(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0132596
(43) 공개일자 2015년11월25일

(51) 국제특허분류(Int. Cl.)
H04L 12/24 (2006.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
H04L 41/0893 (2013.01)
H04L 41/082 (2013.01)
(21) 출원번호 10-2015-7032055
(22) 출원일자(국제) 2014년04월09일
심사청구일자 2015년11월10일
(85) 번역문제출일자 2015년11월09일
(86) 국제출원번호 PCT/US2014/033524
(87) 국제공개번호 WO 2014/169054
국제공개일자 2014년10월16일
(30) 우선권주장
61/810,480 2013년04월10일 미국(US)
61/899,468 2013년11월04일 미국(US)

(71) 출원인
일루미오, 아이엔씨.
미국 94086 캘리포니아주 써니베일 샌 가브리엘 드라이브 160
(72) 발명자
키르너, 폴, 제이.
미국 94086 캘리포니아주 써니베일 샌 가브리엘 드라이브 160 일루미오, 아이엔씨.
쿡, 다니엘, 알.
미국 94086 캘리포니아주 써니베일 샌 가브리엘 드라이브 160 일루미오, 아이엔씨.
(뒷면에 계속)
(74) 대리인
김정훈

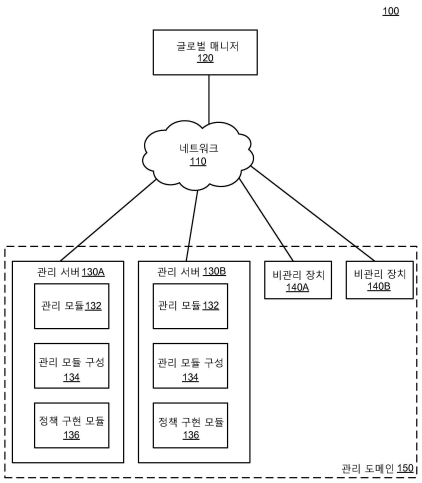
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **로지컬 다차원 레이블기반 정책 모델을 이용한 분산 네트워크 관리**

(57) 요 약

관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들은 하나 이상의 규칙들의 세트를 포함하는 관리 도메인-전역 관리 정책에 따라 생성된다. 상기 관리 도메인은 복수의 관리 서버들을 포함한다. 상기 규칙들의 세트 내에서 상기 특정 관리 서버에 관련된 규칙들에 관한 결정이 이루어진다. 기능-레벨 명령들은 관련된 것으로 결정된 규칙들에 기반하여 생성된다. 상기 복수의 관리 서버들 내에서 어떤 관리 서버들이 상기 특정 서버와 관련되는지에 관해 결정이 이루어진다. 상기 기능-레벨 명령들 및 상기 관련된 것으로 결정된 관리 서버들에 관한 정보는 상기 특정 관리 서버로 전송된다. 상기 특정 관리 서버는 상기 기능-레벨 명령들 및 관리 모듈을 구성하기 위해 상기 관리 서버들에 관한 정보를 이용하고, 상기 구성된 관리 모듈은 상기 관리 도메인-전역 관리 정책을 구현한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 41/0869 (2013.01)
H04L 41/145 (2013.01)
H04L 63/10 (2013.01)

(72) 발명자
팬들리, 유라이, 쥐.
미국 94086 캘리포니아주 써니베일 샌 가브리엘 드라이브 160 일루미오, 아이엔씨.
글렌, 매튜, 케이.
미국 94086 캘리포니아주 써니베일 샌 가브리엘 드라이브 160 일루미오, 아이엔씨.
굽타, 무케시
미국 94086 캘리포니아주 써니베일 샌 가브리엘 드라이브 160 일루미오, 아이엔씨.
루빈, 앤드류, 에스.
미국 94086 캘리포니아주 써니베일 샌 가브리엘 드라이브 160 일루미오, 아이엔씨.
스코트, 제리, 비.
미국 94086 캘리포니아주 써니베일 샌 가브리엘 드라이브 160 일루미오, 아이엔씨.
장, 세효
미국 94086 캘리포니아주 써니베일 샌 가브리엘 드라이브 160 일루미오, 아이엔씨.
스토콜, 앨런, 비.
미국 94086 캘리포니아주 써니베일 샌 가브리엘 드라이브 160 일루미오, 아이엔씨.

명 세 서

청구범위

청구항 1

하나 이상의 규칙들의 세트(set of one or more rules)를 포함하는 관리 도메인-전역 관리 정책(administrative domain-wide management policy)에 따른 관리 도메인(administrative domain) 내에서 특정 관리 서버(particular managed server)를 위한 관리 명령들(management instructions)을 생성하는 방법에 있어서, 상기 관리 도메인은 복수의 관리 서버들을 포함하고, 상기 방법은:

상기 규칙들의 세트 내에서 어떤 규칙들이 상기 특정 관리 서버와 관련되는지를 결정하는 단계;

상기 관련된 것으로 결정된 규칙들에 기반하여 기능-레벨(function-level) 명령들을 생성하는 단계;

상기 복수의 관리 서버들 내에서 어떤 관리 서버들이 상기 특정 관리 서버와 관련되는지를 결정하는 단계; 및

상기 기능-레벨 명령들 및 상기 관련된 것으로 결정된 관리 서버들에 관한 정보를 상기 특정 관리 서버로 전송하는 단계

를 포함하고,

상기 특정 관리 서버는 상기 기능-레벨 명령들 및 관리 모듈을 구성하기 위해 상기 관리 서버들에 관한 정보를 이용하고, 상기 구성된 관리 모듈은 상기 관리 도메인-전역 관리 정책을 구현하는

관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들을 생성하는 방법.

청구항 2

제1항에 있어서,

상기 특정 관리 서버는 가상 서버(virtual server)인

관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들을 생성하는 방법.

청구항 3

제1항에 있어서,

상기 관리 도메인-전역 관리 정책은 관리 서버가 액세스하는 것이 허용되는지 여부 또는 그 방법, 또는 장치에 의해 액세스되는지 여부 또는 그 방법을 명시하는

관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들을 생성하는 방법.

청구항 4

제1항에 있어서,

상기 규칙들은 관리 서버의 차원(dimension) 및 상기 차원에 대한 값을 명시함으로써 관리 서버들을 명시하고, 상기 차원은 역할(Role), 환경(Environment), 어플리케이션(Application), 비즈니스의 라인(Line of Business), 및 위치(Location)를 포함하는 그룹 중 하나의 요소인

관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들을 생성하는 방법.

청구항 5

제1항에 있어서,

상기 규칙들은 어떤 관리 서버들이 서비스를 제공하기 위해 허용된 것인지를 명시하고, 규칙이 서비스를 제공하기 위해 허용된 상기 특정 관리 서버를 명시하면, 상기 규칙은 상기 특정 관리 서버와 관련되는

관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들을 생성하는 방법.

청구항 6

제1항에 있어서,

상기 규칙들은 관리 서버들이 서비스들을 소비하기 위해 허용되는지 여부 또는 그 방법을 명시하고, 규칙이 상기 특정 관리 서버가 서비스를 소비하기 위해 허용되는지 여부 또는 그 방법을 명시하면, 상기 규칙은 상기 특정 관리 서버와 관련되는

관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들을 생성하는 방법.

청구항 7

제1항에 있어서,

상기 복수의 관리 서버들 내에서 어떤 관리 서버들이 상기 특정 관리 서버와 관련되는지를 결정하는 단계는,

상기 복수의 관리 서버들 내에서 어떤 관리 서버들이 상기 관련되는 것으로 결정된 규칙들과 관련되는지를 결정하는 단계

를 포함하는 관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들을 생성하는 방법.

청구항 8

제1항에 있어서,

상기 관리 서버들에 관한 정보는 상기 관리 서버들의 네트워크 노출 정보(network exposure information)를 포함하는

관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들을 생성하는 방법.

청구항 9

제1항에 있어서,

상기 관리 모듈은 로우-레벨(low-level) 네트워크 또는 보안 엔진(security engine)을 포함하는

관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들을 생성하는 방법.

청구항 10

제1항에 있어서,

상기 복수의 관리 서버들 내에서 어떤 관리 서버들이 상기 특정 관리 서버와 관련되는지를 결정하기 전에 상기 복수의 관리 서버들 내에서 상기 관리 서버들을 열거하는 단계

를 더 포함하는 관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들을 생성하는 방법.

청구항 11

하나 이상의 규칙들의 세트를 포함하는 관리 도메인-전역 관리 정책에 따른 관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들을 생성하기 위한 컴퓨터 프로그램 모듈들을 저장하는 비일시적 컴퓨터 판독 가능한 기억 매체(non-transitory computer-readable storage medium)에 있어서, 상기 관리 도메인은 복수의 관리 서버들을 포함하고, 상기 컴퓨터 프로그램 모듈들은 방법을 수행하기 위해 실행가능하고, 상기 방법은:

상기 규칙들의 세트 내에서 어떤 규칙들이 상기 특정 관리 서버와 관련되는지를 결정하는 단계;

상기 관련된 것으로 결정된 규칙들에 기반하여 기능-레벨 명령들을 생성하는 단계;

상기 복수의 관리 서버들 내에서 어떤 관리 서버들이 상기 특정 관리 서버와 관련되는지를 결정하는 단계; 및

상기 기능-레벨 명령들 및 상기 관련된 것으로 결정된 관리 서버들에 관한 정보를 상기 특정 관리 서버로 전송하는 단계

를 포함하고,

상기 특정 관리 서버는 상기 기능-레벨 명령들 및 관리 모듈을 구성하기 위해 상기 관리 서버들에 관한 정보를 이용하고, 상기 구성된 관리 모듈은 상기 관리 도메인-전역 관리 정책을 구현하는

컴퓨터 판독 가능한 기억 매체.

청구항 12

제11항에 있어서,

상기 특정 관리 서버는 가상 서버인

컴퓨터 판독 가능한 기억 매체.

청구항 13

제11항에 있어서,

상기 관리 도메인-전역 관리 정책은 관리 서버가 액세스하는 것이 허용되는지 여부 또는 그 방법, 또는 장치에 의해 액세스되는지 여부 또는 그 방법을 명시하는

컴퓨터 판독 가능한 기억 매체.

청구항 14

제11항에 있어서,

상기 규칙들은 관리 서버의 차원(dimension) 및 상기 차원에 대한 값을 명시함으로써 관리 서버들을 명시하고, 상기 차원은 역할(Role), 환경(Environment), 어플리케이션(Application), 비즈니스의 라인(Line of Business), 및 위치(Location)를 포함하는 그룹 중 하나의 요소인

컴퓨터 판독 가능한 기억 매체.

청구항 15

제11항에 있어서,

상기 규칙들은 어떤 관리 서버들이 서비스를 제공하기 위해 허용된 것인지를 명시하고, 규칙이 서비스를 제공하기 위해 허용된 상기 특정 관리 서버를 명시하면, 상기 규칙은 상기 특정 관리 서버와 관련되는

컴퓨터 판독 가능한 기억 매체.

청구항 16

제11항에 있어서,

상기 규칙들은 관리 서버들이 서비스들을 소비하기 위해 허용되는지 여부 또는 그 방법을 명시하고, 규칙이 상기 특정 관리 서버가 서비스를 소비하기 위해 허용되는지 여부 또는 그 방법을 명시하면, 상기 규칙은 상기 특정 관리 서버와 관련되는

컴퓨터 판독 가능한 기억 매체.

청구항 17

제11항에 있어서,

상기 복수의 관리 서버들 내에서 어떤 관리 서버들이 상기 특정 관리 서버와 관련되는지를 결정하는 단계는,

상기 복수의 관리 서버들 내에서 어떤 관리 서버들이 상기 관련되는 것으로 결정된 규칙들과 관련되는지를 결정하는 단계

를 포함하는 컴퓨터 판독 가능한 기억 매체.

청구항 18

제11항에 있어서,

상기 관리 서버들에 관한 정보는 상기 관리 서버들의 네트워크 노출 정보(network exposure information)를 포함하는

컴퓨터 판독 가능한 기억 매체.

청구항 19

제1항에 있어서,

상기 관리 모듈은 로우-레벨(low-level) 네트워크 또는 보안 엔진(security engine)을 포함하는

컴퓨터 판독 가능한 기억 매체.

청구항 20

하나 이상의 규칙들의 세트를 포함하는 관리 도메인-전역 관리 정책에 따른 관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들을 생성하기 위한 시스템에 있어서, 상기 관리 도메인은 복수의 관리 서버들을 포함하고, 상기 시스템은:

방법을 수행하기 위해 실행 가능한 컴퓨터 프로그램 모듈들을 저장하는 비일시적 컴퓨터 판독 가능한 기억 매체(non-transitory computer-readable storage medium)를 포함하고,

상기 방법은:

상기 규칙들의 세트 내에서 어떤 규칙들이 상기 특정 관리 서버와 관련되는지를 결정하는 단계;

상기 관련된 것으로 규칙들에 기반하여 기능-레벨 명령들을 생성하는 단계;

상기 복수의 관리 서버들 내에서 어떤 관리 서버들이 상기 특정 관리 서버와 관련되는지를 결정하는 단계; 및

상기 기능-레벨 명령들 및 상기 관련된 것으로 결정된 관리 서버들에 관한 정보를 상기 특정 관리 서버로 전송하는 단계를 포함하고,

상기 컴퓨터 프로그램 모듈들을 실행하기 위한 컴퓨터 프로세서(computer processor)

를 포함하고,

상기 특정 관리 서버는 상기 기능-레벨 명령들 및 관리 모듈을 구성하기 위해 상기 관리 서버들에 관한 정보를 이용하고, 상기 구성된 관리 모듈은 상기 관리 도메인-전역 관리 정책을 구현하는

관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들을 생성하기 위한 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 관리 도메인(administrative domain)의 서버들(물리(physical) 또는 가상(virtual))을 관리하는 분야에 관련된 것으로, 더욱 상세하게는 로지컬 다차원 레벨기반 정책 모델을 고수하는 관리 도메인-전역 정책(administrative domain-wide policy)에 따라 서버들을 관리하는 것에 관련된 것이다.

배 경 기 술

[0002] 관리 도메인의 서버들(물리또는 가상)은 정책에 따라 관리된다. 예를 들어, 보안 정책(security policy)은 액세스 제어(access control) 및/또는 보안 연결(secure connectivity)을 명시할 수 있고, 반면에 자원-사용 정책(resource-usage policy)은 상기 관리 도메인의 컴퓨팅 자원들(computing resources)(예를 들어, 디스크들 및/또는 주변장치들(peripherals))의 사용을 명시할 수 있다. 종래의 정책들은 물리 장치들을 참조하고, IP 주소들(Internet Protocol addresses), IP 주소 범위들(IP address ranges), 서브네트워크들(subnetworks), 및 네트워크 인터페이스들(network interfaces)과 같은 로우-레벨(low-level) 구조들(constructs)의 측면에서 예상된다. 이러한 로우-레벨 구조들은 추상적이고(abstract), 자연적인 방법으로 세밀한 정책(fine-grained policy)을 쓰는 것을 어렵게 만든다.

발명의 내용

과제의 해결 수단

[0003] 상술된 문제점들 및 다른 문제점들은 하나 이상의 규칙들의 세트를 포함하는 관리 도메인-전역 관리 정책에 따른 관리 도메인 내에서 특정 관리 서버를 위한 관리 명령들을 생성하기 위한 방법, 비일시적 컴퓨터 판독 가능한 기록 매체, 및 시스템에 의해 해결된다. 상기 관리 도메인은 복수의 관리 서버들을 포함한다. 상기 방법의 실시예는 상기 규칙들의 세트 내에서 어떤 규칙들이 상기 특정 관리 서버와 관련되는지를 결정하는 단계를 포함한다. 상기 방법은 상기 관련된 것으로 결정된 규칙들에 기반하여 기능-레벨(function-level) 명령들을 생성하는 단계를 더 포함한다. 상기 복수의 관리 서버들 내에서 어떤 관리 서버들이 상기 특정 관리 서버와 관련되는지를 결정하는 단계를 더 포함한다. 상기 방법은 상기 기능-레벨 명령들 및 상기 관련된 것으로 결정된 관리 서버들에 관한 정보를 상기 특정 관리 서버로 전송하는 단계를 더 포함한다. 상기 특정 관리 서버는 상기 기능-레벨 명령들 및 관리 모듈을 구성하기 위해 상기 관리 서버들에 관한 정보를 이용하고, 상기 구성된 관리 모듈은 상기 관리 도메인-전역 관리 정책을 구현한다.

[0004] 상기 매체의 실시예는 방법을 수행하기 위해 실행 가능한 컴퓨터 프로그램 모듈들을 저장한다. 상기 방법은 상기 규칙들의 세트 내에서 어떤 규칙들이 상기 특정 관리 서버와 관련되는지를 결정하는 단계를 포함한다. 상기 방법은 상기 관련된 것으로 결정된 규칙들에 기반하여 기능-레벨 명령들을 생성하는 단계를 더 포함한다. 상기 방법은 상기 복수의 관리 서버들 내에서 어떤 관리 서버들이 상기 특정 관리 서버와 관련되는지를 결정하는 단계를 더 포함한다. 상기 단계는 상기 기능-레벨 명령들 및 상기 관련된 것으로 결정된 관리 서버들에 관한 정보를 상기 특정 관리 서버로 전송하는 단계를 더 포함한다. 상기 특정 관리 서버는 상기 기능-레벨 명령들 및 관리 모듈을 구성하기 위해 상기 관리 서버들에 관한 정보를 이용하고, 상기 구성된 관리 모듈은 상기 관리 도메인-전역 관리 정책을 구현한다.

[0005] 상기 시스템의 실시예는 방법을 수행하기 위해 실행 가능한 컴퓨터 프로그램 모듈들을 저장하는 비일시적 컴퓨터 판독 가능한 기억 매체를 포함한다. 상기 방법은 상기 규칙들의 세트 내에서 어떤 규칙들이 상기 특정 관리 서버와 관련되는지를 결정하는 단계를 포함한다. 상기 방법은 상기 관련된 것으로 규칙들에 기반하여 기능-레벨 명령들을 생성하는 단계를 더 포함한다. 상기 방법은 상기 복수의 관리 서버들 내에서 어떤 관리 서버들이 상기 특정 관리 서버와 관련되는지를 결정하는 단계를 더 포함한다. 상기 방법은 상기 기능-레벨 명령들 및 상기 관련된 것으로 결정된 관리 서버들에 관한 정보를 상기 특정 관리 서버로 전송하는 단계를 더 포함한다. 상기 특정 관리 서버는 상기 기능-레벨 명령들 및 관리 모듈을 구성하기 위해 상기 관리 서버들에 관한 정보를 이용하고, 상기 구성된 관리 모듈은 상기 관리 도메인-전역 관리 정책을 구현한다.

도면의 간단한 설명

[0006] 도 1은 일 실시예에 따른 관리 도메인의 서버들(물리 또는 가상)을 관리하기 위한 환경을 나타내는 하이-레벨 블록 다이어그램이다.

도 2는 일 실시예에 따른 도 1에 나타낸 하나 이상의 개체들(entities)을 사용하기 위한 컴퓨터의 예를 나타내는 하이-레벨 블록 다이어그램이다.

도 3은 일 실시예에 따른 글로벌 매니저(global manager)의 상세도를 나타내는 하이-레벨 블록 다이어그램이다.

도 4는 일 실시예에 따른 관리 서버의 정책 구현 모듈의 상세도를 나타내는 하이-레벨 블록 다이어그램이다.

도 5는 일 실시예에 따른 특정 관리 서버를 위한 관리 명령들을 생성하는 방법을 나타내는 흐름도이다.

도 6은 일 실시예에 따른 관리 서버의 관리 모듈을 위한 구성을 생성하는 방법을 나타내는 흐름도이다.

도 7은 일 실시예에 따른 관리 서버의 로컬 상태(local state)를 모니터링 하는 방법을 나타내는 흐름도이다.

