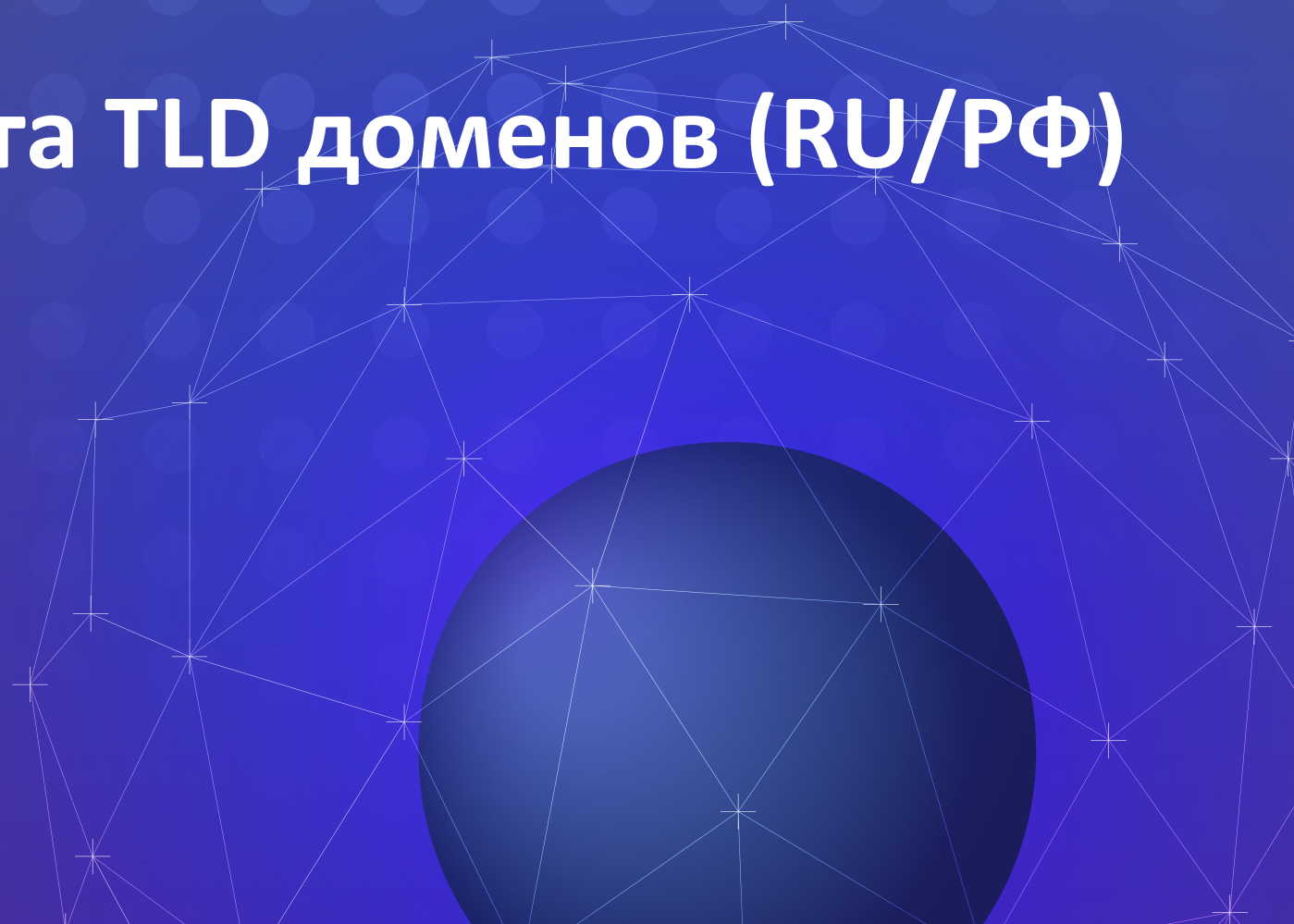




Система мониторинга TLD доменов (RU/РФ)

Александр Ильин
СТО MSK-IX



Авторитетный DNS gTLD



Система распределенных Anycast облаков DNS



18 узлов в Европе, Азии, Северной и Южной Америке, в том числе 9 в России



Технология anycast для оптимальной доступности DNS-сервера из любой точки сети Интернет



