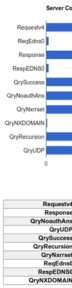
Автор:
12.05.14 20:33 -

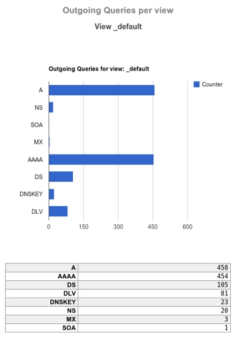
После двух лет разработки консорциум ISC представил первый стабильный релиз новой ветки DNS-сервера BIND 9.10. При подготовке новой ветки основное внимание было уделено увеличению производительности работы рекурсивного и авторитативного сервера, а также развитию средств для диагностики проблем и вывода статистики о работе сервера.

Ключевые новшества BIND 9.10.0:

- Возможность сохранения предкомпилированного представления файлов с DNS зонами, что позволяет существенно сократить время загрузки зон при запуске сервера, благодаря исключения стадии парсинга зоны. Новая возможность окажется особенно полезной на slave-серверах, для использования предкомпилированного формата для кэшируемых зон следует добавить опцию "masterfile-format map";
- В резолвер добавлена и включена по умолчанию функция упреждающего обновления кэша (режим pre-fetch). Если ранее, содержимое прокэшированной записи не обновлялось до истечения её времени жизни, то теперь, если не истёк заданный через директиву prefetch таймаут, запрос прокэшированного элемента приводит к отложенному обновлению данных в кэше, т.е. актуальность элемента в кэше продляется на время TTL относительно последнего запроса. Например, TTL некоторых популярных доменов установлен всего в несколько десятков секунд, что приводило к постоянному выпаданию элементов из кэша, при использовании pre-fetch время жизни записи постоянно сдвигается;
- Представления (views) теперь могут совместно использовать данные зон, что позволяет избежать дублирвоания информации зоны в нескольких представлениях. Управление производится через опцию "in-view";
- Существенно увеличена производительность и масштабируемость механизма Response Policy Zones (RPZ), позволяющего на лету вычислять "репутацию" для DNS-имен через создание специальной децентрализованной DNS-зоны (аналог DNSBL для борьбы с хостами спамеров и мошенников);
- При обработке EDNS (механизм работы с пакетами, размером более 512 байт) улучшено отслеживание возможностей удалённого сервера при выполнении рекурсивных запросов. Вместо изначальной отправки больших пакетов с последующим уменьшением размера при возникновении ошибок, BIND теперь применяет более эффективный противоположный метод, начинает с мелких пакетов и постепенно увеличивает их размер до возникновения ошибок;
- Добавлен набор преднастроенных опций для тюнинга производительности крупных серверов, подходящий для систем с большим объёмом памяти. Параметры меняются при сборке с использованием флага "configure --with-tuning=large";

- Обеспечена возможность отдачи статистики в форматах XML и JSON. Отдача в JSON осуществляется значительно быстрее, чем XML, но пока не поддерживается на платформе Windows. Поддержка формата XML теперь включена по умолчанию и не требует сборки со специальной опцией.
- Добавлены новые виды статистики, доступные для систем мониторинга. Например, добавлен вывод статистики работы резолвера, кэша, базы адресов, менеджера задач и отправки. Обеспечено отслеживание счётчиков TCP и UDP запросов для отдельных зон. Обеспечено кэширование XSL-стилей для наглядной интерпретации XML-статистики;





A	458
AAAA	454
DS	105
DLV	81
DNSKEY	23
NS	20
MX	3
SOA	1

- Поддержка GeoIP для привязки правил доступа к местоположению (например, можно открыть доступ только для IP из определённой страны);
- BIND теперь по умолчанию принимает запросы по IPv6, без необходимости указания опции listen-on-v6;
- По умолчанию включена сборка с поддержкой многопоточности, в том числе и на платформе Linux;
- Добавлена поддержка расширения Source Identity Token (SIT) для защиты от спуфинга;
- На смену связке dig и sigchase пришла новая утилита диагностики delv (Domain Entity Lookup and Validation). По своим возможностям и методам использования delv во многом напоминает dig, но отличается полноценной встроенной поддержкой DNSSEC и полностью новой кодовой базой;
- В dig добавлена поддержка опций EDNS client-subnet (dig +subnet) и EDNS Expire (dig +expire);
- В утилиту named-checkconf добавлена поддержка опции "-px" для вывода содержимого файлов конфигурации со скрытием конфиденциальных данных, что позволяет не заботиться о вырезании приватной информации при прикреплении файла конфигурации к отчёту об проблемах;
- В утилитах named-checkzone и named-compilezone обеспечена возможность чтения файлов с журналом для вывода текущего состояния динамической зоны без предварительной синхронизации зоны с журналом;

- Добавлена утилита named-rrchecker для проверки синтаксической корректности отдельных ресурсных записей или для преобразования нового формата записей RR в канонический, поддерживаемый старыми версиями BIND;
- Добавлена команда "rndc zonestatus" для вывода детальной информации о состоянии определённой зоны, включая данные о конфигурации, времени последней загрузки, серийном номере и времени запланированных событий.
- Поддержка технологии RRL (Response Rate Limiting), позволяющей ограничить интенсивность отправки ответов DNS-сервером, что даёт администраторам средства для эффективной защиты от вовлечения их сервера в проведение DDoS-атак, в которых DNS сервер используется в роли усилителя трафика. RRL даёт возможность установить лимит на интенсивность отправки ответов в привязке к адресу получателя. Заданные через RRL ограничения действуют только на исходящие запросы и не влияют на входящие. Управление RRL производится через директиву responses-per-second, указываемую в блоке rate-limit и позволяющую задать допустимое число ответов в секунду. Поддержка RRL также была бэкпортирована в ветку 9.9 и вошла в состав выпуска 9.9.4.

Почти сразу выпущено первое корректирующее обновление 9.10.0-p1 , в котором по горячим следам устранена
уязвимость
, позволяющая вызвать крах обслуживающего рекурсивные запросы серверного процесса через отправку специально оформленного запроса.

Read more http://www.opennet.ru/opennews/art.shtml?num=39740