도 8은 일 실시예에 따른 관리 도메인의 컴퓨터 네트워크 인프라의 상태에 대한 변경을 처리하는 방법을 나타내는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0007] 상기 도면들 및 상기 다음의 설명은 예시의 방법으로만 특정 실시예들을 설명한다. 여기에 나타낸 구조들 및 방법들의 다른 실시예들이 본원에 기재된 원리를 벗어나지 않고 적용될 수 있는 다음의 설명으로부터 당업자가 용이하게 인식할 수 있다. 몇몇 실시예들을 위한 참조의 예시들은 첨부된 도면들에 도시된다. 실행 가능한 유사하

거나 동일한 참조 번호들이 상기 도면들에서 사용되고, 유사하거나 동일한 기능을 나타낸다.

[0008] 도 1은 일 실시예에 따른 관리 도메인 (150)의 서버들(물리 또는 가상)(130)을 관리하기 위한 환경(100)을 나타내는 하이-레벨(high-level) 블록 다이어그램이다. 상기 관리 도메인(150)은 예를 들어, 서비스 제공자(service provider), 법인(corporation), 대학교(university), 또는 정부 기관(government agency)과 같은 기업에 상응할 수 있다. 상기 환경(100)은 상기 기업에 의해 또는 상기 기업이 그것의 서버들(130)을 관리하는 것을 돕는 제3자(예를 들어, 제2 기업(second enterprise))에 의해 유지될 수 있다. 나타낸 것과 같이, 상기 환경(100)은 네트워크(100), 글로벌 매니저(120), 다중 관리 서버들(multiple managed servers)(130), 및 다중 비관리 장치들(multiple unmanaged devices)(140)을 포함한다. 상기 다중 관리 서버들(130) 및 상기 다중 비관리 장치들(140)은 상기 관리 도메인(150)과 관련될 수 있다. 예를 들어, 그것들은 기업 또는 상기 기업을 대신하는 제3자(예를 들어, 퍼블릭 클라우드 서비스 제공자(public cloud service provider))에 의해 동작될 수 있다. 하나의 글로벌 매니저(120), 두 개의 관리 서버들(130), 및 두 개의 비관리 장치들(140)을 명확히 하기 위해 도 1에 묘사된 실시예에서 나타낸 반면에, 다른 실시예들은 다른 수의 글로벌 매니저들(120), 관리 서버들(130), 및/또는 비관리 장치들(140)을 가질 수 있다.

[0009] 상기 네트워크(110)는 상기 글로벌 매니저(120), 상기 관리서버들(130), 및 상기 비관리 장치들(140) 간에 통신 경로(communication pathway)를 나타낸다. 일 실시예에서, 상기 네트워크(110)는 표준 통신 기술들(standard communications technologies) 및/또는 프로토콜들(protocols)을 사용하고, 상기 인터넷을 포함할 수 있다. 또 다른 실시예에서, 상기 네트워크(110) 상의 상기 개체들은 커스텀(custom) 및/또는 전용 데이터 통신 기술들(dedicated data communications technologies)을 사용할 수 있다.

[0010] 관리 서버(130)는 관리 도메인-전역 관리 도메인-전역 관리 정책 (330)(도 3에 나타낸)을 구현하는 머신(물리 또는 가상)이다. 일 실시예에서, 서버는 운영 체제-레벨 가상화(operating system-level virtualization)에 따른 가상 서버 (때때로 컨테이너(container), 가상화 엔진(virtualization engine), 가상 개인 서버(virtual private server), 또는 제일(jail)이라고 부르는)를 대신하는 사용자-공간(user-space)이고, 이것은 하나의 인스턴스 대신, 다중 분리된 사용자-공간 인스턴스들(multiple isolated user-space instances)를 활성화하는 운영 체제의 커널(kernel of an operating system)에서 서버 가상화 방법이다. 관리 서버(130)가 물리 머신(physical machine)인 경우, 상기 관리 서버(130)는 컴퓨터 또는 컴퓨터들의 세트일 수 있다. 관리 서버(130)가 가상 머신(virtual machine)인 경우, 상기 관리 서버(130)는 컴퓨터 또는 컴퓨터들의 세트 상에서 실행한다. 상기 관리 도메인-전역 관리 정책(330)은 상기 관리 도메인(150)과 관련된 개체들(executes)이 다른 개체들 또는 소모(consume)(또는 제공(provide)) 서비스들에 액세스하기 위해 어떻게 할당되는지 여부를 명시한다. 예를 들어, 상기 관리 도메인-전역 관리 정책(330)은 보안 또는 자원 사용(resource usage)을 명시한다. 보안 정책은 액세스 제어, 보안 연결, 디스크 암호화(disk encryption), 및/또는 실행 가능한 프로세스들의 제어(control of executable processes)를 명시할 수 있는 반면, 자원-사용 정책은 상기 관리 도메인의 컴퓨팅 자원들(administrative domain's computing resources)(예를 들어, 디스크들(disks), 주변 장치들, 및/또는 대역폭(bandwidth))의 사용을 명시 할 수 있다.

[0011] 관리 서버(130)는 관리 모듈(132), 관리 모듈 구성 (134), 및 정책 구현 모듈(136)을 포함한다. 상기 관리 모듈(132)은 상기 관리 도메인-전역 관리 정책(330)을 구현한다. 예를 들어, 보안의 경우, 상기 관리 모듈(132)은 로우-레벨 네트워크(low-level network) 또는 운영 체제-레벨 방화벽(operating system-level firewall), 인터넷 프로토콜 보안 엔진(IPsec: Internet Protocol security engine), 또는 네트워크 트래픽 필터링 엔진(network traffic filtering engine)(예를 들처, 윈도우 필터링 플랫폼(WFP: Windows Filtering Platform) 개발 플랫폼에 기반하여)과 같은 보안 엔진(security engine)이 될 수 있다. 자원 사용의 경우, 상기 관리 모듈(132)은 디스크-사용 엔진(disk-usage engine) 또는 주변장치-사용 엔진(peripheral-usage engine)이 될 수 있다.

[0012] 상기 관리 모듈 구성(134)은 상기 관리 모듈(132)의 동작에 영향을 미칠 수 있다. 예를 들어, 보안의 경우, 상기 관리 모듈 구성(134)은 방화벽에 의해 적용된 액세스 제어 규칙들, 인터넷 프로토콜 보안 엔진(IPsec: Internet Protocol security engine)(예를 들어, 상기 리눅스 운영 체제에서 ip테이블 개체들(iptables entries) 및 ip세트 개체들(ipset entries)로써 구현되는)에 의해 적용된 보안 연결 정책들(secure connectivity policies) 또는 필터링 엔진에 의해 적용되는 필터링 규칙들이 될 수 있다. 자원 사용의 경우, 상기 관리 모듈 구성(134)은 디스크-사용 엔진에 의해 적용된 디스크-사용 정책들(disk-usage policies) 또는 주변장치- 사용 엔진에 의해 적용된 주변장치-사용 정책들이 될 수 있다.

[0013] 상기 정책 구현 모듈(136)은 a) 상기 글로벌 매니저(120)로부터 수신된 관리 명령들 및 b) 상기 관리 서버(130)의 상태에 기반하여 상기 관리 모듈 구성(134)을 생성한다. 상기 관리 명령들은 상기 관리 도메인-전역 관리 정책(330)에 기반하여 부분적으로 생성된다. 상기 정책 구현 모듈(136)에 의해 생성된 상기 관리 모듈 구성(134)은 관리 도메인-전역 관리 정책(330)을 구현한다(상기 정책이 관리 서버(130)에 영향을 미치도록). 이러한 두-단계 프로세스(two-step process)(관리 명령들을 생성하고, 상기 관리 모듈 구성(134)를 생성하는)는 "인스턴시에이팅(instantiating)" 관리 정책이라고 한다. 상기 정책 구현 모듈(136)은 또한 상기 관리 서버(130)의 로컬 상태를 모니터하고, 로컬 상태 정보를 상기 글로벌 매니저(120)로 전송한다.

[0014] 일 실시예에서, 상기 정책 구현 모듈(136)은 더 큰 등록 모듈(larger proprietary module)(도시하지 않음)의 부분이다. 상기 등록 모듈(proprietary module)은 이미 관리 모듈(132) 및 관리 모듈 구성(134)을 구비한 장치로 로드됨(loaded)으로써, 상기 장치를 비관리 장치(140)로부터 관리 서버(130)로 변형(transforming)시킨다. 상기 정책 구현 모듈(136)은 도 4, 6 및 7을 참조하여 아래에서 더 설명된다.

[0015] 비관리 장치(140)는 정책 구현 모듈(136)을 포함하지 않는 컴퓨터(또는 컴퓨터들의 세트)이다. 비관리 장치(140)는 상기 관리 도메인-전역 관리 정책(330)을 구현하지 않는다. 하지만, 관리 서버(130) 및 비관리 장치(140) 간에 상호작용은 상기 관리 도메인-전역 관리 정책(330)의 대상이 될 수 있다(상기 관리 서버(130)에 의해 구현됨으로써). 비관리 장치(140)의 일예는 관리 도메인(150)에 의해 사용되는 네트워크 회로(network circuit)이다. 비관리 장치(140)의 또 다른 예는 상기 관리 도메인(150)(예를 들어, 노트북(notebook) 또는 데스크탑 컴퓨터(desktop computer), 태블릿 컴퓨터(tablet computer), 또는 모바일 폰(mobile phone))에 스스로를 인증하는 사람(a person to authenticate himself)에 의해 사용되는 장치이다.

[0016] 상기 글로벌 매니저(120)는 관리 서버들(130)을 위한 관리 명령들을 생성하고 상기 생성된 관리 명령들을 상기 서버들로 전송하는 컴퓨터(또는 컴퓨터의 세트)이다. 상기 관리 명령들은 a) 상기 관리 도메인의 컴퓨터 네트워크 인프라의 상태(state of the administrative domain's computer network infrastructure)(320) 및 b) 관리 도메인-전역 관리 정책(330)에 기반하여 생성된다. 상기 관리 도메인의 컴퓨터 네트워크 인프라의 상태(320)는 관리 서버들(130)의 디스크립션들(descriptions) 및 (선택적으로(optionally)) 비관리 장치들(140)의 디스크립션들을 포함한다. 상기 글로벌 매니저(120)는 또한 관리 서버들(130)로부터 수신된 로컬 상태 정보를 처리한다.

[0017] 로컬 관리 모델에 기반하는 상기 관리 도메인-전역 관리 정책(330)은 IP 주소들, IP 주소 범위들, 서브네트워크들(subnetworks), 및 네트워크 인터페이스들과 같은 로우-레벨 구조들(low-level constructs)을 사용하는 관리 서버들(130)을 참조하지 않는다. 대신에, 상기 로컬 관리 모델은 "레이블들(labels)"이라고 하는 그들의 하이-레벨 특성들(their high-level characteristics)에 기반하는 관리 서버들(130)을 참조한다. 상기 레이블은 한 쌍이고, "차원(dimension)"(하이-레벨 특성들) 및 "값(value)"(상기 하이-레벨 특성들의 값)을 포함한다. 이러한 다차원 공간(multi-dimensional space)으로 구성되는 관리 정책은 싱글-특성 네트워크/IP 주소-기반 정책 모델(single-characteristic network/IP address-based policy model)에 따라 구성된 관리 정책보다 더 풍부하다(more expressive). 특히, "레이블들"의 하이-레벨 추상적 개념을 사용하는 표현 관리 정책(expressing management policy)은 사람이 더욱 잘 이해할 수 있도록 하고, 시각화하고, 관리 정책을 수정한다.

[0018] 상기 로컬 관리 모델(예를 들어, 상기 이용 가능한 차원들의 숫자 및 유형들(number and types of dimensions available) 및 차원의 가능한 값들(dimensions' possible values))이 구성 가능하다. 일 실시예에서, 상기 로컬 관리 모델은 아래 차원들 및 값들을 포함하고, 표 1에 나타내었다:

차원(Dimension)	M(Meaning), V(Values)
Role(역할)	M: 상기 관리 도메인 내에서 상기 관리 서버의 역할 V: 웹(web), API, 데이터베이스(database)
환경(Environment)	M: 상기 관리 서버의 상기 라이프사이클 스테이지 V: 생산(production), 단계(staging), 개발(development)
어플리케이션(Application)	M: 어떤 관리 서버에 속한 상기 로컬 어플리케이션(관리 서버들의 하이-레벨 그룹화) V: 거래(trading), 인적 자원들(human resources)
비즈니스의 라인(Line of Business)	M: 어떤 관리 서버에 속한 상기 비즈니스부(business unit) V: 마케팅(marketing), 엔지니어링(engineering)
위치(Location)	M: 상기 관리 서버의 위치. 물리적(physical)(예를 들어, 국가(country) 또는 지리적 영역(geographical region)) 또는 지역적(logical)일 수 있다. 물리적 위치는 특히 지리적 규정 요건들(geographic compliance requirements)을 표현하기 위해 유용하다. V: US 또는 EU(물리적), us-west-1 또는 us-east-2(로지컬)

[0019]

[0020] <표 1> 로지컬 관리 모델의 예

[0021] 하나 이상의 레이블들("레이블 세트(label set)"라고 하는)을 명시함으로써 함께 그룹화되도록 다중 관리 서버들(130)을 활성화하는 상기 로지컬 관리 모델은 상기 그룹에서 모든 상기 관리 서버들(130)을 설명한다. 레이블 세트는 상기 로지컬 관리 모델에서 차원을 위한 제로 값들(zero values) 또는 1 값(one value) 중 하나를 포함한다. 레이블 세트는 상기 로지컬 관리 모델에서 모든 차원들을 위해 레이블들을 포함하는 것을 필요로 하지 않는다. 이러한 방법에서, 상기 로지컬 관리 모델은 관리 도메인의 관리 서버들(130)의 분할 및 분리를 활성화하고, 관리 서버들(130)의 임의의 그룹들의 생성을 활성화한다. 상기 로지컬 관리 모델을 또한 싱글 관리 서버(130)가 다중 오버랩핑 세트들(multiple overlapping sets)(다시 말해, 관리 서버들의 다중 오버랩핑 그룹들(multiple overlapping groups of managed servers))에서 존재하도록 허용한다. 상기 로지컬 관리 모델은 상기 싱글 관리 서버(130)가 중첩된 세트들의 계층(hierarchy of nested sets)으로 존재하는 것을 제한하지 않는다.

[0022] 예를 들어, 상기 보안의 경우, 분리(segmentation)는 특정 정책들을 대상으로 하는 관리 서버들(130)의 그룹들을 정의하기 위한 액세스 제어 정책들(access control policies)로 사용될 수 있다. 유사하게 분리는 관리 서버들(130)의 그룹들을 정의하기 위한 보안 연결 정책들로 사용될 수 있고, 상기 정책들은 인트라-그룹 통신들(intra-group communications) 및 내부-그룹 통신들(inter-group communications)을 적용한다. 따라서, 관리 서버들(130)의 제1 그룹(제1 레이블 세트에 의해 명시된) 사이의 통신들은 제1 보안 연결 세팅(first secure connection setting)(예를 들어, 보안 통신이 요구되지 않는)으로 제한될 수 있고, 상기 관리 서버들의 제1 그룹 및 관리 서버들의 제2 그룹(제2 레이블 세트에 의해 명시된) 간의 통신들은 제2 보안 연결 세팅(second secure connection setting)(예를 들어, IPsec ESP(IPsec Encapsulating Security Payload)/AH(Authentication Header)/AES(Advanced Encryption Standard)/SHA-2(Secure Hash Algorithm-2))으로 제한될 수 있다.

[0023] 상기 환경(100)에서 각 관리 서버(130)는 상기 관리 도메인-전역 관리 정책(330)(상기 정책이 상기 관리 서버(130)에 영향을 미치는 정도에 대한)을 구현한다. 그 결과, 상기 관리 도메인-전역 관리 정책(330)은 상기 관리 도메인(150)을 통해 분산 방식(fashion)이 적용되고, 초크 포인트(choke point)가 없다. 또한, 상기 관리 도메인-전역 관리 정책(330)은 상기 관리 도메인의 물리적 네크워크 토폴로지(administrative domain's physical network topology) 및 네트워크 어드레싱 기법들(network addressing schemes)과는 별도로 로지컬 레벨에 적용

된다.

[0024] 상기 글로벌 매니저(120), 상기 관리 도메인의 컴퓨터 네트워크 인프라(320), 및 상기 관리 도메인-전역 매니저 정책(330)은 도 3, 5, 및 8을 참조하여 아래에서 더 설명된다.

[0025] 도 2는 일 실시예에 따른 도 1에 나타낸 하나 이상의 개체들(entities)을 사용하기 위한 컴퓨터(200)의 예를 나타내는 하이-레벨 블록 다이어그램이다. 도시된 적어도 하나의 프로세서(202)는 칩셋(chipset)(204)에 연결된다. 상기 칩셋(204)은 메모리 제어기 허브(memory controller hub)(220) 및 입력/출력 제어기 허브(input/output (I/O) controller hub)(222)를 포함한다. 메모리(206) 및 그래픽 어댑터(graphics adapter)(212)는 상기 메모리 제어기 허브(220)에 연결되고, 디스플레이 장치(display device)(218)는 상기 그래픽 어댑터(212)에 연결된다. 저장 장치(storage device)(208), 키보드(keyboard)(210), 포인팅 장치(pointing device)(214), 및 네트워크 어댑터(network adapter)(216)는 상기 I/O 제어기 허브(222)에 연결된다. 상기 컴퓨터(200)의 다른 실시예들은 다른 아키텍처들을 갖는다. 예를 들어, 상기 메모리(206)는 일부 실시예에서 상기 프로세서(202)에 직접 연결된다.

[0026] 상기 저장장치(208)는 하드 디스크(hard drive), CD-ROM(compact disk read-only memory), DVD, 또는 반도체를 이용한 메모리 장치(solid-state memory device)와 같은 하나 이상의 비일시적 컴퓨터 판독 가능한 기억 매체(non-transitory computer-readable storage media)를 포함한다. 상기 메모리(206)는 상기 프로세서(202)에 의해 사용되는 명령 및 데이터를 보유한다. 상기 포인팅 장치(214)는 데이터를 상기 컴퓨터 시스템(200)에 입력하기 위한 상기 키보드(210)와 결합하여 사용된다. 상기 그래픽 어댑터(212)는 이미지 및 다른 정보를 상기 디스플레이 장치(218)에 디스플레이 한다. 일부 실시예들에서, 상기 디스플레이 장치(218)는 사용자 입력 및 선택들을 수신하기 것이 가능한 터치 스크린을 포함한다. 상기 네트워크 어댑터(216)는 상기 컴퓨터 시스템(200)을 상기 네트워크(110)에 연결한다. 상기 컴퓨터(200)의 일부 실시예들은 도 2에 나타낸 것보다 다른 및/또는 기타 요소들을 구비할 수 있다. 예를 들어, 상기 글로벌 매니저(120) 및/또는 상기 관리 서버(130)는 다중 블레이드 서버들(multiple blade servers)로 형성될 수 있고, 디스플레이 장치, 키보드, 및 다른 요소들이 없을 수 있고, 반면에 상기 비관리 장치(140)는 노트북 또는 데스크탑 컴퓨터, 태블릿 컴퓨터, 또는 모바일 폰일 수 있다.

[0027] 상기 컴퓨터(200)는 본 발명에 기재된 기능을 제공하기 위한 컴퓨터 프로그램 모듈들을 실행하기 위해 적용된다. 본 발명에 따른, 상기 용어 "모듈"은 컴퓨터 프로그램 명령 및/또는 상기 명시된 기능을 제공하기 위해 사용된 다른 로직을 나타낸다. 그러므로, 모듈은 하드웨어, 펌웨어, 및/또는 소프트웨어로 구현될 수 있다. 일 실시예에서, 실행 가능한 컴퓨터 프로그램 명령들로 형성된 프로그램 모듈들은 상기 저장 장치(208) 상에 저장되고, 상기 메모리(206)로 로드되고, 상기 프로세서(202)에 의해 실행된다.

