(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 698 31 548 T2** 2006.06.14

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 913 966 B1**
(21) Deutsches Aktenzeichen: **698 31 548.0**
(96) Europäisches Aktenzeichen: **98 308 895.6**
(96) Europäischer Anmeldetag: **30.10.1998**
(97) Erstveröffentlichung durch das EPA: **06.05.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **14.09.2005**
(47) Veröffentlichungstag im Patentblatt: **14.06.2006**

(51) Int Cl.[8]: ***H04L 12/24*** (2006.01)
G06F 1/00 (2000.01)

(30) Unionspriorität:
962089 **31.10.1997** **US**

(84) Benannte Vertragsstaaten:
DE, FR, GB, NL, SE

(73) Patentinhaber:
Sun Microsystems, Inc., Palo Alto, Calif., US

(74) Vertreter:
Meissner, Bolte & Partner GbR, 80538 München

(72) Erfinder:
Angal, Rajeev, Santa Clara, California 95051, US; Allavarpu, Sai V.S., Pleasanton, California 94566, US; Bhat, Shivaram, Cupertino, California 95014, US; Fisher, Bart Lee, Sunnyvale, California 94086, US; Luo, Ping, Union City, US

(54) Bezeichnung: **Verteiltes System und Verfahren zur Zugriffskontrolle auf Netzwerkressourcen**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

[0001] Die vorliegende Erfindung betrifft primär das Management von Computernetzen und speziell ein System und ein Verfahren zur Begrenzung des Zugriffs auf die Managementobjekte eines Computernetzes auf berechtigte Benutzer der Netzmanagementobjekte.

HINTERGRUND DER ERFINDUNG

[0002] Das SNMP (einfaches Netzmanagementprotokoll) wurde entwickelt, um ein Werkzeug für ein herstellerneutrales, gemeinsam betreibbares Netzmanagement zu schaffen. Das SNMP bietet eine Menge von Standards für das Netzmanagement, umfassend ein Protokoll, eine Datenbankstrukturspezifikation und eine Menge von Datenobjekten. Das SNMP wurde 1989 als der Standard für Verbundnetze auf TCP/IP-Basis angenommen.

[0003] Eine Erläuterung der SNMP-Technologie geht über den Umfang des vorliegenden Dokuments hinaus, und es wird davon ausgegangen, daß der Leser entweder mit dem SNMP vertraut ist oder Zugang zu herkömmlichen Lehrbüchern über den Gegenstand hat wie etwa William Stallings, "SNMP, SNMPv2 and RMON", Addison Wesley (1996), das hier insgesamt als Hintergrundinformation eingeführt wird.

[0004] CMIP (Netzverwaltungsinformationsprotokoll) ist ein Netzmanagementprotokoll wie SNMP, basiert jedoch auf OSI-Standards. Das Buch: "SNMP, SNMPv2 and CMIP: The Practical Guide to Network Management Standards" von William Stallings, das eine ausgezeichnete Quelle für Basisinformation über CMIP und über auf CMIP bezogene Standards ist, wird hier insgesamt als Hintergrundinformation eingeführt.

[0005] Viele Netze verwenden einen Netzmanager und irgendeine Form von SNMP oder CMIP zur Verwaltung des Netzes. Als Teil seiner Managementaufgaben überwacht der Netzmanager automatisch den Status der Einrichtungen an dem Netz. Der Netzmanager sendet Ereignisanforderungen an die Einrichtungen, die aufgefordert werden, Antworten zu senden, wenn bestimmte Ereignisse eintreten. Beispielsweise kann ein Plattenspeicheragent aufgefordert werden, eine Antwort zu senden, wenn der verfügbare Plattenspeicherplatz unter 50 % fällt.

[0006] Eine mit SNMP verwaltungsfähige (oder mit CMIP verwaltungsfähige) Einrichtung speichert in ihrem Speicher eine Managementinformationsbasis MIB, eine Sammlung von Objekten oder Variablen, die verschiedene Aspekte der Einrichtung darstellen (z. B. Konfiguration, Statistiken, Status, Steuerung). Für jede Klasse von Einrichtung hat die MIB einen Kern von Standardvariablen. Jeder Hersteller einer Einrichtung fügt dem Kern Variablen hinzu, von denen er glaubt, daß sie für das Management seiner Einrichtung wichtig sind.

[0007] Die MIBs für die verwaltungsfähigen Einrichtungen in einem Netz speichern nicht nur Managementinformationen, die abgerufen werden können, sondern enthalten auch Variablen, deren Werte, wenn sie von einem Netzmanager modifiziert werden, die Operation der Einrichtung modifizieren. Einfache Beispiele sind das Sperren des Betriebs einer Einrichtung, Ändern der Prioritäten, die verschiedenen von einer Einrichtung ausgeführten Aufgaben zugewiesen sind, und Ändern der Menge von Meldungen, die von der Einrichtung erzeugt werden, und der Menge von Destinationen, an welche diese Meldungen gesendet werden.

[0008] Es ist offensichtlich wichtig zu verhindern, daß unberechtigte Personen Zugriff auf die Managementinformationsobjekte in einem Netz erhalten. Andernfalls erhalten unberechtigte Personen nicht nur vertrauliche Informationen, sondern das Netz wäre auch offen für Sabotagehandlungen. Die vorliegende Erfindung befaßt sich mit dem Gegenstand der Zugangssteuerung für Netzmanagementinformationsobjekte.

[0009] ITU-T X.741 (1995) ist ein Industriestandard, veröffentlicht von dem Telekommunikations-Standardisierungsbereich der International Telecommunication Union, früher bekannt als CCITT, mit dem Titel Data Networks and Open System Communications, OSI Management. Der Standard X.741 spezifiziert ein Zugriffssteuerungssicherheitsmodell und die Managementinformation, die notwendig ist, um eine Zugriffssteuerung im Zusammenhang mit OSI-Systemmanagement (OSI=offene Kommunikation) zu erschaffen und anzuwenden.

[0010] Es gibt eine Reihe von verwandten ITU-T-Standards, die das OSI-Systemmanagement betreffen und für die vorliegende Erfindung relevant sind, insbesondere X.740 (1992) (Sicherheitsauditleitwegfunktion) und X.812 (1995) (Kommunikationssicherheit für Datennetze und offene Systeme).

[0011] Die Standards X.741, X.740 und X.812 definieren ein recht umfassendes Zugriffssteuerrahmenwerk zur Steuerung des Zugriffs auf Netzmanagementobjekte, es verbleiben jedoch zahlreiche Aspekte der Zugriffssteuerung und des Managements, die von diesen Standards nicht berührt bzw. nicht gelöst werden.

[0012] Wenn insbesondere ein Netz zehntausende oder hunderttausende Komponenten (hier als Objekte bezeichnet) hat, kann die Anwendung eines einzigen Managementservers zur Verarbeitung sämtlicher

Zugriffsanforderungen zu Serviceengpässen führen. Die oben erörterten Standards befassen sich nicht mit der Aufgabe der effizienten Verwaltung der Zugriffssteuerung auf Managementobjekte in großen Netzen.

[0013] Beispiele der vorliegenden Erfindung ermöglichen ein verteiltes Zugriffssteuersystem, das auf effiziente Weise große Mengen von Zugriffsanforderungen an ein großes Netz abwickeln kann, das zehn- oder hunderttausende von Managementobjekten hat.

[0014] Der Standard X.741 und die verwandten Standards definieren die Zugriffssteuerung zur Begrenzung des Zugriffs auf Managementobjekte, aber diese Standards befassen sich nicht bzw. beschreiben nicht einen Mechanismus zur Begrenzung des Zugriffs auf Ereignisberichte. Ereignisberichte (die gewöhnlich als Ereignisbenachrichtigungen bezeichnet werden) wie etwa die Mitteilungen, die erzeugt werden, wenn ein Objekt erschaffen wird, gelöscht wird oder ein Managementparameter einen bestimmten Schwellenwert überschreitet, werden in vielen System an sämtliche Empfangsstationen übertragen. Das ist offensichtlich nicht akzeptabel, wenn das Netz beispielsweise das Fernsprechvermittlungsnetz einer großen Telekommunikationsgesellschaft ist und die Ereignisbenachrichtigungen Ressourcen betreffen, die für einen bestimmten Kunden installiert sind oder genutzt werden. Das heißt also, Kunde A darf keine Möglichkeit haben, Ereignisbenachrichtigungen über Netzressourcen zu empfangen, die für den Kunden B genutzt werden.

[0015] Tatsächlich gehen X.741 und die verwandten Standards von der Annahme aus, daß die Ereignisbenachrichtigungssicherheit unter Anwendung eines Mechanismus implementiert werden sollte, der von dem Zugriffssteuermechanismus getrennt ist, der zur Begrenzung des Zugriffs auf Managementobjekte angewandt wird. Schließlich filtert die Steuerung des Zugriffs auf Managementobjekte ankommende Mitteilungen, die Zugriff auf Objekte anfordern, wogegen Ereignisbenachrichtigungen abgehende Mitteilungen sind.

[0016] Die Erfinder der vorliegenden Erfindung haben jedoch beobachtet, daß in vielen Fällen diejenigen Objekte, auf die der Zugriff durch eine Person verboten ist, auch die Objekte sind, von denen diese Person keine Ereignisbenachrichtigungen empfangen sollte. Unter erneuter Bezugnahme auf das obige Beispiel dürfen Angestellte des Kunden A auf Ereignisbenachrichtigungen für jedes der Objekte, die dem Kunden B zugeordnet sind, weder Zugriff haben noch Ereignisbenachrichtigungen empfangen.

[0017] Beispiele der vorliegenden Erfindung bieten daher ein integriertes Sicherheitssystem zur Begrenzung des Zugriffs auf Managementobjekte und Ereignisbenachrichtigungen.

[0018] Schließlich fordern Kunden großer Netze die Möglichkeit zum Erzeugen von Netzmanagementmitteilungen unter Verwendung von Mitteilungsgeneratoren vom "SQL"-Typ (SQL=structured query language [Abfragesprache]). Das heißt, die Anwender solcher Netze verlangen die Fähigkeit zum Erzeugen von Mitteilungen über den Status ihrer Netzressourcen unter gleichzeitiger Vermeidung der Komplexitäten des Netzmanagementinformationsabrufs unter Anwendung von SNMP (oder eines anderen Netzmanagementprotokolls). X.741 und die verwandten Standards verlangen oder erwähnen keine Art von direktem oder SQL-Zugriff auf die Managementobjektdatenbank zum Zweck der Erzeugung von Managementbenachrichtigungen. Ein direkter Zugriff vom SQL-Typ könnte sogar als im Gegensatz zu den Zielen von X.741 betrachtet werden, da dies eine potentielle Quelle von Sicherheitslücken ist.

[0019] Beispiele der vorliegenden Erfindung bieten ferner direkten SQL-Zugriff auf die Managementobjektdatenbank für die Zweck der Erzeugung von Mitteilungen im Gegensatz zu anderen Arten von Objektzugriff. Der Zweck des Direktzugriffsmechanismus ist es, Anwendern die Verwendung von Standard-DBMS-Mitteilungsgeneratoren zu ermöglichen, um Benachrichtigungen über den Status oder die in der Vergangenheit liegende Leistung von Netzobjekten zu definieren und zu erzeugen, während gleichzeitig die gleichen Zugriffseinschränkungen wie diejenigen vorgesehen sind, die für normale Managementinformationszugriffsanforderungen gelten.

[0020] EP-A-0789301 beschreibt ein Verfahren zur Steuerung des Zugriffs auf die Datenbankobjekte, die für die Verwaltung eines Telekommunikationsnetzes relevant sind.

[0021] WO-98/00784-A (MCI Communications Corp.), veröffentlicht am 8. Januar 1998, beschreibt ein System und ein Verfahren zum direkten Berichten über Teilnehmerbedingungen von Telekommunikationsdiensten, an denen der Kunde teilnimmt. Dieses Dokument fällt unter Art. 54(3) EPU und ist für die Frage des erfinderischen Schritts nicht relevant. Das Dokument "Views for multilevel database security", Denning et al., IEEE Transactions on Software Engineering, Vol. 13, Nr. 2 (1. Feb. 1987), beschreibt die grundsätzlichen Betrachtungskonzepte für ein sicheres mehrstufiges relationales Datenbankmodell.

ZUSAMMENFASSUNG DER ERFINDUNG

[0022] Zusammenfassend stellt die vorliegende Erfindung ein System und ein Verfahren bereit zur Steuerung des Zugriffs auf Managementobjekte in einem

Computernetz, wie in Anspruch 1 bzw. Anspruch 6 angegeben ist. Ausführungsformen der vorliegenden Erfindung umfassen eine Zugriffssteuerdatenbank, die Zugriffsrechte durch die Verwendung von Zugriffssteuerobjekten definiert. Die Zugriffssteuerobjekte umfassen Gruppenobjekte, die jeweils eine Gruppe und eine Menge von Benutzern definieren, die Mitglieder der Gruppe sind, und Regelobjekte. Einige der Regelobjekte spezifizieren jeweils eine Menge der Gruppenobjekte, eine Menge der Managementobjekte und Zugriffsrechte durch die Benutzer, die Mitglieder der durch die spezifizierte Menge der Gruppenobjekte definierten Gruppen sind, für die spezifizierte Menge von Managementobjekten.

[0023] Ausführungsformen umfassen ferner eine Vielzahl von Zugriffssteuerservern, die zur Verarbeitung von Zugriffsanforderungen dienen. Jeder Zugriffssteuerserver steuert den Zugriff auf eine bestimmte Teilmenge der Managementobjekte gemäß den in der Zugriffssteuerdatenbank spezifizierten Zugriffsberechtigungen. Mindestens einer von den Zugriffssteuerservern empfängt Zugriffsanforderungen von den Benutzern und verteilt die empfangenen Zugriffsanforderungen unter den Zugriffssteuerservern zur Verarbeitung. Eine Teilmenge der Zugriffsanforderungen spezifiziert Operationen, die an spezifizierten Mengen der Managementobjekte auszuführen sind. Jede dieser Anforderungen wird zur Verarbeitung an einen oder mehrere von den Zugriffssteuerservern gesendet gemäß den Managementobjekten, für die Zugriff angefordert wird.

[0024] Die Zugriffssteuerserver reagieren auf die Zugriffsanforderungen von den Benutzern, indem sie den in jeder Zugriffsanforderung angeforderten Zugriff gemäß den in der Zugriffssteuerdatenbank spezifizierten Zugriffsberechtigungen gewähren, ablehnen und teilweise gewähren und ablehnen.

[0025] Weitere Ausführungsformen der vorliegenden Erfindung sehen vor, daß einer von den Zugriffssteuerservern ein Managementinformationsserver ist, der die von Benutzern an das Zugriffssteuersystem übermittelten Zugriffsanforderungen empfängt. Der Managementinformationsserver unterteilt eine Zugriffsanforderung in zwei oder mehr Zugriffs-Teilanforderungen, wenn der Zugriff zu der Menge von Managementobjekten, die durch die Zugriffsanforderung spezifiziert werden, von zwei oder mehr von den Zugriffssteuerservern gesteuert wird, und sendet die Zugriffs-Teilanforderungen an diese zwei oder mehr Zugriffssteuerserver zur Verarbeitung. Der Managementinformationsserver kombiniert außerdem Antworten auf die zwei oder mehr Zugriffs-Teilanforderungen, die von den zwei oder mehr Zugriffssteuerservern nach Verarbeitung der Zugriffs-Teilanforderungen erzeugt werden, und sendet eine kombinierte Antwort an den Benutzer zurück, der die Zugriffsanforderung, die unterteilt wurde, übermittelt hat.

