NTP e NTS

SINCRONISMO DE TEMPO NA INTERNET DE FORMA CORRETA E SEGURA

Antonio Marcos Moreiras

29/09/2021

Agenda

1. Por que usar o NTP?
2. O tempo e os relógios.
3. Conceitos importantes e funcionamento básico do NTP.
4. NTP e segurança.
5. NTS: a nova extensão de segurança do NTP.
6. O NTP.br e o NTS
7. Como utilizar o NTP na prática: topologias e softwares sugeridos
8. Cliente NTP com ntpsec usando NTS
9. Cliente NTP com chrony usando NTS
10. Servidor NTP com ntpsec usando NTS
11. Servidor NTP com chrony usando NTS

Parte 1:

Por que usar o NTP?

Por que usar o NTP?

Registrar o tempo corretamente não é importante….

Até o momento em que é!

Por que usar o NTP?

- Os relógios dos computadores e dispositivos de rede, por si mesmos, **não são bons em medir o tempo**.
  - podem “errar” em vários segundos por dia
  - alguns dispositivos sequer mantêm o registro do tempo quando desligados

Por outro lado, muitos softwares e sistemas dependem do correto registro do tempo

Problemas

O relógio de um computador ou grupo de computadores

- pode estar **diferente do horário correto**;
- pode ter sido **ajustado para o passado**;
- pode **discordar dos outros computadores**.

Distribuição de conteúdos

- O tempo pode ser usado para controlar expiração de documentos e funcionamento do cache. O relógio errado pode causar perda de informações ou impedir o acesso às mesmas.

Sistemas de arquivos (filesystems)

- A criação e modificação de arquivos é um dos metadados dos sistemas de arquivos. Algumas aplicações dependem dessas informações.
- Datas de criação e modificação no futuro podem impedir aplicações de funcionar.
- Sistemas de gerenciamento de versões, como cvs e git podem ser afetadas, sistemas de compilação automática, como make, sistemas de backup e de banco de dados.

Agendadores de eventos

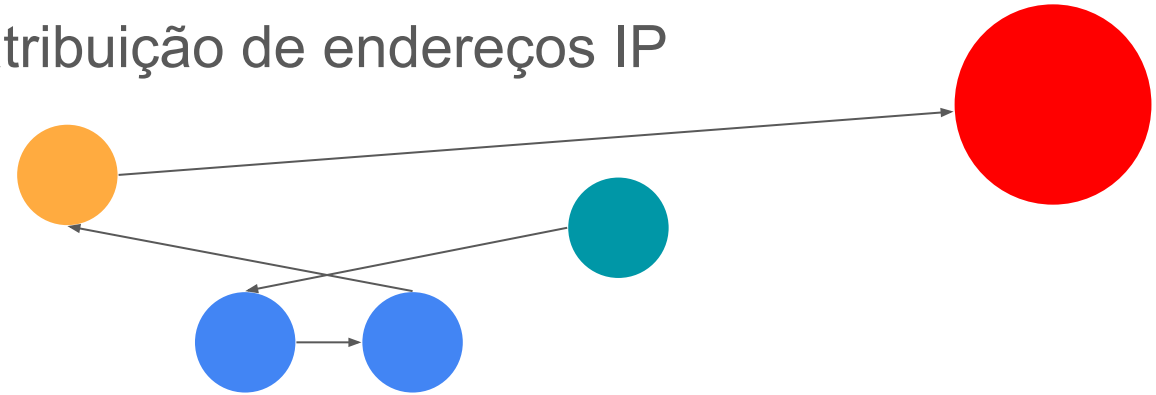
- Aplicações como cron e at podem ser afetadas.

Autenticação

- A validação dos certificados TLS depende do tempo
- Alguns serviços expõem APIs que requerem autenticação cada vez que uma aplicação faz uma consulta. Pra prevenir ataques de repetição, normalmente os clientes têm que informar ao servidor um timestamp que está dentro de um pequeno intervalo de tempo do relógio do servidor.
    - Por exemplo: o Amazon S3 tolera uma janela de 15 minutos. Kerberos, alguns poucos minutos.

Investigação de incidentes

- Os diversos sistemas fazem registros diversos (logs)
- Quando ocorre um incidente, para pesquisar sua causa, precisamos saber o momento e a ordem correta dos acontecimentos
  - Exemplos: investigação de queda de sistemas, registro de atribuição de endereços IP



NTP como solução

- O NTP é um sistema que utiliza poucos recursos computacionais e sua configuração é simples. Em muitos sistemas hoje já vem instalado e configurado por padrão.
  - Nem sempre a configuração padrão é a mais adequada e nem sempre ela existe!
- O NTS, agora disponível, e novas implementações de clientes e servidores, tornaram o NTP mais robusto e seguro nos últimos anos.

Parte 2:

O tempo e os relógios

O que é o tempo?

- O conceito do tempo está relacionado à CAUSALIDADE.

o EVENTO 1 acontece e
por CAUSA dele
o EVENTO 2 acontece

- o EVENTO 1 acontece ANTES
- o EVENTO 2 acontece DEPOIS

o TEMPO mede o intervalo entre a CAUSA e o EFEITO

O tempo não é tão simples

- Para nós parece que o tempo avança de forma sempre igual, linear. Mas a verdade é que o tempo não é o que parece, ele está intimamente ligado ao espaço, à velocidade e à gravidade.
  - Viagens no tempo acontecem e são corriqueiras.
  - Quanto mais gravidade, mais lento o fluir do tempo.
  - Quanto mais movimento (na dimensão do espaço), mais lento o fluir do tempo.

Os relógios atômicos nos satélites do sistema GPS adiantam por dia cerca de 38.6 μs

Felizmente, para nós, o tempo é simples

- Para efeitos práticos, no dia a dia da Internet e redes, enquanto estivermos falando de uma rede apenas GLOBAL, os efeitos relativísticos podem ser desconsiderados!
- As correções no sistema GPS são feitas automaticamente e os receptores já nos informam a posição e a medição de tempo de forma acurada.

Referência de tempo

- Historicamente, o tempo foi medido com base no dia solar médio. O segundo era 1/86400 do dia solar médio. Ou seja, com base na rotação da Terra.
- Em 1954 definiu-se o segundo com base na translação da Terra, em torno do Sol. O segundo passou a ser 1/31.556.925,9747 do tempo que a Terra leva para dar uma volta completa no Sol, tendo como base as 12h do dia 04/01/1900.

Referência de tempo

- Desde 1967 o segundo é definido com base na medição dos ciclos energéticos de átomos de Césio, ou seja, com base nos relógios atômicos.

"O segundo é a duração de 9.192.631.770 períodos da radiação correspondente à transição entre dois níveis hiperfinos do estado fundamental do átomo de césio 133."

Quem mede o tempo?

- Laboratórios metrológicos em todo o mundo, de forma coordenada, a partir de relógios atômicos.
  - No Brasil o **Observatório Nacional**
  - https://www.gov.br/observatorio/pt-br/assuntos/areas-de-atuacao/tempo-e-frequencia
  - Trabalho coordenado mundialmente pelo bureau International des Poids et Mesures (BIPM)

Escalas de tempo

- TAI (Temps Atomique International)
  - Calculada pelo BIPM
  - mais de 260 relógios atômicos em todo o mundo
  - erro em relação a um relógio imaginário perfeito da ordem de 100ns ao ano