[0028] 도 3은 일 실시예에 따른 글로벌 매니저(120)의 상세도를 나타내는 하이-레벨 블록 다이어그램이다. 상기 글로벌 매니저(120)는 저장부(repository)(300) 및 프로세싱 서버(310)를 포함한다. 상기 저장부(300)는 상기 관리 도메인의 컴퓨터 네트워크 인프라(320)의 상태 및 상기 관리 도메인-전역 관리 정책(330)을 저장하는 컴퓨터(또는 컴퓨터들의 세트)이다. 일 실시예에서, 서버를 포함하는 상기 저장부(300)는 상기 프로세싱 서버(310)가 요청들에 응답하여 상기 관리 도메인 상태(320) 및 상기 관리 정책(330)에 액세스하는 것을 제공한다.

[0029] 상기 관리 도메인의 컴퓨터 네트워크 인프라(320)는 관리 서버들(130)의 디스크립션들 및 (선택적으로) 비관리 장치들(140)의 디스크립션들을 포함한다. 예를 들어, 관리 서버(130)의 디스크립션은 고유 식별자 (unique identifier; UID), 온라인/오프라인 표시(online/offline indicator), 하나 이상의 구성된 특성들(one or more configured characteristic)(선택적으로), 네트워크 노출 정보(network exposure information), 서비스 정보(service information), 및 상기 관리 서버(130)를 설명하는 하나 이상의 레이블들(레이블 세트)을 포함한다.

[0030] 상기 UID는 상기 관리 서버(130)를 독특하게 식별한다. 상기 온라인/오프라인 표시는 상기 관리 서버(130)가 온라인 또는 오프라인인지 여부를 나타낸다. "구성된 특성(configured characteristic)"은 상기 관리 서버(130)와 관련된 값을 저장하고, 정보의 어떤 유형(예를 들어, 어떤 동작 시스템이 상기 관리 서버 상에서 동작하는지 나타내는)이 될 수 있다. 구성된 특성은 규칙의 조건 부분(rule's condition portion)(아래에 설명됨)과 함께 사용된다.

[0031] 상기 네트워크 노출 정보는 상기 관리 서버의 네트워크 인터페이스들에 영향을 미친다. 일 실시예에서, 상기 관리 서버의 네트워크 인터페이스들의 각각에 대하여, 상기 네트워크 노출 정보는 어떤 네트워크 인터페이스가 부착되었는지에 대한 "양방향-도달 가능한 네트워크(BRN: bidirectionally-reachable network)"의 식별자 및 상기 BRN 내에서 동작을 위해 사용된 제로(zero) 또는 더 많은 IP 주소들(및 해당 서브넷들(subnets))을

포함한다. 또 다른 실시예에서, 상기 네트워크 노출 정보는 라우팅 정보(routing information) 및/또는 상기 관리 서버가 NAT(network address translator)를 뒤에 있는지 여부(그리고, 그것이 NAT 뒤에 있는 경우, NAT - 1:1 또는 1:N 중 어떤 유형인지)를 포함한다. 조직(organization) 또는 조직 전체(across organizations) 내에서, BRN은 서브넷들(subnets)의 세트이고, 상기 BRN 내에서 어떤 노드(any node)는 상기 BRN에서 어떤 다른 노드(any other node)로 통신을 설정할 수 있다. 예를 들어, BRN에서 상기 노드들 전체는 특유의 IP 주소(unique IP addresses)를 가질 수 있다. 다시 말해, BRN은 어떤 NATs을 포함하지 않는다. 네트워크 노출 정보(예를 들어, 네트워크 인터페이스의 BRN 식별자)는 규칙의 조건 부분과 함께 사용될 수 있다.

[0032] 예를 들어, 상기 서비스 정보는 프로세스 정보(process information) 및/또는 패키지 정보(package information)를 포함한다. 예를 들어, 프로세스 정보는 상기 관리 서버(130)가 동작하는 프로세스들의 네임들(names of processes), 어떤 네트워크 포트들 및 네트워크 인터페이스들의 해당 프로세스들이 수신 대기 중인지, 어떤 사용자들이 해당 프로세스들을 시작했는지, 해당 프로세스들의 구성, 및 해당 프로세스들의 커맨드-라인 시작 아규먼트들(command-line launch arguments)을 포함한다. (해당 프로세스들은 서비스를 제공하거나 서비스를 사용하는 상기 관리 서버(130)에 해당한다.) 예를 들어, 패키지 정보는 어떤 패키지들(실행 가능한 것들(executables), 라이브러리들(libraries), 또는 다른 요소들(other components))이 상기 관리 서버(130) 상에 설치되었는지, 해당 패키지들의 버전들(versions), 해당 패키지들의 구성들, 및 해당 패키지들의 해시 값들(hash values)을 포함한다.

[0033] 예를 들어, 비관리 장치(140)의 디스크립션은 네트워크 노출 정보(예를 들어, 상기 비관리 장치의 IP 주소들 및 어떤 비관리 장치가 연결되었는지에 대한 상기 BRN의 식별자)를 포함한다. 비관리 장치(140)는 "비관리 장치 그룹(UDG: unmanaged device group)"의 부분이다. 하나의 UDG는 하나 이상의 비관리 장치들(140)을 포함한다. 예를 들어, 상기 "헤드쿼터 UDG(Headquarters UDG)"는 일차 회로(primary circuit) 및 관리 도메인의 헤드쿼터로서 사용된 백업 회로(backup circuit)를 포함할 수 있고, 각 회로는 IP주소들과 관련된다. 하나의 UDG는 UID(unique identifier)와 관련된다. UDG와 관하여 상기 관리 도메인 상태(320)에 저장된 정보는 상기 UDG의 UID 및 상기 UDG에서 비관리 장치들(140)에 관한 정보(예를 들어, 그것들의 네트워크 노출 정보)를 포함한다.

[0034] 관리 서버들(130) 및 비관리 장치들(140)의 디스크립션은 상기 글로벌 매니저(120)와 GUI(graphical user interface)을 통해 상호 작용하는 방법 또는 API(application programming interface)와 같은 다양한 방법들로 상기 관리 도메인 상태(320)로 로드될 수 있다. 관리 서버들(130)의 디스크립션은 또한 관리 서버들로부터 수신된 로컬 등급 정보(local status information)에 기반하여 상기 관리 도메인 상태(320)로 로드될 수 있다(아래에 설명됨).

[0035] 특히 관리 서버의 레이블들(managed servers' s labels) (및 구성된 특성들, 있는 경우)에 관하여, 상기 차원을 위한 값(value for a dimension)(또는 구성된 특성의 값의 세팅)의 할당이 더 많은 방법들로 수행될 수 있다. 예를 들어, 상기 할당/세팅은 권한 설정 관리 서버(provisioning a managed server)(130)의 부분으로서 배포(deployment) 및 구성 툴(configuration tool)을 사용하여 수행될 수 있다. 기성 타사 툴들(예를 들어, 퍼펫 랩의 퍼펫 소프트웨어(Puppet Labs' Puppet software), 오프스코드의 셰프 소프트웨어(Opscode's Chef software), 또는 씨에프엔진 에이에스의 씨에프엔진 소프트웨어(CFEngine AS's CFEngine software))를 포함하는 툴이 사용될 수 있다.

[0036] 또 다른 예로써, 상기 할당/세팅은 레이블들 및/또는 구성된 특성("CC") 값들을 계산하는 "레이블/구성된 특성 엔진(label/configured characteristic engine)"(도시하지 않은)에 의해 수행될 수 있다. 일 실시예에서, 상기 레이블/CC 엔진은 레이블/CC 할당 규칙들에 기반하여 레이블들/CC 값들을 계산한다. 레이블/CC 할당 규칙은 상기 관리 도메인 상태(320)로부터 데이터를 액세스하고, 레이블 또는 CC 값을 할당(또는 할당을 제안)하는 기능이다. 레이블/CC 할당 규칙은 미리 설정되거나 사용자 구성이 가능할 수 있다. 예를 들어, 상기 글로벌 매니저(120)는 미리 정의된 규칙들의 세트를 포함하지만, 최종-사용자는 해당 규칙들을 수정 및/또는 삭제할 수 있고 상기 사용자의 사용자 요구사항들에 기반하여 새로운 규칙들을 추가할 수 있다. 레이블/CC 할당은 상기 초기화 프로세스 동안 관리 서버(130)를 위해 평가될 수 있다. 그러면 레이블/CC 값 제안들(Label/CC value suggestions)이 어떤 차원/CC를 위해 생성될 수 있고, 상기 최종-사용자는 해당 제안들을 수용 또는 거절할 수 있다. 예를 들어, 관리 서버(130)가 포스트그레스 데이터베이스(Postgres database), 또는 MySQL 데이터베이스를 실행하고 있을 경우, 그러면 상기 제안된 레이블은 <Role, Database>일 수 있다. 관리 서버가 상기 리눅스 동작 시스템을 실행하고 있을 경우, 그러면 상기 동작 시스템 CC를 위한 제안된 값은 "Linux."일 수 있다.

[0037] 또 다른 실시예에서, 상기 레이블/CC 엔진은 클러스터 분석에 기반하여 레이블/CC 값들을 계산한다. 예를 들어, 상기 레이블/CC 엔진은 고도로 연결된(highly-connected) 관리 서버들(130)의 클러스터를 자동적으로 식별하는 연결된 그래프들의 추가적 휴리스틱(heuristics)과 함께 분-컷(min-cut) 및 K-평균 알고리즘(K-means algorithms)의 조합을 사용한다. 상기 관리 서버들(130)의 클러스터는 상기 관리 도메인(150)에서 "어플리케이션(application)"(표 1을 참조)에 해당할 수 있다. 상기 최종-사용자는 상기 어플리케이션 차원(Application dimension)(또는 어떤 다른 차원)을 위한 값을 해당 관리 서버들(130)에 한꺼번에 적용하기 위해 선택될 수 있다.

[0038] 상기 관리 도메인-전역 정책(330)은 하나 이상의 규칙들을 포함한다. 대체로, "규칙(rule)"은 서비스의 하나 이상의 제공자들(one or more providers) 및 해당 서비스의 하나 이상의 소비자들(one or more consumers) 간의 관계를 명시한다.

[0039] 규칙 기능(Rule Function)- 상기 관계는 "규칙 기능(rule function)"을 위해 제안되고, 이것은 상기 규칙의 실제 효과이다. 예를 들면, 보안의 경우, 상기 규칙 기능은 액세스 제어, 보안 연결, 디스크 암호화, 또는 실행 가능한 프로세스들의 제어일 수 있다. 액세스 제어 기능을 갖는 규칙은 소비자가 제공자의 서비스를 사용하는지 여부를 명시한다. 일 실시에에서, 상기 액세스 제어 기능은 퓨어(pure) "화이트리스트(whitelist)" 모델을 사용하고, 이것은 허용 가능한 관계들(allowable relationships) 만이 표현되고, 모든 다른 관계들은 디폴트(default)에 의해 차단되는 것을 의미한다. 보안 연결 기능을 갖는 규칙은 소비자가 제공자의 서비스를 사용할 수 있는 보안 채널들(예를 들어, 포인트-투-포인트 데이터 암호화(point-to-point data encryption)를 사용하는 암호화된 네트워크 세션들(encrypted network sessions))을 통해 명시한다. 예를 들어, 보안 연결 기능을 갖는 규칙은 상기 제공자가 US에 위치하고, 소비자가 EU에 위치할 때 암호화되어야 되는 제공자의 서비스들의 사용을 명시할 수 있다. 디스크 암호화 기능을 갖는 규칙은 제공자가 암호화된 파일 시스템(encrypted file system) 상에 데이터를 저장해야 하는지 여부를 명시한다. 실행 가능한 프로세스-제어 기능을 갖는 규칙은 제공자가 암호화된 파일 시스템 상에서 실행해야 하는지 여부를 명시한다.

[0040] 자원 사용의 경우에서, 상기 규칙 기능은 디스크-사용(disk-usage) 또는 주변장치-사용(peripheral-usage)일 수 있다. 디스크-사용 기능을 갖는 규칙은 소비자가 제공자에 저장할 수 있는 데이터의 양을 명시한다. 규칙은 다른 규칙 기능들뿐만 아니라, 액세스 제어, 보안 연결, 디스크 암호화, 실행 가능한 프로세스의 제어, 디스크 사용, 및 주변장치 사용을 명시할 수 있다는 것을 나타낸다. 예를 들어, 규칙 기능은 네트워크 트래픽에 적용하기 위한 OSI(Open Systems Interconnection) 모델 레이어-7 서비스들(model Layer-7 services), 보안 분석들을 위해 수집하기 위한 메타 데이터의 양(amount of metadata), 또는 전체 네트워크 패킷(complete network packet)을 컴퓨팅하기 위한 트리거들(triggers)을 명시할 수 있다. 상기 관리 정책 모델은 임의의 수의 적용될 수 있는 규칙 기능들을 지원할 수 있다.

[0041] 하나 이상의 세팅들("기능 프로파일(function profile)"이라고 하는)과 관련된 규칙 기능은 상기 규칙의 실제 효과와 관련하여 상세한 사항들을 명시할 수 있다. 예를 들어, 보안 연결 규칙 기능과 관련된 세팅들은 암호화 네트워크 트래픽에 사용된 암호화 알고리즘(cryptographic algorithms)의 리스트일 수 있다. 일 실시예에서, 규칙 기능은 다중 기능 프로파일들과 관련되고, 기능 프로파일은 정책을 포함한다. 이러한 정책은 아래에 설명된 기능-레벨 명령 생성 모델(function-level instruction generation module)(360)에 의해 사용된다.

[0042] 서비스- 일반적으로 "서비스"는 특정 네트워크 프로토콜(specific network protocol)을 사용하는 특정 네트워크 포트(specific network port) 상에서 실행하는 임의의 프로세스이다. 상기 관리 정책(330) 내에서 규칙의 서비스는 프로세스 정보 및/또는 패키지 정보(상기 관리 도메인 상태(320) 내에서 관리 서버(130)의 디스크립션에 대하여 상술된) 같은, 포트/프로토콜 쌍(port/protocol pair) 및 (선택적으로) 추가적인 자격(additional qualifications)이 명시된다. 관리 서버(130)가 다중 네트워크 인터페이스를 갖는 경우, 그러면 서비스는 모든 네트워크들 상에 노출되거나 해당 네트워크들의 서브세트(subset) 상에만 노출될 수 있다. 상기 최종-사용자는 어떤 네트워크들 상에 서비스가 노출되었는지 명시할 수 있다.

[0043] 제공자/소비자- 상기 서비스의 하나 이상의 제공자들 및 상기 서비스의 하나 이상의 소비자들(다시 말해, 사용자들)은 관리 서버들(130) 및/또는 비관리 장치들(140)이다.

[0044] 일 실시예에서, 규칙은 규칙 기능 포션(rule function portion), 서비스 포션(service portion), 제공된 포션(provided-by portion), 사용된 포션(used-by portion), 및 선택적 규칙 조건 포션(optional rule condition portion)을 포함하는 정보의 세트를 사용하는 상기 관리 도메인-전역 관리 정책(330) 내에서 표시된다. 상기 규칙 기능 포션은 상기 규칙의 실제 효과를 설명하고, 하나 이상의 세팅들(기능 프로파일들)과 관련될 수 있다.

상기 서비스 포션은 상기 서비스에 어떤 규칙을 적용하는지 설명한다. 상기 서비스 포션이 "전체(All)"를 나타낼 경우, 그러면 상기 규칙은 모든 서비스들에 적용한다.

[0045] 상기 제공된(PB: provided-by) 포션은 어떤 관리 서버들(130) 및/또는 비관리 장치들(140)이 상기 서비스를 제공할 수 있는지(다시 말해, "제공자(providers)"가 누구인지) 설명한다. 상기 PB 포션이 "누구든지(Anybody)"을 나타낼 경우, 그러면 누구든지(예를 들어, 어떤 관리 서버(130) 또는 비관리 장치(140)) 상기 서비스를 제공할 수 있다. 상기 제공된 포션이 "임의의 관리 서버(Any managed server)"를 나타낼 경우, 그러면 임의의 관리 서버(130)가 상기 서비스를 제공할 수 있다. ("임의의 관리 서버"는 와일드카드(wildcard)를 포함하는 명시하는 레이블 세트(specifying a label set)와 동일하므로, 모든 관리 서버들(130)과 매칭된다.) 상기 사용된(UB: used-by) 포션은 어떤 관리 서버들(130) 및/또는 비관리 장치들(140)이 상기 서비스를 사용할 수 있는지(다시 말해, 누가 "소비자(consumers)"인지) 설명한다. 상기 PB 포션과 유사하게, 상기 UB 포션은 또한 "누구든지(Anybody)" 또는 포션이 "임의의 관리 서버(Any managed server)"를 나타낼 수 있다.

[0046] 상기 PB 포션 및 UB 포션 내에서, 관리 서버(130)는 레이블 세트(다시 말해, 상기 관리 서버를 설명하는 하나 이상의 레이블들) 또는 UID를 사용함으로써 명시될 수 있다. 레이블 세트들을 사용하는 상기 관리 서버들(130)을 명시하는 능력은 그들의 차원들 및 값들(레이블들)에 기반하여 관리 서버들을 참조하는 상기 로지컬 관리 모델로부터 기인한다. 비관리 장치(140)는 비관리 장치 그룹(UDG: unmanaged device group)의 UID를 사용함으로써 명시된다. 규칙이 UDG를 명시할 경우, 그러면 상기 규칙은 해당 그룹에서 상기 비관리 장치들(140)에 관하여 추가적인 정보(예를 들어, 상기 장치의 네트워크 노출 정보)를 포함한다. 상기 규칙의 PB 포션 및/또는 상기 규칙의 UB 포션은 다중 아이템들(multiple items), 포함하는 레이블 세트들(including label sets)(관리 서버(130)를 명시하기 위한), 관리 서버 UIDs(managed server UIDs), 및/또는 UDG UIDs를 포함할 수 있다.

[0047] 상기 추가적인 규칙 조건 포션은 상기 규칙을 특정 관리 서버(130) 및/또는 해당 관리 서버의 특정 네트워크 인터페이스에 적용하는지 여부를 명시한다. 상기 규칙 조건 포션은 하나 이상의 구성된 특성들("CCs"; 상기 관리 도메인 상태(320)에서 관리 서버의 디스크립션의 부분) 및/또는 네트워크 노출 정보(예를 들어, 네트워크 인터페이스의 BRN 식별자; 또는 상기 관리 도메인 상태(320)에서 관리 서버의 디스크립션의 부분)을 포함하는 불 연산식(Boolean expression)이다. 상기 연산식의 CC 포션은 상기 규칙을 상기 특정 관리 서버에 적용하는지 여부를 명시하고, 반면에 상기 연산식의 네트워크 노출 정보 포션은 상기 규칙을 해당 관리 서버의 특정 네트워크 인터페이스에 적용하는지 여부를 명시한다. 상기 연산식이 특정 관리 서버의 구성된 특성들(특히, 해당 관리 서버의 구성된 특성들의 상기 값을 위해) 및 특정 네트워크 인터페이스의 정보에 대해 "참(true)"을 평가할 경우, 그러면 상기 규칙은 해당 관리 서버 및 해당 관리 서버의 관련 네트워크 인터페이스에 적용한다. 상기 연산식이 "거짓(false)"을 평가할 경우, 그러면 상기 규칙은 해당 관리 서버 및 해당 관리 서버의 관련 네트워크 인터페이스에 적용하지 않는다. 예를 들어, 구성된 특성이 어떤 운영 체제가 상기 관리 서버 상에서 동작하고 있는지 명령을 저장하는 경우, 그러면 규칙 조건 포션은 상기 규칙이 해당 서버의 운영 체제에 기반하여 특정 관리 서버에 적용되는지 여부를 제어할 수 있는 구성된 특성을 포함한다.

