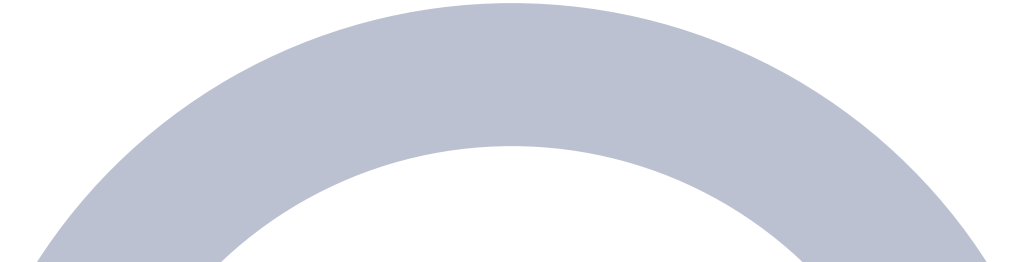
Доверенный NTP
как фактор безопасности сети

12.09.2023

NTP – Network Time Protocol

NTPv0	***NTPv1***	***NTPv2***	***NTPv3***	***NTPv4***	***NTS – RFC 8915 = NTPv4+TLS+AEAD***
1985 год	1988 год	1989 год	1992 год	2015 год	
RFC 958	RFC 1059	RFC 1119	RFC 1305 + 1361 + 1769	RFC 2030 + 4330 + 5905	
	client–server and peer-to-peer modes	state machine	новые метрики, улучшен алгоритм выбора когда сервера дают большую разницу, broadcast mode, symetric key	Port rand, MAC change, ext. Field, autokey	

No NTPv5



Состояние часов влияет… на всё

“Network boxes" с NOS

- От "криптошлюзов" и прочих VPN концентраторов — от "pizza box" like до больших модульных сетевых шкафов на десятки юнитов
- Логи - самая небольшая проблема. Просто у вас будет мешанина в SIEM системах какая именно - зависит от pipeline сбора → хранения → обработки логов. может так: NOS → SIEM, а может и так: NOS → SLOG → SIEM(s)
- Внутренний скриптинг. Commit scripts, биллинговый аккаунтинг через счётчики фильтров/интерфейсов, AS PATH prepend
- Кластеризация и стекирование - непредсказуемо
- Телеметрия - netflow / JFlow / JTI / SFlow / IPFIX - и т.д.

Состояние часов влияет… на всё

Сервера с вашими любимыми OS

- Hoster. Сдаю в аренду CPU+RAM+HDD/SSD@VPS/VDS — у клиентов пускай цветут 1000 цветов. А как же soft СХД? GlusterFS / CEPH deployment prerequisites - Synchronize time across all storage servers using the Network Time Protocol
- Enterprise. Контролируемая среда, запускаем на IaaS (почти) одинаковые(?) VM и/или контейнеры десятками/сотнями. Неправильное время на хосте повлияет на ВСЕХ гостей
- Оператор связи. Всё что рядом с биллингом, тарифами – деньги. Всё что рядом с управлением конфигурациями сети и мониторингом - SLA
- Контент генератор. Много логики в CDN завязано на что-то-по-расписанию
- Сервисы. Бесконечное разнообразие проблем
- Данные. Возможно будут испорчены

Состояние часов влияет… на всё

• *PCI DSS - Payment Card Industry Data Security Standard*

- Постоянно обновляющийся стандарт
- 2004 → 1.0 / 2006 → 1.1 / 2008 → 1.2 / … / 2022 → 4.0
- 12 главных направлений (больших категорий), 440 проверочных процедур
- Одно из них - "Протоколирование событий и действий"
- В 4.0 появилось требование мультифакторной аутентификации – «PCI DSS requires multi-factor authentication for all non-consumer users and administrators on all system components»
- Multifactor auth → TOTP (Time-based one-time Password)

- ***На что повлияет у вас? Проверьте сами. Устройте «учения»***

  - Лучше делать на дублирующей инфраструктуре
  - Детально продумайте сценарий
  - У вас же есть бекапы, которые вы тестируете?
  - И процедуры «disaster recovery»?

