Symmetricom®

Audit Server for Domain Time II

Verifiable Audit Trail of the Time Synchronization of Your Network

KEY FEATURES

- Automatically Audit the Time on Your Network

- Clear, Indisputable Records

- Generate Alerts if Time or Audit Period Exceeds Specified Tolerances

- Integrates Perfectly with DomainTime II Time Synchronization Software Suite

- Integrates with Existing Network Management Programs

- 64-bit and VISTA Support

KEY BENEFITS

- Complete Records of Time Synchronization Accuracy of the Computers on Your Network

- Know When a Machine was Last Synchronized, with What Time Source, as Well as its Variance from the Reference Time Source

- Peace of Mind From an Automatic Software System Routinely Auditing Time on Your Network

- Know That You Will be Notified if Time or Audit Period is Out of Tolerance

- Cross Check Network Time with Independent Time Sources for Historical Validation
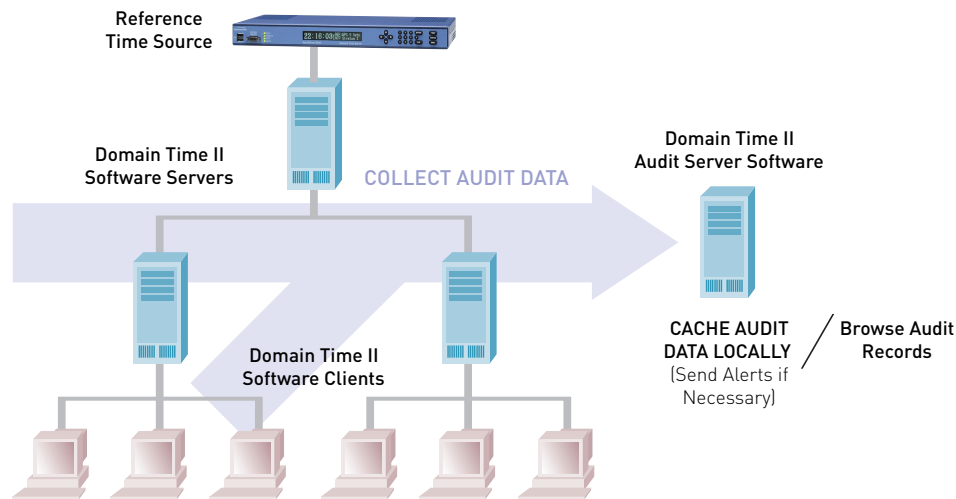
Audit Server is a software system designed to work in conjunction with Domain Time II time synchronization software components to provide a secure, verifiable audit trail of the time synchronization of your network. It automatically provides the clear, indisputable records you need to easily resolve any contested timestamp issue that may arise.

Federal regulatory agencies as well as major securities organizations like NASDAQ with their OATS (Order Audit Trail System) already require this type of audit collection to prevent fraud and to establish the validity of transactions. Audit Server meets or exceeds such requirements and makes it painless to comply with the regulations.

The records collected by Audit Server include complete information to allow auditors to determine precisely when a machine was last synchronized, with what time source, as well as its variance from the reference time source.

Audited Time is being able to prove conclusively (on demand) whether the time on any monitored system was correctly synchronized at a particular time and date with a specified time source.

Audit Server uses the built-in time synchronization and data collection capabilities of the Domain Time II time synchronization products (Domain Time II Server and Clients) to construct and maintain a verifiable and

Reference Time Source

Domain Time II Software Servers

COLLECT AUDIT DATA

Domain Time II Audit Server Software

Domain Time II Software Clients

CACHE AUDIT DATA LOCALLY (Send Alerts if Necessary)