Прямой пиринг с сетями 100+ операторов, открытая пиринговая политика на MSK-IX



Отказоустойчивая архитектура на аппаратном и сетевом уровне



Непрерывный мониторинг и круглосуточная техническая поддержка



Регулярные аудиты безопасности и защита от DDoS-атак

Облака Anycast (DNS .RU)

B DNS

Москва
Санкт-Петербург
Новосибирск
Владивосток
Казань
Ростов-на-Дону
Ставрополь
Екатеринбург
Самара

A DNS

Москва (2 узла)
Санкт-Петербург

D DNS

Новосибирск
Гонконг
Астана
Лос Анжелес

E DNS

Амстердам
Франкфурт
Прага

F DNS

Нью Йорк
Окланд
Сан Паоло
Сингапур

Цели системы мониторинга

- Контролировать максимальную доступность сервиса
- Контролировать время отклика DNS
- Гарантировать стабильность платформы
- Контролировать соблюдение SLA

Компоненты мониторинга

- Сетевой мониторинг
- Мониторинг параметров серверов
- Мониторинг DNS узлов
- Мониторинг DNS облаков
- Анализ, корреляция событий, генерация отчетов
- Контроль показателей для защиты от атак

Технические решения



- Разработанная система внутреннего анализа, опроса оборудования и корреляции событий
- Развернутая сеть собственных пробников по всему миру
- Применение внешних пробников RIPE Atlas
- Визуализация внешних пробников ICANN MOSAPI

Защита от DDoS

- Сервис защиты у Upstream операторов
 - Блокирование больших потоков данных
 - Тонкая очистка DNS трафика с учетом профилей
- Собственная сеть детектирования атак
 - На базе статистики и FastNetMon
 - Быстрое реагирование с отчетом для детального анализа
 - Изучаем блокировку на базе flowspec

SLA new gTLD (ICANN)

2. Service Level Agreement Matrix

	Parameter	SLR (monthly basis)
DNS	DNS service availability	0 min downtime = 100% availability
	DNS name server availability	≤ 432 min of downtime ($\approx 99\%$)
	TCP DNS resolution RTT	≤ 1500 ms, for at least 95% of the queries
	UDP DNS resolution RTT	≤ 500 ms, for at least 95% of the queries
	DNS update time	≤ 60 min, for at least 95% of the probes

Что мы проверяем?

- Целостность доменных зон, доступность серверов дистрибуции
- Параметры сетевой инфраструктуры, каналов связи, жизнеспособность серверов
- Корреляция параметров в рамках облака.
Измерение метрик для каждого облака в целом

Методика внутреннего тестирования



- 1 запрос (без рекурсии) по протоколам UDP или TCP.
- Ответ должен содержать информацию из MSK-IX DNS, иначе запрос считаем неответченным.
- Запрос с $RTT > 2$ секунды будет считаться неответченным.

Возможные результаты теста DNS: число в миллисекундах (ms), соответствующее RTT разрешения DNS или неопределенное / неответченный.

- "Измерение параметров DNS" выполняется каждую минуту, каждый зонд DNS выполняет тест DNS по протоколам UDP или TCP для каждого из зарегистрированных IP-адресов, обслуживающих сервис MSK-IX DNS.
- Если результат теста DNS не определен / не получен ответ, IP-адрес считается недоступным для этого теста до следующих измерений.