[0048] 상기 관리 도메인-전역 관리 정책(330) 내에서 규칙들은 규칙 리스트들로 조직화된다. 특히, 상기 관리 정책(330)은 하나 이상의 규칙 리스트들을 포함하고, 규칙 리스트는 하나 이상의 규칙들 및 (선택적으로) 하나 이상의 범위들(scopes)을 포함한다. "범위"는 어디에(다시 말해, 어떤 관리 서버들(130)에) 규칙이 적용되는지를 포함한다. 범위는 상기 규칙 리스트에서 상기 규칙들의 어플리케이션을 제한하는 제공된 포션 및 사용된 포션을 포함한다. 상기 범위의 제공된 포션은 상기 규칙들의 PB 포션을 제한하고, 상기 범위의 UB 포션은 상기 규칙들의 UB 포션을 제한한다. 상기 범위의 PB 및 UB 포션들은 레이블 세트를 사용함으로써 관리 서버들(130)의 그룹을 명시할 수 있다. 상기 레이블 세트가 특정 차원을 위한 레이블을 포함하지 않을 경우, 그러면 상기 관리 서버들(130)의 결과 그룹(resulting group)을 위한 해당 차원의 범위가 없다. 규칙 리스트가 임의의 범위들을 포함하지 않을 경우, 그러면 이것의 규칙들은 글로벌하게 적용된다.

[0049] 다른 범위들이 싱글 규칙 리스트에 적용될 수 있다. 예를 들어, 최종-사용자는 웹 서비스 티어(web service tier)가 상기 데이터베이스 티어(database tier)로부터 어떻게 서비스들을 소비하는지, 로드-밸런싱 티어(load-balancing tier)가 상기 웹 서비스 티어로부터 어떻게 서비스를 소비하는지 등을 표현하는 규칙들의 세트를 형성할 수 있다. 그러면, 상기 최종-사용자가 이러한 규칙 리스트를 그의 생산 환경(production environment) 및 그의 스테이징 환경(staging environment)에 적용을 원하는 경우, 그는 상기 규칙 리스트의 카피 또는 복제를 필요로 하지 않는다. 대신에, 그는 싱글 규칙 리스트(single rule list)에 다중 범위들을 적용한다. 상기 범위 추상(scope abstraction)은 이용 가능한 관점(usability perspective) 및 계산적 관점(computational

perspective)으로부터 상기 규칙 리스트 스케일을 형성한다.

[0050] 이제 상기 관리 도메인-전역 관리 정책(330)을 설명하고, 이것은 몇몇 예시들을 통해 유용하게 설명한다. 두 개의-티어 어플리케이션(two-tier application)을 갖는 관리 도메인(150)을 고려하고, 사용자 장치는 웹 서버(web server)(제1 티어(the first tier))에 액세스 하고, 상기 웹 서버는 데이터베이스 서버(database server)(제2 티어(the second tier))에 액세스한다. 상기 제1 티어에서, 상기 사용자 장치는 상기 소비자이고, 상기 웹 서버는 상기 제공자이다. 상기 제2 티어에서, 상기 웹 서버는 상기 소비자이고, 상기 데이터베이스는 상기 제공자이다. 상기 관리 도메인(150)은 이러한 어플리케이션의 두 가지 경우들을 포함한다: 하나는 생산 환경에서이고, 하나는 스테이징 환경에서이다.

[0051] 상기 웹 서버들 및 상기 데이터 베이스 서버들은 관리 서버들(130)이고, 그것들의 디스크립션들(예를 들어, 레이블 세트들)은 현재 상기 관리 도메인 상태(320)이다. 예를 들어, 그것들의 레이블 세트들은:

[0052] 생산에서 웹 서버(web server in production): <Role, Web> 및 <Environment, Production>

[0053] 생산에서 데이터베이스 서버(database server in production): <Role, Database> 및 <Environment, Production>

[0054] 스테이징에서 웹 서버(web server in staging): <Role, Web> 및 <Environment, Staging>

[0055] 스테이징에서 데이터베이스 서버(database server in staging): <Role, Database> 및 <Environment, Staging>

[0056] (상기 어플리케이션 차원(Application dimension), 상기 불 연산식의 라인(Line of Business dimension), 상기 위치 차원(Location dimension)은 이러한 예시와 연관되지 않고, 그것들의 레이블들은 생략된다.)

[0057] 이제 아래 관리 도메인-전역 관리 정책(330)을 고려하고, 이것은 액세스 제어 및 보안 연결을 명시하는 보안 정책이다.

[0058] 규칙 리스트(Rule List) #1

[0059] - 범위(Scopes)

[0060] <Environment, Production>

[0061] <Environment, Staging>

[0062] - 규칙(Rules)

[0063] #1

[0064] Function: Access Control

[0065] Service: Apache

[0066] PB: <Role, Web>

[0067] UB: Anybody

[0068] #2

[0069] Function: Access Control

[0070] Service: PostgreSQL

[0071] PB: <Role, Database>

[0072] UB: <Role, Web>

[0073] 규칙 리스트(Rule List) #2

[0074] - 범위(Scopes): None

[0075] - 규칙(Rules)

[0076] #1

[0077] Function: Secure Connectivity

[0078] Service: All

[0079] PB: <Role, Database>

[0080] UB: Any managed server

[0081] 상기 규칙들은 서비스와 관련 있고, 명확성을 위해 단순하게 "Apache" 및 "PostgreSQL"이라고 한다. 서비스는 프로세스이고, 프로세스 정보 및/또는 패키지 정보(상기 관리 도메인 상태(320) 내에서 관리 서버(130)의 디스크립션에 대하여 상술된)와 같은 포트/프로토콜 쌍 및 (선택적으로) 추가적인 자격들에 의해 명시된다는 것을 상기한다.

[0082] 규칙 리스트(Rule List) #1/규칙(Rule) #1은 웹 서버와 연결하고, 아파치 서비스(Apache service)를 사용하기 위한 임의의 장치(예를 들어, 사용자 장치)를 허용한다. 특히, 상기 연결의 허용은 기능 옵션(Function portion)에서 "액세스 제어(Access Control)"로 명시된다. 상기 "임의의 장치(any device)"는 상기 UB 포션에서 "누구든지(Anybody)"로 명시된다. 상기 "웹 서버"는 상기 PB 포션에서 "<Role, Web>"(하나의 레이블만을 포함하는 레이블 세트)로 명시된다. 상기 아파치 서비스는 상기 서비스 포션에서 "아파치(Apache)"로 명시된다.

[0083] 규칙 리스트(Rule List) #2/규칙(Rule) #2는 웹 서버를 데이터베이스 서버 상에서 PostgreSQL 에 연결하도록 허용한다. 특히, 상기 연결의 허용은 상기 기능 포션에서 "액세스 제어(Access Control)"로 명시된다. 상기 "웹 서버"는 상기 UB 포션에서 "<Role, Web>"로 명시된다. 상기 "PostgreSQL"는 서비스 포션에서 "PostgreSQL"로 명시된다. 상기 "데이터베이스(database server)"는 PB 포션에서 <Role, Database>(하나의 레이블만 포함하는 레이블 세트)로 명시된다.

[0084] 규칙 리스트(Rule List) #1는 또한 상기 웹 서버 및 데이터베이스 서버가 모두 동일한 환경(예를 들어, 모두 생산 환경 또는 모두 스테이징 환경)일 경우 내부-환경 연결들(inter-environment connections)을 방지한다. 예를 들어, 웹 서버는 데이터베이스 서버 상에서 PostgreSQL에 연결되도록 허용된다. 상기 생산 환경에서 두 서버들은 상기 범위 포션(Scope portion)에서 "<Environment, Production>"(하나의 레이블만을 포함하는 레이블 세트)로 명시되고, 반면에 상기 스테이징 환경에서 두 서버들은 상기 범위 포션에서 "<Environment, Staging>"(하나의 레이블만을 포함하는 레이블 세트)로 명시된다. 그 결과, 웹 서버는 상기 서버들이 다른 환경들에 있는 경우(예를 들어, 상기 웹 서버가 상기 스테이징 환경에 있고, 상기 데이터베이스 서버가 상기 생산 환경에 있는 경우) 데이터베이스 서버 상에서 PostgreSQL와의 연결을 허용하지 않는다.

[0085] 규칙 리스트(Rule List) #2 임의의 관리 서버가 데이터베이스 서버에 연결되는지 여부를 나타내고, 해당 연결은 암호화된 채널(encrypted channel)을 통해 수행되어야만 한다. 특히, 상기 "데이터 서버(database server)"는 상기 PB 포션 상에서 "<Role, Database>"로 명시된다. 상기 "암호화된 채널"은 상기 기능 포션에서 "보안 연결(Secure Connectivity)"로 명시된다. 상기 "임의의 관리 서버(any managed server)"는 상기 UB 포션에서 "임의의 관리 서버(Any managed server)"로 명시된다. 상기 "언제든지(whenever)"는 상기 서비스 포션에서 "전체(All)"로 명시된다.

[0086] 상기 예시로부터 벗어나, 아래 두 개의 관리 서버들(130)을 고려하여: 서버 1은 생산의 부분(part of production), 어플리케이션1의 부분(part of app1), 및 캘리포니아에서 소유된 엔지니어링(owned by engineering in California) 웹 서버이고, 이것은 다음과 같이 레이블된다:

[0087] <Role, Web>

[0088] <Environment, Production>

[0089] <Application, app1>

[0090] <LB, Engineering>

[0091] <Location, US>

[0092] 서버 2는 생산의 부분(part of production), 또한 어플리케이션1의 부분(part of app1), 및 또한 독일에서 소유되지 않은 엔지니어링(owned by engineering but in Germany) 데이터베이스 서버이다. 이것은 다음과 같이 레이블된다:

[0093] <Role, Database Server>

[0094] <Environment, Production>

[0095] <Application, app1>

[0096] <LB, Engineering>

[0097] <Location, EU>

[0098] 액세스 제어 규칙이 어플리케이션1의 부분(part of app1)인 모든 관리 서버들(130)에 대한 모든 액세스을 허용한다고 가정한다. 이러한 규칙은 서버 1 및 서버 2가 서로 통신하도록 허용하고, 서버 1 또는 서버 2와의 통신으로부터 어플리케이션2의 부분(part of app2)인 독일의 관리 서버(130)를 허용하지 않는다. 이제 보안 연결 규칙이 EU 및 US 간의 모든 네트워크 트래픽(all network traffic)이 암호화되어야 한다는 것을 명시한다고 가정한다. 다시 말해, 상기 보안 연결 규칙은 상기 액세스 제어 규칙과 관계없이 적용된 분리 정책이다. 그 결과, 서버 1로부터 서버 2로의 상기 네트워크 트래픽은 허용되고(상기 액세스 제어 규칙이 주어짐), 암호화된다(상기 보안 연결 규칙이 주어짐).

[0099] 도 3을 참조하면, 상기 프로세싱 서버(310)는 관리 서버들(130)을 위한 관리 명령들을 생성하고 상기 생성된 관리 명령들을 상기 서버들로 전송한다. 상기 프로세싱 서버(310)는 또한 관리 서버들(130)로부터 수신된 로컬 상태 정보를 처리한다. 상기 프로세싱 서버(310)는 정책 엔진 모듈 (340), 관련 규칙 모듈(relevant rules module)(350), 기능-레벨 명령 생성 모듈(function-level instruction generation module)(360), 액터 열거 모듈(actor enumeration module)(370), 관련 액터 모듈(relevant actors module)(380), 및 관리 도메인 상태 업데이트 모듈(administrative domain state update module)(385)과 같은 다양한 모듈들을 포함한다. 일 실시예에서, 상기 프로세싱 서버(310)는 상기 저장부(300)와 통신하고, 데이터(예를 들어, 정책 엔진 모듈(policy engine module)(340), 관련 규칙 모듈(relevant rules module)(350), 기능-레벨 명령 생성 모듈(function-level instruction generation module)(360), 액터 열거 모듈(actor enumeration module)(370), 관련 액터 모듈(relevant actors module)(380), 및 관리 도메인 상태 업데이트 모듈(administrative domain state update module)(385)을 실행함에 따른)를 처리하는 컴퓨터(또는 컴퓨터들의 세트)를 포함한다.

[0100] 상기 관련 규칙 모듈(350)은 관리 도메인-전역 관리 정책(330) 및 해당 서버와 관련된 규칙들의 세트를 생성하는 특정 관리 서버(130)(예를 들어, 해당 서버의 UID)의 명령을 입력으로 받아들이고, 상기 규칙들의 세트를 출력한다. 이것은 상기 관련 규칙 모듈(350)이 상기 관리 정책(330)을 검토하고, 주어진 관리 서버(130)를 위한 관련 규칙들만을 추출하는 것에 의한 필터링 처리이다. 상기 관련 규칙 모듈(350)은 상기 관리 정책(330)에서 규칙 리스트들 전체를 반복하고, 상기 범위들을 해당 관리 서버(130) 적용할지 여부를 결정하기 위해 상기 각 규칙 리스트의 범위를 분석하고, (상기 범위들을 이러한 관리 서버(130)에 적용할 경우) 해당 규칙들을 해당 관리 서버(130)에 적용할지 여부를 결정하기 위해 상기 각 규칙 리스트의 규칙들을 분석함으로써 상기 필터링을 수행한다. 규칙은 a) 상기 규칙의 PB 포션 및/또는 상기 규칙의 UB 포션이 상기 관리 서버를 명시할 경우, b) 상기 규칙의 조건 포션(현재일 경우)이 해당 관리 서버에 대하여 "참(true)"으로 평가할 경우(특히, 상기 해당 관리 서버의 구성된 특성들의 값들 및 네트워크 노출 정보에 대하여) 관리 서버(130)에 적용한다. 상기 최종 결과("관리 정책 관점"에 관련된)는 규칙들의 두 세트들의 모임이다: 해당 관리 서버(130)가 서비스를 제공하는 규칙들 및 해당 관리 서버(130)가 서비스를 소비하는 규칙들.

[0101] 기능-레벨 명령 생성 모듈(360)은 규칙들의 세트(예를 들어, 상기 관련 규칙 모듈(350)에 의해 생성된 관리 정책 관점)를 입력으로 받아들이고, 기능-레벨 명령들 생성하고, 상기 기능-레벨 명령들을 출력한다. 상기 기능-레벨 명령은 상기 관리 명령들의 부분으로서 관리 서버(130)로 나중에 전송된다. 기능-레벨 명령은 규칙 기능 포션, 서비스 포션, PB 포션, 및 UB 포션을 포함하는 각각의 규칙과 유사하다. 하지만, 규칙은 그것의 PB 포션 및/또는 UB 포션(레이블 세트들, 관리 서버 UIDs, 및/또는 UDG UIDs를 포함하는) 내에서 다중 아이템들(multiple items)을 포함하는 반면, 기능-레벨 명령은 그것의 PB 포션 내에서 하나의 아이템만을 포함하고, 그것의 UB 포션 내에서 하나의 아이템만을 포함한다. 또한, 규칙은 그것의 PB 포션 및/또는 UB 포션 내에서 관리 서버(다중 네트워크 인터페이스들을 포함하는)를 명시할 수 있는 반면, 기능-레벨 명령은 그것의 PB 포션 및 UB 포션 내에서 하나의 네트워크 인터페이스만을 포함한다.

[0102] 상기 기능-레벨 명령 생성 모듈(360)은 규칙을 분석하고, 해당 규칙에 기반하여 하나 이상의 기능-레벨 명령들을 생성한다. 상기 규칙의 PB 포션은 다중 아이템들을 포함하고, 상기 규칙의 UB 포션은 다중 아이템들을 포함하고, 또는 상기 규칙에 의해 참조된다 관리 서버는 다중 네트워크 인터페이스들을 구비하고, 그러면 상기 기능-레벨 명령 생성 모듈(360)은 다중 기능-레벨 명령들(예를 들어, PB 아이템, UB아이템, 및 특정 네트워크 인터

페이스 각각의 가능한 조합을 위한 하나의 기능-레벨 명령)을 생성한다.

[0103] 그것의 PB 포션(A 및 B)에서 두 개의 아이템들 및 그것의 UB 포션(C 및 D)에서 두 개의 아이템들을 포함하는 규칙을 고려한다. 상기 기능-레벨 명령 생성 모듈(360)은 아래의 PB 및 UB 포션들을 갖는 네 개의 기능-레벨 명령들을 생성한다: 1) PB = A, UB = C; 2) PB = A, UB = D; 3) PB = B, UB = C; 4) PB = B, UB = D. 이제 그것의 PB 포션 또는 UB 포션에서 관리 서버를 커버하는 규칙(예를 들어, UID 또는 레이블 세트를 명시함으로써)을 고려하고, 해당 관리 서버는 다중 네트워크 인터페이스들을 구비한다. 상기 기능-레벨 명령 생성 모듈(360)은 다중 기능-레벨 명령들을 생성한다(예를 들어, 상기 관리 서버의 각 네트워크 인터페이스를 위한 하나의 기능-레벨 명령).

[0104] 상기 기능-레벨 명령 생성 모듈(360)은 상기 규칙들, 해당 규칙들 내에서의 상기 기능들, 및 해당 규칙들에 의해 참조되는 상기 기능 프로파일들(function profiles)을 분석한다. 규칙 리스트가 다중 범위들(multiple scopes)을 포함하는 경우, 그러면 상기 기능-레벨 명령 생성 모듈(360)은 해당 범위들 다중 아이템들(scopes multiple times)을 상기 규칙 리스트에 반복적으로 적용한다(따라서 각 범위를 위한 기능-레벨 명령들의 전체 세트를 생성하는). 규칙 기능은 다중 기능 프로파일들과 관련될 수 있고, 기능 프로파일은 우선순위(priority)을 포함할 수 있다는 것을 상기한다. 상기 기능-레벨 명령 생성 모듈(360)은 상기 다양한 기능 프로파일들의 상기 우선순위들에 기반하여 상기 규칙들을 명령하고 가장 높은 우선순위를 갖는 상기 기능 프로파일이 사용된다. 상기 기능-레벨 명령 생성 모듈(360)은 상기 명령된 규칙들을 상기 관리 서버(130)을 실행하기 위한 기능-레벨 명령들로 변환한다. 기능-레벨 명령들은 상기 적절한 관리 서버들(130) 및/또는 비관리 장치들(140)을 참조하고(예를 들어, 입력 규칙들에서 상기 관리 서버들(130) 및/또는 비관리 장치들(140)이 참조된다), 상기 규칙들과 관련된 서비스들의 네트워크 노출 세부사항들(network exposure details)을 고려한다.

[0105] 상기 기능-레벨 명령 생성 모듈(360)은 해당 서버를 위해 적절하지 않은 것으로 판단되는 특정 관리 서버(130)을 위한 기능-레벨 명령을 생성할 수 있다. 예를 들어, 해당 관리 서버는 상기 규칙의 PB(provided-by)에 의해 커버되고, 상기 기능-레벨 명령 생성 모듈(360)은 해당 기능-레벨 명령을 생성한다. 하지만, 상기 규칙은 또한 상기 관리 서버의 로컬 상태(예를 들어, 상기 제공된 서비스를 설명하는 서비스 포션)를 명시하는 포션을 포함한다. 상기 글로벌 매니저(120)는 상기 관리 서버의 로컬 상태(예를 들어, 상기 관리 서버가 실제로 서비스를 제공하는지 여부)를 알지 못하기 때문에, 상기 생성된 기능-레벨 명령은 상기 관리 서버로 전송된다. 상기 관리 서버는 그것의 로컬 상태(예를 들어, 그것이 서비스를 제공하는지 여부)를 체크하고, 상기 정책 컴필레이션 모듈(policy compilation module)(410)을 참조하여 아래에 설명된 것과 같이 상기 기능-레벨 명령에 따라 처리한다.