[0026] Eine zweite Teilmenge der Regelobjekte in der Zugriffssteuerdatenbank kann verwendet werden, um Zugriffsberechtigungen zu den Zugriffssteuerobjekten zu spezifizieren. Ein Zugriffssteuerdatenbankserver speichert die Zugriffssteuerdatenbank dauerhaft, empfängt Zugriffsanforderungen für die Zugriffssteuerobjekte, und die Zugriffsanforderungen für das Zugriffssteuerobjekt werden von ihm gemäß den in der Zugriffssteuerdatenbank spezifizierten Zugriffsberechtigungen gewährt und abgelehnt.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0027] Weitere Ziele und Merkmale von Beispielen der Erfindung ergeben sich aus der nachstehenden genauen Beschreibung und den beigefügten Patentansprüchen im Zusammenhang mit den Zeichnungen; diese zeigen in:

[0028] Fig. 1 ein Blockbild einer Zugriffssteuermaschine zur Begrenzung des Zugriffs auf die Managementobjekte in einem Netz;

[0029] Fig. 2 die Datenstruktur einer Zugriffsanforderung;

[0030] Fig. 3 eine verteilte Zugriffssteuermaschine (ACE) gemäß einer bevorzugten Ausführungsform der vorliegenden Erfindung;

[0031] Fig. 4 die Zugriffssteuerdatenbank und einen Mechanismus zum Hinzufügen von Objekten zu der Datenbank und zum Modifizieren der bereits in der Datenbank befindlichen Objekte;

[0032] Fig. 5 die Reihenfolge, in der Zugriffsregeln angewandt werden, um jede Zugriffsanforderung zu verarbeiten;

[0033] Fig. 6 einen Ablauf zum Verarbeiten einer Zugriffsanforderung, Aufteilen derselben unter den zuständigen Zugriffsservern, Sortieren der Antworten und Rücksenden einer kombinierten Antwort an den Anfordernden;

[0034] Fig. 7 eine Übersicht, die zeigt, wie Zugriffsanforderungsantworten kombiniert werden, wenn das Ziel einer Zugriffsanforderung mehr als ein Managementobjekt umfaßt;

[0035] Fig. 8 die Ereignisregistratur- und Ereignis-Routerbereiche eines Managementinformationsservers in einer bevorzugten Ausführungsform der vorliegenden Erfindung;

[0036] Fig. 9 einen zusätzlichen Zugriffsmechanismus für den Nur-Lese-Zugriff vom SQL-Typ auf Protokollaufzeichnungen, die Ereignisbenachrichtigungen betreffen, die von Managementobjekten erzeugt wurden, während gleichzeitig die gleichen Sicher-

heitseinschränkungen für den Zugriff auf Managementobjektinformation aufrechterhalten werden, die von dem Managementinformationsserver für das Netz vorgegeben sind.

BESCHREIBUNG DER BEVORZUGTEN AUSFÜHRUNGSFORMEN

[0037] Fig. 1 zeigt ein Netzmanagementsystem **100**, das eine Zugriffssteuermaschine (ACE) **102** hat, die den Zugriff durch Initiatoren **104** (z. B. Benutzer und im Auftrag von Benutzern handelnde Anwendungsprogramme) auf die Managementobjekte in einem Netz **106** beschränkt. Das Netz **106** kann praktisch jede Art von computer-implementiertem Netz sein, das ein Managementprotokoll verwendet, um Managementfunktionen auszuführen. Für die Zwecke des vorliegenden Dokuments werden nur die Managementobjekte in dem Netz betrachtet, die Managementinformation und Ressourcensteuerungs-Variablen enthalten. Außerdem werden für die Zwecke des vorliegenden Dokuments primär Methoden der Zugriffsbegrenzung auf Managementobjekte und auf von Managementobjekten erzeugte Ereignisbenachrichtigungen betrachtet, und es wird keine spezielle Aufmerksamkeit auf den Inhalt und die Funktionen der Managementobjekte gelegt.

[0038] Es ist zu beachten, daß in vielen Dokumenten Managementobjekte als "gemanagte Objektinstanzen" (MOIs) bezeichnet werden. In diesen Dokumenten stehen die Abkürzungen "OI" und "OC" für "Objektinstanz" und "Objektklasse". In der Terminologie des vorliegenden Dokuments ist ein Objekt tatsächlich eine Objektinstanz, weil jedes Objekt eine Instanz einer jeweiligen Objektklasse ist. Beispielsweise ist jedes "Router-Managementobjekt" in einem Netz eine Instanz einer jeweiligen Router-Managementobjektklasse. Im vorliegenden Dokument wird – außer wenn es aus Gründen der Klarheit notwendig erscheint – der Ausdruck "Objekt" anstelle von "Objektinstanz" verwendet. Außerdem sind bei der bevorzugten Ausführungsform sämtliche Managementobjekte und Zugriffssteuerobjekte GDMO-konform (GDMO = Guidelines for Definitions of Managed Objects).

[0039] Die Zugriffssteuermaschine enthält eine Zugriffssteuerdatenbank **108**. Ebenso wie das Netz selber besteht die Zugriffssteuerdatenbank **108** aus einer Hierarchie von Objekten. Verschiedene Aspekte der Zugriffssteuerdatenbank gemäß der Implementierung in der vorliegenden Erfindung werden nachstehend im einzelnen erläutert. Die Zugriffssteuerdatenbank **108** enthält Zugriffssteuerregeln, die auf Zugriffsanforderungen anwendbar sind, um zu bestimmen, ob diese Anforderungen abgelehnt oder gewährt werden sollen.

[0040] Eine Zugriffssteuer-Entscheidungsfunktion (ACDF) **110** ist der Vorgang (oder die Menge von Vorgängen), der die Zugriffssteuerregeln auf jede Zugriffsanforderung anwendet, um zu bestimmen, ob der angeforderte Zugriff auf ein Managementobjekt gewährt oder abgelehnt werden sollte. Wenn, wie noch im einzelnen erläutert wird, eine Zugriffsanforderung ein Ziel von mehr als einem Managementobjekt hat, können einige Teile einer Zugriffsanforderung gewährt werden, wogegen andere Teile abgelehnt werden.

[0041] Eine Zugriffssteuer-Erzwingungsfunktion (ACEF) **112** ist der Vorgang (oder die Menge von Vorgängen) zum Erzwingen der von der Zugriffssteuer-Entscheidungsfunktion (**110**) getroffenen Entscheidungen. Dabei sendet die Zugriffssteuer-Erzwingungsfunktion **112** Zugriffsablehnungsantworten, wenn die Zugriffssteuer-Entscheidungsfunktion **110** eine Zugriffsablehnung zurücksendet, und leitet die Zugriffsanforderung an die entsprechenden Netzmanagementobjekte weiter, wenn der Zugriff gewährt wird.

[0042] Gemäß Fig. 2 ist jede Zugriffsanforderung **120** eine Datenstruktur oder ein Objekt, das eine Menge von vordefinierten Feldern enthält, die folgendes aufweisen:

– Benutzerinformation, die den Anforderungsinitiator identifiziert;
– Operation, die der Typ von Operation ist, die an dem (den) spezifizierten Zielobjekten) auszuführen ist; definierte Operationen umfassen Beschaffen, Einrichten, Erschaffen, Löschen, Aktion, Filter, Vielfachobjektwahl sowie "Empfang von Mitteilungen von"; es ist zu beachten, daß die Operation "Empfang von Mitteilungen von"(an anderer Stelle in diesem Dokument gewöhnlich als "Ereignismitteilung" bezeichnet) keine der von X.741 definierten Operationen, sondern eine neue Operation ist, die von den Erfindern aus Gründen, die nachstehend noch erläutert werden, hinzugefügt wurde;
– Modus, gleich bestätigt oder unbestätigt, was anzeigt, ob der Managementinformationsserver Antwortmeldungen an den Initiator senden sollte oder nicht; wenn der Modul gleich unbestätigt ist, werden an den Initiator keine Antwortmitteilungen (z. B. Zugriffsablehnungsmitteilungen) gesendet; wenn der Modus gleich bestätigt ist, werden an den Initiator Antwortmitteilungen gesendet;
– synch, gleich "unteilbar" oder "bestmöglich"; wenn synch auf unteilbar eingestellt ist, wird eine Zugriffsanforderung, die sich auf mehr als ein Objekt richtet, abgebrochen, wenn irgendein Teil der Anforderung abgelehnt wird; wenn synch auf bestmöglich eingestellt ist, wird die Zugriffsanforderung an den Objekten, für die Zugriff gewährt wird, ausgeführt, und die entsprechenden Ergebnisse werden an den Initiator rückgeleitet; und
– Ziel, womit das Objekt oder die Objekte spezifi-

ziert werden, für die der Initiator Zugriff wünscht.

[0043] Das Ziel in der Zugriffsanforderung **120** ist durch drei Felder spezifiziert:

– Basisobjekt, bezeichnet ein bestimmtes Objekt in dem Netzmanagementobjektbaum;

– Umfang, bezeichnet den Bereich von Objekten über oder unter dem Basisobjekt in dem Baum, auf den Zugriff erfolgen soll; bei der bevorzugten Ausführungsform ist das Basisobjekt immer das Objekt in der Zielmenge, das der Wurzel am nächsten kommt, und der Umfang bezeichnet eine Anzahl von Objektbaumebenen unter dem Basisobjekt (d. h. weiter entfernt von der Wurzel), die als Teil der Zielmenge einzuschließen ist; und

– Filter, nennt eine Filterbedingung (z. B. könnte ein Filter bedeuten, daß nur Managementobjekte für Router in Menlo Park, Kalifornien, in die Zielmenge aufzunehmen sind) zur Begrenzung der Menge von Objekten, die in die Zielmenge aufzunehmen sind; das Filterfeld ist das Äquivalent eines "Wo"-Satzes in einer Datenbankabfrage. Ein Filter kann auch dazu dienen, die Art von Ereignismitteilungen zu spezifizieren, die der Benutzer empfangen möchte (z. B. SNMP- oder CMIP-Ereignismitteilungen).

[0044] Eine Anforderung, die eine Zielmenge von nur einem Objekt hat, weil das Umfangsfeld in der Anforderung ungenutzt ist, wird als "umfangsfreie" Anforderung angesehen. Eine Anforderung, die eine Zielmenge von mehr als einem Objekt hat, weil das Umfangsfeld in der Anforderung anzeigt, daß Zugriff auf mehr als ein Objekt erfolgen soll, wird als "Umfangs"-Anforderung angesehen.

Verteilung der Zugriffssteuerung auf mehrere Server

[0045] Gemäß Fig. 3 sind die Funktionen der Zugriffssteuermaschine **102** (Fig. 1) auf eine Vielzahl von Servern verteilt, um dadurch die Geschwindigkeit zu steigern, mit der die Zugriffssteuerung abgewickelt wird. Es versteht sich, daß die nachstehende Erläuterung von Fig. 3 kurze "Übersichts"-Erläuterungen der Funktionen enthält, die von einigen der in Fig. 3 gezeigten Systemkomponenten ausgeführt werden, und daß detailliertere Erläuterungen dieser Aspekte der Erfindung, die in den oben angegebenen Standards (z. B. X.741) nicht angegeben sind, in anderen Abschnitten des vorliegenden Dokuments aufgeführt werden.

[0046] In vielen Fällen wie etwa in Telefonnetzen ist die Zahl von Netzmanagementobjekten außerordentlich groß, die Zahl von Personen, die Zugriff auf die Managementobjekte anfordern, ist entsprechend groß ebenso wie das tägliche Volumen von Zugriffsanforderungen. Die meisten Zugriffsanforderungen sind relativ eng fokussiert. Beispielsweise verlangt eine typische Zugriffsanforderung Zugriff für die Managementobjekte eines bestimmten Typs an einem bestimmten Platz. Ein anderes Beispiel: Wenn ein Teil des Netzes für Reparaturen abgeschaltet werden muß, bezeichnet die Zielmenge für die Zugriffsanforderung die Managementobjekte für die abzuschaltenden Vorrichtungen. Andere Zugriffsanforderungen, insbesondere Anforderungen zum Sammeln von Statusinformation, können sehr große Zielmengen umfassen.

[0047] Ein Managementinformationsserver (MIS) **150** empfängt alle Managementobjektzugriffsanforderungen **120** und verteilt jede Anforderung oder Teile der Anforderung auf eine Menge von Zusatzservern **152** entsprechend dem Bereich (den Bereichen) des durch die Anforderung angesprochenen Managementobjektbaums. Jeder Server **150** und **152** führt sowohl Zugriffssteuerfunktionen als auch die Anforderungsantwortsammelfunktionen aus. Somit wird die Zugriffssteuerverarbeitung unter dem MIS **150** und den Zusatzservern **152** aufgeteilt, was eine raschere Verarbeitung von Zugriffsanforderungen in anforderungsstarken Zeiten ermöglicht.

[0048] Insbesondere führt der MIS **150** nur die Zugriffssteuerung für Objekte am oberen Ende des Managementobjektbaums aus, während jeder von den Zusatzservern die Zugriffssteuerung für Objekte in jeweils bezeichneten Teilbäumen des Managementobjektbaums ausführt. Eine wichtige Ausnahme der vorstehenden Angabe ist, daß alle Zugriffsanforderungen für Ereignisbenachrichtigungen (d. h. mit einer Operation von "Mitteilung empfangen von") an ein Ereignisregistrationsmodul in dem MIS gesendet werden, und zwar unabhängig davon, welche Objekte die Ziele der Zugriffsanforderung sind. Dies wird noch im einzelnen unter Bezugnahme auf die Ereignismitteilungszugriffssteuerung erörtert.

[0049] Außerdem wird ein spezieller Zusatzserver **154** verwendet, um sämtliche Aktualisierungen des Zugriffssteuerobjektbaums **170** abzuwickeln (der aus den noch zu erläuternden Gründen nicht der gleiche wie der bekannte Zugriffssteuerbaum **108** ist). Bei einigen Implementierungen kann der spezielle Zusatzserver **154** mit dem MIS **150** oder einem der regulären Zusatzserver **152** vereinigt sein. Alternativ kann in Systemen mit relativ geringem Zugriffsanforderungsverkehr der spezielle Zusatzserver **154** als eine separate Software-Entität an derselben physischen Serverhardware wie einer der anderen Server implementiert sein.

[0050] In jedem von dem MIS **150** und den Zusatzservern **152**, **154** ist eine vollständige Kopie des Zugriffssteuerobjektbaums **170** gespeichert, aber jeder dieser Server ist nur für die Verarbeitung von Anforderungen für den Zugriff auf einen jeweiligen Bereich des Netzmanagementobjektbaums zuständig. Bei einer alternativen Ausführungsform könnte in jedem

von dem MIS und den Zusatzservern nur der Bereich des Zugriffssteuerobjektbaums **170** gespeichert sein, der benötigt wird, um die zugewiesenen Zugriffssteuerfunktionen auszuführen.

[0051] Wenn eine Zugriffsanforderung Zielobjekte in den Bereichen des Managementobjektbaums hat, die von mehr als einem Server behandelt werden, wird die Zugriffsanforderung in Teil-Zugriffsanforderungen von dem MIS **150** aufgeteilt und zu den entsprechenden Zusatzservern **152** übermittelt. Die von allen Servern erzeugten Antworten auf die Teil-Zugriffsanforderungen werden von dem MIS **150** gesammelt und gemeinsam an den anfordernden Benutzer oder die anfordernde Anwendung zurückgeleitet.

[0052] Der MIS **150** weist folgendes auf:

– eine Schnittstelle **160** zum Empfang von Zugriffsanforderungen;
– eine oder mehrere Zentraleinheiten bzw. CPUs **162** zur Ausführung von im Speicher **164** des MIS gespeicherten Zugriffssteuerprozessen;
– einen Speicher **164**, der sowohl einen flüchtigen Hochgeschwindigkeits-RAM als auch einen nichtflüchtigen Speicher wie etwa einen Magnetplattenspeicher aufweist;
– eine Schnittstelle **166** zur Abwicklung von sicheren Verbindungen zwischen dem MIS **150** und den Zugriffssteuer-Zusatzservern **152**, **154**; und
– einen oder mehrere interne Busse **168** zum Übertragen von Daten und Programmen zwischen den oben genannten Elementen des MIS **150**.

[0053] In dem Speicher **164** kann gespeichert sein:

– eine teilweise oder vollständige Kopie **170** eines Zugriffssteuerbaums; es ist zu beachten, daß der Zugriffssteuerbaum **170** bei der bevorzugten Ausführungsform andere Komponenten und eine andere Organisation als in X.741 angegeben hat, und daher ist der Zugriffssteuerbaum **108** in Fig. 1 nicht gleich dem Zugriffssteuerbaum **170**, der bei der vorliegenden Erfindung verwendet wird;
– einen Zugriffsanforderungsaufteilungs- und -routingprozeß **172** zur Aufteilung von Zugriffsanforderungen in Zugriffs-Teilanforderungen an die entsprechenden Server für die Zugriffssteuerverarbeitung;
– einen Teilbaum zu einer Serverabbildungstabelle **173**, in der die Information gespeichert ist, die der MIS **150** benötigt, um den oder die Server zu bestimmen, an die jede Zugriffsanforderung zur Zugriffssteuerverarbeitung zu senden ist;
– eine Zugriffssteuer-Erzwingungsfunktion **174**, deren Funktionalität gleich derjenigen der in Fig. 1 gezeigten Zugriffssteuer-Erzwingungsfunktion **112** ist;
– eine Zugriffssteuer-Entscheidungsfunktion **176**, deren Funktionalität gleich derjenigen der Zugriffssteuer-Entscheidungsfunktion **110** von Fig. 1 ist;
– einen Anforderungsantwortkombinationsprozeß **178** zum Kombinieren der von den verschiedenen Servern auf jede einzelne Zugriffsanforderung erzeugten Antworten und Rücksenden einer einzigen kombinierten Antwort an den Initiator;
– ein Array **180** von Statusinformation über Zugriffsanforderungen, deren Verarbeitung noch nicht abgeschlossen ist;
– einen Sicherheitsauditleitweg **182**, um eine Aufzeichnung von allen Zugriffsanforderungen zu halten;
– eine Ereignisregistratur **184**, die ein Mechanismus ist, um Ereignismitteilungen zu verfolgen, die von bestimmten Benutzern angefordert wurden; und
– einen Ereignis-Router **186**, der ein Modul ist, um Ereignismitteilungen an Benutzer oder Anwendungen zu senden, die (A) diese Ereignismitteilungen angefordert haben und (B) berechtigt sind, diese zu empfangen.

