

SERVIDOR NTP: O QUE É, COMO FUNCIONA E SINCRONISMO EM REDES E SUBESTAÇÕES

Entenda o que é servidor NTP, stratum, fontes, holdover, NTP versus PTP, sincronismo em SCADA, subestações, CFTV, segurança, projeto e testes.

SUMÁRIO

1. O QUE É NTP	3
2. POR QUE O SINCRONISMO É IMPORTANTE	3
3. COMO FUNCIONA A SINCRONIZAÇÃO NTP	3
4. UTC, FUSO HORÁRIO E HORÁRIO LOCAL	4
5. O QUE SÃO STRATUM 0, 1, 2 E 3	4
6. SERVIDOR NTP INTERNO	4
7. ARQUITETURA DE REFERÊNCIA	4
8. FONTES PRINCIPAL E ALTERNATIVA	5
9. HOLDOVER	5
10. NTP, SNTP, PTP E IRIG-B	5
11. NTP E PTP EM SUBESTAÇÕES	5
12. SINCRONISMO EM SCADA E SEQUENCIAMENTO DE EVENTOS	6
13. NTP EM CFTV E CONTROLE DE ACESSO	6
14. NTP E CIBERSEGURANÇA	6
15. NTS E AUTENTICAÇÃO	6
16. PORTAS E FIREWALL	7
17. MONITORAMENTO DO SERVIÇO DE TEMPO	7
18. PROJETO E DOCUMENTAÇÃO	7
19. TESTES E COMISSIONAMENTO	7
20. ERROS COMUNS	7
20.1. APONTAR TODOS OS ATIVOS PARA A INTERNET	7
20.2. UTILIZAR UMA ÚNICA FONTE	7
20.3. CONFUNDIR STRATUM COM PRECISÃO GARANTIDA	7
20.4. IGNORAR FUSO HORÁRIO	7
20.5. NÃO MONITORAR HOLDOVER	8
20.6. MISTURAR NTP E PTP SEM ARQUITETURA	8
20.7. NÃO TESTAR PERDA DE SINCRONISMO	8
21. CONCLUSÃO	8

Um **servidor NTP** distribui referência de tempo para computadores, servidores, equipamentos de rede, sistemas de segurança, dispositivos industriais e plataformas de automação. O protocolo NTP – Network Time Protocol – permite que os relógios internos sejam ajustados em relação a fontes confiáveis, mantendo eventos, registros e operações com horários coerentes.

Em ambientes corporativos, o sincronismo facilita autenticação, logs, certificados, bancos de dados e investigação de incidentes. Em subestações e centros de operação, a referência temporal também sustenta sequenciamento de eventos, análise de ocorrências, SCADA, relés, IEDs, teleproteção, vídeo operativo e correlação entre sistemas.

Configurar todos os equipamentos para consultar um servidor público não constitui uma arquitetura adequada. O projeto precisa considerar fontes primárias e alternativas, estratos, redundância, holdover, segurança, redes, protocolos compatíveis e comportamento durante perda da referência externa.

1. O QUE É NTP

NTP é um protocolo utilizado para sincronizar relógios em redes IP. Clientes consultam servidores de tempo, estimam atraso e diferença de relógio e ajustam gradualmente seu horário.

O protocolo trabalha com uma hierarquia de fontes. Servidores próximos a uma referência primária distribuem tempo para outros servidores e clientes.

O NTP não cria o tempo. Ele transporta e compara referências provenientes de fontes como:

2. POR QUE O SINCRONISMO É IMPORTANTE

Relógios divergentes dificultam a análise de eventos. Um login pode parecer ocorrer depois de uma alteração, uma câmera pode registrar horário diferente do controle de acesso e um relé pode apresentar sequência incompatível com o SCADA.

O sincronismo é necessário para:

3. COMO FUNCIONA A SINCRONIZAÇÃO NTP

O cliente troca mensagens com o servidor e registra quatro instantes: envio da solicitação, recebimento pelo servidor, envio da resposta e recebimento pelo cliente.

Com essas informações, estima:

O relógio pode ser ajustado gradualmente, evitando saltos que prejudiquem aplicações. Em situações específicas, pode ocorrer correção imediata, mas isso precisa ser controlado.

4. UTC, FUSO HORÁRIO E HORÁRIO LOCAL

Sistemas devem armazenar e trocar tempo de forma coerente, normalmente com base em UTC. A apresentação ao usuário pode aplicar fuso horário.