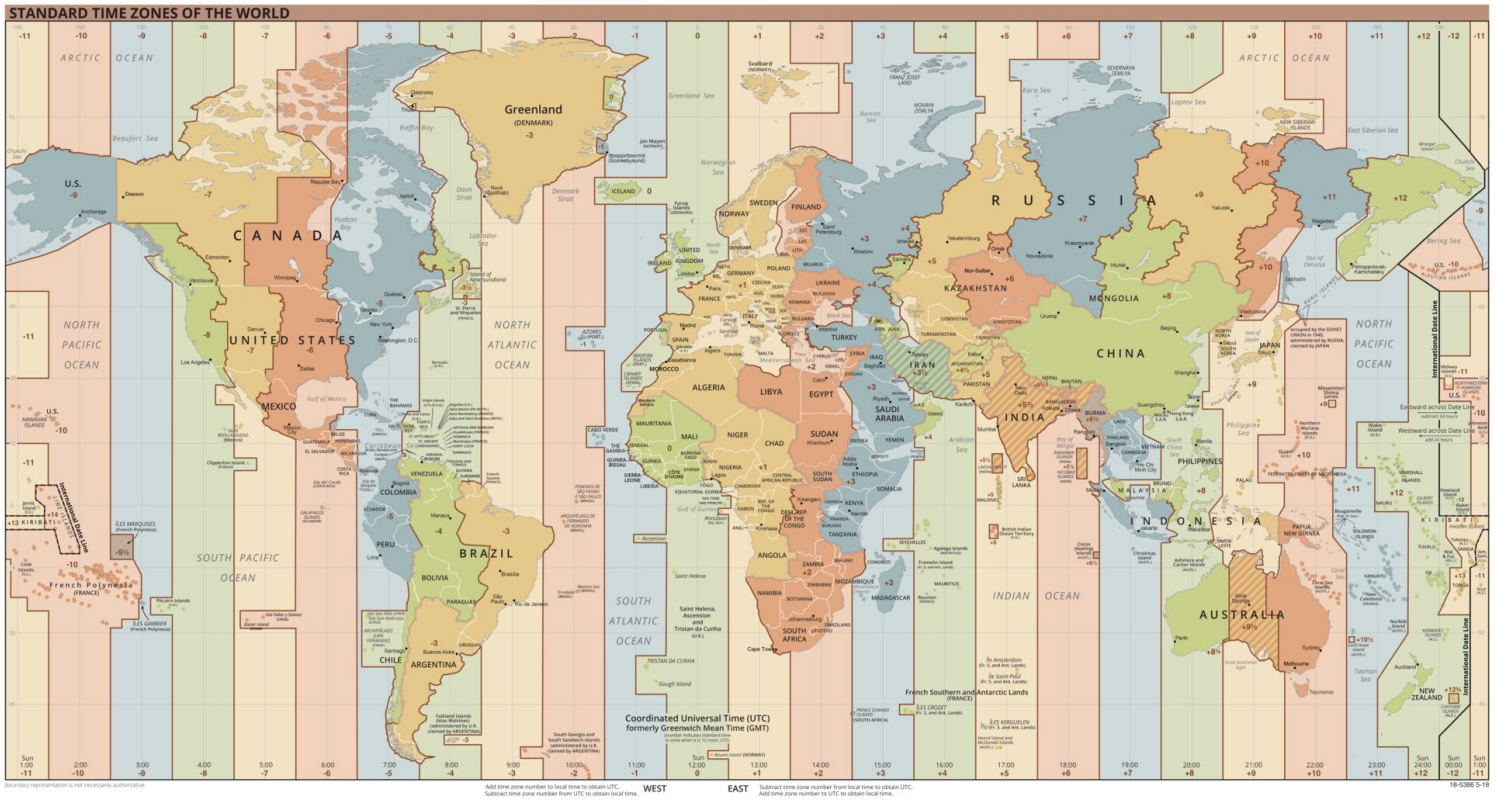
Escalas de tempo

- UTC (Universal Time Coordinated)
  - Baseada no TAI, mas disciplinada pelo Sol
  - Um leap second pode ser acrescentado ou removido, quando necessário, para garantir que o Sol esteja exatamente sobre o meridiano de Greenwich as 12h, com erro máximo de 0,9s.
  - Ou seja, o UTC é “compatível” e sucessor do antigo GMT (Greenwich Mean Time), que era usado quando o tempo era baseado no dia solar.
  - **O UTC é o que usamos no dia a dia e no NTP.**

Escalas de tempo

- TA(k)
  - Escala “real” de um conjunto de relógios atômicos específicos. Por exemplo, o ON gera o TA(ONRJ) e contribuí com ela para o TAI. TA(NIST) é a escala mantida pelo US National Institute of Standards and Technology.
- GPS Time
  - Os GPS adotaram uma escala sincronizada com o UTC em 1980, mas não fizeram correções de leap seconds. Até a data em que essa apresentação foi feita houve 18 leap seconds. Na prática os receptores calculam isso e normalmente não precisamos nos preocupar com essa diferença.

Tempo Local (fusos horários)



Tempo Local (fusos horários)

- O Brasil usa 4 fusos horários diferentes
- Lei 12.876 de 2013
- Não há mais horário de verão no Brasil (mudança de fusos horários ao longo do ano)
- O NTP não lida com fusos horários nem horário de verão. Sempre trabalha com UTC.
- O sistema operacional lida com os fusos horários e horário de verão.
- Recomenda-se registrar o tempo nos logs em UTC (sem o horário local)

Parte 3:

Conceitos importantes e funcionamento básico do NTP

Como os relógios (dos computadores) funcionam

- **oscilador**
- **contador**
- **dispositivo de leitura ou visualização**

Como os relógios (dos computadores) funcionam

- **oscilador**
  - gera eventos cíclicos a uma taxa constante
  - frequência (ritmo)
    - **sintonia**
    - **sincronismo**
  - cristais de quartzo

Como os relógios (dos computadores) funcionam

- **contador**
  - conta, acumula, os ciclos do oscilador, e os converte para medidas conhecidas, como nanosegundos, microsegundos, segundos, horas, etc
  - o valor do contador normalmente é registrado como um ***timestamp***
  - **monotonicidade**

- **dispositivo de leitura ou visualização**
  - software

Propriedades

- ***Accuracy* (exatidão, acurácia)**
  - quanto um relógio está certo ou errado, quanto está próximo às referências
  - para garantir a ***accuracy*** disciplinamos o relógio
    - fase e frequência, sincronismo e sintonia
- ***Precision* (precisão)**
  - *resolution, granularity*
  - menor incremento possível do contador, “passo” do contador
  - depende da frequência do oscilador do relógio, da frequência da CPU, do software que faz a leitura

Propriedades

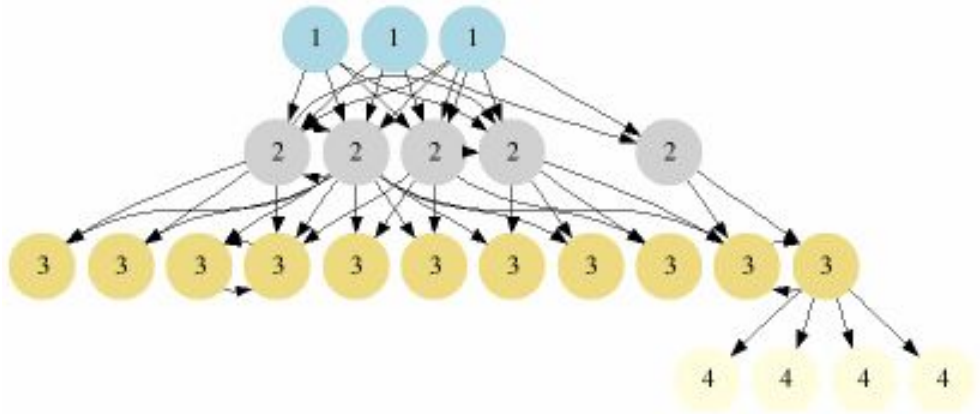
- ***Offset*** **(diferença, deslocamento)**
  - diferença entre o relógio local e uma referência
- ***Dispersion*** **(dispersão)**
  - erro estimado na medição
    - variações no oscilador, excesso de uso da CPU, latência causada por interrupções, latência na rede, etc.
- ***Jitter***
  - variação entre diferentes medições para uma mesma referência

Propriedades

- ***Aging*** **(envelhecimento)**
  - é a medida da instabilidade na frequência do oscilador causada por fatores internos, quando os externos (temperatura, radiação, pressão, umidade) são constantes.
- ***Drift*** **(escorregamento)**
  - é a instabilidade total na frequência do oscilador, considerando fatores externos e internos, como variações de radiação, pressão, temperatura, umidade e envelhecimento.

O NTP (Network Time Protocol)

Topologia hierárquica

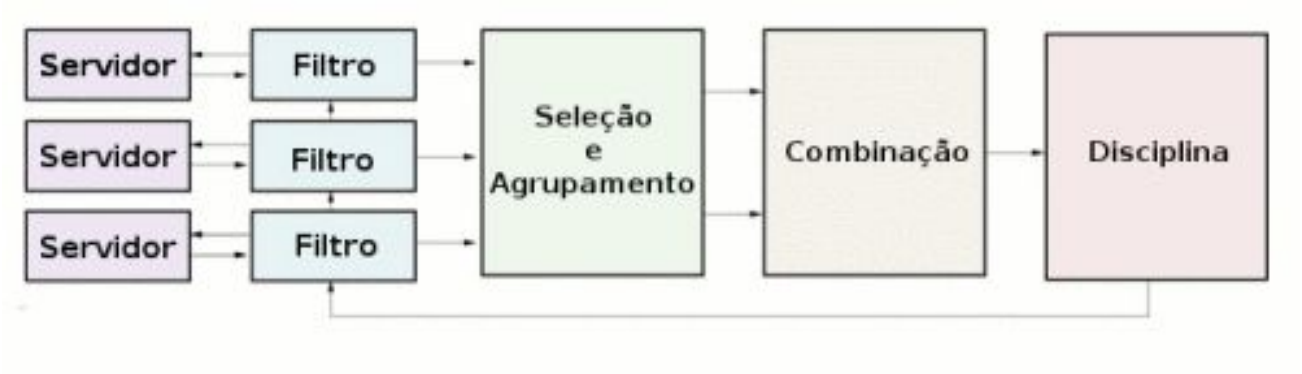


Topologia Hierárquica

- Cliente / Servidor
  - existem outros modos de operação, como o modo simétrico, os os servidores funcionam como “pares” (mesmo nível hierárquico), e o modo multicast
    - recomendação: não use
- Na prática, faz pouca diferença qual stratum você utiliza
- Na prática, há necessidade de poucos níveis, porque o protocolo é muito leve e um servidor suporta muitos clientes

O NTP (Network Time Protocol)

