

4.12 Zeit-, Zeitzonen- und Synchronisationsfehler

Eine falsche Systemzeit kann Fehler verursachen, die zunächst wie Netzwerk-, Zertifikats-, Anmelde- oder Anwendungsprobleme wirken. Besonders in Active-Directory-Umgebungen, verteilten Systemen, Datenbanken, Clustern und virtualisierten Umgebungen ist eine zuverlässige Zeitsynchronisation entscheidend.

Typische Auswirkungen sind:

- Domänenanmeldungen schlagen fehl.
- Kerberos-Tickets werden abgelehnt.
- Zertifikate erscheinen noch nicht oder nicht mehr gültig.
- HTTPS- und TLS-Verbindungen schlagen fehl.
- Protokolle verschiedener Systeme lassen sich nicht zeitlich zuordnen.
- Datenbanken speichern Ereignisse in falscher Reihenfolge.
- Geplante Aufgaben starten zu früh, zu spät oder gar nicht.
- Sicherungen und Synchronisationsaufgaben verhalten sich unerwartet.
- Einmalpasswörter und zeitbasierte Multifaktor-Authentifizierung schlagen fehl.
- Cluster, Replikationen oder verteilte Anwendungen melden Inkonsistenzen.
- Dateien besitzen scheinbar zukünftige oder unlogische Zeitstempel.
- Nach einem Neustart springt die Uhrzeit erneut auf einen falschen Wert.

“ **Wichtig:** Datum, Uhrzeit, Zeitzone und Zeitsynchronisation sind unterschiedliche Prüfbereiche. Eine korrekt aussehende Uhrzeit bedeutet nicht automatisch, dass das System korrekt synchronisiert ist.

Kennzeichnung der Befehle

Kennzeichnung	Bedeutung
[RO]	Nur lesender Befehl
[TEST]	Führt eine aktive Prüfung aus
[PRIV]	Erhöhte Berechtigungen erforderlich
[SENS]	Ausgabe kann sensible Informationen enthalten
[CHANGE]	Verändert Konfiguration oder Systemzustand
[DISRUPT]	Kann laufende Dienste oder Anwendungen beeinflussen

1. Warum eine korrekte Systemzeit wichtig ist

Viele IT-Systeme verwenden Zeitstempel nicht nur zur Anzeige, sondern als Bestandteil ihrer Sicherheits- und Ablaufsteuerung.

System oder Funktion	Bedeutung der Systemzeit
Active Directory	Kerberos verwendet Zeitstempel zum Schutz vor wiederholten Anmeldeversuchen
TLS und Zertifikate	Gültigkeitsbeginn und Gültigkeitsende werden gegen die Systemzeit geprüft
Protokollierung	Ereignisse verschiedener Systeme müssen zeitlich vergleichbar sein
Datenbanken	Transaktionen, Replikation und Datensätze besitzen Zeitstempel
Sicherungen	Zeitpläne und inkrementelle Sicherungen hängen von Zeitinformationen ab
MFA und TOTP	Einmalpasswörter werden aus Zeitintervallen berechnet
E-Mail	Nachrichten und Signaturen enthalten Zeitstempel
Monitoring	Messwerte müssen in der richtigen Reihenfolge gespeichert werden
Cluster	Knoten müssen Ereignisse zeitlich konsistent bewerten
Dateisynchronisation	Änderungszeiten beeinflussen die Entscheidung, welche Datei neuer ist
Lizenzsysteme	Lizenzen können an Zeiträume gebunden sein
Aufgabenplanung	Startzeitpunkte hängen von lokaler Zeit und Zeitzone ab

Eine Zeitabweichung kann daher gleichzeitig mehrere scheinbar unabhängige Dienste beeinträchtigen.

2. Fehlerbild strukturiert aufnehmen

Zuerst muss festgestellt werden, welche Zeitinformation tatsächlich falsch ist.

Zu prüfende Fragen

- Sind Datum und Uhrzeit falsch?
- Ist nur die Zeitzone falsch?
- Beträgt die Abweichung genau eine oder mehrere volle Stunden?
- Wächst die Abweichung kontinuierlich?
- Springt die Zeit nach einem Neustart zurück?
- Ist nur eine virtuelle Maschine betroffen?
- Sind mehrere Geräte am gleichen Standort betroffen?

- Ist die UTC-Zeit korrekt, aber die lokale Anzeige falsch?
- Ist der eingetragene Zeitserver erreichbar?
- Wird die erwartete Zeitquelle tatsächlich verwendet?
- Trat das Problem nach einem Snapshot, einer Migration oder einem Standby auf?
- Ist das System Mitglied einer Active-Directory-Domäne?
- Verwaltet eine Gruppenrichtlinie oder Geräteverwaltung die Zeiteinstellungen?
- Wurde die Zeit manuell verändert?

Abweichungsmuster und erste Hinweise

Beobachtung	Mögliche Ursache
Abweichung um genau eine Stunde	Falsche Zeitzone oder Sommerzeitregel
Abweichung um mehrere volle Stunden	Falsche Zeitzone
Abweichung wächst langsam	Ungenauere lokale Uhr oder fehlende Synchronisation
Zeit springt nach einem Neustart zurück	Hardwareuhr, Firmware, Host oder leere CMOS-Batterie
Nur virtuelle Maschinen betroffen	Hypervisor-Zeitquelle oder Snapshot
Alle Domänenmitglieder betroffen	Fehler in der AD-Zeithierarchie
Nur ein Domänenmitglied betroffen	Lokaler Zeitdienst, Netzwerk oder Richtlinie
Uhrzeit stimmt, TLS schlägt trotzdem fehl	UTC, Datum und Zertifikatszeitraum kontrollieren
Protokolle wirken zeitversetzt	UTC- und Lokalzeitdarstellung vergleichen
Zeitserver ist per Ping erreichbar, Synchronisation scheitert	NTP, Firewall oder Serverantwort prüfen

“ Eine Abweichung um eine volle Stunde deutet meistens eher auf die Zeitzone als auf eine fehlerhafte NTP-Synchronisation hin.

