韓國 컴퓨터情報學會 論文誌
第10卷 第5號, 2005. 11.

2005-10-5-2-6

고 가용성과 업무의 연속성 보장을 위한 지능적 웹 서비스 접속관리의 구현 방안에 관한 연구

강 현 중*, 이 광 형**

Implementation of Intelligent Web Service Access Management for Supporting High Availability and Business Continuity

Kang-Hyun Joong *, Kwang-Hyoung Lee **

요 약

웹 기반의 응용 어플리케이션 환경에서 서비스의 가용성과 업무의 연속성 보장은 중요한 고려사항이 되었으며, 이를 위해 서버 및 장비의 이중화, 센터의 이중화, 재난복구 센터의 구축 등의 이중화된 통합센터 구조를 갖는 경우를 볼 수 있다. 이러한 아키텍처로 구현될 경우 웹 브라우저 사용자는 URL이라는 웹 사이트 주소를 통해서 해당 센터의 웹 서버에 접근하게 되는데, 이는 웹 브라우저 사용자들이 임의로 URL을 변경하고 임의의 센터에 접속하여 데이터의 저장위치를 비정상적으로 정의하여 데이터의 무결성을 보장하지 못할 수도 있다. 본 논문에서는 사용자 인증방안, 공인인증기관 연계방안, 장애시 업무의 연속성 보장방안 등의 구현방안을 소개하고, 지능적 서비스 접속관리를 제시한다.

Abstract

High availability and business continuity in the mission critical enterprise environment have been a matter of primary concern. It is desirable to implement replicated servers, duplicated devices and disaster recovery sites so that these issues are accomplished. When that happens, web browser's users may be accessed web server through a specific Uniform Resource Locator. A critical issue arises if web browser's users recklessly change the URL and access into other site. In this case, data integrity between duplicated sites may not be guaranteed. In this paper, we introduce the method of integrating the technologies of user authentication, certificate authority and business continuity and propose the design and implementation of intelligent service access management.

▸ Keyword : 업무의 연속성(Business Continuity), 접속관리(Connection Management), 지능적 도메인 네임 서비스(Intelligent DNS)

• 제1저자 : 강형중
• 접수일 : 2005.09.28, 심사완료일 : 2005.11.01
* 서일대학 인터넷정보과 부교수, ** 서일대학 인터넷정보과 전임강사

Ⅰ. 서 론

현재 업무의 형태들이 점점 더 인터넷 기반 중심으로 바뀌어가고 있고, 이로 인해 웹 기반의 어플리케이션이 급속도로 변화, 성장하고 있다[1]. 이러한 환경의 변화에서 서비스의 가용성과 업무의 연속성은 반드시 고려되어야 할 필수항목으로 자리매김하고 있으며, 대국민 서비스를 제공하는 기업 혹은 정부는 이러한 측면을 고려하여 서버 및 장비의 이중화, 센터의 이중화, 재난복구 센터의 구축 등의 솔루션을 채택하고 있는 실정이다[2][14]. 이러한 이중화된 통합센터 구조는 다음과 같은 특징을 갖는다.

- 사용자는 인터넷 사용자와 인트라넷 사용자로 구분된다.
- 해당 서버의 자원을 접근할 때는 인터넷 접속표준 방식인 URL을 사용하게 된다.
- 인터넷 및 인트라넷 사용자는 미리 정의되어 있는 해당 센터로 접속하여 업무를 처리할 수 있으며, 비정상적인 데이터 저장이 일어나지 못하도록 다른 센터로의 접근은 방지되어야 한다.
- 해당 센터의 장애시 인터넷 및 인트라넷 사용자가 업무의 연속성을 보장받을 수 있기 위해서는 다른 인접센터로의 접근이 가능해야 하며, 이를 통한 신속한 업무대행 서비스를 제공하여야 한다.

따라서 본 연구에서는 센터 간의 데이터 일치성 보장 측면과 센터 장애 시 업무의 연속성 측면을 고려한 웹 상에서의 통합접속관리 구현방안을 제시하고자 한다. 이를 위한 본 논문의 구성은 2장에서 지능적 도메인 네임 서비스와 접속자원의 권한제어 측면을 통해 URL 변경방지 제어 구현의 필요성을 설명하고, 3장에서는 업무 프로세스 모델 설계, 4장에서는 전체 구성도, 구성내역, 구현방안 등을 제안하고, 5장에서는 지능적 도메인 네임 서비스를 통한 시험을 통해 제안하고자 하는 구현 방안의 타당성을 검증하였고, 마지막 6장에서는 결론을 제시하였다.