Não é apenas um protocolo, mas também
um conjunto complexo de ALGORITMOS



NTP: protocolo e algoritmos

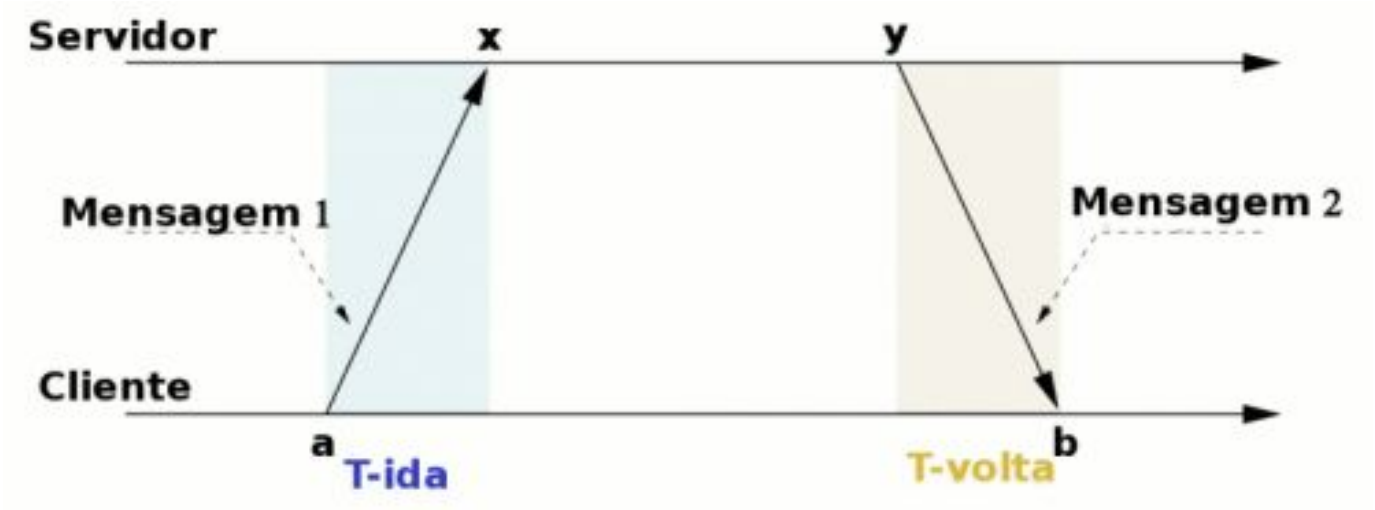
- Obtém informações do relógio de vários servidores
- Seleciona os que têm ou não o relógio correto
- Escolhe a melhor referência entre os corretos, e o conjunto de referências secundárias a serem levadas em consideração
- Disciplina o relógio local
- Garante a monotonicidade do tempo
- Usa criptografia para aumentar a confiabilidade do sistema como um todo

O NTP (Network Time Protocol)

O protocolo e o cálculo da diferença entre os relógios

delay = (a-b) - (y-x), podemos SUPOR que Tida = Tvolta

offset = x - (a + Tida) = (x + y - a - b)/2

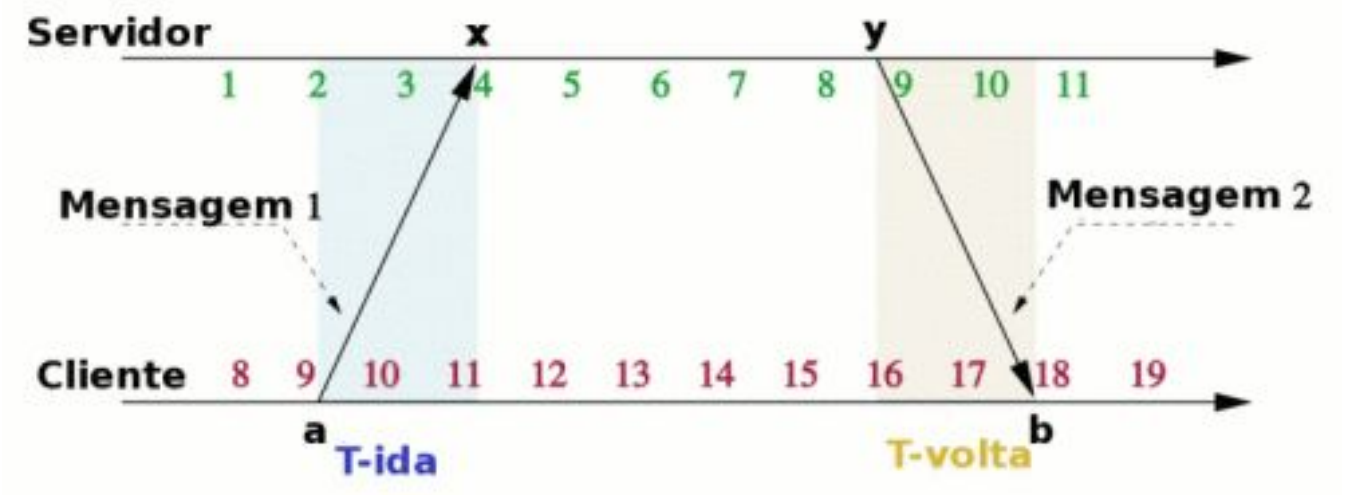


O NTP (Network Time Protocol)

O protocolo e o cálculo da diferença entre os relógios

delay = (18-9) - (9-4) = 9-5 = 4, podemos SUPOR que Tida = Tvolta = 2

offset = 4 - (9 + 2) = -7 (o cliente tem que atrasar seu relógio em 7)



O NTP (Network Time Protocol)

Funciona sobre UDP

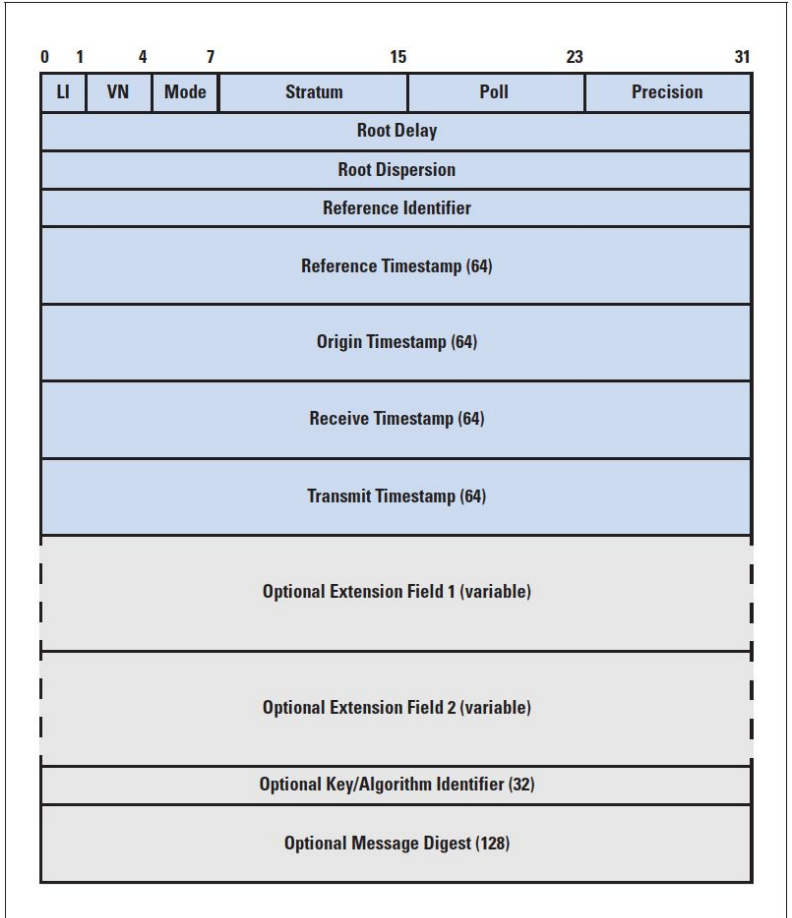
Usa por padrão a porta 123 UDP

48 bytes

Tráfego baixo = 1 pacote para cada servidor configurado a cada 16 minutos em regime

Estimativa = 3 servidores x 100 bytes / 1 min =

= 3 x 800 bits / 60s =~ 40bps

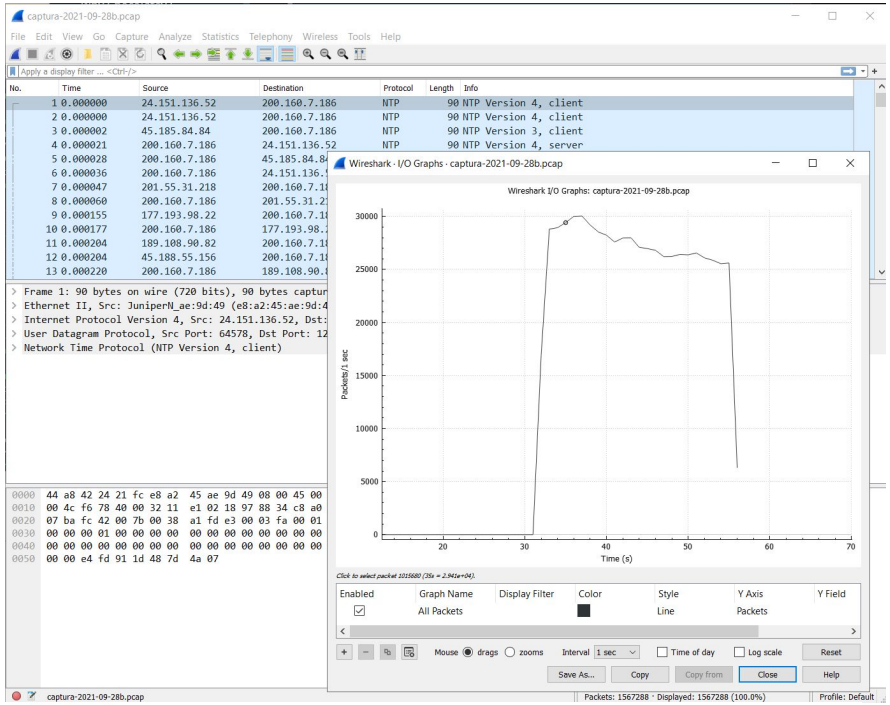


O NTP (exemplo)

