Microsoft Windows Server 2003

Active Directory

그룹 정책 가이드

Microsoft


Microsoft
Windows Server 2003

저자의 글

관리되지 않는 클라이언트에 의한 바이러스 유포나 해킹에 대한 보안 위협이 커짐에 따라 많은 기업들이 클라이언트 보안에 관심을 가지게 되면서, Active Directory의 그룹 정책이 클라이언트의 보안을 강화하는 방안으로 제시되고 있습니다.
그룹 정책을 이용해서 관리자는 중앙에서 컴퓨터와 사용자에게 적용할 정책을 정의하고, 강제적으로 적용함으로써 보안을 강화할 수 있습니다.
이에 본 포켓 가이드는 Microsoft Windows Server 2003 그룹 정책의 개요부터 관리까지 관리자가 반드시 알아두어야 할 사항들에 대해 다루었습니다.
본 가이드의 내용을 기반으로 사용자들에게 신뢰할 수 있는 컴퓨팅 환경을 제공할 수 있기를 바랍니다.

저자 약력

최철원 / ㈜필라넷 수석 컨설턴트

- Active Directory 인프라 컨설팅 (두산, 삼성생명, 삼성토탈, 알리안츠 생명, 중소기업진흥공단, 한진중공업, 제일은행, 롯데마트 등)
- High Availability 컨설팅 및 기술 지원
- Microsoft .NET Advisor Windows Server 소모임 팀장
- 저서
  - Windows Server 2003 클러스터 설계와 구축

감수자의 글

수 많은 프로젝트를 경험한 베테랑 컨설턴트라 하더라도, 자신이 알고 있고 경험한 것을 정리하는 일은 결코 쉬운 일이 아닙니다. 때문에 Active Directory와 Clustering 분야에서 타의 추종을 불허하는 경험과 기술을 보유한 필자의 노하우가 이렇게 정리되었다는 것에 찬사를 보내고 싶습니다. 아울러 이렇게 정리된 본 가이드가 IT Pro 들에게 많은 도움이 될 것이라 확신합니다.

감수자 약력

이순신 / ㈜필라넷 이사

- Active Directory 및 Exchange Server 인프라 컨설팅
  (KTF, 국민은행, 신한금융지주, 호남석유화학, 제일은행, LG 화재 등)
- Exchange 사용자 그룹 시샵
- 저서
  - Janggoon' s Exchange 2000 Server
  - Exchange 2000 Server 포켓 컨설턴트(번역)

목차

그룹 정책 개요

Active Directory의 그룹 정책을 이용해서 관리자는 회사 네트워크에 존재하는 컴퓨터와 사용자를 관리할 수 있습니다. 그룹 정책은 사용자가 사용할 수 있는 프로그램, 사용자 데스크톱에 표시되는 프로그램, 시작 메뉴 옵션 등과 같이 관리자가 컴퓨터와 사용자를 관리하는 데 필요한 다양한 구성 요소를 정의합니다.

그룹 정책은 사용자 및 클라이언트 컴퓨터뿐 아니라 서버, 도메인 컨트롤러 및 관리 범위 안에 있는 다른 모든 Microsoft® Windows® 2000 이상의 운영 체제가 설치된 컴퓨터에 적용됩니다.

그룹 정책을 사용하여 관리자는 다음 작업을 수행할 수 있습니다.

- **보안 설정 지정** : 보안을 강화하기 위해 사용자 계정에 대한 암호 및 계정 잠금 정책 등을 설정하여 도메인에 모든 사용자에게 강제할 수 있습니다.

- **관리 템플릿을 통해 레지스트리 기반의 정책 관리** : 컴퓨터 구성의 관리 템플릿을 이용해서 시스템과 네트워크에 대한 제어가 가능합니다. 사용자 구성의 관리 템플릿을 이용해서 작업 표시줄 및 시작 메뉴, 바탕 화면, 제어판과 같이 다양한 사용자 데스크톱 환경에 대한 제어가 가능합니다. 컴퓨터 구성의 관리 템플릿은 컴퓨터가 시작할 때 다운로드 되어 HKEY_LOCAL_MACHINE 아래의 해당 레지스트리에 기록됩니다.

사용자 구성의 관리 템플릿은 사용자가 로그온 할 때 다운로드 되어 HKEY_CURRENT_USER 아래의 해당 레지스트리에 기록됩니다.

- **스크립트 할당** : 컴퓨터 시작 및 종료, 사용자 로그온 및 로그오프 때에 동작하여 원하는 작업을 수행하는 스크립트를 지정합니다.

- **폴더 리디렉션** : 내 문서 및 시작 메뉴와 같은 폴더를 로컬 컴퓨터의 Documents and Settings 폴더에서 네트워크 위치로 리디렉션 합니다.

- **소프트웨어 설정** : 관리자는 그룹 정책을 이용하여 중앙에서 사용자들이 사용할 소프트웨어 설치, 업데이트, 복구, 삭제를 제어할 수 있습니다.

그룹 정책 관리 콘솔(GPMC)

그룹 정책 관리 콘솔(GPMC)이 발표 되기 이전에 관리자는 그룹 정책을 관리하기 위해 Active Directory 사용자 및 컴퓨터, Active Directory 사이트 및 서비스, 그룹 정책 개체 편집기 그리고 정책 결과 집합 스냅인과 같은 다양한 도구들을 사용했습니다. 하지만 그룹 정책 관리 콘솔이 발표된 후에는 그룹 정책을 관리하는 대부분의 작업을 그룹 정책 관리 콘솔만으로 수행이 가능합니다.

그룹 정책 관리 콘솔(Group Policy Management Console)은 엔터프라이즈 환경하에서 복잡하고 다양한 그룹 정책을 보다 효율적으로 관리할 수 있도록 제공된 새로운 관리 도구입니다. 그룹 정책 관리 콘솔은 그룹 정책에 관련된 모든 관리 작업을 한 곳에서 수행할 수 있도록 다음과 같은 기능을 제공하여 그룹 정책 관리를 단순화 하였습니다.

- 그룹 정책을 보다 쉽게 생성/관리 할 수 있도록 단순화한 사용자 인터페이스(UI)
- 그룹 정책 개체(GPO)의 백업과 복원
- 그룹 정책 개체(GPO)의 복사와 가져오기
- 그룹 정책과 관련한 보안 정책을 쉽게 관리
- GPO 설정에 대한 HTML 레포팅과 정책 결과 집합 제공

GPMC 시스템 요구사항

GPMC는 Windows 2000과 Windows Server 2003 기반의 Active Directory 그룹 정책을 관리 할 수 있는 기능을 제공합니다. 관리자가 GPMC를 사용하기 위해서는 반드시 다음과 같은 운영체제에서 GPMC를 설치해야 합니다.

- Windows Server 2003

- Windows XP Professional SP1 & .Net Framework : 서비스 팩 1이 설치된 Windows XP Professional에는 Q326469 핫픽스를 설치해야 합니다. Q326469 핫픽스는 GPMC가 정상적으로 동작하기 위해 필요한 gpedit.dll(Version 5.1.2600.1186)을 업데이트합니다. GPMC의 각 언어 버전에는 해당 언어로 된 핫픽스가 포함되어 있고, 운영 체제의 언어가 GPMC의 언어와 일치할 경우에만 GPMC 설치 프로그램이 자동으로 핫픽스를 설치합니다. 만약 GPMC 언어 버전과 운영 체제의 언어가 다를 경우에는 자동으로 핫픽스가 설치되지 않기 때문에 GPMC 설치 프로그램이 중단되며 핫픽스를 설치해야만 계속 진행할 수 있습니다. Windows XP 서비스 팩 2에는 관련 핫픽스가 포함되어 있습니다.

GPMC 설치하기

Microsoft 다운로드 사이트에서 GPMC SP1를 다운로드 받은 후, 그룹 정책을 관리할 컴퓨터에 설치합니다. GPMC 설치 파일은 Windows Installer(MSI) 패키지로 구성되어 있기 때문에 쉽게 설치가 가능합니다.

[따라하기] GPMC 설치하기

다운로드 받은 GPMC SP1을 설치하는 과정은 다음과 같습니다.

1. Windows 탐색기에서 gpmc.msi 패키지를 더블 클릭합니다.
2. GPMC가 동작하기 위해서 MSXML4 SP2가 필요합니다. 예 버튼을 클릭하여 MSXML4 SP2를 설치합니다.

그림 1 MSXML4 SP2 설치

3. Group Policy Management Console with Service Pack 1 Setup Wizard가 실행됩니다. 간단한 도움말을 읽은 후, Next 버튼을 클릭합니다.
4. License Agreement 페이지가 나타납니다. I Agree 옵션을 선택한 후, Next 버튼을 클릭합니다.
5. 설치가 완료되면 Finish 버튼을 클릭하여, Setup Wizard를 종료합니다.

GPMC 설치 후에는 Active Directory 관리 도구의 사이트, 도메인 그리고 조직 구성 단위(OU) 등록 정보에서 그룹 정책 탭이 업데이트 됩니다. GPMC 설치 전에는 〈그림 2〉와 같이 그룹 정책 탭에서 그룹 정책을 관리할 수 있도록 관리 작업에 필요한 버튼들이 존재합니다.

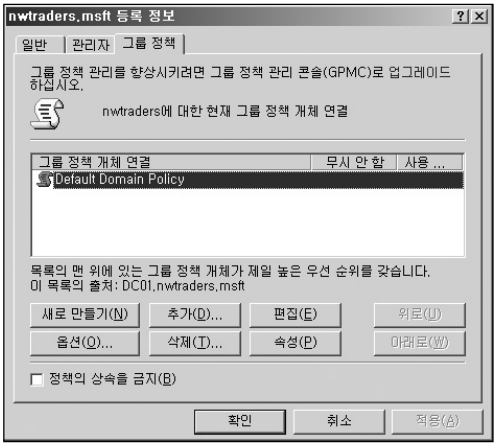

그림 2 GPMC 설치 전에 그룹 정책 탭

하지만 GPMC가 설치되면 기존에 그룹 정책 탭에서 수행하던 관리 작업들을 모두 GPMC에서 수행 가능하기 때문에 〈그림 3〉과 같이 바로 GPMC를 실행하는 버튼만 존재하도록 업데이트 됩니다.

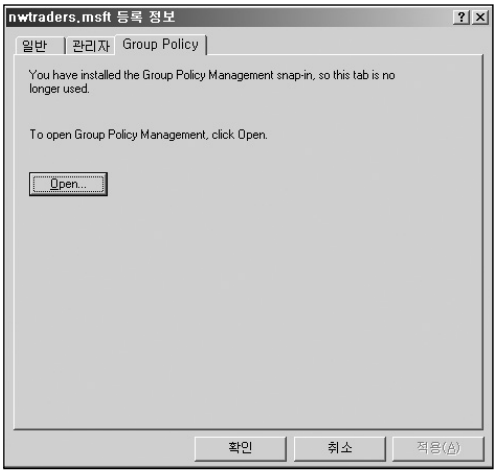

그림 3 GPMC 설치 후에 그룹 정책 탭

GPMC를 실행하기 위해 〈그림 3〉의 Open 버튼을 클릭해도 되지만, 다음과 같은 방법을 이용하면 보다 빠르게 GPMC를 실행할 수 있습니다.

- 시작 → 실행 메뉴를 선택한 후, gpmc.msc를 입력하여 GPMC를 실행합니다.
- 시작 메뉴나 제어판의 관리 도구 → Group Policy Management 메뉴를 선택하여 GPMC를 실행합니다.

GPMC는 다중 도메인 및 포리스트를 지원하기 때문에, 관리자는 엔터프라이즈 급의 복잡한 환경하에서 그룹 정책을 보다 쉽게 관리할 수 있습니다.

GPMC는 처음 시작할 때 현재 컴퓨터에 로그온 한 사용자를 포함하고 있는 도메인과 포리스트를 로딩합니다. GPMC를 종료하면, GPMC는 현재 설정을 자동으로 저장하여 향후 관리자가 다시 GPMC를 실행 했을 때 가장 최근의 상태로 복원합니다.

GPMC의 왼쪽 콘솔 트리에는 루트 노트로 Group Policy Management를 포함합니다. GPMC의 루트 노드 아래에는 〈그림 4〉와 같이 관리하는 포리스트 이름이 나타납니다. 포리스트 아래에는 네 개의 하위 노드(Domains, Sites, Group Policy Modeling, Group Policy Results)가 존재합니다.

하위 노드 중에 Group Policy Modeling은 Active Directory에 Windows Server 2003 스키마를 포함하고 있는 포리스트일 경우에만 나타납니다. Group Policy Modeling을 사용하기 위해서는 Windows Server 2003 이상이 동작중인 도메인 컨트롤러가 적어도 한 대 이상 포리스트에 존재해야 합니다.

그림 4 그룹 정책 관리 콘솔

포리스트 하위에 존재하는 네 개의 노드에 대한 자세한 설명은 다음과 같습니다.

- Domains : 이 노드의 하위에는 포리스트에 존재하는 도메인의 FQDN으로 표시되는 하위 노드가 존재합니다. 관리자는 포리스트에 존재하는 도메인 중에서 원하는 도메인만 하위 노드에 나타나도록 설정할 수 있습니다. Domains 노드를 마우스 오른쪽 버튼으로 클릭한 후, Show Domains 메뉴를 선택하면, 〈그림 5〉와 같은 대화 상자가 나타납니다. 예제 포리스트가 단일 도메인으로 구성되어 있어 〈그림 5〉의 도메인 목록에는 하나의 도메인만 나타나지만, 포리스트가 다중 도메인으로 구성되어 있다면 목록에 출력된 도메인 중에서 그룹 정책을 관리할 도메인만 선택할 수 있습니다. 여러 도메인을 선택하면 선택된 도메인의 FQDN으로 구성된 하위 노드들이 생성됩니다. 상위 도메인에 설정된 그룹 정책이 하위 도메인으로 상속되지 않기 때문에 포리스트의 도메인 구조와 상관없이 모든 선택된 도메인은 같은 하위 노드로 생성됩니다.

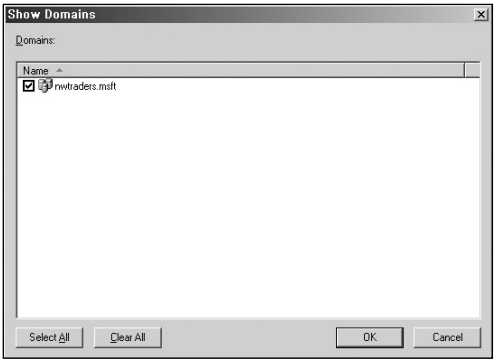

그림 5 도메인 선택

- Sites : 이 노드의 하위에는 포리스트에 존재하는 사이트를 표시하는 하위 노드가 존재합니다. 관리자는 포리스트에 존재하는 사이트 중에서 원하는 사이트만 하위 노드에 나타나도록 설정할 수 있습니다. Sites 노드를 마우스 오른쪽 버튼으로 클릭한 후, Show Sites 메뉴를 선택하면, 〈그림 6〉과 같은 대화 상자가 나타납니다. 포리스트가 다중 사이트로 구성되어 있다면 목록에 출력된 사이트 중에서 그룹 정책을 관리할 사이트만 선택할 수 있습니다. 여러 사이트를 선택하면 선택된 사이트의 이름으로 구성된 하위 노드들이 생성됩니다. 디폴트로 GPMC에서는 Sites 하위에 노드가 존재하지 않습니다. 이는 포리스트에 존재하는 많은 사이트 정보를 출력하기 위해 GPMC의 성능이 하락하는 것을 방지하기 위해서입니다.

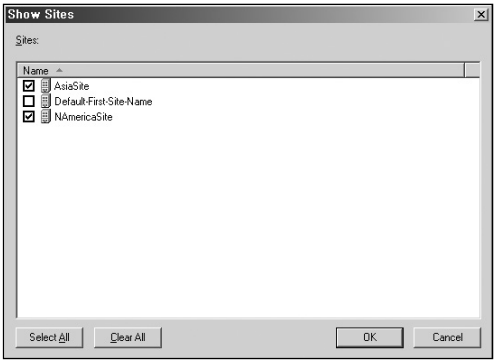

그림 6 사이트 선택

- Group Policy Modeling : 이 노드는 관리자가 그룹 정책 결과 집합(RSoP)의 계획 모드를 액세스할 수 있도록 합니다. 이 기능을 이용해서 관리자는 그룹 정책을 적용하기 전에 컴퓨터나 사용자에게 적용할 그룹 정책을 시뮬레이션 할 수 있습니다. 관리자는 포리스트에 존재하는 특정 컴퓨터나 사용자에게 적용될 그룹 정책을 시뮬레이션 하는 것이 가능합니다. 시뮬레이션은 Windows Server 2003이 설치된 도메인 컨트롤러에서만 동작하는 서비스에 의해 수행되기 때문에, 이 기능을 사용하기 위해서는 포리스트에 적어도 한 대 이상의 Windows Server 2003 운영 체제가 설치된 도메인 컨트롤러가 존재해야 합니다.

- Group Policy Results : 이 노드는 관리자가 그룹 정책 결과 집합(RSoP)의 로깅 모드에 액세스 할 수 있도록 합니다. 시뮬레이션 하는 계획 모드와 달리 로깅 모드는 포리스트에 존재하는 컴퓨터나 사용자에게 실제 적용된 그룹 정책에 대한 정보를 제공합니다. 직접 지정된 컴퓨터나 사용자에

게 질의를 하여, 기 적용된 그룹 정책 정보를 획득하기 때문에 Windows XP, Windows Server 2003 이상의 운영 체제가 설치된 컴퓨터에서만 그룹 정책 결과 집합 정보의 획득이 가능합니다.

[따라하기] GPMC에 포리스트 추가하기

GPMC를 이용해서 다중 포리스트를 관리하기 위해서는 다음과 같이 관리할 포리스트를 추가합니다.

1. GPMC의 콘솔 트리에서 루트 노드인 Group Policy Management를 마우스 오른쪽 버튼으로 클릭한 후, Add Forest 메뉴를 선택합니다.
2. Domain 입력창에 추가할 포리스트를 구성하는 도메인의 FQDN을 입력한 후, OK 버튼을 클릭합니다.

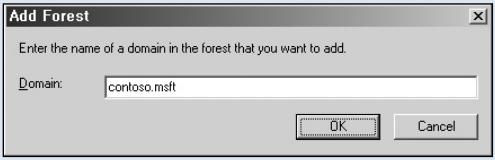

그림 7 포리스트 추가

도메인 노드

GPMC의 각 도메인 노드 하위에는 〈그림 8〉과 같이 다음과 같은 정보를 출력합니다.

- 도메인에 연결된 모든 GPO
- OU 구조와 각 OU에 연결된 GPO

- 도메인에 생성된 모든 GPO를 포함하고 있는 Group Policy Objects 노드
- 도메인에 생성된 모든 WMI Filter를 포함하고 있는 WMI Filters 노드

Group Policy Objects 노드는 도메인에 생성된 GPO의 목록을 출력합니다. 〈그림 8〉에서는 아직 GPO를 생성하지 않았기 때문에 도메인이 생성 될 때 자동으로 생성되는 Default Domain Controller Policy GPO와 Default Domain Policy GPO만이 출력되어 있는 것을 볼 수 있습니다.

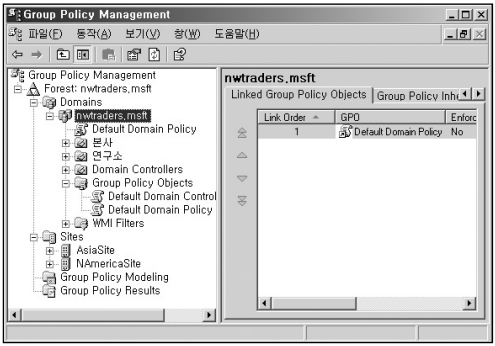

그림 8 도메인 하위 노드들

그룹 정책 개체(GPO)

컴퓨터와 사용자에게 적용할 정책 설정은 그룹 정책 개체(GPO)에 저장됩니다. 각 GPO에 대한 설정은 그룹 정책 개체 편집기를 사용하여 편집합니다. 일반적으로 그룹 정책 관리 콘솔(GPMC)를 설치한 후에는 GPMC에서 GPO를 수정할 때 그룹 정책 개체 편집기를 엽니다.