Ⅱ. 이슈사항

2.1 지능적인 DNS 서비스 측면

인터넷의 중심에는 서버의 IP 주소를 호스트 네임으로 해석해 주는 도메인 네임 서비스가 있어 사용자와 접속하고자하는 서버까지 IP 주소가 아닌 도메인 이름을 이용하여 손쉽게 연결을 하고 있다[3][4][5][12]. 인터넷 환경에서 도메인 네임 서비스가 필수적인 솔루션인 것은 명확하지만 지능적이라고 하기에는 아직 부족한데, 고유기능인 호스트 이름 해석을 잘 수행했다고 하더라도 접속될 서버들의 가용성 여부와 건강도 체크에 있어서는 상당히 미약하다. 따라서, 클라이언트의 요청을 전혀 응답이 없는 서버로 연결시키는 경우가 수시 발생하고 있으며, 이는 업무의 연속성 측면에서 저해하는 요소가 되어왔다. 도메인 네임 서비스는 현재의 네트워크 및 서버의 가용성 등에 관한 상황을 전혀 파악하지 못하고 단순히 이름 해석 작업만을 하고 있으며, 가장 적절히 응답하는 서버로 클라이언트를 지능적으로 연결시켜주지 못하고 있다[6].

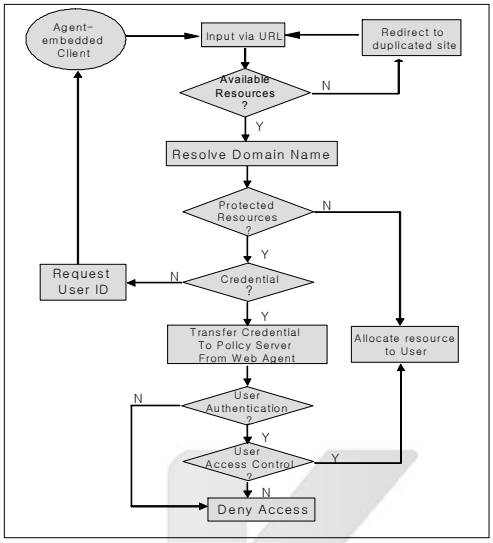
2.2 접속자원의 권한제어 측면

웹의 소개와 함께 인터넷, 인트라넷, 엑스트라넷은 눈부시게 발전을 거듭하고 있고 기술의 발전과 더불어 인터넷을 통해 비즈니스를 창출하고 있는 환경에서 다음과 같은 이슈사항을 고려할 필요가 있다[7].

- 사용자들이 보안상의 위험에 노출되지 않은 상태에서 사이트를 사용할 수 있도록 해야 하며, 완벽한 보안이 요구되는 인증과 인가가 필요하다.
- 자원에 대한 접근은 사용자별 접근 레벨을 다르게 유지하는 사용자 자격 부여에 기초되어야 하며, 접근 권한을 정의한 사용자 프로파일이 효과적으로 관리되어야 한다.
- SSO(Single Sign On)와 사용자 관리 기능을 위임 할 수 있어야 하고, 기존 인프라에 쉽게 통합되어야 한다.

III. 업무 프로세스 모델 설계

표 1 업무 프로세스 기능 모델
Table 1 Business Process Functional Model



웹 클라이언트가 웹 서버에 접속하기 위해서는 반드시 URL을 사용하여야 하며, 이 해석과정에서는 도메인 이름을 IP 주소로 해석되어 목적지 웹 서버에 접속하여 초기 웹페이지를 검색하게 된다. 사용자는 로그인 과정을 통해 웹 페이지에 대한 접속권한을 부여받게 되는데, 2.1절과 2.2절과 같은 이슈사항이 존재한다. <표 1>은 업무 프로세스별 해당 기능영역을 나타낸 것이다.

IV. 통합접속관리의 적용방안

4.1 전체 구성도와 구성내역

지능적인 도메인 네임 서비스 측면과 접속 자원의 권한 제어 측면을 고려하여 (그림 1) 과 같이 구성한다. 이 때, 초기 사이트에 접속할 때나 장애시 업무 대행으로 사용자의 트래픽의 흐름을 제어하기 위한 솔루션으로 지능적 도메인 네임 서비스를 채택하였고, 사용자의 인증과 인가, 자원에 대한 접근 제어 등을 담당하는 디렉토리 기반의 정책서버와 에이전트를 채택하였다.