Источники

GNSS	– дорого (карта, кабель, антенна). Проблемный жизненный цикл платформы. Не везде и не всегда устойчивый приём
Атомные часы	– очень дорого, отдельные самостоятельные устройства, можно использовать для “дисциплинирования” часов, сложные интерфейсы сопряжения. Иногда нужен «нестандартный OPEX», кто поймёт что с ними всё ОК? Вибрации? Изменение температуры? Поверка от других атомных часов?
Рубидиевые и цезиевые “кубики”	– ставят вместе с другим источником, можно брать PPS, не самостоятельны
Коробочный NTP сервер	– готовые 1-2U коробки → vendor lock (внутри x86 COTS задорого), сложно и дорого мониторить, интегрировать с NMS, защищать, обновлять цикл платформы. Не везде и не всегда устойчивый приём
pool.ntp.org	– давайте посмотрим на него внимательно

pool.ntp.org

- pool.ntp.org - кто-то, где-то, как-то, в том числе на адресах "Dynamic IP Pool for Broadband Customers" (далеко и не надёжно).
- всё (все версии протокола) для всех – единственный рекомендованный софт для участников – ISC NTP

Ноябрь 2022, один из участников pool.ntp.org

NTP ver	No. of Q	% Total Q	% IPv4	% IPv6	No. of clients
4	5,942,781,255	81.59	98.07	1.92	45,037,414
3	1,292,326,962	17.74	93.63	6.36	127,218,626
1	43,996,867	0.6	99.99	0.005	6,967,648
2	2,535,364	0.03	99.7	0.29	37,055

pool.ntp.org

- ✗ Зона не подписана! Доверяем DNS?
- ✗ SRC IP spoofing. Кто вам присылает пакеты?
- ✗ SLA? - не для пользователей, только проверки пробниками участников пула
- ✗ Не публикуют детальную статистику, только график доступности (картинку) за последние два дня
- ✗ Нет рейтинга (ранжирования) участников
- ✗ Можно очень долго выбирать лучших самостоятельно оценивая связность, количество точек присутствия, репутацию, компетенции...
- ✗ Но о том какова нагрузка на сервисе (ресурсы CPU/NET) и сможет ли владелец отмасштабировать инстанс(ы) вы никогда не узнаете

Где брать NTP?

- Те, кто делает различные хорошие, сложные (атомные) часы. Умеют в приборы и методики, ограничены своей инфраструктурой
- Операторы связи, телеком. Хорошо умеют делать инфраструктуру, а сервисы – по разному. Некоторые могут дать сервис внутри вашего L3VPN, но возможно небесплатно. Autokey – не дадут. Хостят сервис только у себя, а мы знаем что не бывает абсолютно надёжных ISP
- Гиперскейлеры - GCP, AWS, другие CLOUD платформы. Небольшие предлагают использовать pool.ntp.org, большие – дают только managed OS (всё низкоуровневое делают за вас)

- ***У тех, кто его сделал для себя (и для вас), например - https://www.msk-ix.ru/ntp-server/***

Как хорошо взять сервис. Дизайн для себя

01 Возьмите время (уже выбрали сервис?) на несколько своих серверов (не сетевых коробок). Почему? Мониторинг, метрики, ACL, понятный софт и жизненный цикл платформы

02 Синхронизируйте их все между собой (авторизовано по autokey)

03 Лучше выбрать современные типы хеширования ключей

04 В конфиге используйте конструкцию:

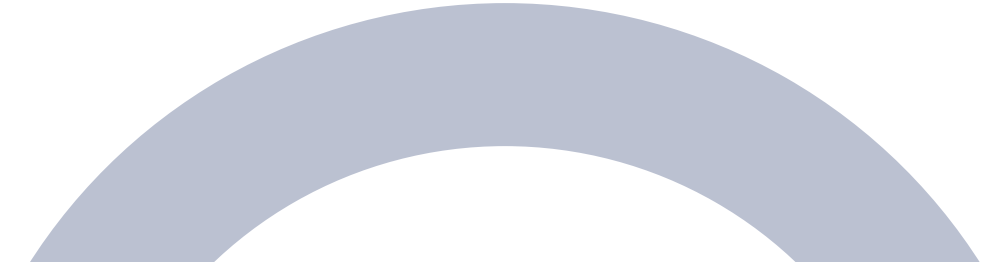
- “pool” с fqdn если у вас хороший DNS
- “server” с IP4/6 если хотите чтобы NTP продолжал работать когда DNS приляжет

05 Сервисный адрес (откуда будут брать время все ваши системы) сделайте (локальным) anycast-ом

06 ACL с rate limit

07 ReadOnly rootfs добавляет XX “поинтов” к надёжности

08 Не забудьте про мониторинг



Вопросы?!

Иван Власов
I.vlasov@msk-ix.ru