US007594267B2

(12) **United States Patent**
Gladstone et al.

(10) **Patent No.: US 7,594,267 B2**
(45) **Date of Patent: Sep. 22, 2009**

(54) **STATEFUL DISTRIBUTED EVENT PROCESSING AND ADAPTIVE SECURITY**

(75) Inventors: **Philip J. S. Gladstone**, Framingham, MA (US); **Jeffrey A. Kramer**, Wellesley, MA (US)

(73) Assignee: **Cisco Technology, Inc.**, San Jose, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 768 days.

(21) Appl. No.: **10/172,305**

(22) Filed: **Jun. 14, 2002**

(65) **Prior Publication Data**

US 2002/0194495 A1 Dec. 19, 2002

Related U.S. Application Data

(60) Provisional application No. 60/298,592, filed on Jun. 14, 2001.

(51) **Int. Cl.**

G06F 7/04	(2006.01)
G06F 9/00	(2006.01)
G06F 11/00	(2006.01)
H04N 7/16	(2006.01)

(52) **U.S. Cl.** **726/23**; 726/11; 726/27; 725/25

(58) **Field of Classification Search** 713/190–210, 713/189; 726/23, 22, 11, 27; 709/223; 725/25
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,647,944	A *	3/1987	Gravesteijn et al.	347/264
5,039,980	A *	8/1991	Aggers et al.	340/506
5,107,249	A *	4/1992	Johnson	340/541
5,761,502	A *	6/1998	Jacobs	707/103 R
6,282,175	B1 *	8/2001	Steele et al.	370/254
6,321,338	B1 *	11/2001	Porras et al.	726/25
6,405,250	B1 *	6/2002	Lin et al.	709/224
6,412,003	B1 *	6/2002	Melen	709/225
6,496,575	B1 *	12/2002	Vasell et al.	379/102.05
6,691,244	B1 *	2/2004	Kampe et al.	714/4
6,708,212	B2 *	3/2004	Porras et al.	709/224
6,839,850	B1 *	1/2005	Campbell et al.	726/23

(Continued)

FOREIGN PATENT DOCUMENTS

WO	WO 99/60462	11/1999

(Continued)

OTHER PUBLICATIONS

Anita K. Jones and Robert S. Sielken ; Computer System Intrusion Detection: A Survey; University of Virginia, 2000.*

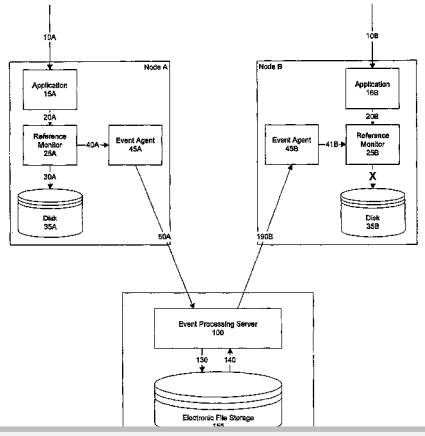
(Continued)

Primary Examiner—Nasser G Moazzami
Assistant Examiner—Mohammad W Reza

(57) **ABSTRACT**

The invention provides method and apparatus for maintaining a networked computer system including first and second nodes and an event processing server, the method comprising the first and second nodes detecting changes in state, the event processing server receiving notification of the changes in state from the first and second nodes, the event processing server correlating changes in state detected in the first and second nodes, and the event processing server executing a maintenance decision which affects the first and second nodes. The detecting, transmitting, correlating, and executing occurs without human intervention.

41 Claims, 6 Drawing Sheets



U.S. PATENT DOCUMENTS

6,973,488	B1 *	12/2005	Yavatkar et al.	709/223
6,986,133	B2 *	1/2006	O'Brien et al.	717/173
6,988,208	B2 *	1/2006	Hrabik et al.	726/23
2002/0082886	A1 *	6/2002	Manganaris et al.	705/7

FOREIGN PATENT DOCUMENTS

WO	WO 01/31420	A2	5/2001

OTHER PUBLICATIONS

R Gopal; Layered model for supporting fault isolation and recovery; 2000.*

R Bueschkes, M Borning, D Kesdogan; Transaction-based Anomaly Detection; Workshop on Intrusion Detection and Network Monitoring, 1999.*

Anderson, Debra et al., "Next-generation Intrusion Detection Expert System (NIDES) A Summary," Technical Report SRI-CSL-95-07, Computer Science Laboratory, SRI International, May 1995, 47 pgs.

Neumann, Peter G. et al., "Experience with EMERALD to Date", 1st USENIX Workshop on Intrusion Detection and Network Monitoring, Santa Clara, California, Apr. 11-12, 1999, pp. 73-80.