[0106] 상기 액터 열거 모듈(actor enumeration module)(370)은 관리 서버(130)의 디스크립션의 모임(collection of descriptions) 및 비관리 장치 그룹들(UDGs: unmanaged device groups)(예를 들어, 상기 관리 도메인의 컴퓨터 네트워크 인프라(320)의 상태)을 입력으로 받아들이고, 열거된 형태("액터-세트(actor-sets)"라고 하는)로 서버들 및 UDGs의 해당 디스크립션들의 표시들(representations)을 생성하고, 상기 액터-세트들을 출력한다. 예를 들어, 상기 액터 열거 모듈(370)은 상기 관리 도메인 상태(320) 및 상기 가능한 레이블 세트들 내에서 상기 관리 서버들(130) 및 상기 UDGs을 열거하고, 각각의 UID(unique identifier)를 할당한다. 이러한 액터-세트들은 관리 서버 UIDs, UDG UIDs, 및/또는 레이블 세트들을 사용하여 액터들을 명시하는 규칙들 및 범위들의 UB 포션들 및 PB 포션들과 함께 사용될 수 있다.

[0107] 차원 $D_i(i=1,\ldots,N)$의 N개의 세트를 포함하는 로컬 관리 모델을 고려하고, 각 D_i차원은 가능한 값들 $V_{ij}(j=1,\ldots,M_i)$의 하나의 세트 S_i을 포함한다(여기에서, 상기 와일드카드"*"는 상기 가능한 값들 중 하나이다). 일 실시예에서, 모든 레이블 세트들을 열거하는 상기 액터 열거 모듈(370)은 상기 로지컬 관리 모델에 기반하여 가능하고, 이것은 $S_1 \times S_2 \times \ldots \times S_N$ 로 주어진 데카르트 곱(Cartesian product)과 동일하다. 이러한 세트의 사이즈는 $M_1 \times M_2 \times \ldots \times M_N$이다. 상기 열거 프로세스는 상기 광리 서버들(130)의 다차원 레이블 공간을 단순하게 열거된 형태로 변형시킨다.

[0108] 또 다른 실시예에서, 해당 레이블 세트들만을 열거하는 상기 액터 열거 모듈(370)은 상기 관리 도메인 상태(320)에 기반하여(예를 들어, 상기 관리 도메인(150) 내에서 관리 서버들의 디스크립션들에 기반하여) 가능하다. 예를 들어, 2 차원(X 및 Y) 포함하는 로지컬 관리 모델을 고려하고, 각 차원은 3 개의 가능한 값(A, B, 및 *)을 포함한다. 상기 레이블 세트 "<X=A>,<Y=B>"을 갖는 관리 서버는 4개의 가능한 레이블 세트들의 멤버

일 수 있다: 1) "<X=A>,<Y=B>", 2) "<X=A>,<Y=*>", 3) "<X=*>,<Y=B>", and 4) "<X=*>,<Y=*>". 상기 관리 서버의 레이블 세트는 2-차원 공간으로 존재하고(X 및 Y), 반면에 가능한 레이블 세트들 2, 3, 및 4는 서브-차원 공간으로의 상기 관리 서버의 레이블 세트의 영사들(projections)이다(레이블 세트 2는 1-차원 공간(X), 레이블 세트 3은 1-차원 공간(Y), 및 레이블 세트 4는 0-차원 공간). 따라서, 상기 액터 열거 모듈(370)은 4개의 가능한 레이블 세트들을 열거한다. 상기 레이블 세트 "<X=A>,<Y=B>"를 갖는 상기 관리 서버는 상기 레이블 세트 "<X=A>,<Y=A>"의 멤버가될 수 없고, 상기 액터 열거 모듈(370)은 해당 레이블 세트를 열거할 수 없다.

[0109] 액터-세트(actor-set)는 UID 및 제로(zero) 또는 더 많은 액터-세트 레코드들(actor-set records)을 포함한다. 액터-세트 레코드는 UID(관리 서버 UID 또는 UDG UID 중 하나), 상기 액터의 운영 체제의 식별자(identifier of the actor's operating system), 및 상기 주어진 특정 BRN의 상기 액터의 IP 주소(IP address of the actor)(관리 서버(130) 또는 비관리 장치(140))를 포함한다. 예를 들어, 액터-세트는 액터-세트 레코드들을 포함할 수 있고, 액터-세트 레코드들의 IP 주소들은 <Role, Database> 및 <Environment, Production>의 상기 레이블 세트에 의해 커버되는 모든 관리 서버들(130)에 해당한다. 또 다른 예로써, 액터-세트는 액터-세트 레코드들을 포함할 수 있고, 액터-세트 레코드들의 IP 주소들은 상기 헤드쿼터 UDG에서 모든 비관리 장치들(140)에 해당한다. 싱글 액터(예를 들어, 관리 서버(130) 또는 비관리 장치(140))는 다중 액터-세트들에서 나타날 수 있다.

[0110] 상기 액터-세트 계산에서 또 다른 팩터는 다중 네트워크 인터페이스를 갖고, 네트워크 주소 변환(NAT: network address translation)과 같은 상기 네트워크 기법의 포함(inclusion)을 추가적으로 갖는 액터들이다. 따라서, 상기 <Role, Database> 및 <Environment, Production>의 레이블 세트를 위한 두 개의 액터-세트들이 있을 수 있다: 해당 관리 서버들(130)의 상기 인터넷-접속 IP 주소들(internet-facing IP addresses)을 갖는 하나의 액터-세트(예를 들어, 제1 BRN과 관련된), 및 해당 관리 서버들의 상기 개인 네트워크-접속 IP 주소들(network-facing IP addresses)을 갖는 해당 동일한 관리 서버들을 위한 다른 액터-세트(예를 들어, 제2 BRN과 관련된).

[0111] 일 실시예에서, 상기 액터 열거 모듈(370)은 또한 상기 관리 도메인의 상태(320)에 대한 변경에 기반하여 액터-세트들을 업데이트 할 수 있다. 예를 들어, 상기 액터 열거 모듈(370)은 액터-세트들(상기 액터 열거 모듈에 의한 이전 출력) 및 관리 서버의 디스크립션에 대한 변경(상기 관리 도메인 상태(320) 내에서)을 입력으로 받아들이고, 업데이트된 액터-세트들(상기 변경된 서버 디스크립션과 일치하는)을 생성하고, 상기 업데이트된 액터-세트들을 출력한다. 상기 액터 열거 모듈(370)은 상기 관리 서버의 디스크리션에 대한 변경의 유형에 따라 다른 방법으로 상기 업데이트된 액터-세트들을 생성한다.

[0112] 오프라인/온라인 변경 - 상기 디스크립션 변경이 상기 서버가 온라인으로부터 오프라인으로 된 것을 나타낼 경우, 그러면 상기 액터 열거 모듈(370)은 상기 서버의 액터-세트 레코드를 상기 서버가 멤버인 모든 입력 액터-세트들로부터 제거함으로써 상기 업데이트된 액터-세트들을 생성한다. 상기 디스크립션 변경이 상기 서버가 오프라인으로부터 온라인으로 된 것을 나타낼 경우, 그러면 상기 액터 열거 모듈(370)은 상기 서버의 액터-세트 레코드를 임의의 관련 입력 액터-세트들에 추가함으로써 업데이트된 액터-세트들을 생성한다. (필요한 경우, 상기 액터 열거 모듈(370)은 새로운 액터-세트를 생성하고, 상기 서버의 액터-세트 레코드를 새로운 액터-세트에 추가한다.)

[0113] 레이블 세트 변경 – 상기 디스크립션 변경이 상기 서버의 레이블 세트가 변경된 것을 나타낼 경우, 그러면 상기 액터 열거 모듈(370)은 이와 같이 제1 서버(상기 이전 레이블 세트(old label set)를 갖는)가 오프라인으로 가고, 제2 서버(새로운 레이블 세트(new label set)를 갖는)가 온라인으로 오도록 다룬다.

[0114] 네트워크 노출 정보 변경 – 상기 디스크립션 변경이 상기 서버가 네트워크 인터페이스를 제거한 것을 나타낼 경우, 그러면 상기 액터 열거 모듈(370)은 상기 서버가 멤버인 모든 입력 액터-세트들(네트워크 인터페이스의 BRN과 관련된)로부터 상기 서버의 액터-세트를 제거함으로써 상기 업데이트된 액터-세트들을 생성한다. 상기 디스크립션 변경이 상기 서버가 네트워크 인터페이스를 추가한 것을 나타낼 경우, 그러면 상기 액터 열거 모듈(370)은 상기 서버의 액터-세트 레코드를 임의의 관련 입력 액터-세트들(네트워크 인터페이스의 BRN과 관련된)에 추가함으로써 상기 업데이트된 액터-세트들을 생성한다. (필요한 경우, 상기 액터 열거 모듈(370)은 새로운 액터-세트(네트워크 인터페이스의 BRN과 관련되)를 생성하고, 상기 서버의 액터-세트 레코드를 새로운 액터-세트에 추가한다.) 상기 디스크립션 변경이 상기 서버가 네트워크 인터페이스의 BRN을 변경한 것을 나타내는 경우, 그러면 액터 열거 모듈(370)은 이와 같이 제1 네트워크 인터페이스(이전 BRN(old BRN)을 갖는)가 제거되고, 제2 네트워크 인터페이스(새로운 BRN(new BRN)을 갖는)가 추가되도록 다룬다. 상기 디스크립션 변경이 상기 서버가 네트워크 인터페이스의 IP 주소를 변경한 것을 나타내는 경우(BRN은 변경되지 않음), 그러면 상기 액터 열거 모듈(370)은 상기 서버가 멤버인 모든 입력 액터-세트들(네트워크 인터페이스의 BRN)에서 상기 서버의 액

터-세트 레코드를 수정함으로써 상기 업데이트된 액터-세트들을 생성한다.

[0115] 상기 관련 액터 모듈(relevant actors module)(380)은 하나 이상의 액터-세트들(예를 들어, 상기 관리 도메인 상태(320) 내에서 열거 형태로된 상기 관리 서버들(130) 및 상기 UDGs) 및 규칙들의 세트(예를 들어, 관리 정책 관점)를 입력으로 받아들이고, 어떤 액터-세트들이 해당 규칙들과 관련되는지 결정하고, 해당 액터-세트들만을 출력한다. 이것은 상기 관련 액터 모듈(380)이 상기 액터-세트들을 검토하고, 상기 주어진 규칙들의 세트를 위한 상기 관련 액터-세트들만을 추출함에 따른 필터링 프로세스이다. 상기 관련 액터 모듈(380)은 모든 입력 액터-세트들을 반복하고, 임의의 규칙의 PB 포션들 또는 UB 포션들에 의해 특정 액터-세트가 참조되었는지 여부를 결정하기 위한 상기 입력 규칙들의 PB 포션들 및 UB 포션들을 분석함으로써 상기 필터링을 수행한다. 상기 최종 결과("액터 관점(actor perspective)"이라고 하는)는 액터-세트들의 모임이다. 상기 액터 관점은 상기 관리 명령들의 부분으로서 관리 서버(130)로 나중에 전송된다.

[0116] 일 실시예에서, 상기 관련 액터 모듈(380)은 "액터-세트 필터(actor-set filter)"를 생성하기 위한 상기 입력 규칙들의 세트를 사용한다. 상기 액터-세트 필터는 상기 입력 액 선택한다.

[0117] 상기 정책 엔진 모듈(340)은 관리 서버들(130)을 위한관리 명령들을 생성하고, 상기 생성된 관리 명령들을 상기 서버들로 전송한다. 상기 정책 엔진 모듈(340)은 a) 상기 관리 도메인의 컴퓨터 네트워크 인프라의 상태(320) 및 b) 상기 관리 도메인-전역 관리 정책(330)에 기반하여 상기 관리 명령들(상기 관련 규칙 모듈(350), 상기 기능-레벨 명령 생성 모듈(360), 상기 액터 열거 모듈(370), 및 상기 관련 액터 모듈(380)을 사용하는)을 생성한다.

[0118] 예를 들어, 상기 정책 엔진 모듈(340)은 상기 관리 도메인-전역 관리 정책(330) 입력 및 상기 특정 관리 서버(130)의 UID를 제공하는 상기 관련 규칙 모듈(350)을 실행한다. 상기 관련 규칙 모듈(350)은 해당 서버("관리 정택 관점")와 관련된 규칙의 세트를 출력한다. 상기 정책 엔진 모듈(340)은 상기 관리 도메인 상태(320) 입력을 제공하는 상기 액터 열거 모듈(370)을 실행한다. 상기 액터 열거 모듈(370)은 상기 관리 도메인 상태(320) 내에서 열거된 형태("액터-세트들(actor-sets)")로 상기 관리 서버들(130) 및 비관리 장치 그룹들(UDGs: unmanaged device groups)의 디스크립션들의 표시를 출력한다. 상기 정책 엔진 모듈(340)은 상기 관리 정책 관점 입력(상기 관련 규칙 모듈(350)에 의한 출력하는)을 제공하는 상기 기능-레벨 명령 생성 모듈(360)을 실행한다. 상기 기능-레벨 명령 생성 모듈(360)은 기능-레벨 명령들을 출력한다. 상기 정책 엔진 모듈(340)은 상기 액터-세트들 입력(상기 열거 모듈(370)에 의한 출력) 및 상기 관리 정책 관점(상기 관련 규칙 모듈(350)에 의한)을 제공하는 상기 관련 액터 모듈(380) 실행한다. 상기 관련 액터 모듈(380)은 해당 규칙들과 관련된 해당 액터-세트들("관련 액터-세트들(relevant actor-sets)")만을 출력한다. 상기 정책 엔진 모듈(340)은 기능-레벨 명령들(상기 기능-레벨 명령 생성 모듈(360)에 의한 출력) 및 상기 관련 액터-세트들(상기 관련 액터 모듈(380)에 의한 출력)을 상기 특정 관리 서버(130)로 전송한다.

[0119] 일 실시예에서, 상기 정책 엔진 모듈(340)은 상기 프로세스 동안 생성된 정보를 캐시(caches)한다. 예를 들어, 상기 특정 관리 서버(130)와 관련된 상기 정책 관리 모듈(340)은 상기 관리 정책 관점, 상기 기능-레벨 명령들, 상기 액터-세트 필터, 및/또는 상기 관련 액터-세트들을 캐시한다. 또 다른 예로서, 상기 정책 엔진 모듈(340)은 상기 액터-세트들(특정 관리 서버(130)에 대하여 명시하지 않은)을 캐시한다.

[0120] 관리 도메인의 액터-세트들인 상기 관리 도메인 상태(320)에 기반하기 때문에, 상기 관리 도메인 상태(320)에 대한 변경은 상기 관리 도메인의 액터-세트들에 대한 변경을 요구할 수 있다. 유사하게, 관리 서버의 관리 명령들은 상기 관리 도메인 상태(320) 및 상기 관리 도메인-전역 관리 정책(330)에 기반하기 때문에, 상기 관리 도메인 상태(320)에 대한 변경 및/또는 상기 관리 도메인-전역 관리 정책(330)은 상기 관리 서버의 관리 명령들에 대한 변경을 요구할 수 있다. 일 실시예에서, 상기 정책 엔진 모듈(340)은 관리 도메인의 액터-세트들을 업데이트할 수 있고, 관리 서버의 관리 명령들을 업데이트할 수 있고, 그러면 관리 서버들(130)에 대한 변경을 (필요한 경우) 배포할 수 있다. 상술된 상기 캐시된 정보는 상기 정책 엔진 모듈(340)이 상기 관리 도메인의 액터-세트들 및/도는 상기 관리 서버의 관리 명령들을 더 효율적으로 업데이트하고 상기 변경들을 배포하도록 돕는다.

[0121] 일 실시예에서, 상기 정책 엔진 모듈(340)은 관리 도메인의 액터-세트들을 업데이트(상기 관리 도메인 상태(320)에 기반하여)하고, 상기 관리 서버들(130)에 대한 변경들을 아래와 같이 배포한다: 상기 정책 엔진 모듈(340)은 상기 캐시된 액터-세트들 입력(상기 액터 열거 모듈에 의한 이전 출력) 및 상기 관리 도메인 상태(320)의 변경된 포션(예를 들어, 상기 변경된 서버 디스크립션)을 제공하는 상기 액터 열거 모듈(370)을 실행한다. 상기 액터 열거 모듈(370)은 상기 업데이트된 액터-세트들 출력한다. 일 실시예에서, 상기 정책 엔진 모듈(340)은 상기 관리 도메인(150) 내에서 모든 관리 서버들(130)로 모든 업데이트된 액터-세트들을 나중에 전송한다.

하지만, 이러한 실시예는 모든 관리 서버가 모든 액터-세트들에 대한 변경에 의한 영향을 받는지 않기 때문에 비효율적이다.

[0122] 또 다른 실시예에서, 선택된 액터-세트만이 선택된 서버들로 전송된다. 예를 들어, 특정 관리 서버는 해당 액터-세트들 a) 해당 서버로 이전에 전송된 b) 변경을 갖는 해당 액터-세트들만 전송된다. 상기 캐시된 관련 액터-세트들은 어떤 액터-세트들이 해당 서버로 이전에 전송되었는지 나타낸다(위 (a)를 참조). 상기 정책 엔진 모듈(340)은 어떤 액터-세트들이 변경된 것인지 결정하기 위해 상기 캐시된 액터-세트들을 상기 업데이트된 액터-세트들과 비교한다(위 (b)를 참조). 그러면 상기 정책 엔진 모듈(340)은 상기 (a) 및 (b)의 명령을 평가한다. 해당 명령에서 액터-세트들은 상기 특정 관리 서버로 전송될 수 있다. 일 실시예에서, 더 큰 효율성을 위해 액터-세트들은 "diff" 포맷(format)로 전송될 수 있다. 예를 들어, 상기 diff 포맷은 액터-세트 식별자(actor-set identifier), 액터 식별자(actor identifier)(예를 들어, 관리 서버 UID 또는 UDG UID), 및 해당 액터가 추가, 제거, 또는 수정되었는지 여부의 명령을 명시한다.

[0123] 또 다른 실시예에서, 두 개의 테이블들이 효율을 개선하기 위해 관리되고 사용된다. 제1 테이블은 관리 서버(130)와 해당 관리 서버가 멤버인 액터-세트들을 연관 짓는다. 제2 테이블은 관리 서버(130)를 해당 관리 서버와 관련된 액터-세트들(예를 들어, 상기 관련 액터 모듈(380)에 의해 결정된)과 연관 짓는다. 이러한 테이블들에서, 관리 서버(130)는 예를 들어, 해당 관리 서버의 UID에 의해 나타내어지고, 액터-세트는 예를 들어, 해당 액터-세트의 UID에 의해 나타내어진다. 상기 정책 엔진 모듈(340)은 어떤 관리 서버의 디스크립션이 변경되었는지 결정하기 위해 상기 관리 도메인 상태(320)의 변경된 포션(다시 말해, 상기 변경된 서버 디스크립션)을 사용한다. 상기 정책 엔진 모듈(340)은 어떤 액터-세트들이 해당 관리 서버가 멤버인지 결정하기 위해 상기 제1 테이블을 사용한다. 이러한 액터-세트는 변경된 서버 디스크립션의 결과로서 변경할 수 있다. 그리고, 상기 정책 엔진 모듈(340)은 어떤 관리 서버가 해당 액터-세트들과 관련있는지를 결정하기 위해 상기 제2 테이블을 사용한다. 상기 정책 엔진 모듈(340)은 해당 관리 서버들만을 위해 위에서 설명된 상기 명령 산출을 수행한다.