10Mbps (em cada sentido)

~ 300.000 clientes

~ 33bps/cliente



Statistics

Measurement	Captured
Packets	1567288
Time span, s	56.244
Average pps	27866.1
Average packet size, B	91
Bytes	142624393
Average bytes/s	2535k
Average bits/s	20M

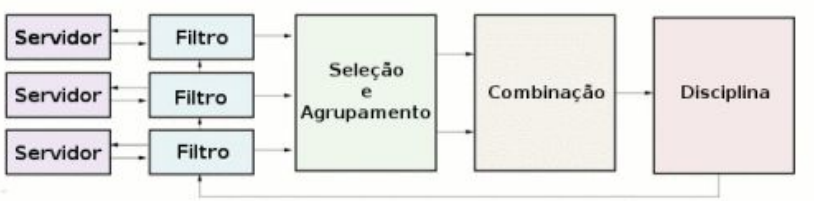
Wireshark · Conversations · captura-2021-09-28b.pcap

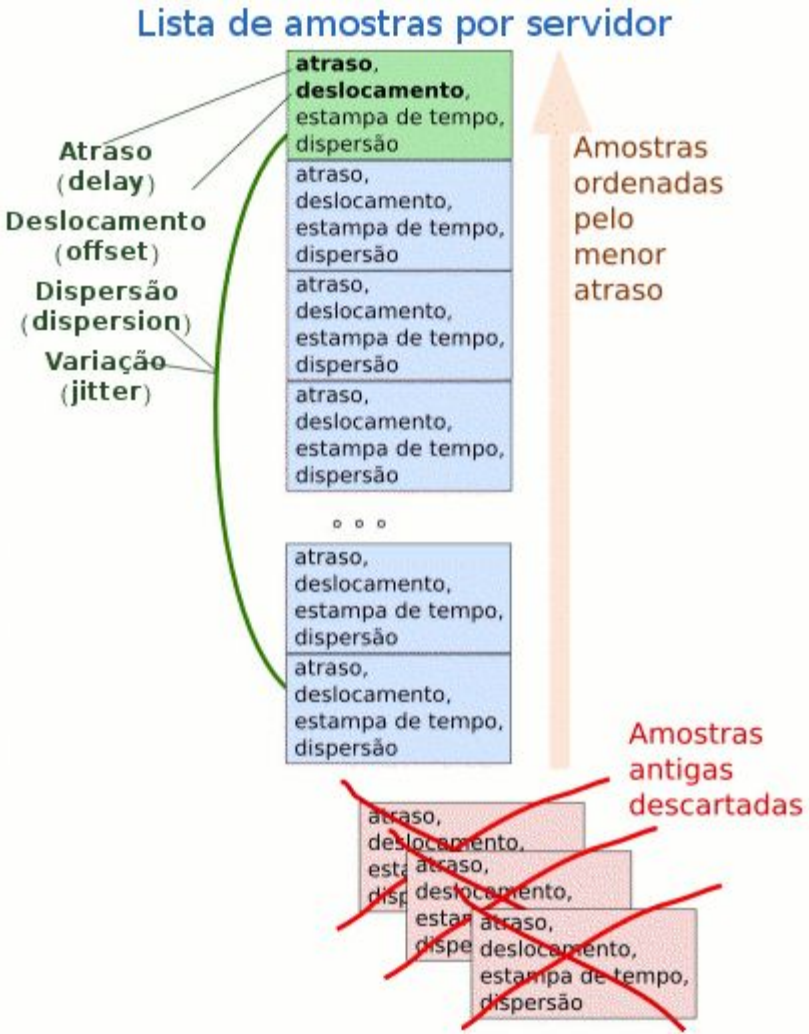
Ethernet · 5 | IPv4 · 279684 | IPv6 · 21303 | TCP | UDP · 537091

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A
2001:d08:100:955:dac6:78ff:fe03:6ab0	2001:12ff:0:7::186	2	220	1	110	1
2001:d08:100:968:c23d:d9ff:fe88:79c0	2001:12ff:0:7::186	4	440	2	220	2
2001:db7:3003:da:dac6:78ff:fe2a:db90	2001:12ff:0:7::186	2	220	1	110	1
2001:db8:2:e09e:8454:2427:fd60:b606	2001:12ff:0:7::186	4	440	2	220	2
2001:db8:7:8014:58bd:6f58:d58b:ea31	2001:12ff:0:7::186	2	220	1	110	1
2001:db8:82:82::2	2001:12ff:0:7::186	2	220	1	110	1
2001:db8:165:a900:5924:57b8:96dd:ec7	2001:12ff:0:7::186	2	220	1	110	1
2001:db8:16b:8e01:c53d:598c:7528:2b3	2001:12ff:0:7::186	2	220	1	110	1
2001:db8:91e:4000:c23d:d9ff:feb0:9258	2001:12ff:0:7::186	2	220	1	110	1

Algoritmos NTP - Filtro

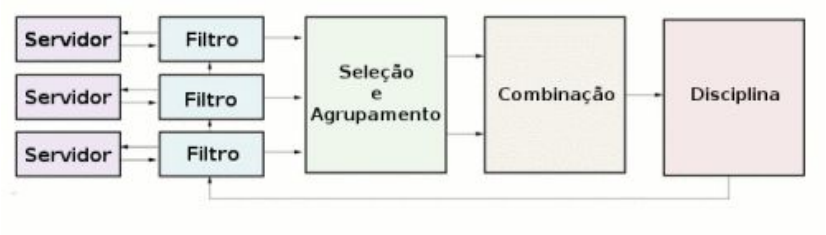
Várias amostras por servidor
Ordena por delay
Calcula parâmetros
Descarta as piores

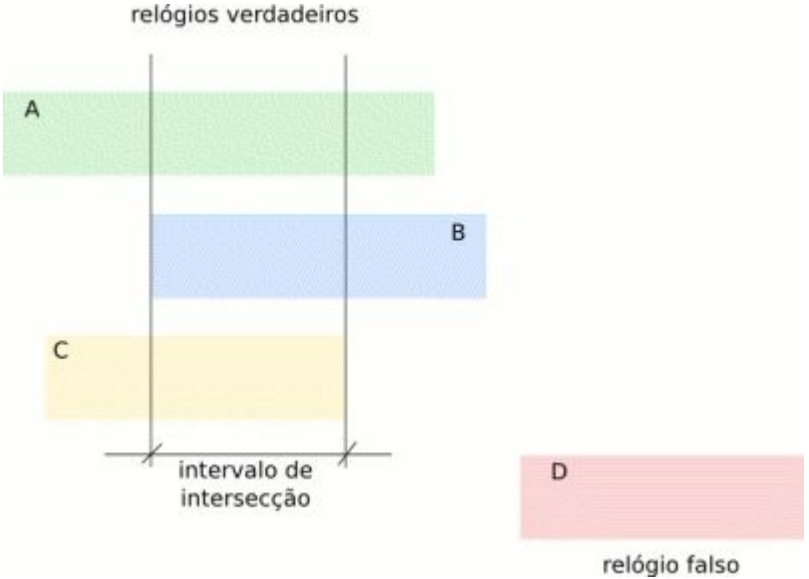




Algoritmos NTP - Seleção e Agrupamentos

Calcula um intervalo de confiança (erro estimado)
Compara os diferentes servidores
Descarta os não coincidentes

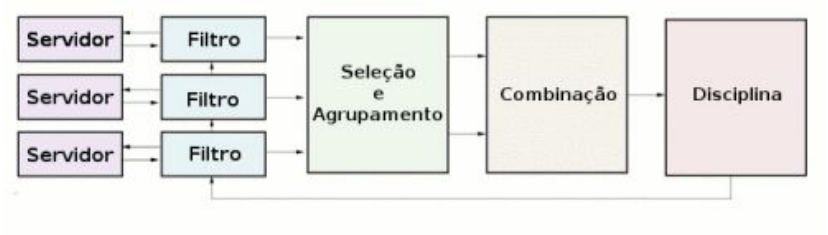


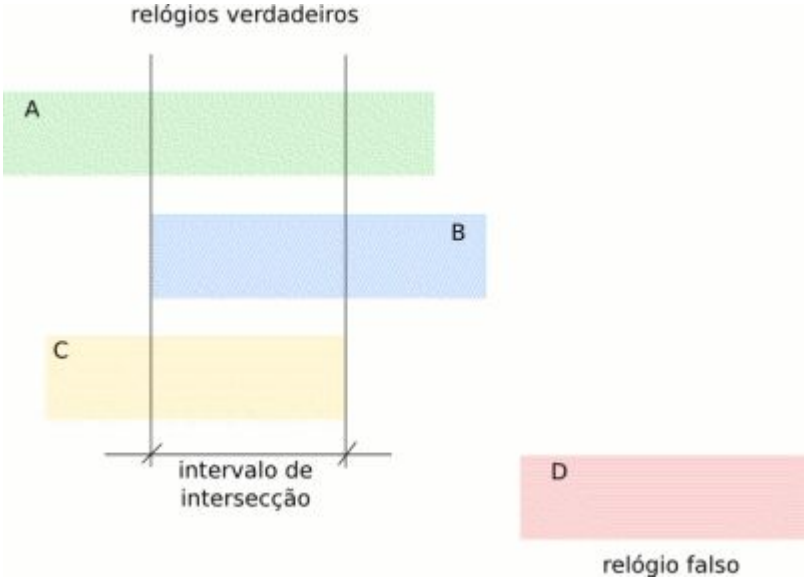


Algoritmos NTP - Seleção e Agrupamento / Combinação

Calcula um intervalo de confiança (erro estimado)
Compara os diferentes servidores
Descarta os não coincidentes

