



Как мы тестируем MSK-IX DNS-Cloud

Дмитрий
Коваленко

Санкт-Петербург 2017 ENOG-13





MSK-IX DNS Cloud

MSK-IX управляет территориально распределенными облаками DNS-серверов для поддержки доменных зон верхнего уровня, что повышает требования к отказоустойчивости.

<https://www.msk-ix.ru/dns/>



Технология Anycast для оптимальной доступности DNS-сервиса из любой точки сети интернет;



Непрерывный мониторинг;



Регулярные аудиты сервиса и защита от DDoS-атак.



Технология Anycast

Как выглядит DNS Anycast облако?

Каждое облако состоит нескольких узлов

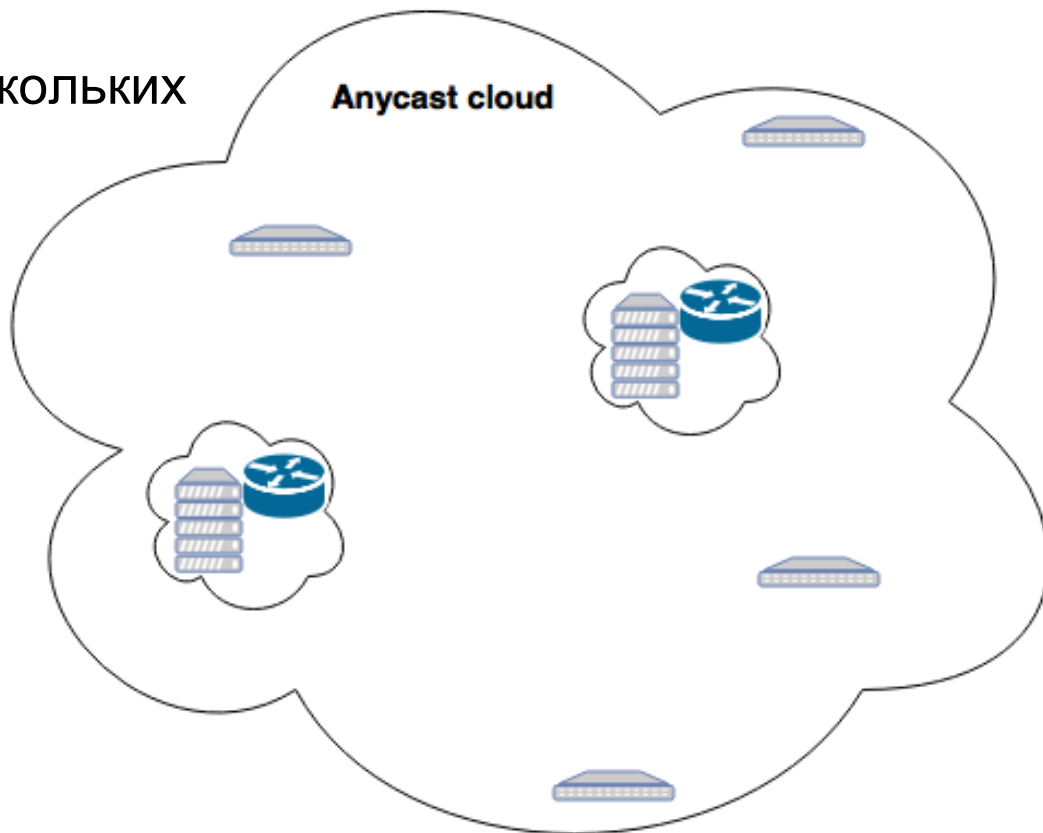
Основной сервис – DNS

Вспомогательные сервисы:

- мониторинг;
- статистика;
- аналитика.

Мы используем 10 Anycast облаков

- ✓ IPv4;
- ✓ IPv6;
- ✓ DNSSEC;
- ✓ Более одной AS.