3. Datum, Uhrzeit und Zeitzone vergleichen

Die Werte sollten möglichst gleichzeitig auf dem betroffenen System und einem vertrauenswürdigen Vergleichssystem erfasst werden.

Aufgabe	Windows	Linux	macOS
Lokale Zeit	<code>[RO] Get-Date -Format o</code>	<code>[RO] date --iso-8601=seconds</code>	<code>[RO] date "+%Y-%m-%dT%H:%M:%SZ"</code>
UTC-Zeit	<code>[RO] (Get-Date).ToUniversalTime().ToString("o")</code>	<code>[RO] date -u "+%Y-%m-%dT%H:%M:%SZ"</code>	<code>[RO] date -u "+%Y-%m-%dT%H:%M:%SZ"</code>

Aufgabe	Windows	Linux	macOS
Zeitzone	[RO] Get-TimeZone	[RO] timedatectl status	[RO][PRIV] sudo systemsetup -gettimezone
Zeitzonendatei	Nicht zutreffend	[RO] readlink -f /etc/localtime	Nicht zutreffend
Hardwareuhr	Nicht direkt erforderlich	[RO][PRIV] sudo hwclock --show	Nicht regulär erforderlich

Warum UTC und lokale Zeit getrennt geprüft werden

- UTC ist die gemeinsame Zeitbasis.
- Die lokale Zeit entsteht aus UTC, Zeitzone und Sommerzeitregel.
- Zwei Systeme können dieselbe UTC-Zeit, aber unterschiedliche lokale Zeiten anzeigen.
- Protokolle können entweder UTC oder lokale Zeit verwenden.
- Server werden häufig in UTC betrieben, während Benutzeroberflächen lokale Zeit anzeigen.

Beispiel

Wenn UTC korrekt ist, die lokale Zeit aber um eine Stunde abweicht, liegt die Ursache wahrscheinlich in der Zeitzone oder Sommerzeitregel und nicht in der eigentlichen Zeitsynchronisation.

4. Windows-Zeitdienst untersuchen

Windows verwendet den Dienst **W32Time** zur Zeitsynchronisation.

Status des Zeitdienstes prüfen

```
[RO] Get-Service -Name W32Time
```

Ausführlicher:

```
[RO] Get-CimInstance Win32_Service -Filter "Name='W32Time'" |
Select-Object Name, State, StartMode, StartName, ExitCode
```

Aktuelle Zeitquelle anzeigen

```
[RO] w32tm /query /source
```

Synchronisationsstatus anzeigen

```
[RO] w32tm /query /status
```

Ausführlichen Status anzeigen

```
[RO] w32tm /query /status /verbose
```

Konfiguration anzeigen

```
[RO][SENS] w32tm /query /configuration
```

Konfigurierte Zeitpartner anzeigen

```
[RO][SENS] w32tm /query /peers
```

Zeitzone anzeigen

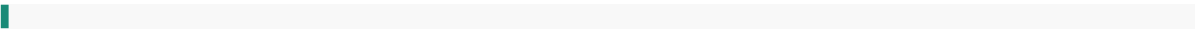
```
[RO] Get-TimeZone
```

oder:

```
[RO] tzutil /g
```

Mögliche Ausgaben bei der Zeitquelle

Ausgabe	Bedeutung
Name eines Domänencontrollers	Synchronisation über die AD-Zeithierarchie
Name eines NTP-Servers	Direkte Synchronisation mit diesem Server
Local CMOS Clock	Lokale Hardwareuhr wird verwendet
VM IC Time Synchronization Provider	Zeit wird über den Hypervisor bereitgestellt
Free-running System Clock	Keine geeignete externe Synchronisation



Local CMOS Clock oder **Free-running System Clock** ist bei einem normalen Domänenmitglied meist ein Hinweis darauf, dass die erwartete Domänenzeitquelle nicht verwendet wird. Bei isolierten Systemen kann die Bewertung anders ausfallen.

5. Windows-Zeitabweichung aktiv messen

Mit **w32tm /stripchart** kann die Abweichung zu einem Zeitserver gemessen werden, ohne die lokale Uhr zu verändern.

```
[TEST] w32tm /stripchart /computer:<ZEITSERVER> /samples:5 /dataonly
```

Beispiel:

```
[TEST] w32tm /stripchart /computer:dc01.example.local /samples:5 /dataonly
```

Fortlaufende Messung:

```
[TEST] w32tm /stripchart /computer:<ZEITSERVER> /dataonly
```

Die fortlaufende Ausgabe wird mit **Strg** + **C** beendet.