Escolhe o melhor ou melhores

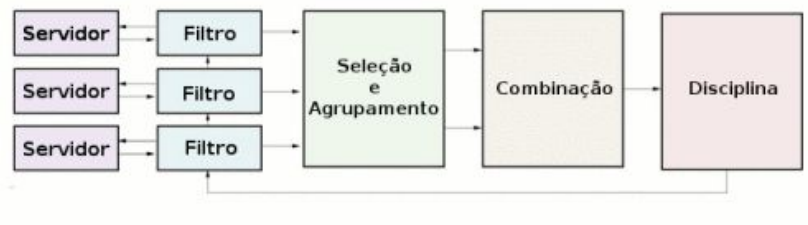




Algoritmos NTP - Disciplina do Relógio Local

Pode ser baseada em Fase ou Frequência
- Fase = acerta o ponteiro do relógio
- Frequência = ajusta o pêndulo ou mola do relógio pra que ele pare de adiantar ou atrasar

A disciplina é feita de forma contínua, mesmo em períodos em que não é possível consultar os servidores de tempo. As características do relógio local são medidas e se tornam conhecidas do NTP.



NTP: segurança

- A **confidencialidade** não é considerada um problema, ou um requisito, no contexto do NTP
- Os algoritmos apresentados até agora garantem de forma bastante satisfatória a **integridade** e a **disponibilidade** do serviço de manter o relógio correto
- Algoritmos de criptografia no contexto do NTP garantem principalmente a **autenticidade**.

NTP: segurança

- Chaves simétricas (symmetric keys)
  - existe desde o NTP v3
  - não oferece meios para transmissão ou armazenamento seguro das chaves
- Autokey
  - introduzido no NTP v4
  - a RFC 5906 não especifica um padrão (informational)
  - não funciona com NAT
  - é complexo e inseguro
  - **não deve ser utilizado!**
- NTS
  - novo!

Parte 4:

NTP e segurança

NTP e segurança

- Segurança não era uma preocupação na correta sincronização dos relógios no passado
- Mas muita coisa mudou:
  - a Internet cresceu e se descentralizou
  - há muitas evidências de um tratamento inadequado da segurança no NTP
  - há um interdependência crescente entre o registro do tempo e a segurança
  - há requisitos legais e de conformidade

NTP e segurança

NEWS

Attackers use NTP reflection in huge DDoS attack

The attack peaked at over 400Gbps, according to CloudFlare, the company whose infrastructure was targeted

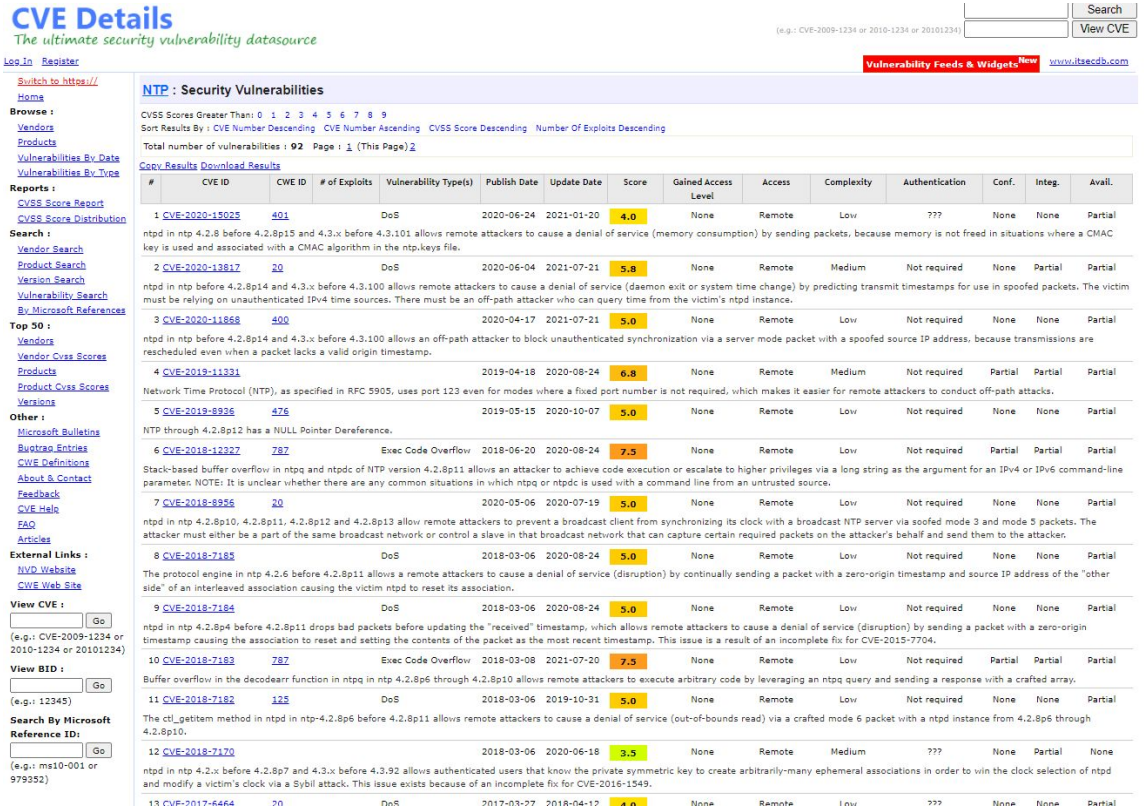
By Lucian Constantin
CSO Senior Writer, IDG News Service | FEB 11, 2014 12:25 PM PST

Attackers abused insecure Network Time Protocol servers to launch what appears to be one of the largest DDoS (distributed denial-of-service) attacks ever reported, this time against the infrastructure of CloudFlare, a company that operates a global content delivery network.

The attack was revealed Monday on Twitter by Matthew Prince, CloudFlare's CEO, who said that it's "the start of ugly things to come" because "someone's got a big, new cannon."

The size of the attack appears to have been just shy of 400Gbps, ranking it among the largest DDoS attacks CloudFlare has seen, Prince said Tuesday via email, adding that the company is still gathering data about the incident from upstream providers.

NTP e segurança



CVE Details
The ultimate security vulnerability datasource

Search
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) View CVE

Log In Register

Vulnerability Feeds & Widgets New www.itsecdb.com

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE : Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
View BID : Go
(e.g.: 12345)
Search By Microsoft Reference ID: Go
(e.g.: ms10-001 or 979352)

NTP : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : 92 Page : 1 (This Page) 2

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2020-15025	401		DoS	2020-06-24	2021-01-20	4.0	None	Remote	Low	???	None	None	Partial
	ntpd in ntp 4.2.8 before 4.2.8p15 and 4.3.x before 4.3.101 allows remote attackers to cause a denial of service (memory consumption) by sending packets, because memory is not freed in situations where a CMAC key is used and associated with a CMAC algorithm in the ntp.keys file.													
2	CVE-2020-13817	20		DoS	2020-06-04	2021-07-21	5.8	None	Remote	Medium	Not required	None	Partial	Partial
	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows remote attackers to cause a denial of service (daemon exit or system time change) by predicting transmit timestamps for use in spoofed packets. The victim must be relying on unauthenticated IPv4 time sources. There must be an off-path attacker who can query time from the victim's ntpd instance.													
3	CVE-2020-11868	400			2020-04-17	2021-07-21	5.0	None	Remote	Low	Not required	None	None	Partial
	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address, because transmissions are rescheduled even when a packet lacks a valid origin timestamp.													
4	CVE-2019-11331				2019-04-18	2020-08-24	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
	Network Time Protocol (NTP), as specified in RFC 5905, uses port 123 even for modes where a fixed port number is not required, which makes it easier for remote attackers to conduct off-path attacks.													
5	CVE-2019-8936	476			2019-05-15	2020-10-07	5.0	None	Remote	Low	Not required	None	None	Partial
	NTP through 4.2.8p12 has a NULL Pointer Dereference.													
6	CVE-2018-12327	787		Exec Code Overflow	2018-06-20	2020-08-24	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	Stack-based buffer overflow in ntpq and ntpdc of NTP version 4.2.8p11 allows an attacker to achieve code execution or escalate to higher privileges via a long string as the argument for an IPv4 or IPv6 command-line parameter. NOTE: It is unclear whether there are any common situations in which ntpq or ntpdc is used with a command line from an untrusted source.													
7	CVE-2018-8956	20			2020-05-06	2020-07-19	5.0	None	Remote	Low	Not required	None	None	Partial
	ntpd in ntp 4.2.8p10, 4.2.8p11, 4.2.8p12 and 4.2.8p13 allow remote attackers to prevent a broadcast client from synchronizing its clock with a broadcast NTP server via soofed mode 3 and mode 5 packets. The attacker must either be a part of the same broadcast network or control a slave in that broadcast network that can capture certain required packets on the attacker's behalf and send them to the attacker.													
8	CVE-2018-7185			DoS	2018-03-06	2020-08-24	5.0	None	Remote	Low	Not required	None	None	Partial
	The protocol engine in ntp 4.2.6 before 4.2.8p11 allows a remote attackers to cause a denial of service (disruption) by continually sending a packet with a zero-origin timestamp and source IP address of the "other side" of an interleaved association causing the victim ntpd to reset its association.													
9	CVE-2018-7184			DoS	2018-03-06	2020-08-24	5.0	None	Remote	Low	Not required	None	None	Partial
	ntpd in ntp 4.2.8p4 before 4.2.8p11 drops bad packets before updating the "received" timestamp, which allows remote attackers to cause a denial of service (disruption) by sending a packet with a zero-origin timestamp causing the association to reset and setting the contents of the packet as the most recent timestamp. This issue is a result of an incomplete fix for CVE-2015-7704.													
10	CVE-2018-7183	787		Exec Code Overflow	2018-03-08	2021-07-20	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	Buffer overflow in the decodearr function in ntpq in ntp 4.2.8p6 through 4.2.8p10 allows remote attackers to execute arbitrary code by leveraging an ntpq query and sending a response with a crafted array.													
11	CVE-2018-7182	125		DoS	2018-03-06	2019-10-31	5.0	None	Remote	Low	Not required	None	None	Partial
	The ctl_getitem method in ntpd in ntp-4.2.8p6 before 4.2.8p11 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mode 6 packet with a ntpd instance from 4.2.8p6 through 4.2.8p10.													
12	CVE-2018-7170				2018-03-06	2020-06-18	3.5	None	Remote	Medium	???	None	Partial	None
	ntpd in ntp 4.2.x before 4.2.8p7 and 4.3.x before 4.3.92 allows authenticated users that know the private symmetric key to create arbitrarily-many ephemeral associations in order to win the clock selection of ntpd and modify a victim's clock via a Sybil attack. This issue exists because of an incomplete fix for CVE-2016-1549.													
13	CVE-2017-6464	20		DoS	2017-03-27	2018-04-12	4.0	None	Remote	Low	???	None	None	Partial

