Zeitsynchronisation Windows Server 2008 R2 PDC Master der FRD mit einer externen Zeitquelle

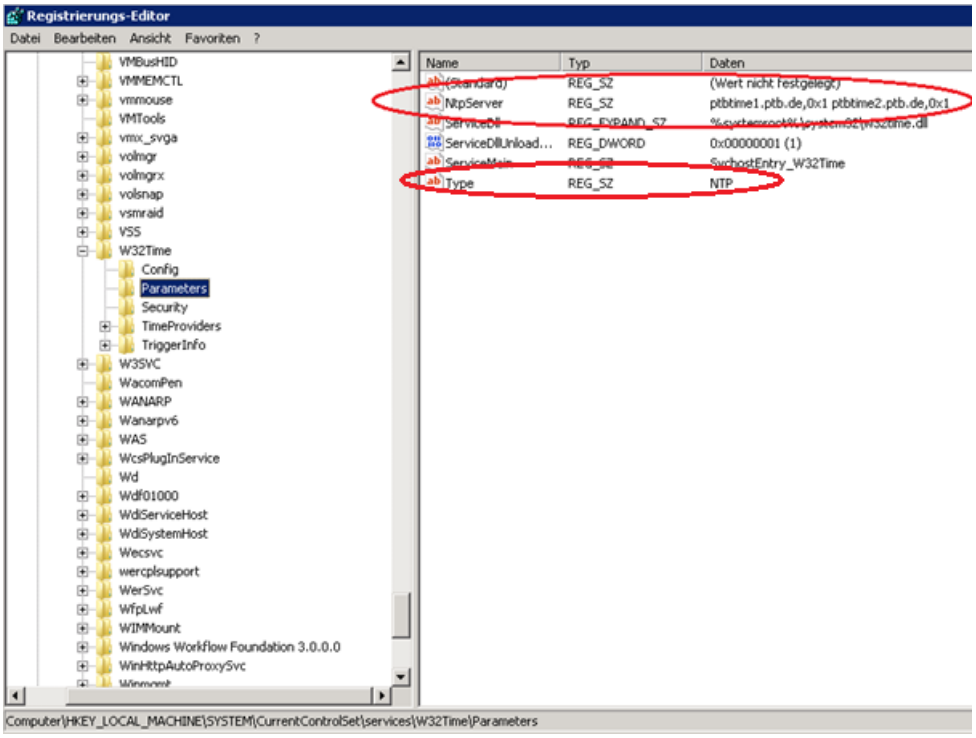
Wie funktioniert die Zeitsynchronisation in Windows Netzwerken:
http://support.microsoft.com/kb/816042
MSDN Blog
http://blogs.msdn.com/w32time/default.aspx
Basis fuer die Konfiguration:
http://support.microsoft.com/kb/816042/en-us

Firewall:

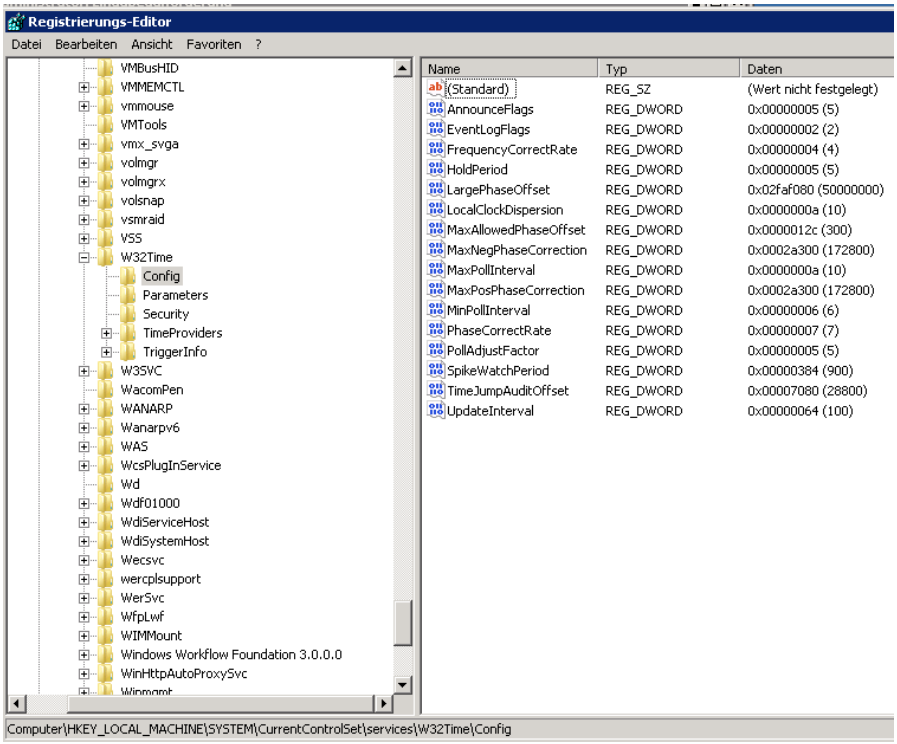
Sicherstellen, dass die Firewall NTP Port 123 UDP vom PDC Master zu den externen Zeitservern erlaubt