Misturar horário local no protocolo ou configurar fusos diferentes entre equipamentos causa ambiguidades. A arquitetura deve definir:

5. O QUE SÃO STRATUM 0, 1, 2 E 3

O conceito de **stratum** representa a distância lógica da referência primária.

EstratoDescriçãoStratum 0fonte de referência, como GNSS ou relógio atômicoStratum 1servidor diretamente conectado à referênciaStratum 2servidor sincronizado com um ou mais stratum 1Stratum 3servidor sincronizado com stratum 2

Um número menor não garante automaticamente melhor serviço. Qualidade depende de estabilidade, caminho, configuração, redundância e saúde da fonte.

6. SERVIDOR NTP INTERNO

Uma arquitetura corporativa deve preferir servidores internos que recebam tempo de fontes controladas e distribuam aos clientes.

Vantagens:

Clientes não precisam conhecer diretamente todas as fontes externas.

7. ARQUITETURA DE REFERÊNCIA

Uma arquitetura possível:

GNSS / fonte oficial / upstream autorizado Servidores NTP principais e alternativos
Servidores intermediários por site ou zona Clientes: servidores, switches, SCADA, VMS e endpoints

Em ambientes OT, podem existir servidores por subestação, centro de operação ou domínio de segurança.

8. FONTES PRINCIPAL E ALTERNATIVA

Utilizar uma única fonte cria ponto único de falha. O cliente deve consultar fontes coerentes e independentes conforme a arquitetura.

O projeto deve analisar:

Fontes conflitantes podem produzir decisões incorretas. A quantidade deve ser acompanhada de política de seleção e monitoramento.

9. HOLDOVER

Holdover é a capacidade de manter uma referência aceitável durante a perda temporária da fonte externa.

A qualidade depende do oscilador interno, temperatura, calibração e tempo desde a última sincronização. Appliances podem utilizar osciladores de maior estabilidade para reduzir deriva.

O requisito deve definir:

10. NTP, SNTP, PTP E IRIG-B

Tecnologia Característica NTP sincronismo em redes IP, adequado a muitas aplicações corporativas e operacionais SNTP implementação simplificada, com menos mecanismos de seleção e disciplina PTP sincronismo de maior precisão em redes compatíveis, com relógios e switches apropriados IRIG-B distribuição temporal por sinal dedicado, comum em sistemas elétricos GNSS fonte externa baseada em satélites

A escolha depende da precisão e da arquitetura. NTP pode ser suficiente para logs e sistemas corporativos, enquanto certas funções de proteção, medição ou barramento de processo podem exigir PTP ou sinais dedicados.

11. NTP E PTP EM SUBESTAÇÕES

Subestações podem utilizar mais de um mecanismo:

O projeto precisa evitar ilhas temporais incompatíveis. Todos os eventos utilizados em análise conjunta devem possuir referência documentada.

12. SINCRONISMO EM SCADA E SEQUENCIAMENTO DE EVENTOS

O SCADA recebe estados, alarmes, telemedidas e eventos de diferentes dispositivos. Para reconstruir uma ocorrência, os timestamps precisam ser confiáveis.

O sequenciamento de eventos pode exigir precisão superior à simples apresentação de horário na tela. A fonte de timestamp pode estar no IED, na UTR, no SSCL ou no servidor, conforme arquitetura.

O projeto deve definir:

13. NTP EM CFTV E CONTROLE DE ACESSO

Câmeras, VMS, gravadores e controladoras precisam compartilhar referência temporal. Divergências prejudicam a correlação entre vídeo, acesso, intrusão e eventos operacionais.

O sistema deve evitar que cada câmera consulte servidores públicos diferentes. O ideal é utilizar fontes internas, monitoradas e redundantes.

A exportação de evidências deve preservar timestamp, fuso e metadados suficientes para interpretação.

14. NTP E CIBERSEGURANÇA

O tempo afeta autenticação, certificados, logs e investigação. Uma alteração indevida pode:

Controles recomendados:

15. NTS E AUTENTICAÇÃO

Network Time Security – NTS – adiciona mecanismos modernos de autenticação e proteção ao NTP. O suporte ainda depende dos clientes, servidores e sistemas operacionais.

Em ambientes legados, podem ser necessárias medidas compensatórias, como segmentação, listas de controle, fontes internas e monitoração de anomalias.

A autenticação não elimina a necessidade de redundância e qualidade da referência.

16. PORTAS E FIREWALL

NTP utiliza normalmente UDP 123. Regras devem limitar:

Servidores não devem oferecer serviços desnecessários nem responder indiscriminadamente a redes externas.