NTP e segurança

- Falhas no software ou na configuração
  - o ntpd é um dinossauro, gigante, com suporte a uma miríade de hardwares e sistemas, as opções padrão não são as mais seguras
- Falhas no protocolo
- Falta de mecanismos adequados de segurança

Certificados TLS

- O TLS é usado para estabelecer conexões seguras e autenticadas na Internet
  - Se um ataque NTP conseguir fazer um cliente voltar no tempo, ele pode aceitar certificados fraudados. Por exemplo certificados emitidos antes de 2014 com a falha do heartbleed.

DNSSEC

- O DNSSEC provê autenticação para o sistema de nomes.
  - Se um resolver está configurado pra fazer “strict validation”, ou seja, não responde se as queries falham a validação do DNSSEC, então um ataque NTP que leva o resolver para frente no tempo pode fazer com que todos os certificados e chaves expirem. Um ataque NTP que leve para o passado pode permitir ataques de repetição.

Cache-flushing

- Muitos sistemas se baseiam em algum tipo de cache para minimizar a carga de processamento ou da rede. O DNS, por exemplo.
  - Um ataque NTP que leve o relógio do DNS para trás 24h fará com que a maior parte das entradas de cache expire. Se isso ocorrer de forma massiva, pode inundar a rede de requisições DNS.

Roteamento na Internet

- O RPKI é um infraestrutura para a segurança do BGP, usando ROAs para autenticar a alocação de endereços IP e ASN.
  - Um ataque NTP pode levar um validador de RPKI para frente no tempo, fazendo com que apague o cache do arquivo de manifesto. Depois voltar o validador no tempo, fazendo com que aceite um arquivo de manifesto antigo como válido.

Bitcoin

- Bitcoin é uma moeda digital que permite que uma rede descentralizada chegue a um consenso sobre a validade de uma cadeia pública de transações, a “blockchain”.
  - Um ataque NTP pode levar a vítima a rejeitar transações válidas, ou a gastar poder computacional processando transações antigas.

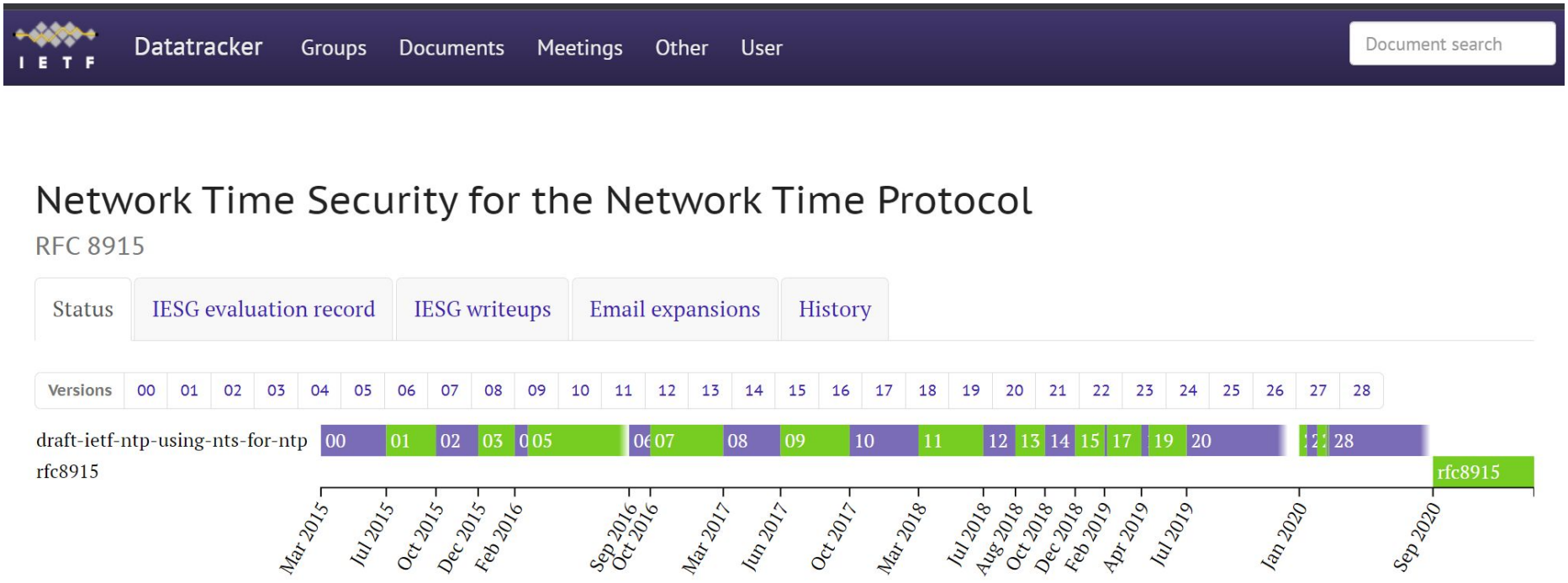
Serviços de autenticação

- Muitos serviços, como o Amazon S3, o DropBox Core API, e outros, expõem APIs que requerem autenticação a cada nova requisição. Normalmente exigem registros de tempo como forma de evitar ataques de repetição.
  - Com o ataque NTP a um servidor de aplicação pode-se fazer uma negação de serviço ou ataques de repetição.

Parte 5:

NTS: a nova extensão de segurança do NTP

NTS: a nova extensão de segurança do NTP



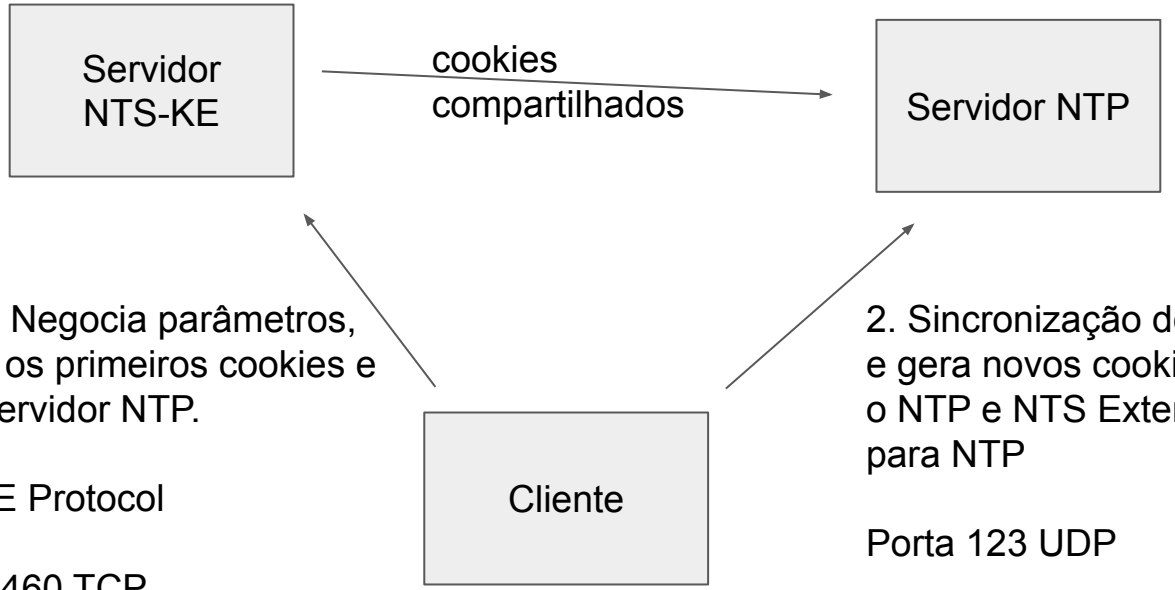
NTS: a nova extensão de segurança do NTP

