In Windows è disponibile il servizio Ora di Windows (W32Time) basato sul SNTP (Simple Network Time Protocol, per ulteriori informazioni si veda l' RFC 1769) richiesto dal protocollo di autenticazione Kerberos. Scopo del servizio Ora è garantire che tutti i computer in cui è installato Microsoft Windows 2000 o versioni successive presenti in un'azienda utilizzino un'ora comune.

Per garantire un'ora comune, il servizio Ora di Windows si basa su una relazione gerarchica che consente di controllare l'autorità e impedire loop. Per impostazione predefinita viene utilizzata la gerarchia seguente:

- Tutti i computer desktop client nominano come partner orario interno il controller di dominio di autenticazione.
- Tutti i server membri nominano come partner orario interno il controller di dominio di autenticazione.
- Tutti i controller di dominio presenti in un dominio nominano come partner orario interno il master operazioni del controller di dominio primario (PDC).
- Tutti i master operazioni del controller di dominio primario rispettano la gerarchia dei domini per la selezione del relativo partner orario interno.

In questa gerarchia il master operazioni del controller di dominio primario situato nella directory principale dell'insieme di strutture diventa quello autorevole per l'organizzazione. Si consiglia di configurare il server di riferimento ora autorevole per ottenere l'ora da un'origine hardware. Quando si configura il server di riferimento ora autorevole per la sincronizzazione con un'origine ora Internet, non viene eseguita l'autenticazione. Si consiglia inoltre di ridurre le impostazioni di correzione dell'ora per i server e i client autonomi. Questi suggerimenti assicurano una maggiore accuratezza e protezione al dominio.

Il master PDC non deve essere configurato per sincronizzarsi con se stesso(per maggiori informazioni si veda la RFC 1305),ma deve sincronizzarsi con un server NTP esterno o un dispositivo hardware connesso localmente.

Per impedire gli attacchi tramite riproduzione di pacchetto Kerberos V5 utilizza i timestamp nell'ambito della definizione del protocollo e per assicurare il funzionamento corretto dei timestamp, gli orologi del client e del controller di dominio devono essere sincronizzati con la massima precisione possibile.

Gli orologi di due computer sono spesso non sincronizzati quindi è possibile utilizzare il Critero Kerberos Tolleranza massima per la sincronizzazione dell'orologio del computer (Configurazione computerImpostazioni di WindowsImpostazioni protezioneCriteri accountCriterio Kerberos) per stabilire la differenza massima che può essere tollerata da Kerberos V5 tra l'orologio del client e l'orologio del controller di dominio (5 minuti per impostazione predefinita). Se la differenza tra l'orologio di un client e l'orologio di un controller di dominio è inferiore alla differenza massima specificata nel criterio, i timestamp utilizzati in una sessione tra due computer verranno considerati autentici. Questa impostazione non è persistente ciò significa che se la si configura e poi si riavvia il computer, l'impostazione verrà riportata al valore predefinito. Per ulteriori informazioni si veda Pericoli e contromisure - Capitolo 2: Criteri a livello di dominio .

Configurazione del servizio Ora di Windows sul master PDC per utilizzare un'origine ora esterna

Per configurare un server di riferimento ora interno (master PDC) in modo che venga effettuata la sincronizzazione con un'origine ora esterna utilizzare la seguente procedura:

1. Impostare la registry key **HKLMSYSTEMCurrentControlSetServicesW32TimeConfigAnnounceFlags** a 5 (il valore predefinito è 10, questa configurazione impone al master PDC di notificarsi come origine ora affidabile e utilizza l'orologio CMOS incorporato senza utilizzare un'origine ora esterna).
   Per ulteriori informazioni si veda Config-AnnounceFlags Entry .
2. Impostare la **HKLMSYSTEMCurrentControlSetServicesW32TimeParametersNtpServer** con l'elenco dei server NTP separati da spazio, l'elenco può comprendere sia indirizzi IP che nomi DNS.
   Specificando dopo il server il flag **,0x1** è possibile ricontattare il server NTP in base al valore della chiave **HKLMSYSTEMCurrentControlSetServicesW32TimeTimeProvidersNtpClientSpecialPollInterval** anzichè in base alle specifiche NTP. In questo modo si riduce l'utilizzo della rete ma si riduce l'accuratezza.
   Per impostare la sincronizzazione verso i server NTP dell' I.N.RI.M (Istituto Nazionale di Ricerca Metrologica) impostare la registry key a:
   ntp1.inrim.it,0x1 ntp2.inrim.it,0x1 in alternativa è possibile impostare questa chiave di registro mediante il comando
   net time /setsntp:"ntp1.inrim.it,0x1 ntp2.inrim.it,0x1"
   Per ulteriori informazioni si veda Parameters-NtpServer .
   *Al seguente Configurazione di un server di riferimento ora autorevole in Windows Server 2003 viene indicato che è necessario aggiungere **,0x1** alla fine di ogni nome*

DNS in caso contrario le modifiche apportate alla chiave
SpecialPollInterval
non avranno effetto.

3. Impostare la registry key **HKLMSYSTEMCurrentControlSetServicesW32TimeParametersType** a **NTP**.
   Se si è utilizzato il comando **net time /setsntp** la registry key Type viene impostata automaticamente a NTP.
   In questo modo si consente la sincronizzazione dalla lista di server NTP specificati nella chiave **HKLMSYSTEMCurrentControlSetServicesW32TimeParametersNtpServer**
   Il resto dei Domain Controller e dei client che seguono la normale gerarchia per la sincronizzazione dell'ora avranno la registry key Type impostata a Nt5DS. Per ulteriori informazioni si veda Parameters-Type Subkey .
4. Riavviare il servizio W32Time tramite il comando:
   net stop w32time && net start w32time.
5. Il protocollo SNTP utilizza la porta UDP (User Datagram Protocol) 123, occorre quindi configurare il firewall aziendale in modo che consente il traffico su questa porta dal master PDC verso i server SNTP Internet utilizzati.
6. Per verificare che le impostazioni relative all'elenco dei server NTP da utilizzare sia stata impostata correttamente è possibile utilizzare il comando:
   net time /querysntp
7. Per forzare la sincronizzazione è possibile utilizzare il comando:
   w32tm /resync /rediscover
   Se la sincronizzazione avviene correttamente verranno registrati nel log di Sistema in sequenza gli eventi informativi W32Time 37,35 e 37. In caso contrario il master PDC contatterà l'origine esterna sulla base del valore impostato nella chiave **SpecialPollInterval** che per impostazione predefinita è di 60 minuti (analogamente è possibile utilizzare il comando anche sui computer client e i server membro).

Per maggior sicurezza è anche possibile utilizzare i server NTP I.N.RI.M autenticati che utilizzano una crittografia a chiave simmetrica (MD5) o una crittografia a chiave pubblica (Autokey 2), oppure configurare il proxy server/firewall come server NTP e sicronizzare il TSAF (Time Server Autoritario della Foresta) a sicronizzarsi con il proxy server/firewall per evitare che il DC comunichi con un time server esterno.

Per ulteriori approfondimenti si faccia riferimento ai seguenti:

- Cenni preliminari sul servizio Ora di Windows
- Windows Time Service Technical Reference
- Configure a client computer for automatic domain time synchronization

- Configurazione di un server di riferimento ora autorevole in Windows Server 2003
- Configurazione di un server di riferimento ora autorevole in Windows XP
- A client computer may not synchronize its time setting with the time setting of the domain controller in Windows XP or in Windows Server 2003
- Configuring the Windows Time Service
- The W32Time service does not synchronize the CMOS clock time to the Internet time on a Windows XP or Windows Server 2003-based computer after the W32Time service stops