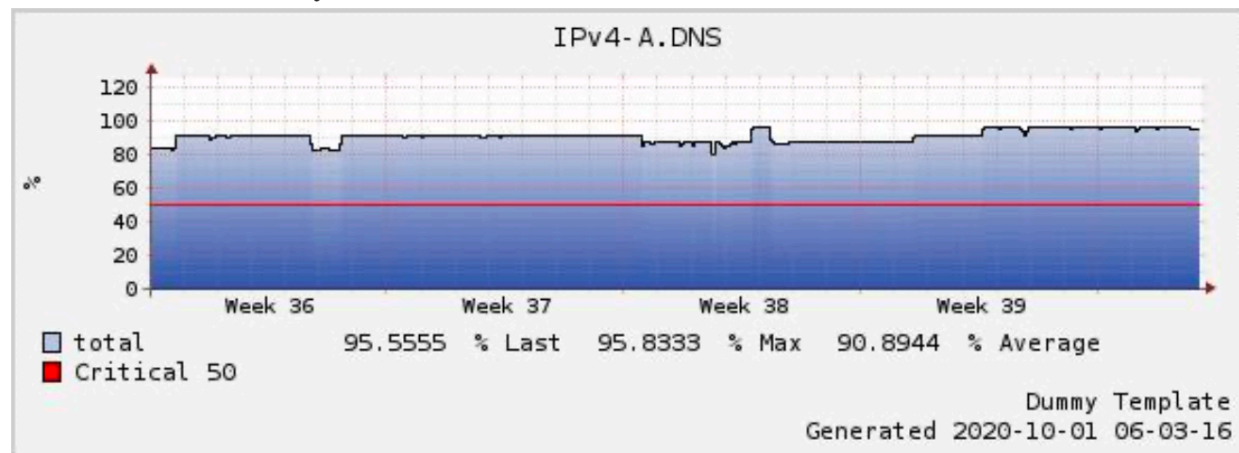
Monthly DNS SLA

Parameter	Status	SLR (monthly basis)
MSK-IX DNS service availability	100%	100% availability
<u>IPv4 A.DNS</u> name server availability	100%	99%
IPv4 TCP DNS resolution RTT	99.807%	less than 1500 ms, for at least 95% of the queries
IPv4 UDP DNS resolution RTT	99.782%	less than 500 ms, for at least 95% of the queries
<u>IPv6 A.DNS</u> name server availability	100%	99%
IPv6 TCP DNS resolution RTT	99.857%	less than 1500 ms, for at least 95% of the queries
IPv6 UDP DNS resolution RTT	99.706%	less than 500 ms, for at least 95% of the queries
<u>IPv4 B.DNS</u> name server availability	100%	99%
IPv4 TCP DNS resolution RTT	99.613%	less than 1500 ms, for at least 95% of the queries
IPv4 UDP DNS resolution RTT	99.309%	less than 500 ms, for at least 95% of the queries

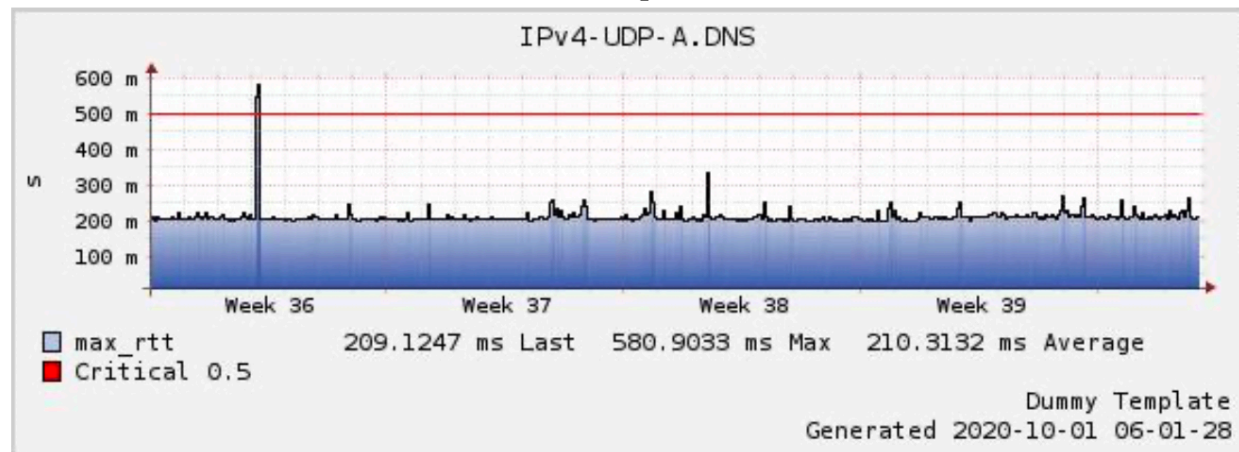
Визуальный анализ

По всем облакам
Для примера a.dns
SA считается в процентах
корректных ответов по
запросам зондов