Wichtige Interpretation

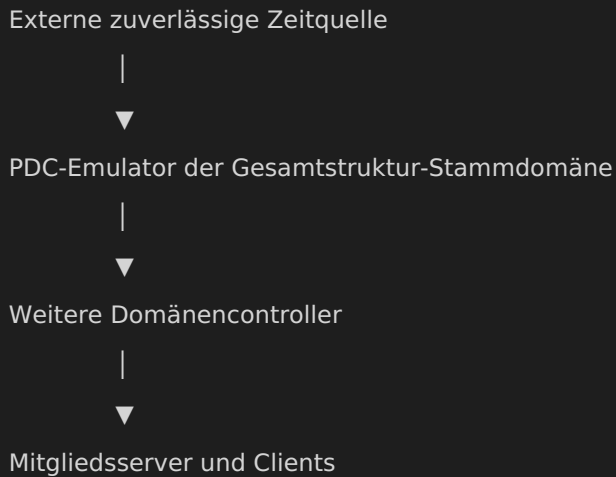
Ergebnis	Bedeutung
Kleine, stabile Abweichung	Synchronisation wahrscheinlich funktionsfähig
Große, stabile Abweichung	Falsche Quelle oder noch nicht korrigierte Uhr
Abweichung wächst	Lokale Uhr driftet oder wird nicht nachgeregelt
Keine Antwort	Name, Netzwerk, Firewall oder NTP-Dienst prüfen
Zeitüberschreitung	NTP-Antwort erreicht den Client nicht

“ Der Test bestätigt nicht automatisch, dass Windows diese Gegenstelle als aktive Zeitquelle verwendet. Die aktive Quelle muss zusätzlich mit **w32tm /query /source** geprüft werden.

6. Active-Directory-Zeithierarchie verstehen

Domänenmitglieder sollten grundsätzlich der Active-Directory-Zeithierarchie folgen.

Vereinfachter Aufbau:



PDC-Emulator ermitteln

```
[RO][SENS] netdom query fsmo
```

Alternativ mit PowerShell:

```
[RO][SENS] Get-ADDomain |  
Select-Object DNSRoot, PDCEmulator
```

Dafür muss das ActiveDirectory-PowerShell-Modul verfügbar sein.

Domänencontroller anzeigen

```
[RO][SENS] nltest /dclist:<DOMÄNE>
```

Verwendeten Domänencontroller anzeigen

```
[RO][SENS] nltest /dsgetdc:<DOMÄNE>
```

Zeitstatus eines entfernten Windows-Systems abfragen

```
[RO][SENS] w32tm /query /computer:<COMPUTER> /status
```

Dafür sind ausreichende Berechtigungen und eine erreichbare Remoteverwaltung erforderlich.

Wichtige Regeln

- Normale Domänenmitglieder sollten nicht unabhängig auf beliebige öffentliche NTP-Server zeigen.
- Der PDC-Emulator der Stammdomäne benötigt eine zuverlässige übergeordnete Zeitquelle.
- Gruppenrichtlinien können lokale Einstellungen überschreiben.
- Auf virtuellen Domänencontrollern dürfen Hypervisor- und Domänenzeitsynchronisation nicht unkontrolliert gegeneinander arbeiten.
- Eine manuelle Uhrzeitkorrektur behebt keine fehlerhafte Zeithierarchie.

7. Windows-Ereignisprotokolle auswerten

Zeitdienst-Ereignisse im Systemprotokoll anzeigen

```
[RO][SENS] Get-WinEvent -FilterHashtable @{  
    LogName      = 'System'  
    ProviderName = 'Microsoft-Windows-Time-Service'  
    StartTime    = (Get-Date).AddHours(-24)  
} |  
Select-Object TimeCreated, LevelDisplayName, Id, Message
```

Operational-Protokoll des Zeitdienstes prüfen

```
[RO][SENS] Get-WinEvent -LogName `  
    'Microsoft-Windows-Time-Service/Operational' `  
    -ErrorAction SilentlyContinue |  
Select-Object -First 100 TimeCreated, LevelDisplayName, Id, Message
```

Dienststatus und letzte Meldungen gemeinsam bewerten

```
[RO] Get-Service W32Time
```

```
[RO] w32tm /query /source
```

```
[RO] w32tm /query /status
```

Typische Hinweise in Ereignissen

- Keine Zeitdaten verfügbar
- Zeitquelle nicht erreichbar
- Zeitquelle wurde gewechselt
- Synchronisation wurde beendet
- Uhrzeitabweichung ist zu groß
- Zeitdienst wurde gestartet oder beendet
- NTP-Anbieter konnte keine gültigen Daten abrufen

“ Einzelne ältere Warnungen beweisen keine aktuelle Störung. Zeitstempel, Wiederholungsrate und aktueller Synchronisationsstatus müssen gemeinsam bewertet werden.

8. Linux mit systemd-timesyncd untersuchen

Viele Linux-Distributionen verwenden `systemd-timesyncd`. Andere Systeme verwenden stattdessen `chrony`, `ntpd` oder eine herstellerspezifische Lösung.

Gesamtstatus anzeigen

```
[RO] timedatectl status
```

Wichtige Felder:

Feld	Bedeutung
<code>Local time</code>	Lokale Uhrzeit
<code>Universal time</code>	UTC-Zeit
<code>RTC time</code>	Hardwareuhr
<code>Time zone</code>	Aktive Zeitzone
<code>System clock synchronized</code>	Synchronisationszustand

Feld	Bedeutung
NTP service	Status eines erkannten NTP-Dienstes
RTC in local TZ	Gibt an, ob die Hardwareuhr Lokalzeit verwendet

Status der Zeitsynchronisation anzeigen

```
[RO] timedatectl timesync-status
```

Alle verfügbaren Synchronisationsinformationen anzeigen

```
[RO] timedatectl show-timesync --all
```

Dienststatus prüfen

```
[RO] systemctl status systemd-timesyncd --no-pager
```

Protokolle anzeigen

```
[RO][PRIV][SENS] sudo journalctl -u systemd-timesyncd \
--since "-24 hours" --no-pager
```

Konfiguration anzeigen

```
[RO][FILE] systemd-analyze cat-config systemd/timesyncd.conf
```

“ `timedatectl timesync-status` und `show-timesync` funktionieren nur, wenn `systemd-timesyncd` verwendet und von der eingesetzten systemd-Version unterstützt wird. Bei chrony oder ntpd müssen deren eigene Werkzeuge verwendet werden.