GPO는 다음과 같은 두 종류가 존재합니다.

- **로컬 GPO** : 로컬 GPO는 정책을 설정한 컴퓨터의 로컬 하드 디스크에 저장됩니다. 따라서 Active Directory 기반 GPO처럼 원하는 다양한 대상에게 설정된 정책을 적용할 수 없고, 오직 로컬 GPO가 설정된 개별 컴퓨터에만 적용됩니다. 로컬 GPO는 Active Directory 환경에서 가장 영향력이 적은 GPO이며, 로컬 GPO에서 설정할 수 있는 정책은 Active Directory 기반 GPO에 있는 정책의 일부만 가능합니다.

- **Active Directory 기반 GPO** : Active Directory 기반 GPO는 Active Directory 환경에서만 사용할 수 있습니다. Active Directory 기반 GPO는 도메인에 저장되며, 도메인의 모든 도메인 컨트롤러에 복제되어 GPO가 연결된 사이트, 도메인 또는 조직 구성 단위에 존재하는 사용자와 컴퓨터에 적용됩니다.

로컬 GPO

Windows 2000 이상의 운영 체제가 설치된 컴퓨터에는 각각 로컬 GPO가 하나씩 존재하며, 관리자는 Active Directory에 가입 여부와 상관없이 개별 컴퓨터에서 로컬 GPO를 설정 할 수 있습니다.

로컬 GPO는 Active Directory 기반 GPO에 비해 설정할 수 있는 정책 항목이 적습니다. 로컬 GPO는 〈표 1〉과 같이 소프트웨어 설치와 폴더 리디렉션 설정을 지원하지 않습니다.

그룹 정책	로컬 GPO 설정 가능 여부
보안 설정	설정 가능
관리 템플릿	설정 가능
소프트웨어 설치	설정 불가
스크립트	설정 가능
폴더 리디렉션	설정 불가
Internet Explorer 유지/보수	설정 가능

표 1 설정 가능한 로컬 GPO 정책

도메인 환경하에서 로컬 GPO 설정은 제일 먼저 적용됩니다. 사이트, 도메인 및 조직 구성 단위에 연결된 Active Directory 기반 GPO의 정책과 충돌이 발생하면 로컬 GPO의 정책은 덮어 쓰여지므로, 로컬 GPO는 Active Directory 환경에서는 가장 영향을 적게 주는 그룹 정책 개체입니다. 하지만 도메인에 가입한 컴퓨터가 아닌 경우에는 Active Directory 기반 GPO가 적용되지 않기 때문에, 관리자는 로컬 GPO를 이용해서만 개별 컴퓨터와 로그온 하는 사용자에게 영향을 미치는 정책을 설정할 수 있습니다.

로컬 GPO는 %WinDir%\System32\GroupPolicy 폴더 아래에 저장 되며, MMC의 그룹 정책 스냅인을 이용해서 수정할 수 있습니다.

[따라하기] 로컬 GPO 수정하기

로컬 GPO를 수정하는 과정은 다음과 같습니다.

1. 시작 → 실행 메뉴를 선택한 후, 다음 명령을 실행합니다.
   mmc
2. 파일 → 스냅인 추가/제거 메뉴를 선택합니다.
3. 스냅인 추가/제거 대화 상자가 나타나면, 추가 버튼을 클릭합니다.
4. 실행 가능한 독립 실행형 스냅인 목록에서 그룹 정책 스냅인을 선택한 후, 추가 버튼을 클릭합니다.
5. 그룹 정책 마법사가 실행됩니다. 수정할 그룹 정책 개체를 선택합니다. Active Directory 기반 GPO를 수정하기 위해서는 찾아보기 버튼을 클릭하여 수정할 GPO를 선택합니다. 로컬 GPO를 수정하기 위해서는 〈그림 9〉와 같이 그룹 정책 개체 입력창에 로컬 컴퓨터가 선택 되어 있는지를 확인한 후, 마침 버튼을 클릭합니다.

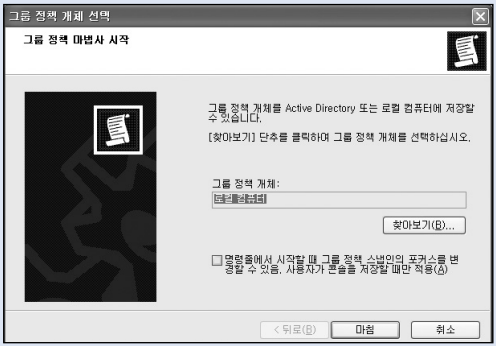

그림 9 그룹 정책 마법사

6. 닫기 버튼을 클릭한 후, 확인 버튼을 클릭하여 스냅인 추가/제거 대화 상자를 종료합니다.
7. 로컬 컴퓨터 정책 하위에서 원하는 로컬 GPO 설정을 수정합니다.

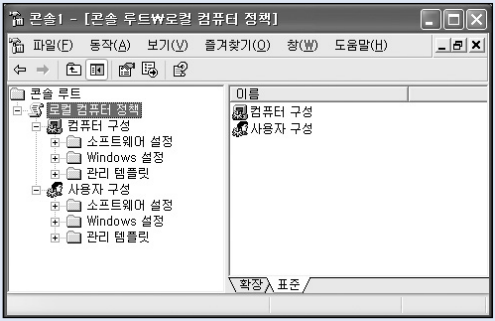

그림 10 로컬 GPO 수정

Active Directory 기반 GPO

일반적으로 그룹 정책은 Active Directory 기반 GPO를 의미합니다. Active Directory 기반 GPO를 이용해서 관리자는 Active Directory에 포함된 컴퓨터와 사용자에게 원하는 정책 설정을 적용할 수 있습니다.

컴퓨터와 사용자에게 정책을 적용하기 위해 관리자가 생성하고 수정하는 그룹 정책 개체(GPO)는 그룹 정책 컨테이너와 그룹 정책 템플릿, 두 곳에 정보를 저장합니다.

[그룹 정책 컨테이너]

그룹 정책 컨테이너(Group Policy Container)는 GPO의 속성을 저장하는 Active Directory 컨테이너입니다. 그룹 정책 컨테이너는 다음과 같은 속성을 저장합니다.

- **버전 정보** : 관리자의 의해 GPO의 정책 설정이 변경될 때마다 버전 정보가 업데이트 됩니다. 이 버전 정보를 이용해서 각 DC는 최신 그룹 정책 템플릿을 동기화 합니다.

- **상태 정보** : GPO의 사용 또는 사용 안 함 상태 여부를 저장합니다.

- GPO에 설정된 컴포넌트 목록

- **Sysvol 파일 시스템 경로** : 그룹 정책 템플릿을 저장하는 Sysvol 폴더의 UNC 경로를 저장합니다.

- **기능 버전** : GPO를 생성한 관리 도구의 버전 정보를 저장합니다.

[그룹 정책 템플릿]

그룹 정책 개체(GPO)는 도메인 컨트롤러의 Sysvol 하위 Policies 폴더에 그룹 정책 템플릿이라 불리는 폴더 구조 안에 그룹 정책 설정을 저장합니다. 그룹 정책 템플릿은 보안 정책, 관리 템플릿 기반의 정책 설정들, 소프트웨어 설치 정보들 그리고 각종 스크립트 파일들을 저장하는 컨테이너로써 컴퓨터와 사용자에게 적용할 실제 정책들을 저장하고 있습니다.

새로운 GPO를 생성하면, 그룹 정책 설정을 저장하기 위한 그룹 정책 템플릿의 폴더 이름으로 GUID가 부여됩니다. 예를 들어 nwtraders.msft 도메인에 새로운 GPO를 생성하면 새로 생성되는 GPO의 설정들을 저장하기 위한 그룹 정책 템플릿 폴더가 다음과 같이 생성됩니다. (GUID는 샘플입니다.)

%systemroot%\SYSVOL\sysvol\nwtraders.msft\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}

[Gpt.ini 파일]
그룹 정책 템플릿 폴더의 루트에는 Gpt.ini 파일이 존재하며, 다음과 같은 두 개의 엔트리 정보를 저장하고 있습니다.

Version=0 //GPO의 버전
DisplayName=본사 정책 //GPO의 이름

[그룹 정책 템플릿 하위 폴더들]
그룹 정책 템플릿 폴더의 하위에는 컴퓨터와 사용자에게 적용할 정책 설정을 저장하는 다음과 같은 폴더들이 존재합니다.

- Adm : GPO의 레지스트리 기반 정책을 정의하고 있는 관리 템플릿 파일(.adm)이 저장되어 있습니다.
- Machine : Machine 폴더에는 컴퓨터에게 적용 될 레지스트리 설정을 저장하는 Registry.pol 파일이 존재합니다. 컴퓨터가 시작될 때, Registry.pol 파일이 컴퓨터에 다운로드 되어 레지스트리의 HKEY_LOCAL_MACHINE에 적용됩니다.

GPO의 컴퓨터 정책 설정에 따라 Machine 폴더 하위에는 정책 설정을 저장하는 다음과 같은 폴더들이 존재합니다.

- Applications : Windows Installer가 사용하는 .aas 파일을 저장합니다. .aas 파일에는 컴퓨터에 설치될 소프트웨어에 대한 정보를 저장하고 있습니다.
- Microsoft\Windows NT\Secedit : Windows 2000 도메인 컨트롤러의 기본 보안 설정을 저장하는 Gpttmpl.inf 파일이 존재합니다.
- Scripts\Startup : 컴퓨터가 시작할 때 실행되는 스크립트를 저장합니다.
- Scripts\Shutdown : 컴퓨터가 종료할 때 실행되는 스크립트를 저장합니다.

• User : User 폴더에는 사용자에게 적용 될 레지스트리 설정을 저장하는 Registry.pol 파일이 존재합니다. 사용자가 컴퓨터에 도메인 계정을 이용해서 로그온 할 때, Registry.pol 파일이 컴퓨터에 다운로드 되어 레지스트리의 HKEY_CURRENT_USER에 적용됩니다.

GPO의 사용자 정책 설정에 따라 User 폴더 하위에는 정책 설정을 저장하는 다음과 같은 폴더들이 존재합니다.

- Applications : Windows Installer가 사용하는 .aas 파일을 저장합니다. .aas 파일에는 사용자에게 설치될 소프트웨어에 대한 정보를 저장하고 있습니다.
- Documents and Settings : 폴더 리디렉션에 대한 정책 설정을 저장하는 Fdeploy.ini 파일이 존재합니다.
- Microsoft\RemoteInstall : 원격 설치 서비스를 이용해서 클라이언트에 운영 체제를 설치하기 위해 필요한 사용자 옵션을 저장하는 OSCfilter . ini 파일이 존재합니다.

- Microsoft\IEAK : Internet Explorer 유지/보수에 설정된 정책을 저장합니다.
- Scripts\logon : 사용자가 로그온 할 때 실행되는 스크립트를 저장합니다.
- Scripts\logoff : 사용자가 로그오프 할 때 실행되는 스크립트를 저장합니다.

GPO가 생성될 때, 그룹 정책 템플릿 폴더의 Adm, Machine, User 폴더는 같이 생성됩니다. 하지만 그 하위 폴더는 컴퓨터나 사용자에게 적용할 정책이 설정될 때만 생성됩니다.

[Registry.pol 파일]

그룹 정책의 관리 템플릿에 설정된 정책은 그룹 정책 템플릿의 Registry.pol이라는 유니코드 파일에 저장됩니다. 그룹 정책 템플릿에는 두 개의 Registry.pol이 생성되는데 하나는 Machine 폴더에 존재하며, 그룹 정책의 컴퓨터 구성\관리 템플릿에서 설정한 정책을 저장합니다. Machine 폴더에 존재하는 Registry.pol 파일은 컴퓨터가 시작될 때 다운로드 되어 레지스트리의 HKEY_LOCAL_MACHINE에 설정이 반영됩니다.

또 다른 하나는 User 폴더에 존재하며, 그룹 정책의 사용자 구성\관리 템플릿에서 설정한 정책을 저장합니다. User 폴더에 존재하는 Registry.pol 파일은 사용자가 도메인 계정으로 컴퓨터에 로그온 할 때 다운로드 되어 레지스트리의 HKEY_CURRENT_USER에 설정이 반영됩니다.

GPO 복제

하나 이상의 도메인 컨트롤러로 구성된 도메인에서는 GPO가 모든 도메인 컨트롤러로 복제되는데 시간이 필요합니다. 도메인 컨트롤러가 상호 저속 네트워크로 연결되어 있다면 변경된 그룹 정책의 복제는 지연될 것입니다.

앞에서 언급했듯이 GPO는 Active Directory와 도메인 컨트롤러의 Sysvol 폴더에 각각 필요한 정보를 따로 저장하고 있지만, 그룹 정책 관리 콘솔(GPMC)나 그룹 정책 개체 편집기는 GPO를 하나의 유닛으로 관리합니다. 예를 들어 관리자가 GPMC를 이용해서 GPO에 사용 권한을 설정한다면, GPMC는 내부적으로 GPO와 관련된 Active Directory와 Sysvol 폴더에 관련 사용 권한을 설정합니다. 따라서 GPMC나 그룹 정책 개체 편집기가 아닌 다른 관리 도구를 이용해서 Active Directory나 Sysvol에 개별적으로 GPO를 수정하는 것은 권장하지 않습니다.

GPO를 구성하는 정보를 저장하는 Active Directory와 Sysvol 폴더는 변경된 GPO의 설정을 다른 도메인 컨트롤러에 복제하기 위해 서로 다른 복제 방식을 사용합니다. Active Directory에 저장된 그룹 정책 컨테이너는 Active Directory 복제에 의해 다른 도메인 컨트롤러로 복제되는 반면에, Sysvol 폴더에 저장된 그룹 정책 템플릿은 파일 복제 서비스(FRS)에 의해 다른 도메인 컨트롤러로 복제됩니다.

Active Directory와 파일 복제 서비스의 복제 방식에 차이가 있기 때문에, 그룹 정책 컨테이너와 그룹 정책 템플릿은 시간차를 두고 도메인 컨트롤러로 복제될 수 있습니다. 예를 들어 DC01에서 GPO가 수정되었다면, Active Directory 복제에 의해 DC02로 수정된 그룹 정책 컨테이너가 복제됩니다. 하지만 DC02의 파일 복제 서비스에 오류가 발생한다면, 오류가 정정되기 전까

지 그룹 정책 템플릿은 DC02의 Sysvol 폴더로 복제가 지연됩니다.

관리 템플릿, 스크립트, 폴더 리디렉션 그리고 보안 설정과 같이 오직 한 곳의 저장소(Active Directory 또는 Sysvol)에만 데이터를 저장하는 그룹 정책 설정들은 복제 지연의 따른 이슈가 없습니다. 하지만 소프트웨어 설치와 같이 양 저장소에 데이터를 저장하는 그룹 정책 설정의 경우에는 Active Directory와 Sysvol의 데이터가 동시에 복제되지 않을 확률을 항상 가지고 있습니다.

예를 들어, 소프트웨어 설치 같은 경우에는 Sysvol 폴더에 Windows Installer가 사용하는 .aas 파일을 저장합니다. 그리고 Active Directory에는 Windows Installer 패키지 설정 정보를 저장합니다. 만일 먼저 Sysvol 폴더에 .ass 파일이 복제되고, Active Directory에는 Windows Installer 패키지 설정 정보가 복제되지 않으면 소프트웨어 설치는 동작하지 않습니다. 반면에 Active Directory에 Windows Installer 패키지 설정 정보는 복제되었지만, Sysvol 폴더에는 .ass 파일이 복제되지 않았다면 소프트웨어 설치가 시도되다가 실패합니다. 차후에 그룹 정책이 적용될 때 다시 소프트웨어 설치를 시도합니다.

복제 지연에 의해 발생하는 문제는 컴퓨터나 사용자에게 정책을 적용할 때만 발생하는 것이 아니라, 관리 작업을 수행할 때도 발생할 수 있습니다. 왜냐하면 관리자가 DC01에서 GPO를 변경한 후, 바로 DC02에 연결하여 같은 GPO를 열었을 때 복제가 아직 안 되었다면 오류가 발생할 수 있습니다.

따라서 그룹 정책을 관리하기 위해 사용하는 그룹 정책 관리 콘솔(GPMC)이나 그룹 정책 개체 편집기와 같은 관리 도구는 동기화 지연에 의해 발생할 수 있는 이슈를 제거하기 위해 도메인의 PDC 에뮬레이터 작업 마스터로 동작하는 도메인 컨트롤러에서만 연결하여 GPO를 수정합니다.

관리자가 어떤 도메인 컨트롤러에 연결해서 GPMC나 그룹 정책 개체 편집기를 실행하더라도 항상 도메인의 PDC 에뮬레이터로 동작하는 도메인 컨트롤러의 Active Directory와 Sysvol에서 GPO 관련 설정을 수정합니다. PDC 에뮬레이터에서 수정된 GPO 설정은 도메인을 구성하는 다른 도메인 컨트롤러로 복제됩니다.

필요하다면 GPMC가 GPO를 항상 수정하는 기본 도메인 컨트롤러를 PDC 에뮬레이터에서 다른 도메인 컨트롤러로 수정하는 것이 가능합니다. 만일 관리자가 PDC 에뮬레이터와 저속 네트워크로 연결되어 있는 원격 사이트에 있다면, 원활한 GPO 관리를 위해 관리자는 같은 네트워크에 존재하는 도메인 컨트롤러를 GPMC가 항상 GPO를 수정하는 기본 도메인 컨트롤러로 설정할 수 있습니다.

[따라하기] GPMC가 GPO를 수정하는 기본 도메인 컨트롤러 변경하기

GPMC가 GPO를 항상 수정하는 기본 도메인 컨트롤러를 PDC 에뮬레이터에서 다른 도메인 컨트롤러로 변경하는 과정은 다음과 같습니다.

1. GPMC의 콘솔 트리에서 Sites를 마우스 오른쪽 버튼으로 클릭한 후, Change Domain Controller 메뉴를 선택합니다.
2. Change Domain Controller 대화 상자가 나타납니다. 특정 도메인 컨트롤러를 기본 도메인 컨트롤러로 수정하기 위해서 This domain controller 옵션을 선택합니다.
3 Domain Controllers 목록에서 GPMC가 GPO를 항상 수정하는 기본 도메인 컨트롤러로 설정할 도메인 컨트롤러를 선택한 후, OK 버튼을 클릭합니다.

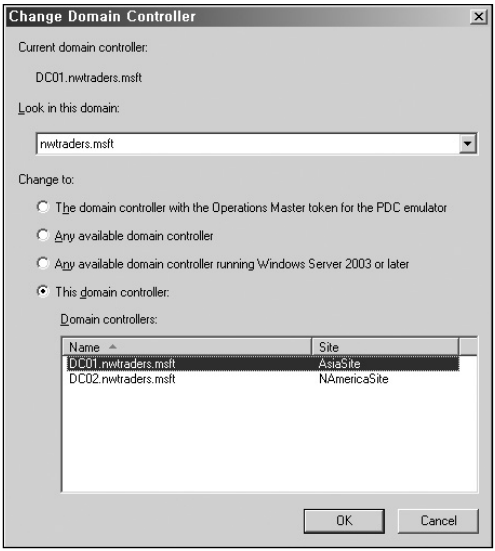

그림 11 도메인 컨트롤러 변경

〈그림 11〉에서 보는 것처럼 GPMC는 다음과 같은 네 가지 옵션을 제공합니다.