- O que é:
  - É um mecanismo para usar TLS para prover segurança criptográfica para o NTP no modo cliente/servidor.
- Dois componentes:
  - NTS-KE - Network Time Security Key Establishment
  - NTS Extension fields para o NTPv4

NTS: a nova extensão de segurança do NTP

- **Identidade**: usa a estrutura de chaves públicas X.509
- **Autenticação**: verifica criptograficamente que a informação de relógio nos pacotes NTP é autêntica, produzida por um servidor identificável.
- **Proteção contra ataques de repetição**: o cliente pode detectar
- **Consistência entre requisições e respostas**: o cliente pode verificar
- **Privacidade**: NTS não vaza nenhuma informação que permitiria a um terceiro determinar que dois pacotes vindos de redes diferentes se originaram no mesmo cliente
- **Não amplificação**: as respostas nunca são maiores do que as requisições
- **Escalabilidade**: os servidores não guardam estado dos clientes, então podem servir a um grande número
- **Desempenho**: o NTS não degrada a qualidade da sincronização dos relógios

NTS: a nova extensão de segurança do NTP



1. TLS. Negocia parâmetros, recebe os primeiros cookies e IP do servidor NTP.

NTS-KE Protocol

Porta 4460 TCP

2. Sincronização dos relógios e gera novos cookies usando o NTP e NTS Extension Fields para NTP

Porta 123 UDP

NTS: a nova extensão de segurança do NTP

- **NTS-KE**
  - o cliente conecta na porta TCP 4460
  - cliente e servidor executam um handshake TLS
  - negociam alguns parâmetros de segurança extra
  - o servidor envia ao cliente alguns cookies, além do endereço IP e porta do servidor NTP para o qual os cookies são válidos
  - nessa altura a fase NTS-KE do protocolo acabou, idealmente o cliente nunca mais precisa se conectar no servidor NTS-KE

NTS: a nova extensão de segurança do NTP

- **Sincronização com NTP e NTS**
  - o cliente envia ao servidor um pacote com vários campos de extensão, entre eles um cookie (dos que recebeu do servidor NTS-KE) e uma tag de autenticação
  - o servidor usa o cookie para recuperar a chave e envia uma resposta autenticada
  - a resposta inclui um cookie novo, criptografado
  - na próxima requisição o cliente enviará esse cookie, sem criptografia
  - essa constante renovação dos cookies garante a privacidade

Parte 6:

O NTP.br e o NTS

O NTP.br e o NTS

- Estamos em fase de implementação e testes do NTS no NTP.br. Atualmente os servidores stratum 1 funcionam com NTS, em caráter experimental.
  - isso quer dizer que em caso de encontrar problemas sérios, podemos deixar de oferecer NTS até conseguir tratá-los
- {a, b, c, d, gps}.ntp.br
- Não temos documentação sobre NTS no site ainda.

Parte 7:

Como utilizar o NTP na prática: topologias e softwares sugeridos

Softwares para NTP e NTS

- NTPsec (ntpsec.org)
  - fork do NTPD (implementação de referência) feito em 2015
  - de 239 mil linhas de código, foram eliminadas 173 mil
  - hardening e modernização do código
  - ativamente mantido por um time experiente
  - NTS
- Chrony (chrony.tuxfamily.org)
  - implementação mais recente e moderna, de excelente qualidade
  - NTS
- OpenNTPd (openntpd.org)
  - implementação minimalista com foco em segurança
  - não implementa NTS (ainda?)