9. Linux mit chrony untersuchen

Chrony wird häufig auf Linux-Servern, virtuellen Maschinen und Systemen mit unregelmäßiger Netzwerkverbindung verwendet.

Synchronisationsstatus anzeigen

```
[RO] chronyc tracking
```

Wichtige Werte:

Wert	Bedeutung
Reference ID	Aktuell verwendete Referenz
Stratum	Entfernung zur ursprünglichen Referenzuhr
Ref time	Zeitpunkt der letzten verwendeten Messung
System time	Abweichung der Systemuhr
Last offset	Zuletzt gemessene Abweichung
RMS offset	Langfristige Abweichung
Leap status	Synchronisations- beziehungsweise Schaltsekundenstatus

Zeitquellen anzeigen

```
[RO] chronyc sources -v
```

Messwerte der Quellen anzeigen

```
[RO] chronyc sourcestats -v
```

Chrony-Aktivität prüfen

```
[RO] chronyc activity
```

Dienststatus anzeigen

```
[RO] systemctl status chronyd --no-pager
```

Je nach Distribution kann der Dienst auch `chrony` heißen:

```
[RO] systemctl status chrony --no-pager
```

Protokolle anzeigen

```
[RO][PRIV][SENS] sudo journalctl -u chronyd \
--since "-24 hours" --no-pager
```

oder:

```
[RO][PRIV][SENS] sudo journalctl -u chrony \
--since "-24 hours" --no-pager
```

Kennzeichen in `chronyc sources -v`

Zeichen	Bedeutung
<code>^*</code>	Aktuell ausgewählte NTP-Quelle
<code>^+</code>	Geeignete zusätzliche Quelle
<code>^-</code>	Geeignete, aber nicht verwendete Quelle
<code>^?</code>	Quelle nicht erreichbar oder noch nicht ausreichend bewertet
<code>^x</code>	Quelle wird als fehlerhaft bewertet
<code>^~</code>	Quelle weist zu große Schwankungen auf

“ Ein erreichbarer Server ist nicht automatisch eine geeignete Zeitquelle. Chrony bewertet unter anderem Abweichung, Stabilität und Messqualität.

10. Linux mit klassischem ntpd untersuchen

Auf älteren oder speziell konfigurierten Systemen kann weiterhin `ntpd` verwendet werden.

Dienststatus prüfen

```
[RO] systemctl status ntp --no-pager
```

oder abhängig von der Distribution:

```
[RO] systemctl status ntpd --no-pager
```

Zeitpartner anzeigen

```
[RO] ntpq -pn
```

Typische Markierungen:

Zeichen	Bedeutung
*	Aktuell ausgewählte Zeitquelle
+	Geeignete zusätzliche Quelle
-	Von der Auswahl verworfene Quelle
x	Als falsch bewertete Quelle
Leerzeichen	Quelle wurde noch nicht ausgewählt

Protokolle anzeigen

```
[RO][PRIV][SENS] sudo journalctl -u ntp \
--since "-24 hours" --no-pager
```

oder:

```
[RO][PRIV][SENS] sudo journalctl -u ntpd \
--since "-24 hours" --no-pager
```

“ Es sollte zuerst ermittelt werden, welcher Zeitdienst tatsächlich aktiv ist. Mehrere parallel aktive Zeitdienste können sich gegenseitig beeinflussen.

11. Aktiven Zeitdienst unter Linux bestimmen

Erkannten NTP-Dienst anzeigen

```
[RO] timedatectl status
```

Typische Dienste prüfen

```
[RO] systemctl is-active systemd-timesyncd
```

```
[RO] systemctl is-active chronyd
```

```
[RO] systemctl is-active chrony
```

```
[RO] systemctl is-active ntpd
```

```
[RO] systemctl is-active ntp
```

Laufende Prozesse suchen

```
[RO] ps -ef |  
grep -E '[c]hronyd|[n]tpd|[s]ystemd-timesyncd'
```

Typische Problemkonstellationen

- Mehrere Zeitdienste sind gleichzeitig aktiv.
- Ein alter Zeitdienst wurde nach einer Migration nicht entfernt.
- Der Dienst läuft, besitzt aber keine verwendbare Quelle.
- Die Distribution verwaltet die Konfiguration über ein anderes Werkzeug.
- Eine virtuelle Maschine erhält zusätzlich Zeit vom Hypervisor.
- Eine Konfigurationsmanagement-Lösung überschreibt lokale Änderungen.

12. Zeitstatus unter macOS untersuchen

Lokale Zeit anzeigen

```
[RO] date "+%Y-%m-%dT%H:%M:%S%Z"
```

UTC-Zeit anzeigen

```
[RO] date -u "+%Y-%m-%dT%H:%M:%SZ"
```

Zeitzone anzeigen

```
[RO][PRIV] sudo systemsetup -gettimezone
```

Prüfen, ob Netzwerkzeit aktiviert ist

```
[RO][PRIV] sudo systemsetup -getusingnetworktime
```

Eingetragenen Netzwerkzeitserver anzeigen

```
[RO][PRIV][SENS] sudo systemsetup -getnetworktimeserver
```

Aktive Systemeinstellungen anzeigen

```
[RO] systemsetup -help
```

`systemsetup` benötigt für viele Abfragen Administratorrechte.