- The one with the Operations Master token for the PDC emulator : 디폴트로 선택되어 있으며 가장 권장 옵션입니다. 이 옵션을 선택하면 GMPC는 항상 PDC 에뮬레이터로 동작하는 도메인 컨트롤러에 연결하여 GPO를 수정합니다.

- Use any available domain controller : 이 옵션을 선택하면 GPMC는 사용 가능한 아무 도메인 컨트롤러에나 연결하여 GPO를 수정합니다. 가장 권장하지 않는 옵션입니다.
- Use any available domain controller that is running Windows Server 2003 or later : 이 옵션은 소프트웨어 설치 설정을 포함하고 있던 GPO를 복원할 때 사용하면 유용합니다. 가능하다면 소프트웨어 설치 설정을 포함하고 있던 GPO를 복원할 경우에는 Windows Server 2003 도메인 컨트롤러에서 복원할 것을 권장합니다.
- This domain controller : 이 옵션을 이용해서 관리자는 원하는 특정 도메인 컨트롤러에서 항상 GPO 설정이 수정되도록 기본 도메인 컨트롤러를 변경할 수 있습니다.

GPO 생성과 수정

Active Directory 환경에서 원하는 컴퓨터와 사용자에게 그룹 정책을 적용하기 위해서는 먼저 GPO를 생성합니다. 새로 생성된 GPO에는 아무런 정책이 설정되어 있지 않으므로, 그룹 정책 개체 편집기를 이용해서 컴퓨터와 사용자에게 적용하고자 하는 정책을 설정해야 합니다.

다음과 같이 GPMC에서 다양한 방법을 이용해서 GPO를 생성할 수 있습니다.

- 도메인이나 조직 구성 단위(OU)를 마우스 오른쪽 버튼으로 클릭한 후, Create and Link a GPO Here 메뉴를 선택합니다. 이 메뉴를 선택하면 새로운 GPO를 생성하면서 동시에 선택한 도메인이나 조직 구성 단위에 GPO를 연결합니다.

- 새 GPO를 생성할 도메인의 Group Policy Objects 노드를 마우스 오른쪽 버튼으로 클릭한 후, New 메뉴를 선택합니다. 이 메뉴를 선택하면 연결되지 않은 GPO를 생성합니다.
- 스크립트를 이용해서 새 GPO를 생성합니다. GPMC에서는 명령 프롬프트에서 새 GPO를 생성할 수 있도록 예제 스크립트로 CreateGPO.wsf 스크립트를 제공합니다. CreateGPO.wsf 스크립트를 이용해서 nwtraders.msft에 본사 정책 GPO를 생성하는 방법은 다음과 같습니다.
  cscript CreateGPO.wsf "본사 정책" nwtraders.msft
- GPO 복사를 이용해서 원본과 동일한 정책이 설정된 새 GPO를 생성합니다.

관리자는 그룹 정책 개체 편집기를 이용해서 컴퓨터와 사용자에게 적용하고자 하는 정책을 설정 합니다. 관리자는 도메인의 Group Policy Objects 노드 아래에서 수정하고자 하는 GPO를 마우스 오른쪽 버튼으로 클릭한 후, Edit 메뉴를 선택합니다. 이 메뉴를 선택하면 선택된 GPO의 설정을 포함하는 그룹 정책 개체 편집기가 실행됩니다.

그룹 정책 개체 편집기는 그룹 정책 개체(GPO)의 설정들을 편집할 때 사용하는 MMC 스냅인입니다. 그룹 정책 개체 편집기는 관리 템플릿, 스크립트, 보안 설정, 소프트웨어 설정, 폴더 리디렉션, 원격 설치 서비스 그리고 Internet Explorer 유지/보수와 같은 다양한 정책 설정들을 수정할 수 있습니다.

그룹 정책 스냅인 네임스페이스

그룹 정책 개체 편집기의 루트 노드는 GPO의 이름과 GPO가 생성된 도메인의 이름으로 구성된 다음과 같은 포맷으로 출력됩니다.

GPO이름 [도메인 FQDN] 정책

그림 12 그룹 정책 개체 편집기

그룹 정책 개체 편집기의 루트 노드 아래는 컴퓨터를 시작(부팅)할 때 컴퓨터에 적용되는 설정을 유지하는 컴퓨터 구성과 로그온 할 때 사용자에게 적용되는 설정을 유지하는 사용자 구성으로 나누어집니다.

컴퓨터 구성과 사용자 구성 하위에는 세 개의 노드(소프트웨어 설정, Windows 설정, 관리 템플릿)로 구성됩니다. 이 세 노드의 하위에는 컴퓨터와 사용자에게 적용할 다양한 그룹 정책을 포함하는 확장 스냅인들로 구성되어 있습니다. 확장 스냅인으로 관리 템플릿, 스크립트, 보안 설정, 소프트웨어 설치, 폴더 리디렉션, 원격 설치 서비스, Internet Explorer 유지/보수 노드들이 〈그림 12〉와 같이 존재합니다.

확장 스냅인은 하위 노드로 또 다른 확장 스냅인을 가질 수 있습니다. 예를 들어 보안 설정 스냅인은 하위에 여러 개의 확장 스냅인을 포함하고 있습니다.

디폴트로 제공하는 정책 외에 추가하고자 하는 정책이 필요하다면, 개발자는 그룹 정책 개체 편집기에 확장 스냅인을 추가하여 정책을 추가할 수 있습니다. 관리 템플릿의 경우에는 .adm 파일을 수정하여 확장이 가능합니다.

기본적으로 그룹 정책 개체 편집기가 시작할 때, 사용 가능한 모든 확장 스냅인이 로딩됩니다. 원한다면 관리자는 그룹 정책의 [사용자 구성\관리 템플릿\Windows 구성 요소\Microsoft Management Console\제한된\허가된 스냅인\그룹 정책\그룹 정책 스냅인 확장 항목]을 이용해 원하는 확장 스냅인만 로딩되도록 제어가 가능합니다.

Windows Server 2003 Active Directory에서는 다양한 정책 설정을 위해 다음과 같은 주요 확장 스냅인을 제공합니다.

- **관리 템플릿** : 관리 템플릿 확장 스냅인은 Windows 2000 이상 운영 체제의 시스템 컴포넌트 뿐만 아니라 각종 응용 프로그램에서 제공하는 다양한 레지스트리 기반 정책 설정을 제공합니다. 관리자는 관리 템플릿에서 제공하는 정책을 이용해서 사용자 데스크탑 환경, 운영 체제 컴포넌트 그리고 레지스트리 기반 정책을 제공하는 응용 프로그램까지 제어가 가능합니다. 그룹 정책 개체 편집기는 adm 파일의 정보를 로딩해서 설정 가능한 레지스트리 기반 정책을 출력합니다.

- **보안 설정** : 보안 설정 확장 스냅인은 컴퓨터와 사용자에게 적용할 다양한 보안 정책을 제공합니다. 관리자는 도메인 계정 정책, 무선 네트워크 정책, 공개키 정책, 소프트웨어 제한 정책, IP 보안 정책과 같은 보안 정책 설정이 가능합니다.

- **소프트웨어 설정** : 소프트웨어 설정 확장 스냅인을 이용하면 관리자는 중앙에서 소프트웨어 관리(소프트웨어 설치, 업데이트, 복구, 삭제)를 수행할 수 있습니다. 컴퓨터 구성\소프트웨어 설정을 이용해서 해당 컴퓨터에 로그온 하는 모든 사용자에게 적용되는 소프트웨어 설정 관리가 가능합니다. 사용자 구성\소프트웨어 설정을 이용해서 로그온 하는 컴퓨터에 상관없이 사용자에게 적용되는 소프트웨어 설정 관리가 가능합니다.

- **스크립트** : 컴퓨터 시작 및 종료, 사용자 로그온 및 로그오프 때에 동작하여 원하는 작업을 수행하는 스크립트를 지정합니다. 스크립트는 Windows Script Host에서 지원하는 VBScript, JavaScript, MS-DOS 배치 파일(.bat, .cmd)과 같은 개발 언어를 이용해서 작성해야 합니다.

- **원격 설치 서비스** : 원격 설치 서비스 확장 스냅인을 이용해서 관리자는 클라이언트의 원격 설치 동작 방식을 제어할 수 있습니다.

- **Internet Explorer 유지/보수** : Internet Explorer 유지/보수 확장 스냅인을 이용해서 관리자는 클라이언트에서 동작하는 Internet Explorer의 동작 및 구성을 관리할 수 있습니다. 관리자가 Windows 9x와 Windows NT 4.0이 설치된 클라이언트의 Internet Explorer 환경을 구성할 수 있도록, 설정된 정책을 각 운영 체제에서 지원하는 .ins나 .cab 파일 포맷으로 내보내는 기능도 제공합니다.

- **폴더 리디렉션** : 폴더 리디렉션 확장 스냅인은 사용자 파일이나 데스크탑 환경을 저장하는 주요 폴더를 로컬 컴퓨터의 Documents and Settings 폴더에서 지정한 네트워크 위치로 리디렉션 하는 기능을 제공 합니다. 리디렉션 가능한 주요 폴더는 Application Data, 바탕 화면, 내 문서, 시작 메뉴입니다.

그룹 정책 확장 스냅인

컴퓨터와 사용자에게 적용할 그룹 정책의 주요 설정들은 모두 그룹 정책 확장 스냅인을 통해 제공됩니다. 사용 가능한 모든 확장 스냅인은 그룹 정책 개체 편집기가 시작할 때 로딩됩니다. 원한다면 관리자는 그룹 정책의 [사용자 구성\관리 템플릿\Windows 구성 요소\Microsoft Management Console\제한된\허가된 스냅인\그룹 정책\그룹 정책 스냅인 확장 항목]을 이용해 원하는 확장 스냅인만 로딩되도록 제어가 가능합니다.

그룹 정책은 주요 정책 설정을 제공하는 다음과 같은 확장 스냅인을 제공합니다.

관리 템플릿

관리자는 관리 템플릿을 이용해서 레지스트리 설정을 관리할 수 있습니다. Active Directory에서는 그룹 정책에서 제어할 수 있는 다양한 레지스트리 설정을 정의한 관리 템플릿 파일(.adm)을 제공합니다.

관리 템플릿 파일은 다음과 같이 두 폴더에 저장됩니다.

- %WinDir%\inf
- Sysvol의 GPO 템플릿 하위에 adm 폴더

관리 템플릿 파일은 그룹 정책 개체 편집기에 레지스트리 정책을 어떻게 설정할 수 있는지를 정의한 카테고리들로 구성된 유니코드 파일입니다. 또한 설정된 레지스트리 정책이 클라이언트에 다운로드 되어 적용 될 레지스트리 위치 정보와 설정 값의 최대, 최소 범위, 디폴트 값, 적용 가능한 운영 체제 등

다양한 정보를 저장하고 있습니다.

관리 템플릿 파일은 컴퓨터나 사용자에게 적용할 실제 정책 설정 값을 저장하는 것이 아니라, 그룹 정책 개체 편집기에서 사용할 사용자 인터페이스, 설정 이름 및 도움말 등을 저장하고 있는 템플릿 파일입니다. 관리자가 그룹 정책 개체 편집기를 이용해서 컴퓨터와 사용자에게 적용하도록 설정한 레지스트리 정책은 Sysvol 폴더의 Registry.pol 파일에 저장되어, 컴퓨터가 시작할 때 또는 사용자가 로그온 할 때 다운로드 되어 적용됩니다.

또한 관리 템플릿 파일은 각 레지스트리 정책 별로 지원 가능한 운영 체제 정보를 저장하고 있습니다. 따라서 클라이언트에 다운로드 된 레지스트리 설정이 클라이언트의 운영 체제를 지원하지 않을 경우에는 해당 레지스트리 설정은 무시됩니다.

관리 템플릿은 디폴트로 로딩한 관리 템플릿 파일의 모든 레지스트리 정책을 출력합니다. 만약 특정 운영 체제를 지원하는 레지스트리 정책만 화면에 출력되게 하거나, 관리자에 의해 설정된 레지스트리 정책만 화면에 출력되게 하려면 필터링을 사용하면 됩니다.

[따라하기] 관리 템플릿 정책 필터링 하기

그룹 정책 개체 편집기를 이용해서 관리 템플릿 정책을 필터링 하는 방법은 다음과 같습니다.

1. 그룹 정책 개체 편집기의 콘솔 트리에서 관리 템플릿을 마우스 오른쪽 버튼으로 클릭한 후, 보기 → 필터 사용 중 메뉴를 선택합니다.

2. 특정 운영 체제나 소프트웨어가 설치되어야만 적용되는 레지스트리 정책을 필터링 하기 위해 요구 사항 정보로 필터링 옵션을 선택한 후, 표시할 항목 선택 목록에서 원하는 요구 사항을 선택합니다.
   관리자에 의해 설정된 레지스트리 정책만 화면에 출력되게 하려면 구성된 정책 설정만 표시 옵션을 선택합니다.
   원하는 필터링 옵션을 선택하였으면 확인 버튼을 클릭합니다.

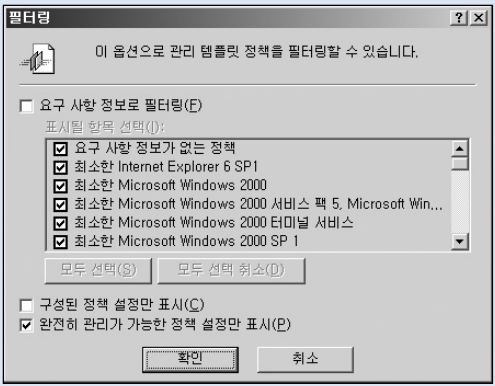

그림 13 필터링 옵션 선택

관리 템플릿 파일은 예전 버전의 레지스트리 정책을 포함하고 있으며, 향후 운영 체제가 버전업 되고, 서비스 팩이 발표될 때마다 계속 최신의 레지스트리 정책을 포함하게 될 것입니다. 가급적이면 최신 관리 템플릿 파일을 %WinDir%\inf 폴더에 저장하고 있는 도메인 컨트롤러에서 GPO를 생성하고 수정할 것을 권장합니다.

Windows Server 2003은 관리 템플릿 노드에 출력되는 모든 레지스트리 정책을 저장하고 있는 다음과 같은 관리 템플릿 파일을 포함하고 있습니다. 〈표 2〉의 관리 템플릿 파일들은 그룹 정책 개체 편집기기 실행될 때 자동으로 로딩됩니다.

관리 템플릿 파일	레지스트리 정책	지원 운영 체제
System.adm	운영 체제를 구성하는 정책들	Windows 2000 Windows Server 2003
Inetres.adm	Internet Explorer를 구성하는 정책들	Windows 2000 Windows Server 2003
Conf.adm	NetMeeting v3을 구성하는 정책들	Windows 2000 Windows Server 2003. 이 도구는 Windows XP 64-Bit Edition과 Windows Server 2003 64-Bit Edition 을 지원하지 않습니다.
Wmplayer.adm	Windows Media Player을 구성하는 정책들	Windows XP Windows Server 2003. 이 도구는 Windows XP 64- Bit Edition과 Windows Server 2003 64-Bit Edition 을 지원하지 않습니다.
Wuau.adm	Windows Update를 구성하는 정책들	Windows 2000 SP3 Windows XP SP1 Windows Server 2003

표 2 관리 템플릿 파일

컴퓨터 구성\관리 템플릿에 설정한 레지스트리 정책은 컴퓨터가 시작할 때 다운로드 되어 다음과 같은 레지스트리 하위에 저장됩니다.

- HKLM\Software\Policies
- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies

사용자 구성\관리 템플릿에 설정한 레지스트리 정책은 사용자가 로그온 할 때 다운로드 되어 다음과 같은 레지스트리 하위에 저장됩니다.

- HKCU\Software\Policies
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies

다운로드 되어 해당 레지스트리에 저장된 정책은 Administrator 권한이 있는 관리자만이 수정할 수 있습니다. 관리자가 관리 템플릿의 정책을 수정하면 해당 레지스트리 하위 트리를 모두 지우고, 다시 수정된 정책을 다운로드 하여 레지스트리 정책 값을 저장합니다.

새 관리 템플릿(.adm) 파일을 생성하는 것이 가능합니다. 그룹 정책을 지원하는 응용 프로그램을 사용한다면, 그룹 정책 개체 편집기에서 정책을 설정할 수 있도록 UI와 응용 프로그램이 사용할 레지스트리 키 정보를 제공하는 새 관리 템플릿 파일을 추가해야 합니다.

다음은 관리 템플릿 파일의 예제입니다.

```
CLASS USER

CATEGORY "확장 레지스트리 정책"

  POLICY "확장한 레지스트리 정책입니다."
    KEYNAME "Software\Policies\Sample"

    PART "설정값:" NUMERIC REQUIRED SPIN 1
      VALUENAME "SampleValue"
      DEFAULT 1
      MAX   10
      MIN   0
    END PART
  END POLICY
END CATEGORY
```

예제 관리 템플릿 파일에서 사용한 각 요소들에 대한 설명은 다음과 같습니다.

- CLASS USER : 사용자 구성\관리 템플릿을 확장함을 의미하며, 확장된 레지스트리 정책들은 다운로드 되어 HKEY_CURRENT_USER에 적용됩니다. 컴퓨터 구성\관리 템플릿을 확장하기 위해서는 CLASS MACHINE을 사용합니다.

- CATEGORY : 관리 템플릿 아래에 노드 이름으로 사용합니다.

- POLICY : 확장 레지스트리 정책의 이름으로 사용합니다.
- KEYNAME : 설정된 레지스트리 정책이 클라이언트에 다운로드 되어 저장될 레지스트리 경로를 지정합니다.
- PART : 확장 레지스트리 정책을 그룹 정책 개체 편집기에서 설정할 수 있도록 UI를 정의합니다. 예제에서는 스핀 버튼을 이용해서 값을 설정하도록 구성합니다.
- VALUENAME : 설정된 레지스트리 정책이 클라이언트에 다운로드 되어 저장될 레지스트리 이름을 지정합니다.
- DEFAULT : 확장 레지스트리 정책을 설정할 때 디폴트로 입력될 값을 지정합니다
- MAX : 최대로 입력할 수 있는 값을 지정합니다.
- MIN : 최소로 입력할 수 있는 값을 지정합니다.
- END : 각 PART, POLICY, CATEGORY의 완료를 의미합니다.

PART의 경우에는 EDITTEXT, NUMERIC, CHECKBOX, COMBOBOX, DROPDOWNLIST, LISTBOX를 사용해서 다양한 UI로 설정 값을 입력할 수 있도록 설정이 가능합니다. 관리 템플릿 파일을 확장하는 방법에 대한 자세한 정보는 다음 문서를 참고하기 바랍니다.

http://www.gpanswers.com/book/download.php?file=downloads/4447_web01.pdf

[따라하기] 관리 템플릿 확장하기

확장할 레지스트리 정책을 저장한 관리 템플릿 파일을 이용해서 관리 템플릿을 확장하는 과정은 다음과 같습니다.

1. 확장할 레지스트리 정책을 저장한 관리 템플릿 파일을 도메인 컨트롤러의 %WinDir%\inf 폴더에 복사합니다.
2. GPMC의 Group Policy Objects 노드 아래에서 확장 레지스트리 정책을 사용할 GPO를 마우스 오른쪽 버튼으로 클릭한 후, Edit 메뉴를 선택합니다.
3. 그룹 정책 개체 편집기의 콘솔 트리에서 컴퓨터 구성\관리 템플릿을 마우스 오른쪽 버튼으로 클릭한 후, 템플릿 추가/제거 메뉴를 선택합니다.
4. 템플릿 추가/제거 대화 상자가 나타납니다. 확장 레지스트리 정책을 저장하고 있는 템플릿 파일을 로딩하기 위해 추가 버튼을 클릭합니다.
5. %WinDir%\inf 폴더에서 확장할 레지스트리 정책을 저장한 관리 템플릿 파일을 선택한 후, 열기 버튼을 클릭합니다.
6. 선택한 관리 템플릿 파일이 현재 정책 템플릿 목록에 나타나는지 확인 한 후, 닫기 버튼을 클릭합니다.

