(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0014367
(43) 공개일자 2009년02월10일

(51) Int. Cl.
G06F 21/22 (2006.01) *G06F 12/16* (2006.01)
(21) 출원번호 10-2008-7029411
(22) 출원일자 2008년12월01일
심사청구일자 없음
번역문제출일자 2008년12월01일
(86) 국제출원번호 PCT/US2007/006598
국제출원일자 2007년03월15일
(87) 국제공개번호 WO 2007/142715
국제공개일자 2007년12월13일
(30) 우선권주장
11/421,996 2006년06월02일 미국(US)

(71) 출원인
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
프라이즈, 로버트 엠.
미국 98052-6399 워싱턴주 레드몬드 원 마이크로소프트 웨이
섭지, 쉬라즈 엠.
미국 98052-6399 워싱턴주 레드몬드 원 마이크로소프트 웨이
(74) 대리인
양영준, 백만기

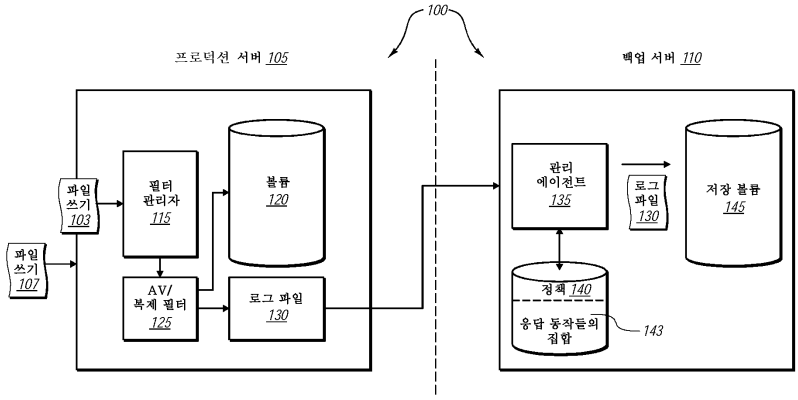
전체 청구항 수 : 총 18 항

(54) 공통 필터를 통해 바이러스 및 백업 필터링을 관리하기 위한 방법, 복제된 데이터를 관리하기 위한 방법 및 컴퓨터판독가능 매체

(57) 요 약

백업 시스템 내의 데이터는 바이러스들에 대해 효과적으로 보호될 수 있는데, 심지어 감염된 데이터가 백업 서버에 백업된 후에 특정 바이러스들에 대한 정의가 발견되었을 때에도 그렇다. 한 구현에서, 앤티바이러스 및 복제 필터링 컴포넌트를 포함하는 결합된 필터는 I/O 시스템 호출(예를 들어, 파일에 대한 쓰기를 포함하는)을 식별하고 프로세스할 수 있다. 바이러스가 존재하면, 결합된 필터의 앤티바이러스 컴포넌트는 파일 및/또는 파일 쓰기를 마킹할 수 있고 (그리고 파일/파일 쓰기를 정화할 수 있고), 그 정보를 복제 컴포넌트에 전달할 수 있다. 파일 쓰기가 백업될 파일과 관련된 경우, 복제 컴포넌트는 파일 쓰기의 카피와 함께 앤티바이러스 필터의 표지들을 전달할 수 있다. 백업 서버는 또한 백업 서버에 저장된 파일의 이전 버전들이 감염되었을 수 있다는 것을 식별할 수 있고, 따라서 임의의 적절한 동작들을 수행할 수 있다.

대 표 도 - 도1A



특허청구의 범위

청구항 1

프로덕션 서버가 하나 이상의 백업 서버에 의해 백업되는, 컴퓨터화된 환경(computerized environment) 내의 상기 프로덕션 서버(production server)에서, 공통 필터(common filter)를 통해 바이러스 및 백업 필터링(filtration)을 관리하기 위한 방법으로서,

공통 필터를 통해 파일들에 대한 하나 이상의 쓰기(writes)를 식별하는 단계;

하나 이상의 바이러스 정의에 따라, 상기 식별된 하나 이상의 파일 쓰기를 상기 공통 필터에서 스캔하는 단계;

식별된 하나 이상의 스캔된 상기 파일 쓰기를 상기 공통 필터에서 하나 이상의 복제 정책(replica policy)들과 비교하는 단계; 및

상기 하나 이상의 스캔된 파일 쓰기들 중 적어도 하나의 카피를 로그 파일에 전송하여, 상기 적어도 하나의 파일 쓰기가 백업 서버에 복제되도록 하는 단계

를 포함하는, 공통 필터를 통해 바이러스 및 백업 필터링을 관리하기 위한 방법.

청구항 2

제1항에 있어서,

상기 하나 이상의 파일 쓰기 중 적어도 하나를 하나 이상의 바이러스에 감염된 것으로서 식별하는 단계를 더 포함하는, 공통 필터를 통해 바이러스 및 백업 필터링을 관리하기 위한 방법.

청구항 3

제2항에 있어서,

상기 하나 이상의 파일 쓰기가 하나 이상의 복제 구성(replica configuration)과 비교되기 전에 상기 적어도 하나의 파일 쓰기를 하나 이상의 바이러스 표지(virus indicator)로 마킹(marking)하는 단계를 더 포함하는, 공통 필터를 통해 바이러스 및 백업 필터링을 관리하기 위한 방법.

청구항 4

제3항에 있어서,

상기 하나 이상의 바이러스 표지는 상기 바이러스가 식별되었지만 제거되지 않았음을 식별하는, 공통 필터를 통해 바이러스 및 백업 필터링을 관리하기 위한 방법.

청구항 5

제3항에 있어서,

상기 적어도 하나의 파일을 감염시키는 상기 하나 이상의 바이러스 중 임의의 것을 제거하는 단계를 더 포함하고, 상기 하나 이상의 바이러스 표지는 상기 적어도 하나의 파일 쓰기가 존재했지만 이제는 제거되었음을 식별하는, 공통 필터를 통해 바이러스 및 백업 필터링을 관리하기 위한 방법.

청구항 6

제3항에 있어서,

상기 하나 이상의 바이러스 표지와 함께 상기 적어도 하나의 파일 쓰기의 카피를 상기 로그 파일에 저장하는 단계를 더 포함하는, 공통 필터를 통해 바이러스 및 백업 필터링을 관리하기 위한 방법.

청구항 7

제3항에 있어서,

상기 백업 서버가 상기 적어도 하나의 파일 쓰기와 하나 이상의 바이러스 표지 사이의 관계를 식별할 수 있도록, 상기 적어도 하나의 파일 쓰기 및 대응하는 하나 이상의 바이러스 표지를 상기 백업 서버에 전송하는

단계를 더 포함하는, 공통 필터를 통해 바이러스 및 백업 필터링을 관리하기 위한 방법.

청구항 8

제7항에 있어서,

감염된 상기 적어도 하나의 파일 쓰기와 관련된 이전 데이터(prior data) 또한 감염되었다는 하나 이상의 표지를 상기 백업 서버에 전송하는 단계를 더 포함하는, 공통 필터를 통해 바이러스 및 백업 필터링을 관리하기 위한 방법.

청구항 9

제3항에 있어서,

감염된 상기 적어도 하나의 파일 쓰기를 복제하지 않도록 결정하는 단계를 더 포함하는, 공통 필터를 통해 바이러스 및 백업 필터링을 관리하기 위한 방법.

청구항 10

제1항에 있어서,

상기 백업 서버에 저장된 데이터를 복구하기 위한 하나 이상의 요청들을 수신하는 단계; 및

상기 하나 이상의 요청들 중 적어도 하나는 하나 이상의 바이러스 표지들과 관련된 데이터를 참조함을 식별하는 단계

를 더 포함하는, 공통 필터를 통해 바이러스 및 백업 필터링을 관리하기 위한 방법.

청구항 11

제10항에 있어서,

상기 식별된 바이러스 표지들에 기초하여 상기 하나 이상의 요청들에 대해 하나 이상의 응답들을 전송하는 단계를 더 포함하는, 공통 필터를 통해 바이러스 및 백업 필터링을 관리하기 위한 방법.

청구항 12

제11항에 있어서,

상기 하나 이상의 응답들 중 적어도 하나는 상기 요청된 데이터가:

(i) 하나 이상의 바이러스와 관련됨

(ii) 하나 이상의 바이러스로 인해 복구될 수 없음, 또는

(iii) 상기 하나 이상의 바이러스들이 우선 제거되었을 경우에만 복구될 수 있음

을 나타내는, 공통 필터를 통해 바이러스 및 백업 필터링을 관리하기 위한 방법.

청구항 13

백업 서버가 하나 이상의 프로덕션 서버에서 데이터를 백업하는, 컴퓨터화된 환경 내의 상기 백업 서버에서, 하나 이상의 프로덕션 서버에서 공통 필터에 의해 제공된 하나 이상의 바이러스 표지들에 따라, 복제된 데이터를 관리하기 위한 방법으로서,

하나 이상의 프로덕션 서버로부터 하나 이상의 데이터 백업들을 수신하는 단계;

수신된 상기 하나 이상의 데이터 백업 내의 하나 이상의 바이러스 표지들을 식별하는 단계 -상기 하나 이상의 바이러스 표지들은 상기 하나 이상의 데이터 백업들 중 적어도 하나는 감염된 데이터와 관련됨을 식별함-;

상기 백업 서버에 대해 하나 이상의 정책들을 식별하는 단계 -상기 하나 이상의 정책들은 상기 하나 이상의 바이러스 표지들에 대응되는 하나 이상의 응답 동작(response action)을 식별함-; 및

상기 하나 이상의 정책들에 따라 상기 하나 이상의 응답 동작들 중 임의의 것을 실행하는 단계

를 포함하는, 복제된 데이터를 관리하기 위한 방법.