NTP-Server aktiv abfragen

```
[TEST] sntp -d <ZEITSERVER>
```

Beispiel:

```
[TEST] sntp -d time.apple.com
```

Dieser Test fragt eine Zeitquelle ab, ändert aber nicht automatisch die lokale Systemzeit.

Zeitbezogene Protokolle der letzten Stunde durchsuchen

```
[RO][PRIV][SENS] sudo log show --last 1h \  
--predicate 'process == "timed" OR process == "sntp"' \  
--style compact
```

Die vorhandenen Prozessnamen und Protokolle können sich zwischen macOS-Versionen unterscheiden.

Grafische Kontrolle

Apple-Menü

→ Systemeinstellungen

→ Allgemein

→ Datum & Uhrzeit

Dort werden unter anderem geprüft:

- Datum und Uhrzeit automatisch einstellen
- Eingetragener Netzwerkzeitserver
- Zeitzone automatisch anhand des Standorts einstellen
- Aktive Zeitzone
- Standortdienste für die automatische Zeitzone

13. Erreichbarkeit des Zeitservers prüfen

NTP verwendet normalerweise UDP-Port 123. Ein erfolgreicher Ping beweist nicht, dass NTP funktioniert.

Namensauflösung prüfen

Windows:

```
[RO] Resolve-DnsName "<ZEITSERVER>"
```

Linux:

```
[RO] getent ahosts "<ZEITSERVER>"
```

macOS:

```
[RO] dscacheutil -q host -a name "<ZEITSERVER>"
```

Windows: NTP-Antwort und Zeitabweichung testen

```
[TEST] w32tm /stripchart /computer:<ZEITSERVER> /samples:5 /dataonly
```

Linux mit chrony

```
[RO] chronyc sources -v
```

macOS

```
[TEST] sntp -d <ZEITSERVER>
```

Netzwerkaufzeichnung unter Linux

```
[TEST][PRIV][SENS] sudo tcpdump -ni any udp port 123
```

Netzwerkaufzeichnung unter macOS

```
[TEST][PRIV][SENS] sudo tcpdump -ni any udp port 123
```

Dabei ist zu prüfen:

1. Verlässt eine Anfrage das System?
2. Wird sie an die erwartete IP-Adresse gesendet?
3. Kommt eine Antwort zurück?
4. Verwendet das System tatsächlich diese Gegenstelle?
5. Blockiert eine lokale oder zentrale Firewall UDP 123?
6. Überschreibt ein VPN die Route oder DNS-Auflösung?

“ Ein einfacher TCP-Porttest ist für NTP ungeeignet, weil NTP normalerweise UDP und nicht TCP verwendet.

14. Zeitzone und Sommerzeit untersuchen

Eine korrekte Synchronisation liefert eine gemeinsame Zeitbasis. Die lokale Darstellung hängt zusätzlich von der Zeitzone ab.

Windows

```
[RO] Get-TimeZone
```

```
[RO] tzutil /g
```

Verfügbare Zeitzonen anzeigen:

```
[RO] Get-TimeZone -ListAvailable
```

Linux

```
[RO] timedatectl status
```

```
[RO] readlink -f /etc/localtime
```

Verfügbare Zeitzonen anzeigen:

```
[RO] timedatectl list-timezones
```

macOS

```
[RO][PRIV] sudo systemsetup -gettimezone
```

Typische Zeitzonefehler

- Ein System verwendet UTC statt `Europe/Berlin`.
- Ein Standortwechsel wurde nicht berücksichtigt.
- Veraltete Zeitzonendaten enthalten falsche Sommerzeitregeln.
- Ein Container besitzt eine andere Zeitzone als der Host.
- Eine Anwendung verwendet eine eigene Zeitzonekonfiguration.
- Die Datenbank speichert UTC, die Anwendung interpretiert sie als Lokalzeit.
- Ein Protokoll zeigt UTC ohne deutliche Kennzeichnung.
- Die Hardwareuhr wird unter Linux als lokale Zeit interpretiert.

Wichtige Unterscheidung

Situation	Bewertung
UTC falsch	Synchronisations- oder Uhrenproblem

Situation	Bewertung
UTC richtig, Lokalzeit falsch	Zeitzoneproblem
Betriebssystemzeit richtig, Anwendung falsch	Anwendungskonfiguration prüfen
Anzeige richtig, Logzeit abweichend	Prüfen, ob das Protokoll UTC verwendet

15. Virtuelle Maschinen und Hypervisor berücksichtigen

Virtuelle Maschinen können ihre Zeit aus mehreren Quellen erhalten:

- Virtuelle Hardwareuhr
- Hypervisor oder Gasterweiterungen
- Betriebssystem-Zeitdienst
- Active-Directory-Zeithierarchie
- Externer NTP-Server

Wenn mehrere Quellen gleichzeitig eingreifen, kann die Uhr springen oder ständig korrigiert werden.

Typische Ursachen

- Host besitzt selbst eine falsche Uhrzeit.
- VM wird nach längerer Pause fortgesetzt.
- Snapshot stellt einen älteren Zustand wieder her.
- Live-Migration verändert die Zeitbasis.
- Hypervisor-Zeitsynchronisation und NTP arbeiten gegeneinander.
- Ein virtueller Domänencontroller verwendet die falsche Quelle.
- Gasterweiterungen sind veraltet oder falsch konfiguriert.
- Die VM war längere Zeit ohne CPU-Zeit oder Netzwerkverbindung.