17. MONITORAMENTO DO SERVIÇO DE TEMPO

Indicadores úteis:

Alarmes precisam ser encaminhados antes que o erro temporal ultrapasse o limite da aplicação.

18. PROJETO E DOCUMENTAÇÃO

Um projeto de sincronismo pode produzir:

19. TESTES E COMISSIONAMENTO

Os testes devem verificar:

20. ERROS COMUNS

20.1. APONTAR TODOS OS ATIVOS PARA A INTERNET

Isso aumenta dependência, exposição e inconsistência.

20.2. UTILIZAR UMA ÚNICA FONTE

A perda do servidor ou GNSS elimina a referência.

20.3. CONFUNDIR STRATUM COM PRECISÃO GARANTIDA

Estrato representa distância lógica, não qualidade absoluta.

20.4. IGNORAR FUSO HORÁRIO

Equipamentos podem registrar o mesmo evento com horários aparentemente diferentes.

20.5. NÃO MONITORAR HOLDOVER

O servidor pode continuar respondendo enquanto o erro aumenta.

20.6. MISTURAR NTP E PTP SEM ARQUITETURA

Diferentes referências podem produzir eventos incompatíveis.

20.7. NÃO TESTAR PERDA DE SINCRONISMO

A operação degradada precisa ser conhecida e sinalizada.

21. CONCLUSÃO

Servidor NTP é um componente de infraestrutura crítica para registros, autenticação e análise de eventos. Em subestações, sua função se conecta a SCADA, relés, telecomunicações, vídeo e centros de operação.

Uma arquitetura confiável utiliza fontes controladas, redundância, holdover, segmentação, monitoramento e testes. O objetivo não é apenas mostrar a hora correta, mas garantir que sistemas diferentes possam ser correlacionados com confiança.

[1] IETF. RFC 5905 — Network Time Protocol Version 4: Protocol and Algorithms Specification.

[2] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR 16932:2020 — Redes e sistemas de comunicação para automação de sistemas de potência — Orientações sobre engenharia de rede.

[3] OPERADOR NACIONAL DO SISTEMA ELÉTRICO. Procedimentos de Rede — Submódulo 2.12: Requisitos mínimos de supervisão e controle para a operação.

[4] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-82 Rev. 3 — Guide to Operational Technology Security.

O que é um servidor NTP? É um servidor que fornece referência de tempo pela rede para clientes como computadores, switches, servidores, câmeras e sistemas de automação.

O que significa stratum no NTP? Stratum indica a distância lógica da fonte primária.

Stratum 1 conecta-se diretamente à referência e stratum 2 sincroniza-se com stratum

1. NTP e PTP são a mesma coisa? Não. NTP atende muitas aplicações de rede, enquanto PTP é utilizado quando se exige maior precisão e a infraestrutura é compatível.

É seguro usar servidor NTP público? Servidores públicos podem ser usados como upstream

autorizado, mas clientes internos devem preferir servidores controlados e regras de acesso definidas. **O que é holdover?** É a capacidade de manter referência temporal durante a perda temporária da fonte externa, usando o oscilador local. **Por que NTP é importante para SCADA?** Porque permite correlacionar estados, alarmes, eventos e comandos de diferentes dispositivos e centros de operação. **Câmeras precisam de NTP?** Sim. Câmeras, VMS e controle de acesso devem compartilhar referência temporal para que eventos e evidências possam ser correlacionados. **Qual porta o NTP utiliza?** Normalmente UDP 123. As regras devem restringir origens e destinos autorizados. **O que é NTS?** Network Time Security é um mecanismo moderno para autenticar e proteger a sincronização NTP, quando suportado pelos sistemas. **Como testar um sistema NTP?** Devem ser testados offset, fontes principal e alternativa, holdover, falhas, alarmes, clientes e correlação de eventos entre sistemas.

Soluções

Serviços de engenharia

Materiais técnicos complementares

Sobre a A3A Engenharia de Sistemas

Com 30 anos de história, a A3A Engenharia de Sistemas se consolidou como referência em serviços de Engenharia, oferecendo soluções integradas de Telecomunicações, Segurança Eletrônica, Segurança Digital e Instalações Elétricas.

A empresa atua em todas as etapas do ciclo de Engenharia, desde a elaboração de projetos e consultoria técnica até a implantação, manutenção e retrofit de sistemas, sempre em conformidade com as normas técnicas e melhores práticas do setor.