Registry

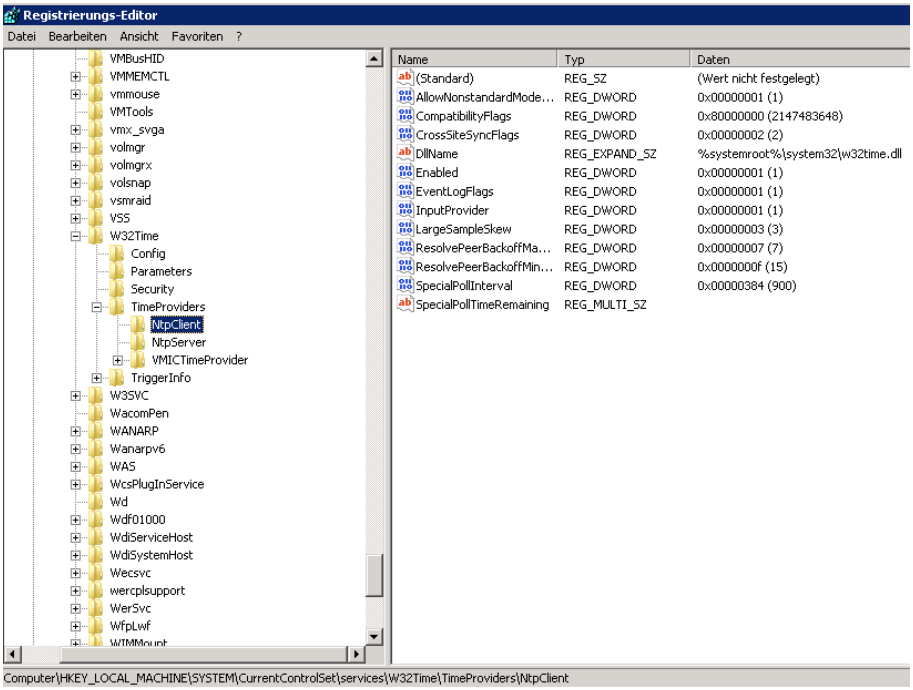
Angabe der externen NTP Server und umstellen des Types von NT5DS auf NTP