청구항 14

제13항에 있어서,

상기 하나 이상의 응답 동작들 중 임의의 것은 상기 하나 이상의 바이러스 표지들과 관련된 상기 수신된 하나 이상의 데이터 백업들 중 임의의 것으로부터 하나 이상의 바이러스들을 제거하는 단계를 포함하는, 복제된 데이터를 관리하기 위한 방법.

청구항 15

제13항에 있어서,

상기 하나 이상의 응답 동작들 중 임의의 것은:

상기 하나 이상의 바이러스 표지들과 관련된 상기 하나 이상의 데이터 백업들의 적어도 일부를 정화(cleansing)하는 단계; 및

상기 백업 서버에 저장된 상기 일부의 이전 카피(prior copy)를 정화하는 단계

를 포함하는, 복제된 데이터를 관리하기 위한 방법.

청구항 16

제13항에 있어서,

상기 하나 이상의 응답 동작들 중 임의의 것은, 상기 하나 이상의 데이터 백업들 중 임의의 것의 상기 하나 이상의 바이러스 표지들을 식별하는 것에 적어도 부분적으로 기초하여 데이터의 기준 카피(baseline copy)가 하나 이상의 바이러스와 관련됨을 식별하는 단계를 포함하는, 복제된 데이터를 관리하기 위한 방법.

청구항 17

제16항에 있어서,

상기 백업 서버에서 상기 데이터의 기준 카피와 관련된 데이터에 대한 하나 이상의 요청들을 수신하는 단계; 및

상기 요청된 데이터의 적어도 일부는 하나 이상의 바이러스 표지들과 관련되었다는 응답을 전송하는 단계

를 더 포함하는, 복제된 데이터를 관리하기 위한 방법.

청구항 18

프로덕션 서버가 하나 이상의 백업 서버에 의해 백업되는, 컴퓨터화된 환경 내의 프로덕션 서버에서, 실행되었을 때 하나 이상의 프로세서로 하여금,

공통 필터를 통해 파일들에 대한 하나 이상의 쓰기를 식별하는 단계;

하나 이상의 바이러스 정의에 따라, 상기 식별된 하나 이상의 파일 쓰기를 상기 공통 필터에서 스캔하는 단계;

식별된 하나 이상의 스캔된 상기 파일 쓰기를 상기 공통 필터에서 하나 이상의 복제 정책들과 비교하는 단계; 및

상기 하나 이상의 스캔된 파일 쓰기들 중 적어도 하나의 카피를 로그 파일에 전송하여, 상기 적어도 하나의 파일 쓰기가 백업 서버에 복제되도록 하는 단계

를 포함하는 방법을 수행하도록 하는 컴퓨터 실행가능 명령어들을 갖는 컴퓨터 판독가능 매체.

명 세 서

배 경 기 술

<l> 적어도 부분적으로는 전자 파일들의 편재성(ubiquity)에 의해, 개인 및 조직들은 마찬가지로 정기적으로 전자 파일들을 보호할 필요가 있다. 전자 파일들을 보호하는 한 방법은 데이터에 대한 신뢰할 수 있는 복원을 생성

하기 위해 주기적으로 파일들을 백업하는 것이다. 개인 수준에서든 또는 기업 수준에서든, 이를 위한 기존의 백업 시스템들은 데이터에 대한 쓰기들(writes to data)이 백업 서버에 백업되어야 하는 것인지를 식별하는 하나 이상의 복제 필터(replication filter)를 포함할 수 있다. 예를 들어, 사용자는 데이터에 하나 이상의 쓰기를 할 수 있고, 그러면 복제 필터는 각 쓰기를 인터셉트(intercept)하고, 그 쓰기가 보호되어야 할(즉, 백업되어야 할) 데이터와 관련되는지를 결정한다. 파일이 보호되어야 하는 것이면, 복제 필터는 복수의 이러한 쓰기들의 로그 파일에 쓰기를 전달할 수 있다.

<2> 다음, 로그 파일(또는 그것의 대응하는 카피)은 하나 이상의 백업 서버에 전송될 수 있다. 예를 들어, 개인용 컴퓨터의 사용자는 로그 파일 및/또는 임의의 다른 이러한 식별된 데이터를, 특정 백업 서버와 관련된 것과 같은 하나 이상의 로컬 또는 원격 저장소 할당(storage allocation)에 복제하는 하나 이상의 백업 프로세스를 실행할 수 있다. 마찬가지로, 프로덕션 서버(production server)의 하나 이상의 복제 에이전트(replica agent)는 프로덕션 서버에 로그 파일의 백업을 스케줄링(schedule)할 수 있고, 다음, 새로운 데이터 쓰기들을 백업 서버에 있는 하나 이상의 저장 할당들에 전달할 수 있다. 그러면 이후의 시점에서, 사용자(또는 프로덕션 서버 관리자)는 백업 서버로부터 복제된 로그 파일과 관련된 데이터를 요청할 수 있다.

<3> 그러나, 이러한 방식으로 데이터를 백업하는 것은 데이터를 보호하는 한가지 방법일 뿐이다. 데이터를 보호하기 위한 다른 방법들은, 예를 들어, 바이러스 스캐닝(virus scanning)을 포함한다. 구체적으로, 컴퓨터 바이러스가 데이터를 파괴하고, 컴퓨터 시스템들에도 해를 가하여(wreak having on computer systems), 처음에 감염되지 않은 파일들의 더 많은 손실을 가져올 수 있다. 따라서, 이러한 위협을 완화하기 위해 사용자 또는 관리자는 하나 이상의 컴퓨터 시스템에 하나 이상의 앤티바이러스 프로그램을 설치할 수 있다. 기존의 앤티바이러스 소프트웨어가 동작할 수 있는 한 방법은, 특정 파일에 대한 쓰기를 식별한 후 쓰기들이 알려진 바이러스를 포함하는지를 확인하기 위해 쓰기를 스캔하는 하나 이상의 앤티바이러스 필터를 통해서이다. 바이러스를 인식하는 앤티바이러스 소프트웨어의 능력은 통상적으로, 파일 쓰기들을 스캔할 때 앤티바이러스 필터가 검사하는 앤티바이러스 정의들의 집합에 기초한다. 이로써, 앤티바이러스 필터가 바이러스를 식별하는지의 여부는 앤티바이러스 정의들이 얼마나 최신의 것인지(up-to-date)에 의존한다. 구체적으로, 앤티바이러스 소프트웨어가 최근에 업데이트되지 않은 경우, 앤티바이러스 필터(들)는 특정 파일이 실제로 최근에 생성된 바이러스를 포함하더라도 그 파일(또는 파일 쓰기)이 깨끗(clean)하다고 식별할 수 있다.

<4> 따라서, 엔티티(개인 또는 조직 등)는 데이터를 보호하기 위해 다수의 다른 프로그램들을 설치할 수 있으며, 이는 서로로부터 독립적으로 동작하는 다수의 다른 소프트웨어 필터들을 포함할 수 있다는 것을 이해할 수 있다. 한 기존의 예에서, 필터가 있는 각 소프트웨어 프로그램은 먼저 그 필터(예를 들어, 앤티바이러스 필터 및/또는 복제 필터)를 운영 체제의 필터 관리자에 등록한다. 다음, 필터 관리자는 각 파일 쓰기를, 필요할 때 또는 필요한 경우, 각 필터에 전달한다. 일반적으로, 임의의 필요한 순서화(ordering)를 보장하기 위해 각 소프트웨어 필터가 어떻게 필터 관리자에 등록되어야 하는지를 구성하기 어려울 수 있다. 따라서, 필터 관리자가 파일 쓰기들을 복제 필터에 전송하고, 다음, 앤티바이러스 필터에 전송할 수 있다. 물론 다른 경우에, 필터 관리자는 파일 쓰기를 복제 필터에 전송하기 전에 먼저 앤티바이러스 필터에 전송할 수 있다.

<5> 불행하게도, 필터들의 구체적인 순서화(ordering)를 구성하기 어려울 수 있지만, 필터들의 순서화는 데이터가 어떻게 보호되고/거나 보존되는지에 대해 상당한 영향을 가질 수 있다. 예를 들어, 백업 시스템들을 구현하는 조직들에서의 하나의 특히 민감한 문제는, 특정 전자 바이러스들에 대한 처리의 실패(failure to account for)가 잠재적으로 백업 프로세스 중에서의 바이러스들의 더 큰 확산을 의미할 수 있다는 것이다. 예를 들어, 복제 필터가 파일 쓰기들을 수신하고, 파일들이 앤티바이러스 필터에 의해 검토되기 전에 그 파일들을 로그 파일에 전송하는 경우 문제는 특히 심각할 수 있다. 이러한 필터들의 순서화는 몇몇 경우에서, 파일이 백업 서버에 전달된 이후가 될 때까지, 감염된 파일이 감염된 것으로 취급되거나 심지어 식별되지 않을 수 있다는 것을 의미한다.