[0054] Andere Aspekte des MIS **150**, die in Fig. 3 nicht gezeigt sind, werden nachstehend beschrieben.

[0055] Der MIS **150** und die Zusatzserver **152**, **154** halten sämtlich identische Kopien einer Bibliothek von Zugriffssteuerprozessen sowie eine Kopie des Zugriffssteuerobjektbaums **170**. Daher enthält jeder Zusatzserver **152**, **154** die gleichen Hardware- und Softwareelemente, die in dem MIS **150** vorhanden sind, mit Ausnahme von (A) den speziellen Prozessen (**172**, **178**) in dem MIS, die der Abwicklung des Empfangs und der Unterteilung von Zugriffsanforderungen und dem Kombinieren von Antworten dienen, und (B) hat jeder nur eine Schnittstelle **160**/**166** zum Empfang von Zugriffsanforderungen und Rückantworten. Jeder Zusatzserver **152** hält entweder eine vollständige Kopie **170** des Zugriffssteuerobjektbaums oder des Bereichs davon, der notwendig ist, um die von diesem Zusatzserver abzuwickelnden Zugriffsanforderungen abzuwickeln.

[0056] Der spezielle Zusatzserver **154** hält dauerhaft gespeichert eine Kopie **190** des Zugriffssteuerobjektbaums **170**, so daß die Zugriffssteuerobjekte zur Nutzung durch sämtliche Zugriffssteuerserver jederzeit verfügbar sind, wenn das Zugriffssteuersystem oder irgendwelche Teile davon aus irgendeinem Grund erneut gebootet oder neu gestartet werden. Der spezielle Zusatzserver **154** ist außerdem für die Abwicklung sämtlicher Aktualisierungen des Zugriffssteuerobjektbaums **170** zuständig.

[0057] Zusätzlich zu den Zugriffssteuerbibliotheksprozessen, die der spezielle Zugriffsserver **154** mit den anderen Servern teilt, hat er einen zusätzlichen Prozeß **194** zur Abwicklung der Zugriffssteuerung zu dem Zugriffssteuerobjektbaum **170**/**190** und zur Ab-

wicklung von Aktualisierungen des Zugriffssteuerobjektbaums **170**/**190**. Die gleiche Art von Zugriffssteuerung, die angewandt wird, um den Zugriff auf Managementobjekte zu begrenzen, wird auch angewandt, um den Zugriff auf den Zugriffssteuerobjektbaum **190**/**170** zu begrenzen. Das heißt, einige der Zielobjekte und Regelobjekte in dem Zugriffssteuerobjektbaum **170** werden verwendet, um Zugriffsberechtigungen zu den Zugriffssteuerobjekten zu definieren, und der spezielle Zusatzserver **154** beschränkt den Zugriff auf die Zugriffssteuerobjekte entsprechend den Regeln, die durch diese Zugriffssteuerobjekte definiert sind. Auf diese Weise können nur berechtigte Benutzer auf den Zugriffssteuerobjektbaum **190**/**170** zugreifen und diesen aktualisieren.

[0058] Der MIS **150** hat ein hinreichendes Wissen über den Objektbaum im Netz, um zu wissen, welche Zusatzserver benötigt werden, um jede Anforderung abzuarbeiten. Speziell hat der MIS **150** einen Zugriffsanforderungsunterteilungs- und -routingprozeß **172** und eine Abbildungstabelle **173**, die Information speichert, die eine Menge von "Baumunterteilungspunktobjekten" (auch als Unterteilungspunktknoten bezeichnet) bezeichnet. Dabei enthält die Abbildungstabelle **173** eine Folge von Aufzeichnungen. Jede Aufzeichnungen bezeichnet einen Managementobjekt-Teilbaum, identifiziert durch ein oberstes Objekt, das als Baumunterteilungspunktobjekt bezeichnet wird, und identifiziert ferner den Server **152** zur Abwicklung der Zugriffsanforderungen auf Objekte in diesem Managementobjekt-Teilbaum. Für jede Zugriffsanforderung wendet der MIS **150** zuerst die "globalen Ablehnungsregeln" an, wie nachstehend noch im einzelnen erläutert wird. Wenn die Anforderung nicht durch eine globale Ablehnungsregel abgewiesen wird, durchläuft der MIS den Netzobjektbaum **170**, um den oder die Server zu identifizieren, die erforderlich sind, um die Zugriffsanforderung weiter zu bearbeiten.

[0059] Dabei durchläuft der MIS für jede empfangene Zugriffsanforderung (außer Zugriffsanforderungen für Ereignisbenachrichtigungen) den Netzobjektbaum, bis er jedes von den Teilungspunktobjekten erreicht. Da alle Managementobjekte unter den Teilungspunktobjekten von einem jeweiligen Zusatzserver zu bearbeiten sind, hält die Baumdurchquerung an diesen Objekten an. In Abhängigkeit davon, wie die Zugriffsmanagementaufgaben unter den Servern aufgeteilt worden sind, ist es möglich, daß eine einzige Zugriffsanforderung in zwei oder mehr Teil-Zugriffsanforderungen aufgeteilt und an zwei oder mehr von den Servern für die weitere Verarbeitung gesendet werden muß. Wenn eine Anforderung für die Verarbeitung durch mehr als einen Server unterteilt wird, werden die Basisobjekt- und die Umfangsbereiche jeder Unterteilung der Zugriffsanforderung (d. h. jeder Teilanforderung) so modifiziert, daß sie nur den Bereich des Managementobjektbaums umfassen, der von dem entsprechenden Server verarbeitet wird.

[0060] Der MIS **150** unterhält außerdem Statusinformation **180** über jede Zugriffsanforderung, deren Verarbeitung noch nicht abgeschlossen ist. Die Statusinformation **180** bezeichnet alle Server, von denen Teilantworten benötigt werden, bevor eine komplette Antwort an den Initiator rückgeleitet werden kann.

[0061] In Abhängigkeit von der Implementierung kann der MIS **150** zusätzlich zur Anwendung der globalen Ablehnungsregel auf jede Anforderung auch zuständig sein zur Begrenzung des Zugriffs auf verschiedene Bereiche des Managementobjektbaums, die keinem der Zusatzserver zugewiesen sind. Beispielsweise ist der MIS **150** typischerweise zuständig für die Begrenzung des Zugriffs auf den Wurzelknoten des Managementobjektbaums und kann auch für jeden speziellen Zweig des Managementobjektbaums verantwortlich gemacht werden.

[0062] Bei einer alternativen Ausführungsform könnten die Verantwortlichkeiten für die Zugriffssteuerung unter den Servern auf andere Weise aufgeteilt sein, beispielsweise auf der Grundlage der Art von Operation, die an den Zielobjekten auszuführen ist. So könnte ein Server für die Abwicklung von Mengenoperationen zuständig sein, ein anderer könnte Operationen erschaffen und löschen, usw.

[0063] Die Zugriffssicherheitsregeln sind in dem MIS **150** und jedem Zusatzserver **152** dauerhaft gespeichert, wobei vor kurzem genutzte Bereiche auch im Cache-Speicher gespeichert sind. Immer dann, wenn eine Zugriffssteuerregel aktualisiert, gelöscht oder dem System hinzugefügt wird, wird die Regelbank in jedem Zusatzserver auf synchronisierte Weise aktualisiert unter Anwendung eines Ereignisfortpflanzungsmechanismus, der auch zur Abwicklung von anderen Arten von Ereignisbenachrichtigungen angewandt wird. Der Prozeß zur Aktualisierung des Zugriffssteuerbaums **108** wird nachstehend im einzelnen erläutert.

Die Zugriffssteuerdatenbank

[0064] X.741 gibt zwar an, daß der Objektzugriff auf benutzerweiser Basis gesteuert werden soll, die vorliegende Erfindung steuert jedoch den Objektzugriff auf gruppenweiser Basis. Das Benutzergruppen-Feature trägt dazu bei, die Datenmenge, die zur Definition jeder Zugriffsregel erforderlich ist, erheblich zu reduzieren. Jeder Benutzer, der berechtigt ist, für Information in dem System Zugriff zu erhalten, wird einer oder mehreren Gruppen zugewiesen. Zugriffsregeln sind in Form von Zugriffsberechtigungen von Gruppen definiert. Beispielsweise ist es wahrscheinlich, daß Objektparameterleseberechtigungen unter Anwendung von Gruppen zugewiesen werden,

die von Gruppen verschieden sind, denen Objektparametereinstellungsberechtigungen zugewiesen werden. Außerdem sind Regeln typischerweise hierarchisch in bezug auf diese Gruppen definiert, wobei beispielsweise der Zugriff auf den Objekt-Teilbaum des Kunden A jedem verwehrt wird, der nicht entweder ein Mitglied der Gruppe des Kunden A oder ein Systemadministrator-Gruppenmitglied ist, und ferner Berechtigungen für Objekte innerhalb des Teilbaums des Kunden A entsprechend Benutzergruppen definiert werden, die von dem Kunden A eingerichtet sind.

[0065] Gemäß Fig. 4 sind die Hauptkomponenten des Zugriffssteuerbaums **170** Gruppendefinitionen **200**, Benutzerdefinitionen **202**, Zieldefinitionen **204**, Zugriffsregeln **206** und Standardregeln **208**.

[0066] Jede Gruppendefinition **200** ist repräsentiert durch ein Gruppenobjekt, das die folgenden Felder hat:

– Gruppenname; und
– eine Liste von Benutzern, die in der Gruppe enthalten sind.

[0067] Die Gruppenobjekte werden verwendet, um Gruppen für Benutzer abzubilden.

[0068] Jeder Benutzerdefinition **202** ist dargestellt durch ein Benutzerobjekt mit den folgenden Feldern:

– Benutzername; und
– Liste von Gruppen, in denen der Benutzer Mitglied ist.

[0069] Die Benutzerobjekte werden verwendet, um sämtliche Gruppen zu bezeichnen, zu denen ein bestimmter Benutzer gehört.

[0070] Es ist dabei zu beachten, daß der Ausdruck "Benutzer" andere Entitäten umfaßt als Benutzer, denen Zugriffsrechte gewährt werden können. Beispielsweise können die Zusatzserver, der Protokollserver und sogar Objekte in dem System als "Benutzer" eingerichtet sein zum Zweck der Definition von Zugriffsrechten, die diesen Entitäten gewährt werden sollen.

[0071] Jede Zieldefinition **204** ist durch ein Zielobjekt dargestellt, das die folgenden Felder hat:

– Zielname; und
– eine Liste von Basismanagementobjekten, die in die Zielmenge aufzunehmen sind, die durch dieses Zielobjekt identifiziert ist;
– eine Liste von Managementobjektklassen; dieses Feld wird nur verwendet, wenn eine Zielmenge sämtliche Managementobjekte einer bestimmten Klasse umfaßt, vorbehaltlich der Filterbedingung (siehe unten);
– Umfang, bezeichnet die Anzahl von Managementobjektbaumebenen unter den aufgelisteten Basismanagementobjekten, die in die Zielmenge aufzunehmen sind; und
– einen Filter, der ein fakultatives Feld ist, das dazu dient, die Menge von Objekten, die in der Zielmenge enthalten sind, zu begrenzen; das Filterfeld ist das Äquivalent eines "Wo"-Satzes in einer Datenbankabfrage; und
– eine Liste von Operationen, welche die Operationen (Beschaffen, Einstellen, usw.) auflistet, auf welche die Zielmenge anwendbar ist.

[0072] Jede Regeldefinition **206** ist repräsentiert durch ein Regelobjekt, das die folgenden Felder hat:

– einen Regelnamen zur Bezeichnung der Regel;
– eine Gruppenliste, die sämtliche Benutzergruppen bezeichnet, auf welche die Regel anwendbar ist;
– eine Liste von Zielen, die eine Liste der Zielobjekte ist, auf welche die Regel anwendbar ist; und
– eine Erzwingungsaktion, die anzeigt, ob die spezifizierten Gruppen von Benutzern Zugriff auf die spezifizierte Zielmenge haben oder nicht; bei einer bevorzugten Ausführungsform kann die Erzwingungsaktion eingestellt sein auf Ablehnen mit Antwort, Ablehnen ohne Antwort oder Gewähren.

[0073] Standardregeln **208** sind dargestellt durch ein Standardregelobjekt, das die folgenden Felder hat:

– eine Liste von Standarderzwingungsaktionen für eine entsprechende vordefinierte Liste von Operationen (z. B. Beschaffen, Erstellen, Löschen usw.); die typischste Liste von Standarderzwingungsaktionen ist die Ablehnung des Zugriffs für alle Operationsarten, aber bei manchen Implementierungen kann der Systemadministrator entscheiden, den Standard für manche Operationen wie etwa die Beschaffungsoperation auf "Gewähren" zu setzen;
– eine Standarderzwingungsaktion für Ereignisbenachrichtigungen; und
– eine Standardablehnungsantwort (d. h. Ablehnen mit Antwort oder Ablehnen ohne Antwort).

[0074] Die Standards **208** sind Standardantworten, die für jede Operation definiert werden, wenn keine Regel definiert worden ist, die für eine bestimmte Zugriffsanforderung gilt. Beispielsweise könnten die Standards auf "Gewähren"-Zugriffsanforderungen gesetzt werden, deren Operation "Beschaffen" ist, und auf "Ablehnen mit Antwort"-Zugriffsanforderungen, deren Operation etwas anderes als "Beschaffen" ist. Es wird jedoch erwartet, daß in den meisten Implementierungen sämtliche Standards entweder auf "Ablehnen mit Antwort" oder "Ablehnen ohne Antwort" gesetzt werden. Die Standards **208** sind bevorzugt durch ein einziges Standardobjekt definiert, das ein Gewähren- oder Ablehnen-Flag für jede der definierten Operationen enthält.

[0075] Jede "Regel" in dem Zugriffssteuerbaum führt entweder zu einer Gewährung oder Ablehnung des Zugriffs durch bestimmte Benutzergruppen (identifiziert durch die in dem Regelobjekt bezeichneten Gruppenobjekte) für eine Menge von Zielobjekten, die durch ein in dem Regelobjekt bezeichnetes Zielobjekt spezifiziert sind. Anders als in X.741 sind Zugriffsregeln nicht auf einer benutzerweisen Basis, sondern statt dessen auf einer gruppenweisen Basis definiert. Infolgedessen brauchen, wenn bestimmte Benutzer in eine die vorliegenden Erfindung anwendende Firma eintreten oder diese verlassen, nur die Benutzer- und Gruppenobjekte aktualisiert zu werden und nicht sämtliche Regelobjekte, die auf diese Benutzer anwendbar waren.

[0076] Zusätzlich zu Regelobjekten, die eine Menge von Zielmanagementobjekten spezifizieren, kann das System ein globales Ablehnungsregelobjekt und ein globales Gewährungsregelobjekt haben. Jedes der globalen Regelobjekte hat die gleiche Struktur wie ein reguläres Regelobjekt, hat aber ein leeres Ziellistenfeld, was bedeutet, daß die Regel eine globale Regel ist. Wenn die globale Ablehnungsregel definiert ist, spezifiziert sie Gruppen von Benutzern, die keine Operationen an irgendwelchen Managementobjekten ausführen können. Wenn die globale Gewährungsregel definiert ist, spezifiziert sie Gruppen von "Superbenutzern" (z. B. Systemadministratoren), denen gestattet ist, alle Operationen an allen Managementobjekten auszuführen.

