Tivoli Compliance Insight Manager Glossary

Frequently used list of key terms used in Tivoli Compliance Insight Manager.

Actuator: A piece of software that automates the collection of logs from event sources and transmits the logs to the Depot. The actuator is also called the Point of Presence.

Aggregation Database: Data and statistics, spanning a longer period, are maintained by a process called aggregation. The aggregation process builds a special database called the aggregation database, which is used for trend and summary reports.

Chunk: Data structure of the archived log files in the Depot. A chunk consists of a header file and one or more data files.

Collect History Report: Tivoli Compliance Insight Manager report that documents log collection events.

Compliance Dashboard: The iView graph that shows the intersection of two W7 groups and their level of compliance with company policy.

Compliance Module: Tivoli Compliance Insight Manager regulation-specific reporting interface.

Depot: Tivoli Compliance Insight Manager secure storage facility for storing and archiving logs.

Enterprise Server: A server that provides centralized log management, performs forensic searches of the log archives, and creates reports.

Event Source: Each Operating System or application from which Tivoli Compliance Insight Manager collects log files (also called audit trails).

GEM (Generic Event Module) Databases: Reporting databases that contain the logs from different event sources.

Tivoli Compliance Insight Manager Cluster: The combination of an Enterprise server, one or more Standard servers, and a collector in a network deployment. A cluster can contain a maximum of three standard servers.

Tivoli Compliance Insight Manager Web Portal: Tivoli Compliance Insight Manager single sign-on user interface provides access to iView, the Policy Generator, Log Manager (only on the Enterprise server), Scoping, and Compliance Modules.

Tivoli Compliance Insight Manager Server: A generic term referring to the Tivoli Compliance Insight Manager engine that collects, archives, and normalizes log data using the W7 methodology. There are two types of Tivoli Compliance Insight Manager servers:

- Standard

- Enterprise

Tivoli Compliance Insight Manager Suite: The Tivoli Compliance Insight Manager Suite refers to the entire Tivoli Compliance Insight Manager application. This includes the Tivoli Compliance Insight Manager server, Point of Presence, analysis engine, Web Portal, iView, Log Manager, and the Compliance Modules.

iView: Tivoli Compliance Insight Manager user interface for compliance reporting.

Logs or **Audit Trails:** The system records that document all activity that occurred on the audited machine.

Log Chunk: The set of events placed in the Depot by the collect mechanism.

Log Collection Event: Each instance of collecting an audit trail, or log chunk, from an audited machine is called a log collection event.

Log Continuity Report: Tivoli Compliance Insight Manager report that documents log continuity status.

Log Manager: Tivoli Compliance Insight Manager centralized log collection, management, and reporting interface. The Log Manager is only available on the enterprise server.

Management Console: Enables you to load data into the databases, add new audited machines and event sources, configure collection and reporting schedules, and add and configure users.

Normalization: The process of standardizing log data by describing them in a single, uniform language.

Point of Presence: A piece of software that automates the collection of logs from event sources and transmits the logs to the Depot. The Point of Presence is also called the actuator.

Policy Exceptions: Actions or network activity that violate company policy.

Policy Generator: Tivoli Compliance Insight Manager tool that can be used to create policies using existing logs to set a baseline for acceptable network activity.

Remote Collect: Agentless log collection facilitated by **ssh** or by **NetBIOS** for Windows.

Scoping: Enables you to define limited access for certain users or for certain groups of users.

Special Attentions: Actions or network activities that may not violate company policy but are suspicious and require additional attention.

Standard Server: The Tivoli Compliance Insight Manager server that collects, archives, and normalizes log data, and generates reports.

W7 Methodology: Tivoli Compliance Insight Manager patent-pending normalization methodology, which translates log files into an English-based language of who, what, on what, when, where, where from, and where to.