Prüfreihenfolge

1. Zeitquelle innerhalb der VM ermitteln.
2. Zeitstatus des Hypervisors prüfen.
3. Gasterweiterungen und Integrationsdienste kontrollieren.
4. Domänenrolle der VM berücksichtigen.
5. Snapshot- oder Migrationseignisse zeitlich vergleichen.
6. Prüfen, ob mehrere Zeitquellen gleichzeitig aktiv sind.
7. Herstellerempfehlung des verwendeten Hypervisors beachten.

Windows-VM

```
[RO] w32tm /query /source
```

Die Ausgabe:

```
VM IC Time Synchronization Provider
```

weist bei Hyper-V auf eine Zeitbereitstellung über die Integrationskomponenten hin.

“ Bei Domänencontrollern muss besonders sorgfältig geplant werden, welche Zeitquelle maßgeblich ist. Eine unkontrollierte Änderung kann die gesamte Domänenzeithierarchie beeinflussen.

16. Container und Zeitzonefehler untersuchen

Container verwenden normalerweise die Kernel-Uhr des Hosts. Die angezeigte lokale Zeit kann dennoch durch Zeitzonendateien, Umgebungsvariablen oder das Container-Image abweichen.

Zeit auf dem Host prüfen

```
[RO] date --iso-8601=seconds
```

Zeit in einem Docker-Container prüfen

```
[RO] docker exec "<CONTAINER>" date --iso-8601=seconds
```

UTC-Zeit im Container prüfen

```
[RO] docker exec "<CONTAINER>" date -u "+%Y-%m-%dT%H:%M:%SZ"
```

Zeitzonenumgebung prüfen

```
[RO][SENS] docker inspect "<CONTAINER>" \
--format '{{range .Config.Env}}{{println .}}{{end}}'
```

In der Ausgabe kann nach einer Variable wie `TZ` gesucht werden.

Typische Ursachen

- Hostzeit ist falsch.
- Im Container fehlt die Zeitzonendatenbank.
- Die Variable `TZ` ist falsch gesetzt.
- `/etc/localtime` enthält eine andere Zeitzone.
- Anwendung verwendet unabhängig vom Betriebssystem UTC.
- Host und Container zeigen dieselbe UTC-Zeit, aber unterschiedliche Lokalzeit.
- Protokolltreiber fügt Zeitstempel in UTC hinzu.

“ Die Systemzeit eines Containers sollte nicht durch zusätzliche Berechtigungen oder manuelle Änderungen korrigiert werden. Zuerst müssen Hostzeit, Zeitzone und Anwendungskonfiguration geprüft werden.

17. Hardwareuhr und Firmware berücksichtigen

Die Hardwareuhr, auch RTC genannt, hält die Zeit während des ausgeschalteten Zustands. Beim Start übernimmt das Betriebssystem einen Ausgangswert und synchronisiert ihn anschließend.

Linux

```
[RO][PRIV] sudo hwclock --show
```

Vergleich mit der Systemzeit:

```
[RO] date --iso-8601=seconds
```

Mögliche Ursachen für eine falsche Startzeit

- Leere oder schwache CMOS-Batterie
- Falsche Uhrzeit im BIOS oder UEFI
- Hardwareuhr wird unterschiedlich als UTC oder Lokalzeit interpretiert
- Dual-Boot-Systeme verwenden verschiedene RTC-Konventionen
- Virtuelle Hardwareuhr liefert einen falschen Wert
- NTP-Synchronisation erfolgt nach dem Start nicht
- System besitzt beim Start keine Netzwerkverbindung

Typisches Fehlerbild einer schwachen CMOS-Batterie

- Uhrzeit ist nach vollständigem Ausschalten wieder falsch.
- Firmware-Einstellungen gehen verloren.
- Datum springt auf einen älteren Standardwert.
- Nach erfolgreicher Netzwerksynchronisation stimmt die Uhr bis zum nächsten Ausschalten.

Bei virtuellen Maschinen existiert keine normale austauschbare CMOS-Batterie. Dort müssen Hypervisor, virtuelle Hardwareuhr und Hostzeit geprüft werden.

18. Zeitabhängige Sicherheitsfehler erkennen

Kerberos

Kerberos verwendet Zeitstempel, um wiederholte Verwendung abgefangener Authentifizierungsdaten zu erschweren. Eine zu große Abweichung zwischen Client, Domänencontroller und Server kann Anmeldungen verhindern.

Typische Meldungen:

- Zeitunterschied zwischen Client und Server
- Kerberos-Ticket noch nicht gültig
- Kerberos-Ticket abgelaufen
- Domänenanmeldung nicht möglich

TLS und Zertifikate

Zertifikate besitzen unter anderem:

- Gültigkeitsbeginn
- Gültigkeitsende

Bei falscher Systemzeit kann ein gültiges Zertifikat erscheinen als:

- Noch nicht gültig
- Abgelaufen
- Außerhalb des Gültigkeitszeitraums

Zeitbasierte Einmalpasswörter

TOTP-Verfahren berechnen Codes aus:

- Gemeinsamen Geheimnis
- Aktuellem Zeitintervall

Wenn Smartphone, Server oder Authentifizierungsdienst zeitlich abweichen, werden korrekte Codes abgelehnt.

Prüfregel

Bei gleichzeitigen Fehlern in Anmeldung, Zertifikaten und MFA sollte die Systemzeit sehr früh in der Diagnose geprüft werden.