[0077] Immer dann, wenn ein Objekt in dem Zugriffssteuerbaum **170** hinzugefügt, gelöscht oder modifiziert wird, müssen eventuell andere Zugriffssteuerobjekte ebenfalls modifiziert werden, um den Zugriffssteuerbaum **170** selbst-konsistent zu halten. Wenn beispielsweise ein Benutzerobjekt modifiziert wird, um alle Gruppen zu löschen, die vorher in der Gruppenliste des Benutzerobjekts enthalten waren, um den identifizierten Benutzer zu einem Mitglied einer vorher definierten "Alle-Ablehnen"-Gruppe zu machen, müssen sämtliche Gruppenobjekte, die in dem Benutzerobjekt gewöhnlich aufgelistet waren, aktualisiert werden, um diesen Benutzer aus ihren Benutzerlisten zu löschen, und das Alle-Ablehnen-Gruppenobjekt muß aktualisiert werden durch Hinzufügen dieses Benutzers zu seiner Benutzerliste. Bei einem anderen Beispiel müssen, wenn ein Zielobjekt aus dem Zugriffsobjektbaum **170** gelöst wird, sämtliche Regelobjekte, die auf das gelöschte Zielobjekt bezogen waren, so modifiziert werden, daß das gelöschte Zielobjekt aus ihren Zielobjektlisten entfernt wird.

[0078] Um sicherzustellen, daß der Zugriffssteuerobjektbaum **170** in einem selbst-konsistenten Zustand gehalten wird, werden alle Änderungen an dem Zugriffssteuerobjektbaum **170** durch einen Prozeß ausgeführt, der als Zugriffssteuerkonfigurationsprozeß **210** bezeichnet wird. Der Zugriffssteuerkonfigurationsprozeß **210** sieht eine grafische Anwenderschnittstelle **212** für Benutzer vor, die berechtigt sind, den Zugriffssteuerbaum **170** zu modifizieren. Der Zugriffssteuerkonfigurationsprozeß **210** gestattet dem berechtigten Benutzer die Navigation, Inspektion und Modifizierung des Zugriffssteuerbaums **170**. Jedesmal, wenn der berechtigte Benutzer eine an dem Zugriffssteuerbaum **170** vorzunehmende Änderung spezifiziert, führt der Zugriffssteuerkonfigurationsprozeß **210** ebenfalls sämtliche anderen Änderungen an dem Zugriffssteuerbaum **170** aus, die erforderlich sind, um diesen selbst-konsistent zu halten.

Anwendung von Zugriffsteuerregeln auf Anforderungen

[0079] Unter Bezugnahme auf Fig. 5 wird zuerst die Operation der Zugriffssteuerentscheidungsfunktion **176** erläutert, ohne die Auswirkung von Teilungsanforderungen zur Bearbeitung durch einen oder mehrere Server zu betrachten. Später werden die Anforderungsteilung und die Aufteilung von Pflichten unter den Servern erläutert.

[0080] Wenn eine Zugriffsanforderung empfangen wird, wird die Zugriffsanforderung nacheinander verglichen mit der globalen Ablehnungsregel (Schritt **220**), den zielgerichteten Ablehnungsregeln (Schritt **222**), der globalen Gewährungsregel (Schritt **224**) und den zielgerichteten Gewährungsregeln (Schritt **226**) in dieser Reihenfolge. Die erste gefundene Regel, die mit der Zugriffsanforderung übereinstimmt, wird auf diese angewandt (Schritt **230**). Wenn keine übereinstimmende Regel gefunden wird, dann wird die entsprechende Standardregel angewandt (Schritt **232**).

[0081] Indem zuerst die Ablehnungsregeln und dann die Gewährungsregeln angewandt werden, erhalten die Zugriffsablehnungsregeln eine höhere Priorität als Zugriffsgewährungsregeln. Außerdem macht es diese Struktur relativ leicht, eine Menge von Zugriffsregeln zu definieren, um einer breiten Gruppe von Benutzern bestimmte Zugriffsberechtigungen zu gewähren, wonach dann Untergruppen spezifiziert werden, denen diese Zugriffsberechtigungen nicht gewährt werden sollen.

[0082] Wenn eine Zugriffsanforderung eine Zielmenge mit mehr als einem Zielobjekt hat, können verschiedene Regeln auf unterschiedliche der Zielobjekte, die durch die Anforderung spezifiziert sind, Anwendung finden. In diesem Fall wird die erste gefundene Regel, die auf jedes spezielle Zielobjekt oder jede spezielle Teilgruppe von Zielobjekten anwendbar ist, auf dieses Ziel oder diese Teilgruppe von Zielen angewandt. Infolgedessen kann es sein, daß einige Teile einer Zugriffsanforderung gewährt werden,

während andere abgelehnt werden.

[0083] Fig. 6 zeigt die Sequenz von Aktionen, die von dem Zugriffsanforderungsunterteilungs- und -routingprozeß **172**, den Zugriffssteuerentscheidungs- und -erzwingungsfunktionen **176**, **174** und dem Anforderungsantwortkombinationsprozeß **178** ausgeführt werden. Es ist zu beachten, daß diese Erörterung nicht für Zugriffsanforderungen für Ereignisbenachrichtigungen gilt, die von der Ereignisregistratur separat abgewickelt werden.

[0084] Jede Zugriffsanforderung wird von dem MIS **150** empfangen, der dann die Zugriffsanforderung mit der globalen Ablehnungsregel vergleicht (Schritt **240**). Wenn eine Übereinstimmung gefunden wird, wird die Anforderung abgelehnt, und eine Antwort wird gegebenenfalls an den Initiator zurückgeleitet (Schritt **242**). Keine Antwort wird an den Initiator zurückgeleitet, wenn (A) die anwendbare globale Ablehnungsregel eine Erzwingungsaktion "Ablehnung ohne Antwort" spezifiziert oder (B) die Anforderung selber einen "unbestätigten" Modus spezifiziert.

[0085] Wenn keine Übereinstimmung mit der globalen Ablehnungsregel gefunden wurde, vergleicht der MIS die in der Anforderung spezifizierte Zielmenge mit dem Teilbaum der Serverabbildungstabelle **173**, um den oder die Server zu bestimmen, an welche die Anforderung zur Verarbeitung gesendet werden wird (Schritt **244**). Wenn die Zielmenge der Anforderung in den Bereich von mehr als einem Server fällt, wird die Zugriffsanforderung in Teilanforderungen unterteilt, und jede Teilanforderung wird an ihren jeweiligen Server übermittelt. Wenn eine Anforderung unterteilt wird, wird die Zielmenge in der ursprünglichen Anforderung für jede Teilmenge so eingestellt, daß sie nur Zielobjekte mit dem Bereich des zugeordneten Servers spezifiziert.

[0086] Wenn die Teilmenge der Anforderung in den Bereich eines einzigen Servers fällt, wird die gesamte Anforderung an diesen einen Server zur Verarbeitung weitergeleitet. In manchen Fällen ist der Server zur Verarbeitung der Anforderung der MIS, und in diesem Fall wird die Anforderung dem Ende der lokalen Anforderungsschlange des MIS hinzugefügt. Jeder Zusatzserver, der eine Anforderung von dem MIS empfängt, stellt die empfangenen Anforderungen in seine lokale Anforderungsschlange zur Verarbeitung. Der MIS unterhält ein Statusinformationsfeld **180** (Fig. 3) für alle offenen Zugriffsanforderungen mit einer Bezeichnung des Servers oder der Serv er, an die sie zur Verarbeitung gesendet wurden.

[0087] An jedem Server, dem eine Zugriffsanforderung zur Verarbeitung übermittelt wird, wird die Zugriffsanforderung ausgeführt, indem die Zugriffssteuerentscheidungsfunktion und dann die Zugriffssteuererzwingungsfunktion ausgeführt wird. Insbesondere werden unter erneuter Bezugnahme auf Fig. 5 die Schritte **222** bis **232** der Zugriffssteuerentscheidungsfunktion an jedem Server ausgeführt, da der Schritt **220** bereits von dem MIS ausgeführt wurde. Die Ablehnen/Gewähren-Entscheidung für jede Zugriffsanforderung kann in einem Sicherheitsauditleitweg gespeichert werden.

[0088] Bei einer bevorzugten Ausführungsform der vorliegenden Erfindung kann die Zugriffssteuerentscheidungsfunktion durch die Verwendung eines globalen Konfigurationsparameters so konfiguriert sein, daß durch die Verwendung eines globalen Konfigurationsparameters eine der folgenden Stufen der "Protokollierung" von Zugriffsentscheidungen in dem Sicherheitsauditleitweg aufgerufen wird: (A) Aus, wobei keine Information protokolliert wird, (B) Speichern von zusammenfassenden Informationen über Gewährungen und Ablehnungen von Zugriffsanforderungen, wobei nur die Identität des Initiators, die angeforderte Operation und das Zielobjekt oder die Menge von Objekten bezeichnet werden, für die der Zugriff gewährt oder abgelehnt wurde, und (C) eine Voll-Protokollierstufe, in der für jede Gewährung oder Ablehnung einer Zugriffsanforderung die gesamte Zugriffsanforderung ebenso protokolliert wird wie vollständige Informationen über die Zielobjekte, auf die Zugriff gewährt oder abgelehnt wurde.

[0089] An jedem Server werden die von Anforderungen und Teilanforderungen erzeugten Antworten bestimmt und an den MIS rückgeleitet (Schritt **246**). Schließlich werden an dem MIS, wenn eine Anforderung in zwei oder mehr Teilanforderungen unterteilt wurde, die Antworten kombiniert und die kombinierte Antwort, falls eine solche vorliegt, an den Initiator rückgeleitet (Schritt **248**). Wenn eine Anforderung nicht unterteilt wurde, wird eine eventuelle Antwort an den Initiator rückgeleitet. Ferner wird die Zugriffsanforderung aus der aktuellen Anforderungsstatustabelle **180** gelöscht (Fig. 3).

[0090] Kombinieren von Antworten, wenn eine Anforderung mehr als ein Zielobjekt hat Fig. 7 ist eine Übersicht, die zeigt, wie Zugriffsanforderungs-Antworten kombiniert werden, wenn die Zielmenge einer Zugriffsanforderung mehr als ein Managementobjekt umfaßt. Die Ubersicht von Fig. 7 wird nur angewandt, wenn der Zugriff auf mindestens ein Zielobjekt, das von einer Anforderung spezifiziert wird, abgelehnt worden ist. Wenn der Zugriff auf alle Zielobjekte gewährt wird, werden die von sämtlichen Zielobjekten erzeugten Antworten einfach kombiniert und an den Initiator rückgeleitet.

[0091] Wenn die Zielmenge einer Anforderung nur ein Objekt enthält, was der Zeile "umfangsfreie Operation" in der Übersicht von Fig. 7 entspricht, ist es nicht notwendig, Antworten zu kombinieren. Wenn die Anforderung eine bestätigte Anforderung ist, wird

die Zugriff-abgelehnt-Antwort, die von der anwendbaren Regel erzeugt wird, an den Initiator rückgeleitet. Wenn die von der anwendbaren Regel erzeugte Antwort eine "Ablehnung-ohne-Antwort" ist, wird keine Antwort rückgeleitet. Wenn die Anforderung eine unbestätigte Anforderung ist, wird ohne Rücksicht darauf, ob die Anforderung gewährt oder abgelehnt wird, keine Antwort rückgeleitet.

[0092] Wenn eine Anforderung mehr als ein Zielobjekt spezifiziert, was dem Bereich "Umfangs-Operation" in Fig. 7 entspricht, ist die Art der rückgeleiteten Antwort von dem synch-Parameter der Anforderung abhängig. Wenn die Anforderung eine unteilbare Anforderung ist und der Zugriff auf eines der Zielobjekte abgelehnt wird, ist die gesamte Operation eine Fehloperation. Wenn die Anforderung eine bestätigte Anforderung ist, wird an den Initiator eine einzige Antwort "Zugriff abgelehnt" rückgeleitet. Andernfalls wird, wenn die Anforderung eine unbestätigte Anforderung ist, keine Antwort an den Initiator rückgeleitet.

[0093] Wenn die Anforderung mehr als ein Zielobjekt spezifiziert ("Umfangsoperation") und einen synch-Modus "bestmöglich" spezifiziert, werden die Antworten, die von den Objekten erzeugt werden, für die Zugriff gewährt wird, an den Benutzer rückgeleitet. Für jedes Objekt, für das der Zugriff abgelehnt wird, wird eine Antwort "Zugriff abgelehnt" rückgeleitet, wenn die Anforderung eine bestätigte Anforderung ist und die anwendbare Regel eine Erzwingungsaktion von "Ablehnung mit Antwort" hat. Andernfalls wird, wenn die anwendbare Regel eine Erzwingungsaktion "Ablehnung ohne Antwort" hat, keine Antwort für das Objekt/die Objekte rückgeleitet, für die der Zugriff abgelehnt wird.

[0094] Wenn schließlich die Anforderung eine unbestätigte Anforderung war, wird an den Initiator keine Antwort rückgeleitet ohne Rücksicht darauf, welche Teile der Anforderung gewährt und welche abgelehnt wurden. Es ist zu beachten, daß eine unbestätigte Anforderung keine "Beschaffen"-Operation haben kann, da definitionsgemäß der Zweck einer "Beschaffen"-Antwort darin besteht, Information abzurufen.

[0095] Die in Fig. 7 zusammengefaßte Operation des Kombinierens von Antworten wird zuerst an jedem Server **150**, **152** ausgeführt, wo die Anforderung oder Teilanforderung verarbeitet wird, und erneut an dem MIS für diejenigen Anforderungen ausgeführt, die in Teilanforderungen unterteilt sind. Für unteilbare Zugriffsanforderungen, die aufgeteilt und an mehr als einem Server verarbeitet werden, wird die Zugriffssteuererzwingungsfunktion erst ausgeführt, nachdem die Ergebnisse für die Zugriffssteuerentscheidungsfunktion von dem MIS kombiniert worden sind. Wenn eine Zugriffsanforderung an nur einem Server verarbeitet wird (d. h. wenn ihre sämtlichen Zielobjekte in den Bereich eines einzigen Servers **150**, **152** fallen), wird die Operation des Kombinierens der Antworten nur von dem Server ausgeführt, der die Anforderung verarbeitet hat.

Begrenzung des Zugriffs auf Ereignisbenachrichtigungen

[0096] Bei der vorliegenden Ausführungsform wird der Zugriff auf Ereignisse (Berichte) auf die gleiche Weise wie der Zugriff auf Objekte gesteuert unter Anwendung von Regeln in der Zugriffssteuerregeldatenbank. X.741 umfaßt Ereignisbenachrichtigungen nicht als einen der Typen von Operationsarten, auf die der Zugriffssteuermechanismus von X.741 anwendbar ist. Ein Beispiel des Problems der Ereignisbenachrichtigungs-Zugriffssteuerung ist folgendes: Eine Telefonnetzgesellschaft wünscht nicht, daß der Kunde A Benachrichtigungen über neue Netzressourcen empfängt, die für den Kunden B installiert wurden, aber Kunde A registriert sich für den Empfang aller Ereignisbenachrichtigungen.

[0097] Die vorliegende Ausführungsform löst das Problem der Zugriffssteuerung von Ereignisbenachrichtigungen dadurch, daß (A) Ereignisbenachrichtigungen zu der Menge von Operationstypen hinzufügt werden, die von Regeln in der Zugriffsregeldatenbank bestimmt sind, und (B) ein Filtermechanismus zu dem Ereignisrouter des Systems hinzugefügt wird, der Ereignisbenachrichtigungs-Meldungen ausfiltert, die auf den Regeln in der Zugriffsregeldatenbank basieren.

[0098] Wenn daher ein Zielobjekt in dem Zugriffssteuerobjektbaum **170** definiert ist, ist eine der Operationen, die in der Operationsliste des Zielobjekts spezifiziert werden können, "Ereignisbenachrichtungen". Bei der bevorzugten Ausführungsform kann die Ereignisbenachrichtigungsoperation, die in einem Zielobjekt spezifiziert ist, entweder alle Ereignisbenachrichtigungen für eine Menge von spezifizierten Managementobjekten bezeichnen, oder sie kann bestimmte spezielle Arten von Ereignisbenachrichtigungen spezifizieren durch Verwendung des Filterfeldes des Zielobjekts, um die Arten von Ereignisbenachrichtigungen zu spezifizieren, die in dem Zielobjekt enthalten sein sollen. Beispielsweise könnte ein Zielobjekt SNMP- oder CMIP-erzeugte Ereignisse betreffen, jedoch keine anderen Arten von Ereignissen wie etwa Objekterstellungs- und -löschungsereignisse.

[0099] Ferner kann ein bestimmtes Zielobjekt verwendet werden, um Zugriffsberechtigungen für eine Menge von Managementobjekten für mehrere Operationen einschließlich Ereignisbenachrichtigungen zu definieren. Beispielsweise enthält ein Zielobjekt, das mit einer Ablehnungsregel zur Ablehnung des Zugriffs für jegliche Information im Hinblick auf eine bestimmte Menge von Managementobjekten ver-

wendet werden soll, typischerweise Ereignisbenachrichtigungen in seiner Liste von Operationen. Alternativ können gegebenenfalls separate Zielobjekte verwendet werden, um Zugriffsberechtigungen für Ereignisbenachrichtigungen zu definieren.