<6> 반대로, 복제 필터 전에 앤티바이러스 필터가 파일 쓰기를 수신한다는 것이 보장가능할지라도, 이는 모든 잠재적 문제들을 반드시 해결하는 것은 아니다. 예를 들어, 앤티바이러스 필터에 사용되는 앤티바이러스 정의들이 오래된 것(out-of-date)인 경우, 예를 들어 파일을 감염시키는 바이러스에 대한 정의가 아직 생성되지 않은 경우, 컴퓨터 시스템 상의 감염된 파일은 검출되지 않은 채로 있을 수 있다. 따라서, 먼저 앤티바이러스 필터에 의해 검사되었을지라도 파일은 복제 필터에 의해 한번 이상 복제되었을 수 있다. 따라서, 이는 백업 서버에 파일의 감염된 버전의 여러 백업 카피들이 존재할 수 있다는 것을 의미할 수 있다. 이 특정 바이러스를 포함하도록 앤티바이러스 필터의 앤티바이러스 정의들이 업데이트되면, 앤티바이러스 필터는 결국 새로운 파일 쓰기들이

감염되었음을 식별할 수 있다.

<7> 그러나, 대부분의 경우, 앤티바이러스 필터는 감염된 파일 및/또는 대응하는 전체 기본 파일(base file)을 프로덕션 서버에서 간단히 스크럽(scrub) 또는 삭제한다. 불행하게도, 복제 필터는 일반적으로 바이러스 ID(virus identification) 및/또는 앤티바이러스 필터에 의한 정화 동작(cleansing action)들에 대한 어떠한 지식도 없을 것이며, 따라서 단순히 정화된 파일 쓰기들을 복제할 것이다. 다음, 정화된 파일에 대한 복제된 파일 및/또는 파일 쓰기들이 로그 파일에 전달되고/거나 달리 일반적으로 이루어지는 바와 같이 다시 백업 서버에 복제된다. 따라서, 백업 서버는 파일이 감염되었었다는 것에 대해 인식하지 못할 것이고, 파일 백업 업데이트들(즉, 새로운 파일 쓰기들을 포함하는)을 이전에 감염된 파일 데이터와 함께 단순히 저장할 것이다. 따라서, 프로덕션 서버에서 앤티바이러스 필터가 복제 필터 앞에 위치하더라도, 백업 서버에 있는 감염된 데이터가 정화된다는 보장이 없다.

<8> 따라서, 백업 시스템에서 바이러스 정보를 어드레스(addressing)하는 것과 관련된 다수의 어려움이 있다.

<9> <발명의 요약>

<10> 본 발명의 구현들은 백업 환경에서 데이터 전체에 걸쳐 앤티바이러스 정보를 효과적으로 전달(propagate)하는 시스템, 방법, 및 컴퓨터 프로그램 제품을 제공한다. 적어도 하나의 구현에서, 예를 들어, 공통 필터(common filter)는 앤티바이러스 및 복제 필터 컴포넌트들을 포함한다. 공통 필터는 파일 쓰기들을 수신할 수 있고, 파일 쓰기들을 앤티바이러스 컴포넌트에 전달할 수 있다. 앤티바이러스 컴포넌트는 각 파일 쓰기를 스캔하고, 각 스캔된 파일 쓰기를 그 파일 쓰기에 대한 임의의 적절한 앤티바이러스 정보와 함께 공통 필터의 복제 필터 컴포넌트에 전달한다. 따라서 복제 필터는 이전에 검출되었을 수 있는 임의의 바이러스 정보를 유지하는 방식으로 특정 파일 쓰기들을 로그 파일에 복제할 수 있다. 따라서, 프로덕션 서버 및 백업 서버 모두 수신된 백업 데이터, 또는 이전에 수신된 백업 데이터가 앤티바이러스 치료(antivirus attention)를 받아야하는지를 식별할 수 있다.

<11> 예를 들어, 프로덕션 서버의 관점에서, 공통 필터를 통해 바이러스 및 백업 필터링(filtration)을 관리하는 한 예시적인 방법은 공통 필터를 통해 파일들에 대한 하나 이상의 쓰기를 식별하는 것을 포함할 수 있다. 또한, 본 방법은 하나 이상의 바이러스 정의에 따라 공통 필터에서 식별된 하나 이상의 파일 쓰기를 스캔하는 것을 포함할 수 있다. 본 방법은 또한 공통 필터에 있는 식별된 하나 이상의 스캔된 파일 쓰기를 하나 이상의 복제 정책들과 비교하는 것을 포함할 수 있다. 또한, 본 방법은 하나 이상의 스캔된 파일 쓰기들 중 적어도 하나의 카피를 로그 파일에 전송하여, 적어도 하나의 파일 쓰기가 백업 서버에 복제되도록 하는 것을 포함할 수 있다.

<12> 반대로, 백업 서버의 관점에서, 하나 이상의 바이러스 표지(virus indicator)에 따라 복제된 데이터를 관리하기 위한 예시적인 방법은 하나 이상의 프로덕션 서버로부터 하나 이상의 데이터 백업을 수신하는 것을 포함할 수 있다. 또한, 본 방법은 수신된 하나 이상의 데이터 백업에 있는 하나 이상의 바이러스 표지를 식별하는 것을 포함할 수 있다. 이러한 경우, 하나 이상의 바이러스 표지는 하나 이상의 데이터 백업들 중 적어도 하나가 감염된 데이터와 관련됨을 식별할 수 있다. 본 방법은 또한 백업 서버에 대한 하나 이상의 정책들을 식별하는 것을 포함할 수 있다. 일반적으로, 하나 이상의 정책들은 하나 이상의 바이러스 표지에 대응되는 하나 이상의 응답 동작들을 식별할 수 있다. 또한, 본 방법은 하나 이상의 정책들에 따라 하나 이상의 응답 동작들 중 임의의 것을 실행하는 것을 포함할 수 있다.

<13> 본 발명의 요약은 아래의 상세한 설명에서 상세히 설명되는 개념들의 선택을 간략한 형태로 소개하기 위해 제공된 것이다. 본 발명의 요약은 청구된 본 발명의 주요 특징 또는 본질적 특징들을 식별하기 위한 것이 아니며, 또한 청구된 본 발명의 범위를 결정하는 데 있어 보조물로서 사용되도록 하기 위한 것이 아니다.

<14> 본 발명의 추가적인 특징 및 이점들은 이어지는 설명에서 제시될 것이며, 부분적으로 설명으로부터 명백해질 것이고, 또는 본 발명의 실행에 의해 습득될 것이다. 본 발명의 특징 및 이점들은 첨부된 청구항들에서 구체적으로 제시된 수단 및 조합들에 의해 실현되고 획득될 수 있다. 이들 및 본 발명의 다른 특징들은 이어지는 설명 및 첨부된 청구항으로부터 더 완전히 명백해질 것이며, 또는 이후에 제시되는 바와 같은 본 발명의 실행에 의해 습득될 것이다.

실 시 예

<20> 본 발명의 구현은 백업 환경에서 데이터 전체에 걸쳐 앤티바이러스 정보를 효과적으로 전달하는 시스템, 방법, 및 컴퓨터 프로그램 제품으로 확장된다. 예를 들어, 적어도 하나의 구현에서, 공통 필터는 앤티바이러스 및 복

제 필터 컴포넌트들을 포함한다. 공통 필터는 파일 쓰기들을 수신할 수 있고, 그 파일 쓰기들을 앤티바이러스 컴포넌트에 전달할 수 있다. 앤티바이러스 컴포넌트는 각 파일 쓰기를 스캔하고, 각 스캔된 파일 쓰기를 그 파일 쓰기에 대한 임의의 적절한 앤티바이러스 정보와 함께 공통 필터의 복제 필터 컴포넌트에 전달한다. 따라서 복제 필터는 이전에 검출되었을 수 있는 임의의 바이러스 정보를 유지하는 방식으로 특정 파일 쓰기들을 로그 파일에 복제할 수 있다. 따라서, 프로덕션 서버 및 백업 서버 모두 수신된 백업 데이터, 또는 이전에 수신된 백업 데이터가 앤티바이러스 치료를 받아야하는지를 식별할 수 있다.

<21> 여기에서 더 완전히 이해되는 바와 같이, 이들 및 본 발명의 다른 특징들은 임의의 수의 컴포넌트, 모듈, 및 스킴을 사용하여 달성될 수 있다. 예를 들어, 아래에서 본 발명의 구현들은 프로덕션 서버에서 생성되고/거나 변경된 데이터를 통신하는 프로덕션 서버와 백업 서버의 관점에서 우선적으로 설명된다. 그러나 이러한 설정(setup)은 모든 구현들에서 반드시 요구되는 것은 아니다. 구체적으로, 프로덕션 서버는 몇몇 경우에서 다른 컴퓨터 시스템에 의해 직접 백업되는(이러한 컴퓨터 시스템이 "서버"로서 간주되는지에 상관없이) 개인용 컴퓨터 시스템을 나타낼 수 있다.