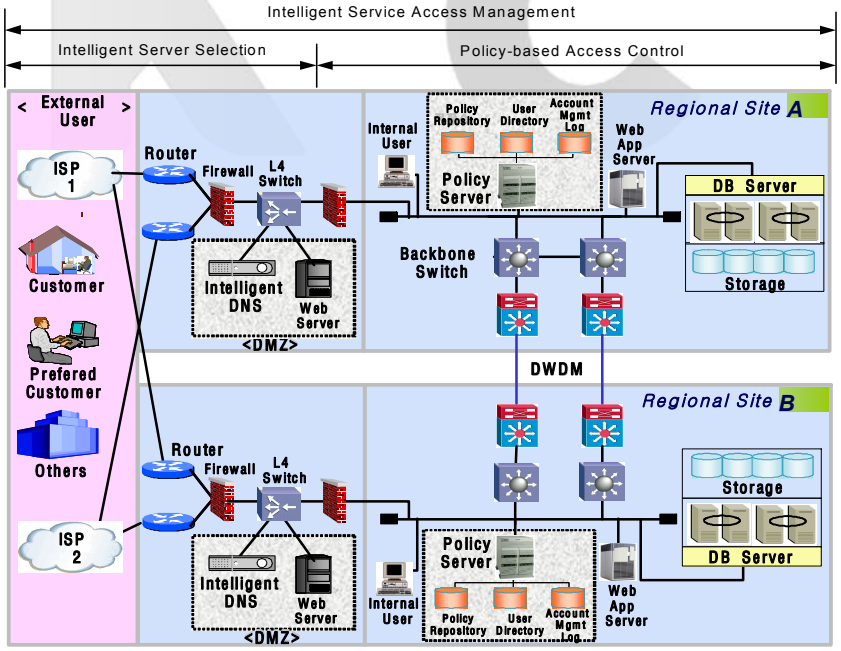


그림 1. 전체 구성도
Fig. 1 System Architecture

지능적 도메인 네임 서비스는 L3(or L4)장비의 바깥쪽에 위치하여 한개의 센터에 문제가 발생하였거나, 접속가능한 센터간의 적절한 응답시간을 지능적으로 판단하여 클라이언트의 응답을 가용한 센터 및 서비스 응답이 빠른 센터로 보낸다. 내부적으로, 지능적 도메인 네임 서비스는 RTT(Round Trip Time), Hit Ratio, 패킷 전송률 등의 메트릭 값을 저장하고 있으며 가장 빠른 응답시간 값을 가진 지능적 도메인 네임 서비스의 정보를 클라이언트의 로컬 DNS에 보내고 클라이언트는 로컬 도메인 네임 서비스의 정보를 받아 최적의 서비스를 받을 수 있는 센터에 접속하게 된다. 이러한 과정을 통해 지능적 도메인 네임 서비스로 2개 이상의 센터간 서비스의 질적 보장 기반의 동적 로드밸런싱 환경을 구현할 수 있다[8][9].

정책서버는 관리자에 의해 수립된 접근 제어 정책을 관리하며, 어떤 자원이 보호되는지, 어떤 사용자 또는 사용자 그룹이 자원에 접근이 허용되는지를 정의한다. 정책서버는 정책 기반의 사용자 관리, 안전한 포탈 관리, 인증 서비스, 인가 서비스, 사용자 등록 서비스, 패스워드 서비스, 세션 관리, 감사(Audit) 서비스 등의 기능을 수행한다[10].

웹 에이전트는 웹 서버 자원 접근을 하기 위한 사용자를 인증, 인가하기 위하여 정책서버와 작업을 한다. 웹 에이전트는 자원에 대한 요청을 인터셉트하고 자원이 보호되었는지를 결정하며, 사용자를 인증하기 위하여 정책서버와 상호작용하고 자원 접근에 대하여 인가 되었는지를 결정한다. 인가가 성공했을 때만, 웹 에이전트는 사용자 요청을 처리한다. 또한, 웹 에이전트는 응답 형식으로 어플리케이션에 추가적으로 사용자에 특별한 속성을 포워드할 수 있고, 컨텐츠의 개인화가 가능하다. 또한, 성능과 정책서버와의 통신을 모니터링 하기 위한 로깅 기능을 제공한다.

4.2 구현 방안

웹상에서의 통합접속관리를 위한 구현 방안으로 지능적 도메인 네임 서비스 방안, 사용자 인증방안, 공인인증기관 연계방안, 장애시 업무의 연속성 보장 방안 등으로 나누어 전개하도록 하겠다.

4.2.1 지능적 도메인 네임 서비스 방안

지능적 도메인 네임 서비스 방안이란 인터넷 및 인트라넷 사용자가 웹 브라우저를 통해 URL로 접속하였을 때 목적지 웹 서버로 접속되는 메커니즘을 지능적으로 수행하는 방법을 말하며, 여기에서는 인터넷 사용자의 트래픽 흐름과 인트라넷 사용자의 트래픽 흐름으로 나누어 좀 더 구체적이고 자세히 설명하겠다.