[0100] Gemäß Fig. 8 unterhält der MIS **150** eine Ereignisregistratur **184**. Genauer gesagt, ist die Ereignisregistratur **184** ein Softwaremodul, das eine Tabelle **260** von Benutzer-Ereignisanforderungen unterhält. Der MIS leitet alle Zugriffsanforderungen, deren spezifizierter Operationstyp "Ereignisbenachrichtigung" ist, an die Ereignisregistratur **184**, und zwar ohne Rücksicht darauf, welche Objekte von der Anforderung spezifiziert wwerden. Die Tabelle **260** speichert Informationen, die für spezifizierte Ereignisbenachrichtigungen, die entweder von den Managementobjekten oder den Zugriffssteuerobjekten erzeugt werden können, angeben, welche Benutzer oder sonstige Entitäten eine Anforderung zum Empfang von Kopien von solchen Ereignisbenachrichtigungen registriert haben. Die Ereignisregistraturtabelle **260** speichert nur Informationen über Ereignisse, die Benutzer und andere Entitäten angefordert haben. Die Ereignisbenachrichtigungs-Registrierungsanforderungen (die Zugriffsanforderungen mit einem Operationstyp gleich "Ereignisbenachrichtigung" sind) können entweder in Form von spezifizierten Objekten, spezifizierten Klassen von Objekten oder spezifizierten Teilbäumen von Objekten spezifiziert werden. Beispielsweise könnte ein Benutzer den Empfang von allen Ereignisbenachrichtigungen für Router-Objekte (d. h. eine Klasse von Objekten) anfordern und ferner einen Filter spezifizieren, etwa nur für Router, die im Staat Kalifornien liegen, oder Router, die von einer bestimmten Firma hergestellt sind. Benutzer und Entitäten können auch frühere Anforderungen widerrufen.

[0101] Bei der bevorzugten Ausführungsform prüft die Ereignisregistratur **184** nur Registrationsanforderungen, um sicherzustellen, daß die Anforderungen semantisch korrekt sind und die spezifizierten Objekte, für die Ereignisse angefordert werden, tatsächlich existieren. Bei der bevorzugten Ausführungsform prüft daher die Ereignisregistratur **184** nicht, ob der Benutzer oder die Entität, die eine Registrationsanforderung abgibt, die Sicherheitsfreigabe hat, um die angeforderten Benachrichtigungen tatsächlich zu erhalten. Diese Aufgabe erhält der Ereignis-Router **186**, der Ereignisbenachrichtigungs-Zugriffsberechtigungen zu dem Zeitpunkt prüft, zu dem jede Ereignisbenachrichtigung verarbeitet wird. Infolgedessen werden alle Änderungen von Zugriffsberechtigungen eines Benutzers für Ereignisbenachrichtigungen von dem Ereignis-Router berücksichtigt und beeinflussen nicht die in der Ereignisregistratur **184** gespeicherte Information.

[0102] Von Benutzern verschiedene Entitäten, die sich für den Empfang von Ereignisbenachrichtigungen registrieren können, umfassen: den MIS **150** und Zusatzserver **152**, den Protokollserver (der noch erläutert wird) und auch Objekte (z. B. Datenbankobjekte, die nachstehend erläutert werden), die Teil der Zugriffssteuermaschine sind.

[0103] Alle Ereignisbenachrichtigungen einschließlich Ereignisbenachrichtigungen, die von Managementobjekten erzeugt werden (die in Fig. 8 mit "andere Ereignisquellen" bezeichnet sind), und Ereignisbenachrichtigungen, die von Zugriffssteuerobjekten erzeugt werden (in Fig. 8 durch den speziellen Zusatzserver **154** bezeichnet), werden zu dem Ereignis-Router **186** in dem MIS **150** geleitet. Der Ereignis-Router **186** hat ferner Zugriff auf den Zugriffssteuerbaum **170** und die Tabelle von Benutzer-Ereignisanforderungen **260** in der Ereignisregistratur **184**. Für jede von dem Ereignis-Router **86** empfangene Ereignisbenachrichtigung bestimmt der Ereignis-Router zuerst, welche Benutzer und Entitäten eine Kopie dieser Ereignisbenachrichtung angefordert haben, und bestimmt dann, welche dieser Benutzer und Entitäten die Berechtigung zum Empfang dieser Ereignisbenachrichtigung haben. Die Bestimmung von Zugriffsberechtigungen für Ereignisbenachrichtigungen wird ausgeführt unter Anwendung der Zugriffssteuerentscheidungsfunktion, die in Fig. 5 gezeigt ist. Somit prüft der Ereignis-Router nacheinander die globale Ablehnungsregel, die zielgerichteten Ablehnungsregeln, die globale Gewährungsregel und die zielgerichteten Gewährungsregeln, bis eine übereinstimmende Regel identifiziert wird. Eine Standardregel wird angewandt, wenn keine übereinstimmende Regel gefunden wird. Eine übereinstimmende Regel muß (A) für die "Ereignisbenachrichtigungs"-Operation gelten, (B) für das Objekt gelten, das die Ereignisbenachrichtung erzeugt hat, und (C) für eine Gruppe gelten, in welcher der Anfordernde Mitglied ist.

[0104] Für jeden Anforderer einer Ereignisbenachrichtigung, der Zugriffsberechtigung für diese Ereignisbenachrichtigung hat, erzeugt der Ereignis-Router eine entsprechende Ereignisbenachrichtigungs-Meldung, die jeweils an einen einzigen berechtigten Benutzer bzw. eine solche Entität adressiert ist. Somit kann eine einzige Ereignisbenachrichtigung entweder in null Ereignisbenachrichtigungs-Meldungen oder vielen davon resultieren in Abhängigkeit von der Anzahl von Anfordernden mit entsprechenden Zugriffsberechtigungen.

[0105] Eine spezielle Anwendung der Ereignisregistratur **184** und des Ereignis-Routers **186**, die bei den bevorzugten Ausführungsformen genutzt wird, ist wie folgt. Es gibt einen speziellen Zusatzserver **154**, der alle Zugriffsanforderungen für den und Modifikationen des Zugriffssteuerbaums **170** abwickelt. Anders ausgedrückt, Zugriffsanforderungen (außer Ereignisbenachrichtigungs-Zugriffsanforderungen), deren

Zielmenge in dem Zugriffssteuerbaum **170** liegt, werden von dem MIS **150** zu dem speziellen Zusatzserver **154** geleitet. Ferner resultieren alle Änderungen an dem Zugriffssteuerbaum **170** in der Erzeugung von Ereignisbenachrichtigungen, die an den Ereignis-Router **186** gesendet werden. Insbesondere resultieren die Erschaffung von neuen Zugriffssteuerobjekten, das Löschen von Zugriffssteuerobjekten und die Modifikation der Attribute jedes Zugriffssteuerobjekts sämtlich in der Erzeugung von Ereignisbenachrichtigungen.

[0106] Der MIS **150** und die Zusatzserver **152** sind sämtlich in der Ereignisregistratur **184** automatisch registriert für den Empfang aller Ereignisbenachrichtigungen, die sich auf Anderungen in dem Zugriffssteuerbaum **170** beziehen. Der MIS **150** und die Zusatzserver sind außerdem in einem Set von "Superbenutzern" mit Zugriffsberechtigungen für alle Ereignisbenachrichtigungen enthalten. Ferner befindet sich unter den Bibliotheksprozessen, die von dem MIS **150** und den Zusatzservern **152** gemeinsam genutzt werden, ein Ereignisempfangs- und -verarbeitungsprozeß **262**. Wenn der MIS **150** und die Zusatzserver **152** irgendwelche Ereignisbenachrichtigungen empfangen, die eine Änderung in dem Zugriffssteuerbaum **170** bedeuten, nimmt der Ereignisverarbeitungsprozeß **262**, der von jedem Server aufgerufen wird, die gleiche Änderung an der lokalen Kopie des Zugriffssteuerbaums **170** in dem Server vor. Infolgedessen werden die lokalen Kopien des Zugriffssteuerbaums **170** in jedem der Server **150**, **152** praktisch gleichzeitig aktualisiert.

Direkter Datenbankzugriff auf Managementinformation

[0107] SQL-Zugriff auf die Managementobjektdatenbank wird von X.741 weder verlangt noch vorgeschlagen. Tatsächlich könnte ein direkter Zugriff über einen DBMS-Mechanismus als gegensätzlich zu den Zielen von X.741 beterachtet werden, da dies eine potentielle Quelle von Sicherheitslücken ist. Firmenkunden großer Kommunikationsnetze verlangen jedoch direkten "Nur-Lese"-Zugriff auf Managementinformation für die Zwecke der Berichtserzeugung.

[0108] Der Direktzugriffsmechanismus der vorliegenden Ausführungsform sieht begrenzten Nur-Lese-Zugriff auf Managementinformation vor unter Verwendung von Standard-DBMS-Berichtsgeneratoren, um Berichte über den Status oder die frühere Leistungsfähigkeit von Netzobjekten zu definieren und zu erzeugen. Das ist für die Benutzer zweckmäßig und vermeidet die Komplexitäten des Netzmanagement-informations-Abrufs unter Anwendung von SNMP (oder eines anderen Netzmanagementprotokolls), wenn die einzige auszuführende Aufgabe die Erzeugung von Statusberichten und anderen die Netzsystemanalyse betreffenden Berichten ist.

[0109] Der Direktzugriffsmechanismus der vorliegenden Ausführungsform erlaubt den Benutzern nur den Zugriff auf Information, der bei Anforderung über die normale Managementschnittstelle zu dem Netz gewährt werden würde.

[0110] Gemäß Fig. 9 sind die Hauptkomponenten des direkten Informationszugriffsmechanisms die folgenden: ein herkömmliches Datenbankmanagementsystem (DBMS) **280** zur Speicherung von Ereignisprotokollen **282**, die jeweils Ereignisbenachrichtigungen speichern, für die verschiedene Benutzer direkten SQL-Zugriff angefordert haben; ein Protokollserver **290**, dessen Hauptfunktion darin besteht, Ereignisbenachrichtigungen in SQL-Einfügungsstatements zur Speicherung von Ereignisbenachrichtigungen in den Ereignisprotokollen umzuwandeln.

[0111] Das DBMS **280**, das konventionell ist, speichert Tabellen von Informationen. Fig. 9 zeigt zwar Ereignisprotokolle **282**, aber jedes Ereignisprotokoll ist tatsächlich eine oder mehrere Datenbanktabellen, wobei in jeder Datenbanktabelle eine andere Art von Ereignisbenachrichtigung gespeichert ist. Das DBMS **280** hat ferner ein Zugriffsprivileg-Modul **284**, das Zugriffsrechte für jede der Tabellen in dem DBMS konfiguriert (d. h. etabliert). Beispielsweise kann das Zugriffsprivileg-Modul **284** eine Zugriffsprivileg-Tabelle haben, die Zugriffsberechtigungsinformation speichert, die angibt, welche Benutzer Zugriff auf die Tabellen haben, welche die Ereignisprotokolle **282** bilden. Das Zugriffsprivileg-Modul **284** kann aber auch auf andere Weise implementiert sein, etwa durch Speichern von Zugriffsprivileg-Information in jeder Datenbanktabelle. Die vorliegende Anmeldung ist nicht von dem speziellen Mechanismus abhängig, der von dem Zugriffsprivileg-Modul **284** angewandt wird, um Datenbanktabellen-Zugriffsrechte zu etablieren.

[0112] Bei der bevorzugten Ausführungsform hat nur der Protokollserver **290** (außer dem Systemadministrator) Schreibzugriff auf die Ereignisprotokolltabellen, während spezifizierte Benutzer Lesezugriff auf spezielle Tabellen haben. Eine Standard-SQL-Maschine **286** verarbeitet Einfügungsstatements von dem Protokollserver **290** sowie Leseanforderungen von Benutzerprozessen oder Workstations **300**, die über eine Benutzerkommunikationsschnittstelle **288** übermittelt werden. Der Protokollserver **290** ist in der Ereignisregistratur registriert zum Empfang aller von dem System erzeugten Ereignisbenachrichtigungen und hat entsprechende Zugriffsberechtigungen. Der Protokollserver **290** ist bevorzugt eine Software-Entität oder ein Prozeß, der auf demselben Computer oder Computerknoten wie der MIS **150** läuft. Eine Gruppe von Filtern **291**, **294** in dem Protokollserver **290** bestimmt, welche Ereignisbenachrichtigungen gespeichert werden und wo sie gespeichert werden. Ein erster Filter **291** in dem

Protokollserver ist als Sicherheitsauditleitwegfilter bezeichnet. Dieser Filter **291** läßt "Zugriff-Gewähren"- und "Zugriff-Ablehnen"-Ereignisbenachrichtigungen durch, die von dem MIS **150** und den Zusatzservern **152** erzeugt werden (siehe Fig. 8). Der Sicherheitsauditleitwegfilter **291** kann selektiv entweder die gesamte Ereignisbenachrichtigung oder einen spezifizierten Anteil davon in der Sicherheitsaudideitwegdatei **182** speichern. Wenn dabei der Sicherheitsauditleitweg so konfiguriert ist, daß er in einem Detailmodus arbeitet, speichert der Sicherheitsaudideitweg **182** jede Zugriffsanforderung und das entsprechende Ergebnis vollständig. Wenn der Sicherheitsauditleitweg so konfiguriert ist, daß er in einem Kurzmodus arbeitet, speichert der Sicherheitsauditleitweg **182** eine verkürzte Darstellung jeder Zugriffsanforderung und des entsprechenden Ergebnisses.

[0113] Ein anderer Protokollserverfilter **292**, der als Sicherheitsalarmfilter bezeichnet ist, dient zur Erzeugung eines Sicherheitsalarmprotokolls **293**, das separat von dem Sicherheitsauditleitweg **182** ist, wobei Sicherheitsalarme nur dann erzeugt und in dem Protokoll gespeichert werden, wenn eine Ablehnung eines Objektzugriffs vorliegt. Bei der bevorzugten Ausführungsform bezeichnen die gespeicherten Sicherheitsalarme den Benutzer, der jede abgelehnte Zugriffsanforderung initiiert hat.

[0114] Der andere Typ von Protokollserverfilter, der in Fig. 9 gezeigt ist, sind die Ereignisprotokollfilter **294**. Jeder Ereignisprotokollfilter ist so eingerichtet, daß er nur eine spezifizierte Menge von Ereignisbenachrichtigungen durchläßt. Beispielsweise kann ein bestimmter Kunde fordern, daß bestimmte Gruppen seiner Angestellten direkten Zugriff auf alle SNMP-Ereignisbenachrichtigungen (CMIP-Ereignisbenachrichtigungen) für Managementobjekte haben, die diesem Kunden zugeordnet sind. Der Protokollerstellungs-/-löschprozeß **296** wird verwendet, um ein entsprechendes Ereignisprotokoll zu definieren durch:

(A) Definieren und Initialisieren einer entsprechenden Menge von DBMS-Tabellen **282** (d. h. eines Ereignisprotokolls) zum Speichern der angeforderten Ereignisbenachrichtigungen (eine gesonderte DBMS-Tabelle pro einzelnem Typ von Ereignisbenachrichtigung);

(B) Definieren und Erstellen eines Datenbankobjekts **298** und Registrieren des Datenbankobjekts **298** in der Ereignisregistratur zum Empfang von Ereignisbenachrichtigungen, welche die Berechtigungen von Nutzern zum Empfang dieser Ereignisbenachrichtigungen betreffen; das Datenbankobjekt **298** umfaßt ein erstes Attribut, das eine Liste der DBMS-Tabellen enthält, in denen das Ereignisprotokoll gespeichert ist, und ein zweites Attribut, das eine Liste der Gruppen mit Zugriffsberechtigungen auf die Ereignisbenachrichtigungen enthält;

(C) da dem Datenbankobjekt **298** zuerst Gruppennamen hinzugefügt werden, sendet das Datenbankobjekt **298** eine Anfangsmenge von Datenbanktabellenzugriffs-Gewährungsbefehlen an das DBMS, um die Anfangsmenge von Benutzern mit Zugriffsberechtigungen für die Tabellen, die das Ereignisprotokoll **282** bilden, zu definieren; und

(D) Definieren und Erstellen eines Ereignisprotokollfilters **282**, der nur die angeforderten Ereignisbenachrichtigungen durchläßt und sie in SQL-Einfügungsstatements umwandelt zum Einfügen jeder durchgelassenen Ereignisbenachrichtigung in eine jeweilige von den DBMS-Tabellen.