Snapp, Steven R. et al., "DIDS (Distributed Intrusion Detection System)—Motivation, Architecture, and An Early Prototype", Proceedings of 14th National Computer Security Conference, Washington, D.C., Oct. 1991, pp. 167-176.

Spafford, Eugene H. et al., "Intrustion detection using autonomous agents", Computer Networks 34 (2000), pp. 547-570.

Wallach, Dan S. et al., "Understanding Java Stack Inspection", IEEE Proceedings of Security & Privacy, May 1998, pp. 1-12.

Vigna G, et al. "NetSTAT: A Network-Based Intrusion Detection Approach," Computer Security Applications Conference, 1998. Proceedings. 14th Annual Phoenix, AZ, USA Dec. 7-11, 1998, Los Alamitos, CA, USA, IEEE Comput. Soc, US, Dec. 7, 1998 pp. 25-34, XP010318630.

Experience with EMERALD to Date, Peter G. Neumann and Phillip A. Porras, Computer Science Laboratory, SRI International, Menlo Park, CA 94025-3493, 1st USENIX Workshop on Intrusion Detection and Network Monitoring Santa Clara, California, Apr. 11-12, 1999, pp. 73-80, BSNDOCID, XP-002230356.

Garcia, et al. "Boundry Expansion of Expert Systems: Incorporating Evolutionary Computation With Intrusion Detection Solutions," Proceedings IEEE Southeastcon 2001. Engineering the Future. Clemson, SC, Mar. 30-Apr. 1, 2001, IEEE Southeastcon, New York, NY: IEEE, US, Mar. 30, 2001, pp. 96-99, XP010542589.

A System for Distributed Intrusion Detection, Steven R. Snapp, et al. "A System for Distributed Intrusion Detection," COMPCON Spring 91. Digest of Papers San Francisco, CA, USA Feb. 25-Mar. 2, 1991, Los Alamitos, CA, USA, IEEE Comput. Soc, US, Feb. 25, 1991, pp. 170-176, XP010022505.

* cited by examiner

FIGURE 1.