Anpassen diverser Einstellungen lt. KB Artikel

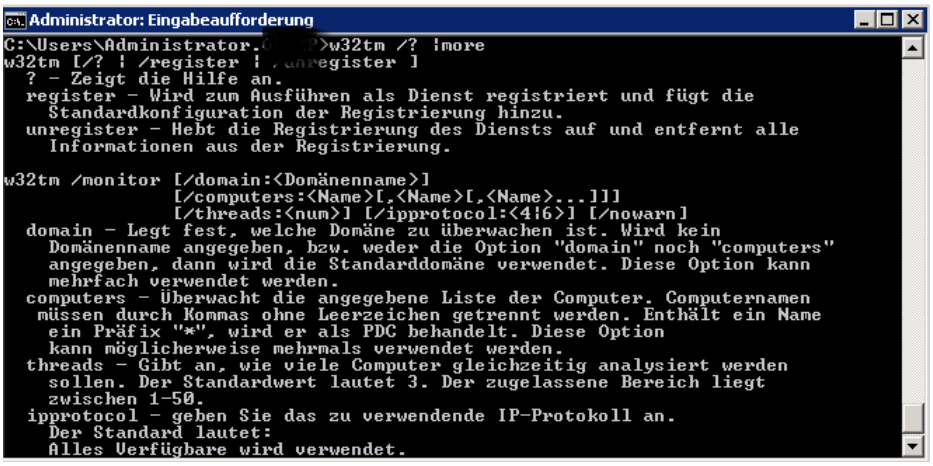


Time Provider NTP Client konfigurieren

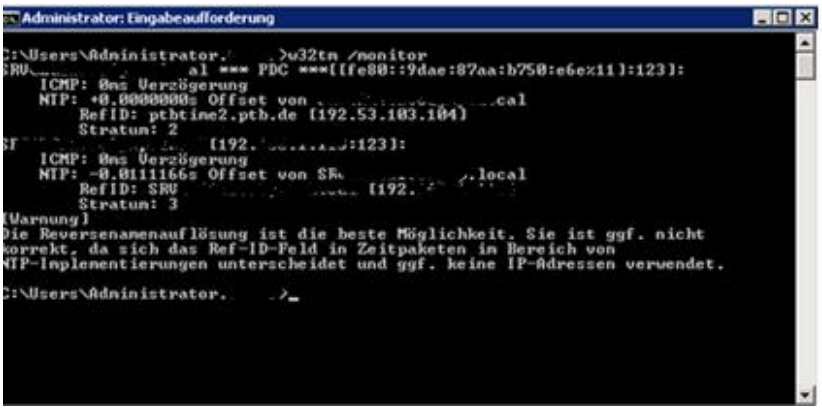


W32TM

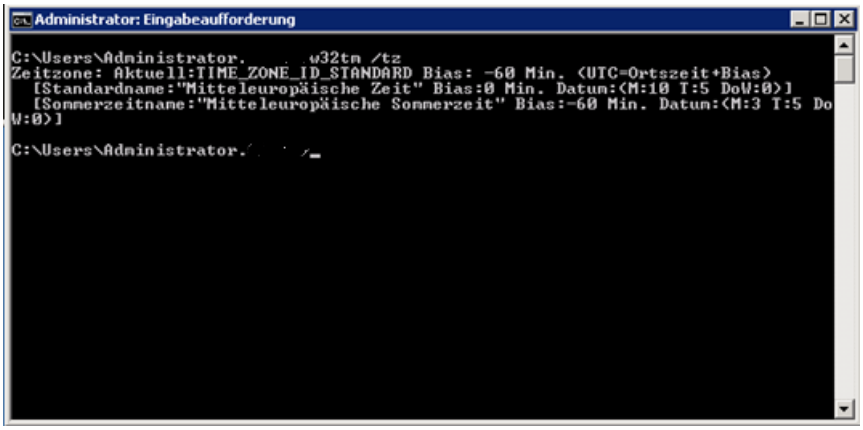
Die Konfiguration / Troubleshooting des W32Time Dienstes erfolgt mit dem Command Line Tool W32TM