<22> 또한, 여기에서 본 발명의 구현들은 앤티바이러스 및 복제 필터-유형 컴포넌트 기능이 액세스되는 단일의 공통 인터페이스를 제공하는 "공통" 필터에 의해 이루어지는 동작들과 관련하여 우선적으로 설명된다. 따라서 공통 필터는 "결합된(combined)" 필터로서 설명될 수 있는데, 이는 앤티바이러스 필터와 복제 필터의 결합된 기능들을 제공하는 필터이다. 여기에서 이해되는 바와 같이, 어쨌든, 단일 필터가 앤티바이러스 컴포넌트 및 복제 필터링 컴포넌트 모두로 구성될 수 있기 때문에, 단일 필터를 생성하는 개발자는 각 컴포넌트에 대해 순서화(ordering)를 설계할 수 있다. 즉, 개발자는 입력/출력("I/O") 시스템 호출이 예를 들어, 먼저, 앤티바이러스 컴포넌트에 의해 다루어지고, 다음, 복제 컴포넌트에 의해 다루어지도록 필터를 구성할 수 있다. 따라서, 앤티바이러스 및 복제 필터링 활동들을 다루기 위해 공통 필터와 같은 단일 필터만이 필터 관리자에 등록될 필요가 있다.

<23> 그러나, 결합된/공통 필터는 본 발명의 하나 이상의 구현들을 달성하기 위한 한 방법일 뿐이라는 것을 이해해야 한다. 예를 들어, 대안적인 구현들에서, 개발자는 특정 순서로 서로 통신하고 식별하기 위한 적절한 수단들을 갖는 개별적인 앤티바이러스 필터와 복제 필터를 생성할 수 있다. 구체적으로, 앤티바이러스 필터 및 복제 필터는 프로덕션 서버에 개별적으로 설치될 수 있지만, 필터 관리자에 대해 특정 순서를 보장하도록 구체적 순서로 설치된다. 그러면, 앤티바이러스 필터 및 복제 필터는, 예를 들어, 대역 외(out-of-band) 통신 채널을 통해 서로 통신하고 식별할 수 있는 하나 이상의 수단을 구비할 수 있다. 따라서, 이어지는 설명 및 청구항을 읽은 후, 여기에 설명된 원리들을 실행할 수 있는 다수의 방법들이 있음을 이해할 것이다.

<24> 어쨌든, 도 1A는 프로덕션 서버(105)가 하나 이상의 파일 쓰기를 수신하고, 그 파일 쓰기들을 공통 필터의 앤티바이러스 및 복제 컴포넌트들로 스캔하고, 그 쓰기들 중 하나 이상을 백업 서버(110)에 전달하는 백업 시스템(100)의 개략적인 개략도를 도시한다. 일반적으로, 파일 쓰기(예를 들어, 103, 107)는 사용자(또는 다른 엔티티)가 데이터를 생성하거나, 기존의 데이터를 수정하거나 변경하는 등의 임의의 시점에 생성될 수 있다. 그러면, 프로덕션 서버(105)는 임의의 수의 메커니즘을 이용하여 이들 각 파일 쓰기들을 인터셉트(intercept)하거나 "필터링"할 수 있다. 본 발명의 적어도 하나의 구현에서, 예를 들어, 프로덕션 서버(105)는 필터 관리자(115)를 통해 각 파일 쓰기(103, 107)를 인터셉트하고 수신한다.

<25> 일반적으로, 필터 관리자(115)는 프로덕션 서버(105)에서 각 I/O 시스템 호출을 인터셉트하고, 각각의 이러한 호출을 하나 이상의 등록된 필터들(예를 들어, 필터(125, 127), 도 1B)에 전달하도록 구성될 수 있다. 이러한 호출들은 "파일 열기(open file)", "파일 닫기(close file)"뿐 아니라 파일들에 대한 다양한 쓰기, 삭제, 변경 기타 등등과 같은 임의의 수의 시스템 요청들을 포함할 수 있다. 구체적으로, 파일에 대한 각 변경은 I/O 시스템 호출을 생성할 수 있고, 몇몇 경우에서 필터 관리자(115)가 인터셉트하도록 구성된 것인 수십 또는 수백 개의 서로 다른 I/O 시스템 호출들이 있을 수 있다. 어떻게 구성되었든 간에, 필터 관리자(115)는 자신이 인터셉트하는 다양한 호출들을 거기에 등록된 임의의 수의 필터들에 궁극적으로 분배(distribute)할 것이다. 구체적으로, 앤티바이러스 필터와 같은 몇몇 필터들은 필터 관리자(115)에 의해 인터셉트되는 모든 호출들을 수신하도록 구성될 수 있고, 한편, 다른 필터들은 I/O 시스템의 특정 유형의 호출들만을 수신하도록 구성될 수 있다.

<26> 본 발명의 적어도 한 구현에서, 필터 관리자(115)는 모든 시스템 호출(예를 들어, 파일 쓰기)들을 결합된 앤티바이러스("AV") 및 복제 필터(125)(또는 "결합된" 또는 "공통" 필터(125))에 전달하도록 구성될 수 있다. 예를 들어, 필터 관리자(115)는 파일 쓰기(103, 107)들을 수신하고, 각각의 이들 파일 쓰기를 공통 필터(125)에 전달한다. 여기에서 더 충분히 이해되는 바와 같이, 다음, 공통 필터(125)는 바이러스에 대해 각각의 수신된 파일

쓰기를 스캔할 수 있고, 만약 필요하다면, 이들 파일 쓰기 중 하나 이상의 임의의 것을 로그 파일(130)에 전달할 수 있다. 일반적으로, 로그 파일(130)과 같은 "로그 파일"은, 보통, 특정 프로덕션 서버(105) 볼륨에 대해 특정된 데이터(specified data)에 대한 모든 변경들(생성, 삭제, 수정 등)의 카피를 보유(hold)하도록 구성된 하나 이상의 전자 파일들을 포함한다. 예를 들어, 로그 파일(130)은 특정 시간에서의 볼륨(120)에 대한 모든 변경들을 나타낼 수 있다.

<27> 그러면 백업 서버(110)는 로그 파일(130)(뿐 아니라 프로덕션 서버(105)에서의 다른 볼륨들에 대한 임의의 추가적인 로그 파일)을 백업할 수 있다. 일반적으로, 백업 프로세스는 임의의 수의 상황들에서 수행될 수 있는데, 예를 들어, 요구에 따라(on demand), 또는 특정 백업 스케줄에 따라 수행될 수 있다. 모든 경우에서, 백업 프로세스는 일반적으로 프로덕션 서버(105)가 로그 파일(130)의 데이터를 백업 서버(110)에 있는 하나 이상의 관리 에이전트(예를 들어, 135)에 전송하는 것을 포함한다. 통상적으로, 다음, 하나 이상의 관리 에이전트(예를 들어, 135)는 특정 데이터에 대한 변경들의 다른 이전의 카피들을 포함할 수 있는 하나 이상의 저장 볼륨(예를 들어, 145)에 수신된 데이터 변경들을 적용할 수 있다.

<28> 그러나, 본 발명의 구현들에 따라, 하나 이상의 관리 에이전트(예를 들어, 135)는 특정 응답 동작(143)을 수행함에 따라, 수신된 백업 데이터를 하나 이상의 정책 설정들(140)에 비교할 수 있다. 여기에서 더 충분히 이해되는 바와 같이, 예를 들어, 관리 에이전트(135)가 로그 파일(130) 내의 임의의 데이터가 바이러스에 대해 플래깅(flagged)된 것(즉, 하나 이상의 바이러스 표지를 포함)을 식별하면, 정책 설정들(140)은 백업 서버(110)로 하여금 임의의 수의 대응하는 응답 동작(143)들을 수행하도록 지시할 것이다. 예를 들어, 정책 설정들(140)은 백업 서버(110)에게 바이러스들로 마킹된 수신된 데이터를 삭제하고, 수신된 백업 데이터를 "스크럽(scrub)"(즉, 바이러스를 정화(clean) 또는 제거)하거나 삭제하고, 그 뿐 아니라 데이터의 이전 카피들도 스크럽하거나 삭제하도록 지시할 수 있다.

<29> 따라서, 본 발명의 적어도 한 양상은 바이러스들에 대해 스캔하는 것을 포함할 뿐 아니라, 또한 바이러스 검출에 대한 임의의 정보가 시스템(100) 내의 관련된 엔티티들에게 효과적으로 전달될 수 있음을 보장하는 것을 포함한다. 적어도 하나의 구현에서, 예를 들어, 이는 파일 쓰기들을 하나 이상의 바이러스 표지들로 태깅(tagging)하고, 필요에 따라, 하나 이상의 바이러스 표지들이 첨부(attach)된 채로 유지됨을 보장함으로써 이루어질 수 있다. 예를 들어, 도 1B는 본 발명의 구현에 따라 더 상세한 개략도를 도시하며, 여기서 프로덕션 서버(105)는 공통 필터(125)를 통해 하나 이상의 바이러스를 식별하고, 공통 필터(125)를 이용하여 하나 이상의 바이러스 표지들을 감염된 파일들에 첨부한다.