Browse Audit Records

FIG. 1 Audit Server gathers data from Domain Time II clients and servers, generates alerts if necessary, and makes audit records available for browsing and archiving.
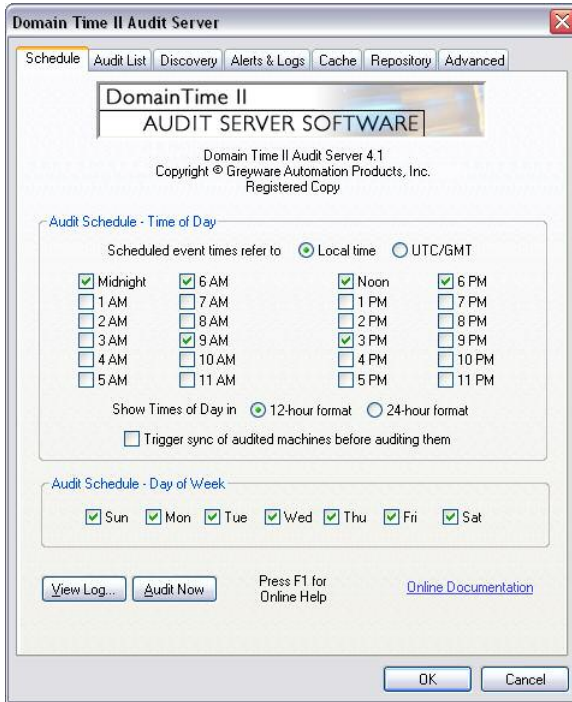
FIG. 2 Specify the schedule when you want Audit Server to audit your network time synchronization.

secure audit trail indicating when the clock on a machine was last synchronized. Domain Time II components all work together to easily and automatically provide Audited Time on your network with minimal intervention on your part.

TO SUCCESSFULLY PROVIDE AUDITED TIME...

- *Monitored machines must be able to be reliably and individually identified*

- *Time on individual machines must be synchronized regularly and accurately with a known time source*

- *Vital information such as when the local clock was last adjusted and with what time source must be easily retrievable*

- *Sync information must be collected regularly and compiled into concise and complete audit records*

IDENTIFYING MONITORED MACHINES

All Domain Time II Server and Client services are individually identified using a unique serial number that is assigned when the Domain Time software is installed. Even if the IP address or name

of the machine changes, the audit records will clearly identify the machine running that particular instance of Domain Time II.

ACCURATE AND RELIABLE NETWORK SYNCHRONIZATION

A Domain Time II Server connects securely to a trusted network time source such as a Symmetricom dedicated GPS referenced network time server, and then distributes that time accurately and verifiably to every time-aware machine on the network using the Domain Time II time distribution system.

In addition, Domain Time II components have a function called Clock Change Monitor that prevents users from manually changing the time on machines to falsify records. Domain Time II also has sophisticated security features to ensure that the entire system time is correct, including protection from rogue time servers, Denial-of-Service attacks, and more.

RETRIEVAL OF VITAL TIME SYNC INFORMATION

Domain Time Servers and Client services keep detailed internal statistics on their operation which is regularly queried by Audit Server. The statistics include such information as the name/IP address and
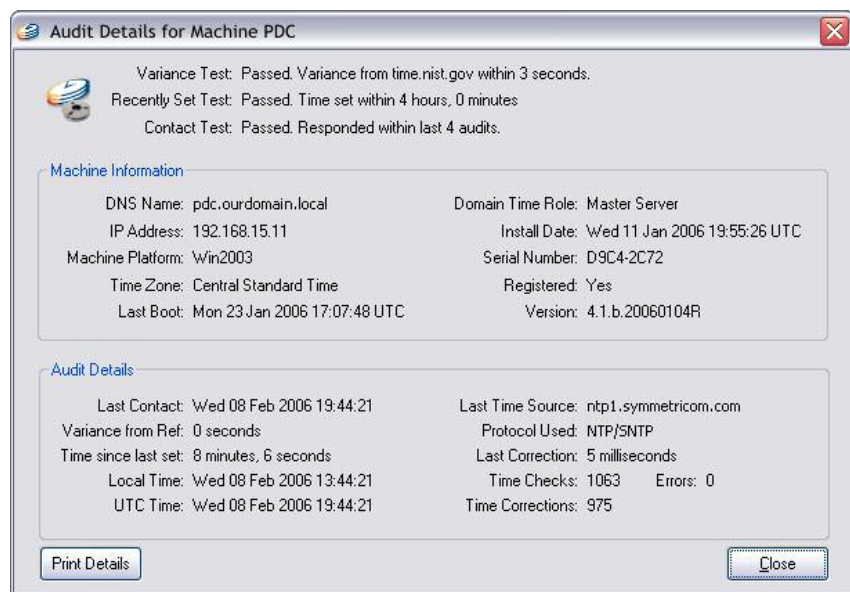