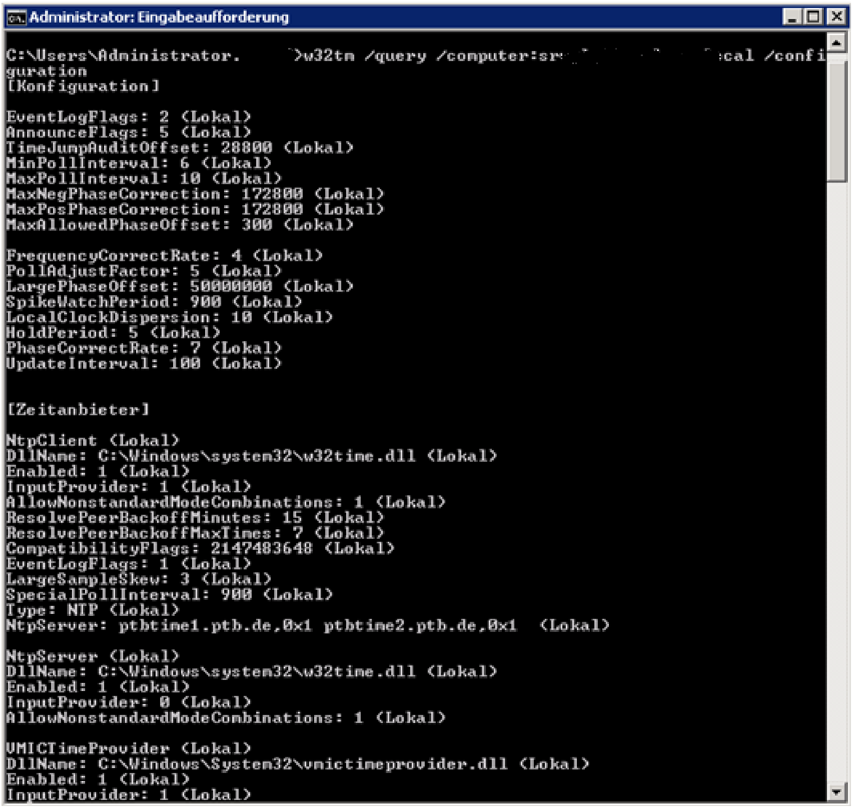
Monitoring der Domaene



Anzeige der Zeitzonenkonfiguration

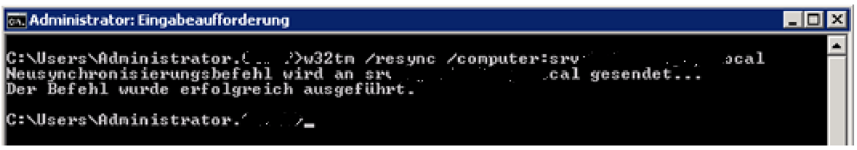


Abfrage der Computerkonfiguration



```
C:\Users\Administrator.      >w32tm /query /computer:sr                cal /confi
guration
[Konfiguration]

EventLogFlags: 2 (Lokal)
AnnounceFlags: 5 (Lokal)
TimeJumpAuditOffset: 28800 (Lokal)
MinPollInterval: 6 (Lokal)
MaxPollInterval: 10 (Lokal)
MaxNegPhaseCorrection: 172800 (Lokal)
MaxPosPhaseCorrection: 172800 (Lokal)
MaxAllowedPhaseOffset: 300 (Lokal)

FrequencyCorrectRate: 4 (Lokal)
PollAdjustFactor: 5 (Lokal)
LargePhaseOffset: 50000000 (Lokal)
SpikeWatchPeriod: 900 (Lokal)
LocalClockDispersion: 10 (Lokal)
HoldPeriod: 5 (Lokal)
PhaseCorrectRate: 7 (Lokal)
UpdateInterval: 100 (Lokal)


[Zeitanbieter]

NtpClient (Lokal)
DllName: C:\Windows\system32\w32time.dll (Lokal)
Enabled: 1 (Lokal)
InputProvider: 1 (Lokal)
AllowNonstandardModeCombinations: 1 (Lokal)
ResolvePeerBackoffMinutes: 15 (Lokal)
ResolvePeerBackoffMaxTimes: 7 (Lokal)
CompatibilityFlags: 2147483648 (Lokal)
EventLogFlags: 1 (Lokal)
LargeSampleSkew: 3 (Lokal)
SpecialPollInterval: 900 (Lokal)
Type: NTP (Lokal)
NtpServer: ptbtime1.ptb.de,0x1 ptbtime2.ptb.de,0x1  (Lokal)

NtpServer (Lokal)
DllName: C:\Windows\system32\w32time.dll (Lokal)
Enabled: 1 (Lokal)
InputProvider: 0 (Lokal)
AllowNonstandardModeCombinations: 1 (Lokal)

VMICTimeProvider (Lokal)
DllName: C:\Windows\System32\vmictimeprovider.dll (Lokal)
Enabled: 1 (Lokal)
InputProvider: 1 (Lokal)
```

Resynchronisation



```
C:\Users\Administrator.     >w32tm /resync /computer:srv              ocal
Neusynchronisierungsbefehl wird an sr              .cal gesendet...
Der Befehl wurde erfolgreich ausgeführt.

C:\Users\Administrator.     >_
```

Noch was zu lesen (Der Artikel stammt aus Windows 2000 Zeiten, vermittelt aber einen guten Ueberblick):

Das SNTP-Protokoll ist in RFC 1769 definiert und ist eine abgespeckte Version des vollen NTP-Protokolls und wird in Netzwerken eingesetzt, bei denen es nicht auf genaueste Zeitsynchronisation und Protokollierungsfähigkeiten ankommt.

Während die korrekten Zeiten in einer AD-Domäne für die Replikation der Verzeichnisinformationen nicht so elementar wichtig sind, wie z. B. bei Novell, weil die Replikation des AD bei MS mit USN und erst dann mit Zeitstempeln arbeitet, ist die korrekte Zeit auf allen Rechnern innerhalb der Domäne für den Einsatz von Kerberos sehr wichtig. Kerberos arbeitet mit Tickets, welche nach gewisser Zeit ablaufen und erneuert werden müssen. Unterscheiden sich die Systemzeiten der Rechner im Netzwerk hier sehr stark, so kann es schnell zu unerwünschten Problemen kommen. Bei der Verwendung von Kerberos werden Zeitfenster von maximal 5 Minuten toleriert.

Um diese Problematik zu lösen, verwendet MS ab Windows 2000 Professional Version den Windows 2000 Server Time Service.