[0124] 일 실시예에서, 상기 정책 엔진 모듈(340)은 관리 서버의 관리 명령을 업데이트하고(상기 관리 도메인 상태(320)에 대한 변경에 기반하여), 상기 업데이트된 관리 명령들을 다음과 같은 상기 관리 서버로 전송한다: 상기 정책 엔진 모듈(340)은 상기 관리 도메인-전역 관리 정책(330) 입력 및 상기 관리 서버(130)의 UID를 제공하는 상기 관련 규칙 모듈(350)을 실행한다. 상기 관련 규칙 모듈(350)은 해당 서버와 관련된("관리 정책 관점") 규칙의 세트를 출력한다. 상기 정책 엔진 모듈(340)은 그것들의 상이함의 여부를 결정하기 위해 상기 캐시된 관리 정책 관점으로만 출력하는 상기 관리 정책 관점을 비교한다. 상기 단지 출력하는 관리 정책 관점(just-output management policy perspective)과 상기 캐시된 관리 정책 관점(cached management policy perspective)이 동일할 경우, 그러면 상기 정책 엔진 모듈(340)은 추가적인 조치(action)를 취하지 않는다. 이러한 상황에서, 상기 이전에 생성된 관리 서버의 관리 명령들(특히, 상기 기능-레벨 명령들 및 관련 액터-세트들)은 상기 관리 도메인 상태(320)에 대한 변경과 일치하고, 재생성 되고 상기 관리 서버로 재전송되는 것은 필요로 하지 않는다.

[0125] 상기 단지-출력하는 관리 정책 관점과 캐시된 관리 정책 관점이 상이한 경우, 그러면 상기 정책 엔진 모듈(340)은 어떤 규칙들이 상기 캐시된 관점에 추가되고, 어떤 규칙들이 상기 캐시된 관점으로부터 제거되어야 하는지 결정한다. 상기 정책 엔진 모듈(340)은 추가하기 위한 상기 규칙들 및 제거하기 위한 상기 규칙들을 입력으로 제공하는 상기 기능-레벨 명령 생성 모듈(360)을 실행한다. 상기 기능-레벨 명령 생성 모듈(360)은 추가하기 위한 기능-레벨 명령들 및 제거하기 위한 기능-레벨 명령들(상기 관리 서버로 이전에 전송된 상기 캐시된 기능-레벨 명령들에 관하여)을 출력한다. 상기 정책 엔진 모듈(340)은 상기 다양한 기능-레벨 명령들을 적절하게 추가 또는 제거하기 위해 상기 관리 서버를 지시한다. 일 실시예에서, 더 좋은 효율성을 위해, 기능-레벨 명령들은 "diff" 포맷으로 전송된다. 예를 들어, 상기 diff 포맷은 기능-레벨 명령 식별자 및 기능-레벨 명령이 상기 이전에 전송된 기능-레벨 명령들로부터 추가 또는 제거되어야 하는지 여부의 표시를 명시한다.

[0126] 상기 정책 엔진 모듈(340)은 또한 상기 캐시된 액터-세트들 및 상기 관리 도메인 상태(320)의 캐시된 포션(다시 말해, 상기 캐시된 서버 디스크립션)을 입력으로 제공하는 상기 액터 열거 모듈(370)을 실행한다. 상기 액터 열거 모듈(370)은 상기 업데이트된 액터-세트들을 출력한다. 상기 정책 엔진 모듈(340)은 상기 업데이트된 액터-세트들 및 단지-출력하는 관리 정책 관점을 입력으로 제공하는 상기 관련 액터 모듈(380)을 실행한다. 상기 관련 액터 모듈(380)은 해당 규칙들과 관련된 이러한 업데이트된 액터-세트들("업데이트된 관련 액터-세트들(updated relevant actor-sets)")만을 출력한다.

[0127] 상기 정책 엔진 모듈(340)은 그것들의 상이함의 여부를 결정하기 위해 상기 업데이트된 관련 액터-세트들을 상기 캐시된 관련 액터-세트들과 비교한다. 상기 업데이트된 관련 액터-세트들 및 상기 캐시된 관련 액터-세트들

이 동일할 경우, 그러면 상기 정책 엔진 모듈(340)은 상기 관리 서버로 액터-세트들을 전송하지 않는다. 이러한 상환에서, 상기 이전에 생성된 관련 액터-세트들은 상기 관리 도메인 상태(320)에 대한 변경과 일치하고, 상기 관리 서버로 재전송(re-sent)되는 것을 필요로 하지 않는다. 상기 업데이트된 관련 액터-세트들 및 상기 캐시된 관련 액터-세트들이 상이할 경우, 그러면 상기 정책 엔진 모듈(340)은 어떤 액터-세트들이 상기 캐시된 관련 액터-세트들에 추가, 제거, 또는 수정되어야 하는지 결정한다. 상기 정책 엔진 모듈(340)은 상기 다양한 액터-세트들을 적절하게 추가, 제거, 수정하도록 상기 관리 서버를 지시한다. 일 실시예에서, 더 좋은 효율성을 위해, 액터-세트들은 "diff" 포맷으로 전송된다. 예를 들어, 상기 diff 포맷은 액터-세트 식별자 및 해당 액터-세트가 상기 이전에 전송된 액터-세트들에 관련하여 추가, 제거, 또는 수정되어야 하지는 여부의 표시를 명시한다.

[0128] 상기 정책 엔진 모듈(340)은 관리 서버의 관리 명령들을 업데이트하고(상기 관리 도메인-전역 관리 정책(330)에 대한 변경에 기반하여), 상기 업데이트된 관리 명령들을 상기 관리 서버로 전송할 수 있다는 것을 상기한다. 상기 관리 정책(330)에 대한 변경은 예를 들어, 상기 규칙 또는 규칙 세트의 추가, 제거, 또는 수정이다. 일 실시예에서, 상기 관리 정책(330)에 대한 변경은 GUI 또는 API를 통해 상기 글로벌 매니저(120)을 갖는 명령에 의해 생성된다. 또 다른 실시예에서, 상기 관리 정책(330)에 대한 변경은 상기 글로벌 매니저(120) 내에서 자동화된 프로세스에 의해 생성된다(예를 들어, 상기 글로벌 매니저에 의해 감지된 보안 위협에 반응하여). 상기 정책 엔진 모듈(340)은 상기 관리 서버의 관리 명령들을 업데이트하고, 상기 업데이트된 관리 명령들을 상기 관리 정책(330)에 대한 변경 또는 상기 관리 도메인 상태(320)에 대한 변경이 있는지 여부에 관계없이 유사한 방법으로 상기 관리 서버로 전송한다. 하지만, 몇몇 차이점이 있다.

[0129] 상기 관리 정책(330)에 대한 변경의 경우에서, 상기 정책 엔진 모듈(340)은 모든 관리 서버들(130)에 대한 관리 명령들의 업데이트를 필요로 하지 않는다. 대신에, 상기 정책 엔진 모듈(340)은 상기 이전 관리 정책(330)과 관련하여 어떤 규칙들이 추가, 제거, 또는 수정되어야 하는지 결정하기 위해 상기 이전 관리 정책(330)을 상기 새로운 관리 정책(330)과 비교한다. 상기 정책 엔진 모듈(340)은 어떤 관리 서버들(130)이 상기 변경된 규칙들에 의해 영향을 받는지 결정한다(예를 들어, 어떤 관리 서버들은 다음에 의해 커버된다 a) 상기 규칙들의 및/도는 범위들의 PB 및/또는 UB 포션들 및 b) 상기 규칙들의 조건 포션들(임의의 경우)). 상기 정책 엔진 모듈(340)은 상기 변경된 규칙들(상기 전체 새로운 관리 정책(330) 대신에) 및 상기 관리 서버(130)의 UID(상기 변경된 규칙들에 의해 영향을 받는 해당 서버들만을 위해)를 입력으로 제공하는 상기 관련 규칙 모듈(350)을 실행한다.

[0130] 상기 관리 도메인 상태 업데이트(ADSU: administrative domain state update) 모듈(385)은 상기 관리 도메인 상태(320)에 대한 변경들을 수신하고, 해당 변경들을 처리한다. 상기 관리 도메인 상태(320)에 대한 변경은 예를 들어, 상기 관리 서버(130)의 디스크립션(상기 관리 서버의 레이블 세트 또는 구성된 특징들의 수정을 포함하는) 또는 비관리 장치 또는 비관리 장치 그룹의 디스크립션의 추가, 제거, 또는 수정이다. 일 실시예에서, 상기 관리 도메인 상태(320)에 대한 변경은 특정 관리 서버(130)로부터 수신된 로컬 상태 정보(local state information)로 조직화한다. 또 다른 일 실시예에서, 상기 관리 도메인 상태(320)에 대한 변경은 GUI 또는 API를 통해 상기 글로벌 매니저(120)와의 상호작용에 의해 생성된다. 또 다른 일 실시예에서, 상기 관리 도메인 상태(320)에 대한 변경은 상기 글로벌 매니저(120) 내에서 자동화 프로세스에 의해 생성된다(예를 들어, 상기 글로벌 매니저에 의해 감지된 보안 위협에 반응하여).

[0131] 예를 들어, 상기 ADSU 모듈(385)은 특정 관리 서버(130)와 관련하여 변경을 수신한다. 상기 ADSU 모듈(385)은 상기 특정 관리 서버(130)의 디스크립션의 부분으로서 상기 관리 도메인 상태(320)에서 새로운 정보를 저장한다. 그러면 상기 ADSU 모듈(385)은 상기 서버와 관련하여 추가적 정보를 결정하기 위해 해당 관리 서버의 디스크립션을 (선택적으로)분석하고, 해당 정보를 상기 디스크립션에 저장한다. 그러면 상기 ADSU 모듈(385)은 상기 관리 서버의 디스크립션에 대한 변경에 기반하여 상기 관리 도메인의 액터-세트들 및/또는 상기 관리 서버의 관리 명령들의 업데이트 여부를 결정한다. 상기 ADSU 모듈(385)은 상기 관리 도메인의 액터-세트들을 업데이트하기 위해 결정하고, 상기 ADSU 모듈(385)은 상기 관리 도메인의 액터-세트들을 업데이트하도록 상기 정책 엔진 모듈(340)을 지시한다. 일 실시예에서, 상기 ADSU 모듈(385)은 상기 관리 도메인의 액터-세트들을 업데이트하도록 상기 정책 엔진 모듈(340)을 지시하기 전에 이벤트가 발생할 때까지 대기한다. 상기 ADSU 모듈(385)이 상기 관리 서버의 관리 명령들을 업데이트하도록 결정하는 경우, 상기 ADSU 모듈(385)은 상기 관리 서버의 관리 명령들을 업데이트하도록 상기 정책 엔진 모듈(340)을 지시한다. 일 실시예에서, 상기 ADSU 모듈(385)은 상기 관리 서버의 관리 명령들을 업데이트하도록 상기 정책 엔진 모듈(340)을 지시하기 전에 이벤트가 발생할 때까지 대기한다. 상술된 이벤트들은 예를 들어, 사용자 명령의 수신(receipt of a user command) 또는 특정 유지 윈도우의 발생(occurrence of a specified maintenance window)일 수 있다.

[0132] 상기 ADSU 모듈(385)이 상기 관리 서버의 디스크립션에 대한 변경의 유형에 의존하여 상기 관리 도메인의 액터-

세트들 및/또는 상기 관리 서버의 관리 명령들의 업데이트 할지 여부를 결정한다. 일 실시예에서, 상기 ADSU 모듈(385)은 표 2에 보여진 것과 같은 결정을 형성한다.

변경의 유형(Type of Change)	업데이트 여부(Whether to Update)
온라인에서 오프라인(Online to offline)	관리 도메인의 액터-세트들(Administrative domain's actor-sets): Yes 관리 서버의 관리 명령들(Managed server's management instructions): No
오프라인에서 온라인(Offline to online)	관리 도메인의 액터-세트들(Administrative domain's actor-sets): Yes 관리 서버의 관리 명령들(Managed server's management instructions): Yes
레이블 세트(Label set)	관리 도메인의 액터-세트들(Administrative domain's actor-sets): Yes 관리 서버의 관리 명령들(Managed server's management instructions): Yes
구성된 특성(Configured characteristic)	관리 도메인의 액터-세트들(Administrative domain's actor-sets): No 관리 서버의 관리 명령들(Managed server's management instructions): Yes
네트워크 노출 정보(Network exposure info)	관리 도메인의 액터-세트들(Administrative domain's actor-sets): Yes 관리 서버의 관리 명령들(Managed server's management instructions): Yes(IP 주소만 변경되지 않는 한)
서비스 정보(Service info)	관리 도메인의 액터-세트들(Administrative domain's actor-sets): No 관리 서버의 관리 명령들(Managed server's management instructions): Yes (특정 상황들(specified situations)에서만)

[0133]

[0134] <표 2> 서버 디스크립션 변경의 유형에 기반한 관리 도메인의 액터-세트들 및/또는 관리 서버의 관리 명령들의 업데이트 여부

[0135] 일 실시예에서, 상기 ADSU 모듈(385)은 상기 레이블/구성된 특성 엔진을 실행하고, 상기 서버의 디스크립션 입력을 제공함으로써 상기 서버와 관련하여 추가 정보를 결정한다. 상기 레이블/CC 엔진은 상기 서버의 디스크립션 및 레이블/CC 할당 규칙들에 기반하여 상기 서버를 위한 레이블들/CC 값들을 산출한다.

[0136] 또 다른 실시예에서, 상기 ADSU 모듈(385)은 상기 관리 서버가 NAT(network address translator)를 뒤에 있는지 여부(그리고, 그것이 NAT 뒤에 있는 경우, NAT – 1:1 또는 1:N 중 어떤 유형인지)를 결정한다. 예를 들어, 상기 ADSU 모듈(385)은 NAT가 상기 글로벌 매니저(120) 및 상기 관리 서버(130) 사이에 존재하는지 여부를 비교함으로써 결정한다 (a) 상기 글로벌 매니저 및 상기 서버 사이의 TCP 연결에 따른 상기 서버의 IP 주소 (b) 상기 서버로부터 수신된 로컬 상태 정보에 따른 상기 서버의 IP 주소. (a) 및 (b)가 상이할 경우, 그러면 NAT는 상기 글로벌 매니저(120) 및 상기 관리 서버(130) 사이에 존재한다. NAT가 존재하지 않을 경우, 그러면 상기 ADSU 모듈(385)은 데이터 센터 결정(data center detection)을 수행함으로써 상기 NAT의 유형(1:1 또는 1:N)을 결정한다. 예를 들어, 상기 ADSU 모듈(385)은 상기 데이터 센터의 공식 IP 주소(data center's public IP

address)에 의한 상기 서버의 데이터 센터(server's data center)를 식별한다. (그러지 않으면, 상기 관리 서버는 상기 내부 데이터 센터(inside the data center)가 아닌 상기 서버의 외부(external to the serve) 정보를 질의함으로써 데이터 센터 결정을 수행한다. 그러면, 상기 서버는 상기 로컬 상태들의 부분으로서 상기 글로벌 매니저로 정보를 전송한다.) 구성 정보는 어떤 유형의 NAT가 어떤 데이터 센터들에 의해 사용되었는지 나타낸다. 특정 데이터 센터와 관련하여 NAT 정보가 없는 경우, 그러면 상기 ADSU 모듈(385)은 상기 NAT 유형이 1:N인 것으로 가정한다.

[0137] 도 4는 일 실시예에 따른 관리 서버(managed server)(130)의 정책 구현 모듈(policy implementation module)(136)의 상세도를 나타내는 하이-레벨 블록 다이어그램이다. 상기 정책 구현 모듈(136)은 로컬 상태 저장부(local state repository)(400), 정책 컴필레이션 모듈(policy compilation module)(410), 및 로컬 상태 업데이트 모듈(local state update module)(420)을 포함한다. 상기 로컬 상태 저장부(400)는 상기 관리 서버(130)의 로컬 상태와 관련된 정보를 저장한다. 일 실시예에서, 상기 로컬 상태 저장부(400)는 상기 관리 서버의 OS(operating system), 네트워크 노출, 및 서비스들과 관련된 정보를 저장한다. OS 정보는 예를 들어, 어떤 OS가 동작하고 있는지의 표시를 포함한다. 네트워크 노출 정보 및 서비스 정보는 상기 관리 도메인 상태(320) 내에서 관리 서버(130)의 디스크립션관 관련하여 상술되었다.

[0138] 상기 정책 컴필레이션 모듈(410)은 관리 명령들 및 관리 서버(130)의 상태를 입력으로 받아들이고, 관리 모듈 구성(management module configuration)(134)을 생성한다. 예를 들어, 상기 관리 명령들은 상기 글로벌 매니저(120)로부터 수신되고, 기능-레벨 명령들(상기 기능-레벨 명령 생성 모듈(360)에 의해 생성된) 및 관련 액터-세트들(상기 관련 액터 모듈(380)에 의한 출력)을 포함한다. 상기 관리 서버(130)의 상태는 상기 로컬 상태 저장부(local state repository)(400)로부터 검색된다. 일 실시예에서, 상기 정책 컴필레이션 모듈(410)의 실행은 a) 상기 관리 서버를 파워 업 함으로써 또는 온라인 상태로 되게 함으로써(coming online), b) 상기 관리 서버가 기능-레벨 명령들을 수신함으로써, 및/또는 c) 상기 로컬 상태 저장부(400)의 콘텐츠(contents)를 변경함으로써 트리거 된다.

[0139] 상기 정책 컴필레이션 모듈(410)은 상기 기능-레벨 명령들 및 관련 액터-세트들을 관리 모듈 구성(134)으로 연결(maps)한다. 예를 들어, 상기 정책 컴필레이션 모듈(410)은 액세스 제어 기능-레벨 명령(access control function-level instruction)(어떤 것이 포트(port) 및 액터-세트 참조(actor-set reference)를 포함하는지)을 리눅스 운영체제(Linux operating system)에서 ip테이블 엔트리(iptables entry) 및 ip세트 엔트리(ipset entry) 또는 윈도우 운영체제(Windows operating system)에서 WFP(Windows Filtering Platform) 규칙(rule)으로 연결한다.

[0140] 상기 관리 서버(130)에서 관리 정책의 어플리케이션은 해당 서버의 로컬 상태에 의해 영향을 받을 수 있다. 일 실시예에서, 상기 정책 컴필레이션 모듈(410)은 수신된 기능-레벨 명령과 관련된 조건을 평가하고, 상기 평가의 결과에 기반하여 상기 관리 모듈 구성(134)을 생성한다. 예를 들어, 상기 정책 컴필레이션 모듈(410)은 상기 관리 서버의 피어(managed server's peer)의 운영체제를 참조하는 조건을 평가하고(다시 말해, 상기 관계에서 다른 액터(other actor in the relationship)), 상기 평가의 결과에 기반하여 기능 프로파일 속성들(function profile attributes)을 선택하고, 상기 선택된 기능 프로파일 속성은 상기 관리 모듈 구성(134)에서 표현된다.

[0141] 또 다른 예로서, 관리 서버(130)가 해당 서버와 관련성이 없는 것으로 판단된 기능-레벨 명령을 수신할 수 있다는 것을 상기한다. 예를 들어, 상기 규칙은 상기 관리 서버의 로컬 상태를 명시하는 포션을 포함한다(예를 들어, 상기 제공된 서비스를 설명하는 서비스 포션). 상기 글로벌 매니저(120)는 상기 관리 서버의 로컬 상태를 알지 못하기 때문에(예를 들어, 상기 관리 서버가 실제로 서비스를 제공하는지 여부), 상기 생성된 기능-레벨 명령은 상기 관리 서버로 전송된다. 상기 정책 컴필레이션 모듈(410)은 상기 관리 서버의 로컬 상태를 체크한다(예를 들어, 상기 관리 서버가 서비스를 결정하는지 여부를 결정). 이러한 결정은 상기 관리 서버의 로컬 상태를 참조하는 조건을 평가하게 된다. 상기 정책 컴필레이션 모듈(410)은 상기 기능-레벨 명령에 따라 처리한다. 상기 정책 컴필레이션 모듈(410)이 상기 조건이 "참"으로 평가한 것을 결정할 경우(예를 들어, 상기 관리 서버가 서비스를 제공하고 있음), 그러면 상기 정책 컴필레이션 모듈(410)은 상기 관리 모듈 구성(134)으로 해당 기능-레벨 명령을 포함한다. 특히, 상기 정책 컴필레이션 모듈(410)은 상기 관련 조건(상기 해당 서버의 로컬 상태에 영향을 미치는)을 평가한 후에만 상기 관리 모듈 구성(134)으로 기능-레벨 명령들을 포함한다. 상기 조건의 평가가 거짓일 경우, 그러면 상기 정책 컴필레이션 모듈(410)은 상기 관리 모듈 구성(134)에서 상기 기능-레벨 명령들을 나타내지 않는다. 상기 특정 조건들(예를 들어, 그것의 자연 및 특정 값들)은 확장 가능하다. 일 실시예에서, 상기 조건들은 상기 "서비스"의 정의와 관련되고 프로세스 정보 및/또는 패키지 정보(상기 관리 도

메인 상태(320) 내에서 관리 서버(130)의 디스크립션에 관하여 상술된)를 포함한다.