[0115] Für jedes Ereignisprotokoll **282** gibt es ein oder mehr entsprechende Zielobjekte in dem Zugriffssteuerobjektbaum **170**, die folgendes definieren: (1) die Zielmenge von Managementobjekten, für die Ereignisbenachrichtigungen in dem Ereignisprotokoll zu speichern sind, und (2) die Arten von Ereignisbenachrichtigungen, die in dem Ereignisprotokoll enthalten. sein sollen. Für jedes bestimmte Ereignisprotokoll muß die Menge von Gruppen von berechtigten Benutzern die gleiche für alle Ereignisbenachrichtigungen in diesem Ereignisprotokoll sein. Alle Änderungen in den Gruppen von Benutzern, denen Zugriff auf das Ereignisprotokoll gewährt werden soll, sind mit dem entsprechenden Datenbankobjekt **198** in Kommunikation durch Registrierung des Datenbankobjekts in der Ereignisregistratur, um Ereignisbenachrichtigungen über Attributänderungen an dem Zielobjekt/den Zielobjekten entsprechend dem Ereignisprotokoll zu empfangen. Das Datenbankobjekt **298** ist außerdem registriert zum Empfang von Ereignisbenachrichtigungen über Attributänderungen an den Gruppenobjekten für die Gruppen, die Zugriffsberechtigungen für das Ereignisprotokoll haben.

[0116] Immer, wenn das Datenbankobjekt **298** für ein bestimmtes Ereignisprotokoll **282** über eine Änderung (d. h. Hinzufügungen und/oder Löschungen) in der Mitgliedschaft von einer der Gruppen mit Zugriffsberechtigungen für das Ereignisprotokoll **291** oder über eine Änderung in der Menge von Gruppen, die Zugriff auf die Ereignisbenachrichtigungen in dem Ereignisprotokoll erhalten sollen, benachrichtigt wird, sendet das Datenbankobjekt **298** entsprechende Zugriffsgewährungs- und Zugriffsaufrufbefehle an das DBMS **280**. Das Zugriffsprivilegmodul **284** rekonfiguriert dann die Datenbanktabellenzugriffsberechtigungen entsprechend.

[0117] Wenn Ereignisbenachrichtigungen entsprechend einem Ereignisprotokoll erzeugt werden, werden sie von dem Ereignis-Router **186** an den Protokollserver **290** weitergeleitet. Der Protokollserver **290** leitet sie an den Filter **294** des Ereignisprotokolls weiter, wo sie in SQL-Einfügungsstatements umgewan-

delt und zur Speicherung an das DBMS **280** gesendet werden. Wenn einige der gleichen Ereignisbenachrichtigungen in zwei (oder mehr) verschiedenen Ereignisprotokollen **282** enthalten sind, wird die gleiche Ereignisbenachrichtigung zweimal (oder mehrmals) in verschiedenen Tabellen des DBMS gespeichert.

[0118] Die SQL-Maschine **286** erzwingt vorher definierte Zugriffsbegrenzungen für die Ereignisprotokolle. Insbesondere wird jede Benutzeranfrage nach Information aus den Tabellen in dem DBMS von der SQL-Maschine **286** hinsichtlich der von dem Zugriffsprivileg-Modul **284** etablierten Zugriffsberechtigungen geprüft, und nur Anfragen, die in voller Übereinstimmung mit diesen Zugriffsberechtigungen sind, werden verarbeitet. Benutzeranfragen, die Information aus Tabellen anfordern, für die der Benutzer keine Zugriffsberechtigungen hat, werden von der SQL-Maschine **286** zurückgewiesen.

[0119] Da Benutzeranforderungen von Information von dem DBMS **280** in Form von SQL-Anfragen übermittelt werden müssen, können sämtliche Berichtserzeugerwerkzeuge, die für das DBMS verfügbar sind, angewandt werden, um SQL-Anfragen für Managementinformation zu erstellen. Somit bietet der in Fig. 9 gezeigte DBMS-Zugriffsmechanismus den Vorteil der Anwendung von schnellen und wohlbekannten DBMS-Zugriffswerkzeugen, während gleichzeitig die gleichen Zugriffsbeschränkungen vorhanden sind, wie sie von dem Managementinformationsserver vorgesehen werden. Ferner werden die Zugriffsbeschränkungen, die von dem DBMS **280** aufgestellt werden, immer dann automatisch aktualisiert, wenn die Zugriffsberechtigungen für die entsprechenden Ereignisbenachrichtigungen in der Hauptzugriffssteuermaschine, die den Zugriff auf Information in dem Managementobjektbaum steuert, modifiziert werden.

Patentansprüche

1. Zugriffssteuersystem (**100**) zur Steuerung des Zugriffs auf Managementobjekte in einem verteilten Netz (**106**), wobei das Zugriffssteuersystem folgendes aufweist:
eine Zugriffssteuerdatenbank (**108**), die Zugriffssteuerobjekte aufweist, wobei die Zugriffssteuerobjekte folgendes aufweisen:
Gruppenobjekte, die jeweils eine Gruppe und eine Menge von Benutzern definieren, die Mitglieder der Gruppe sind; und
Regelobjekte, wobei eine Teilmenge der Regelobjekte jeweils folgendes spezifiziert: eine Menge der Gruppenobjekte, eine Menge der Managementobjekte und Zugriffsberechtigungen durch die Benutzer, die Mitglieder der durch die spezifizierte Menge der Gruppenobjekte definierten Gruppen sind, für die spezifizierte Menge von Managementobjekten; und
eine Vielzahl von Zugriffssteuerservern, wobei jeder Zugriffssteuerserver den Zugriff auf eine bestimmte Teilmenge der Managementobjekte gemäß den in der Zugriffssteuerdatenbank (**108**) spezifizierten Zugriffsberechtigungen steuert; wobei mindestens einer von den Zugriffssteuerservern Zugriffsanforderungen von den Benutzern empfängt und die empfangenen Zugriffsanforderungen unter den Zugriffssteuerservern zur Verarbeitung verteilt; eine Teilmenge der Zugriffsanforderungen Operationen, die an spezifizierten Mengen der Managementobjekte auszuführen sind, spezifiziert; wobei jede Zugriffsanforderung in der Teilmenge zur Verarbeitung an einen oder mehrere von den Zugriffssteuerservern gesendet wird gemäß den Managementobjekten, auf die durch die Zugriffsanforderung Zugriff angefordert wird;
wobei die Zugriffssteuerserver auf die Zugriffsanforderungen von den Benutzern reagieren, indem sie den in jeder Zugriffsanforderung angeforderten Zugriff gemäß den in der Zugriffssteuerdatenbank spezifizierten Zugriffsberechtigungen gewähren, ablehnen und teilweise gewähren und ablehnen.

2. Zugriffssteuersystem nach Anspruch 1, wobei
einer von den Zugriffssteuerservern ein Managementinformationsserver (**150**) ist, der die von Benutzern an das Zugriffssteuersystem übermittelten Zugriffsanforderungen (**120**) empfängt;
der Managementinformationsserver (**150**) aufweist: eine Einrichtung zum Unterteilen einer Zugriffsanforderung in zwei oder mehr Zugriffs-Teilanforderungen, wenn der Zugriff zu der Menge von Managementobjekten, die durch die Zugriffsanforderung spezifiziert werden, von zwei oder mehr von den Zugriffssteuerservern gesteuert wird, und zum Senden der Zugriffs-Teilanforderungen an diese zwei oder mehr Zugriffssteuerserver zur Verarbeitung; und
und der Managementinformationsserver (**150**) aufweist: eine Einrichtung zum Kombinieren von Antworten auf die zwei oder mehr Zugriffs-Teilanforderungen, die von den zwei oder mehr Zugriffssteuerservern nach der Verarbeitung der Zugriffs-Teilanforderungen erzeugt werden, und zum Rücksenden einer kombinierten Antwort an den Benutzer, der die Zugriffsanforderung, die unterteilt wurde, übermittelt hat.

3. Zugriffssteuersystem (**100**) nach Anspruch 1, wobei
eine zweite Teilmenge der Regelobjekte in der Zugriffssteuerdatenbank (**108**) folgendes spezifiziert: eine Menge der Gruppenobjekte, eine Menge der Zugriffssteuerobjekte und Zugriffsberechtigungen durch die Benutzer, die Mitglieder der durch die spezifizierte Menge der Gruppenobjekte definierten Gruppen sind, für die spezifizierte Menge von Zugriffssteuerobjekten; und
das Zugriffssteuersystem (**100**) aufweist: eine Zugriffssteuerdatenbankeinrichtung (**108**), die die Zugriffssteuerdatenbank dauerhaft speichert, Zu-

griffsanforderungen auf die Zugriffssteuerobjekte empfängt, die Zugriffsanforderungen auf die Zugriffssteuerobjekte gemäß den in der Zugriffssteuerdatenbank spezifizierten Zugriffsberechtigungen gewährt und ablehnt.

4. Zugriffssteuersystem (**100**) nach Anspruch 1, wobei
eine zweite Teilmenge der Regelobjekte in der Zugriffssteuerdatenbank (**108**) jeweils folgendes spezifiziert: eine Menge der Gruppenobjekte, eine Menge der Managementobjekte und Zugriffsberechtigungen durch die Benutzer, die Mitglieder der durch die spezifizierte Menge der Gruppenobjekte definierten Gruppen sind, für durch die spezifizierte Menge von Managementobjekten erzeugte Ereignisbenachrichtigungen; und
das Zugriffssteuersystem (**100**) aufweist: einen Ereignis-Router (**186**), der durch die Managementobjekte erzeugte Ereigisbenachrichtigungen empfängt und entsprechende Ereignisbenachrichtigungsmeldungen nur an Benutzer in Gruppen sendet, die gemäß den in der Zugriffssteuerdatenbank spezifizierten Zugriffsberechtigungen Zugriffsberechtigungen für diese Ereignisbenachrichtigungen haben.

5. Zugriffssteuersystem (**100**) nach Anspruch 4, wobei
das Zugriffssteuersystem aufweist: eine Ereignisregistratur (**184**) zum Registrieren von Ereignisbenachrichtungsanforderungen durch Benutzer, wobei jede Ereignisbenachrichtigungsanforderung Ereignisbenachrichtigungen von spezifizierten Mengen der Managementobjekte spezifiziert, die angefordert werden;
der Ereignis-Router (**186**) aufweist: eine Einrichtung, um in Abhängigkeit von jeder empfangenen Ereignisbenachrichtigung entsprechende Ereignisbenachrichtungsmeldungen an Benutzer zu senden, die in der Ereignisregistratur (**184**) eine entsprechende Ereignisbenachrichtungsanforderung registriert haben und die ferner gemäß den in der Zugriffsteuerdatenbank spezifizierten Zugriffsberechtigungen Zugriffsberechtigungen für die empfangene Ereignisbenachrichtigung haben.

6. Verfahren zum Steuern des Zugriffs auf Managementobjekte in einem verteilten Netz, wobei das Verfahren die folgenden Schritte aufweist:
Speichern einer Menge von Zugriffsteuerobjekten in einer Zugriffssteuerdatenbank (**108**), wobei die Zugriffssteuerobjekte folgendes aufweisen:
Gruppenobjekte, die jeweils eine Gruppe und eine Menge von Benutzern definieren, die Mitglieder der Gruppe sind; und
Regelobjekte, wobei eine Teilmenge der Regelobjekte jeweils folgendes spezifiziert: eine Menge der Gruppenobjekte, eine Menge der Managementobjekte und Zugriffsberechtigungen durch die Benutzer, die Mitglieder der durch die spezifizierte Menge der Gruppenobjekte definierten Gruppen sind, für die spezifizierte Menge von Managementobjekten; und
Empfangen von Zugriffsanforderungen von den Benutzern und Verteilen der empfangenen Zugriffsanforderungen unter einer Vielzahl von Zugriffssteuerservern zur Verarbeitung; wobei eine Teilmenge der Zugriffsanforderungen an spezifizierten Mengen der Managementobjekte auszuführende Operationen spezifiziert; wobei jeder Zugriffssteuerserver den Zugriff zu einer bestimmten Teilmenge der Managementobjekte gemäß den in der Zugriffssteuerdatenbank spezifizierten Zugriffsberechtigungen steuert; wobei jede Zugriffsanforderung in der Teilmenge zur Verarbeitung an einen oder mehrere von den Zugriffssteuerservern gesendet wird gemäß den Managementobjekten, auf die durch die Zugriffsanforderung Zugriff angefordert wird,;
an den Zugriffssteuerservern, Reagieren auf die Zugriffsanforderungen von den Benutzern durch Gewähren, Ablehnen und teilweises Gewähren und Ablehnen des in jeder Zugriffsanforderung angeforderten Zugriffs gemäß den in der Zugriffssteuerdatenbank spezifizierten Zugriffsberechtigungen.

7. Zugriffssteuerungsverfahren nach Anspruch 6, wobei
sämtliche durch Benutzer übermittelten Zugriffsanforderungen an einem von den Zugriffssteuerservern empfangen werden;
an dem einen Zugriffssteuerserver eine Zugriffsanforderung in zwei oder mehr Zugriffs-Teilanforderungen unterteilt wird, wenn der Zugriff auf die Menge von Managementobjekten, die durch die Zugriffsanforderung spezifiziert werden, durch zwei oder mehr von den Zugriffssteuerservern gesteuert wird, und die Zugriffs-Teilanforderungen an diese zwei oder mehr Zugriffsteuerserver zur Verarbeitung gesendet werden; und
an dem einen Zugriffssteuerserver Antworten auf die zwei oder mehr Zugriffs-Teilanforderungen kombiniert werden, die von den zwei oder mehr von den Zugriffssteuerservern nach der Verarbeitung der Zugriffs-Teilanforderungen erzeugt werden, und Rücksenden einer kombinierten Antwort an den Benutzer, der die Zugriffsanforderung, die unterteilt wurde, übermittelt hat.

8. Zugriffssteuerungsverfahren nach Anspruch 6, wobei
eine zweite Teilmenge der Regelobjekte in der Zugriffssteuerdatenbank (**108**) folgendes spezifiziert: eine Menge der Gruppenobjekte, eine Menge der Zugriffssteuerobjekte und Zugriffsberechtigungen durch die Benutzer, die Mitglieder der durch die spezifizierte Menge der Gruppenobjekte definierten Gruppen sind, für die spezifizierte Menge von Zugriffssteuerobjekten; und
an einem Zugriffssteuerdatenbankserver die Zugriffssteuerdatenbank (**108**) dauerhaft gespeichert wird, Zugriffsanforderungen auf die Zugriffssteuerobjekte

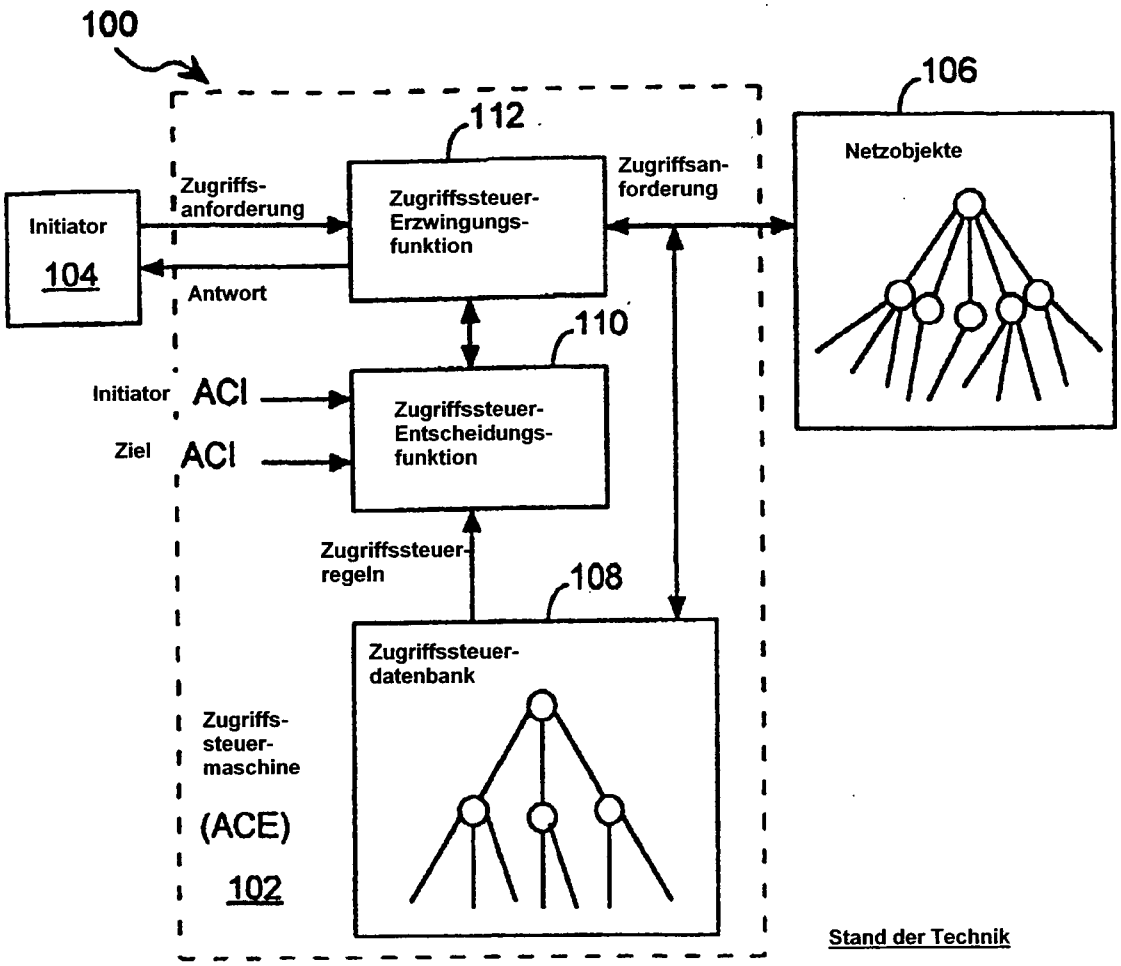
empfangen werden, die Zugriffsanforderungen auf die Zugriffssteuerobjekte gemäß den in der Zugriffssteuerdatenbank spezifizierten Zugriffsberechtigungen gewährt und abgelehnt werden.