<30> 구체적으로, 앞서 도 1A에서 설명된 바와 같이, 도 1B는 필터 관리자(115)가 파일 쓰기들(103 및 107)을 수신할 수 있음을 도시한다. 또한, 도 1B는 적어도 하나의 파일 쓰기(103)가 바이러스(예를 들어, 113)로 감염되었음을 도시한다. 그러면, 필터 관리자(115)는 파일 쓰기들(103 및 107)을 필터(125, 127 등)와 같은 임의의 수의 적절히 등록된 필터들에 전달한다. 예를 들어, 도 1B는 필터 관리자(115)가 파일 쓰기(103)(및 첨부된 바이러스(113))뿐 아니라 파일 쓰기(107)를 공통 AV/복제 필터(125)에 전달함을 도시한다. 앞서 언급된 바와 같이, 다음, 공통 필터(125)는 적어도 앤티바이러스 컴포넌트(123) 및 복제 컴포넌트(127)를 포함하는 임의의 수의 적절한 컴포넌트들을 포함할 수 있다. 일반적으로, 필터(125)는 필터 관리자(115)로부터 수신된 모든 쓰기들이 복제 컴포넌트(127)에 전달되기 전에 처음에 앤티바이러스 컴포넌트(123)에 전달되도록 구성될 수 있다. 그러나, 이러한 방식의 컴포넌트들의 순서화는, 파일 쓰기들이 로그 파일(예를 들어, 130)에 전달되기 전에 하나 이상의 바이러스 표지들로 태깅될 수 있는 한, 반드시 요구되지는 않는다.

<31> 어쨌든, 도 1B는 공통 필터(125)가 파일 쓰기들(103 및 107)을 수신할 수 있고, 임의의 수의 스캔 및 태깅 동작들을 수행할 수 있음을 도시한다. 예를 들어, 필터(125)의 앤티바이러스 컴포넌트(123)는 파일 쓰기(103)를 스캔할 수 있고, 그 안에 포함된 데이터를 임의의 수의 앤티바이러스 정의(150)와 비교할 수 있다. 이 경우, 필터(125)는 파일 쓰기(103) 상의 바이러스(113)의 존재를 식별한다. 이와 대조하여, 앤티바이러스 컴포넌트(123)는 파일 쓰기(107)도 수신하지만, 그 안의 임의의 바이러스(들)를 인식하지 않는다. 따라서, 도 1B는 앤티바이러스 컴포넌트(123)가 파일 쓰기(107)를 그대로 단순히 복제 컴포넌트(127)에 전달하지만, 파일 쓰기(103)와 관련하여서는 다수의 추가적인 동작들을 수행할 수 있음을 도시하고 있다.

<32> 예를 들어, 바이러스(113)를 검출하면, 앤티바이러스 컴포넌트(123)는 그 바이러스를 제거할 수 있다. 그러나, 다른 경우들에서, 앤티바이러스 컴포넌트(123)는 단순히 바이러스를 검출하고 제거하지 않을 수 있고, 또는 바이러스로 보이는 것을 검출하고 바이러스가 존재할 수도 있다는 표시(indication)를 제공할 수 있다. 따라서, 도 1B는 앤티바이러스 컴포넌트(123)가 앤티바이러스 컴포넌트(123)의 동작들 및/또는 결정들과 관련된 표시들

을 포함하는 하나 이상의 바이러스 표지(117)들로 파일 쓰기(103)를 마킹함을 도시한다. 예를 들어, 하나 이상의 바이러스 표지(117)들은 파일 쓰기(103) 내에 바이러스(113)가 여전히 포함되어 있다는 정보를 포함할 수 있고, 또는 확인되지는 않았지만 바이러스(113)가 존재하는 것으로 보인다는 정보를 포함할 수 있다. 마찬가지로, 하나 이상의 바이러스 표지(117)들은 앤티바이러스 컴포넌트(123)가 파일 쓰기(103)로부터 바이러스를 검출 및 제거 모두 하였지만, 그럼에도 불구하고 바이러스(113)가 한때는 존재했었다는 것을 나타낼 수 있다. 따라서, 하나 이상의 바이러스 표지(117)들은 이어지는 컴포넌트 및 모듈들로 하여금 파일 쓰기(103)뿐 아니라 그의 바탕이 되는 파일(underlying file)(예를 들어, 133)에 대한 추가적인 결정들을 할 수 있도록 하는 임의의 수의 표지들을 포함할 수 있음을 이해해야 한다.

<33> 어떻게 마킹 또는 태깅되었든 간에, 그러면 앤티바이러스 컴포넌트(123)는 하나 이상의 바이러스 표지(117)들과 함께 파일 쓰기(103)를 복제 컴포넌트(127)에 전송할 수 있다. 예를 들어, 도 1B는 복제 컴포넌트가 파일 쓰기(103) 및 파일 쓰기(107) 모두를 수신함을 도시한다. 궁극적으로, 복제 컴포넌트(127)는 파일 쓰기들과 관련된 파일들이 복제되도록 스케줄링되었는지를 결정하기 위해, 이 파일 쓰기(103, 107) 각각을 복제 정책들(155)과 비교한다. 예를 들어, 도 1B는 파일 쓰기(107)가 복제되도록 스케줄링되지 않았음을 도시하고, 따라서, 복제 컴포넌트(127)는 단순히 파일 쓰기(107)를 볼륨에 전달하고, 이 파일 쓰기를 대응하는 파일(137)에 추가한다. 이와 대조하여, 도 1B는 복제 컴포넌트(127)가, 파일 쓰기(103)가 복제 정책들(155)에 기초하여 복제되도록 스케줄링된 파일(133)에 관련되었음을 결정함을 도시한다.

<34> 물론, 복제 에이전트(127)는 임의의 바이러스 표지(예를 들어, 117)들의 존재에 기초하여 자신의 통상적인(customary) 메커니즘을 변경할 수 있다. 예를 들어, 복제 정책들(155)은, 하나 이상의 바이러스 표지(예를 들어, 117)들이 존재할 경우, 그렇지 않으면 복제되도록 스케줄링된 파일들이 복제로부터 제외될 것을 나타낼 수 있다. 즉, 파일 쓰기(103)를 검역(quarantine)하고, 로그 파일(130)에 카피를 두지 않고도 볼륨(120)에 파일 쓰기(103)를 전달할 수 있고, 또한 (또는 대안적으로) 대응하는 파일 쓰기 데이터 없이 하나 이상의 바이러스 표지들을 로그 파일(130)에 전송할 수 있다. 따라서, 복제 컴포넌트(127)가 구성될 수 있는 다수의 동작들이 있다.

<35> 어쨌든, 도 1B는 파일 쓰기(103)가 복제되어야 함을 복제 컴포넌트(127)가 식별하고 따라서 파일 쓰기의 카피(103a)를 생성함을 도시한다. 도시된 바와 같이, 파일 쓰기 카피(103a)는 또한 하나 이상의 바이러스 표지들의 카피(즉, 117a)를 포함한다. 따라서, 도 1B는 복제 컴포넌트(127)가 파일 쓰기(103)를 볼륨(120)에 전달하고, 여기서 파일 쓰기(103)가 그의 바탕이 되는 기본 파일(133)에 포함됨을 도시한다. 이와 대조하여, 복제 컴포넌트(127)는 파일 쓰기 카피(103a) 및 대응하는 바이러스 표지 카피(들)(117a)를 로그 파일(130)에 전달한다. 그 결과, 파일 쓰기(103)뿐 아니라 첨부된 하나 이상의 바이러스 표지(117)들은 백업 프로세스에 포함될 수 있다(즉, 카피(103a, 117a)를 통해).

<36> 앞서 언급된 바와 같이, 이로써, 백업 서버(110)로 하여금 추가적인 바이러스 스캔들을 수행하도록 반드시 요구하지 않고도, 수신된 또는 저장된 데이터에 대한 임의의 알려진 바이러스 정보를 백업 서버(110)가 수신하고 식별할 수 있음(또한 대응하는 동작들을 수신된 또는 저장된 데이터에 수행할 수 있음)을 의미한다. 도 1C에 도시된 바와 같이, 예를 들어, 백업 서버(110)는 가장 최근의 파일 쓰기 카피(103a) 및 대응하는 하나 이상의 바이러스 표지(117a)를 포함하는 로그 파일(130)의 데이터를 수신한다. 구체적으로, 백업 서버(110)는 하나 이상의 관리 에이전트(예를 들어, 135)를 통해 로그 파일(130)의 데이터를 수신하고 식별한다. 일반적으로, 관리 에이전트는 복제 프로세스들을 개시하는 것, 수신된 데이터에 동작들을 수행하는 것 등과 같은 임의의 수의 프로세스를 위해 구현된 임의의 수의 컴퓨터 실행가능 명령어들을 포함한다. 구체적으로, 각 관리 에이전트(135)는 앤티바이러스 에이전트(160)와 같은 하나 이상의 추가적인 에이전트를 더 포함(또는 그와 관련될 수 있음)할 수 있다.