[0142] 예를 들어, 기능-레벨 명령이 포트(80) 상에서 상기 아파치 서비스 인바운드(Apache service inbound)에만 액세스를 허용하는 것을 상기한다(예를 들어, 상기 관리 서버(130)는 "제공자" 또는 최종포인트(endpoint)이다). 상기 관리 서버(130)는 포트(80) 상에서 수신하고 있는 어플리케이션이 실제로 아파치(Apache)인지 아니면 어떤 다른 어플리케이션(로그(rogue) 또는 다른)인지 여부에 영향을 미치는 상기 관련 조건을 평가한 후에만 포트(80) 상에서 액세스를 허용하기 위해 상기 관리 모듈 구성(134)에서 이러한 기능-레벨 명령을 나타낸다. 상기 관리 서버(130)는 상기 관련 조건이 "참"으로 평가한 것을 결정한 후에만 상기 관리 모듈 구성(134)에서 이러한 기능-레벨 명령을 나타낸다. 상기 관련 조건이 "거짓"으로 평가한 경우, 그러면 상기 관리 서버(130)는 상기 관리 모듈 구성(134)에서 이러한 기능-레벨 명령을 나타내지 않는다. 그 결과, 상기 네트워크 트래픽은 차단된다.

[0143] 일 실시예에서, 관리 서버(130)은 그것의 아웃바운드 연결들(outbound connections)을 모니터 한다. 상기 관리 서버(130)는 해당 테이블에서 어떤 프로세스들이 해당 아웃바운드 연결들을 실행하고 있는지 결정하기 위해 아웃바운드 네트워크 트래픽(outbound network traffic)을 그것의 내부 프로세스 테이블(internal process table)과 비교한다. 상기 관리 서버(130)는 아웃바운드 연결을 설정하기 위해 특정 프로세스들(상술된 주어진 요구사항들의 세트)만을 허용하는 규칙을 실행할 수 있다.

[0144] 일 실시예에서(도시되지 않은), 상기 정책 컴필레이션 모듈(410)은 상기 관리 서버(130) 대신에 상기 글로벌 매니저(120)에 위치될 수 있다. 이러한 실시예에서, 상기 글로벌 매니저(120)는 상기 관리 서버(130)로 관리 명령들을 전송하지 않는다. 대신에, 상기 관리 서버(130)가 그것의 로컬 상태를 상기 글로벌 매니저(120)로 전송한다. 상기 정책 컴필레이션 모듈(410)이 상기 관리 모듈 구성(134)을 생성한 후에(상기 글로벌 매니저(120)에서), 상기 관리 모듈 구성(134)은 상기 글로벌 매니저(120)로부터 상기 관리 서버(130)로 전송된다.

[0145] 상기 로컬 상태 업데이트(LSU: local state update) 모듈(420)은 상기 관리 서버(130)의 로컬 상태를 모니터하고, 로컬 상태 정보를 상기 글로벌 매니저(120)로 전송한다. 일 실시예에서, 상기 LSU 모듈(420)은 상기 관리 서버(130)의 초기 로컬 상태(initial local state)를 결정하고, 상기 로컬 상태 저장부(400)에서 적절한 로컬 상태 정보를 저장하고, 로컬 상태 정보를 상기 글로벌 매니저(120)로 전송한다. 상기 LSU 모듈(420)은 상기 서버의 운영체제(OS) 및/또는 파일 시스템의 다양한 부분들을 점검함으로써 상기 관리 서버(130)의 로컬 상태를 결정한다. 예를 들어, 상기 LSU 모듈(420)은 상기 OS의 커널 테이블들(OS' kernel tables)(네트워킹 정보), 상기 OS의 시스템 테이블들(OS' system tables)(패키지 정보), 및 상기 파일 시스템(file system)(파일들 및 해시 값들)으로부터 서비스 정보를 획득한다. 상기 LSU 모듈(420)은 상기 OS의 커널(OS' kernel) 및/또는 OS-레벨 데이터 구조들로부터 네트워크 노출 정보를 획득한다.

[0146] 상기 LSU 모듈(420)이 상기 초기 로컬 상태 정보를 상기 글로벌 매니저(120)로 전송한 후에, 상기 LSU 모듈은 상기 로컬 상태에 대한 변경들을 모니터 한다. 상기 LSU 모듈은 예를 들어, 폴링(polling)(예를 들어, 주기적인 점검을 수행함으로써), 또는 수신(listening)(예를 들어, 이벤트 스트림을 수신함으로써(subscribing))함으로써 변경들을 모니터 한다. 상기 LUS 모듈(420)은 최근-획득된 로컬 상태 정보를 상기 로컬 상태 저장부(400)에 이전에 저장된 정보(information already stored)와 비교한다. 상기 정보가 매치하는 경우, 그러면 상기 LSU 모듈(420)은 더 이상 조치를 취하지 않는다(로컬 상태 정보가 다시 획득될 때까지). 상기 정보가 다를 경우, 그러면 상기 LSU 모듈(420)은 상기 최근-획득된 정보를 상기 로컬 상태 저장부(400)에 저장하고, 상기 관리 모듈 구성(134)을 재생성하기 위해 상기 정책 컴필레이션 모듈(410)을 실행하고, 상기 글로벌 매니저(120)의 변경을 알린다. 일 실시예에서, 상기 LSU 모듈(420)은 로컬 상태 정보에 대한 변경들을 "diff" 포맷으로 상기 글로벌 매니저(120)로 전송한다. 예를 들어, 상기 diff 포맷은 로컬 상태 정보의 유형(예를 들어, 운영체제) 및 해당 정보 유형을 위한 새로운 값을 명시한다. 또 다른 실시예에서, 상기 LSU 모듈(420)은 상기 로컬 상태 저장부(400)의 전체 콘텐츠(entire contents)를 상기 글로벌 매니저(120)로 전송한다.

[0147] 도 5는 일 실시예에 따른 특정 관리 서버(130)를 위해 관리 명령들을 생성하는 방법(500)을 나타내는 흐름도이다. 다른 실시예들이 다른 방법으로 상기 방법들을 수행할 수 있고, 다른 및/또는 추가적인 방법들을 포함할 수 있다. 추가적으로, 어떤 또는 모든 방법들이 도 1에 도시된 이외의 다른 개체에 의해 수행될 수 있다. 일 실시예에서, 상기 방법(500)은 여러 번 실행될 수 있다(예를 들어, 관리 도메인(150)에서 각 관리 서버(130)에 대하여 한번씩).

[0148] 상기 방법(500)이 시작할 때, 상기 관리 도메인의 컴퓨터 네트워크 인프라 상태(320) 및 관리 도메인-전역 관리 정책(330)이 상기 글로벌 매니저(120)의 상기 저장부(300)에 미리 저장될 수 있다. 이러한 포인트에서, 상기 방법(500)이 시작한다.

[0149] 단계(510)에서, 상기 관리 도메인 상태(320) 및 상기 관리 도메인-전역 관리 정책(330)은 액세스된다. 예를 들어, 상기 정책 엔진 모듈(340)은 상기 저장부(330)로 요청을 전송하고, 응답으로 상기 관리 도메인 상태(320) 및 상기 관리 도메인-전역 관리 정책(330)을 수신한다.

[0150] 단계(520)에서, 하나이상의 관련 규칙들이 결정된다. 예를 들어, 상기 정책 엔진 모듈(340)은 상기 관리 도메인-전역 관리 정책(330) 입력 및 상기 특정 관리 서버(130)의 UID를 제공하는 상기 관련 규칙 모듈(350)을 실행한다. 상기 관련 규칙 모듈(350)은 해당 서버와 관련된 규칙들의 세트를 출력한다(관리 정책 관점).

[0151] 단계(530)에서, 액터들은 열거된다. 예를 들어, 상기 정책 엔진 모듈(340)은 관리 도메인 상태(320) 입력을 제공하는 상기 액터 열거 모듈(370)을 실행한다. 상기 액터 열거 모듈(370)은 상기 관리 도메인 상태(320) 내에서 열거된 형태(액터-세트들)로 상기 관리 서버들(130)의 표시 및 열거된 장치 그룹들(UDGs)을 생성한다.

[0152] 단계(540)에서, 하나이상의 기능-레벨 명령들이 생성된다. 예를 들어, 상기 정책 엔진 모듈(340)이 상기 관리 정책 관점 입력(단계(520)에서 생성된)을 제공하는 상기 기능-레벨 명령 생성 모듈(360)을 실행한다. 상기 기능-레벨 명령 생성 모듈(360)은 기능-레벨 명령들을 생성한다.

[0153] 단계(550)에서, 하나이상의 관련 액터들이 결정된다. 예를 들어, 상기 정책 엔진 모듈(340)은 상기 액터-세트들 입력(단계(530)에서 생성된) 및 관리 정책 관점(단계(520)에서 생성된)을 제공하는 상기 관련 액터 모듈(380)을 실행한다. 상기 관련 액터 모듈(380)은 해당 규칙들과 관련된 해당 액터-세트들(관련 액터-세트들)만을 출력한다.

[0154] 단계(560)에서, 관리 명령들이 상기 정책 관리 서버(130)로 전송된다. 예를 들어, 상기 정책 엔진 모듈(340)은 상기 기능-레벨 명령들(단계(540)에서 생성된) 및 상기 관련 액터-세트들(단계(550)에서 생성된)을 상기 특정 관리 서버(130)로 전송한다.

[0155] 단계(520) 및 단계(540)는 특정 관리 서버(130)를 위한 상기 관리 정책 관점 생성(및 기능-레벨 명령들 생성)에 영향을 미치고, 반면에 단계(530) 및 단계(550)는 해당 관리 서버를 위한 상기 액터 관점 생성에 영향을 미친다. 단계(520)이 단계(550)에 의해 사용되는 규칙들의 세트를 생성하기 때문에, 상기 관리 정책 관점의 생성 및 상기 액터 관점의 생성은 서로에게 최소한으로 의존한다. 그렇지만, 상기 관리 정책 산출들(다시 말해, 단계(520) 및 단계(540)) 및 상기 액터-세트 산출들(다시 말해, 단계(530) 및 단계(550)) 분리하여 유지하는 것은 상기 정책 엔진 모듈(340)의 확장성을 향상시킨다. 상기 관리 정책 산출들 및 상기 액터-세트 산출들은 거의 분리되어 유지되기 때문에, 그들은 병렬로 수행될 수 있다(예를 들어, 동일한 관리 서버(130)에 대해서도). 게다가, 다른 관리 서버들(130)을 위한 관점 산출들(perspective calculations)이 또한 병렬로 수행될 수 있다. 또한 액터가 변경되는 경우, 그러면 상기 액터-세트들만이 재산출되는 것을 필요로 한다. (상기 기능-레벨 명령들은 재산출되는 것을 필요로 하지 않는다.) 규칙이 변경되는 경우, 그러면 상기 기능-레벨 명령들 및 상기 관련 액터-세트들만이 재열거되는 것을 필요로 한다. (상기 액터들은 재열거되는 것을 필요로 하지 않는다.)

[0156] 도 6은 일 실시예에 따른 관리 서버(130)의 관리 모듈(132)을 위한 구성(134)을 생성하는 방법(600)을 나타내는 흐름도이다. 다른 실시예들이 다른 방법으로 상기 방법들을 수행할 수 있고, 다른 및/또는 추가적인 방법들을 포함할 수 있다. 추가적으로, 어떤 또는 모든 방법들이 도 1에 도시된 이외의 다른 개체에 의해 수행될 수 있다.

[0157] 상기 방법(600)이 시작할 때, 상기 관리 서버(130)의 로컬 상태와 관련된 정보는 상기 관리 서버(130)에서 상기 정책 구현 모듈(136)의 상기 로컬 상태 저장부(400)에 미리 저장될 수 있다. 이러한 포인트에서, 상기 방법(600)을 시작한다.

[0158] 단계(610)에서, 관리 명령들이 상기 글로벌 매니저(120)로부터 수신된다. 예를 들어, 상기 정책 컴필레이션 모듈(410)은 상기 글로벌 매니저(120)로부터 기능-레벨 명령들 및 관련 액터-세트들을 수신한다.

[0159] 단계(620)에서, 상기 로컬 상태가 액세스된다. 예를 들어, 상기 정책 컴필레이션 모듈(410)은 상기 로컬 상태 저장부(400)에 저장된 상기 관리 서버(130)의 로컬 상태 관련 정보를 액세스한다.

[0160] 단계(630)에서, 관리 모듈 구성(134)이 생성된다. 예를 들어, 상기 정책 컴필레이션 모듈(410)은 상기 관리 명령들(단계(610)에서 수신된) 및 상기 로컬 상태(단계(620)에서 액세스된)를 입력으로 받아들이고, 관리 모듈 구성(134)을 생성한다.

[0161] 단계(640)에서, 관리 모듈(132)이 구성된다. 예를 들어, 상기 정책 컴필레이션 모듈(410)은 상기 관리 모듈 구

성(134)(단계(630)에서 생성된)에 따라 동작하도록 상기 관리 모듈(132)을 구성한다.

[0162] 도 7은 일 실시예에 따른 관리 서버(130)의 로컬 상태를 모니터 하고, 로컬 상태 정보를 글로벌 매니저(120)로 전송하는 방법(700)을 나타내는 흐름도이다. 다른 실시예들이 다른 방법으로 상기 방법들을 수행할 수 있고, 다른 및/또는 추가적인 방법들을 포함할 수 있다. 추가적으로, 어떤 또는 모든 방법들이 도 1에 도시된 이외의 다른 개체에 의해 수행될 수 있다.

[0163] 상기 단계(700)이 시작할 때, 상기 관리 서버(130)의 로컬 상태와 관련된 정보는 상기 관리 서버(130)의 상기 로컬 상태 저장부(400)에 미리 저장될 수 있다. 이러한 포인트에서, 상기 방법(700)이 시작된다.

[0164] 단계(710)에서, 상기 관리 서버(130)의 현재 로컬 상태와 관련된 정보가 결정된다. 예를 들어, 상기 LSU 모듈(420)은 상기 서버의 운영체제 및/또는 파일 시스템의 다양한 부분을 점검함으로써 상기 관리 서버(130)의 로컬 상태를 결정한다.

[0165] 단계(720)에서, 상기 현재 로컬 상태와 관련된 정보가 상기 로컬 상태 저장부(400)에 저장된 정보와 상이한지 여부와 관련된 결정이 수행된다. 예를 들어, 상기 LSU 모듈(420)은 이러한 결정을 수행한다. 상기 정보가 다르지 않을 경우, 그러면 상기 방법은 단계(730)로 이동하고, 종료한다. 상기 정보가 다를 경우, 그러면 상기 방법은 단계(740)로 이동한다.

[0166] 단계(740)에서, 상기 상이한 정보는 상기 로컬 상태 저장부(400)에 저장된다. 예를 들어, 상기 LSU 모듈(420)은 이러한 단계를 수행한다.

[0167] 단계(750)에서, 상기 관리 모듈 구성(134)이 재생성되고(상기 로컬 상태 저장부(400)의 콘텐츠가 변경되기 때문에), 상기 관리 모듈(132)은 이에 따라 재구성된다. 예를 들어, 상기 LSU 모듈(420)은 상기 관리 모듈 구성(134)을 재생성하는 상기 정책 컴필레이션 모듈(410)을 실행한다.

[0168] 단계(760)에서, 상기 상이한 정보는 상기 글로벌 매니저(120)으로 전송된다. 예를 들어, 상기 LSU 모듈(420)은 이러한 단계를 수행한다.

[0169] 도 8은 일 실시예에 따른 상기 관리 도메인의 컴퓨터 네트워크 인프라(320)의 상태에 대한 변경을 처리하는 방법(800)을 나타내는 흐름도이다. 다른 실시예들이 다른 방법으로 상기 방법들을 수행할 수 있고, 다른 및/또는 추가적인 방법들을 포함할 수 있다. 추가적으로, 어떤 또는 모든 방법들이 도 1에 도시된 것 이외의 다른 개체에 의해 수행될 수 있다.

[0170] 단계(810)에서, 특정 관리 서버(130)에 관한 변경이 수신된다. 예를 들어, 상기 관리 도메인 상태 업데이트(ADSU: administrative domain state update) 모듈(385)은 상기 관리 관리 서버(130)로부터 로컬 상태 정보의 부분으로 온라인/오프라인 표시(online/offline indicator), 운영체제 표시(operating system indicator), 네트워크 노출 정보(network exposure information), 및/또는 서비스 정보를 수신한다.

[0171] 단계(820)에서, 상기 수신된 정보는 저장된다. 예를 들어, 상기 ADSU 모듈(385)은 상기 수신된 온라인/오프라인 표지, 네트워크 노출 정보, 및/또는 서비스 정보를 상기 관리 도메인 상태(320)(특히, 상기 관리 서버(130)의 디스크립션에 어떤 정보가 존재하는지를)에 저장한다.

[0172] 단계(830)에서, 상기 서버 디스크립션은 상기 서버와 관련된 추가적인 정보를 결정하기 위해 분석된다. 예를 들어, 상기 ADSU 모듈(385)은 상기 서버를 위한 레이블/CC값을 산출하기 위해 레이블/구성된 특성 엔진을 사용하고, 및/또는 상기 서버가 NAT(network address translator) 뒤에 있는지 여부를 결정하고(그리고, NAT 뒤에 있는 경우, NAT의 유형은 1:1 또는 1:N이다), 해당 정보를 상기 서버 디스크립션에 저장한다. 단계(830)은 선택적이다.

[0173] 단계(840)에서, 상기 관리 도메인의 액터-세트들의 업데이트 여부와 관련된 결정이 이루어진다. 예를 들어, 상기 ADSU 모듈(385)은 상기 관리 서버의 디스크립션에 대한 변경에 기반하여 상기 관리 도메인의 액터-세트들의 업데이트 여부를 결정한다. 상기 관리 도메인의 액터-세트들의 업데이트가 결정되는 경우, 그러면 상기 방법은 단계(850)로 이동한다. 상기 관리 도메인의 액터-세트들의 업데이트가 결정되지 않는 경우, 그러면 상기 방법은 단계(860)로 이동한다.

[0174] 단계(850)에서, 상기 관리 도메인의 액터-세트들은 업데이트된다. 예를 들어, 상기 ADSU 모듈(385)는 상기 관리 도메인의 액터-세트들을 업데이트하도록 상기 정책 엔진 모듈(340)을 지시한다. 일 실시예에서(도시하지 않은), 상기 ADSU 모듈(385)은 상기 관리 도메인의 액터-세트들을 업데이트하도록 상기 정책 엔진 모듈(340)을 지시하

기 전에 이벤트가 발생할 때까지 대기한다.

[0175] 단계(860)에서, 상기 관리 서버의 관리 명령들의 업데이트 여부와 관련된 결정이 이루어진다. 예를 들어, 상기 ADSU 모듈(385)은 상기 관리 서버의 디스크립션에 대한 변경에 기반하여 상기 관리 서버의 관리 명령들의 업데이트 여부를 결정한다. 상기 관리 서버의 관리 명령을 업데이트하도록 결정한 경우, 그러면 상기 방법은 단계(870)로 이동한다. 상기 관리 도메인의 액터-세트들을 업데이트하지 않도록 결정한 경우, 그러면 상기 방법은 단계(880)로 이동한다.