9. Zugriffssteuerungsverfahren nach Anspruch 6, wobei
eine zweite Teilmenge der Regelobjekte in der Zugriffssteuerdatenbank (**108**) jeweils folgendes spezifiziert: eine Menge der Gruppenobjekte, eine Menge der Managementobjekte und Zugriffsberechtigungen durch die Benutzer, die Mitglieder der durch die spezifizierte Menge der Gruppenobjekte definierten Gruppen sind, für durch die spezifizierte Menge von Managementobjekten erzeugte Ereignisbenachrichtigungen; und
an einem Ereignis-Router (**186**) durch die Managementobjekte erzeugte Ereignisbenachrichtigungen empfangen werden und entsprechende Ereignisbenachrichtigungsmeldungen nur an Benutzer in Gruppen gesendet werden, die gemäß den in der Zugriffssteuerdatenbank spezifizierten Zugriffsberechtigungen Zugriffsberechtigungen für diese Ereignisbenachrichtigungen haben.

10. Zugriffssteuerungsverfahren nach Anspruch 9, wobei
an einer Ereignisregistratur (**184**) Ereignisbenachrichtigungsanforderungen durch Benutzer registriert werden, wobei jede Ereignisbenachrichtigungsanforderung Ereignisbenachrichtigungen von spezifizierten Mengen der Managementobjekte spezifiziert, die angefordert werden;
an dem Ereignis-Router in Abhängigkeit von jeder empfangenen Ereignisbenachrichtigung entsprechende Ereignisbenachrichtigungsmeldungen an Benutzer gesendet werden, die in der Ereignisregistratur eine entsprechende Ereignisbenachrichtungsanforderung registriert haben und die gemäß den in der Zugriffssteuerdatenbank spezifizierten Zugriffsberechtigungen Zugriffsberechtigungen für die empfangene Ereignisbenachrichtigung haben.

Es folgen 7 Blatt Zeichnungen

Anhängende Zeichnungen



Stand der Technik

FIG. 1

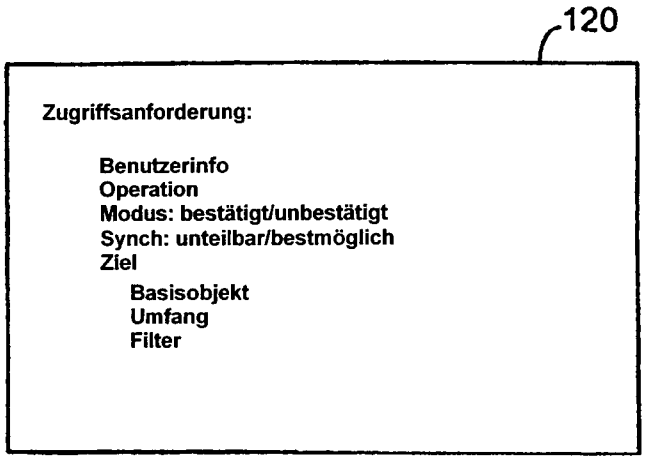


FIG. 2

Stand der Technik

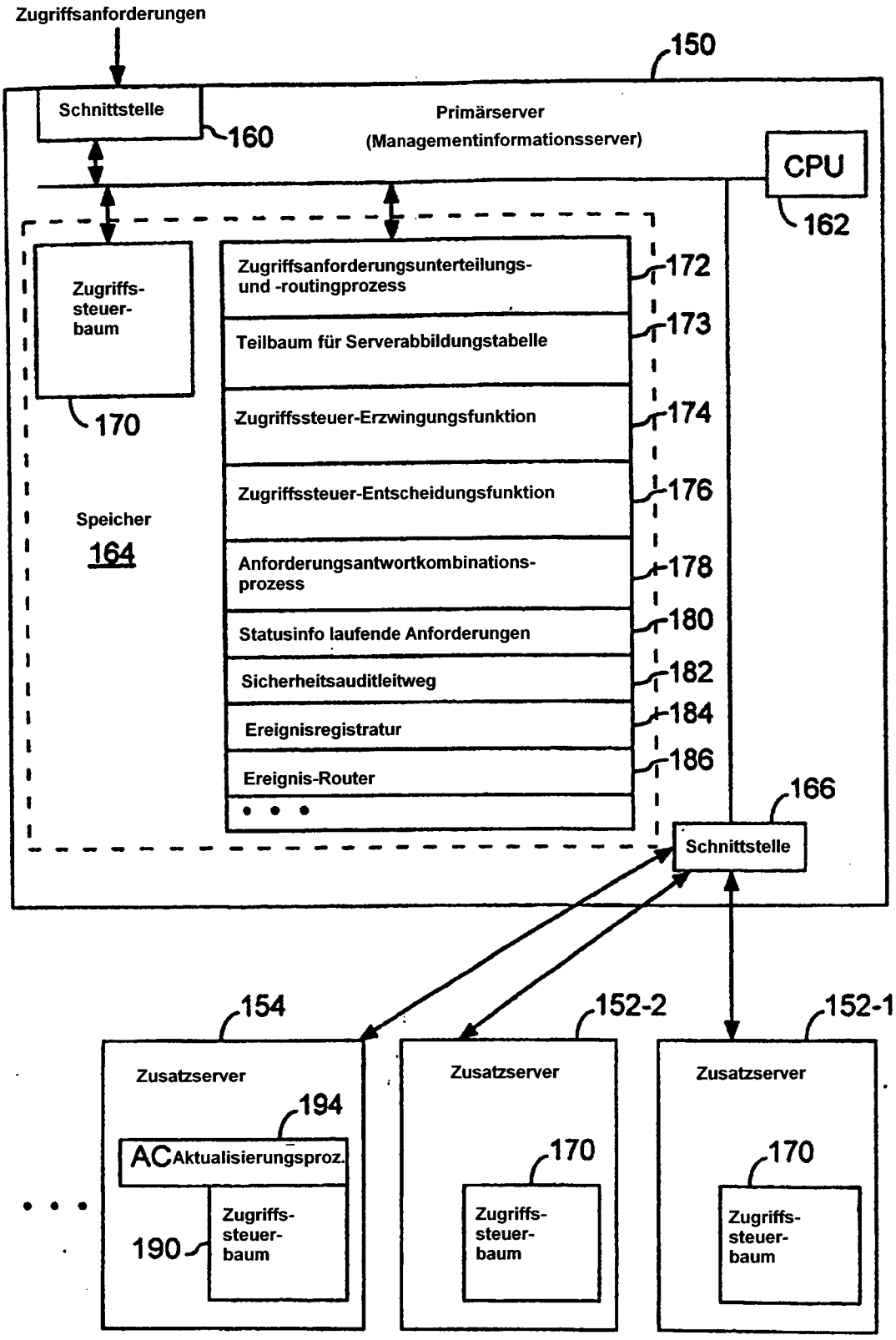

Zugriffsanforderungen
150
Schnittstelle
160
Primärserver
(Managementinformationsserver)
CPU
162
Zugriffs-
steuer-
baum
170
Speicher
164
Zugriffsanforderungsunterteilungs-
und -routingprozess
172
Teilbaum für Serverabbildungstabelle
173
Zugriffssteuer-Erzwingungsfunktion
174
Zugriffssteuer-Entscheidungsfunktion
176
Anforderungsantwortkombinations-
prozess
178
Statusinfo laufende Anforderungen
180
Sicherheitsauditleitweg
182
Ereignisregistratur
184
Ereignis-Router
186
166
Schnittstelle
154
152-2
152-1
Zusatzserver
Zusatzserver
Zusatzserver
194
AC Aktualisierungsproz.
190
Zugriffs-
steuer-
baum
170
Zugriffs-
steuer-
baum
170
Zugriffs-
steuer-
baum

FIG. 3

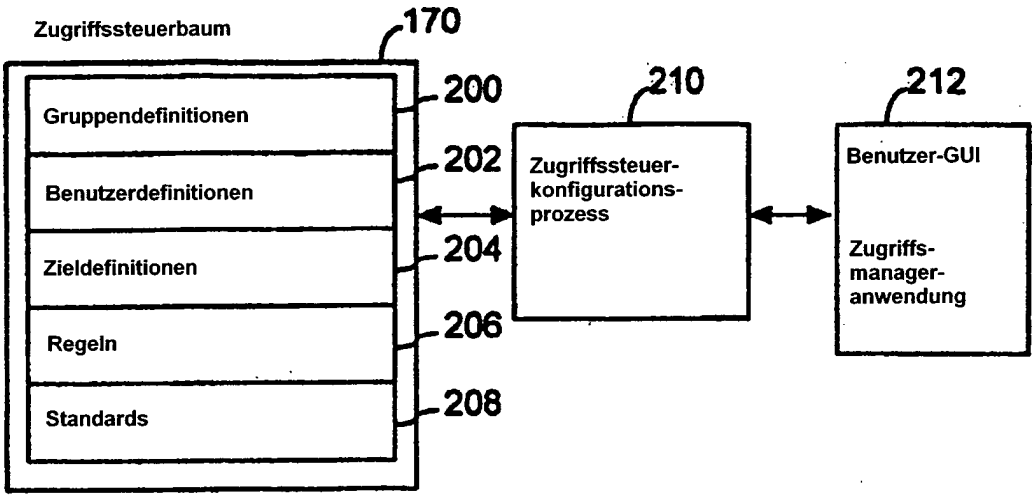

Zugriffssteuerbaum
170
Gruppendefinitionen
200
Benutzerdefinitionen
202
Zieldefinitionen
204
Regeln
206
Standards
208
210
Zugriffssteuer-konfigurations-prozess
212
Benutzer-GUI
Zugriffs-manager-anwendung

FIG. 4

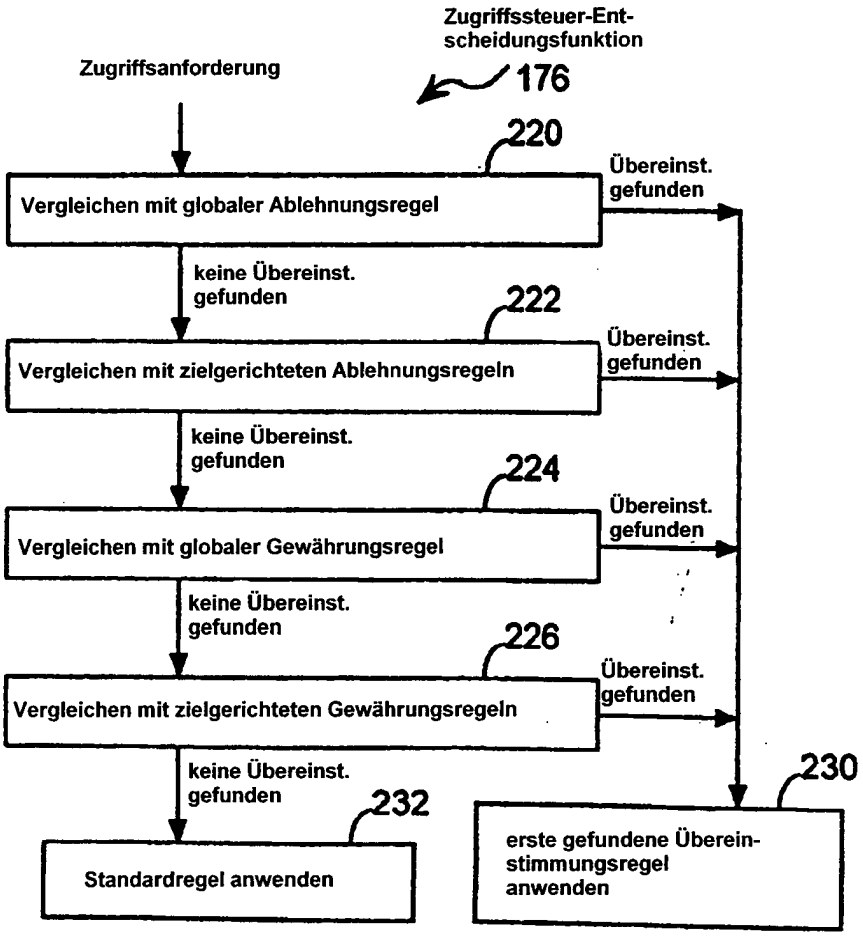

Zugriffssteuer-Ent-scheidungsfunktion
176
Zugriffsanforderung
220
Vergleichen mit globaler Ablehnungsregel
Übereinst. gefunden
keine Übereinst. gefunden
222
Vergleichen mit zielgerichteten Ablehnungsregeln
Übereinst. gefunden
keine Übereinst. gefunden
224
Vergleichen mit globaler Gewährungsregel
Übereinst. gefunden
keine Übereinst. gefunden
226
Vergleichen mit zielgerichteten Gewährungsregeln
Übereinst. gefunden
keine Übereinst. gefunden
232
Standardregel anwenden
230
erste gefundene Übereinstimmungsregel anwenden

FIG. 5

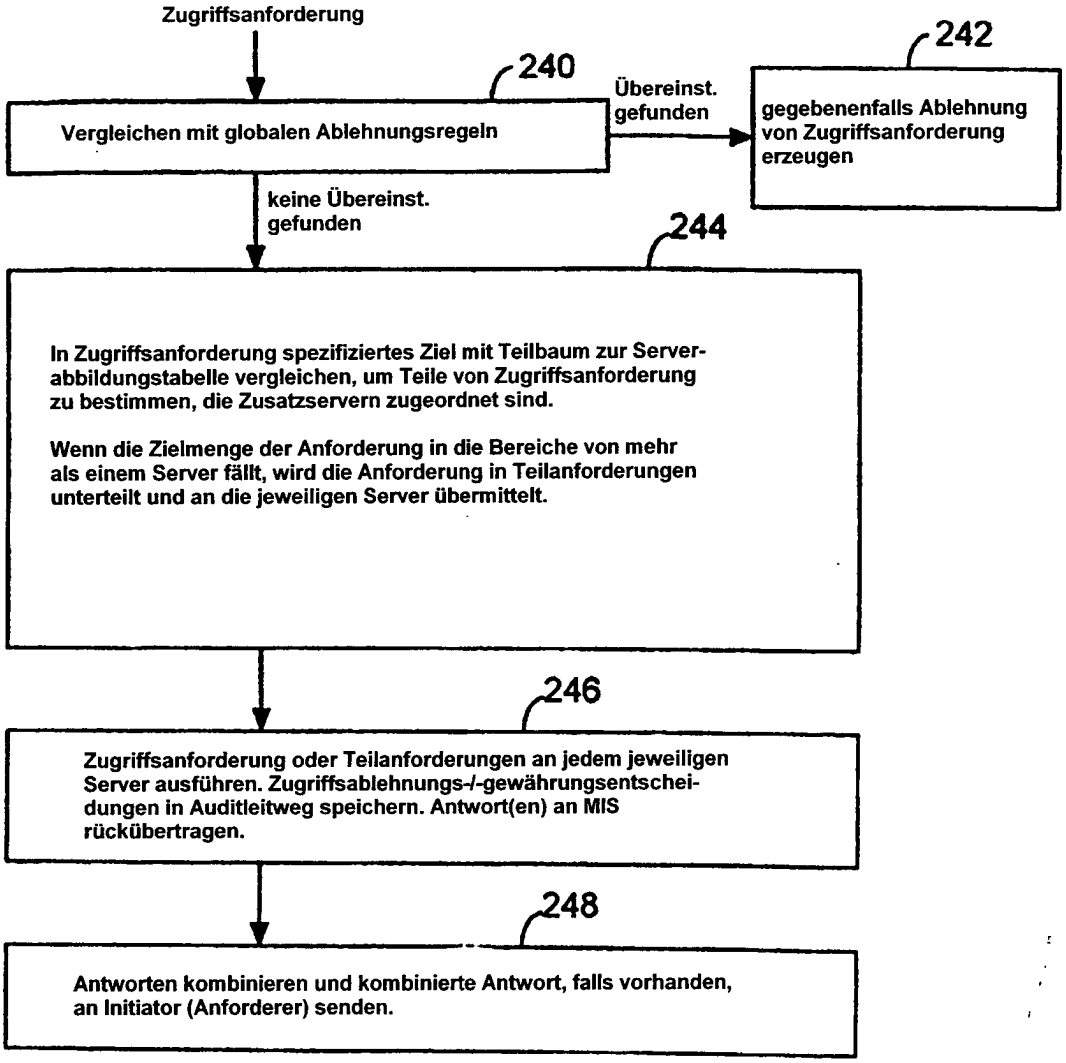

Zugriffsanforderung
240
Vergleichen mit globalen Ablehnungsregeln
Übereinst. gefunden
242
gegebenenfalls Ablehnung von Zugriffsanforderung erzeugen
keine Übereinst. gefunden
244
In Zugriffsanforderung spezifiziertes Ziel mit Teilbaum zur Serverabbildungstabelle vergleichen, um Teile von Zugriffsanforderung zu bestimmen, die Zusatzservern zugeordnet sind.
Wenn die Zielmenge der Anforderung in die Bereiche von mehr als einem Server fällt, wird die Anforderung in Teilanforderungen unterteilt und an die jeweiligen Server übermittelt.
246
Zugriffsanforderung oder Teilanforderungen an jedem jeweiligen Server ausführen. Zugriffsablehnungs-/-gewährungsentscheidungen in Auditleitweg speichern. Antwort(en) an MIS rückübertragen.
248
Antworten kombinieren und kombinierte Antwort, falls vorhanden, an Initiator (Anforderer) senden.