<37> 따라서, 로그 파일(130)을 수신하면, 관리 에이전트(135)는 하나 이상의 바이러스 표지(117a)들을 식별할 수 있다. 다음, 관리 에이전트(135)는 하나 이상의 동작들이 수행되어야 함을 결정할 수 있고, 따라서 하나 이상의 정책 설정들(140)을 더 고려한다(consult). 예를 들어, 하나 이상의 정책 설정들(140)은 감염된 파일 쓰기를 폐기(discard)하고, 감염된 파일 쓰기를 검역하고, 및/또는 데이터의 이전 카피들에 유사한 동작들을 수행하기 위한 하나 이상의 명령어들을 포함할 수 있다. 도 1C에 도시된 바와 같이, 예를 들어, 관리 에이전트(135)는 정책 설정들(140)로부터 응답 동작(147)을 수행하기 위한 명령어들의 집합을 식별한다. 이 예에서, 응답 동작(147)은 바탕이 되는 기본 파일(133) 복제의 모든 카피들 및 그것의 반복되는 업데이트들을 "스크럽"하기 위한 명령어들을 포함한다. 구체적으로, 정책 설정들(140)은 특정 파일 쓰기(예를 들어, 103a)에 대해 바이러스 표지(예를 들어, 117)가 수신되는 모든 때에, 바탕이 되는 기본 파일(예를 들어, 복제(165))이 바이러스를 포함하

는 것으로 추정된다는 것을 관리 에이전트(135)에게 알릴 수 있다.

<38> 예를 들어, 백업 서버(110)는 파일(133)의 (다른 백업 이벤트들에 기초한) 다수의 이전 카피들을 (예를 들어, 저장 볼륨(145)을 통해) 이미 저장했다. 구체적으로, 도 1C는 백업 서버(110)가 시간 "t_0"에서 파일(133)의 최초 복제(165)를, 시간 "t_1"에 대해 파일의 업데이트(170)를, 시간 "t_2"에 대해 파일의 업데이트(175)를, 시간 "t_3"에 대해 업데이트(180)를, 그리고 시간 "t_4"에 대해 업데이트(185)를 저장하였음을 도시한다. 따라서, 이 경우에 파일 쓰기(103a)는 시간 "t_5"에서의 복제(165)(즉, 파일(133)에 대해)에 대한 업데이트이다.

<39> 따라서, 이 특정 예에서, 그리고 응답 동작(147)의 명령어들에 응답하여, 관리 에이전트(135)는 (이미 스크럽되거나 "정화(cleansed)"되지 않았다면) 앤티바이러스 에이전트(160)를 통해 파일 쓰기(103a)를 스크럽한다. 관리 에이전트(135)는 또한 서로 다른 복제들(165, 170, 175, 180, 185) 각각을 스크럽하기 위해 앤티바이러스 에이전트(160)를 사용할 수 있다. 각 카피를 이렇게 정화한 후, 따라서, 관리 에이전트(135)는 파일 복제들(165, 170, 175, 180 및 185)을 새로운 데이터(195)로 대체하기 위한 대응하는 명령어들(190)을 전송한다. 다음, 데이터(195)는 식별된 바이러스 없이 기본 파일 및 이어지는 업데이트들(즉, "t_0-t_5")을 포함할 수 있다.

<40> 따라서, 도 1A-1C는 프로덕션 서버 수준(production server level)에서 바이러스들을 식별하고, 그 정보를 백업 서버 수준(backup server level)으로 전달하고, 각각의 이러한 수준에서 임의의 수의 대응하는 동작들을 수행하기 위한 다수의 개략도 및 컴포넌트들을 제공한다. 앞서 말한 것에 더해, 또한 본 발명의 구현들은 특정 결과를 달성하기 위한 동작들의 하나 이상의 시퀀스를 포함하는 방법의 흐름도와 관련하여 설명될 수 있다. 예를 들어, 도 2는 프로덕션 서버(105)와 백업 서버(110) 모두의 관점에서, 공통/결합된 AV/복제 필터(125)를 이용한 파일 쓰기의 필터링의 흐름도를 도시한다. 도 2의 동작들은 도 1A 내지 도 1C의 개략도 및 컴포넌트들과 관련하여 아래에서 설명된다.

<41> 예를 들어, 도 2는 프로덕션 서버(105)의 관점에서, 공통 필터를 통해 바이러스 및 백업 필터링 프로세스들을 관리하는 방법은 하나 이상의 파일 쓰기들을 식별하는 동작(200)을 포함할 수 있음을 도시한다. 동작(200)은 공통 필터를 통해 하나 이상의 쓰기를 식별하는 것을 포함한다. 예를 들어, 도 1A 및 도 1B에 도시된 바와 같이, 프로덕션 서버(105)는 필터 관리자(115)를 통해 파일 쓰기들(103 및 107)(즉, 임의의 수의 I/O 시스템 호출)을 수신한다. 다음, 필터 관리자(115)는 이 쓰기들을 공통 AV/복제 필터(125)에 전달한다.

<42> 이에 더해, 도 2는 프로덕션 서버(105)의 관점에서, 방법은 바이러스들에 대해 파일 쓰기들을 스캔하는 동작(210)을 포함할 수 있음을 도시한다. 동작(210)은 하나 이상의 바이러스 정의들에 따라, 식별된 하나 이상의 파일 쓰기들을 공통 필터에서 스캔하는 것을 포함할 수 있다. 도 1B에 도시된 바와 같이, 예를 들어, 공통 AV/복제 필터(125)는 파일 쓰기들(103 및 107)을 수신하고, 앤티바이러스 컴포넌트(123)를 통해 대응하는 데이터를 하나 이상의 앤티바이러스 정의(150)들과 비교한다. 그러면, 공통 AV/복제 필터(125)는 앤티바이러스 컴포넌트(123)를 통해 파일 쓰기(103)가 바이러스(113)를 포함함을 결정한다.

<43> 또한, 도 2는 프로덕션 서버(105)의 관점에서, 방법은 스캔된 파일들을 복제 정책과 비교하는 동작(220)을 포함할 수 있음을 도시한다. 동작(220)은 식별된 하나 이상의 스캔된 파일 쓰기를 공통 필터에서 하나 이상의 복제 정책과 비교하는 것을 포함한다. 예를 들어, 도 1B는 AV/복제 필터(125)가 또한 파일 쓰기들(103 및 107)을 앤티바이러스 컴포넌트(123)에 의해 처리(treated)/스캔된 후에 복제 컴포넌트(127) 내에 수신함을 도시한다. 그러면, 복제 컴포넌트(127)는 파일 쓰기들(103 및 107)을 복제 정책들(155)과 비교하여, 이 파일 쓰기들이 백업 프로세스들을 통해 보호되어야 하는 것인지를 결정한다.

<44> 또한, 도 2는 프로덕션 서버(105)의 관점에서, 방법은 파일 쓰기들을 로그 파일에 전송하는 동작(230)을 포함할 수 있음을 도시한다. 동작(230)은 적어도 하나의 파일 쓰기가 백업 서버에 복제되도록, 하나 이상의 스캔된 파일 쓰기들 중 적어도 하나의 카피를 로그 파일에 전송하는 것을 포함한다. 예를 들어 도 1B에 도시된 바와 같이, 공통 AV/복제 필터(125)가 파일 쓰기들(103 및 107)을 수신하지만, 복제 필터는 파일 쓰기(103)만이 복제되도록 스케줄링되었음을 식별한다. 따라서, 복제 컴포넌트(127)는 파일 쓰기(103)만을 (즉, 카피(103a)로서) 로그 파일(130)에 카피하지만, 파일 쓰기(103 및 107) 모두를 저장 볼륨(120)에 전송한다.

<45> 따라서, 도 2는 백업 서버(110)의 관점에서, 하나 이상의 프로덕션 서버에서 공통 필터에 의해 제공된 하나 이상의 바이러스 표지들에 따라 복제된 데이터를 관리하는 방법은 데이터 백업들을 수신하는 동작(240)을 포함할 수 있음을 도시한다. 동작(240)은 하나 이상의 프로덕션 서버로부터 하나 이상의 데이터 백업들을 수신하는 것을 포함한다. 예를 들어, 도 1C에 도시된 바와 같이, 백업 서버(110)의 관리 에이전트(130)는 프로덕션 서버

(105)로부터 적어도 로그 파일(130)의 백업 데이터를 수신한다.

<46> 또한, 도 2는 백업 서버(110)의 관점에서, 방법은 수신된 데이터 내에서 하나 이상의 바이러스 표지들을 식별하는 동작(250)을 포함할 수 있음을 도시한다. 동작(250)은 수신된 하나 이상의 데이터 백업에서 하나 이상의 바이러스 표지들을 식별하는 것을 포함하며, 여기서 하나 이상의 바이러스 표지들은 하나 이상의 데이터 백업 중 적어도 하나가 감염된 데이터와 관련됨을 식별한다. 예를 들어, 도 1C는 관리 에이전트(135)가 파일 쓰기(103a) 및 하나 이상의 바이러스 표지(117a)를 포함하는 로그 파일(130)의 데이터를 수신함을 도시한다. 따라서, 관리 에이전트(135)는 하나 이상의 바이러스 표지(117a)로부터 바이러스가 존재한다는 것, 또는 바이러스가 제거되었지만 그럼에도 파일의 이전 버전에 존재했음을 식별한다.

<47> 또한, 도 2는 백업 서버(110)의 관점에서, 방법은 응답 동작들에 대한 하나 이상의 정책들을 식별하는 동작(260)을 포함할 수 있음을 도시한다. 동작(260)은 백업 서버에 대해 하나 이상의 정책들을 식별하는 것을 포함하며, 여기서 하나 이상의 정책들은 하나 이상의 바이러스 표지들에 대응되는 하나 이상의 응답 동작들을 식별한다. 예를 들어, 도 1C는 관리 에이전트(135)가 정책 설정들(140)을 고려하고(consult), 백업 서버(110)로 하여금 파일(133)(즉, 쓰기(103a)에 대한 바탕이 되는 파일)의 이전 또는 현재 카피들 모두를 스크럽할 것을 요구하는, 응답 동작(147)을 구현하기 위한 명령어들을 수신함을 도시한다.