IPv4 Server Availability: 100%



IPv4 UDP RTT < 500 ms, for 99.782% of the queries



IPv4 TCP RTT < 1500 ms, for 99.807% of the queries

Анализ мониторинга ICANN



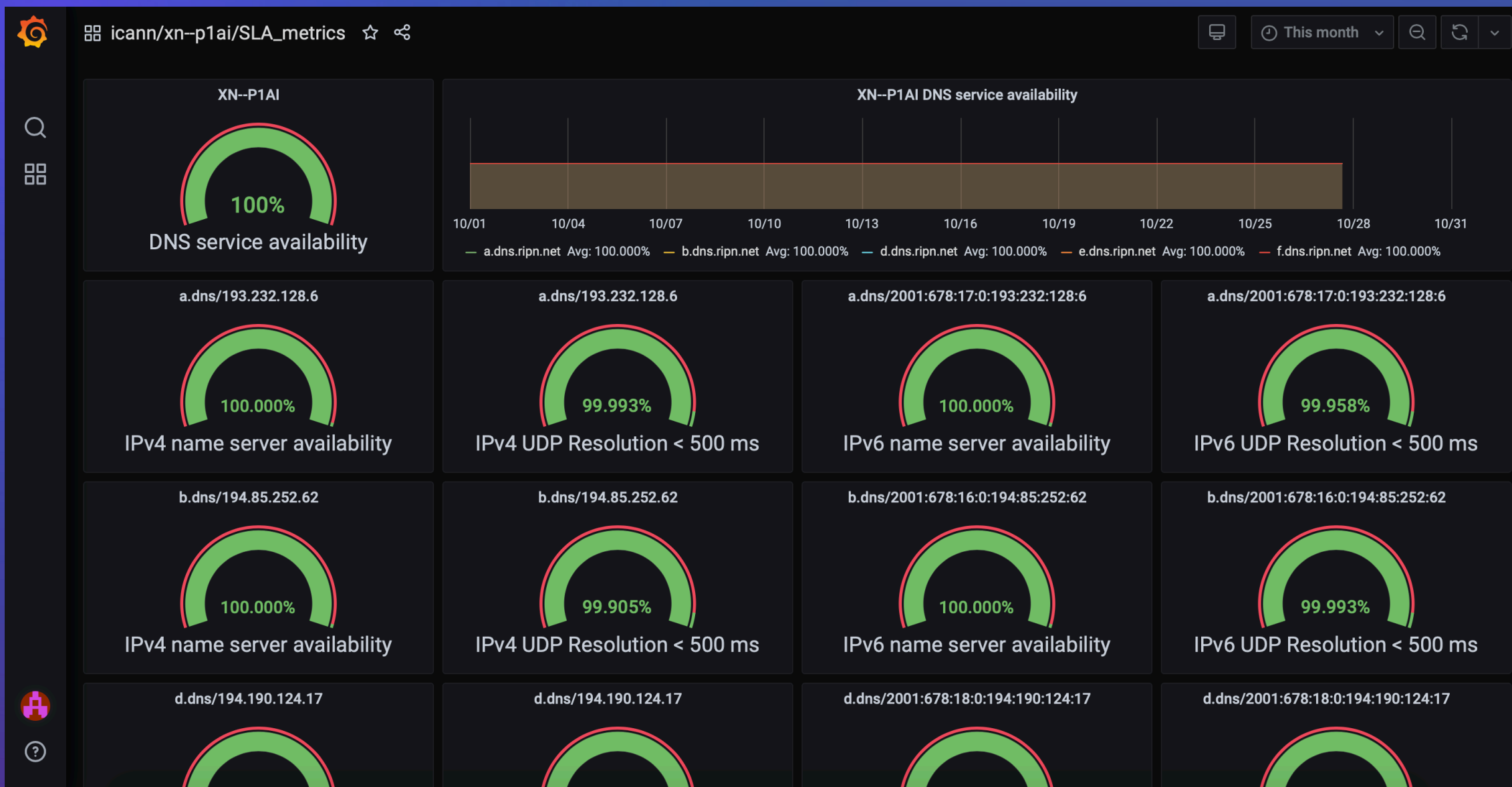
Интеграция с ICANN:

- Сбор данных (текущее состояние, данные измерений)
- Хранение данных (БД Clickhouse)
- Визуализация данных (Grafana)