   예제에서는 Sample.adm 파일을 선택하여 현재 정책 템플릿 목록에 Sample이 출력된 것을 볼 수 있습니다.

그림 14 템플릿 추가/제거

7. 선택한 관리 템플릿 파일이 로딩됩니다. 〈그림 15〉의 그룹 정책 개체 편집기를 보면 예제 관리 템플릿 파일의 CATEGORY에서 설정된 "확장 레지스트리 정책" 이 관리 템플릿 아래에 노드 이름으로 사용된 것을 볼 수 있습니다. 또한 POLICY에서 설정한 "확장한 레지스트리 정책입니다." 가 오른쪽 설정 창에 나타나는 것을 볼 수 있습니다.

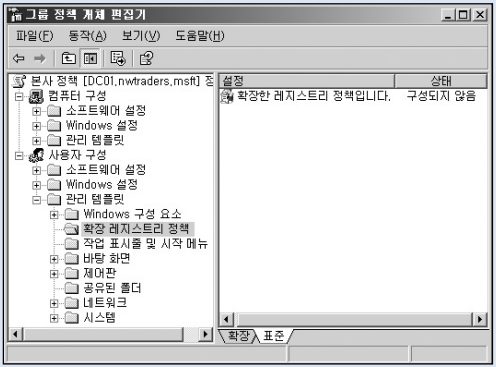

그림 15 확장된 관리 템플릿

8. 설정하고자 하는 확장 레지스트리 정책을 더블 클릭합니다.

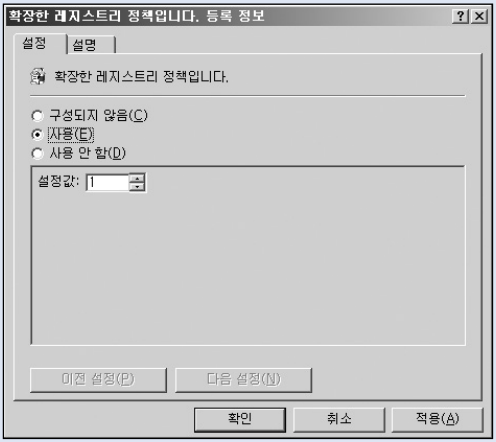

그림 16 확장 레지스트리 정책 설정

9. 사용 옵션을 선택한 후, 적절한 설정 값을 입력한 후, 확인 버튼을 클릭합니다.

〈그림 16〉에서 예제 관리 템플릿 파일의 PART에서 설정한 UI가 출력된 것을 볼 수 있습니다.

예제 관리 템플릿을 이용해서 레지스트리 정책을 확장하였다면, 그룹 정책을 적용 받는 사용자가 로그온 할 때 〈그림 17〉과 같이 예제 관리 템플릿의 KEYNAME과 VALUENAME에서 정의한 레지스트리에 값이 설정됩니다. 따라서 응용 프로그램이 그룹 정책을 지원한다면 예제와 같이 클라이언트에 다운로드 되어 설정된 레지스트리 값을 읽어서 적절히 동작합니다.

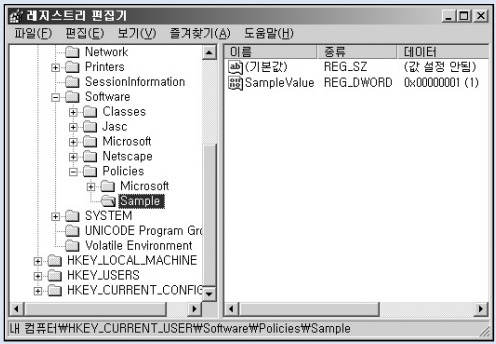

그림 17 클라이언트에 다운로드 된 확장 레지스트리 정책

보안 설정

관리자는 GPO의 보안 설정을 이용해서 도메인에 가입한 모든 컴퓨터와 사용자에게 보안 정책을 적용할 수 있습니다. 보안 설정은 Windows 2000, Windows XP, Windows Server 2003 운영 체제를 지원하는 다양한 보안 정책을 지원합니다.

GPO의 컴퓨터 구성\보안 설정 하위에는 다음과 같은 보안 정책을 제공하는 노드들이 존재합니다.

- **계정 정책** : Windows 2000, Windows Server 2003 도메인에 포함된 모든 사용자에게 적용할 암호 정책, 계정 잠금 정책, Kerberos 정책을 설정합니다.

- **로컬 정책** : 감사 정책, 사용자 권한 할당, 보안 옵션을 설정합니다.

- **이벤트 로그** : 이벤트 뷰어의 시스템 로그, 보안 로그, 응용 프로그램 로그의 보안 설정을 제어할 수 있습니다.

- **제한된 그룹** : 제한된 그룹 정책을 이용해서 관리자는 주요 그룹의 구성원을 제어할 수 있습니다. 예를 들어 Administrators와 같이 주요한 그룹의 멤버로 AdminA와 AdminB만 구성원이 되도록 제한된 그룹에 정책을 설정하였습니다. 그 후 UserC가 어떤 이유에 의해 Administrators 그룹에 구성원이 되었다면, 다음 그룹 정책이 컴퓨터에 적용될 때 제한된 그룹 정책에 의해 UserC는 Administrators 그룹의 구성원에서 제거됩니다.

- **시스템 서비스** : 컴퓨터에서 동작하는 Win32 서비스의 시작 모드 및 권한을 설정합니다. 관리자는 시스템 서비스 정책을 이용해서 클라이언트에서 특정 서비스(예를 들면 IIS)가 동작하지 못하도록 설정할 수 있습니다.

- **레지스트리** : NTFS 파일 시스템의 폴더와 파일에 사용 권한을 부여하듯이 레지스트리 키에 사용 권한을 부여할 때 사용합니다.

- **파일 시스템** : NTFS 파일 시스템의 폴더와 파일에 사용 권한을 부여할 때 사용합니다.

- **무선 네트워크(IEEE 802.11) 정책** : WEP 설정, 802.1x 설정과 같은 무선 네트워크를 연결하기 위해 필요한 설정을 구성할 때 사용합니다. 관리자가 무선 네트워크(IEEE 802.11) 정책을 무선 클라이언트 컴퓨터에 적용함으로써, 사용자들은 보다 쉽게 무선 연결이 가능합니다.

- **공개키 정책** : 발급된 인증서를 자동으로 설치하거나, 신뢰할 수 있는 루트 인증 기관 설치와 같은 다양한 공개키 정책을 설정할 수 있습니다.

- **소프트웨어 제한 정책** : 신뢰할 수 없는 응용 프로그램이 클라이언트 컴퓨터에서 실행되는 것을 차단할 때 사용합니다.

- **IP 보안 정책** : IPSec 정책을 컴퓨터에 적용하여 네트워크 보안을 강화할 때 사용합니다.

소프트웨어 설정

관리자는 소프트웨어 설정을 이용해서 컴퓨터가 시작할 때, 사용자가 로그온 할 때 또는 사용자의 요구에 의해 응용 프로그램을 설치 할 수 있습니다. 또한 소프트웨어 설정을 이용해서 기존 설치된 응용 프로그램을 업그레이드 하고, 더 이상 필요 없는 응용 프로그램을 제거하고, 서비스 팩을 배포할 수 있습니다. 그리고 다음과 같은 상황에서도 사용자들은 정상적으로 응용 프로그램을 사용할 수 있습니다.

- **응용 프로그램 관련 파일 삭제** : 소프트웨어 설정을 이용해서 배포한 응용 프로그램의 파일을 사용자가 실수로 삭제했을 경우에, Windows Installer Service는 응용 프로그램을 실행할 때 자동으로 응용 프로그램을 설치 파일을 다운로드 받아 재설치 합니다.

- **컴퓨터 이동** : 사용자가 기존에 응용 프로그램이 설치된 컴퓨터가 아닌 다른 컴퓨터에 로그온 하면 자동 또는 요구에 의해 필요한 응용 프로그램을 설치합니다.

- **파일 확장자 연결** : 사용자가 로그온 한 컴퓨터에 응용 프로그램이 설치되어 있지 않은 경우에 응용 프로그램에 연결된 파일 확장자를 사용하는 파일을 열면, 자동으로 응용 프로그램이 설치된 후 파일이 열립니다.

관리자는 응용 프로그램을 배포하기 위해 Windows Installer 기반의 파일(.msi)을 사용해야 합니다. msi 파일은 다운로드 되어 Windows Installer Service에 의해 설치되기 때문에, 로그온 한 컴퓨터에 사용자가 administrator 권한을 가지고 있지 않아도 정상적으로 설치됩니다.

Windows Installer에 의해 설치된 응용 프로그램이 실행 될 때마다, Windows Installer Service는 응용 프로그램이 사용하는 파일들이 정상적인지 점검하고, 필요하다면 자동으로 재설치를 통해 응용 프로그램을 구성하는 파일이나 설정을 복원합니다.

소프트웨어 설정은 사용자의 컴퓨터에 응용 프로그램을 배포하는 방법으로 게시와 할당을 제공합니다.

[응용 프로그램 할당]
관리자는 그룹 정책을 이용해서 컴퓨터나 사용자에게 응용 프로그램을 할당할 수 있습니다. 컴퓨터에 응용 프로그램을 할당하면, GPO가 적용되는 컴퓨터가 시작할 때 자동으로 할당된 응용 프로그램이 설치됩니다. 사용자에게 응용 프로그램을 할당할 때, 관리자는 응용 프로그램이 사용자가 로그온 할 때 자동으로 설치되게 할 것인지 또는 사용자 요구에 의해서만 설치되게 할 것인지를 선택할 수 있습니다.

〈그림 18〉에서와 같이 로그온 시 이 응용 프로그램 설치 옵션을 선택하면, 사용자가 로그온 할 때 할당 된 응용 프로그램이 자동으로 설치됩니다. 이 옵션의 선택을 해제하면 응용 프로그램은 연결된 파일 확장명을 가진 파일을 활성화 할 때나, 시작 메뉴에 생성된 응용 프로그램 메뉴를 사용자가 선택했을 때 설치됩니다.

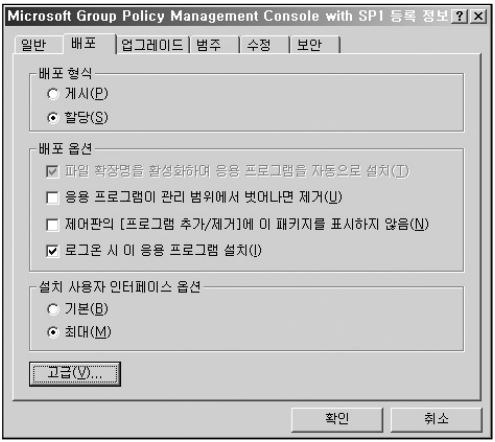

그림 18 응용 프로그램 할당

[응용 프로그램 게시]

관리자가 그룹 정책을 이용해서 사용자에게 응용 프로그램을 게시하면, 제어판의 프로그램 추가/제거에 게시한 응용 프로그램이 나타납니다. 사용자는 필요한 응용 프로그램을 선택하여 설치할 수 있습니다.

응용 프로그램 게시도 할당과 마찬가지로 파일 확장명을 활성화하여 응용 프로그램을 자동으로 설치 옵션을 선택하면, 사용자가 연결된 파일 확장명을 가진 파일을 활성화 할 때 자동으로 설치되도록 구성이 가능합니다.

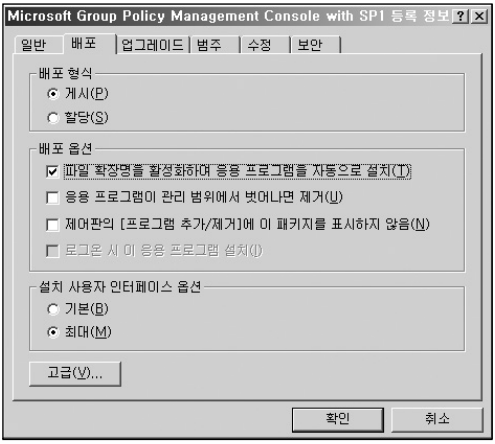

그림 19 응용 프로그램 게시

스크립트

관리자는 컴퓨터 시작 및 종료, 사용자 로그온 및 로그오프 때에 동작하여 원하는 작업을 수행하는 스크립트를 설정할 수 있습니다. 스크립트는 Windows Script Host에서 지원하는 VBScript, JavaScript, MS-DOS 배치 파일(.bat, .cmd)과 같은 개발 언어를 이용해서 작성해야 합니다.

관리자는 다음과 같은 정책을 이용해서 스크립트의 동작 방식을 제어할 수 있습니다.

컴퓨터 구성\관리 템플릿\시스템\스크립트	설명
로그온 스크립트 동기적으로 실행	디폴트로 로그온 스크립트는 비동기적으로 실행됩니다. 따라서 로그온 스크립트가 실행되면서 동시에 사용자 데스크탑이 복원 됩니다. 관리자가 이 정책을 설정하면 설정된 로그온 스크립트들이 순차적으로 실행되고, 모든 로그온 스크립트의 실행이 완료되어야만 사용자의 데스크톱 화면이 복원됩니다. 동일한 구성이 사용자 구성에도 존재합니다. 만일 컴퓨터 구성과 사용자 구성에 모두 정책이 설정되었다면 컴퓨터 구성의 정책이 우선 순위가 높습니다.
시작 스크립트 비동기적으로 실행	디폴트로 시작 스크립트는 동기적으로 실행되고, 모든 시작 스크립트의 실행이 완료되어야만 Windows 로그온 대화 상자가 나타납니다. 하지만 시작 스크립트가 실행되는데 오랜 시간이 걸린다면 이 정책을 설정하여 시작 스크립트가 실행되면서 동시에 사용자가 로그온 할 수 있도록 구성이 가능 합니다.
시작 스크립트 실행 표시	이 정책이 설정되면 시작 스크립트가 명령 프롬프트상에서 실행됩니다.
종료 스크립트 실행 표시	이 정책이 설정되면 종료 스크립트가 명령 프롬프트상에서 실행됩니다.
그룹 정책 스크립트 최대 대기 시간	스크립트가 실행되는 최대 시간을 지정합니다. 시작 스크립트는 디폴트로 동기적으로 실행되기 때문에 모든 스크립트가 완료되어야만 Windows 로그온 대화 상자가 나타납니다. 하지만 특정 스크립트가 장시간 실행되거나 스크립트 내부 오류에 의해 종료가 안 되면 무한대로 대기해야 하는 문제가 있기 때문에 이 정책을 제공합니다. 이 정책의 기본값은 600초이며, 최대 대기 시간 이상으로 실행되는 스크립트는 강제로 종료됩니다.

사용자 구성\관리 템플릿\시스템\스크립트	설명
로그온 스크립트 동기적으로 실행	디폴트로 로그온 스크립트는 비동기적으로 실행됩니다. 따라서 로그온 스크립트가 실행되면서 동시에 사용자 데스크탑이 복원됩니다. 관리자가 이 정책을 설정하면 설정된 로그온 스크립트들이 순차적으로 실행되고, 모든 로그온 스크립트의 실행이 완료되어야만 사용자의 데스크톱 화면이 복원됩니다. 동일한 구성이 컴퓨터 구성에도 존재합니다. 만일 컴퓨터 구성과 사용자 구성에 모두 정책이 설정되었다면 컴퓨터 구성의 정책이 우선 순위가 높습니다.
레거시 로그온 스크립트 실행 숨기기	이 정책이 설정되면 Windows NT 4.0이나 이전 버전용으로 쓰여진 로그온 스크립트를 백그라운드로 실행합니다.
로그온 스크립트 실행 표시	이 정책이 설정되면 로그온 스크립트가 명령 프롬프트상에서 실행됩니다.
로그오프 스크립트 실행 표시	이 정책이 설정되면 로그오프 스크립트가 명령 프롬프트상에서 실행됩니다.

표 3 스크립트 동작 방식 설정 그룹 정책들

원격 설치 서비스

관리자는 원격 설치 서비스를 이용해서 PXE 부트를 지원하는 컴퓨터에 Windows XP 운영 체제를 원격에서 설치할 수 있습니다. 그룹 정책을 이용해서 관리자는 운영 체제를 설치할 때 사용자에게 제공하는 옵션을 제어할 수 있습니다.

PXE 부트를 지원하는 컴퓨터가 시작하면 운영 체제를 설치하기 위해 RIS 서버에 접속합니다. RIS 서버는 사용자에게 적용하도록 설정된 그룹 정책의 원격 설치 옵션이 있는지 점검합니다. 설정 여부에 따라 사용자에게 정의된 적절한 메뉴가 출력됩니다.

Internet Explorer 유지/보수

Internet Explorer 유지/보수 확장 스냅인에서는 다음과 같은 정책을 제공합니다.

- **브라우저 사용자 인터페이스** : 브라우저 제목, 로고, 브라우저 도구 모음 같이 브라우저의 사용자 인터페이스를 변경 합니다.
- **연결** : LAN이나 전화 접속과 같은 연결을 관리합니다.
- **URL** : 즐겨 찾기, 홈 페이지, 검색 페이지 URL들을 정의합니다.
- **보안** : 보안 영역, 콘텐트 등급 같은 보안 설정을 정의합니다.
- **프로그램** : 전자 메일을 읽고 뉴스 그룹을 보는 것과 같은 작업을 수행할 디폴트 인터넷 프로그램들을 정의합니다.

폴더 리디렉션

폴더 리디렉션 확장 스냅인은 사용자 파일이나 데스크탑 환경을 저장하는 주요 폴더를 로컬 컴퓨터의 Documents and Settings 폴더에서 그룹 정책에서 지정한 네트워크 위치로 리디렉션 하는 기능을 제공 합니다.

리디렉션 가능한 주요 폴더는 다음과 같습니다.

- Application Data
- 바탕 화면
- 내 문서

- 시작 메뉴

예를 들어, 관리자는 사용자의 내 문서 폴더를 \\FileServer\Share\% username% 폴더로 리디렉션 할 수 있습니다. 내 문서를 리디렉션 하면 다음과 같은 장점을 제공합니다.

- 사용자가 도메인의 어떤 클라이언트에 로그온 하더라도 내 문서 폴더에 접근하여 작업을 진행할 수 있습니다.
- 사용자의 데이터를 서버에 저장하기 때문에 관리자의 의해 백업과 복원을 원활하게 수행할 수 있습니다.
- 사용자가 내 문서를 리디렉션 한 서버에 접속할 수 없는 외부에 있을 경우에도 내 문서의 파일을 이용해서 작업을 수행할 수 있도록 오프라인 폴더 기능을 사용합니다.

GPO 범위 제어

컴퓨터나 사용자에게 적용할 그룹 정책을 생성, 수정한 후에 GPO를 원하는 대상 컴퓨터나 사용자에게 적용하기 위해서 관리자는 GPO를 사이트, 도메인, 조직 구성 단위에 연결 해야 합니다. 연결된 GPO는 대상 컨테이너 안에 있는 모든 컴퓨터와 사용자에게 적용됩니다. 때에 따라 관리자는 필터링을 통해 대상 컨테이너 안에 있는 특정 컴퓨터나 사용자에게만 GPO가 적용되게 할 수 있습니다.

관리자는 GPO가 적용되는 범위를 제어하기 위해 다음과 같은 세 가지 방법을 사용할 수 있습니다.

