

WAPPLES 운영 가이드

WAPPLES 4.0 DB 인스턴스 정리 Script

Penta Institute | 2017

목차

- I. 개요
- II. 스크립트 설명
- III. 스크립트 사용 순서
- IV. 스크립트 상세 화면
- V. 스크립트 적용 사례
- VI. 주의 및 참고 사항

I. 개요

1. 개요

- 1) Postgresql wrap around failure를 극복하기 위한 스크립트

2. 기능

- 1) 새로운 DB Instance를 만들어서 데이터베이스를 fresh하게 사용할 수 있게 하는 스크립트

3. 전제조건

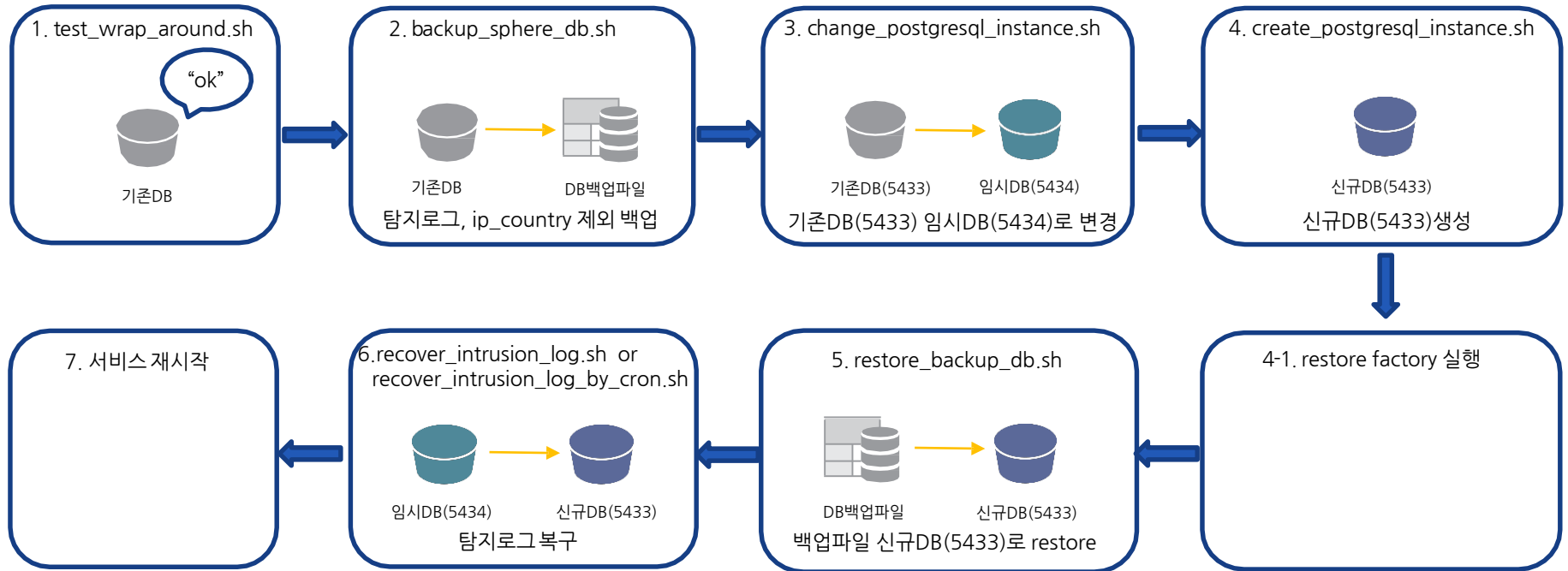
- 1) recover_db_20160513.tar.gz 파일을 /usr/penta_np/download 폴더로 업로드 후 압축 해제
→ 압축 해제 명령어 : tar xf recover_db_20160513.tar.gz
- 2) 압축 해제 시 /usr/penta_np/download/recover_db/ 디렉토리 생성
- 3) 스크립트 실행 전 H/W or S/W bypass 실행

주의사항 1 ※ PLS 동기화, WAPPLES-MS 연결 및 DB와 관련된 설정은 종료 해야 하며, 관리도구 접속 종료 후 실행

주의사항 2 ※ 압축해제시 반드시 장비 내에서 압축 해제 할 것

I. 개요

4. 스크립트 흐름도



II. 스크립트 설명

1. test_wrap_around.sh

- 1) 현재 DB 상태가 wrap around failure가 발생했는지 검사하는 스크립트
- 2) “OK” 라는 메시지가 나오면 wrap around가 발생하지 않은 DB
- 3) “OK” 메시지가 나온 장비에 대해서만 스크립트 정상 작동
- 4) DB 검사조건
 - A. DB 트랜잭션 값이 wrap around 되어 음수 값이 있는지 검사
 - B. 테이블 중복 검사
 - C. 테이블이 없는지 검사
 - D. 글로벌 설정 테이블이 백업 되는지 검사