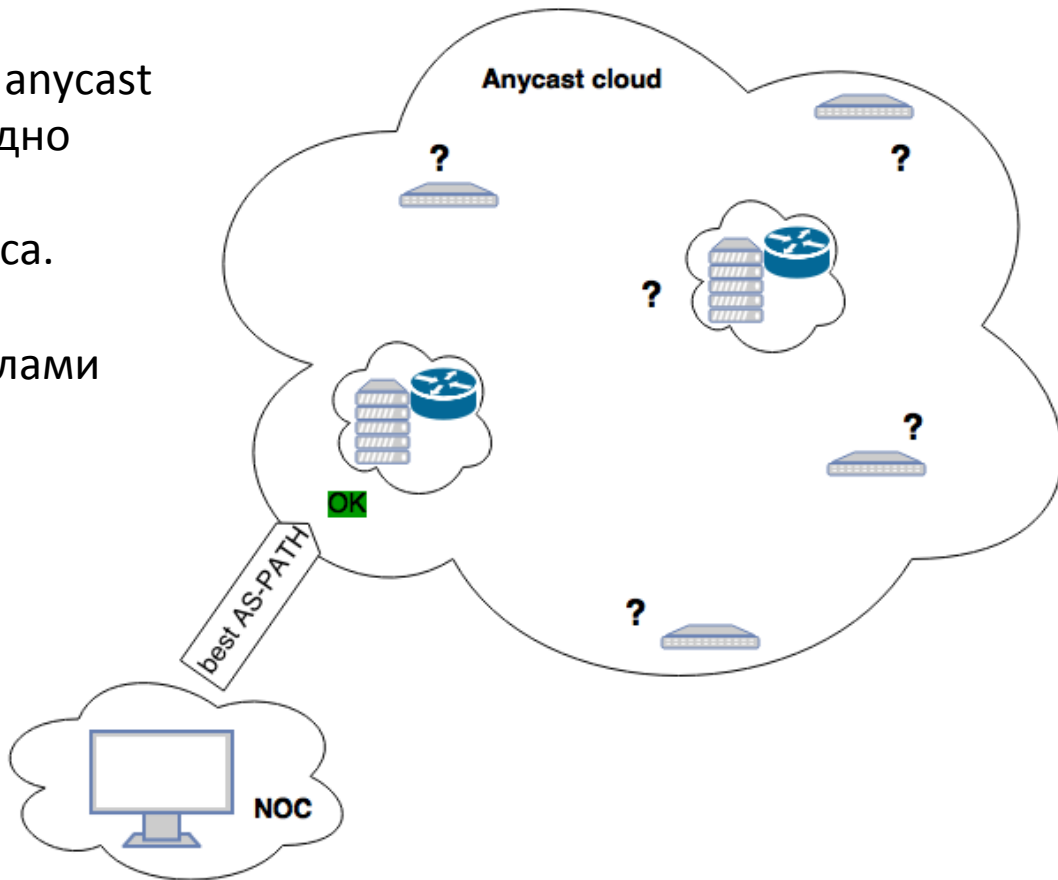


Мониторинг

Как мониторить anycast облако?