19. Sichere Korrekturmaßnahmen

Vor jeder Änderung muss die Ursache bestimmt werden. Ein manuelles Stellen der Uhr kann Protokolle, Datenbanken, Cluster und laufende Anwendungen beeinflussen.

Windows: erneute Synchronisation anfordern

```
[CHANGE][PRIV] w32tm /resync
```

Mit erneuter Erkennung der Zeitquelle:

```
[CHANGE][PRIV] w32tm /resync /rediscover
```

Linux mit systemd-timesyncd

Zeitdienst nur nach bestätigter Ursache neu starten:

```
[CHANGE][PRIV] sudo systemctl restart systemd-timesyncd
```

Linux mit chrony

Dienst nur nach bestätigter Ursache neu starten:

```
[CHANGE][PRIV] sudo systemctl restart chronyd
```

Abhängig von der Distribution:

```
[CHANGE][PRIV] sudo systemctl restart chrony
```

Große Zeitkorrekturen

Große Zeitsprünge können:

- Datenbanktransaktionen beeinflussen
- Protokolle unbrauchbar machen
- Sitzungen und Tickets ungültig machen
- Cluster irritieren
- Aufgaben doppelt oder gar nicht ausführen
- Monitoringdaten in die falsche Reihenfolge bringen
- Anwendungen mit zeitabhängigen Sperren beeinträchtigen

Vor einer großen Korrektur sind deshalb zu prüfen:

- Größe und Richtung der Abweichung
- Rolle des Systems
- Laufende Datenbanken und Cluster
- Domänenfunktion
- Virtualisierung
- Wartungsfenster
- Sicherung und Rückfallplan
- Herstellerdokumentation der betroffenen Anwendung

“ Die Zeit niemals absichtlich zurückstellen, ohne die Auswirkungen auf Datenbanken, Protokolle und verteilte Systeme zu bewerten.

20. Typische Fehlinterpretationen vermeiden

Fehlinterpretation	Richtige Bewertung
„Die Uhr in der Taskleiste stimmt.“	Quelle, Synchronisationsstatus, UTC und Zeitzone zusätzlich prüfen.
„Ping zum Zeitserver funktioniert.“	Ping prüft nicht die NTP-Kommunikation über UDP 123.
„Der Zeitdienst läuft, also synchronisiert er.“	Ein aktiver Dienst kann ohne brauchbare Quelle laufen.
„Eine Stunde Abweichung ist ein NTP-Fehler.“	Häufig ist die Zeitzone oder Sommerzeitregel falsch.
„Alle Systeme müssen dieselbe lokale Uhrzeit anzeigen.“	Systeme in verschiedenen Zeitzonen können dieselbe UTC-Zeit verwenden.
„Die Uhr kann gefahrlos manuell gestellt werden.“	Zeitsprünge können Anwendungen und Protokolle beeinflussen.
„Jeder Domänenclient sollte einen öffentlichen NTP-Server verwenden.“	Domänenmitglieder sollten normalerweise der AD-Zeithierarchie folgen.

Fehlinterpretation	Richtige Bewertung
„Der Hypervisor regelt die Zeit vollständig.“	Gastzeitdienst und Hypervisor können gleichzeitig eingreifen.
„Container besitzen eine vollständig eigene Uhr.“	Container verwenden normalerweise die Kernel-Uhr des Hosts.
„Ein Neustart behebt die Zeit dauerhaft.“	Eine fehlerhafte Quelle oder Konfiguration bleibt bestehen.

21. Sichere Reihenfolge der Fehleranalyse

1. Fehlerzeitpunkt und originale Fehlermeldung dokumentieren.
2. Lokale Zeit und UTC-Zeit erfassen.
3. Zeitzone kontrollieren.
4. Abweichung mit einem vertrauenswürdigen Vergleichssystem bestimmen.
5. Aktiven Zeitdienst identifizieren.
6. Tatsächlich verwendete Zeitquelle ermitteln.
7. Synchronisationsstatus und letzte erfolgreiche Messung prüfen.
8. Namensauflösung der Zeitquelle testen.
9. NTP-Antwort beziehungsweise Zeitabweichung aktiv prüfen.
10. Firewall, Routing und UDP 123 untersuchen.
11. Ereignis- beziehungsweise Systemprotokolle auswerten.
12. Domänen-, Virtualisierungs- oder Containerstruktur berücksichtigen.
13. Erst danach eine erneute Synchronisation oder Konfigurationsänderung durchführen.
14. Nach der Maßnahme Quelle, Status und Abweichung erneut kontrollieren.
15. Ursache und Korrektur dokumentieren.

22. Schnelle Befehlsübersicht

Aufgabe	Windows	Linux	macOS
Lokale Zeit	[RO] Get-Date -Format o	[RO] date --iso-8601=seconds	[RO] date "+%Y-%m-%dT%H:%M:%SZ"
UTC-Zeit	[RO] (Get-Date).ToUniversalTime().ToString("o")	[RO] date -u "+%Y-%m-%dT%H:%M:%SZ"	[RO] date -u "+%Y-%m-%dT%H:%M:%SZ"
Zeitzone	[RO] Get-TimeZone	[RO] timedatectl status	[RO][PRIV] sudo systemsetup -gettimezone
Zeitdienst	[RO] Get-Service W32Time	[RO] systemctl status <DIENST>	Systemdienst wird durch macOS verwaltet
Zeitquelle	[RO] w32tm /query /source	[RO] timedatectl timesync-status oder [RO] chronyc tracking	[RO][PRIV] sudo systemsetup -getnetworktimeserver