2. backup_sphere_db.sh

- 1) 현재 데이터베이스의 데이터를 백업
- 2) 단, 탐지로그와 ip_country데이터는 백업대상에서 제외
- 3) /usr/penta_np/download/backup_sphere_db 디렉토리 하위에 실행 시간으로 백업파일 생성
- 4) 백업 실패 시 백업 디렉토리는 자동 삭제되며, 성공한 백업만 디렉토리에 존재함
- 5) 주기적으로 백업을 실행하여 필요 시 복구할 수 있음
- 6) 백업에 실패 한다면 스크립트 정상 동작하지 않음

II. 스크립트 설명

3. change_postgresql_instance.sh

- 1) 현재 사용중인 DB instance를 임시 DB instance로 변경
- 2) Instance 변경 시 기존 DB 포트(5433)가 아닌 임시 DB 포트(5434)로 시동
 - A. netstat -lntp 명령어로 5434 포트가 떠 있는지 확인
- 3) 기존 DB 경로 /var/lib/postgresql 변경 DB 경로 /var/lib/postgresql_old
- 4) /var/lib/postgresql_old 디렉토리가 존재한다면 동작하지 않음. 존재한다면 postgresql_old 디렉토리 삭제, 변경 후 사용

4. create_postgresql_instance.sh

- 1) DB instance(5433) 새로 생성
- 2) 탐지로그 시퀀스 정보는 경로를 변경한 postgresql_old(5434)에서 가져온 시퀀스 정보로 보정
 - A. 보정 이유는 탐지로그 복구시 시퀀스 문제가 일어나지 않도록 하기 위함이고 새로운 탐지로그가 쌓이지 않는 문제를 해결하기 위함

5. restore_backup_db.sh

- 1) 백업 디렉토리(/usr/penta_np/download/backup_sphere_db/파일명)를 인자로 받아 현재 DB를 백업 디렉토리 데이터로 복구
 - ex) restore_backup_db.sh /usr/penta_np/download/backup_sphere_db/2014-10-15_15-48-37

II. 스크립트 설명

6. recover_intrusion_log.sh

- 1) 경로를 변경한 postgresql_old(5434)로 부터 탐지로그를 복구 시킬 준비 또는 한번에 탐지로그를 복구
- 2) 복구할 탐지로그 개월 수를 인자로 받음(ex : recover_intrusion_log.sh -n 6(6개월 치 복구)) → 인자를 넣지 않으면 모든 탐지로그 복구
- 3) 동작방식
 - A. 스크립트 실행하면 입력 받은 탐지로그 데이터 개수를 표시
 - B. 해당 탐지로그를 복구할 것인지 확인(복구한다면 'yes' 입력), 복구하지 않는다면 스크립트 중지
 - C. 사용자에게 한번에 복구할 것인지(one shot), 크론 설정을 통해 복구할 것인지 여부 체크
 - ① 사용자가 한번에(one shot) 복구를 실행하면(yes) 그 즉시 새로 만든 DB에 해당 로그 복구
 - ② 사용자가 한번에 복구 실행하지 않는다면(no) 크론 설정을 하라는 메시지와 함께 스크립트 종료

7. recover_intrusion_log_by_cron.sh

- 1) 크론탭에 설정하여 탐지로그 복구
- 2) 실행 인자로는 한번 실행으로 복구할 탐지로그 개수 설정 가능(ex : recover_intrusion_log_by_cron.sh -n 1000 (한번 실행으로 1000개씩 복구함))
- 3) recover_intrusion_log.sh 스크립트가 실행되지 않았다면 실행되지 않음
- 4) 동작 방식
 - A. Recover_intrusion_log.sh 스크립트가 저장한 시퀀스 정보를 이용하여 복구
 - B. 최신 시퀀스부터 사용자가 설정한 복구 탐지로그 개수 만큼 로그 복구
- 5) 설정 방법
 - A. /sphere/cron_list 편집
 - B. 설정 예시
 - ① *3-5 * * * /usr/penta_np/download/recover_db/recover_intrusion_log_by_cron.sh -n 1000 (매일 3-5시 사이에 매분 마다 1000개씩 복구하도록 설정)
 - ② 매 분마다 동작 시키려면 복구 탐지로그 개수 10000개 이하로 설정

II. 스크립트 설명

8. measure_intrusion_log_count.sh

- 1) 현재 DB에 탐지로그 개수를 조회
- 2) 실행 인자로 조회하고 싶은 개월 수 설정 가능 (ex : `measure_intrusion_log_count.sh -n 6` (6개월 간의 탐지로그 개수 조회))