- GPO를 사이트, 도메인, 조직 구성 단위에 연결
- GPO에 보안 그룹 필터링
- GPO에 WMI 필터링

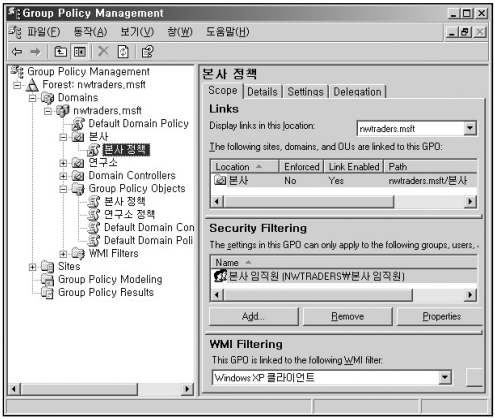

그림 20 GPO 범위 제어

〈그림 20〉의 예를 보면 총 네 개의 GPO가 생성되어 있는 것을 볼 수 있습니다. Default Domain Controller Policy와 Default Domain Policy는 도메인이 생성될 때 자동으로 생성된 GPO입니다. 그리고 본사 정책 GPO와 연구소 정책 GPO는 각 부서에 적용할 정책이 설정된 GPO입니다. 본사 정책 GPO는 본사 OU에 연결되어 있으므로 본사 OU 안에 컴퓨터와 사용자에게 적용 됩니다.

하지만 본사 OU안에는 본사에서 근무하는 임직원과 임시 직원의 사용자 계정이 같이 존재합니다. 관리자는 본사 정책 GPO를 본사에서 근무하는 임직원에게만 적용하길 원하기 때문에, 본사에서 근무하는 임직원의 컴퓨터와 사용자 계정을 구성원으로 포함하는 본사 임직원 그룹을 이용해서 보안 그룹 필터링을 설정했습니다.

또한 본사 정책 GPO는 Windows XP를 운영 체제로 사용하는 클라이언트에만 적용되도록 하기 위해 WMI 필터링도 적용하였습니다. 따라서 〈그림 20〉과 같이 설정했다면 본사 정책 GPO는 본사 OU에 존재하는 컴퓨터와 사용자 중에서 본사 임직원 그룹에 구성원으로 포함되어 있고, 운영 체제가 Windows XP를 사용하는 컴퓨터와 사용자에게만 적용됩니다.

GPO 연결

GPO에 설정한 정책을 컴퓨터와 사용자에게 적용하기 위해서 제일 먼저 해야 할 일은 Active Directory의 사이트, 도메인, 조직 구성 단위에 GPO를 연결하는 것입니다. Active Directory를 구성하는 컴포넌트 중에서 GPO를 연결할 수 있는 컴포넌트를 SOM(Scope of Management)라 정의하며, 세 종류의 SOM(사이트, 도메인, 조직 구성 단위)이 존재합니다. 컴퓨터나 사용자 계정은 SOM이 아닙니다. 즉 GPO를 컴퓨터나 사용자 계정에 직접 연결하는 것은 불가능합니다.

특정 SOM에 여러 개의 GPO를 동시에 연결할 수 있고, 또한 하나의 GPO를 여러 SOM에 연결하는 것도 가능합니다.

[따라하기] GPO 연결하기

GPMC를 이용해서 SOM에 GPO를 연결하는 과정은 다음과 같습니다.

1. GPO를 연결할 사이트, 도메인, 조직 구성 단위를 마우스 오른쪽 버튼으로 클릭한 후, Link an Existing GPO 메뉴를 선택합니다.
2. Select GPO 대화 상자가 나타납니다. Group Policy objects 목록에서 연결할 GPO를 선택한 후, OK 버튼을 클릭합니다.

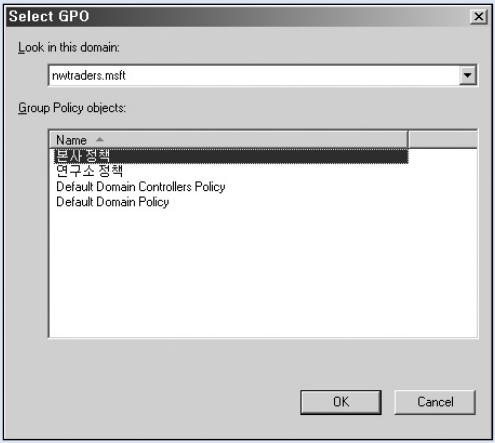

그림 21 연결할 GPO 선택

보안 그룹 필터링

관리자가 특별히 필터링을 설정하지 않으면 디폴트로 GPO가 연결된 SOM 아래에 존재하는 모든 컴퓨터와 사용자에게 설정된 정책이 적용됩니다. 때에 따라 관리자는 GPO가 연결된 SOM 아래에 존재하는 컴퓨터와 사용자중에서 정책을 적용 받을 대상을 필터링 할 필요가 있습니다. 이 때 보안 그룹을 이용해서 원하는 컴퓨터와 사용자에게만 GPO가 적용되도록 할 수 있는데, 이를 보안 그룹 필터링이라 합니다.

새 GPO가 생성되면 〈그림 22〉와 같이 Authenticated Users 그룹이 Security Filtering 세션에 포함되어 있습니다. Authenticated Users 그룹은 모든 컴퓨터와 사용자 계정을 포함하고 있기 때문에 결국 GPO가 연결된 SOM 아래에 모든 컴퓨터와 사용자에게 설정된 정책이 적용됩니다.

그림 22 보안 그룹 필터링

보안 그룹 필터링을 사용하기 위해서는 먼저 GPO를 적용할 컴퓨터와 사용자 계정을 구성원으로 포함하는 보안 그룹을 생성합니다. 그리고 GPO의 Security Filtering 세션에서 Authenticated Users를 제거하고, 보안 그룹을 추가합니다.

[따라하기] 보안 그룹 필터링 하기

GPMC를 이용해서 GPO의 보안 그룹 필터링을 설정하는 과정은 다음과 같습니다.

1. 보안 그룹 필터링을 설정할 GPO를 GPMC의 Group Policy Objects 노드 아래에서 선택합니다.
2. Scope 탭의 Security Filtering 섹션에서 Authenticated Users 그룹을 선택한 후, Remove 버튼을 클릭합니다.
3. 보안 그룹을 제거할 것인지에 대해 묻는 대화 상자가 나타납니다. 확인 버튼을 클릭합니다.

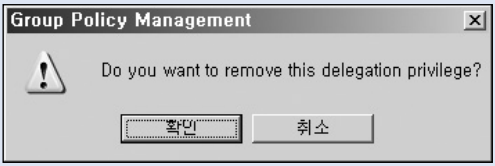

그림 23 보안 그룹 제거

4. GPO를 적용할 컴퓨터와 사용자 계정을 구성원으로 포함하는 보안 그룹을 추가하기 위해 Add 버튼을 클릭합니다.
5. 필터링 할 보안 그룹의 이름을 입력한 후, 확인 버튼을 클릭합니다.

WMI 필터링

관리자는 WMI 필터링을 이용해서 컴퓨터의 속성에 따라 동적으로 GPO를 적용할 대상을 지정할 수 있습니다. WMI 필터는 컴퓨터의 WMI를 이용해서 참 또는 거짓 값을 리턴 하는 쿼리로 구성됩니다.

만약 GPO에 WMI 필터가 설정되어 있다면, 컴퓨터에 GPO를 적용하기 전에 먼저 WMI 필터의 쿼리를 실행합니다. WMI 필터가 거짓 값을 리턴 하면 컴퓨터에 GPO는 적용되지 않습니다. 반대로 WMI 필터가 참 값을 리턴 하면 컴퓨터에 GPO가 적용합니다.

Windows XP, Windows Server 2003 컴퓨터가 공존하는 도메인 환경하에서 Windows XP를 운영 체제로 사용하는 컴퓨터에게만 GPO를 적용해야 하는 요구사항이 발생했다고 가정하겠습니다. 이 요구 사항을 만족하기 위해 보안 그룹 필터링을 사용할 수도 있습니다. 보안 그룹을 생성한 후, Windows XP 운영 체제를 사용하는 컴퓨터들을 모두 보안 그룹에 구성원으로 포함합니다. 그리고 이 보안 그룹에 대해 보안 그룹 필터링을 설정한다면 요구 사항을 만족합니다.

하지만 Windows Server 2003 운영 체제를 사용하던 컴퓨터를 Windows XP로 변경 할 때마다 관리자는 보안 그룹의 구성원을 업데이트 해 주어야 합니다. 따라서 보안 그룹 필터링을 사용할 경우에는 항상 요구 사항을 만족할 수 있도록 보안 그룹의 구성원을 업데이트 해야 하는 관리 부하가 발생합니다.

반면에 WMI 필터를 이용한다면 관리자는 Windows XP 운영 체제일 경우에 참 값을 리턴 하는 쿼리를 포함하는 WMI 필터를 생성 한 후, GPO에 WMI 필터를 연결함으로써 요구 사항을 만족할 수 있습니다. 클라이언트의 운영 체제에 변화가 있어도 쿼리가 리턴 하는 값에 따라 Windows XP 클라이언트에는 항상 GPO가 적용됩니다.

WMI 필터는 GPO와 별개의 개체입니다. GPO에 WMI 필터링을 사용하기 위해서는 먼저 WMI 필터를 생성한 후, WMI 필터링을 적용할 GPO에 연결합니다. WMI 필터링을 사용할 때 한가지 알아두어야 할 점은 WMI 필터링은 Windows XP 이상의 운영 체제에서만 동작한다는 것입니다. Windows XP 이상의 운영 체제에서만 WMI 필터의 쿼리가 실행되어 참 또는 거짓 여부에 따라 GPO가 적용됩니다. Windows 2000 클라이언트에서는 WMI 필터링을 무시하기 때문에 항상 GPO가 적용됩니다.

[따라하기] WMI 필터링 하기

GPMC를 이용해서 GPO의 WMI 필터링을 설정하는 과정은 다음과 같습니다.

1. WMI 필터를 생성하기 위해 GPMC의 WMI Filters 노드를 마우스 오른쪽 버튼으로 클릭한 후, New 메뉴를 선택합니다.
2. Name 입력창에 WMI 필터의 이름을 입력한 후, Add 버튼을 클릭합니다.
3. Query 입력창에 특정 조건일 때 참 값을 리턴 하는 쿼리를 입력한 후, OK 버튼을 클릭합니다.
4. 쿼리 입력을 완료한 후에는 Save 버튼을 클릭하여 WMI 필터를 생성합니다. 〈그림 24〉는 Windows XP 운영 체제일 경우에 참 값을 리턴 하는 쿼리 예제입니다.

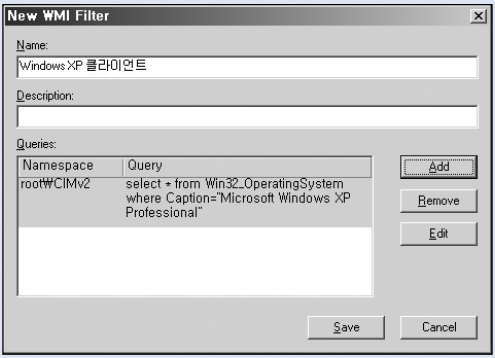

그림 24 WMI 필터 생성

5. WMI 필터를 연결할 GPO를 GPMC의 Group Policy Objects 노드 아래에서 선택합니다.
6. Scope 탭의 WMI Filtering 섹션에서 콤보 박스를 클릭 한 후, GPO에 연결할 WMI 필터를 선택합니다.

GPO 상속

SOM(사이트, 도메인, 조직 구성 단위)에 연결된 GPO는 하위 컨테이너에 상속됩니다. 따라서 상위 컨테이너에 적용된 GPO들이 상속되면, 상속된 모든 GPO들이 컴퓨터와 사용자에게 누적되어 적용됩니다.

클라이언트에 GPO가 누적되어 적용될 때는 다음과 같은 순서로 적용됩니다.

- **로컬 GPO** : 각 컴퓨터의 로컬에 설정된 로컬 GPO가 제일 먼저 적용됩니다.

- **사이트** : 컴퓨터가 속한 사이트에 연결된 GPO가 로컬 GPO 다음으로 적용됩니다.

- **도메인** : 도메인에 연결된 GPO가 사이트에 연결된 GPO 다음으로 적용됩니다.

- **조직 구성 단위** : 조직 구성 단위에 연결된 GPO가 마지막에 적용됩니다. 조직 구성 단위가 다중 구조로 이루어져 있을 경우에는 상위 조직 구성 단위에 연결된 GPO가 먼저 적용되고 하위 조직 구성 단위에 연결된 GPO가 적용됩니다.

로컬 GPO는 각 컴퓨터마다 오직 하나의 GPO만 존재합니다. 하지만 사이트, 도메인, 조직 구성 단위에는 하나 또는 다중 GPO를 연결할 수 있습니다. 동일 SOM에 다중 GPO가 연결되어 있을 경우에는 GPMC의 Linked Group Policy Objects 탭에서 Link Order를 이용해서 적용되는 순서를 제어할 수 있습니다.

같은 정책이 여러 GPO에서 설정되어 있어 충돌이 발생하면, 마지막에 적용된 GPO의 정책설정 값이 최종적으로 컴퓨터와 사용자에게 적용됩니다.

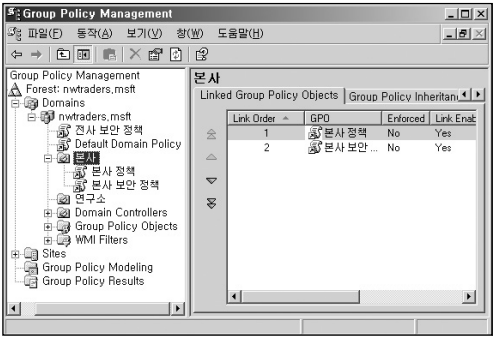

그림 25 GPO 상속

〈그림 25〉를 이용해서 GPO 상속에 대한 예를 들어 보도록 하겠습니다. 예제에서 nwtraders.msft 도메인에는 다음과 같이 두 개의 GPO가 연결되어 있습니다.

- 전사 보안 정책
- Default Domain Policy

그리고 본사 OU에는 다음과 같이 두 개의 GPO가 연결되어 있습니다.

- 본사 정책
- 본사 보안 정책

연결된 GPO가 상속되어 본사 OU에 있는 컴퓨터와 사용자에게는 총 4 개의 GPO가 적용됩니다. 먼저 도메인에 연결된 GPO의 정책들이 적용되고, 그 다음에 본사 OU에 연결된 정책들이 적용됩니다.

기본적으로 SOM에 연결된 GPO들은 상속되어 순차적으로 적용 되지만, 다음과 같은 방법들을 이용해서 관리자는 컴퓨터와 사용자에게 적용될 GPO의 순서를 제어할 수 있습니다.

연결 순서 변경

같은 SOM에 연결된 GPO의 적용 순서는 GPMC의 Linked Group Policy Objects 탭에서 Link Order를 이용해서 제어할 수 있습니다. 같은 SOM에 연결된 GPO들은 Link Order의 아래에서 위로 순차적으로 적용됩니다. 〈그림 25〉의 예제에서 본사 OU에 연결된 두 GPO는 Link Order의 아래에 있는 본사 보안 정책 GPO가 먼저 적용된 후, 상위에 있는 본사 정책 GPO가 적용됩니다.

만약 본사 보안 정책 GPO와 본사 정책 GPO의 정책 설정 값에 충돌이 발생하면 나중에 적용된 본사 정책 GPO의 정책 설정 값이 최종 적용됩니다. 정책 설정 값 충돌이 발생하면 나중에 적용된 GPO의 정책이 컴퓨터와 사용자에게 최종 적용 되기 때문에 필요하다면 관리자는 Linked Group Policy Objects 탭의 화살표 버튼을 이용해서 GPO의 Link Order를 변경할 수 있습니다.

제어판\디스플레이의 화면 보호기 제한 시간 정책을 예를 들어 정책 설정 값 충돌에 대해 설명하겠습니다. 〈그림 25〉의 본사 정책 GPO에는 30분 동안 마우스나 키보드 입력이 없으면 화면 보호기가 동작하도록 설정되어 있고, 본사 보안 정책 GPO에는 10분 동안 마우스나 키보드 입력이 없으면 화면 보호기가 동작하도록 설정되어 있습니다.

우선 순위에 따라 먼저 본사 보안 정책 GPO가 클라이언트에 적용되기 때문에 클라이언트의 화면 보호기 제한 시간은 10분으로 설정됩니다. 하지만 이어서 본사 정책 GPO가 클라이언트에 적용되면 설정 값 충돌이 발생합니다. 정책 설정 값의 충돌이 발생하면 우선 순위가 높은 나중에 적용된 정책의 설정 값이 최종 적용되기 때문에 결국 클라이언트의 화면 보호기 제한 시간은 30분으로 설정됩니다.

만약 관리자가 본사 직원의 화면 보호기 제한 시간이 10분이 되길 원한다면 우선 순위를 변경함으로써 원하는 목적을 달성할 수 있습니다.
관리자 입장에서는 특정 OU에 속한 컴퓨터와 사용자에게 상속되어 적용되는 모든 GPO의 목록과 적용 순서를 파악할 필요가 있습니다. GPMC는 이런 요구 사항을 만족하기 위해 〈그림 26〉와 같이 Group Policy Inheritance 탭을 제공합니다.

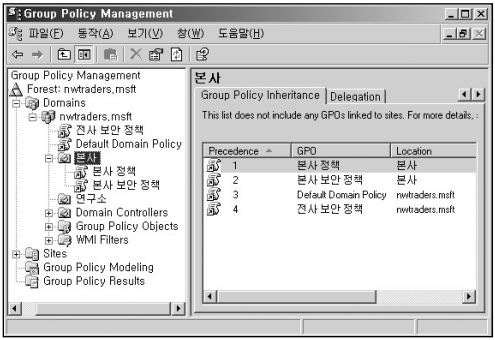

그림 26 GPO 우선순위

Group Policy Inheritance 탭에는 선택한 SOM에 포함되어 있는 컴퓨터와 사용자에게 적용될 전체 GPO의 목록, 우선 순위 그리고 각 GPO가 연결된 SOM에 대한 정보를 제공합니다.

GPO는 아래에서 위로 순차적으로 적용되기 때문에 〈그림 26〉과 같은 경우에는 제일 먼저 전사 보안 정책 GPO가 적용되고, 마지막으로 본사 정책 GPO가 적용됩니다.

정책 상속 금지

디폴트로 SOM의 하위 컨테이너에는 상위 컨테이너에 연결된 정책들이 상속됩니다. 하지만 관리자는 필요하다면 GPO의 자동 상속을 금지할 수 있습니다. 특정 SOM에서 정책 상속을 금지하면 상위 컨테이너의 모든 정책은 해당 SOM으로 상속되지 않습니다.

예를 들어 〈그림 25〉와 같은 경우에 본사 OU에 정책 상속 금지를 설정하면 상위 컨테이너인 도메인에 연결된 두 GPO는 상속 금지에 따라 본사 OU의 컴퓨터와 사용자에게 더 이상 적용되지 않습니다. 하지만 본사 OU에 직접 연결된 GPO는 정상적으로 적용됩니다.

정책 상속 금지는 SOM에 설정하는 것이기 때문에 특정 GPO 단위로 상속 금지를 설정할 수 없습니다. 예를 들어 도메인에 연결된 전사 보안 정책 GPO만 본사 OU에 상속되는 것을 금지 할 수는 없습니다.

[따라하기] 정책 상속 금지 설정하기

GPMC를 이용해서 특정 SOM에 정책 상속을 금지하는 과정은 다음과 같습니다.

1. 정책 상속을 금지할 SOM(도메인 또는 조직 구성 단위)를 마우스 오른쪽 버튼으로 클릭한 후, Block Inheritance 메뉴를 선택합니다.

   〈그림 27〉는 본사 OU에 대해 정책 상속 금지를 설정한 것으로, 본사 OU 노드에 느낌표 아이콘이 나타나는 것을 볼 수 있습니다. 또한 Group Policy Inheritance 탭에는 도메인에 연결된 두 개의 GPO가 상속 금지에 따라 상속되지 않아 본사 OU에 연결된 GPO만 나타나는 것을 볼 수 있습니다.

