zurück

NTP – Network Time Protocol

NTP (**N**etwork **T**ime **P**rotocol) ist ein Protokoll, mit dem Geräte ihre Uhrzeit exakt und automatisch synchronisieren.
Genaue Zeit ist entscheidend für Sicherheit, Logs, Zertifikate und Netzwerkdienste.

Warum ist Zeit so wichtig in der IT?

- Log-Dateien müssen zeitlich übereinstimmen
- Zertifikate sind zeitabhängig (Gültigkeitsfenster)
- Kerberos-Authentifizierung scheitert bei >5 Minuten Abweichung
- Cluster und Datenbanken benötigen gleiche Zeit
- NAC-, Firewall- und IDS-Ereignisse müssen korrekt geordnet werden

Beispiel: Ein Server geht 7 Minuten falsch → Kerberos-Login schlägt fehl → Nutzer kann sich nicht anmelden.

Wie funktioniert NTP?

NTP arbeitet nach einem hierarchischen System aus Zeitservern, in sogenannten **Stratum-Ebenen**.

Stratum-Level

- **Stratum 0** – Zeitreferenz
  - Atomuhren
  - GPS-Empfänger
  - Funkuhren
- **Stratum 1** – direkt mit Stratum 0 verbunden
  - professionelle Zeitserver
  - sehr hohe Genauigkeit
- **Stratum 2** – synchronisieren sich mit Stratum 1
- **Stratum 3+** – weitere Ebenen nach unten

ASCII-Übersicht:

```
[Stratum 0] → [Stratum 1] → [Stratum 2] → [Stratum 3…]
 Atomuhren     Zeitserver    Unternehmensserver
```

Ports & Protokolle

- Port: **123/UDP**
- arbeitet auf Layer 7
- kleiner, schneller Austausch von Zeitstempeln

NTP vs SNTP

Protokoll	Bedeutung	Genauigkeit	Einsatz
———–	—————	————-	———
NTP	vollwertiges Protokoll	hoch	Server, Schlüsselsysteme
SNTP	vereinfachtes NTP	mittel	IoT-Geräte, Drucker

Zeitberechnung in NTP

NTP berechnet:

- Laufzeit der Pakete (Delay)
- Zeitunterschied zwischen Server & Client (Offset)
- Schwankungen (Jitter)

Damit kann sich ein Client millisekundengenau einstellen.

Öffentliche NTP-Server

Bekannte Pools:

```
pool.ntp.org
de.pool.ntp.org
europe.pool.ntp.org
```

Google Public NTP:

```
time.google.com
```

Deutsche Forschungsinstitute:

```
ptbtime1.ptb.de
ptbtime2.ptb.de
ptbtime3.ptb.de
```

NTP in Unternehmen

Empfohlene Struktur:

```
Internet-NTP  →  Unternehmens-NTP  →  alle Server  →  alle Clients
```

Warum nicht alle Clients nach außen?

- unnötige Last
- weniger Abhängigkeit
- Sicherheit

Konfiguration auf Linux

Chrony (modern)

Chrony ist heute Standard auf vielen Distributionen (z. B. Debian, RHEL, Ubuntu):

Konfigurationsdatei:

```
/etc/chrony/chrony.conf
```

Beispiel:

```
server de.pool.ntp.org iburst
server 0.pool.ntp.org iburst

allow 192.168.0.0/16
local stratum 10
```

Status prüfen:

```
chronyc sources -v
chronyc tracking
```

NTPD (älter)

```
ntpq -p
```

Konfiguration auf Windows

Aktuellen Zeitserver anzeigen:

```
w32tm /query /status
```

Setzen eines NTP-Servers:

```
w32tm /config /manualpeerlist:"time.windows.com" /syncfromflags:manual
/update
```

NTP-Sicherheit

Probleme:

- Manipulation der Zeit → gefährlich für Logins & Zertifikate
- Reflection-Angriffe (NTP Amplification)

Schutzmaßnahmen:

- nur vertrauenswürdige Server verwenden
- eingehende NTP-Pakete blockieren
- internen NTP-Server nutzen
- NTP-Rate-Limits aktivieren

Warum driftet Zeit überhaupt?

Uhren in Computern basieren auf Quarzen. Temperatur, Spannung und Alter lassen sie langsam vor-/nachgehen.

NTP korrigiert diese Abweichungen automatisch.

Prüfung der Zeitabweichung

Linux:

```
timedatectl
```

Windows:

```
w32tm /stripchart /computer:TIME.SERVER
```

Zusammenfassung

- NTP synchronisiert Uhrzeiten im Netzwerk
  - Stratum-Hierarchie: 0 → 1 → 2 usw.
    * Port 123/UDP
    * unverzichtbar für Sicherheit, Authentifizierung und Logs
    * Chrony ist moderner Standard
    * Unternehmen nutzen interne NTP-Server für Zuverlässigkeit