III. 스크립트 사용 순서

1. H/W or S/W bypass 설정
2. `test_wrap_around.sh` → DB 상태 체크
3. `backup_sphere_db.sh` → 스크립트를 이용하여 현재 설정 백업
4. `change_postgresql_instance.sh` → 스크립트를 이용하여 기존 instance 임시 instance로 변경
5. `create_postgresql_instance.sh` → 스크립트 이용하여 신규 instance 생성
6. **restore factory 실행**
 - 1) `penta# configure terminal`
`penta(config)# wapples`
`penta(config-wapples)# backup`
`penta(config-wapples-backup)# restore factory`
7. `restore_backup_db.sh` → 스크립트 이용하여 설정 백업 restore
8. `recover_intrusion_log.sh` 또는 `recover_intrusion_log_by_cron.sh`
→ 탐지로그 복구 방법 선택하여 탐지로그 복구
 - 1) 크론 설정을 통하여 복구할 경우 `recover_intrusion_log.sh` 스크립트 먼저 실행 후
`recover_intrusion_log_by_cron.sh` 스크립트 실행 해야 함
 - 2) 로그 복구 시(`restore_backup_db.sh` 끝난 후)에는 서비스 재시작 가능
 - A. 단, 트래픽이 많거나 시스템 리소스를 많이 사용하고 있는 경우는 부하가 발생할 수 있음

III. 스크립트 사용 순서

9. 서비스 재시작

- 1) penta# configure terminal
penta(config)# wapples
penta(config-wapples)# system
penta(config-wapples-system)# restart

IV. 스크립트 상세 화면

1. test_wrap_around.sh



warp around 발생 확인

2. backup_sphere_db.sh



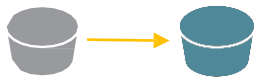
탐지로그, ip_country 제외 백업

2번 스크립트 실행 후
/usr/penta_np/download/backup_sphere_db/~
디렉토리를 메모 -> 정책 백업시 사용(5번 스크립트)

```
penta-np recover_db # ./1.test_wrap_around.sh
OK
penta-np recover_db #
penta-np recover_db #
penta-np recover_db # ./2.backup_sphere_db.sh
2017-03-27_15-10-20/
2017-03-27_15-10-20/version_requirements.sql
2017-03-27_15-10-20/policy_rule_tmp.sql
2017-03-27_15-10-20/ms_global_config.sql
2017-03-27_15-10-20/table_info.sql
2017-03-27_15-10-20/act_result.sql
2017-03-27_15-10-20/log_hmac.sql
2017-03-27_15-10-20/virtual_host.sql
2017-03-27_15-10-20/pls_missing_log.sql
2017-03-27_15-10-20/sync_status.sql
2017-03-27_15-10-20/country_code.sql
2017-03-27_15-10-20/user_defined.sql
2017-03-27_15-10-20/user_defined_select.sql
2017-03-27_15-10-20/alive_check.sql
2017-03-27_15-10-20/network_conf.sql
2017-03-27_15-10-20/system_res_org.sql
2017-03-27_15-10-20/audit.sql
2017-03-27_15-10-20/user_info.sql
2017-03-27_15-10-20/known_attack_policy.sql
2017-03-27_15-10-20/host_name_alias.sql
2017-03-27_15-10-20/virtual_host_rule_exception.sql
2017-03-27_15-10-20/sphere_tmp.sql
2017-03-27_15-10-20/log_error.sql
2017-03-27_15-10-20/system_res.sql
2017-03-27_15-10-20/access_log.sql
2017-03-27_15-10-20/update_info.sql
2017-03-27_15-10-20/web_site_defacement.sql
2017-03-27_15-10-20/read_seq.sql
2017-03-27_15-10-20/uri_list.sql
2017-03-27_15-10-20/sphere.sql
2017-03-27_15-10-20/route_table.sql
2017-03-27_15-10-20/virtual_host_notice_page.sql
2017-03-27_15-10-20/network_stat.sql
2017-03-27_15-10-20/monitor_user.sql
2017-03-27_15-10-20/update_log.sql
2017-03-27_15-10-20/search_bot_from.sql
2017-03-27_15-10-20/report_auto_config.sql
2017-03-27_15-10-20/ha_update_info_table.sql
2017-03-27_15-10-20/sync.sql
2017-03-27_15-10-20/firewall.sql
./2.backup_sphere_db.sh: Sphere Database backup is completed. backup d
irectory is /usr/penta_np/download/backup_sphere_db/2017-03-27_15-10-2
0 except tables. (intrusionlog, ip_country, ipv6_country, web_statist
ics tables)
```