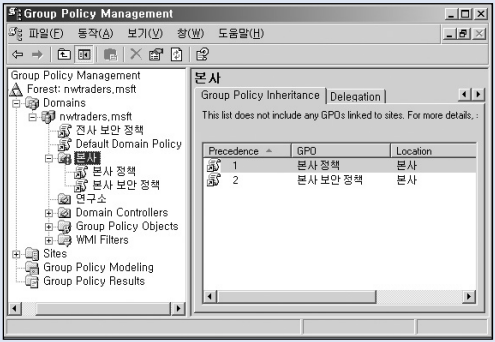

그림 27 정책 상속 금지

정책 무시 안 함

관리자는 SOM에 연결된 GPO에 대해 정책 무시 안 함 설정을 할 수 있습니다. 정책 무시 안 함이 설정된 GPO는 하위에 정책 상속이 금지된 SOM에도 그룹 정책이 적용됩니다. 또한 정책 무시 안 함을 설정한 GPO는 최상위 우선 순위가 되기 때문에 가장 마지막에 정책이 적용됩니다.

따라서 관리자는 매우 중요한 정책을 포함하고 있어서 어떤 경우에라도 반드시 적용해야 하는 GPO에 대해 정책 무시 안 함 옵션을 설정하면 유용합니다. 일반적으로 도메인의 모든 컴퓨터와 사용자에게 반드시 적용되어야 하는 정책을 포함하는 도메인에 연결된 GPO에 정책 무시 안 함을 설정합니다.

[따라하기] 정책 무시 안 함 설정하기

GPMC를 이용해서 SOM에 연결된 GPO에 정책 무시 안 함을 설정하는 과정은 다음과 같습니다.

1. 정책 무시 안 함을 설정할 GPO를 마우스 오른쪽 버튼으로 클릭한 후, Enforced 메뉴를 선택합니다.
   〈그림 28〉는 본사 OU에 대해 정책 상속 금지를 설정한 상태에서, 도메인에 연결된 본사 보안 정책 GPO에 정책 무시 안 함을 설정한 것입니다. 정책 무시 안 함이 설정된 GPO의 아이콘에 자물쇠가 나타나는 것을 볼 수 있습니다.
   본사 OU에 정책 상속 금지가 설정된 상태이기 때문에 본사 OU 상위에 연결된 모든 GPO는 정책 상속이 금지되지만, 정책 무시 안 함이 설정된 전사 보안 정책 GPO는 상속되어 적용되는 것을 Group Policy Inheritance 탭에서 확인 할 수 있습니다.

일반적인 경우에 〈그림 26〉과 같이 도메인에 연결된 정책이 먼저 적용된 후, 조직 구성 단위에 연결된 GPO가 적용됩니다. 하지만 정책 무시 안 함이 설정된 GPO는 최상위 우선 순위가 되기 때문에 〈그림 28〉에서 보는 바와 같이 본사 OU에 연결된 두 정책이 먼저 적용된 후에 도메인에 연결된 전사 보안 정책이 적용됩니다.

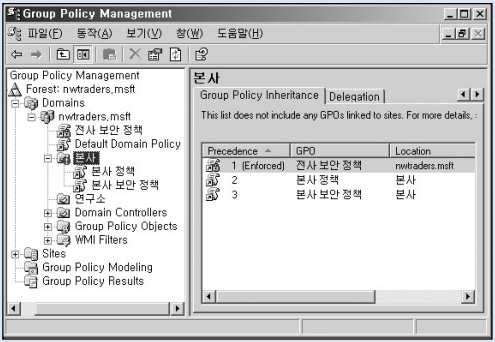

그림 28 정책 무시 안 함

그룹 정책 동작 방식

관리자가 GPMC를 이용해서 설정한 GPO는 컴퓨터가 시작하고 사용자가 로그온 할 때, 클라이언트에서 동작하는 CSE(Client-Side Extensions)에 의해 다운로드 되어 적용 됩니다. 컴퓨터가 동작중인 상태에서는 주기적으로 백그라운드 작업을 통해 GPO의 변경 여부를 점거하고, GPO가 변경되었을 경우에는 다시 다운로드 하여 적용합니다. 필요에 따라서 gpupdate.exe를 이용해서 변경된 GPO 정책을 바로 적용할 수 있습니다.

그럼, 클라이언트에서 그룹 정책이 처리 되는 방식을 이해하기 위해 먼저 그룹 정책 아키텍쳐에 대해 살펴보도록 하겠습니다.

그룹 정책 아키텍쳐

컴퓨터가 시작하고 사용자가 로그온 할 때 클라이언트는 〈그림 29〉와 같은 그룹 정책 아키텍쳐에 의해 적용할 GPO를 처리합니다.

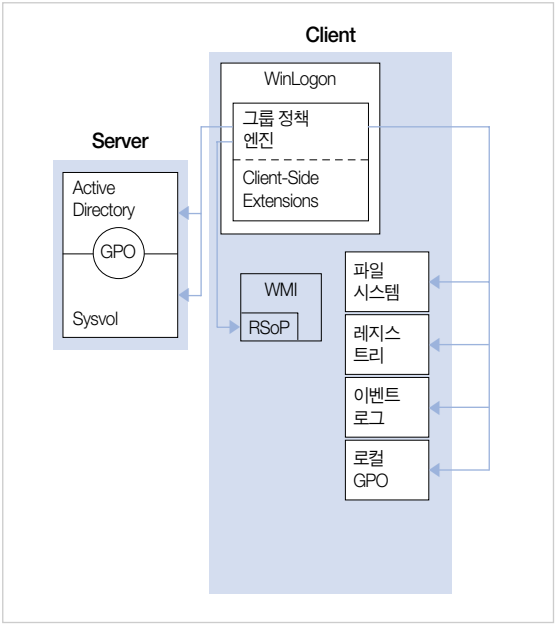

그림 29 그룹 정책 아키텍쳐

그룹 정책을 처리하기 위해 서버에는 다음과 같은 컴포넌트가 동작합니다.

- Active Directory : Windows 기반 디렉터리 서비스인 Active Directory는 컴퓨터와 사용자 개체에 대한 정보를 저장합니다. 또한 그룹 정책 컨테이너로써 GPO의 속성 정보를 저장합니다.

- Sysvol : Sysvol은 Active Directory가 동작하는데 중요한 정보를 저장하는 폴더입니다. GPO는 도메인 컨트롤러의 Sysvol 하위의 Policies 폴더에 그룹 정책 템플릿이라 불리는 폴더 구조 안에 그룹 정책 설정을 저장합니다. 그룹 정책 템플릿은 보안 정책, 관리 템플릿 기반의 정책 설정들, 소프트웨어 설치 정보들 그리고 각종 스크립트 파일들을 저장하는 컨테이너로써 컴퓨터와 사용자에게 적용할 실제 정책들을 저장하고 있습니다.

그룹 정책을 처리하기 위해 클라이언트에는 다음과 같은 컴포넌트가 동작합니다.

- WinLogon : 로컬 로그온을 지원하는 운영 체제 컴포넌트로 내부에서 그룹 정책 엔진이 동작하는 서비스 입니다.

- **그룹 정책 엔진** : 그룹 정책 엔진은 레지스트리 기반 설정과 Client-Side Extensions를 제어하는 프레임워크입니다.

- Client-Side Extensions : CSE는 DLL로 동작하며, 클라이언트에서 그룹 정책을 처리할 때 로딩되어 실질적으로 GPO를 처리합니다.

- **파일 시스템** : 보안 설정에 따라 NTFS 권한이 설정됩니다.

- **레지스트리** : 컴퓨터 구성\관리 템플릿과 사용자 구성\관리 템플릿에 설정된 레지스트리 정책이 다운로드 되어 저장 됩니다.

- **이벤트 로그** : 보안 설정에 따라 이벤트 로그에 대한 설정이 적용되며, CSE이 그룹 정책을 처리하면서 발생한 정보, 경고, 오류가 기록됩니다.

- **로컬 GPO** : 로컬 GPO는 모든 클라이언트 컴퓨터의 %WinDir%\System32\GroupPolicy 에 저장됩니다. 도메인 가입 여부와 상관없이 모든 컴퓨터에 로컬 GPO가 적용됩니다. 하지만 도메인 환경하에서는 Active Directory 기반 GPO가 우선 순위가 높기 때문에 가장 영향력이 작은 GPO입니다.

- **그룹 정책 결과 집합(RSoP)** : 모든 그룹 정책 처리 정보는 수집되어 로컬 컴퓨터의 CIMOM(Common Information Model Object Management) 데이터베이스에 저장 됩니다. 이 정보는 그룹 정책 결과 집합을 통해 확인할 수 있습니다.

CSE는 클라이언트 컴퓨터가 그룹 정책을 처리할 때 필요에 따라 로딩되어 동작합니다. 클라이언트 컴퓨터가 시작할 때 먼저 클라이언트에 적용해야 할 GPO 목록을 생성합니다. 그리고 적용할 GPO에 CSE가 처리해야 할 정책 설정이 존재하는지 점검합니다. 만일 GPO에 CSE가 처리해야 할 정책 설정이 존재하면, 정책 설정을 다운로드 해서 클라이언트에 적용할 적절한 CSE이 로딩됩니다. 만일 GPO에 CSE가 처리해야 할 정책 설정이 존재하지 않으면 CSE는 로딩되지 않습니다.

클라이언트에서 그룹 정책을 처리하기 위해 〈표 4〉와 같이 7 개의 CSE가 제공됩니다.

CES	처리하는 그룹 정책 설정
GPTest.dll	✓ 스크립트 정책 ✓ IP 보안 정책 ✓ 무선 정책
Fdeploy.dll	✓ 폴더 리디렉션 정책
Scecli.dll	✓ 보안 정책
Dskquota.dll	✓ 디스크 할당량 정책
Iedkcs32.dll	✓ Internet Explorer 유지 관리 정책
AppMgmts.dll	✓ 소프트웨어 설치 정책
UserEnv.dll	✓ 관리 템플릿 ✓ 소프트웨어 제한 정책 ✓ 공개키 정책

표 4 Client-Side Extensions

[CSE 그룹 정책]

컴퓨터 정책(컴퓨터 구성\관리 템플릿\시스템\그룹 정책)에는 CSE의 동작 방식을 제어할 수 있는 그룹 정책이 제공됩니다. 〈그림 30〉은 Internet Explorer 유지 관리 정책을 처리하는 옵션들이며, CSE 별로 동작 방식을 제어하는 최대 세 개의 옵션을 제공합니다.

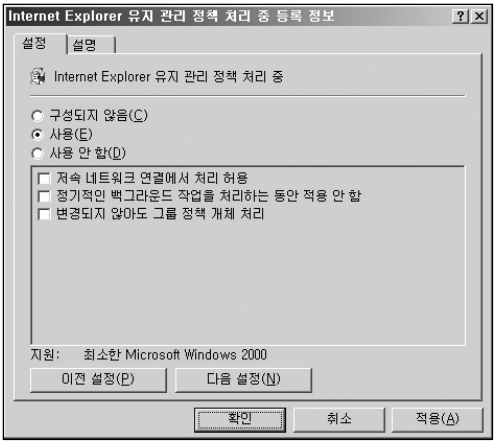

그림 30 CSE 그룹 정책

CSE의 동작 방식을 제어하는 세 개의 옵션은 다음과 같습니다.

- **저속 네트워크 연결에서 처리 허용** : 저속 네트워크일 경우에 정책을 다운로드 받아 클라이언트에 적용할 것인지를 설정합니다. 일부 CSE는 많은 양의 데이터를 다운로드 받아야 하기 때문에 저속 네트워크에서 성능상의 문제를 유발 할 수 있습니다. 예를 소프트웨어 설치 같은 경우에 사용자가 56K 모뎀을 이용해서 접속했을 때 설치 파일을 다운로드 한다면 사용자는 병목 현상이 발생해서 네트워크를 거의 사용할 수 없을 것입니다. 따라서 관리자는 이 옵션을 이용해서 특정 CSE에 대해 데이터의 크기와 상관없이 저속 네트워크에서 정책을 다운로드 받아 적용할 것인지 여부를 제어할 수 있습니다.

- **정기적인 백그라운드 작업을 처리하는 동안 적용 안 함** : 컴퓨터 정책은 컴퓨터 시작할 때 적용되고, 그 후 대략 90분 주기로 변경된 정책을 체크해서 백그라운드에서 재 적용 됩니다. 사용자 정책은 사용자가 로그온 할 때 적용되고, 역시 대략 90분 주기로 변경된 정책을 체크해서 백그라운드에서 재 적용 됩니다. 관리자는 이 옵션을 이용해서 대략 90분 주기로 그룹 정책을 백그라운드로 적용하는 작업을 수행할 것인지 여부를 제어할 수 있습니다. 특정 CSE에 이 옵션을 선택하면 CSE는 컴퓨터가 시작할 때와 사용자가 로그온 할 때만 로딩되어 정책을 다운로드 받아 적용합니다.

- **변경되지 않아도 그룹 정책 개체 처리** : 디폴트로 클라이언트에 기 적용된 GPO는 정책 설정이 변경되지 않는 한, 다시 다운로드 받아 적용하지 않습니다. 하지만 클라이언트에 administrator 권한을 가지는 사용자일 경우에는 GPO에 의해 설정된 레지스트리나 NTFS 권한을 변경할 수 있습니다. 따라서 관리자는 필요에 따라 클라이언트에 기 적용된 GPO가 변경되지 않아도, 컴퓨터 시작 및 사용자 로그온 할 때나 정기적인 백그라운드 작업 시에 이 옵션이 설정된 CSE는 항상 다시 정책 설정을 재 적용하도록 설정할 수 있습니다.

CSE 별로 동작 방식을 제어하는 최대 세 개의 옵션을 제공하지만, 일부 CSE에는 두 개의 옵션만 제공합니다. 이런 경우에는 해당 CSE에 특정 옵션이 적절치 못하기 때문입니다. 〈표 5〉는 특정 옵션을 제공하지 않는 CSE와 그 이유에 대해 정리한 것입니다.

CSE	미 제공 옵션	이유
레지스트리 정책	✓ 저속 네트워크 연결에서 처리 허용	✓ 다른 CSE 옵션을 제어하기 때문에 저속 네트워크와 상관없이 정책을 다운로드 해서 적용
보안 정책	✓ 저속 네트워크 연결에서 처리 허용	✓ 보안 정책의 일관성을 유지하기위해 저속 네트워크와 상관없이 정책을 다운로드 해서 적용
폴더 리디렉션 정책	✓ 정기적인 백그라운드 작업을처리하는 동안 적용 안 함	✓ 사용자 로그온 시에만 처리
소프트웨어 설치 정책	✓ 정기적인 백그라운드 작업을처리하는 동안 적용 안 함	✓ 컴퓨터 시작/사용자 로그온 시에만 처리

표 5 예외 옵션을 가지는 CSE

레지스트리 정책과 보안 정책을 처리하는 CSE는 저속 네트워크로 연결되어 있다 할 지라도 주요 보안 정책의 일관적인 적용을 유지하기 위해서 저속 네트워크 연결에서 처리 허용 옵션을 제공하지 않습니다. 따라서 레지스트리 정책과 보안 정책은 저속 네트워크 연결 여부와 상관없이 항상 클라이언트에 다운로드 되어 적용됩니다.

폴더 리디렉션 정책은 사용자가 로그온 할 때에만 적용되기 때문에 정기적인 백그라운드 작업을 처리하는 동안 적용 안 함 옵션을 제공하지 않습니다. 사용자가 로그온 해서 내 문서에서 작업을 수행하는 중에, 관리자가 변경한 폴더 리디렉션 정책이 백그라운드에서 적용 되어 내 문서가 네트워크에 지정된

서버로 리디렉션 된다면 오류가 발생할 수 있기 때문입니다.

유사한 이유로 소프트웨어 설치 정책도 정기적인 백그라운드 작업을 처리하는 동안 적용 안 함 옵션을 제공하지 않습니다. 따라서 소프트웨어 설치 정책은 컴퓨터 시작과 사용자 로그온 시에만 적용됩니다.

Initial Processing

GPO의 컴퓨터 구성에 설정된 정책들은 컴퓨터가 시작할 때 적용됩니다. 반면에 GPO의 사용자 구성에 설정한 정책들은 사용자가 로그온 할 때 적용됩니다. 그룹 정책은 디폴트로 동기화 방식으로 처리됩니다. 컴퓨터가 시작할 때 컴퓨터에게 적용해야 할 GPO들이 우선 순위에 따라 다운로드 되어 순차적으로 정책 적용이 모두 완료 되어야만 WinLogon 대화 상자가 나타납니다. 사용자가 로그온 할 때도 마찬가지로 사용자에게 적용해야 할 GPO들이 우선 순위에 따라 다운로드 되어 순차적으로 정책 적용이 모두 완료 되어야만, 사용자 데스크탑이 복원됩니다.

[동기화 방식과 비 동기화 방식]
그룹 정책에서 동기화 방식은 하나의 GPO가 다운로드 되어 클라이언트에 적용이 완료되어야만, 다음 적용할 GPO가 처리되는 방식을 의미합니다. 반면에 비 동기화 방식은 클라이언트에 적용해야 할 GPO를 동시 다발적으로 다운로드 받아 클라이언트에 적용하는 방식을 의미합니다.

디폴트로 그룹 정책 처리 방식은 동기화 방식으로 설정되어 있기 때문에 하나의 GPO 처리가 완료되어야만 다음 작업이 진행됩니다. 관리자는 정책 설정을 이용해서 동기화 방식 대신 비 동기화 방식으로 GPO가 처리되도록 제

어할 수 있습니다. 하지만 비 동기화 방식으로 GPO를 처리하면 예측할 수 없는 일들이 발생할 수 있기 때문에 권장하지 않습니다.

예를 들어 GPO에서 시작 메뉴의 실행 메뉴를 제거하는 정책을 설정했다고 가정하겠습니다. 비 동기화 방식으로 설정되기 때문에 사용자 로그온 시에 GPO가 순차적으로 적용된 후 사용자 데스크탑이 복원 되는 것이 아니라, 사용자 데스크탑이 복원됨과 동시에 백그라운드에서 적용할 GPO들이 적용됩니다. 만일 실행 메뉴를 제거하는 정책이 적용되기 전에 데스크 탑이 복원된다면 사용자는 시작 메뉴의 실행 메뉴에 접근할 수 있습니다. 그 후 정책이 적용되면 실행 메뉴가 제거될 것이지만, 정책의 일관성 측면이 결여되고 사용자의 혼란을 유발할 수 있습니다.

[Windows XP Fast Logon]
디폴트로 도메인이나 워크그룹 멤버인 Windows XP Professional에 대해 Fast Logon 기능을 제공합니다. 이 기능은 사용자가 보다 빠르게 컴퓨터에 로그온 할 수 있도록 하기 위해 컴퓨터가 시작할 때 네트워크를 초기화 하지 않고, 사용자가 로그온 한 후에 네트워크를 초기화 합니다. 따라서 도메인에 가입한 클라이언트의 경우에는 캐시 된 정보를 이용해서 사용자를 로그온 한 후, 네트워크가 초기화 되면 비 동기화 방식으로 컴퓨터 정책과 사용자 정책을 적용합니다.

따라서 이 기능을 이용하면 컴퓨터가 시작할 때 컴퓨터 정책을 적용하는 과정이 생략되고, 컴퓨터와 사용자 정책이 사용자 데스크탑 복원 후에 비 동기화 방식으로 처리되기 때문에 사용자 입장에서 빠른 데스크탑 사용이 가능합니다.

하지만 다음과 같은 경우에 사용자 정책만은 동기화 방식으로 처리합니다. 즉 로그온 시에 네트워크를 초기화 한 후, 사용자 정책을 모두 적용한 후에 사용자 데스크탑을 복원합니다. 다음과 같은 경우에도 컴퓨터 정책은 여전히 사용자 데스크탑 복원 후에 백그라운드에서 비 동기화 방식으로 처리합니다.