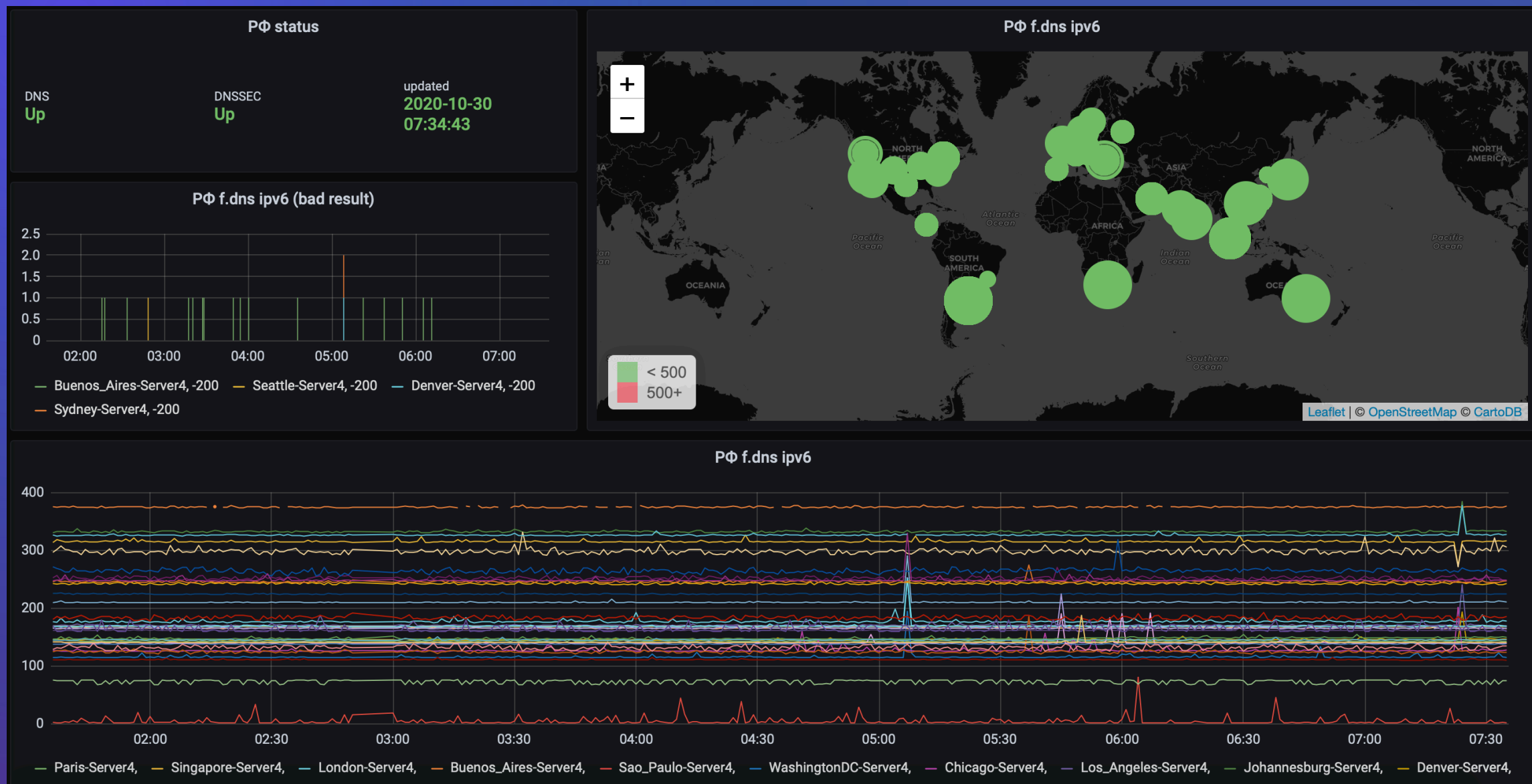
Визуализируются основные метрики

- DNS service availability
- DNS name server availability
- DNS resolution RTT

Визуализация мониторинга ICANN



Визуализация мониторинга ICANN (2)



Спасибо за внимание!

Ваши вопросы?

Александр Ильин
СТО MSK-IX

+7 (495) 737-92-95

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



Адрес в сети

msk-ix.ru



Facebook

facebook.com/msk.ix