IV. 스크립트 상세 화면

3. change_postgresql_instance.sh



기존DB(5433) 임시DB(5434)
기존DB(5433) 임시DB(5434)로 변경

스크립트 실행 로그 확인

임시 DB(5434 port) 확인

```
penta-np recover_db # ./3.change_postgresql_instance.sh
./stop_service.sh: cron process is down.
./stop_service.sh: sphered process is down.
./stop_service.sh: wapples process is down.
./stop_service.sh: httpd process is down.
* Stopping PostgreSQL ...
* WARNING: postgresql has not yet been started.
* Caching service dependencies ...
* Service 'syslogd' already provides 'logger!';
* Not adding service 'syslog-ng'...
* Cannot add provide 'cron', as a service with the same name exists!
* Services 'cron' and 'local' have circular
* dependency of type 'iafter'; continuing...
* Starting PostgreSQL ...

./3.change_postgresql_instance.sh: /var/lib/postgresql_old/data moved.
./3.change_postgresql_instance.sh: postgresql instance is listening to 5434 port.
./3.change_postgresql_instance.sh: change postgresql instance succeed.

penta-np recover_db #
penta-np recover_db #
penta-np recover_db # netstat -ntnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:5434             0.0.0.0:*               LISTEN      28057/postmaster
tcp        0      0 0.0.0.0:199              0.0.0.0:*               LISTEN      3410/snmpd
tcp        0      0 :::22                   :::*                   LISTEN      3652/sshd
tcp        0      0 :::5434                  :::*                   LISTEN      28057/postmaster
penta-np recover_db #
```

IV. 스크립트 상세 화면

4. create_postgresql_instance.sh



신규DB(5433)

신규DB(5433)생성

임시DB와 신규DB 포트확인

```
Inserting ID(SE-MINI-110)...
INSERT 0 1
DROP INTRUSIONLOG FKEY
ALTER TABLE
CLEAR COUNTRY_CODE TABLE & INSERT COUNTRY_CODE DATA
=====
    register new crontab for root
    setval
-----
    18
(1 row)

./4.create_postgresql_instance.sh: Preserve the log sequence intrusion. Log sequence value is 18
penta-np recover_db #
penta-np recover_db #
penta-np recover_db # netstat -lntp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:5433            0.0.0.0:*               LISTEN      18367/postmaster
tcp        0      0 0.0.0.0:5434            0.0.0.0:*               LISTEN      17532/postmaster
tcp        0      0 0.0.0.0:199            0.0.0.0:*               LISTEN      3410/snmpd
tcp        0      0 :::80                  :::*                    LISTEN      19058/httpd
tcp        0      0 :::22                  :::*                    LISTEN      3652/sshd
tcp        0      0 :::5433                :::*                    LISTEN      18367/postmaster
tcp        0      0 :::5434                :::*                    LISTEN      17532/postmaster
tcp        0      0 :::443                 :::*                    LISTEN      19058/httpd
tcp        0      0 :::5000                :::*                    LISTEN      19058/httpd
tcp        0      0 :::5001                :::*                    LISTEN      19058/httpd
penta-np recover_db #
```

IV. 스크립트 상세 화면

4-1. restore factory 실행

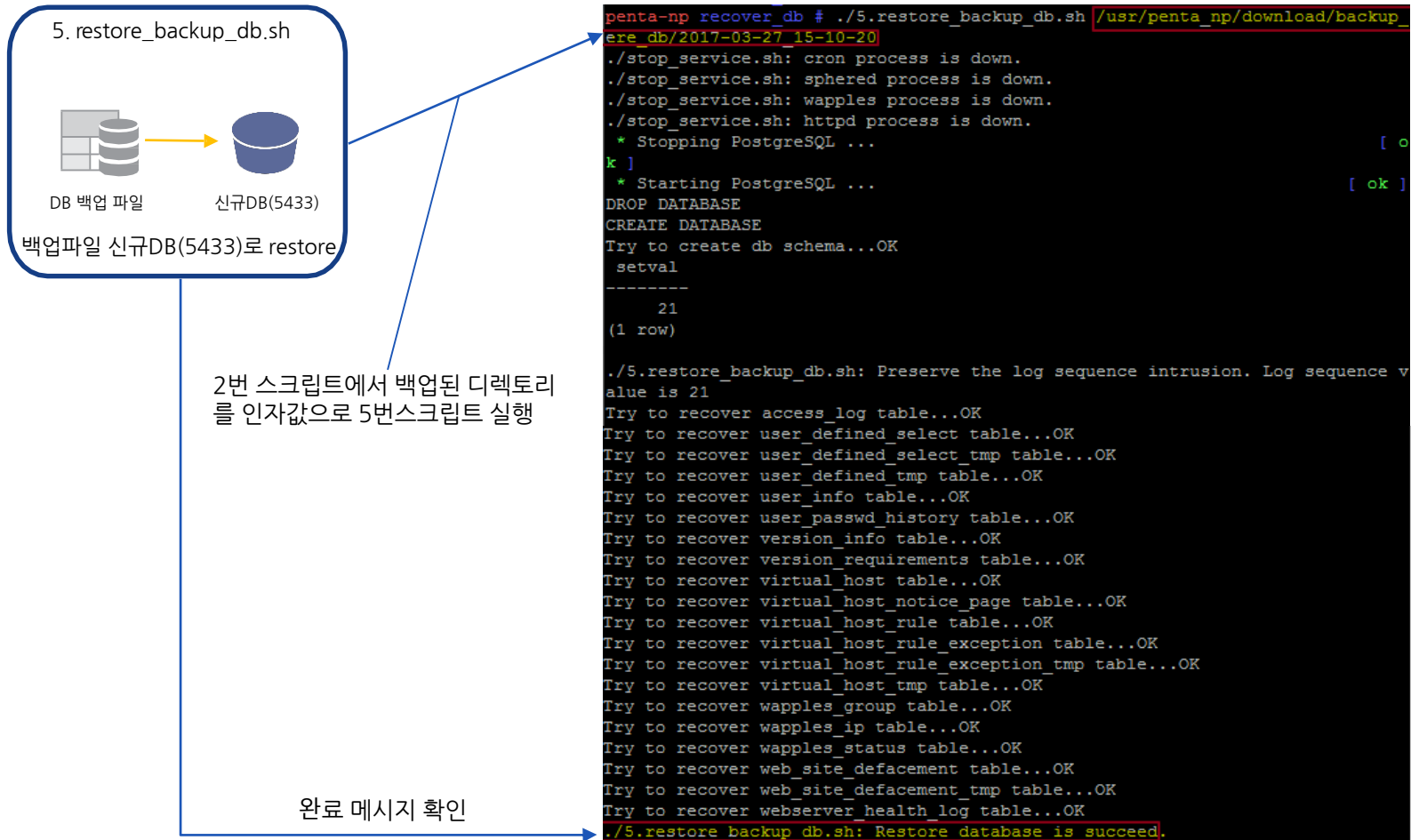
penta# configure terminal
penta(config)# wapples
penta(config-wapples)# backup
penta(config-wapples-backup)#
restore factory