- **사용자가 해당 클라이언트 컴퓨터에 최초 로그온** : 해당 클라이언트에 처음 로그온 하는 경우에는 로컬에 캐시 된 사용자 정보가 없기 때문에 네트워크를 초기화 한 후, 도메인 인증을 거쳐야 합니다. 인증 후에는 동기화 방식으로 사용자 정책이 적용됩니다.

- **사용자가 로밍 프로필이나 홈 폴더를 사용**

- **사용자에게 동기화 방식으로 동작하는 로그온 스크립트가 적용되어 있는 경우**

관리자는 컴퓨터 구성\관리 템플릿\시스템\로그온 노드에서 〈그림 31〉과 같이 컴퓨터 시작 및 로그온 시 네트워크가 초기화될 때까지 항상 대기 정책을 사용으로 설정함으로써 도메인 환경하에서 Fast Logon 기능을 사용하지 않도록 정책 설정이 가능합니다.

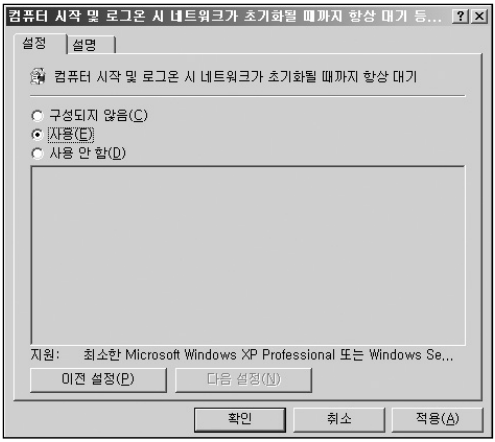

그림 31 Windows XP Fast Logon 기능 정지

Background Processing

GPO는 컴퓨터가 시작하고 사용자가 로그온 할 때 적용되면서, 또한 정기적으로 백그라운드에서 변경된 정책이 적용됩니다. 정기적 백그라운드 정책 적용 시에 CSE는 오직 정책 설정이 변경된 GPO를 검색하여 설정을 클라이언트에 적용합니다.

모든 CSE가 정기적 백그라운드 정책 적용 시에 동작하는 것은 아닙니다. 소프트웨어 설치 및 폴더 리디렉션은 컴퓨터가 시작하고 사용자가 로그온 할 때만 적용됩니다.

도메인에 가입한 클라이언트 컴퓨터는 디폴트로 90분에 랜덤하게 발생한 0에서 30분의 오프셋 간격을 더한 시간 간격으로 그룹 정책을 적용합니다. 도메인 컨트롤러의 경우에는 보다 빠르게 수정된 정책이 적용되도록 하기 위해 5분 간격으로 그룹 정책이 적용합니다.

클라이언트의 백그라운드 정책 적용 예를 들면, ComA 컴퓨터는 90분에 랜덤하게 발생한 오프셋 시간이 10분이면 100분 주기로 도메인 컨트롤러에 접속하여 변경된 GPO를 검색하고, 정책을 다운로드 합니다. ComB 컴퓨터의 경우에 90분에 랜덤하게 발생한 오프셋 시간이 25분이면 115분 주기로 백그라운드 정책 적용을 수행합니다. 최소 0에서 최대 30분까지의 랜덤한 오프셋 시간을 더하는 이유는 클라이언트 별로 서로 다른 주기로 정책을 적용하게 함으로써, 도메인 컨트롤러에 한꺼번에 많은 클라이언트가 동시에 백그라운드 정책 적용을 위해 접근하는 것을 막기 위함입니다.

백그라운드 정책 적용 주기는 정책 설정을 통해 변경할 수 있습니다. 주의할 사항은 정책 적용 주기를 너무 짧게 설정하면, 백그라운드 정책 적용 할 때 Windows Shell이 재시작하면서 화면이 깜빡 거리는 현상이 자주 발생하여 사용자 불편을 초래할 수 있습니다.

관리자는 컴퓨터 구성\관리 템플릿\시스템\그룹 정책 노드에서 도메인 컨트롤러에 대한 그룹 정책 새로 고침 정책의 설정을 수정하여 도메인 컨트롤러의 백그라운드 정책 적용 주기를 변경 할 수 있습니다.

또한 관리자는 컴퓨터 구성\관리 템플릿\시스템\그룹 정책 노드에서 〈그림 32〉와 같이 컴퓨터에 대한 그룹 정책 새로 고침 정책의 설정을 수정하여 클라이언트의 백그라운드 정책 적용 주기를 변경 할 수 있습니다.

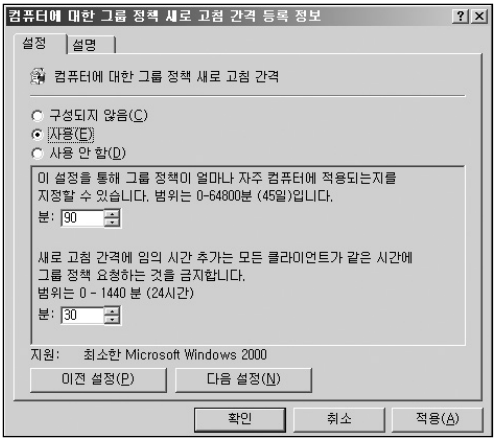

그림 32 백그라운드 정책 적용 주기 변경

On-Demand Processing

관리자는 백그라운드 정책 적용 주기와 상관없이 변경된 그룹 정책이 바로 클라이언트에 적용되도록 해야 할 경우가 있습니다.

이런 경우에 관리자는 클라이언트 컴퓨터에 다음과 같은 gpupdate.exe 명령어를 이용해서 그룹 정책 적용을 강제화 할 수 있습니다.

gpupdate [/target:{computer | user}] [/force] [/logoff] [/boot]

gpupdate 명령에 사용할 수 있는 옵션은 〈표 6〉과 같습니다.

옵션	설명
/target:{computer | user}	지정한 매개 변수에 따라 컴퓨터 정책(computer) 또는 사용자 정책(user)을 적용합니다. Target 옵션을 생략하면 gpupdate는 컴퓨터 정책과 사용자 정책을 모두 클라이언트에 적용합니다.
/force	모든 GPO의 정책을 다시 강제 재 적용합니다. Force 옵션을 생략하면 gpupdate는 변경된 정책 설정만 다운로드 해서 클라이언트에 적용합니다.
/logoff	정책 적용 후에 로그오프 합니다. 이 옵션은 소프트웨어 설치, 폴더 리디렉션과 같이 컴퓨터 시작 또는 사용자 로그온 시에만 적용되는 정책을 적용하기 위해 사용자를 로그오프 시킬 때 사용합니다.
/boot	정책 적용 후에 컴퓨터를 재시작합니다. 이 옵션은 소프트웨어 설치, 폴더 리디렉션과 같이 컴퓨터 시작 또는 사용자 로그온 시에만 적용되는 정책을 적용하기 위해 컴퓨터를 재시작 시킬 때 사용합니다.
/?	옵션들에 대한 도움말을 출력합니다.

표 6 gpupdate 옵션

저속 연결

클라이언트에서 그룹 정책을 적용할 때, 클라이언트와 도메인 컨트롤러가 저속 네트워크로 연결된 것으로 감지되면, 개별 CSE 별로 그룹 정책의 저속 네트워크 연결에서 처리 허용 옵션 설정 여부를 점검하여 정책 설정의 다운로드 여부를 결정합니다.

CSE 별로 저속 네트워크에서 처리 허용 여부 설정은 〈표 7〉과 같습니다.

CSE	처리 허용 여부	비고
레지스트리 정책	허용 함	정책 설정을 이용해서 허용 안 함으로 변경 불가. 정책 일관성을 위해 저속 네트워크 연결 여부와 상관없이 항상 정책 적용 함
보안 정책	허용 함	정책 설정을 이용해서 허용 안함으로 변경 불가. 정책 일관성을 위해 저속 네트워크 연결 여부와 상관없이 항상 정책 적용 함
소프트웨어 설치 정책	허용 안 함	정책 설정을 이용해서 허용 안 함으로 변경 가능
스크립트	허용 안 함	정책 설정을 이용해서 허용 안 함으로 변경 가능
폴더 리디렉션 정책	허용 안 함	정책 설정을 이용해서 허용 안 함으로 변경 가능

표 7 저속 네트워크에서 처리 허용 여부

그룹 정책은 IP Ping 알고리즘을 이용해서 저속 네트워크를 여부를 감지합니다. 따라서 클라이언트와 도메인 컨트롤러 사이에 ICMP 프로토콜 사용이 가능해야만 저속 네트워크 여부를 감지할 수 있습니다. 만일 클라이언트와 도메인 컨트롤러 사이에 ICMP 프로토콜 통신이 허용되지 않으면, 관리자는 컴퓨터 구성\관리 템플릿\시스템\그룹 정책 노드에서 그룹 정책 저속 연결 검색 정책을 사용 안 함으로 설정할 것을 권장합니다.

디폴트로 500 Kbps 미만을 저속 네트워크로, 그 이상을 고속 네트워크로 인지합니다. 이 값은 컴퓨터 구성\관리 템플릿\시스템\그룹 정책 노드에서 〈그림 33〉과 같이 그룹 정책 저속 연결 검색 정책의 설정을 이용해서 변경할 수 있습니다.

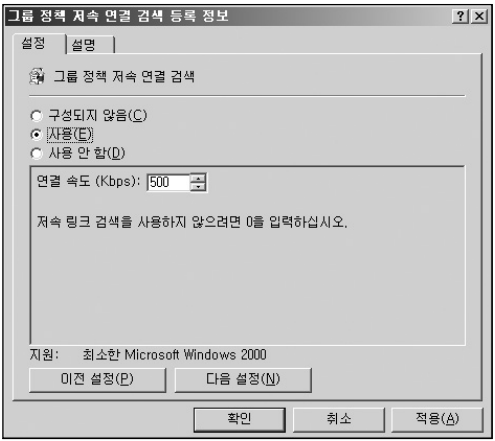

그림 33 저속 네트워크 연결 속도 설정

그룹 정책 모델링과 결과

관리자는 그룹 정책 모델링과 그룹 정책 결과를 이용해서 그룹 정책에 대한 계획, 적용 결과, 문제 해결까지 다양한 관리 작업에 활용할 수 있습니다. 복잡한 Active Directory 구조와 많은 수의 GPO가 연결되어 있는 경우에는 컴퓨터와 사용자에게 적용되는 정책 설정들에 충돌이 발생할 수 있습니다. 충돌이 발생하면 가장 마지막에 적용된 GPO의 정책 설정 값이 최종적으로 적용됩니다.

관리자는 Windows XP와 Windows Server 2003에서 제공하는 정책 결과 집합(RSoP)를 이용해서 컴퓨터와 사용자에게 적용된 GPO 목록과 최종 적용된 설정 결과까지 정보를 확인할 수 있습니다.

관리자는 다음과 같은 정보를 확인하고 할 때, 정책 결과 집합을 사용하면 유용합니다.

- 최종적으로 컴퓨터와 사용자에게 적용된 정책 설정 값
- 최종적으로 적용된 정책 설정 값을 지정하는 GPO (Winning GPO)
- 충돌이 발생한 정책 설정을 적용하려는 GPO들의 우선 순위 및 각 GPO가 적용하려고 한 정책 설정 값

그룹 정책 모델링

Windows Server 2003은 실제로 그룹 정책을 적용하기 전에 컴퓨터와 사용자에게 적용될 그룹 정책을 시뮬레이션 할 수 있는 그룹 정책 관리 기능을 제공합니다. 이 기능을 Windows Server 2003에서는 그룹 정책 결과 집합(RSoP)-계획 모드라고 부르고, GPMC에서는 그룹 정책 모델링이라고 부릅니다.

그룹 정책 모델링은 Windows Server 2003이 설치된 도메인 컨트롤러에서만 동작하는 서비스에 의해 수행되기 때문에, 이 기능을 사용하기 위해서는 포리스트에 적어도 한 대 이상의 Windows Server 2003 운영 체제가 설치된 도메인 컨트롤러가 존재해야 합니다.

그룹 정책 모델링을 이용해서 관리자는 기존 Active Directory 환경하에서 그룹 정책을 적용하기 전에 컴퓨터나 사용자에게 적용할 그룹 정책을 시뮬레이션 할 수 있습니다. 또한 컴퓨터나 사용자가 속한 보안 그룹이나 조직 구성 단위가 변경될 경우에 컴퓨터나 사용자에게 적용될 정책의 변화에 대해서도 시뮬레이션이 가능합니다.

[따라하기] 그룹 정책 모델링을 사용해서 정책 시뮬레이션 하기

GPMC의 그룹 정책 모델링을 이용해서 컴퓨터나 사용자에게 적용될 그룹 정책을 시뮬레이션 하는 과정은 다음과 같습니다.

1. GPMC의 Group Policy Modeling 노드를 마우스 오른쪽 버튼으로 클릭한 후, Group Policy Modeling Wizard 메뉴를 선택합니다.

2. Group Policy Modeling Wizard가 실행됩니다. 간단한 도움말을 읽은 후에 다음 버튼을 클릭합니다.
3. 시뮬레이션을 수행할 도메인 컨트롤러를 선택합니다. 디폴트로 Any available domain controller running Windows Server 2003 or later 옵션이 선택되어 있어서 Windows Server 2003 이상 운영 체제가 설치된 임의의 도메인 컨트롤러에서 시뮬레이션을 수행합니다. 특정 도메인 컨트롤러에서 시뮬레이션을 수행하길 원한다면 This domain controller 옵션을 선택한 후, 시뮬레이션을 수행 할 도메인 컨트롤러를 목록에서 선택합니다.
   시뮬레이션을 수행할 도메인 컨트롤러를 적절히 선택한 후, 다음 버튼을 클릭합니다.

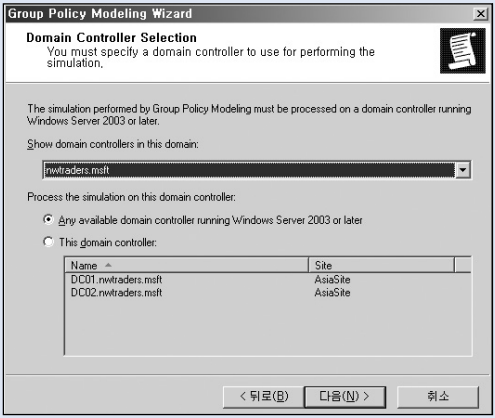

그림 34 시뮬레이션을 수행할 도메인 컨트롤러 선택

4. 적용될 그룹 정책을 시뮬레이션 할 컴퓨터나 사용자 계정 또는 컨테이너를 지정합니다.

   도메인이나 조직 구성 단위에 속해 있는 모든 사용자에게 적용되는 정책을 시뮬레이션 하려면 User information의 Container 옵션을 선택한 후, 도메인이나 조직 구성 단위를 Browse 버튼을 클릭하여 지정합니다. 특정 사용자 계정에 적용되는 정책을 시뮬레이션 하려면 User 옵션을 선택한 후, 사용자 계정을 Browse 버튼을 클릭하여 지정합니다.

   도메인이나 조직 구성 단위에 속해 있는 모든 컴퓨터에게 적용되는 정책을 시뮬레이션 하려면 Computer information의 Container 옵션을 선택한 후, 도메인이나 조직 구성 단위를 Browse 버튼을 클릭하여 지정합니다. 특정 컴퓨터 계정에 적용되는 정책을 시뮬레이션 하려면 Computer 옵션을 선택한 후, 컴퓨터 계정을 Browse 버튼을 클릭하여 지정합니다.

   〈그림 35〉에서는 nwtraders.msft 도메인의 본사 OU에 존재하는 ComA 컴퓨터 개체와 Gildong.Hong 사용자 계정에게 적용되는 정책을 시뮬레이션 하기 위해 해당 개체를 지정했습니다. 정책을 시뮬레이션 할 대상을 지정한 후, 다음 버튼을 클릭합니다.

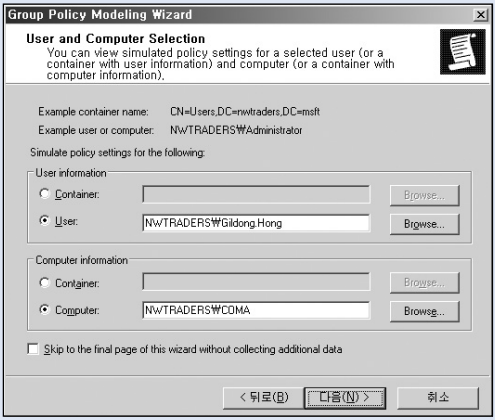

그림 35 시뮬레이션을 수행할 대상 컴퓨터와 사용자 개체 선택

5. 컴퓨터 개체에 적용되는 정책을 시뮬레이션 하기 위해 추가 옵션을 선택합니다. 컴퓨터가 저속 네트워크에 연결되었을 때 적용되는 정책을 시뮬레이션 하려면, Slow network connection 옵션을 선택합니다. 루프백 처리가 동작할 경우에 적용되는 정책을 시뮬레이션 하려면, Loopback processing 옵션을 선택한 후, 처리 모드를 선택합니다. 컴퓨터가 특정 사이트에 속했을 때 적용되는 정책을 시뮬레이션 하려면, Site 목록에서 사이트를 선택합니다.

   시뮬레이션 하기 원하는 추가 옵션을 선택한 후, 다음 버튼을 클릭합니다.

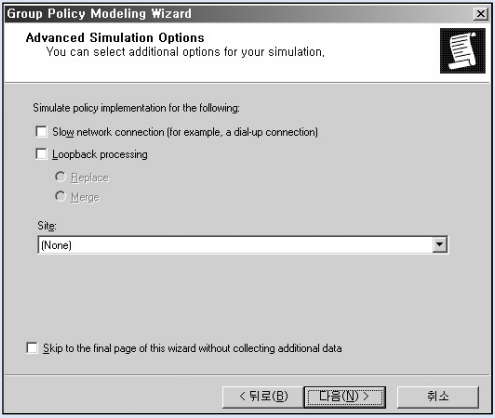

그림 36 시뮬레이션 옵션 선택

6. 디폴트로 현재 사용자와 컴퓨터 계정이 속해 있는 컨테이너의 경로가 입력되어 있습니다. 만약 사용자나 컴퓨터 계정이 다른 OU로 이동했을 경우에 적용되는 정책 설정의 변화를 시뮬레이션 하길 원한다면 User location과 Computer location에 계정이 이동할 OU 경로를 입력한 후, 다음 버튼을 클릭합니다.

〈그림 37〉에서는 본사 OU에 있는 사용자 계정이 연구소 OU로 위치가 변경되었을 경우를 시뮬레이션 하기 위해 연구소 OU의 경로를 입력했습니다.

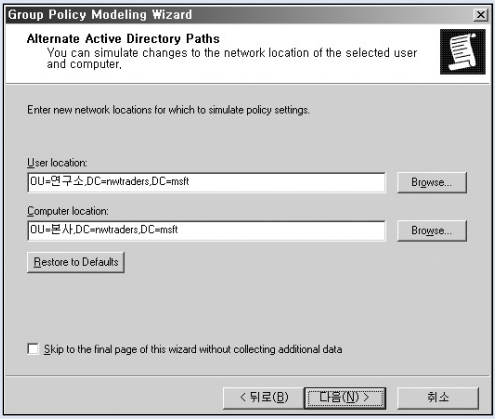

그림 37 대체 Active Directory 경로 지정

7. 현재 사용자 계정이 구성원으로 포함되어 있는 보안 그룹이 출력됩니다. 만약 사용자 계정을 포함하는 보안 그룹이 변경되었을 경우에 적용되는 정책 설정의 변화를 시뮬레이션 하길 원한다면 Add와 Remove 버튼을 클릭해서 사용자 계정을 포함하는 보안 그룹을 변경한 후, 다음 버튼을 클릭합니다.