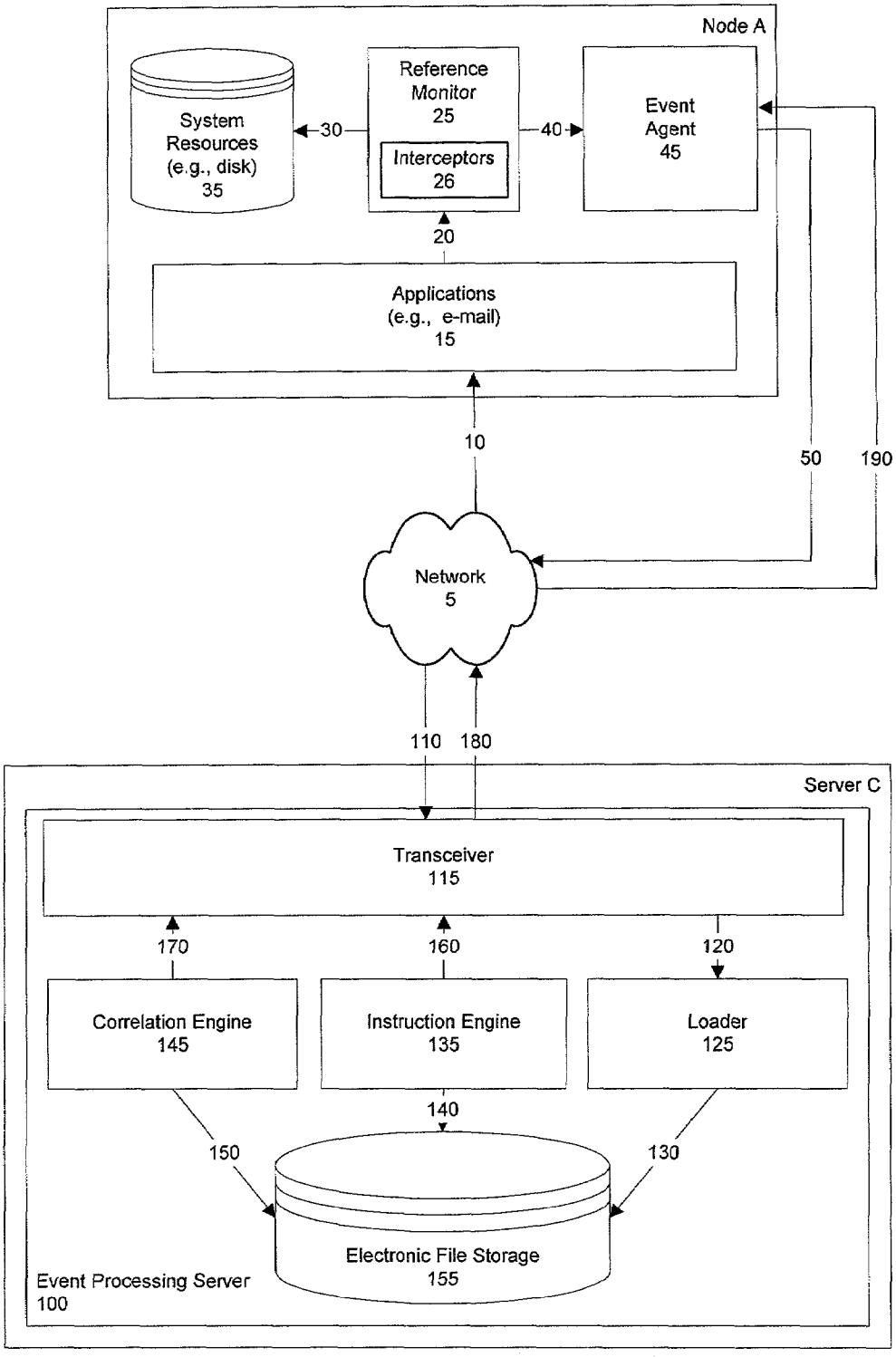


FIGURE 2.