4.0.36.15 이전 버전 : restore factory

4.0.36.15 이후 버전 : restore factory db 실행

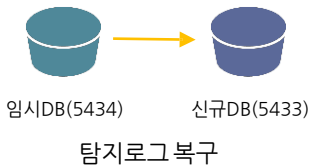
```
penta-np recover_db # exit
exit
penta-np# configure terminal
penta-np(config)#
penta-np(config)# wapples
penta-np(config-wapples)#
penta-np(config-wapples)# backup
penta-np(config-wapples-backup)#
penta-np(config-wapples-backup)# restore factory
% Command incomplete.
penta-np(config-wapples-backup)#
penta-np(config-wapples-backup)# restore factory db
Warning! reset all of configuration... GO on ?[y/n] :y
Start DB Clear & Initialize...
Restore Factory...[OK]
penta-np(config-wapples-backup)#
```

IV. 스크립트 상세 화면



IV. 스크립트 상세 화면

6.Recover_intrusion_log.sh or
recover_intrusion_log_by_cron.
sh



모든 탐지로그 즉시 복원

```
penta-np recover_db # ./6-0.rerecover_intrusion_log.sh
./6-0.rerecover_intrusion_log.sh: Number logs = 16
Do you want repair intrusion log in this period? y
./6-0.rerecover_intrusion_log.sh: The recovered data is from 2 to 17.
Do you want repair intrusion log at one shot? y
ALTER TABLE
./6-0.rerecover_intrusion_log.sh: The log recover succeed.
```

```
PGPORT=5433
* * * * * /iupdater/ver2.0/bin/heartbeat_client.sh >& /dev/null
0 1 * * * /sphere/scripts/tracelog.sh >& /dev/null
0 * * * * /.packages/version_info/version_sync.sh /.packages/version_info/current_version
>& /dev/null
* * * * * sh /sphere/scripts/check_sshd.sh >& /dev/null
* * * * * sh /sphere/scripts/memory_recover.sh >& /dev/null
* * * * * sh /sphere/scripts/execReboot.sh > /dev/null
* * * * * /sphere/scripts/ctrl_coredump_directory.sh > /dev/null
*/10 * * * * /sphere/scripts/mailexender.py >& /dev/null
*/5 * * * * /sphere/scripts/daemonmonitor.sh >& /dev/null
10 */6 * * * sh /sphere/scripts/removeTmpFiles.sh > /dev/null
0,15,30,45 5 * * * sh /sphere/scripts/send_report.sh > /dev/null
0 4 * * * psql sphere sphere -c "analyze intrusionlog"
* * * * * /sphere/bin/agentManager /sphere/conf/agent.conf /var/log/ >& /dev/null
* * * * * sh /sphere/scripts/user_index_buffer_trouble_shooting.sh >& /dev/null
* 3-5 * * * /usr/penta np/download/recover_db/recover_intrusion_log_by_cron.sh -n 1000
```

recover_intrusion_log_by_cron.sh

스크립트 사용시에는

‘Do you want repair intrusion log at one shot?’

