Changes to be aware of when moving from BIND 9.18 to 9.20 (VitalQIP DNS 6.5)

변경사항

인라인 서명

1. Inline Signing 기능 변경
   - inline-signing 을 이제 dnssec-policy 내부에서도 설정할 수 있으며, **기본값은 yes 임.**
   - dnssec-policy 를 사용하는 모든 존은 별도 설정이 없으면 inline-signing yes 가 기본값임. 인라인 방식을 원치 않는 존들은 예외처리 해야함.

   - zone 레벨에서 설정하면 dnssec-policy 의 설정을 덮어씀.

2. 기존 DNSSEC 존 사용 시 주의사항

기존 DNSSEC 서명된 zone 을 운영 중인 경우, zone 및 DNSSEC 서명 유지 관련 설정을 검토해야 함. 기본값을 유지하면 기존 존이 예상치 않게 inline-signed 로 변환될 수 있음.

- dnssec-policy 에 inline-signing no 라고 되어있어도
- 특정 zone 설정에 inline-signing yes 라고 되어있으면 그 특정(zone)은 yes 로 동작함.

→개별 설정이 공통 규칙을 덮음. dnssec-policy(전체규칙) < zone 설정(개별규칙)

3. BIND 9.20 의 새로운 동작

dnssec-policy 를 사용하는 모든 DNSSEC 서명된 존은 명시적으로 비활성화(no) 하지 않는 한 자동으로 inline-signed 가 됨. → 이로 인해 존 파일 옆에 저널 파일이 생성됨.

BIND 9.20 이전 동작

BIND 9.20 이전에는 dnssec-policy 사용 시, 동적 업데이트로 존을 유지하거나 inline-signing 기능을 활성화해야 했음. 둘 다 설정하지 않으면 named 가 잘못된 설정으로 보고됨.

4. **업그레이드 후 조치사항**

위 시나리오를 피하려면 적절한 곳에 inline-signing no 를 명시적으로 설정해야함. dnssec-policy 를 사용하지 않는 운영자는 이 변경사항의 영향을 받지 않음.

성능

1. BIND 는 이제 RBTDB 에서 **QPDB** 라는 새로운 인메모리 데이터베이스를 사용
    - 기존 RBTDB 는 여전히 사용할 수 있지만 기본값 x
    - QPzone/QPtire 라고도 함.

자원사용

- 메모리, RAM, CPU 를 조금 더 쓸 수 있지만, 사용자가 몰릴 때 (고부하 시) 버티는 힘이 훨씬 좋아짐.
- 성능이 특히 중요한 환경이라면 모니터링과 테스트 및 단계적 배포를 권장.

런타임 구성

1. allow-transfer
    - 기본값이 none 으로 설정됨.
2. dnssec-validation
    - yes 로 설정할 경우, 이제 명시적인 trust-anchors 설정 필요.
    - 대부분의 리졸버 환경에서는 기본값인 auto 사용을 권장.
3. **로그 분리**
    - 이제 notify 와 xfer-in 을 위한 별도의 로깅 카테고리가 사용됨.

4. **옵션 명칭 변경**

    - parental-agents 와 primaries 옵션은 이제 remote-servers 라는 새로운 명칭으로 선호됨. 기존 명칭들은 별칭(Alias)으로 계속 지원.

기타

1. named-compilezone
    - 무결성 검사(Integrity checks)가 기본적으로 생략됨.

지원 종료 예정 (Deprecated)

지원 종료 예정 or 경고	상세 내용	대체 방안
NSEC3 Iterations	0 이외의 반복 횟수 지원 중단	0 으로 설정
max-zone-ttl	options 또는 zone 블록 내 설정 지원 중단	dnssec-policy 설정 사용
sortlist		
rrset-order "fixed"	값이 fixed 인 경우	
DLZ	외부 데이터베이스에서 영역 데이터를 직접 가져올 수 있도록 하는 기능	

삭제

> 아래는 named.conf 에 사용되거나 포함된 것 중 제거된 항목. 사용시 에러/named 가 시작되지 않음.

- auto-dnssec
- dnskey-sig-validity
- dnssec-dnskey-kskonly
- dnssec-update-mode
- sig-validity-interval
- update-check-ksk

- dnssec-secure-to-insecure
- glue-cache
- alt-transfer-source
- alt-transfer-source-v6
- use-alt-transfer-source
- resolver-nonbackoff-tries
- resolver-retry-interval
- stale-answer-client-timeout == 0
- keep-response-order
- cookie-algorithm aes
- delegation-only
- root-delegation-only
- coresize
- datasize
- files
- stacksize
- lock-file
- dscp
- ip_dscp

> 빌드 및 라이브러리 (Build and libraries)에서 삭제
>
> - **configure** 의 **-with-tuning** 옵션
> - **libbind9** 라이브러리 (**libisc** + **libisccfg** 로 대체됨)

- libirs 라이브러리 (유일하게 남아있던 익스포트인 irs_resconf 는 libdns 로 이동됨)

> 기타 삭제

- named 의 U 명령줄 스위치 (UDP 작업자 수 설정).
- DSCP(Differentiated Services Code Point)와 관련된 모든 설정.
- TKEY 모드 2(Diffie-Hellman Exchanged Keying Mode) 지원.
- Microsoft Windows 2000 GSS-TSIG 지원 (명령어 nsupdate 의 o 옵션 및 oldgsstsig 설정 포함).

---

*DNSSEC Key and Signing Policy 에 관해

9.19.16 버전 이후 auto-dnssec → dnssec-policy 로 대체됨