1) 인터넷 사용자의 트래픽 흐름 절차

- 인터넷 사용자의 웹 클라이언트는 해당 주소(URL)에 대해 자신이 속한 ISP의 로컬 도메인 네임 서비스에 도메인 이름 해석을 요청
- 로컬 도메인 네임 서비스는 상위 도메인 네임 서비스 (혹은 루트 도메인 네임 서비스)에 해당 도메인 이름 해석을 요청
- 상위 도메인 네임 서비스(혹은 루트 도메인 네임 서비스)는 해당 도메인 서버의 IP 주소를 로컬 도메인 네임 서비스에게 통지
- 로컬 도메인 네임 서비스는 해당 도메인 서버에게 해당 주소(URL)의 IP 해석을 요청
- 해당 도메인 서버(여기에서는 지능적 도메인 네임 서비스가 도메인 서버가 됨)는 해당 사이트의 L4 스위치 혹은 해당 서버의 정상 혹은 장애 등을 감시 (이는 지능적 도메인 네임 서비스가 iQuery 통신을 통해 메트릭 정보를 실시간으로 수집함)
- 지능적 도메인 네임 서비스는 가장 적합한 해당 서버의 IP 주소를 로컬 도메인 네임 서비스에 통지
- 로컬 도메인 네임 서비스는 최종적으로 웹 클라이언트에게 접속할 해당 서버의 IP 주소를 통지
- 웹 클라이언트는 로컬 도메인 네임 서비스로부터 받은 IP 주소로 해당 서버에 접속

2) 인트라넷 사용자의 트래픽 흐름 절차

- 인트라넷 사용자의 웹 클라이언트는 해당 도메인 서버(여기에서는 지능적 도메인 네임 서비스가 도메인 서버가 됨)에게 해당 주소(URL)의 IP 해석을 요청
- 해당 도메인 서버(여기에서는 지능적 도메인 네임 서비스가 도메인 서버가 됨)는 해당 사이트의 L4 스위치 혹은 해당 서버의 정상 혹은 장애 등을 감시 (이는 지능적 도메인 네임 서비스가 iQuery 통신을 통해 메트릭 정보를 실시간으로 수집함)
- 도메인 서버는 최종적으로 웹 클라이언트에게 접속할 해당 서버의 IP 주소를 통지
- 웹 클라이언트는 도메인 서버로부터 받은 IP 주소로 해당 서버에 접속

4.2.2 보안 정책 설계

통합접속관리의 이행을 위해서 먼저 보안정책을 설계해야 한다.

1) 정책

정책은 사용자와 보호된 자원에 대한 사용자와의 관계를 가지고 만들어지며, 자원에 대한 사용자 접근을 명시적으로 허용 또는 거부 함으로서 자원을 보호한다. 또한, 자원에 접근하는 사용자 또는 그룹, 접근이 허용되는 조건, 그리고 인가된 사용자에 대한 자원의 전달 메소드를 기술한다. 사용자가 자원에 대한 접근이 거부된다면 정책 또한 그 사용자를 어떻게 다룰지를 결정한다. 이러한 정책은 모든 권한정보 데이터베이스가 되는 정책 저장소에 저장된다. 다시 요약하면, 정책은 특정 자원에 대한 접근을 허용하거나 거절하는 규칙, 사용자 식별, 규칙과 일치할 경우 일어나는 행위, 정책이 적용되는 IP 주소, 정책이 일치하거나 일치되지 않는 시간 제한, 정책에 대한 확장 옵션 등으로 구성된다[11].

2) 자원

자원은 사용자의 사용을 위해 웹 에이전트, 어플리케이션 서버 에이전트 등에 의해 보호 받는 객체를 의미한다. 보통, 웹 페이지, CGI 스크립트, 디렉토리, 서블릿 또는 EJB, JSP 페이지 등이 모두 자원이 될 수 있다.

3) 규칙

규칙은 보호된 자원에 대한 일련의 행위를 규정한다. 예를 들어, 보호되는 일련의 CGI 스크립트가 있을 때, 그룹의 사용자는 이 CGI 스크립트를 사용할 수 있고, 다른

4) 응답

규칙이 수행될 때 정책서버는 웹 에이전트로 응답의 속성을 반환한다. 에이전트는 HTTP 헤더에 정책서버에서 반환된 속성을 삽입하며, 이 속성을 서버 상의 어플리케이션이 사용하게 된다. ASP(Active Server Page), Java 서블릿, JSP(Java Server Page), CGI 호환 환경과 같은 일반적인 스크립트 언어와 프로그래밍 환경을 이용해 작성될 수 있다.

4.2.3 사용자 인증 방안

인터넷 및 인트라넷 사용자를 인증하기 위해서 클라이언트 에이전트를 통해 정책서버로부터 인증 토큰을 발급 받고, 해당 웹 서버에 설치되어 있는 웹 서버 에이전트에서 인증을 확인한다[13]. (그림 2)는 사용자가 웹 브라우저를 통해 URL로 해당 자원을 참조할 때 그 사용자의 인증과 해당 접속권한을 부여받기 위해 웹 클라이언트, 웹 서버, 정책서버와의 수행 절차를 나타낸 것이다.