물음에 no로 대답하며, cron설정 별도 진행

vi /sphere/cron_list에서 추가

IV. 스크립트 상세 화면

7. 서비스 재시작

```
penta# configure terminal
penta(config)# wapples
penta(config-wapples)# system
penta(config-wapples-system)# restart
```

```
penta-np# configure terminal
penta-np(config)# wapples
penta-np(config-wapples)# system
penta-np(config-wapples-system)# restart
Restart! WAPPLES, Wait...
=====
      clear crontab for root
cron: no process killed
* Stopping PostgreSQL ... [ ok ]
* Stopping z99sphered ... [ ok ]
* Manually resetting z99sphered to stopped state.
* Manually resetting postgresql to stopped state.
* Starting PostgreSQL ... [ ok ]
* Starting sphered ...
cat: /var/run/.wpn: No such file or directory [ ok ]
=====
      register new crontab for root
```

V. 스크립트 적용 사례

- Test_wrap_around.sh 스크립트 실행 시 “OK” 메시지가 나온 DB

- DB Size : 약 100G

- 6개월 분량의 로그 복구 (약 16G)

- 소요 시간: 총 약 1시간30분

- ① H/W or S/W bypass 설정
- ② backup_sphere_db.sh
- ③ change_postgresql_instance.sh
- ④ create_postgresql_instance.sh
- ⑤ restore_backup_db.sh

1,2,3,4,5 번과정 약30분

- ⑥ recover_intrusion_log.sh -n 6 (one shot 으로 한번에 복구)

6 번과정 약1시간

VI. 주의 및 참고사항

- 스크립트간 강제 종료문제

- 탐지로그 count단계에서 로그량이 많을 경우 다소 1~5분 정도 걸릴 수 있으나, 해당 작업 간 강제로 Transaction을 종료하더라도 해당 Query는 계속 실행되므로 문제가 될 수 있음
- 해당 형태의 경우 아래와 같이 DB를 재 시작 하여 다시 하는 것을 권고
/etc/init.d/postgresql restart
/etc/init.d/postgresql_old restart

- Test_wrap_around.sh 시 다른 DB가 wrap around 발생시

- DB자체가 wrap around 발생 시, 실제 복구에는 어려울 수 있으나 아래와 같이 다른 DB에서 발생하였을 경우에는 정상적으로 처리가 가능할 수도 있음에 따라, 다음 STEP으로 진행하여 정상 처리 유무 확인 필요

```
neozizz recover_db # ./test_wrap_around.sh
template0 is wrap arounded. template0 transaction id is -2028494126
error!!!! sphere database occurred transaction wrap around.
```

- 스크립트 사용시 기존 DB로 복원 해야 할 경우

- 경로를 변경한 postgresql_old(기존DB) -> postgresql 경로로 복원 방법
- /var/lib 밑에 postgresql 이름으로 된 폴더가 없어야 됨
- change_postgresql_db.sh -R
(rollback 인자를 주어 postgresql_old DB를 -> postgresql DB로 바꿈)

```
penta-pk@ recover_db # ./3.change_postgresql_instance.sh -R
./stop_service.sh: cron process is down.
./stop_service.sh: sphered process is down.
./stop_service.sh: wapples process is down.
./stop_service.sh: httpd process is down.
* Stopping PostgreSQL ...
No process in pidfile '/var/lib/postgresql/data/postmaster.pid' found running; n
* Stopping PostgreSQL ...
/sbin/start-stop-daemon: warning: failed to kill 7722: No such process
No process in pidfile '/var/lib/postgresql_old/data/postmaster.pid' found running
* Manually resetting postgresql_old to stopped state.
* Caching service dependencies ...
* Service 'sysklogd' already provides 'logger!';
* Not adding service 'syslog-ng'...
* Cannot add provide 'cron', as a service with the same name exists!
* Services 'cron' and 'local' have circular
* dependency of type 'iafter'; continuing...
* Starting PostgreSQL ...

./3.change_postgresql_instance.sh: /var/lib/postgresql/data moved.
./3.change_postgresql_instance.sh: postgresql instance is listening to 5433 port
./3.change_postgresql_instance.sh: change postgresql instance succeed.
penta-pk@ recover_db #
```

VI. 주의 및 참고사항

- 3.change_postgresql_instance.sh 에러발생 시(1)

```
penta-np recover_db # ./3.change_postgresql_instance.sh
./stop_service.sh: cron process is down.
./stop_service.sh: sphered process is down.
./stop_service.sh: wapples process is down.
./stop_service.sh: httpd process is down.
* Stopping PostgreSQL ... [ ok ]
* WARNING: postgresql has not yet been started.
./3.change_postgresql_instance.sh[14627]: already postgresql_old directory exist.
./3.change_postgresql_instance.sh[14628]: remove directory is manually.
penta-np recover_db #
penta-np recover_db # netstat -lntp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program
name
tcp        0      0 0.0.0.0:199             0.0.0.0:*                LISTEN      3410/enmpd
tcp        0      0 :::22                  :::*                    LISTEN      3652/sshd
```

- 이미 /var/lib/postgresql_old 디렉토리가 존재하여 에러가 발생
→ 이전 해당 장비 db인스턴스 작업을 실행하여 디렉토리가 존재하는데, 삭제 혹은 파일 이름을 변경하여야 함
- /var/lib/postgresql_old 디렉토리에 대한 조치를 취한 후 db 재시작 후 스크립트 재실행
/etc/init.d/postgresql restart