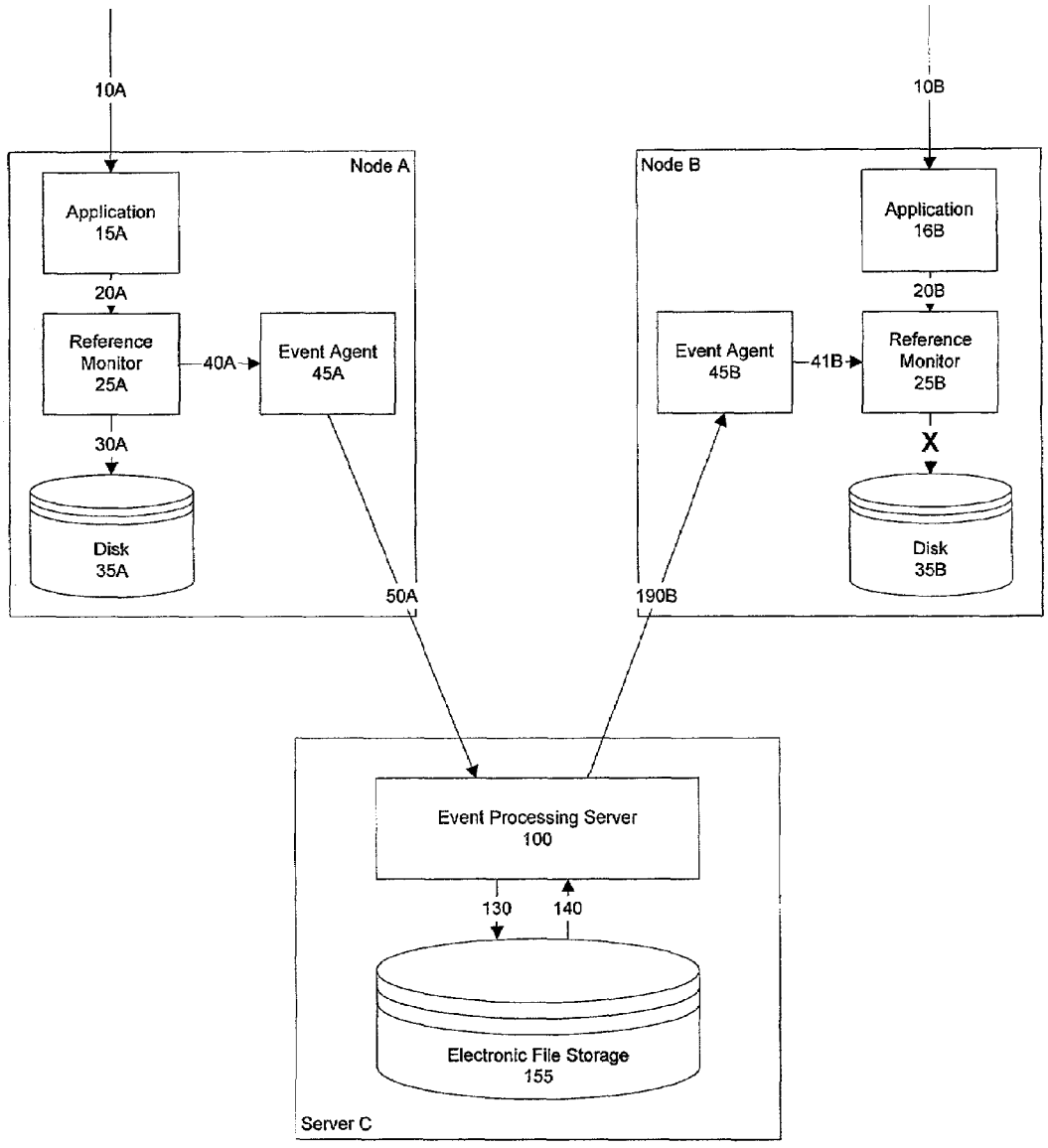
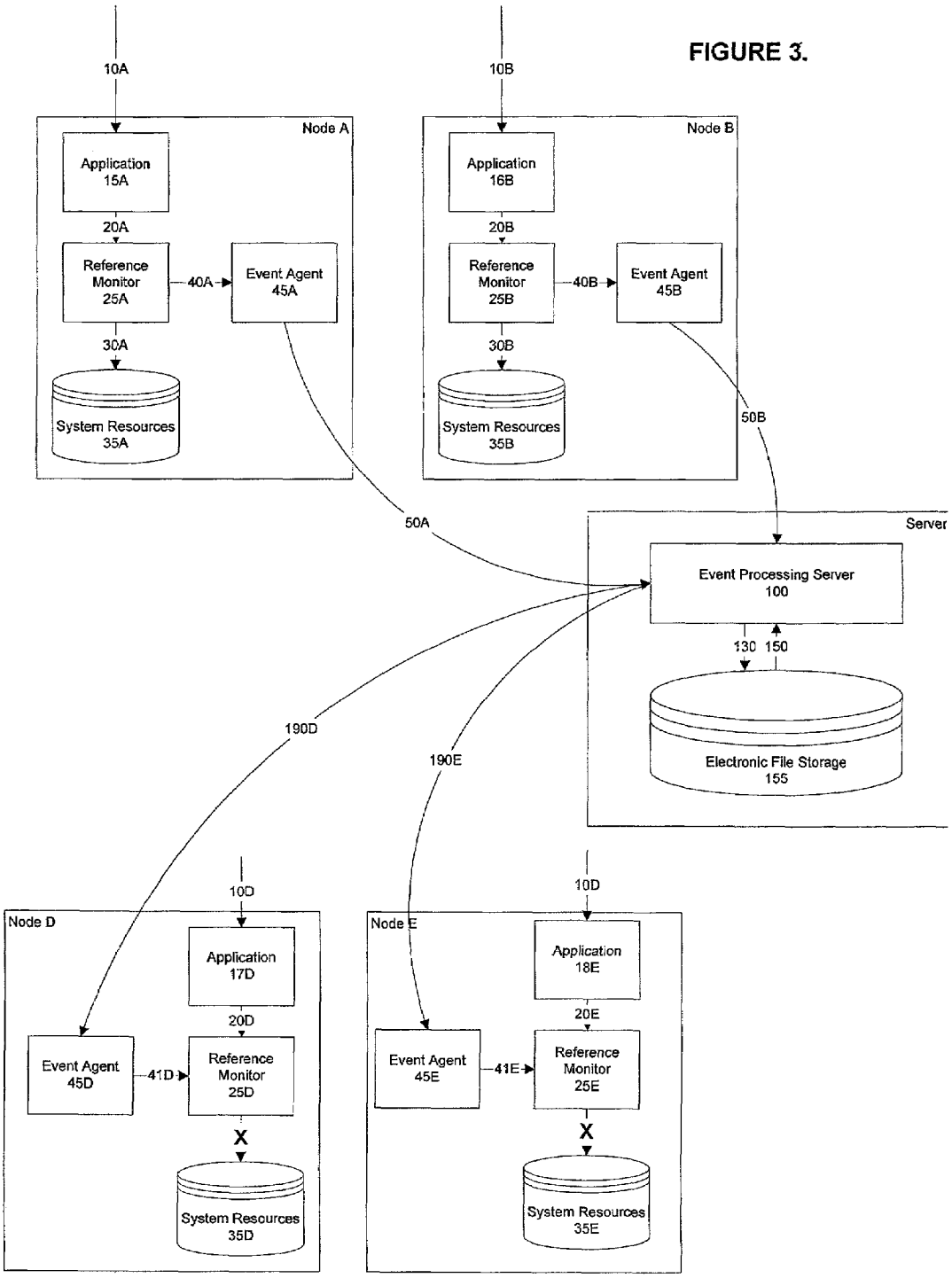


FIGURE 3.



DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.