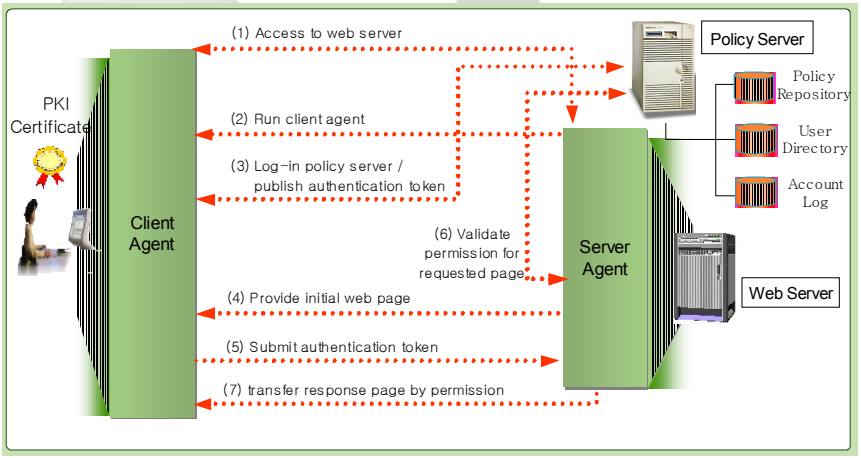


그림 2. 사용자 인증 절차
Fig. 2 Procedure of User Authentication

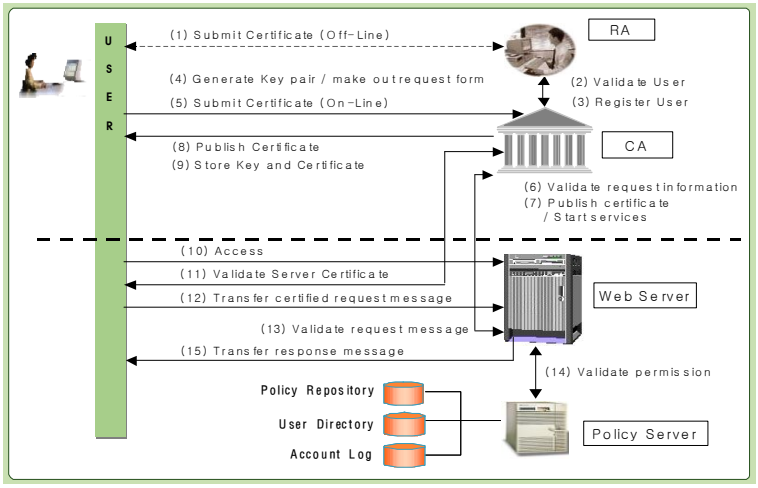


그림 3. 공인인증기관과의 연계 절차
Fig. 3 Procedure for connecting with Certificate Authority

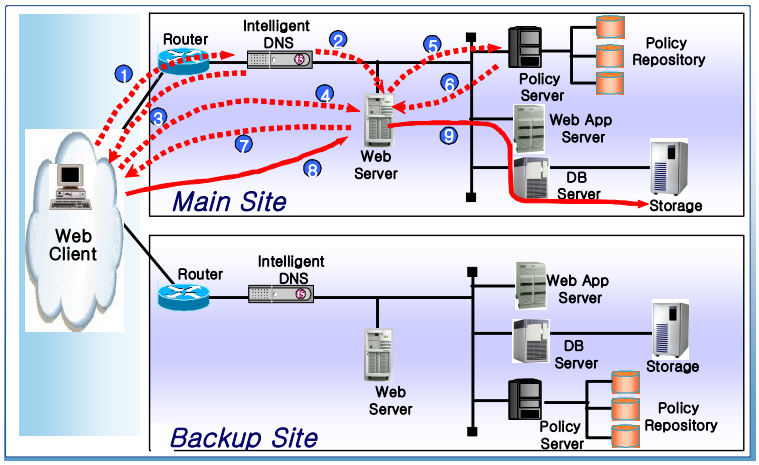


그림 4. 트래픽 흐름 절차
Fig. 4 Traffic Flow Diagram

4.2.4 공인인증기관 연계 방안

사용자 인증 및 데이터 암복호화시 국가 공인인증기관에서 발급한 인증서를 사용할 수도 있다. (그림 3)은 공인인증기관으로부터 인증서 발급 절차 및 발급된 인증서를 가지고 해당 자원에 접속하는 과정을 보여준다.

4.2.5 장애시 업무의 연속성 보장 방안

지역센터에 구축되어 있는 웹 서버, 웹 어플리케이션 서버, 데이터베이스 서버, 지능적 도메인 네임 서비스, 정책서버 등 지역센터의 주요 구성요소들의 장애가 발생될 경우 관리자의 장애 대응 방안 및 장애 대응으로 인해 변경된 트래픽 경로 흐름에 대해 설명하기로 한다. 이는 장애시 업무의 연속성을 보장하는데 중요한 이슈가 될 수 있을 것이다. (그림 4)는 이중화된 통합센터 구조를 갖는 환경에서의 지능적 서비스 접속관리의 트래픽 흐름 절차를 보인 것이다.