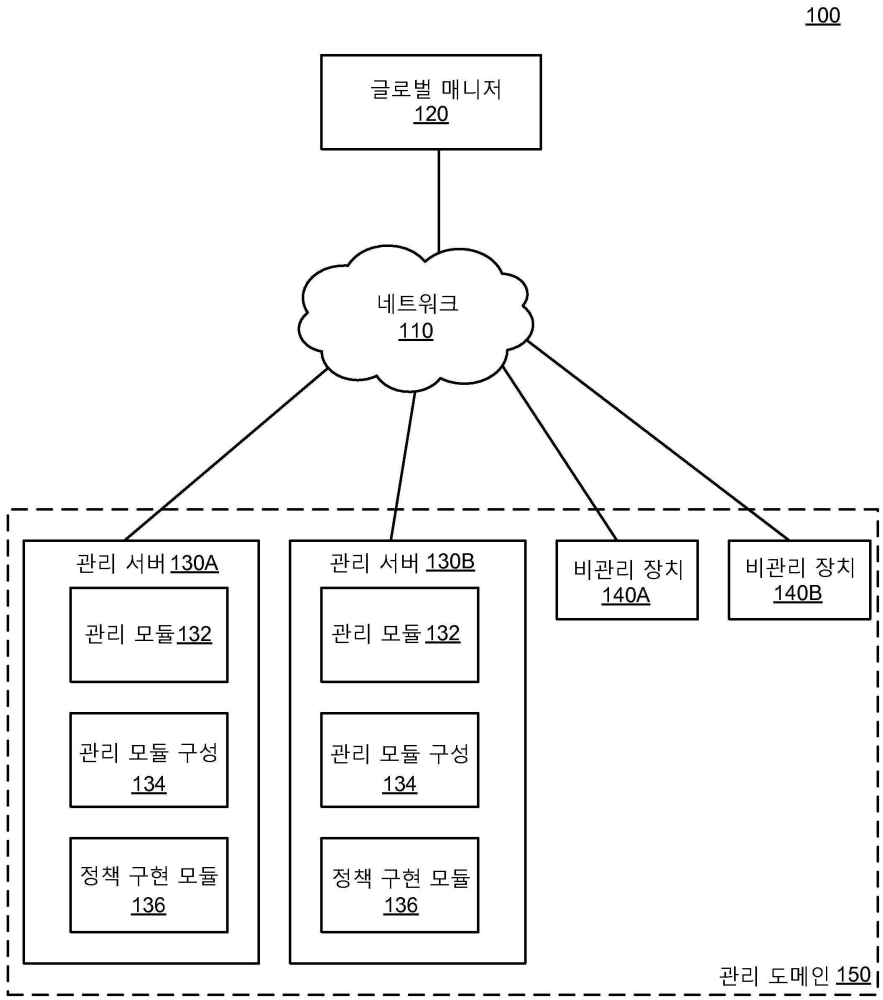
[0176] 단계(870)에서, 상기 관리 서버의 관리 명령들은 업데이트된다. 예를 들어, 상기 ADSU 모듈(385)은 상기 관리 서버의 관리 명령들을 업데이트하도록 상기 정책 엔진 모듈(340)을 지시한다. 일 실시예에서(도시하지 않은), 상기 ADSU 모듈(385)은 상기 관리 서버의 관리 명령들을 업데이트하도록 상기 정책 엔진 모듈(340)을 명령하기 전에 이벤트가 발생할 때까지 대기한다.

[0177] 단계(880)에서, 상기 방법을 종료한다.

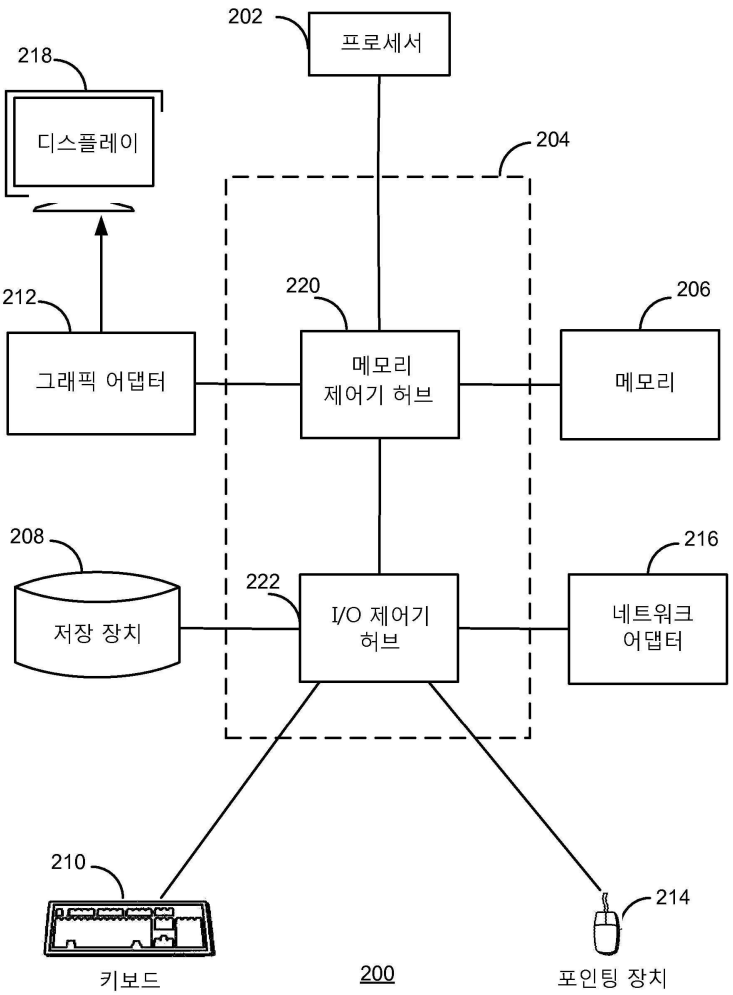
[0178] 상기 설명은 특정 실시예의 동작을 예시하기 위해 포함되고, 본 발명의 범위를 제한하는 것을 의미하지 않는다. 본 발명은 첨부된 청구항에 의해서만 한정된다. 상기 설명으로부터, 본 발명의 사상 및 기술 범위에 속하는 관련분야의 통상의 기술자로부터 다양한 변형은 명백해진다.

도면

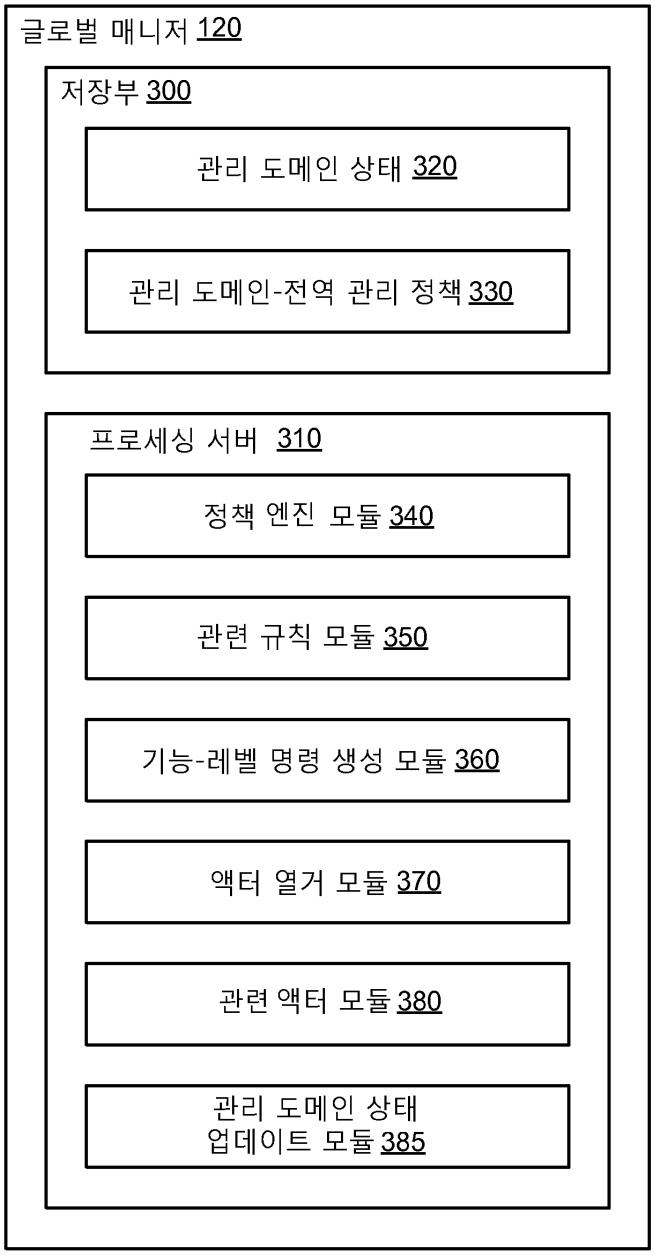
도면1



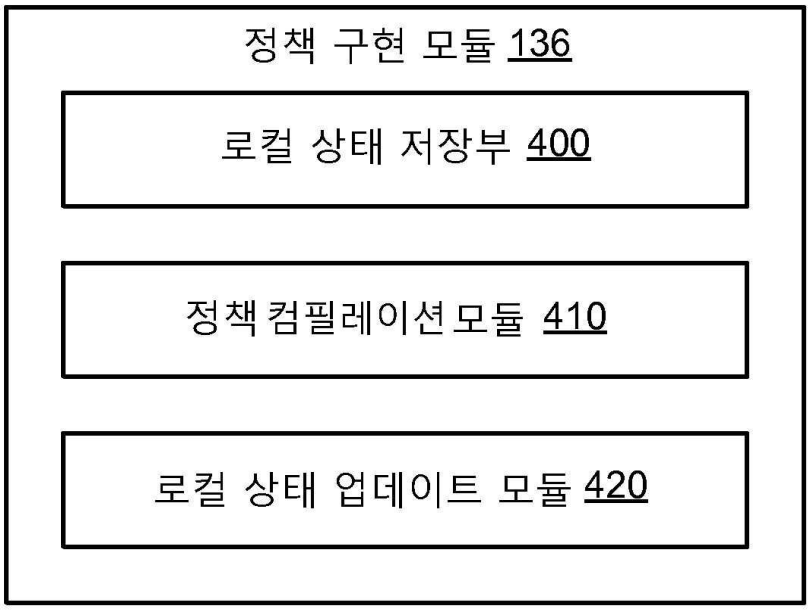
도면2


202
프로세서
218
디스플레이
204
212
220
206
그래픽 어댑터
메모리
제어기 허브
메모리
208
216
222
저장 장치
I/O 제어기
허브
네트워크
어댑터
210
214
키보드
200
포인팅 장치

도면3

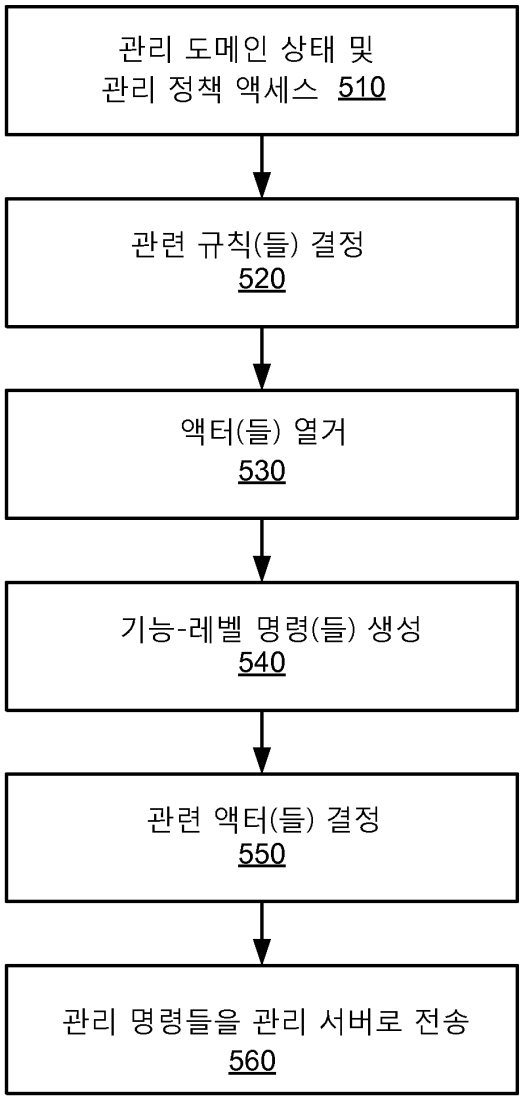

글로벌 매니저 120
저장부 300
관리 도메인 상태 320
관리 도메인-전역 관리 정책 330
프로세싱 서버 310
정책 엔진 모듈 340
관련 규칙 모듈 350
기능-레벨 명령 생성 모듈 360
액터 열거 모듈 370
관련 액터 모듈 380
관리 도메인 상태
업데이트 모듈 385

도면4

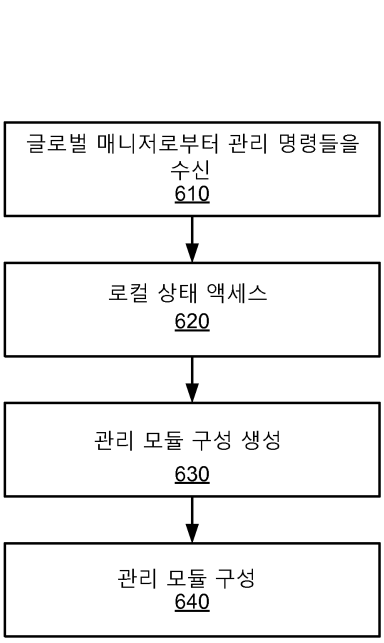


도면5

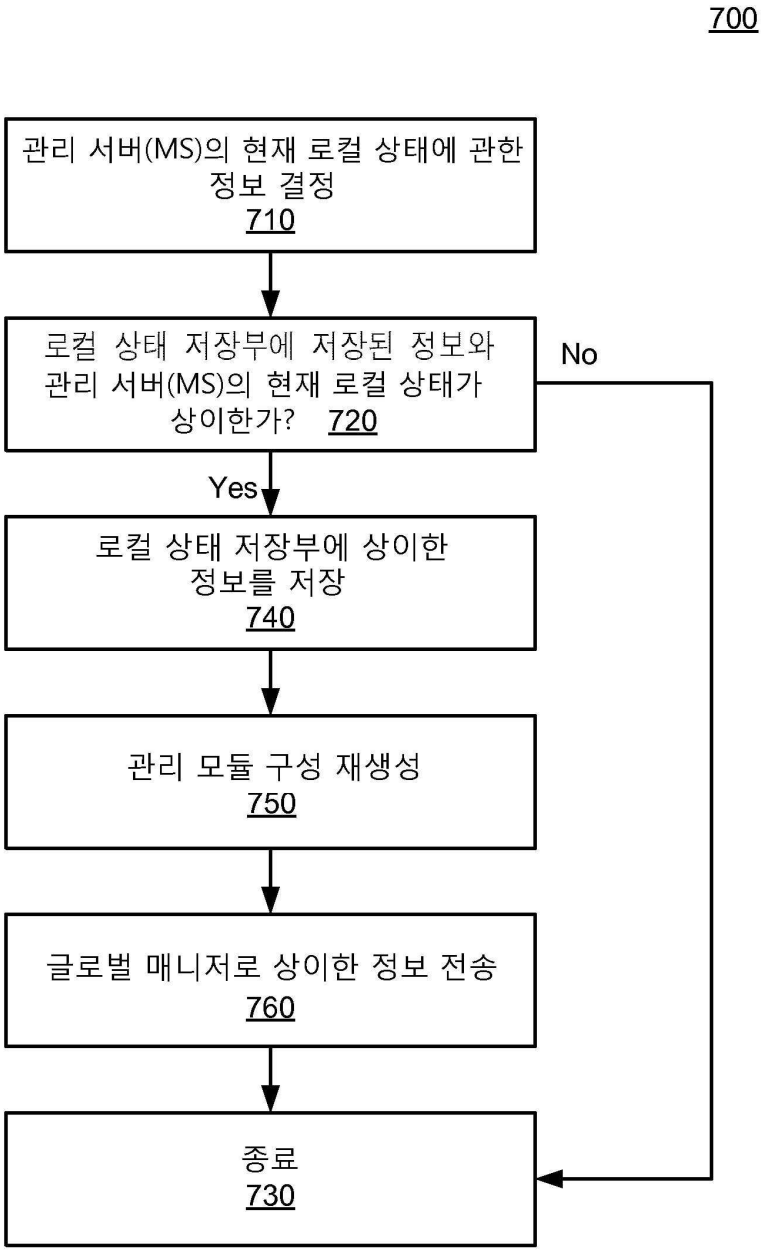
500


관리 도메인 상태 및
관리 정책 액세스 510
관련 규칙(들) 결정
520
액터(들) 열거
530
기능-레벨 명령(들) 생성
540
관련 액터(들) 결정
550
관리 명령들을 관리 서버로 전송
560

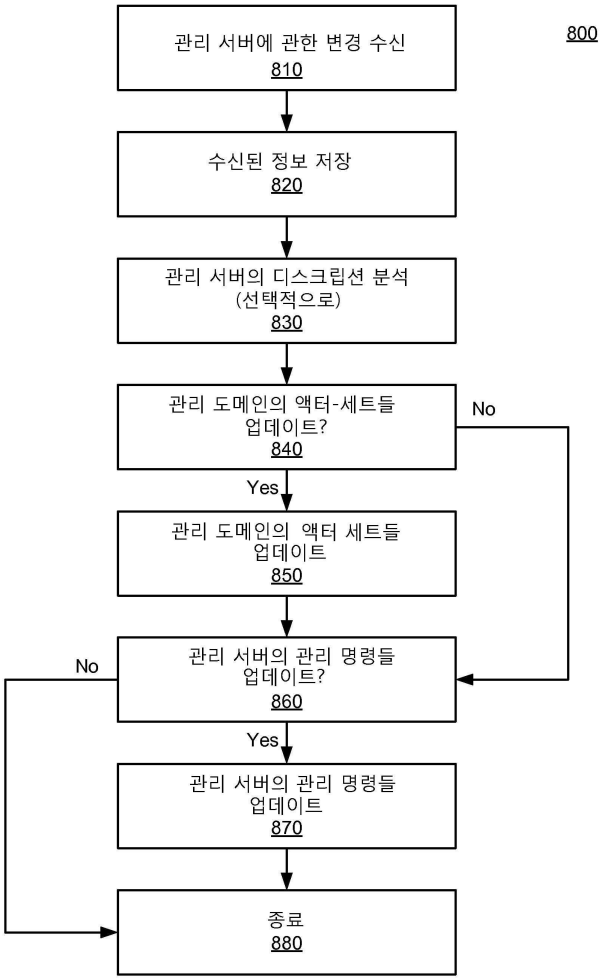
도면6


600
글로벌 매니저로부터 관리 명령들을 수신
610
로컬 상태 액세스
620
관리 모듈 구성 생성
630
관리 모듈 구성
640

도면7


700
관리 서버(MS)의 현재 로컬 상태에 관한 정보 결정
710
로컬 상태 저장부에 저장된 정보와 관리 서버(MS)의 현재 로컬 상태가 상이한가? 720
No
Yes
로컬 상태 저장부에 상이한 정보를 저장
740
관리 모듈 구성 재생성
750
글로벌 매니저로 상이한 정보 전송
760
종료
730

도면8


800
관리 서버에 관한 변경 수신
810
수신된 정보 저장
820
관리 서버의 디스크립션 분석
(선택적으로)
830
관리 도메인의 액터-세트들
업데이트?
840
No
Yes
관리 도메인의 액터 세트들
업데이트
850
관리 서버의 관리 명령들
업데이트?
860
No
Yes
관리 서버의 관리 명령들
업데이트
870
종료
880