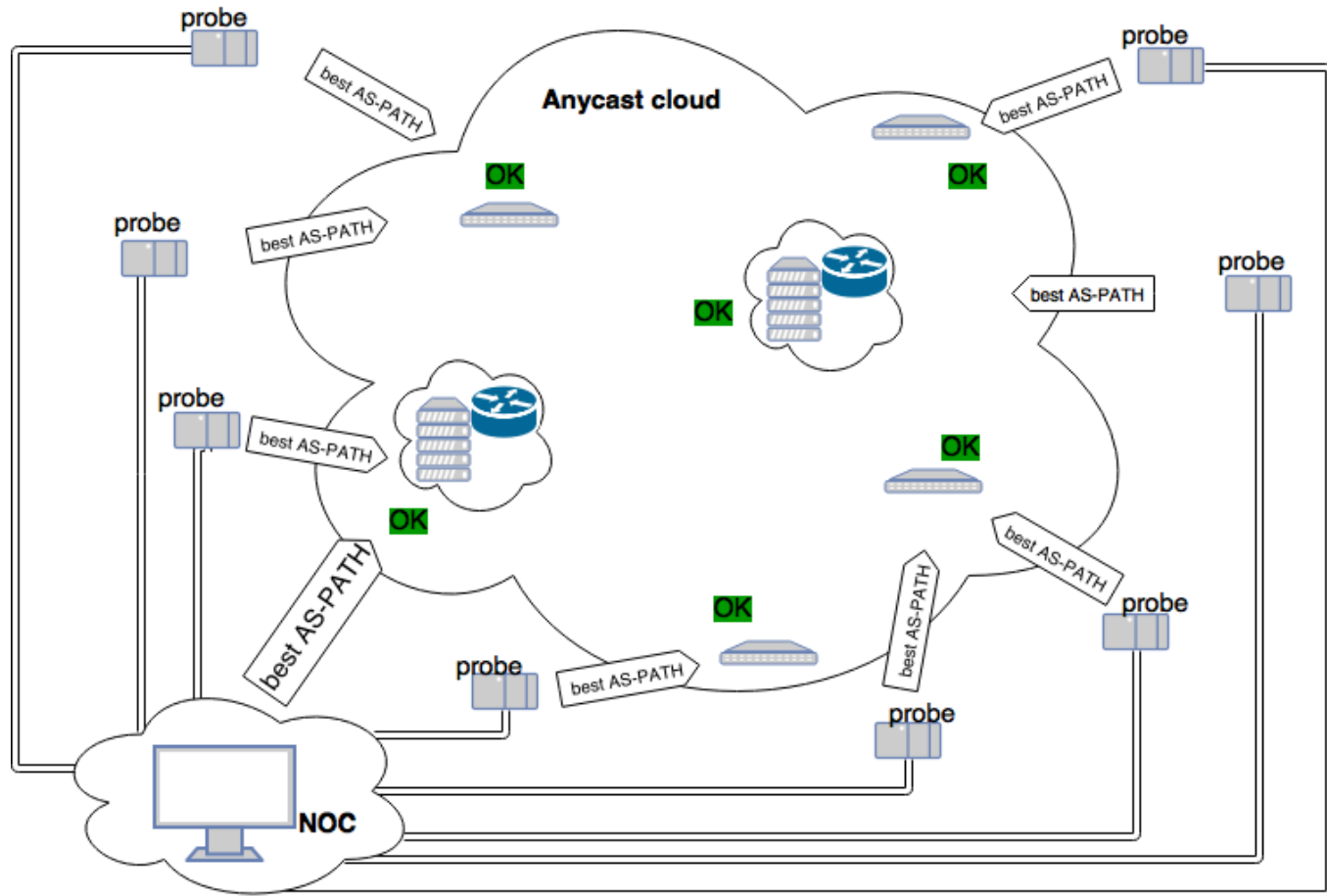
При контроле сервисного anycast адреса из одной точки видно только один узел, как при мониторинге unicast адреса.

Как быть с остальными узлами anycast облака?



Как мониторить anycast облако?

Использовать
распределенный
мониторинг, состоящий
из множества
пробников.





Чем мониторить Anycast облака?

Главный вопрос : Какое приложение будем мониторить?

Well Known: Ping, Traceroute, DNS, HTTP

- RIPE Atlas;
- NLNOG RING.

Что-то особенное или нужен полный контроль над инфраструктурой?

- Собственная сеть пробников.

Мы используем гибридный вариант: собственная сеть пробников + RIPE Atlas

- ✓ Наши пробники работают с внешними IPv4 и IPv6 адресами;
- ✓ Все данные от измерений попадают в центральную систему мониторинга.



Как мы мониторим наши серверы и облака

Каждый DNS-сервер имеет внутренние средства контроля

- целостности размещенных доменных зон;
- доступности серверов дистрибуции.