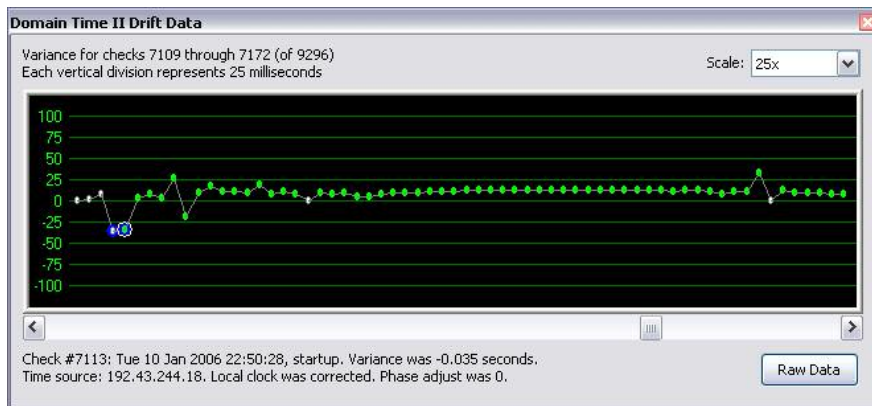FIG. 3 Sample of the information contained in an individual audit record.

FIG. 4 Numeric log data can also be viewed graphically as well as in text form to analyze time drift data.

time of the last time source used for synchronization, the amount of correction to the local clock that was made, the protocol used to set the time, etc. Statistics are regularly retrieved from clients and servers using the Domain Time II protocol, which allows for efficient transfer of the information to the Audit Server, with a very small amount of traffic. This means that the audit process is very low-overhead and has minimal impact on the network.

Audit Server can also obtain the current time from an NTP time source at the time an audit occurs. This allows the audit record to include at least basic information from any NTP machines (such as a GPS based network time server or router) that may also be involved in providing time to the network. This also can serve as a time cross check and historical valididation if you also monitor an official public time source.

REGULAR COLLECTION OF AUDIT RECORDS
The Audit Server automatically contacts Domain Time II Servers and Clients (and any specified NTP servers) to collect their audit data on a schedule you specify.

This information is compiled into compact record files that include all relevant information about each monitored system. Each record is optimized to minimize the amount of disk space used to retain the records. The Audit Record Viewer allows you to view the data in an easy-to-read format, and to extract the data to text files in a summary or full-detail form.

AUTOMATIC ERROR NOTIFICATION
Audit Server verifies that machines you have selected to be audited are actually having their time set and that they are responding to the audits. If any machine fails to be synchronized within your desired tolerance, or if a machine misses more audits than your specified maximum error limit, an email alert is automatically generated so that the problem can be addressed immediately.

INTEGRATION WITH EXISTING NETWORK MANAGEMENT SYSTEMS
Audit Server can create a special summary log of audit records each day if you are using your own log file collection and analysis program and need the audit record information to appear in a particular format to be imported correctly. This allows Audit Server to do its work yet you can continue to use your preferred network management system to monitor the network.

DOCUMENTATION
• All documentation is online at
  http:\\dtdocs.ntp-systems.com

SYSTEM REQUIREMENTS
• Requires Domain Time II Server and Clients (version 4.1 or later) to be installed.
• Windows NT/2K/XP/2003Vista*

* Native 64-bit support for XP/2003/Vista on AMD64 or Intel EM64T (x64) processors. (no Intel Itanium support)