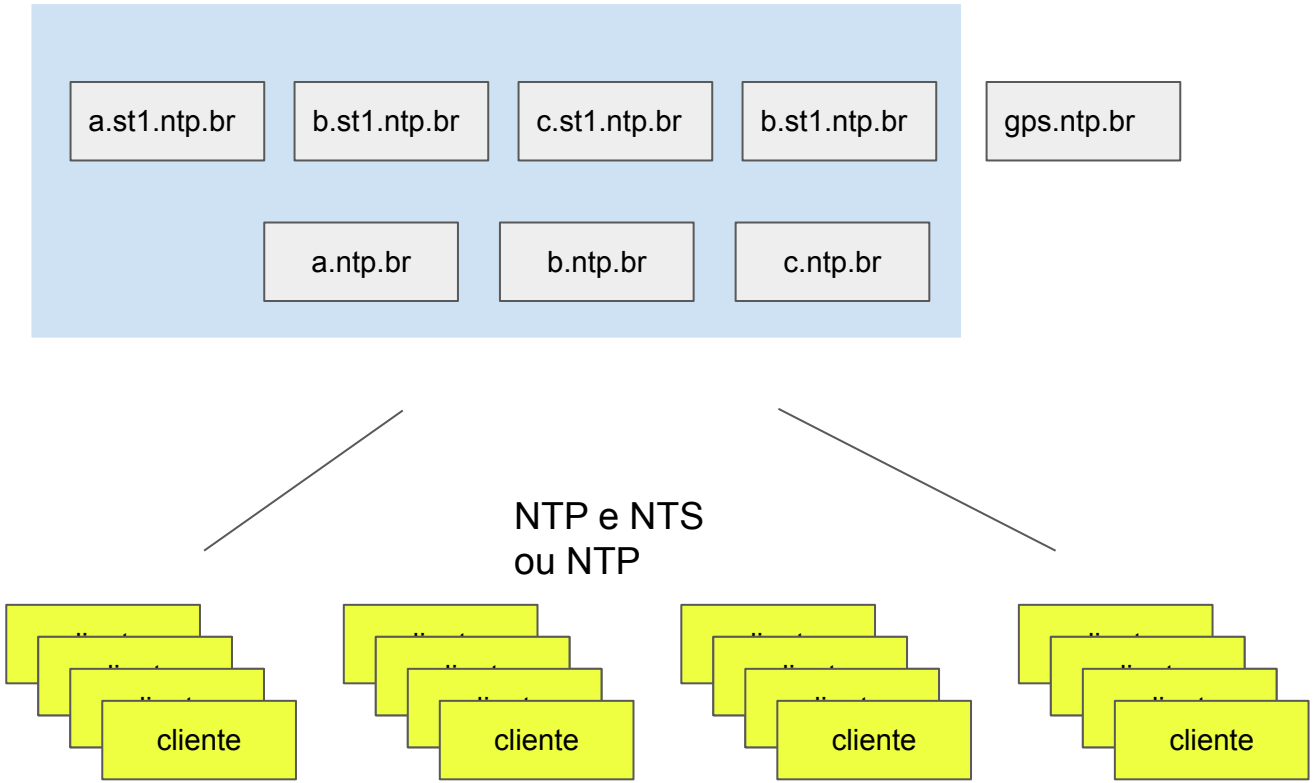
Softwares para NTP e NTS

- NTPd (ntp.org)
  - implementação de referência
  - RECOMENDAMOS NÃO USAR

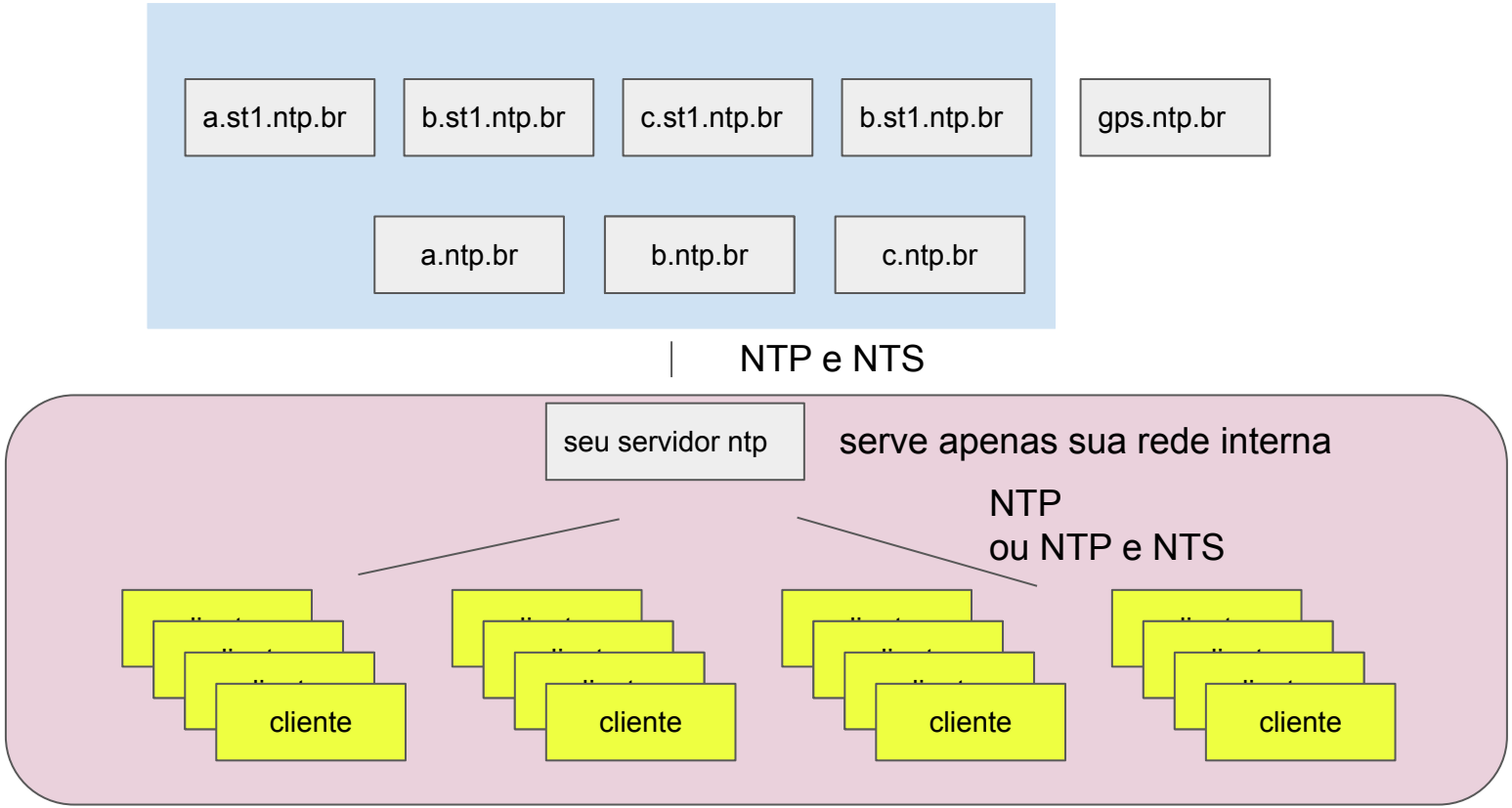
Softwares para NTP e NTS

- Windows / Mac / equipamentos de rede
  - não usar como servidores
    - se não puder desabilitar a função servidor, bloquear no firewall do dispositivo
  - usar o cliente nativo
  - provavelmente não haverá opção de suporte a NTS por um bom tempo ainda

Topologia


a.st1.ntp.br
b.st1.ntp.br
c.st1.ntp.br
b.st1.ntp.br
gps.ntp.br
a.ntp.br
b.ntp.br
c.ntp.br
NTP e NTS
ou NTP
cliente
cliente
cliente
cliente

Topologia


a.st1.ntp.br
b.st1.ntp.br
c.st1.ntp.br
b.st1.ntp.br
gps.ntp.br
a.ntp.br
b.ntp.br
c.ntp.br
NTP e NTS
seu servidor ntp
serve apenas sua rede interna
NTP
ou NTP e NTS
cliente
cliente
cliente
cliente

Parte 8:

Cliente NTP com ntpsec usando NTS

#apt-get install ntpsec

substituir as diretivas poll do arquivo de configuração em /etc/ntpsec/ntp.conf por:

```
server a.st1.ntp.br iburst nts
server b.st1.ntp.br iburst nts
server c.st1.ntp.br iburst nts
server d.st1.ntp.br iburst nts
```

reiniciar o serviço
#/etc/init.d/ntpsec restart

verificar o funcionamento e a sincronização
#ntpq -p

```
root@debian:/home/moreiras# ntpq -p
     remote                                refid      st t when poll reach   delay   offset   jitter
==============================================================================
+a.st1.ntp.br                            .ONBR.           1 8    2   64    3  12.6769  -0.6477   1.7892
 b.st1.ntp.br                            .NTS.           16 u    -  68m    0   0.0000   0.0000   0.0001
+c.st1.ntp.br                            .ONBR.           1 8   52   64    1  29.4421   3.8805   5.2145
*d.st1.ntp.br                            .ONBR.           1 8   53   64    1  20.9121  -1.4399   2.0345
```

Parte 9:

Cliente NTP com chrony usando NTS

#apt-get install chrony

substituir a diretiva poll do arquivo de configuração em /etc/chrony/chrony.conf por:

server a.st1.ntp.br iburst nts
server b.st1.ntp.br iburst nts
server c.st1.ntp.br iburst nts
server d.st1.ntp.br iburst nts

reiniciar o serviço
#/etc/init.d/chrony restart

verificar
o funcionamento
e a
sincronização

```
root@debian:/home/moreiras# chronyc sources
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^- a.st1.ntp.br                  1   6    17     1  -1755us[-1755us] +/- 7860us
^? b.st1.ntp.br                  0   7     0     -     +0ns[   +0ns] +/-    0ns
^- c.st1.ntp.br                  1   6    17     1  -3994us[-3994us] +/-   14ms
^* d.st1.ntp.br                  1   6    17     1  +4990us[+4962us] +/-   16ms
root@debian:/home/moreiras# chronyc tracking
Reference ID    : C814BA4C (d.st1.ntp.br)
Stratum         : 2
Ref time (UTC)  : Wed Sep 29 06:38:07 2021
System time     : 0.000026991 seconds slow of NTP time
Last offset     : -0.000027520 seconds
RMS offset      : 0.000027520 seconds
Frequency       : 2.720 ppm slow
Residual freq   : +327.395 ppm
Skew            : 1000000.000 ppm
Root delay      : 0.032182854 seconds
Root dispersion : 11.995963097 seconds
Update interval : 1.4 seconds
Leap status     : Normal
```

verificar o funcionamento e a sincronização

```
root@debian:/home/moreiras# chronyc -N authdata
Name/IP address             Mode KeyID Type KLen Last Atmp  NAK Cook CLen
==============================================================================
a.st1.ntp.br                 NTS     1   15  256  33m    0    0    8  104
b.st1.ntp.br                 NTS     0    0    0    -     3    0    0    0
c.st1.ntp.br                 NTS     1   15  256  33m    0    0    8  100
d.st1.ntp.br                 NTS     1   15  256  33m    0    0    8  100
```

Parte 10:

Servidor NTP para sua rede com ntpsec usando NTS

Instalação do Certbot (Letsencrypt)

```
apt install ca-certificates certbot
certbot register --agree-tos --email seu-email@seudominio.com.br --no-eff-email
certbot certonly --standalone --preferred-chain "ISRG Root X1" --domain seu-servidor-ntp.com.br
cp -L -v /etc/letsencrypt/live/seu-servidor-ntp.com.br/fullchain.pem /etc/ntpsec/cert-chain.pem
cp -L -v /etc/letsencrypt/live/seu-servidor-ntp.com.br/privkey.pem /etc/ntpsec/key.pem
chown -R -v ntpsec: /etc/ntpsec
```

Firewall

```
ufw allow 123/udp comment 'NTP'
ufw allow 4460/tcp comment 'NTS-KE'
ufw allow 80/tcp comment 'HTTP'
```

Configuração do NTP e NTS

```
driftfile /var/lib/ntpsec/ntp.drift
leapfile /usr/share/zoneinfo/leap-seconds.list

nts cert /etc/ntpsec/cert-chain.pem
nts key /etc/ntpsec/key.pem
nts enable

statsdir /var/log/ntpsec/
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

tos maxclock 11
server a.st1.ntp.br minpoll 4 maxpoll 6 nts
server b.st1.ntp.br minpoll 4 maxpoll 6 nts
server c.st1.ntp.br minpoll 4 maxpoll 6 nts
server d.st1.ntp.br minpoll 4 maxpoll 6 nts

restrict 1.1.0.0/20 kod limited nomodify noquery  #(sua rede)
restrict 2001:0db8::/32 kod limited nomodify noquery  #(sua rede)

restrict 127.0.0.1
restrict ::1
```

Parte 11:

Servidor NTP para sua rede com chrony usando NTS

Instalação do Certbot (Letsencrypt)

```
apt install ca-certificates certbot
certbot register --agree-tos --email seu-email@seudominio.com.br --no-eff-email
certbot certonly --standalone --preferred-chain "ISRG Root X1" --domain seu-servidor-ntp.com.br
cp -L -v /etc/letsencrypt/live/seu-servidor-ntp.com.br/fullchain.pem /etc/chrony/cert-chain.pem
cp -L -v /etc/letsencrypt/live/seu-servidor-ntp.com.br/privkey.pem /etc/chrony/key.pem
chown -R -v chrony: /etc/chrony
```

Firewall

```
ufw allow 123/udp comment 'NTP'
ufw allow 4460/tcp comment 'NTS-KE'
ufw allow 80/tcp comment 'HTTP'
```

Configuração do NTP e NTS

```
allow 2001:db8::/32
allow 6.7.8.9/22 #sua rede
driftfile /var/lib/chrony/chrony.drift
keyfile /etc/chrony/chrony.keys
leapsectz right/UTC
log measurements statistics tracking rtc refclocks tempcomp
logdir /var/log/chrony
makestep 1 3
maxntsconnections 1024
maxupdateskew 100.0
ntsdumpdir /var/lib/chrony
ntsprocesses 4
ntsservercert /etc/chrony/cert-chain.pem
ntsserverkey /etc/chrony/key.pem
rtcsync
server a.st1.ntp.br iburst nts
server b.st1.ntp.br iburst nts
server c.st1.ntp.br iburst nts
server d.st1.ntp.br iburst nts
```

Antonio M. Moreiras
moreiras@nic.br
@moreiras na maior parte das redes sociais
https://www.linkedin.com/in/moreiras/