VI. 주의 및 참고사항

- 3.change_postgresql_instance.sh 에러발생 시(2)

```
penta-np recover_db # ./3.change_postgresql_instance.sh
./stop_service.sh: cron process is down.
./stop_service.sh: sphered process is down.
./stop_service.sh: wapples process is down.
./stop_service.sh: httpd process is down.
* WARNING: postgresql has not yet been started.
* Caching service dependencies ...
* Service 'syslogd' already provides 'logger!';
* Not adding service 'syslog-ng'...
* Cannot add provide 'cron', as a service with the same name exists!
* Services 'cron' and 'local' have circular
* dependency of type 'iafter'; continuing... [ ok ]
* WARNING: postgresql old has already been started.
./3.change_postgresql_instance.sh[16563]: error!!!! change postgresql instance.
```

- 5433 port가 죽어있을 때 해당 스크립트를 실행할 때 에러가 발생

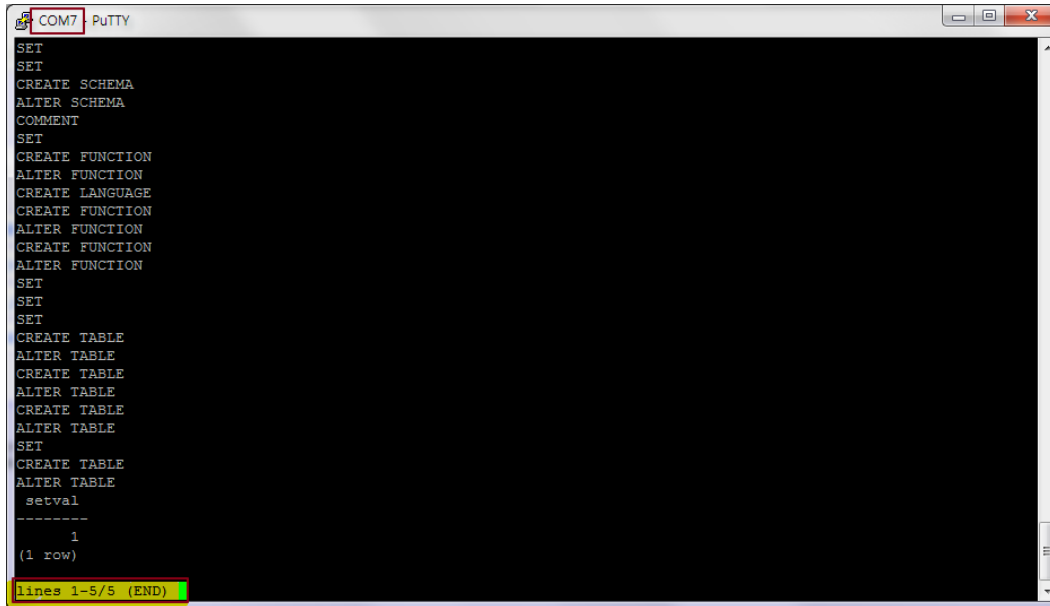
```
penta-np recover_db # ./3.change_postgresql_instance.sh -R
./stop_service.sh: cron process is down.
./stop_service.sh: sphered process is down.
./stop_service.sh: wapples process is down.
./stop_service.sh: httpd process is down.
* Stopping PostgreSQL ...
No process in pidfile '/var/lib/postgresql_old/data/postmaster.pid' found running; none killed. [ ok ]
* Caching service dependencies ...
* Service 'syslogd' already provides 'logger!';
* Not adding service 'syslog-ng'...
* Cannot add provide 'cron', as a service with the same name exists!
* Services 'cron' and 'local' have circular
* dependency of type 'iafter'; continuing... [ ok ]
* Starting PostgreSQL ... [ ok ]

./3.change_postgresql_instance.sh: /var/lib/postgresql/data moved.
./3.change_postgresql_instance.sh: postgresql instance is listening to 5433 port.
./3.change_postgresql_instance.sh: change postgresql instance succeed.
penta-np recover_db # /etc/init.d/postgresql restart
* Stopping PostgreSQL ... [ ok ]
* Starting PostgreSQL ... [ ok ]
```

- 3번스크립트의 -R 옵션을 주고 롤백 후 스크립트 재실행

VI. 주의 및 참고사항

- 4.create_postgresql_instance.sh 멈춤 현상



```
COM7 PuTTY
SET
SET
CREATE SCHEMA
ALTER SCHEMA
COMMENT
SET
CREATE FUNCTION
ALTER FUNCTION
CREATE LANGUAGE
CREATE FUNCTION
ALTER FUNCTION
CREATE FUNCTION
ALTER FUNCTION
SET
SET
SET
CREATE TABLE
ALTER TABLE
CREATE TABLE
ALTER TABLE
CREATE TABLE
ALTER TABLE
SET
CREATE TABLE
ALTER TABLE
setval
-----
      1
(1 row)
```

lines 1-5/5 (END)