Каждый DNS-узел контролируется системой мониторинга

- параметры серверов;
- параметры сетевого оборудования;
- параметры внешних и внутренних сетевых каналов.

Каждое DNS-облако контролируется системой распределенного мониторинга

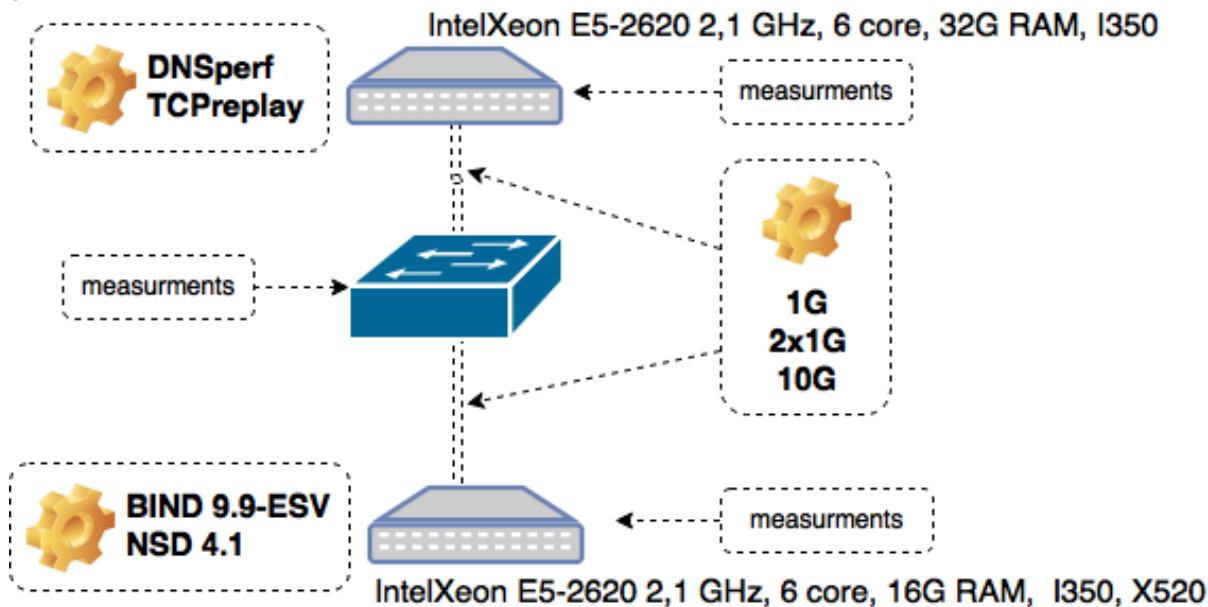
- доступность сервиса;
- сетевая задержка.

Стресс-тесты ПО и сетевой инфраструктуры

Как мы тестируем производительность софта

Периодически мы тестируем DNS-решения различных производителей (BIND, NSD, Knot и т.д.)

Целью данного исследования было выяснение с помощью серий стресс-тестов максимальной производительности каждого из пакетов BIND и NSD, развернутых на серверной платформе заданной конфигурации





Чем мы тестировали BIND и NSD и чего добились

Нагрузочный тест

DNS-сервер: Аналог зоны RU, содержащий несколько миллионов записей типа A, AAAA, NS, RRSIG, NSEC3