Aufgabe	Windows	Linux	macOS
Synchronisationsstatus	[RO] w32tm /query /status	[RO] timedatectl status oder [RO] chronyc tracking	[RO][PRIV] sudo systemsetup -getusingnetworktime
Zeitpartner	[RO] w32tm /query /peers	[RO] chronyc sources -v oder [RO] ntpq -pn	Eingetragener Netzwerkzeitserver
Abweichung testen	[TEST] w32tm /stripchart ...	Quellenstatus des verwendeten Dienstes	[TEST] sntp -d <ZEITSERVER>
Protokolle	[RO] Get-WinEvent ...	[RO][PRIV] sudo journalctl -u <DIENST>	[RO][PRIV] sudo log show ...
Hardwareuhr	Nicht üblicherweise separat	[RO][PRIV] sudo hwclock --show	Nicht regulär erforderlich
Synchronisation anfordern	[CHANGE][PRIV] w32tm /resync	Abhängig vom eingesetzten Dienst	Durch macOS beziehungsweise Systemeinstellungen
NTP-Verkehr erfassen	Paketaufzeichnung erforderlich	[TEST][PRIV] sudo tcpdump -ni any udp port 123	[TEST][PRIV] sudo tcpdump -ni any udp port 123

23. Entscheidungsmatrix

Befund	Wahrscheinliche Ursache	Nächster Schritt
UTC korrekt, Lokalzeit falsch	Zeitzone oder Sommerzeit	Zeitzonekonfiguration prüfen
UTC und Lokalzeit falsch	Zeitquelle oder Synchronisation	Dienst und Quelle untersuchen
Zeitdienst läuft, keine Quelle	Netzwerk, DNS, Firewall oder Konfiguration	Erreichbarkeit und Zeitpartner prüfen
Quelle ist lokale Hardwareuhr	Keine externe Synchronisation	Erwartete Zeitarchitektur prüfen
Nur Domänenanmeldungen betroffen	Kerberos-Zeitabweichung möglich	Client, Server und DC vergleichen
TLS und MFA gleichzeitig fehlerhaft	Systemzeit wahrscheinlich falsch	Datum, UTC und Quelle sofort prüfen
Zeit springt nach Neustart zurück	RTC, Firmware, Host oder CMOS-Batterie	Startzeit und Hardware prüfen
Nur eine VM betroffen	Hypervisor- oder Gastkonfiguration	Beide Zeitquellen vergleichen
Alle Domänensysteme betroffen	Fehler in der AD-Zeithierarchie	PDC-Emulator und übergeordnete Quelle prüfen
Abweichung wächst kontinuierlich	Uhrdrift oder keine Nachregelung	Messwerte und Dienstprotokolle untersuchen
Exakt eine Stunde Abweichung	Zeitzone oder Sommerzeit	Zeitzone statt NTP-Konfiguration prüfen

Befund	Wahrscheinliche Ursache	Nächster Schritt
Host korrekt, Container falsch	Container-Zeitzone oder Anwendung	 Zeitzonendateien und Anwendung prüfen

24. Dokumentationsvorlage

Ticket:

Datum und Uhrzeit der Analyse:

Bearbeiter:

Betroffenes System:

Betriebssystem:

Systemrolle:

Physisch, virtuell oder Container:

Domänenmitglied:

Betroffene Anwendung oder Funktion:

Originale Fehlermeldung:

Lokale Zeit:

UTC-Zeit:

Zeitzone:

Vergleichssystem:

Gemessene Abweichung:

Aktiver Zeitdienst:

Dienststatus:

Aktive Zeitquelle:

Konfigurierte Zeitpartner:

Letzte erfolgreiche Synchronisation:

Stratum beziehungsweise Hierarchie:

NTP-Antwort erhalten:

UDP 123 erreichbar:

DNS-Auflösung:

Zeitbezogene Protokollmeldungen:

Hypervisor-Zeitquelle:

Snapshot oder Migration:

Hardwareuhr:

Gruppenrichtlinie oder Geräteverwaltung:

Vermutete Ursache:

Durchgeführte Tests:

Durchgeführte Änderung:

Auswirkung der Änderung:

Rückfallplan:

Zeitquelle nach der Maßnahme:

Abweichung nach der Maßnahme:

Synchronisationsstatus nach der Maßnahme:

Funktionsprüfung:

Weiterführende Maßnahmen:

Merksatz

“ Bei Zeitfehlern werden immer vier Dinge getrennt geprüft: aktuelle UTC-Zeit, lokale Zeitzone, verwendete Zeitquelle und tatsächlicher Synchronisationsstatus. Die Uhr wird erst verändert, wenn Ursache und Auswirkungen geklärt sind.

Quellen und weiterführende Dokumentation

- [Microsoft Learn – Windows Time Service Tools and Settings](#)
- [Microsoft Learn – Funktionsweise des Windows-Zeitdiensts](#)
- [Microsoft Learn – Windows Server Time Accuracy Improvements](#)
- [Microsoft Learn – Windows Time Service Technical Reference](#)
- [systemd – timedatectl](#)
- [systemd – systemd-timesyncd](#)
- [chrony – Dokumentation](#)
- [chrony – chronyc](#)
- [Linux-Handbuch – hwclock](#)
- [Apple – Datum und Uhrzeit auf dem Mac automatisch einstellen](#)
- [Apple – Einstellungen für Datum und Uhrzeit](#)
- [Apple – Fehlerhafte Uhrzeit oder Zeitzone korrigieren](#)