Der Windows Server Time Service kann nicht über ein MMC-SnapIn konfiguriert werden, sondern nur über die Systemsteuerung der jeweiligen Workstation.

Windows 2000 implementiert RFC 1361, den Simple Network Time Protocol Dienst, welche eine vereinfachte Version des Network Time Protocols (NTP) darstellt.

Microsoft verwendet nicht den vollen NTP-Dienst, weil es unter Windows 2000 nicht auf Protokollierfähigkeiten und die genaueste Zeit im Millisekundenbereich ankommt. Im Laufe der Zeit wurde die Zeitsychchronisation mit jeder Windows Version verfeinert.

Sie können die Zeitkonfiguration auch manuell über die Registry vornehmen. Ändern Sie die Standardeinstellungen des NTP-Servers, indem Sie einen neuen Eintrag vom Typ REG_SZ mit dem Value NTPServer in der Struktur HKLM\System\CurrentControlSet\Services\W32Time\Parameters setzen. Der Eintrag muss den DNS-Namen oder die IP-Adresse des Zeitservers enthalten. Zusätzlich müssen Sie den Wert Nt5DS zu NTP ändern.

Administratoren können auch externe Zeitserver für die Zeitsynchronisation verwenden, indem sie an der Kommandozeile den Befehl: NET TIME /SETSNTP:<SERVER-LISTE> eingeben.

Wie funktioniert die Zeitsynchronisation:

- Die Workstation kontaktiert den authentifizierenden DC. Es erfolgt ein Paketaustausch um die zeitliche Latenz zwischen den zwei Maschinen zu ermitteln.
- Die lokale Zeit der Workstation wird geändert. Wenn die Zielzeit auf der Workstation hinter der lokalen Zeit des DC ist, wird die Zeit des Servers gesetzt.
- Wenn die Zielzeit des Servers hinter der Zeit der lokalen Workstation ist, wird die Echtzeituhr der Workstation für die nächsten 20 Minuten „verlangsamt“ um die Zeiten abzugleichen. Divergiert die lokale Zeit jedoch mehr als 2 Minuten von der Zielzeit des Servers, wird die korrekte Zeit sofort gesetzt.
- Die Workstation prüft in regelmäßigen Abständen (zunächst alle 8 Stunden) die Zeit mit dem Zielserver. Wenn die lokale Zeit sich mehr als 2 Sekunden von der des DC unterscheidet, wird das Intervall halbiert, bis eine minimale Frequenz von 45 Minuten entsteht.

Windows 2000 Server arbeiten folgendermaßen:

- Alle Mitgliedserver arbeiten nach dem gleichen Verfahren wie Windows 2000 Professional
- Alle PDCs in der Domäne verwenden den FSMO als Zeitserver
- Alle PDC FSMO verwenden den „Inbound“-Partner DC als Zeitserver

NTP-Protokoll

Das NTP-Protokoll ist in RFC 1305 spezifiziert. NTP Synchronisation ist Part eines Software Packages, welches zusätzlich noch diverse NTP Optionen und Algorithmen enthält.

SNTP Sicherheit

SNTP verwendet die Credentials des Clients um eine sichere Verbindung von einem SNTP-Client zu einem SNTP-Server aufzubauen. SNTP verwendet dazu den sicheren Kanal den eine Win2K Prof.-Maschine mit einem Win2K-Server aufbaut. (Netlogon Secure Channel). W32Time benutzt den sicheren Client Account um eine Signatur für SNTP-Pakete zu erstellen welche über das Netzwerk gesendet werden.

Außerhalb einer Domäne ist der W32Time-Dienst relativ unsicher und nicht geschützt, da keine sicheren Verbindungen verwendet werden können.

Zeitsynchronisation

W32Time wird standardmäßig auf allen Windows 2000 Professional Maschinen, Win2K Servern usw. installiert. W32Time verwendet UTC (Universal Time Coordination) welches auf einer atomaren Zeitskala basiert.

W32Time wird automatisch auf Computern gestartet welche zur Domäne hinzugefügt wurden. Auf Rechnern welche nicht Mitglied einer Domäne sind, muss der W32Time-Dienst manuelle gestartet und konfiguriert werden.

W32Time prüft in regelmäßigen Abständen die richtige Systemzeit. Zuerst beim Starten des Systems, dann in Intervallen von 45 Minuten bis die Systemzeit mit der Zeitquelle synchronisiert ist und nach erfolgter Synchronisation alle acht Stunden. Taucht ein Fehler auf, beginnt der Prozess der Zeitsynchronisation wieder von vorne.