- SSH 접속이 아닌 Serial(console) cable을 이용하여 작업시 위 화면처럼 멈춤 현상 발생
 - q버튼을 누르면 다음화면으로 넘어가니 참고
- 만약 ctrl+c로 해당 화면에서 벗어나면 db가 정상적으로 생성되지 않으니 주의

VI. 주의 및 참고사항

- 6-0.recover_intrusion_log.sh 에러 발생시

```
penta-np recover_db # ./6-0.rerecover_intrusion_log.sh
psql: could not connect to server: Connection refused
        Is the server running locally and accepting
        connections on Unix domain socket "/tmp/.s.PGSQL.5434"?
./6-0.rerecover_intrusion_log.sh: line 31: [: -eq: unary operator expected
psql: could not connect to server: Connection refused
        Is the server running locally and accepting
        connections on Unix domain socket "/tmp/.s.PGSQL.5434"?
./6-0.rerecover_intrusion_log.sh: Number logs =
./6-0.rerecover_intrusion_log.sh: line 40: [: -eq: unary operator expected
Do you want repair intrusion log in this period? ^C
```

- 임시DB(5434 port)가 열려있지 않아 에러가 발생
- 해당 형태의 경우 아래와 같이 임시 DB를 재 시작 하여 다시 하는 것을 권고
/etc/init.d/postgresql_old restart

```
penta-np recover_db # /etc/init.d/postgresql_old restart
* Stopping PostgreSQL ...
/sbin/start-stop-daemon: warning: failed to kill 28057: No such process
No process in pidfile '/var/lib/postgresql_old/data/postmaster.pid' found running; none killed.
* Starting PostgreSQL ...
penta-np recover_db #
penta-np recover_db # ./6-0.rerecover_intrusion_log.sh
./6-0.rerecover_intrusion_log.sh: Number logs = 16
Do you want repair intrusion log in this period? █
```

VI. 주의 및 참고사항

- SSD사용 장비 확인사항

- /var/lib/ 디렉토리에 ls -al 명령어로 심볼릭 링크가 걸려있는지 확인

```
penta-np lib # ls -al
total 92
drwxr-xr-x 21 root    root    4096 2017-03-28 14:29 .
drwxr-xr-x 13 root    root    4096 2016-11-18 15:02 ..
drwxr-xr-x  2 root    root    4096 2009-06-23 20:53 arpd
drwxr-xr-x  2 apache  apache 4096 2009-06-23 23:07 dav
drwxr-xr-x  2 root    root    4096 2016-06-15 22:15 dbus
drwxr-xr-x  2 root    root    4096 2017-03-28 13:23 dhclient
drwxr-xr-x  3 root    root    4096 2009-06-24 20:22 eselect
drwxr-xr-x  3 root    root    4096 2009-06-25 02:25 gentoo
drwxr-xr-x 16 root    root    4096 2017-03-28 14:29 init.d
drwxr-xr-x  2 root    root    4096 2009-06-23 19:02 ip6tables
drwxr-xr-x  2 root    root    4096 2009-06-23 19:02 iptables
drwxr-xr-x  2 root    root    4096 2009-06-23 18:48 krb5kdc
-rw-r--r--  1 root    root    1955 2017-03-28 14:00 logrotate.status
drwxr-xr-x  2 root    root    4096 2009-06-23 18:51 misc
drwxr-xr-x  2 root    root    4096 2017-03-28 13:26 net-snmp
drwxr-xr-x  2 ntp     ntp    4096 2017-03-28 13:24 ntp
drwx-----  2 ldap   ldap    4096 2009-06-23 18:49 openldap-data
drwxr-xr-x  3 root    root    4096 2011-12-07 15:04 php-pkg
drwxr-s---  2 root    portage 4096 2017-03-28 13:24 portage
lrwxrwxrwx  1 root    root    17 2017-03-28 14:29 postgresql -> /data/postgresql/
drwxr-xr-x  3 postgres postgres 4096 2010-06-03 18:23 postgresql_org
drwxr-xr-x  2 root    root    4096 2017-03-28 13:24 rpm
-rw-r--r--  1 root    root    41 2017-03-28 13:24 syslog-ng.persist
drwxr-xr-x  2 root    root    4096 2009-06-24 21:16 xkb
```

- SSD 사용 장비의 경우 postgresql 실제 디렉토리가 /data/postgresql/에 존재하고 /var/lib/postgresql/에 심볼릭링크(바로가기)가 걸려있음
→ 만약 위와 같이 설정되어있지 않으면 SSD 용량이 full 될 가능성 존재
- /var/lib/postgresql/ 디렉토리를 /data/ 디렉토리에 옮기고 심볼릭링크 설정
→ 심볼릭링크 설정법 : ln -s /data/postgresql/ /var/lib/

t h a n k y o u



KOREA	Yeouido, Seoul	www.pentasecurity.com (HQ)
U.S.A.	Houston, Texas	www.pentasecurity.com/en
JAPAN	Shinjuku-Ku, Tokyo	www.pentasecurity.co.jp