<48> 또한, 도 2는 백업 서버(110)의 관점에서, 방법은 바이러스 표지들에 대해 응답 동작을 실행하는 동작(270)을 포함할 수 있음을 도시한다. 동작(270)은 하나 이상의 정책들에 따라 하나 이상의 응답 동작들 중 임의의 것을 실행하는 것을 포함한다. 예를 들어, 도 1C는 관리 에이전트(135)가 (예를 들어, 앤티바이러스 에이전트(160)를 통해) 파일(133)에 대한 각 기준 카피(baseline copy) 및 (즉, 시간 "t_0"-"t_5"에 대해) 업데이트를 가지고 임의의 바이러스 감염들을 제거함을 도시한다. 다음, 관리 에이전트(135)는 이 데이터의 깨끗한 카피(clean copy)(195)를 준비하고, 저장 볼륨(145) 내에 있는 이 데이터의 원래 카피들(165, 170, 175, 180, 185)을 새로운 깨끗한 데이터(195)로 대체하기 위해 대응하는 명령어들(190)을 전송한다.

<49> 따라서, 도 1A-2는 식별된 바이러스 정보가 백업 시스템(100) 전체에 걸쳐 효과적으로 전달될 수 있음을 보장하는 다수의 컴포넌트 및 메커니즘들을 제공한다. 이들 및 기타 특징들에 의해, 바이러스에 대한 의도치 않은 복제와 관련한 위협은 더 효과적으로 완화될 수 있다. 구체적으로, 바이러스 정보의 넓은 분포는 여기에 논의된 원리들에 따른 다수의 추가적인 특징들을 가능하게 한다. 예를 들어, 프로덕션 서버(105)는 감염된 또는 감염되었던 데이터에 대한 하나 이상의 요청을 수신할 수 있다. 예를 들어 공통 필터(125)를 통해, 프로덕션 서버(105)는 요청이 하나 이상의 바이러스 표지와 관련된 하나 이상의 파일들과 관련됨을 결정할 수 있고, 임의의 수의 프로덕션 서버 정책에 기초하여 요청을 거부하거나 허용할 수 있다.

<50> 특정 백업 데이터에 대한 요청들 또한 유사한 방식으로 취급될 수 있다. 예를 들어, 사용자는 백업 서버(110)에 저장된(즉, 백업된) 하나 이상의 파일을 요청할 수 있다. 공통 필터(125)(또는 다른 적절한 에이전트)는 요청이 이전의 한 시점에서 하나 이상의 바이러스 표지와 관련되었던 하나 이상의 파일들과 관련된다는 것을 인덱스(index)로부터 식별할 수 있다. 그러면 프로덕션 서버(105)는 사용자에게 경고를 제공하거나, 또는 심지어, 요청에 기초하여 이후에 백업 서버(110)로부터 수신된 임의의 대응하는 데이터를 스캔하고 제거할 수 있다.

<51> 마찬가지로, 백업 데이터를 위해 프로덕션 서버(105)로부터 백업 서버(110)로 전달된 요청들은 같은 논리(calculus)를 포함할 수 있다. 즉, 관리 에이전트(135)는 하나 이상의 요청으로부터, 요청된 데이터가 하나 이상의 바이러스 표지와 관련되거나, 반대로 하나 이상의 바이러스 표지들에 첨부된 하나 이상의 파일들과 관련된다는 것을 식별할 수 있다. 그러면, 관리 에이전트(135)는 임의의 수의 정책 설정들에 따라, 데이터를 반환하기 전에 바이러스 제거할 수 있고, 요청을 거부할 수 있고, 또는 이와 유사한 것 등을 할 수 있다.

<52> 아래 더 상세히 논의되는 바와 같이, 본 발명의 실시예들은 다양한 컴퓨터 하드웨어를 포함하는 특수 목적 또는 범용 컴퓨터를 포함할 수 있다. 본 발명의 범위 내의 실시예들은 또한 컴퓨터 실행가능 명령어 또는 그에 저장된 데이터 구조를 지니거나(carrying) 가지기(having) 위한 컴퓨터 판독가능 매체를 포함한다. 이러한 컴퓨터 판독가능 매체는 범용 또는 특수 목적 컴퓨터에 의해 액세스될 수 있는 임의의 사용가능한 매체일 수 있다.

<53> 예로서, 이러한 컴퓨터 판독가능 매체는 RAM, ROM, EEPROM, CD-ROM, 또는 기타 광학 디스크 저장소, 자기 디스크 저장소 또는 다른 자기 저장 장치, 또는 컴퓨터 실행가능 명령어 또는 데이터 구조의 형태로 원하는 프로그램 코드를 지니거나 저장하는 데 사용될 수 있고 범용 또는 특수 목적 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있지만 이에 제한되지는 않는다. 정보가 네트워크 또는 다른 통신 연결(유선, 무선, 또는 유선과 무선의 조합)을 통해 컴퓨터에 전송되거나 제공될 때, 컴퓨터는 연결을 컴퓨터 판독가능 매체로서 적

절하게 간주한다. 따라서, 임의의 이러한 연결은 컴퓨터 판독가능 매체라고 적절히 불린다. 상기의 조합들 또한 컴퓨터 판독가능 매체의 범위 내에 포함되어야 한다.

<54> 컴퓨터 실행가능 명령어는, 예를 들어, 범용 컴퓨터, 특수 목적 컴퓨터, 또는 특수 목적 프로세싱 장치로 하여금 특정 기능 또는 기능들의 그룹을 수행하도록 하는 명령어 및 데이터를 포함한다. 본 발명이 구조적 특징 및/또는 방법론적 동작들에 있어 구체적인 언어로 설명되었지만, 첨부된 청구항들에 정의된 본 발명은 반드시 위에서 설명된 구체적 특징 또는 동작들에 제한되지 않는다는 것을 이해해야 한다. 오히려, 위에서 설명된 구체적 특징 및 동작들은 청구항을 구현하기 위한 예시적인 형태로서 개시된다.

<55> 본 발명은 그의 정신 또는 본질적 특징들을 벗어나지 않고 다른 구체적 형태에 구현될 수 있다. 설명된 실시예들은 모든 관점에서 단지 설명적인 것으로서 고려되어야 하며 제한적인 것으로 고려되어서는 안된다. 따라서, 본 발명의 범위는 앞선 설명보다는 첨부된 청구항들에 의해 나타난다. 청구들과 동등한 의미 및 범위 내에 포함되는 모든 변경들은 청구항의 범위 내에 포함되는 것이다.

도면의 간단한 설명

<15> 위에서 열거된 것 및 본 발명의 다른 이점 및 특징들을 얻을 수 있는 방식을 설명하기 위해, 위에서 간략히 설명된 본 발명에 대한 더 구체적인 설명이 첨부된 도면에 도시된 구체적 실시예들과 관련하여 제시될 것이다. 이 도면들은 본 발명의 전형적인 실시예들로서만 도시된 것이며, 따라서 본 발명의 범위를 제한하는 것으로 고려되어서는 안된다는 것을 이해하면서, 본 발명은 첨부된 도면의 사용을 통해 추가적인 특수성(specificity) 및 세부 사항들로 묘사되고 설명될 것이다.

<16> 도 1A는 본 발명의 구현에 따라 개략적인 개략도를 도시하며, 여기서 프로덕션 서버는 공통 앤티바이러스/복제 필터를 통해 파일 쓰기들을 스캔하고, 그 파일 쓰기들을 백업 서버에 제공한다.

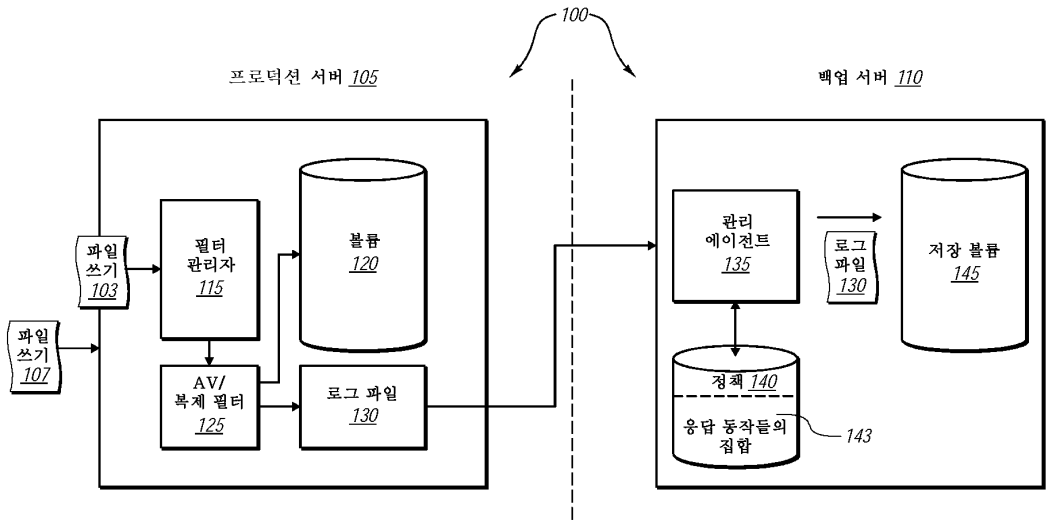
<17> 도 1B는 본 발명의 구현에 따라 프로덕션 서버에서의 프로세스에 대한 더 상세한 개략도를 도시하며, 여기서 공통 앤티바이러스/복제 필터는, 파일 쓰기들을 로그 파일에 전송하기 전에, 하나 이상의 수신된 파일 쓰기들을 하나 이상의 바이러스 표지로 마킹(mark)한다.