1) 데이터베이스 서버 장애

주센터의 데이터베이스 서버 장애시 관리자는 장애 감지를 인식하고 업무 대행 절차를 수행할 수 있다. 먼저, 정책서버의 정책을 다음과 같이 변경한다.

- 주센터에서 정상적인 업무를 담당했던 모든 자원들에 대해 접근을 불허한다.
- 주센터의 데이터베이스 서버 장애시 사용될 업무 대행용 자원들을 해당 접근 권한자 그룹에 접근을 허용시킨다.

2) 웹 어플리케이션 서버 장애

주센터의 웹 어플리케이션 서버 장애시 관리자는 장애 감지를 인식하고 업무 대행 절차를 수행할 수 있다. 먼저, 정책서버의 정책을 다음과 같이 변경한다.

- 주센터에서 정상적인 업무를 담당했던 모든 자원들에 대해 접근을 불허한다.
- 주센터의 데이터베이스 서버 장애시 사용될 업무 대행용 자원들을 해당 접근 권한자 그룹에 접근을 허용시킨다.

3) 웹 서버 장애

주센터의 웹 서버 장애시 지능적 도메인 네임 서비스는 장애 감지를 자동으로 인식하여 WAN 및 LAN 상의 트래픽을 백업센터로 이동시킨다. 한편, 관리자는 웹 서버의 장애를 인식하여 업무 대행 절차를 수행할 수 있다. 먼저, 정책서버의 정책을 다음과 같이 변경한다.

- 주센터에서 정상적인 업무를 담당했던 모든 자원들에 대해 접근을 불허한다.
- 주센터의 웹 서버 장애시 사용될 업무 대행용 자원들을 해당 접근 권한자 그룹에 접근을 허용시킨다.

4) 정책서버 장애

정상 상태에서는 주센터의 정책서버는 주 정책서버가 되며, 백업센터의 정책서버는 보조 정책서버로 구성되어 있다. 주 정책서버와 보조 정책서버는 각 서버의 상태를 체크하고 있으며, 주 정책서버 장애시 보조 정책서버가 주 정책서버를 대행하게 된다. 따라서, 관리자의 특별한 개입없이 보조 정책서버가 주 정책서버의 인증 및 인가 서비스를 수행하게 된다.

5) 지능적 도메인 네임 서비스 서버 장애

주센터의 지능적 도메인 네임 서비스와 백업센터의 지능적 도메인 네임 서비스는 서로 건강도 체크를 하고 있으며, 주센터의 지능적 도메인 네임 서비스 장애시 장애 발생을 백업센터의 지능적 도메인 네임 서비스가 인지하여 WAN 구간 및 LAN 구간의 트래픽을 담당하여 URL 접속에 대한 모든 도메인 해석을 수행하게 된다.

V. 시험

5.1 시험 목적

본 시험에서는 웹서버 장애시, 웹서비스 장애시, 3DNS 장애시, 네트워크 케이블 장애시 3DNS의 지능적 DNS 서비스 기능을 시험하였다. 여기서 3DNS는 앞장에서 소개한 지능적 접속관리 기능이 구현된 도메인 네임 서비스를 명명한 것이며, 본 논문에서는 지역적으로 분산된 통합센터에서의 지능적 접속관리의 방안에 대해서만 초점을 맞추고 있는 바 3DNS의 구현에 대한 설명은 배제하기로 한다.

5.2 시험 환경

(그림 5)와 같이 크게 3개의 네트워크로 구성하였다. 20.20.20.1인 서울 네트워크, 30.30.30.1인 대전 네트워크, 10.10.10.1인 외부 네트워크로 나누었다. 서울 네트워크와 대전 네트워크에는 트래픽 제어 및 도메인 이름해석을 담당하는 3DNS가 각각 구성되어 있으며, 서울 네트워크에는 웹서버 1과 대전 네트워크에는 웹서버 2번이 웹서비스를 수행하고 있다.

5.3 시나리오

본 테스트에서는 다음과 같은 질문에 대해 어떤 결과를 보이는가에 따라 각 시나리오는 수행하였다.

시나리오 1) 서울 네트워크의 웹서버1 하드웨어 장애시 내부 사용자 PC의 웹 클라이언트가 대전 네트워크의 웹서버2로 자동 접속되는가?

시나리오 2) 서울 네트워크의 웹서버1 상에 동작 중인 웹서비스를 종료(웹서비스 데몬 Down)시 내부 사용자 PC의 웹 클라이언트가 대전 네트워크의 웹서버2로 자동 접속되는가?