Hierarchie der Zeitkonvergenz

W32Time unterstützt drei verschiedene Synchronisationsvarianten.

1. Domänen-Hierarchie basierende Zeitsynchronisation mit Hilfe des PDC der Forest Root Domain als primärer Zeitserver.

Bei der Domänen-Hierarchie basierenden Zeitsynchronisation spricht man von sogenannten Stratums. Ein Stratum definiert die Reihenfolge der Abarbeitung der Zeitsynchronisation.

Stratum	**Beschreibung**
0	Externe NTP Zeitquelle
1	PDC Emulator der Forest Root Domain
2	DC in der Forest Root Domain oder PDC Emulatoren in Child Domains
3	Workstations und Member Server in der Forest Root Domain oder DCs in Child Domains
4	Workstations und Member Server in Child Domains

Preferences zur Auswahl einer Zeitquelle

Preference	Computer	Standort	Verfügbarkeit der Zeitquelle
1	Parent Domain Controller	Intrasite	Verfügbar
2	Local Domain Controller	Intrasite	Verfügbar
3	Parent Domain Controller	Intrasite	Nicht verfügbar
4	Local PDC Emulator	Intrasite	Nicht verfügbar
5	Parent Domain Controller	Intersite	Verfügbar
6	Local Domain Controller	Intersite	Verfügbar
7	Parent Domain Controller	Intersite	Nicht verfügbar
8	Local PDC Emulator	Intersite	Nicht verfügbar

2. Manuell konfigurierte Synchronisation

Manuell konfigurierte Zeitsynchonisation erfolgt mit Hilfe des NET TIME Befehls.

3. Keine konfigurierte Zeitsynchronisation

Die Zeitsynchronisation ist auch mit Hilfe von Drittanbieterprodukten möglich.

Der W32Time-Dienst kann manuelle von der Kommandozeile gestartet und gestoppt werden.

NET STOP W32TIME
NET START W32TIME

NET TIME PARAMETER

Parameter	Beschreibung
NET TIME	Zeigt die Zeit auf einem Zeitserver an
NET TIME \\COMPUTERNAME	Zeigt die Zeit auf einem bestimmten Rechner an
NET TIME /DOMAIN:DOMÄNENNAME	Zeigt die Zeit auf einem Domänencontroller an
NET TIME /RTSDOMAIN:DOMÄNENNAME	Zeigt die Zeit auf dem Zeitserver an
NET TIME /QUERYSNTP	Zeigt die manuell konfigurierte Zeitquelle an
NET TIME /SETSNTP:NTPSERVER	Setzt die manuelle Zeitquelle für diesen Computer
NET TIME /SETSNTP	Löscht die manuell konfigurierte Zeitquelle für diesen Computer

W32TM ist ein Diagnoseutility für den W32Time-Service. Wenn das Tool auf einem DC genutzt wird ist es erforderlich den W32Time-Dienst zu stoppen.

Eintrag	Datentyp	Beschreibung
ReliableTimeSource	REG_DWORD	Wird verwendet um festzustellen, dass die zuverlässige Zeit verwendet wird 0 = markiert Computer als nicht reliable 1 = markiert Computer als reliable
Period	REG_DWORD oder REG_SZ	Wird verwendet um festzulegen, wie oft W32TIME die Zeit synchronisiert. 65531 = alle 45 Minuten bis die Synchronisation erfolgt ist, dann alle 1 Tag 65532 = alle 45 Minuten bis die Synchronisation erfolgt ist, sonst alle 8 Stunden 65533 = alle sieben Tage 65534 = alle drei Tage
AvoidTimeSyncOnWan	REG_DWORD	Verhindert die Synchronisation über Standorte hinweg 0 = Site wird ignoriert 1 = Zeit wird nicht synchronisiert bei „fremden“ Sites
LocalNTP	REG_DWORD	Startet den SNTP-Server
Type	REG_SZ	Wird verwendet um einzustellen, wie der Server startet
NtpServer	REG_SZ optional	Wird verwendet um die Zeitquelle manuell zu konfigurieren
GetDcBackoffMinutes	REG_DWORD optional	Die anfängliche Anzahl an Minuten bevor ein anderer Zeitserver gesucht wird wenn der lokale nicht reagiert
GetDcBackoffMaxTimes	REG_DWORD optional	Die maximale Anzahl an Zeit um das Backoff Intervall zu erhöhen um einen DC zu finden