<18> 도 1C는 본 발명의 구현에 따라, 백업 서버가 하나 이상의 바이러스 표지를 포함하는 하나 이상의 데이터 백업을 수신하고, 하나 이상의 대응하는 응답 동작들을 수행하는 개략도를 도시한다.

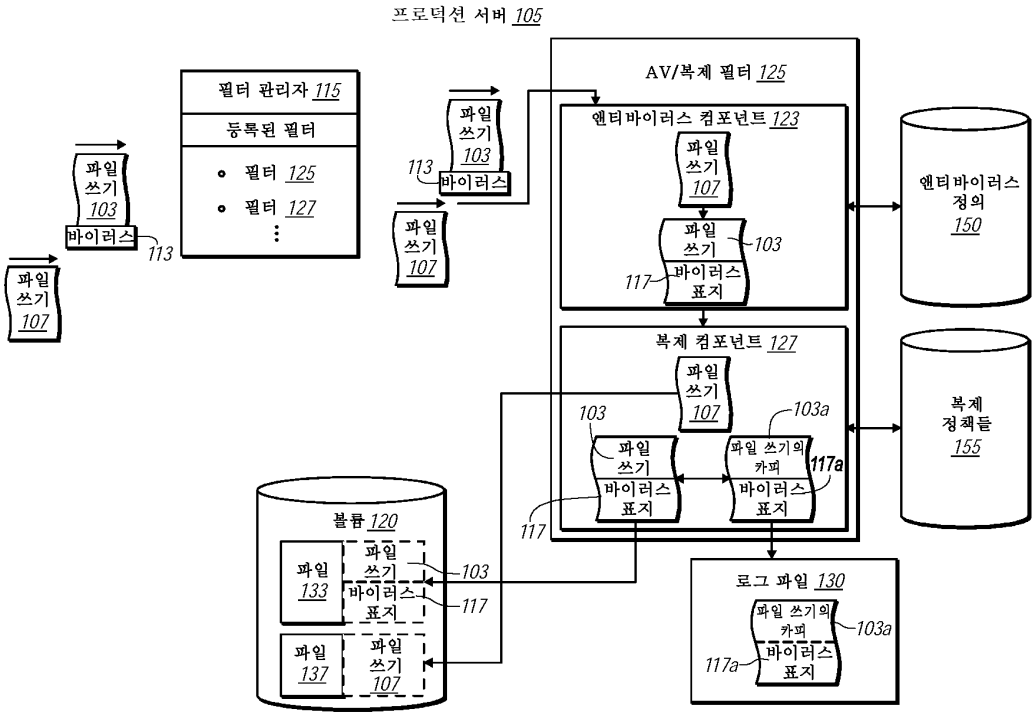
<19> 도 2는 본 발명의 구현에 따라, 프로덕션 서버 및 백업 서버의 관점에서, 백업 시스템 전체에 걸쳐 파일 쓰기들에 대한 앤티바이러스 주석(annotation)을 전달(propagate)하기 위한 방법의 흐름도를 도시한다.

도면

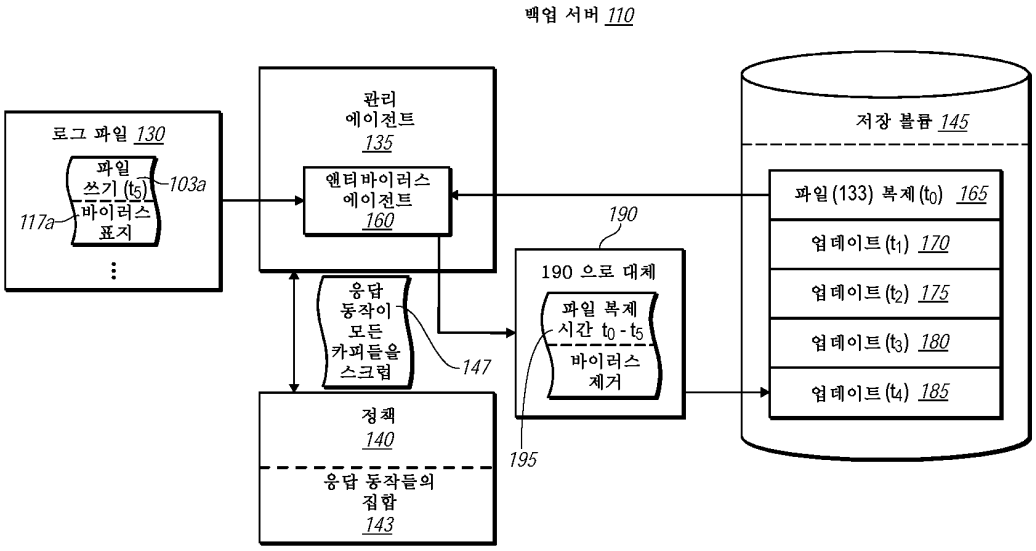
도면1A



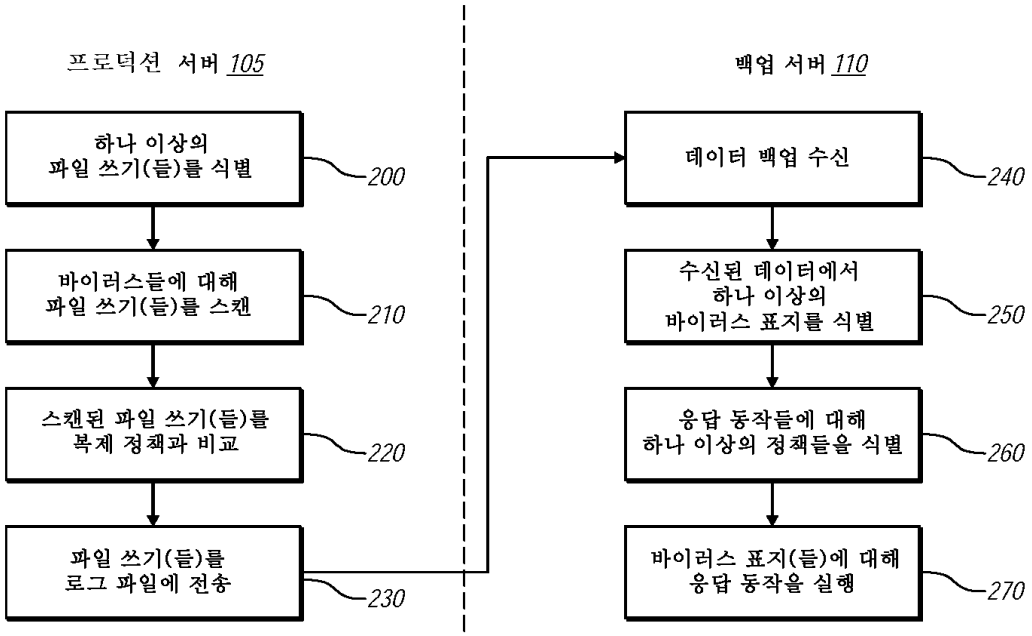
도면1B


프로덕션 서버 105
필터 관리자 115
등록된 필터
필터 125
필터 127
파일 쓰기 103
바이러스
113
파일 쓰기 107
AV/복제 필터 125
앤티바이러스 컴포넌트 123
파일 쓰기 107
파일 쓰기 103
바이러스 표지
117
앤티바이러스 정의 150
복제 컴포넌트 127
파일 쓰기 107
103
103a
파일 쓰기
바이러스 표지
파일 쓰기의 카피
117a
복제 정책들 155
볼륨 120
파일 133
파일 쓰기
바이러스 표지
파일 137
로그 파일 130
파일 쓰기의 카피
바이러스 표지

도면1C


백업 서버 110
로그 파일 130
파일 쓰기 (t5)
103a
바이러스 표지
117a
관리 에이전트 135
앤티바이러스 에이전트 160
응답 동작이 모든 카피들을 스크럽
147
정책 140
응답 동작들의 집합 143
190
190 으로 대체
파일 복제 시간 t0 - t5
바이러스 제거
195
저장 볼륨 145
파일 (133) 복제 (t0) 165
업데이트 (t1) 170
업데이트 (t2) 175
업데이트 (t3) 180
업데이트 (t4) 185

도면2


프로덕션 서버 105
하나 이상의 파일 쓰기(들)를 식별
200
바이러스들에 대해 파일 쓰기(들)를 스캔
210
스캔된 파일 쓰기(들)를 복제 정책과 비교
220
파일 쓰기(들)를 로그 파일에 전송
230
백업 서버 110
데이터 백업 수신
240
수신된 데이터에서 하나 이상의 바이러스 표지를 식별
250
응답 동작들에 대해 하나 이상의 정책들을 식별
260
바이러스 표지(들)에 대해 응답 동작을 실행
270