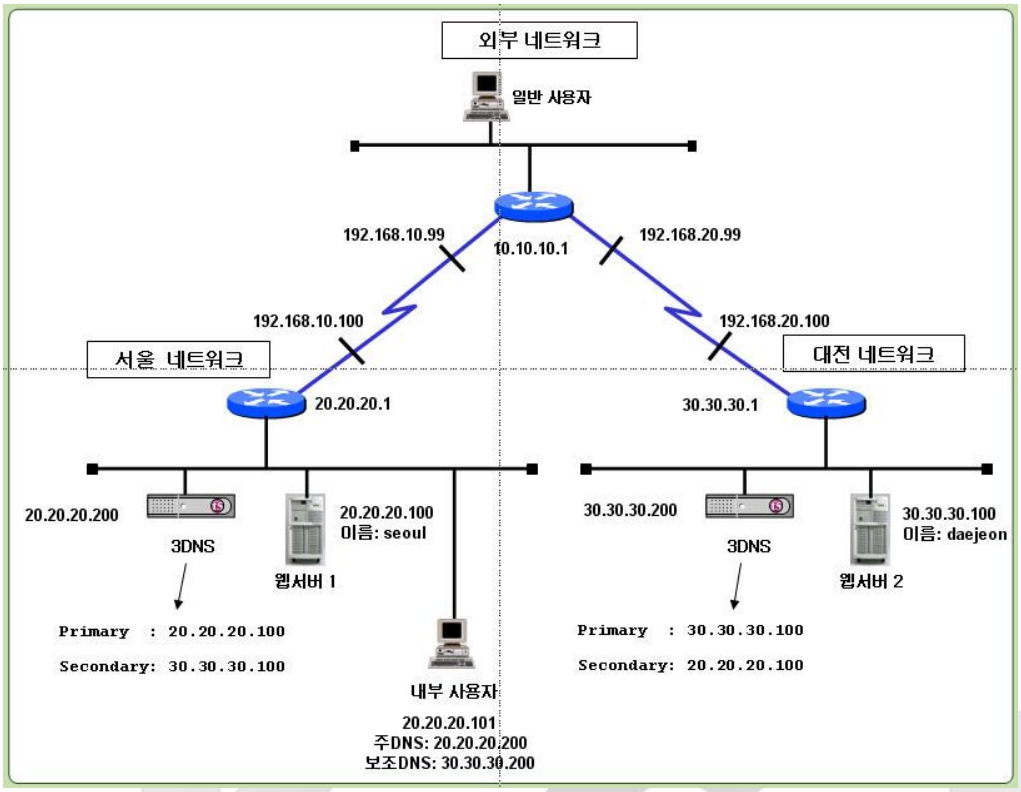


그림 5. 시험 환경
Fig. 5 Test Bed

표 1 시험 환경 구성표
Table 1 Configuration of Test Bed

위치	구성 장치	도메인	IP 주소	서브넷마스크	Gateway
서울 네트워크	3DNS	ds1.test.com	20.20.20.200	N/A	20.20.20.1
	웹서버1	Seoul.test.com	20.20.20.100	255.255.255.0	20.20.20.1
	라우터	N/A	20.20.20.1	N/A	N/A
	내부 PC	N/A	20.20.20.101	255.255.255.0	20.20.20.1
대전 네트워크	3DNS	ds2.test.com	30.30.30.200	N/A	30.30.30.1
	웹서버2	daejeon.test.com	30.30.30.100	255.255.255.0	30.30.30.1
	라우터	N/A	30.30.30.1	N/A	N/A

5.4 시험 결과

본 시험의 결과는 다음과 같다. 시나리오 1)와 2)의 작업을 수행한 결과 (그림 6)과 같은 결과를 보였다. 이는 가상의 서울 네트워크의 로컬 사용자 (IP주소: 20.20.20.101)가 로컬 도메인 네임 서비스 (20.20.20.200)에게 질의한 결과 거리상으로 가까운 웹서버1의 접속을 회피하고, 원격지 대전 네트워크의 웹서버2(30.30.30.100)로 전환되었음을 알 수 있다.

```
c:₩>tracert www.test.com

Tracing route to www.test.com [30.30.30.100]
over a maximum of 30 hops:

  1   <10 ms    <10 ms    <10 ms    192.168.10.99
  2   <10 ms    <10 ms    <10 ms    192.168.20.100
  3   <10 ms    <10 ms    <10 ms    30.30.30.1
  4   <10 ms    <10 ms    <10 ms    www.test.com [30.30.30.100]

Trace complete.
c:₩>
```

그림 6. 서울 네트워크 장애 발생시 서울 네트워크의 사용자가 웹서버(www.test.com)로 trace route한 결과
Fig. 6 When Network impediment result of trace-route to web-server network user in seoul

Ⅵ. 결론

본 논문에서는 응용 어플리케이션을 웹 기반의 통합 아키텍처로 구현하고자 할 때 발생할 수 있는 이슈과제 중 URL 변경방지 제어 구현의 필요성, 비정상적인 데이터의 저장 방지, 사이트 장애시 업무의 연속성 보장 측면에서 가능한 구현방안을 기술적으로 도출해 보았다.

이슈 및 요구사항에 대해 도출된 내용을 요약하면 다음과 같다.

