidores BDC, por lo tanto, si un usuario intenta autentificarse antes de que los cambios se hayan actualizado en el BDC, dicho usuario no tiene garantizados todos sus derechos y privilegios, debido a que el BDC está utilizando una base de datos no actualizada.

2.1. Como se realiza la replicación

El servidor *NetLogon* comprueba el estado de la base de datos y envía un pulso, o una notificación de cambio, a los BDCs cuando se ha producido un cambio. El intervalo de comprobación se conoce como *intervalo de replicación*

> **Nota:** Si el intervalo de replicación es muy alto, implicará que el PDC incremente su carga, pero si este es demasiado bajo, el tráfico de red será muy elevado entre los servidores. Para controlar este hecho, muchos BDCs son actualizados simultáneamente.

La configuración del pulso se realiza de la siguiente forma en el registro de MS Windows:

```
Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services\NetLogon\Parameters
Type: REG_DWORD
Name: PulseCurrency
Value: # of BDCs to simultaneously update
Default=10 BDCs, min=1, max=500
```

Cuando el tiempo del pulso se ha agotado, todas las bases de datos SAM son actualizadas. No se envía ningún pulso a aquellos BDCs que están actualizados.

Período de espera del PDC antes de enviar un pulso de actualización:

```
HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services\NetLogon\Parameters
Type: REG_DWORD
Name: Pulse
Value: value in seconds
min=60 ; default= 300 (5 min) ; max=172,800 (48hrs)
```

Envío de un pulso, tanto si la base de datos SAM de los BDCs están actualizadas como si no:

```
Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services\NetLogon\Parameters
Type: REG_DWORD
```

```
Name: PulseMaximum
Value: value in seconds
min=60 ; default=7200 ; max=86400
```

Tiempo de espera del PDC a que responda el BDC al pulso. Si el BDC no responde, este se considerará controlador sin respuesta.

```
Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services\NetLogon\Parameters
Type: REG_DWORD
Name: PulseTimeout1
Value: value in seconds
min=1 ; default=5 ; max=120
```

Tiempo de espera del PDC a que el BDC complete la sincronización parcial. Si el BDC no responde se considerará como servidor *sin respuesta*:

```
Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services\NetLogon\Parameters
Type: REG_DWORD
Name: PulseTimeout2
Value: value in seconds
min=60 ; default=300 ; max=3600
```

% de 128K de un paquete estándar utilizado para la sincronización del dominio:

```
Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services\NetLogon\Parameters
Type: REG_DWORD
Name: ReplicationGovernor
Value: % bandwidth
min=0 Default=100%
```

3. Replicación de un dominio con Samba (BDC)

La replicación de la base de datos SAM de Samba es controlable manualmente, siendo automatizable gracias al demonio cron. Para esto, samba ha de configurarse primeramente como un BDC, un ejemplo de configuración puede ser:

```
[global]
workgroup = NTDOMAIN
password server = pdcname
; because the pdc is the
; domain master!
domain master = no
domain logons = yes
security = user
encrypt passwords = yes
server schannel = yes
client schannel = yes
```

```
[netlogon]
; stores login scripts
read only = yes
path = /usr/local/samba/netlogon
```

Una vez realizado lo anterior y Samba se ha unido al dominio, ya estamos en disposición de replicar la base de datos SAM, en caso de ser necesario.

Actualmente, los protocolos de replicación de la base de datos SAM de MS Windows no han sido completamente implementados en Samba, por lo que no es posible hacer una replicación a partir de un servidor MS Windows. Es decir, un servidor BDC de Samba, sólo puede funcionar con un servidor PDC de Samba.

El archivo `smbpasswd` ha de ser replicado siempre que este cambie, lo que implica actualizar dicho archivo muy a menudo. Hay muchas posibles formas de replicación, siendo una de ellas la utilización de la herramienta rsync. Como los datos almacenados en el archivo `smbpasswd` están en texto plano, es más que recomendable hacer uso de encriptación para transmitirlos por la red. Esto se soluciona haciendo uso de ssh, ya que rsync soporta la transferencia de datos por este protocolo.

> **Nota:** El método arriba expuesto no es el mejor ni el más fiable, pero muestra la forma en la que se ha de replicar la base de datos SAM. Una forma más elegante de replicar dicha base de datos, es haciendo uso de LDAP.

4. Replication with slurpd

El acrónimo slurpd significa: *Standalone LDAP Update Replication Daemon* y su misión es propagar los cambios de una base de datos slapd hacia otra. Si slapd está configurado para producir logs de replicación, slurpd los lee y envía los cambios a las instancias slapd esclavas a través del protocolo LDAP. slurpd se arranca, normalmente, en el arranque del sistema.

Una vez arrancado, slurpd normalmente hace un fork de si mismo y se independiza de la *tty* que lo ha llamado, luego lee el log de replicación (dado bien por la directiva *replogfile* del archivo de configuración de slapd, bien por la opción *-r* de la línea de comandos). Si el archivo log de replicación no existe o está vacío, slurpd *se duerme*. Después, cada cierto tiempo, *se despierta* y verifica si hay cambios que propagar.

Cuando slurpd encuentra cambios a propagar hacia las instancias slapd esclavas, bloquea el log de replicación, hace una copia privada del mismo, libera el bloqueo anteriormente puesto y crea un fork de si mismo para réplica de slapd que ha de ser actualizada. Cada proceso hijo se asocia con el demonio slapd esclavo, y envía los cambios.

Un ejemplo de replicación podría ser:

- El cliente LDAP envía una modificación LDAP al slapd esclavo.
- El slapd esclavo devuelve una remisión hacia el cliente LDAP, referenciandolo hacia el servidor slapd maestro.

- El cliente LDAP envía la operación de modificación LDAP hacia el slapd maestro.
- El slapd maestro realiza la operación de modificación, escribe los cambios en su archivo log de replicación y devuelve un código de éxito hacia el cliente.
- El proceso slurpd verifica que se ha añadido una nueva entrada al archivo log de replicación, lee la entrada del log de replicación y envía el cambio hacia el servidor slapd esclavo vía LDAP.
- El servidor slapd esclavo realiza la operación de modificación y un código de éxito hacia el proceso slurpd.

5. Sobre este documento

Bibliografía

Documentación

[Account management (http://www.pinoy7.com/winnt/pt6_5.htm)]

[Windows NT Domain Controller Synchronization and Replication Parameters (http://is-it-true.org/nt/registry/rtips97.shtml)]

[Samba Project Documentation (http://www.samba.org/)] Jelmer R. Vernooij, John H. Terpstra, y Gerald Carter.

[Samba and Windows NT Security Interoperability (http://www.usenix.org/events/lisa-nt2000/full_papers/leighton/leighton.pdf)] Luke Kenneth Casson Leighton.

[OpenLDAP 2.1 Administrator's Guide (http://www.openldap.org/)] The OpenLDAP Project.

[Página del manual de slurpd] The OpenLDAP Project.