FIG. 6

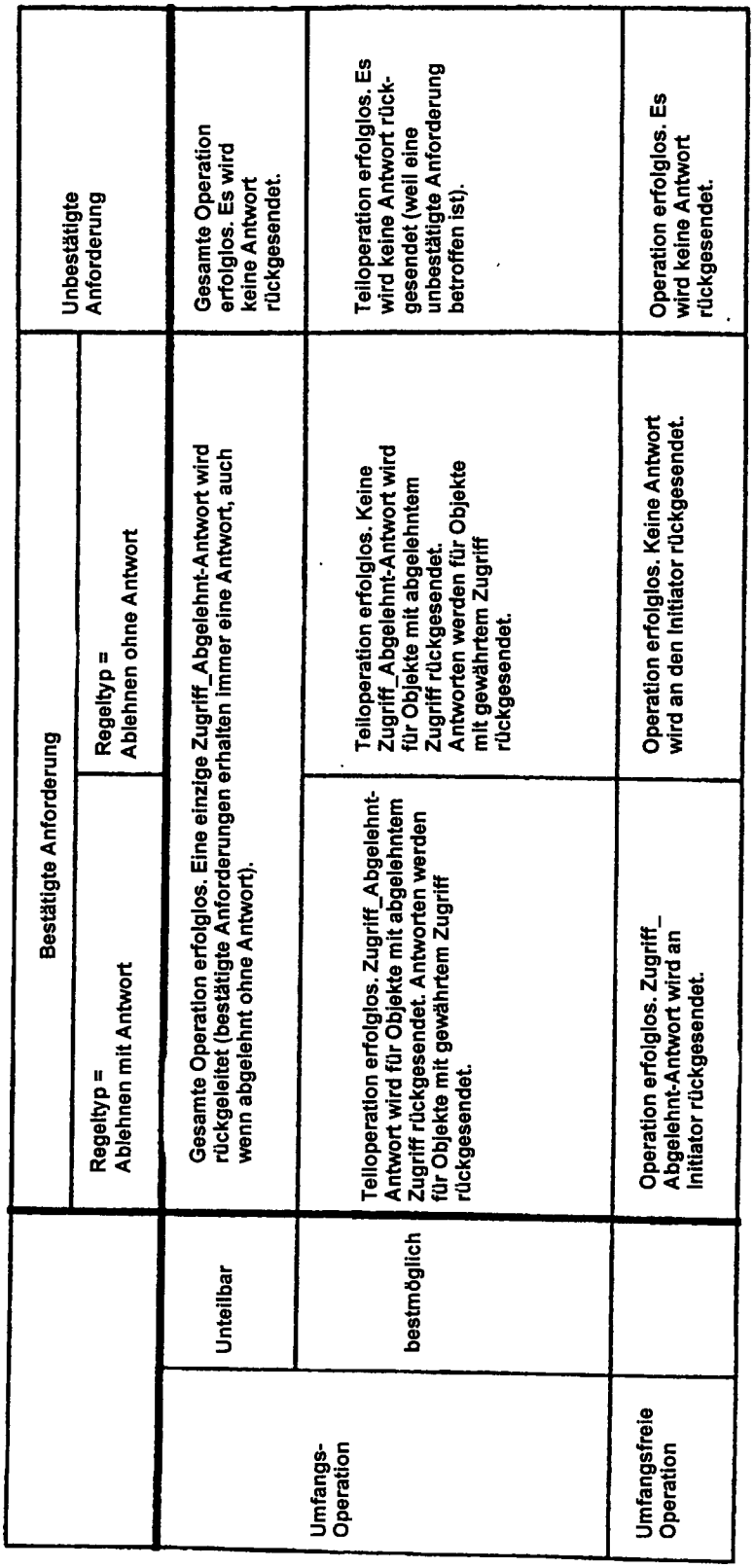

Bestätigte Anforderung
Regeltyp = Ablehnen mit Antwort
Regeltyp = Ablehnen ohne Antwort
Unbestätigte Anforderung
Umfangs-Operation
Unteilbar
bestmöglich
Umfangsfreie Operation
Gesamte Operation erfolglos. Eine einzige Zugriff_Abgelehnt-Antwort wird rückgeleitet (bestätigte Anforderungen erhalten immer eine Antwort, auch wenn abgelehnt ohne Antwort).
Gesamte Operation erfolglos. Es wird keine Antwort rückgesendet.
Teiloperation erfolglos. Zugriff_Abgelehnt-Antwort wird für Objekte mit abgelehntem Zugriff rückgesendet. Antworten werden für Objekte mit gewährtem Zugriff rückgesendet.
Teiloperation erfolglos. Keine Zugriff_Abgelehnt-Antwort wird für Objekte mit abgelehntem Zugriff rückgesendet. Antworten werden für Objekte mit gewährtem Zugriff rückgesendet.
Teiloperation erfolglos. Es wird keine Antwort rückgesendet (weil eine unbestätigte Anforderung betroffen ist).
Operation erfolglos. Zugriff_Abgelehnt-Antwort wird an Initiator rückgesendet.
Operation erfolglos. Keine Antwort wird an den Initiator rückgesendet.
Operation erfolglos. Es wird keine Antwort rückgesendet.

FIG. 7

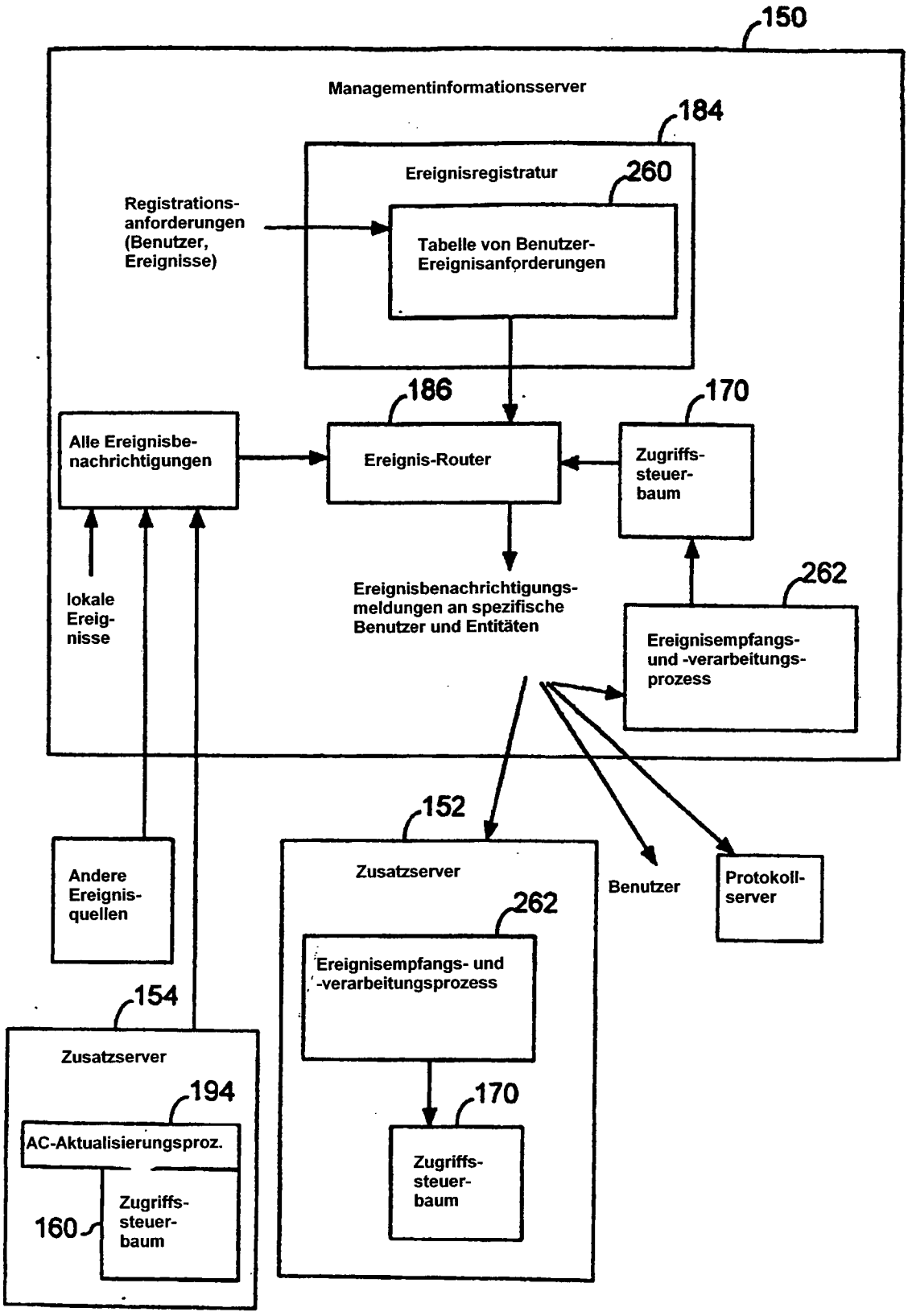

150
Managementinformationsserver
184
Ereignisregistratur
260
Registrations-
anforderungen
(Benutzer,
Ereignisse)
Tabelle von Benutzer-
Ereignisanforderungen
186
170
Alle Ereignisbe-
nachrichtigungen
Ereignis-Router
Zugriffs-
steuer-
baum
lokale
Ereig-
nisse
Ereignisbenachrichtigungs-
meldungen an spezifische
Benutzer und Entitäten
262
Ereignisempfangs-
und -verarbeitungs-
prozess
152
Andere
Ereignis-
quellen
Zusatzserver
Benutzer
Protokoll-
server
262
Ereignisempfangs- und
-verarbeitungsprozess
154
Zusatzserver
170
Zugriffs-
steuer-
baum
194
AC-Aktualisierungsproz.
160
Zugriffs-
steuer-
baum

FIG. 8

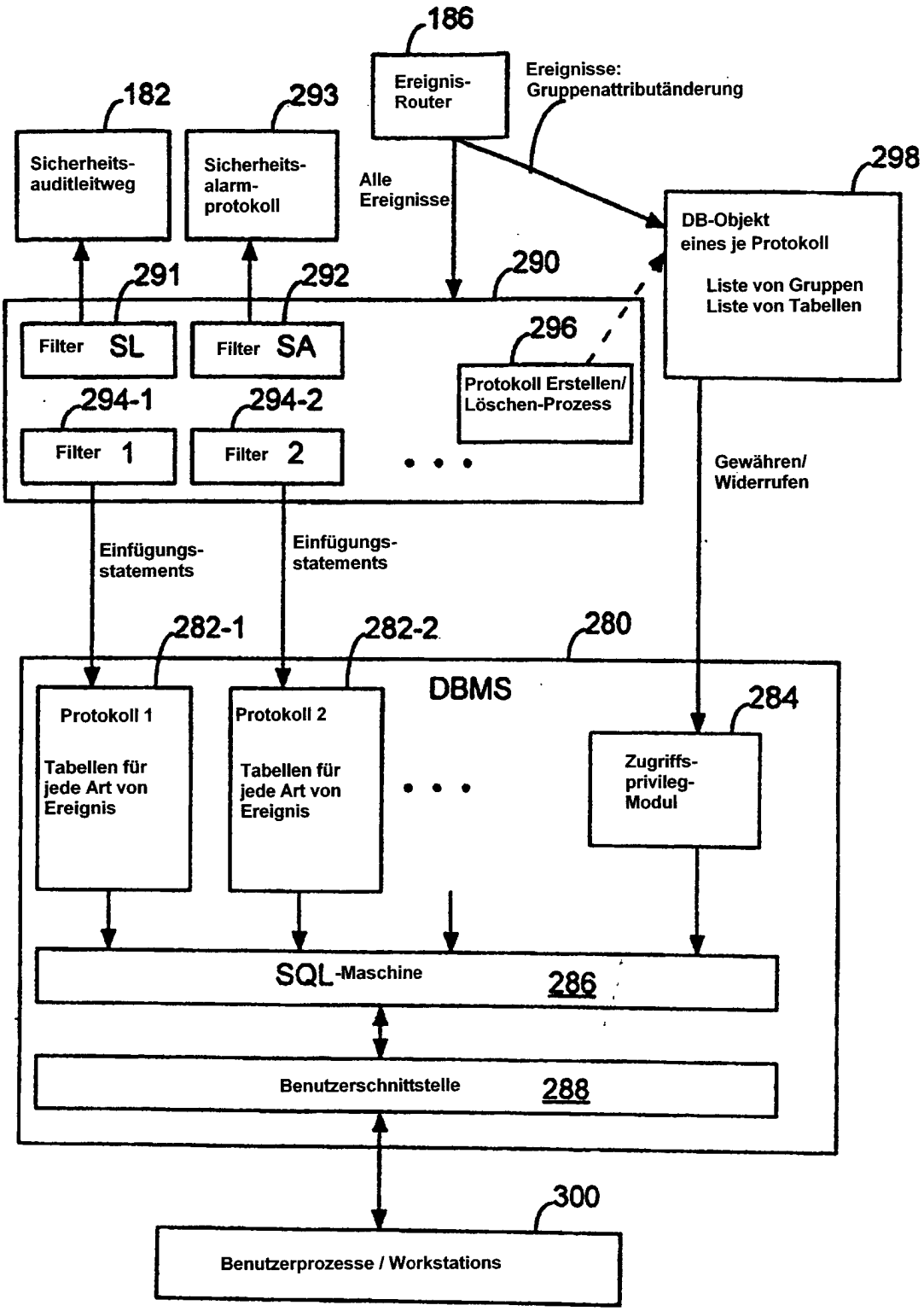

186
Ereignis-Router
Ereignisse: Gruppenattributänderung
182
Sicherheits-auditleitweg
293
Sicherheits-alarm-protokoll
Alle Ereignisse
298
DB-Objekt eines je Protokoll
Liste von Gruppen
Liste von Tabellen
291
292
290
Filter SL
Filter SA
296
Protokoll Erstellen/ Löschen-Prozess
294-1
294-2
Filter 1
Filter 2
Gewähren/ Widerrufen
Einfügungs-statements
Einfügungs-statements
282-1
282-2
280
DBMS
Protokoll 1
Tabellen für jede Art von Ereignis
Protokoll 2
Tabellen für jede Art von Ereignis
284
Zugriffs-privileg-Modul
SQL-Maschine
286
Benutzerschnittstelle
288
300
Benutzerprozesse / Workstations

FIG. 9