- 인터넷 상에서의 자원 접근 메커니즘인 URL을 클라이언트 측에서 소프트웨어적으로 변경방지를 제어하기 보다는 자원에 대한 접근을 사용자별 접근 레벨을 다르게 유지하며 접근 권한을 통합적으로 관리하여야 한다.
- 사용자들에 대한 완벽한 보안이 요구되는 인증 및 인가 절차를 거쳐 유효한 데이터에 접근하여 업무를 하여야 하며, 이를 위해서는 정책 저장소, 사용자 디렉토리, 계정 관리 로그를 포함한 정책 서버가 있어야 한다.
- 사이트 내의 구성요소들의 장애로 인해 업무의 중단을 최소화할 수 있으며, 관리자의 관리지침 및 업무 대행 지침이 좀 더 수월하고 간결하여야 한다. 본 논문에서는 각 지역 센터에 구축되어 있는 웹 서버, 웹 어플리케이션 서버, 데이터베이스 서버, 지능적 도메인 네임 서비스 서버, 정책서버 등 센터의 주요 구성요소들의 장애가 발생될 경우 관리자의 장애 대응 방안 및 장애 대응으로 인해 변경된 트래픽 경로 흐름에 대해 자세히 설명하였다.

이러한 요구사항을 충족할 수 있는 가능한 구현방안을 제시하였고, 전체 구성도와 구성 내역, 지능적인 도메인 네임 서비스 방안, 보안 정책 설계, 사용자 인증 방안, 공인 인증기관 연계 방안, 장애시 업무의 연속성 보장 방안 등으로 구분하여 전개하였다.

참고문헌

[1] The Global Market Forecast for Internet Usage and Commerce, Int'l. Data Corp., 1998

[2] Wing Lam, "Ensuring Business Continuity," IT Professional, p.19~25, 2002

[3] W. R. Stevens, TCP/IP Illustrated, Vol. 1: The Protocols, Reading, MA: Addison Wesley, 1994

[4] W. R. Stevens, TCP/IP Illustrated, Vol. 3, TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols, Reading, MA: Addison Wesley, 1996

[5] J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners Lee, "Hypertext Transfer Protocol HTTP/1.1," June 1999

[6] W. Tang, F. Du, M.W. Mutka, L.M. Ni, A. H. Esfahanian, "Supporting global replicated services by a routing metric aware DNS," WECWIS, p.67~74, 2000

[7] S. Wakid, J. Barkley, M. Skall, "Object retrieval and access management in electronic commerce,"

IEEE Communications Magazine, p.74~p.77, Sept. 1999

[8] Thomas P. Brisco, "DNS support for load balancing," RFC 1794, April 1995

[9] A. Shaikh, R.Tewari, M. Agrawal, "On the Effectiveness of DNS based Server Selection," INFOCOM 2001, Proceedings, IEEE, Vol. 3, 2001

[10] D. F. Ferraiolo, J. F. Barkley, and D. R. Kuhm, "A Role Based Access Control Model and Reference Implementation within a Corporate Intranet," ACM Trans. Info. Sys. Sec., vol. 1, no. 2, Feb. 1999

[11] 정연서, 박배욱, 손승원, 오창석, "안전한 인터넷을 위한 보안관리 시스템 설계", 한국컴퓨터정보학회 7권 3호, pp.75, 2002

[12] 이만희, 장행진, 박형우, 변옥환, "안전한 도메인 네임 시스템 관리를 위한 관리 정보 개체 정의에 관한 연구," 한국정보과학회, pp.323 325, 1998.

[13] 하창승, 조익성, "SHA 1 방식을 이용한 제한된 웹 페이지에 접근하기 위한 서버 독립적인 패스워드 인증방안", 한국컴퓨터정보학회 6권 4호, pp.148, 2001

[14] 김기윤, 나관식, "정보시스템에 대한 재난복구 Comdisco사의 실시간 재난복구서비스사례," 한국정보보호학회지, 6(1), pp. 103 116, 1996.

저 자 소 개

강 현 중

1980년 성균관대대학교 수학교육학(학사)

1986년 연세대학교대학원 전자계산학과(이학 석사)

1996년 2월 성균관대학교 대학원 정보공학(공학 박사)

1979년 11월~1982년 2월 한국과학기술연구소(KIST)연구원

1982년 3월~1989년 2월 한화종합금융(주) 전산팀장

1989년 3월~현재 서일대학 인터넷정보전공 부교수

<관심분야> 데이터통신, 프로그래밍언어

이 광 형

1998년 광주대학교 전자계산학과(이학사)

2002년 숭실대학교 대학원 컴퓨터학과(공학석사)

2005년 숭실대학교 대학원 컴퓨터공학과 (공학박사)

현 재 서일대학 인터넷 정보과 전임강사

<관심분야> 영상처리,에이전트시스템, 멀티미디어데이터검색, RFID 응용