Генератор: TCPReplay + PCAP-файл с реальными запросами

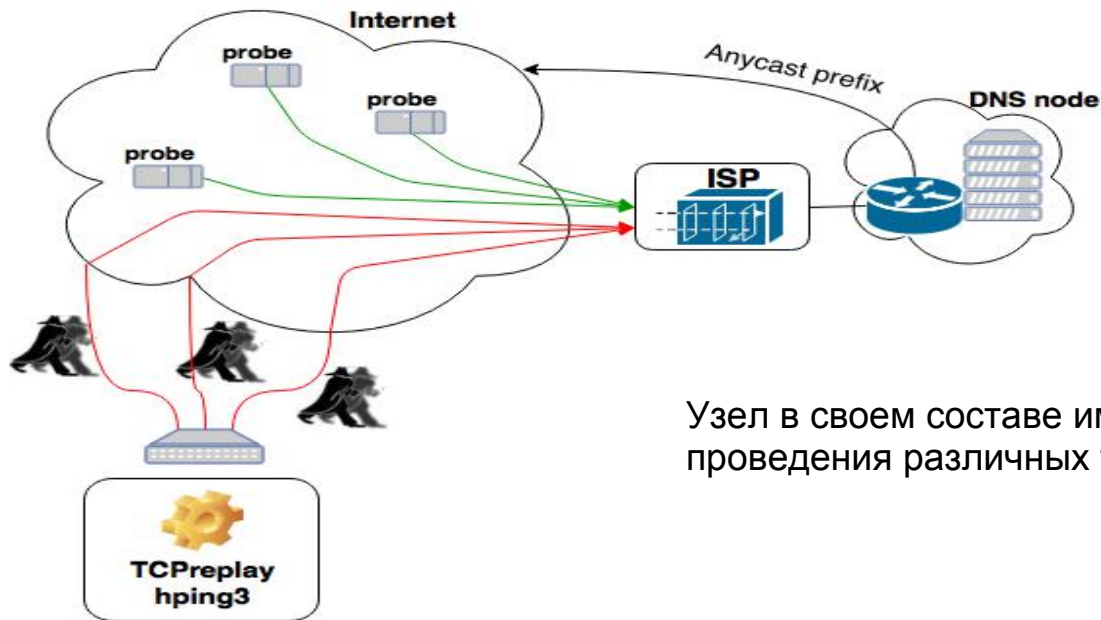
Результаты

| BIND99-ESV | | NSD-4.1 | |
|-------------|-----|-------------|------|
| Kpps in/out | | Kpps in/out | |
| 120 | 120 | 530 | 530 |
| Mbps in/out | | Mbps in/out | |
| 90 | 520 | 400 | 2300 |

Стресс-тесты сетевой инфраструктуры

Цели:

- отработать взаимодействие с оператором связи
- подготовить шаблон защиты для подавления DDoS-атаки



Узел в своем составе имеет тестовый сервер, для проведения различных тестов



Тестируем без клиентского трафика

Нагрузочный тест:

1. Отправляем «плохой» поток, не превышающей заданную полосу. Этот поток должен быть отброшен собственными фильтрами;
2. Отправляем «плохие» потоки на сервисные порты тестового адреса;
3. Отправляем «плохие» и «хорошие» потоки на сервисные порты тестового адреса.

На каждом шаге проверяем:

- наличие уведомлений от системы митигации оператора связи ;
- появление заданий митигации в личном кабинете оператора связи;
- показания пробников собственных и внешних;
- отсутствие «плохих» потоков на сервере;
- наличие «хороших» потоков.

Результат:

- опыт взаимодействия с технической службой оператора связи;
- понимание со стороны оператора связи какой сервис нуждается в защите;
- шаблон защиты от типовых угроз для нашего сервиса.

- ✓ Anycast – улучшает доступность сервиса (У нас открытая пиринговая политика);
- ✓ Непрерывный мониторинг из различных мест сети интернет – позволяет гарантировать определенный уровень обслуживания (SLA);
- ✓ Регулярные стресс-тесты ПО и сетевой инфраструктуры - повышают отказоустойчивость.

Полученные знания и опыт в результате тестирования мы успешно применяем в наших технологических решениях.



СПАСИБО ЗА ВНИМАНИЕ! ВАШИ ВОПРОСЫ?



Дмитрий Коваленко

d.kovalenko@msk-ix.ru



www.msk-ix.ru



[/MSK.IX](https://www.facebook.com/MSK.IX)



[@mskixru](https://twitter.com/mskixru)

+7 (495) 737-9295

127083, г. Москва, ул. 8 марта, д. 1, стр. 12

Санкт Петербург 2017 ENOG-13