그림 38 사용자 보안 그룹 변경

8. 현재 컴퓨터 계정이 구성원으로 포함되어 있는 보안 그룹이 출력됩니다. 만약 컴퓨터 계정을 포함하는 보안 그룹이 변경되었을 경우에 적용되는 정책 설정의 변화를 시뮬레이션 하길 원한다면, Add와 Remove 버튼을 클릭해서 컴퓨터 계정을 포함하는 보안 그룹을 변경한 후, 다음 버튼을 클릭합니다.
9. 사용자 계정에게 적용할 WMI 필터를 선택합니다. GPO에 연결되어 있는 모든 WMI 필터가 조건을 만족할 경우에, 사용자에 적용되는 정책 설정을 시뮬레이션 하기 위해서는 All linked filters 옵션을 선택합니다. 특정 WMI 필터만 조건을 만족할 경우에, 사용자에 적용되는 정책 설정을 시뮬레이션 하기 위해서는 Only these filters 옵션을 선택한 후, 목록에서 적용 할 WMI 필터를 선택합니다.

사용자 계정에게 적용할 WMI 필터를 선택한 후, 다음 버튼을 클릭합니다.

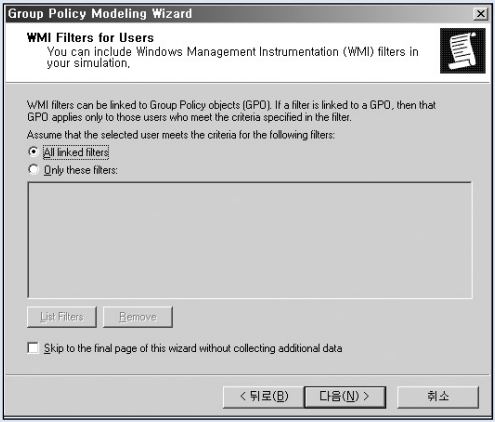

그림 39 시뮬레이션 할 WMI 필터 선택

10. 컴퓨터 계정에게 적용할 WMI 필터를 선택합니다. GPO에 연결되어 있는 모든 WMI 필터가 조건을 만족할 경우에, 컴퓨터에 적용되는 정책 설정을 시뮬레이션 하기 위해서는 All linked filters 옵션을 선택합니다. 특정 WMI 필터만 조건을 만족할 경우에, 컴퓨터에 적용되는 정책 설정을 시뮬레이션 하기 위해서는 Only these filters 옵션을 선택한 후, 목록에서 적용 할 WMI 필터를 선택합니다.
    컴퓨터 계정에게 적용할 WMI 필터를 선택한 후, 다음 버튼을 클릭합니다.

11. 선택한 시뮬레이션 할 조건들에 대한 요약 정보가 출력됩니다. 〈그림 40〉에서는 사용자 계정을 지정한 OU로 이동할 경우만을 시뮬레이션 하도록 설정하고, 나머지 조건은 선택하지 않았습니다.
정책 설정을 시뮬레이션 할 조건들을 확인한 후, 다음 버튼을 클릭합니다. 선택한 조건에 따라 그룹 정책에 대한 시뮬레이션이 수행됩니다.

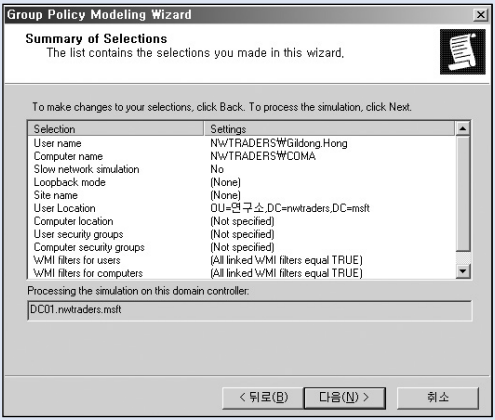

그림 40 선택 사항 요약

12. 마침 버튼을 클릭하여 Group Policy Modeling Wizard를 종료합니다.

Group Policy Modeling Wizard를 종료하면 Group Policy Modeling 노드 아래에 RSoP 데이터를 출력하는 새로운 노드가 생성되며, 이 노드를 이용해서 관리자는 향후 입력한 조건에 따라 시뮬레이션 된 정책 결과 집합을 언제든지 확인 할 수 있습니다.

정책 결과 집합을 출력하는 노드는 〈그림 52〉와 같이 세 개의 탭을 통해 정보를 제공합니다.

- Summary : GPO, 보안 그룹, WMI 필터를 포함한 시뮬레이션 결과에 따른 요약 정보를 HTML 리포트로 제공합니다.

- Settings : 선택한 조건에 따라 컴퓨터와 사용자에게 적용 될 정책 설정값을 HTML 리포트로 제공합니다.

- Query : Group Policy Modeling Wizard를 이용해서 입력한 시뮬레이션 조건을 출력합니다.

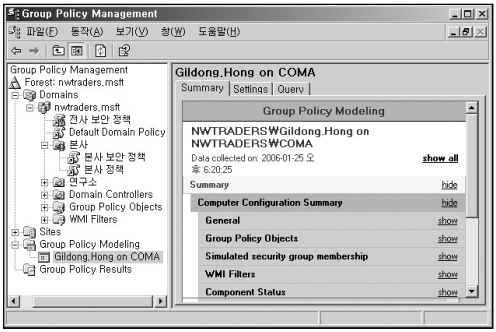

그림 41 시뮬레이션 한 정책 결과 집합 출력

그룹 정책 결과

그룹 정책 결과는 지정한 컴퓨터와 그 컴퓨터에 로그온 한 사용자에게 적용된 그룹 정책 설정 값을 수집하여 출력합니다. 이 기능을 Windows Server 2003에서는 그룹 정책 결과 집합(RSoP)-로깅 모드라고 부르고, GPMC에서는 그룹 정책 결과라고 부릅니다.

출력된 정보는 그룹 정책 모델링에서 보여주는 정보와 유사해 보이지만, 도메인 컨트롤러에서 시뮬레이션 한 결과를 보여주는 그룹 정책 모델링과는 달리, 그룹 정책 결과는 지정한 컴퓨터에서 직접 적용된 정책 설정 값을 수집합니다.

지정한 컴퓨터에서 직접 데이터를 수집하기 때문에, 그룹 정책 결과는 Windows XP, Windows Server 2003 이상에서만 적용된 정책 설정 값을 수

집할 수 있습니다. 따라서 Windows 2000 클라이언트에 대해서는 그룹 정책 결과를 수집할 수 없습니다.

[따라하기] 그룹 정책 결과를 이용해서 적용된 정책 설정 값 수집하기

GPMC의 그룹 정책 결과를 이용해서 특정 컴퓨터와 그 컴퓨터에 로그온 한 사용자에게 적용된 그룹 정책 설정 값을 수집하는 과정은 다음과 같습니다.

1. GPMC의 Group Policy Results 노드를 마우스 오른쪽 버튼으로 클릭한 후, Group Policy Results Wizard 메뉴를 선택합니다.
2. Group Policy Results Wizard가 실행됩니다. 간단한 도움말을 읽은 후에 다음 버튼을 클릭합니다.
3. 정책 결과 집합을 수집할 대상 컴퓨터를 지정합니다. 현재 GPMC를 실행하는 컴퓨터에서 정책 결과 집합을 수집하려면 This computer 옵션을 선택합니다. 다른 컴퓨터에서 정책 결과 집합을 수집하려면 Another Computer 옵션을 선택한 후, Browser 버튼을 클릭하여 원하는 대상 컴퓨터 이름을 지정합니다.

   대상 컴퓨터를 지정한 후, 다음 버튼을 클릭합니다.

그림 42 정책 설정 값을 수집할 컴퓨터 선택

4. 정책 결과 집합을 수집할 대상 사용자를 지정합니다. 정책 결과 집합을 수집하기 위해 지정한 컴퓨터에 현재 로그온 한 사용자 계정이 출력됩니다. 현재 로그온 한 사용자 계정의 정책 결과 집합을 수집하기 위해서 사용자 계정이 선택되어 있는지 확인합니다. 만약 사용자에게 적용된 정책 결과 집합을 수집하지 않으면, Do not display user policy settings in the results 옵션을 선택합니다.

   대상 사용자를 지정한 후, 다음 버튼을 클릭합니다.

그림 43 정책 설정 값을 수집할 사용자 선택

5. 〈그림 44〉와 같이 정책 결과 집합을 수집하도록 지정한 컴퓨터와 사용자 계정에 대한 요약 정보가 출력됩니다.
선택 조건들을 확인한 후, 다음 버튼을 클릭합니다. 선택한 조건에 따라 대상 컴퓨터에 접속하여 컴퓨터와 사용자에게 적용된 그룹 정책 설정 값 데이터를 수집합니다.

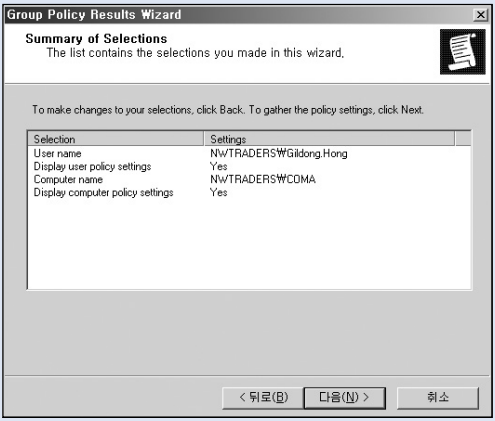

그림 44 선택 사항 요약

Group Policy Results Wizard를 종료하면 Group Policy Results 노드 아래에 수집된 그룹 정책 결과 데이터를 출력하는 새로운 노드가 생성되며, 이 노드를 이용해서 관리자는 지정한 컴퓨터와 사용자에게 적용된 정책 결과 집합을 확인 할 수 있습니다.

정책 결과 집합을 출력하는 노드는 〈그림 45〉와 같이 세 개의 탭을 통해 정보를 제공합니다.

- Summary : GPO, 보안 그룹, WMI 필터를 포함한 수집 결과에 따른 요약 정보를 HTML 리포트로 제공합니다.

- Settings : 컴퓨터와 사용자에게 적용 된 정책 설정 값을 HTML 리포트로 제공합니다.

- Events : 지정한 컴퓨터에 기록된 그룹 정책과 관련한 이벤트를 수집하여 출력합니다. 이 정보는 그룹 정책과 관련한 문제 해결에 유용합니다.

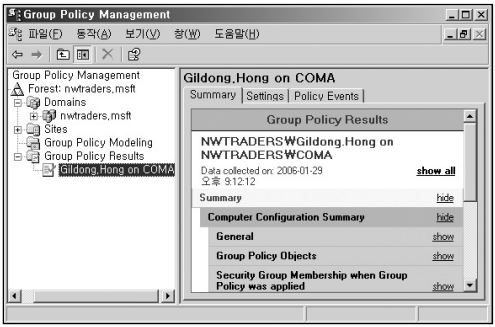

그림 45 수집한 정책 결과 집합 출력

그룹 정책 권한 위임

Windows 2000 또는 Windows Server 2003으로 구성된 Active Directory에서 그룹 정책은 관리의 중요한 한 부분을 차지합니다. 그룹 정책을 관리하기 위해 필요한 다양한 작업들을 수행할 수 있는 권한을 적절한 관리자들에게 위임함으로써 효율적인 그룹 정책 관리가 가능합니다.

특히 복잡한 엔터프라이즈 급의 Active Directory 환경하에서 한 명의 관리자가 그룹 정책의 모든 관리 작업을 수행하면 상당한 부하가 발생할 수 있습니다. 따라서 GPO 생성, 수정, 연결등과 같은 일련의 관리 작업들을 서로 다른 관리자에게 각각 권한 위임함으로써 관리의 효율성을 높일 수 있습니다.

그룹 정책에서는 다음과 같은 권한 위임이 가능합니다.

- GPO에 대한 권한 위임
  - GPO 생성
  - GPO 수정

- SOM에 대한 권한 위임
  - SOM에 GPO 연결
  - SOM에 대한 그룹 정책 모델링 작업 수행
  - SOM에 대한 그룹 정책 결과 집합 정보 수집

- WMI 필터에 대한 권한 위임
  - WMI 필터 생성
  - WMI 필터 수정

GPMC에서는 권한 위임을 보다 손쉽게 설정할 수 있습니다. GPMC 이전에 관리자는 특정 관리자에서 그룹 정책과 관련한 권한을 위임하기 위해 ACE 에디터를 이용해야만 했지만, GPMC에서는 Delegation 탭을 이용해서 보다 쉽게 권한 위임이 가능합니다. 만일 관리자가 ACL 에디터를 이용해서 권한 위임을 수행하길 원한다면 Delegation 탭의 Advanced 버튼을 클릭하여 여전히 ACL 에디터를 사용할 수 있습니다.

GPO에 대한 권한 위임

관리자는 GPO에 대한 두 관리 작업을 수행할 수 있는 권한을 다른 관리자에게 위임할 수 있습니다. 첫 번째 관리 작업은 GPO를 생성할 수 있는 권한이고, 두 번째 관리 작업은 GPO를 수정할 수 있는 권한입니다.

GPO 생성

디폴트로 Group Policy Creator Owners 그룹의 구성원은 GPO를 생성할 수 있습니다. GPMC가 발표되기 이전에 GPO를 생성하는 권한을 위임하는 유일한 방법은 Group Policy Creator Owners 그룹의 구성원에 대상 관리자의 계정을 포함시키는 것이었습니다.

하지만 GPMC에서는 Group Policy Object 노드의 Delegation 탭에서 GPO를 생성할 수 있는 권한을 위임하는 기능이 제공됩니다. Delegation 탭은 Group Policy Creator Owners 그룹을 포함해서 도메인에 GPO를 생성할 수

있는 권한을 가지는 그룹이나 사용자 계정 목록을 출력합니다. 관리자는 기존에 추가되어 있는 그룹의 구성원을 변경하거나 또는 그룹을 추가, 제거하는 관리 작업을 수행할 수 있습니다.

도메인에 GPO를 생성할 수 있는 권한을 위임 받은 관리자는 GPO를 생성할 수 있고, 본인이 생성한 GPO에 대해서는 모든 권한을 행사할 수 있습니다. 하지만 생성한 GPO를 특정 SOM에 연결하는 권한은 없으며, 또한 본인이 생성하지 않은 다른 GPO를 수정하거나 삭제할 수 없습니다.

[따라하기] GPO 생성 권한 위임하기

GPMC를 이용해서 GPO를 생성할 수 있는 권한을 위임하는 과정은 다음과 같습니다.

1. GPMC의 Group Policy objects 노드를 클릭합니다.
2. Delegation 탭을 클릭합니다. 〈그림 46〉과 같이 현재 도메인에 GPO를 생성할 수 있는 권한을 가지는 그룹이나 사용자 계정 목록이 출력됩니다.

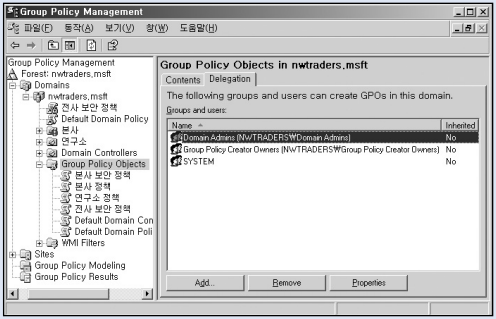

그림 46 GPO 생성 권한 위임

3. Add 버튼을 클릭한 후, GPO를 생성할 수 있는 권한을 위임할 그룹이나 사용자 계정을 추가합니다. Properties 버튼을 클릭하면 기존에 추가되어 있는 그룹의 구성원을 변경 할 수 있습니다.

GPO 수정

GPMC를 이용하면 관리자는 개별 GPO에 대한 권한 위임을 간편하게 수행할 수 있습니다. GPMC 이전에, 관리자는 ACL 편집기를 이용해서 GPO에 대해 사용 권한을 직접 부여 했습니다.

GPMC를 이용해서 관리자는 개별 GPO에 대해 〈표 8〉과 같은 권한을 위임할 수 있습니다.

사용 권한	설명
Read	GPO에 대한 읽기 권한을 부여합니다.
Edit settings	GPO에 대한 읽기, 쓰기, 모든 자식 개체 만들기, 모든 자식 개체 삭제 권한을 부여합니다. 개별 GPO에 대해 이 권한을 부여 받은 관리자는 정책 설정을 수정할 수 있습니다.
Edit, delete, and modify security	GPO에 대한 읽기, 쓰기, 모든 자식 개체 만들기,모든 자식 개체 삭제, 삭제, 사용 권한 수정, 소유자 수정 권한을 부여합니다. 이 사용 권한을 선택하면 "그룹 정책 적용" 권한만 제외하고 GPO에 대한 모든 권한을 부여합니다.

사용 권한	설명
Read (from Security Filtering)	GPO가 적용되도록 Security Filtering 섹션에서 설정한 그룹이나 사용자 계정에게 부여되는 권한입니다. GPO에 대해 읽기와 그룹 정책 적용 권한을 부여합니다.
Custom	ACL 편집기를 이용해서 GPO에 대해 다양한 사용 권한을 부여할 수 있습니다.

표 8 GPO 사용 권한

〈표 8〉의 사용 권한 중에 Read/Edit settings/Edit, delete, and modify security는 관리자가 개별 GPO에 대해 보다 빠르게 권한 위임을 할 수 있도록 자주 사용하는 ACL을 조합한 것입니다. 관리자가 다른 관리자에게 GPO에 대한 권한을 위임할 때는 다음 두 사용 권한을 주로 사용합니다.

- Edit settings
- Edit, delete, and modify security

특정 GPO에 대해 정책 설정만을 수정할 수 있도록 권한을 위임할 경우에는 대상 관리자에게 Edit settings 사용 권한을 부여하면 됩니다. 반면에 특정 GPO에 대해 모든 권한을 위임할 경우에는 Edit, delete, and modify security 사용 권한을 부여하면 됩니다.

[따라하기] GPO 수정 권한 위임하기

GPMC를 이용해서 개별 GPO를 수정 할 수 있는 권한을 위임하는 과정은 다음과 같습니다.

1. GPMC의 Group Policy objects 노드에서 정책 설정을 수정할 수 있도록 권한을 위임할 GPO를 클릭 합니다.
2. Delegation 탭을 클릭합니다. 현재 선택된 GPO에 사용 권한을 가지는 그룹이나 사용자 계정 목록이 출력됩니다.
3. 선택한 GPO에 대한 관리 권한을 위임할 그룹이나 사용자 계정을 선택하기 하기 위해 Add 버튼을 클릭합니다.
4. 사용자, 컴퓨터 또는 그룹 선택 대화 상자에서 권한을 위임할 그룹이나 사용자 계정을 입력한 후, 확인 버튼을 클릭합니다.
5. 선택한 그룹이나 사용자 계정에게 위임할 사용 권한을 선택합니다. 〈그림 47〉과 같이 세 종류의 사용 권한 중에 위임할 사용 권한을 선택한 후, OK 버튼을 클릭합니다.

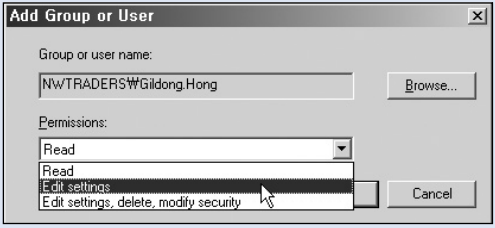

그림 47 위임할 권한 선택

6. 목록에 이미 추가되어 있는 그룹이나 사용자 계정의 권한을 변경하기 위해서는 〈그림 48〉과 같이 사용 권한을 변경할 그룹이나 사용자 계정을 마우스 오른쪽 버튼으로 클릭한 후, 메뉴에서 변경할 권한을 선택합니다.

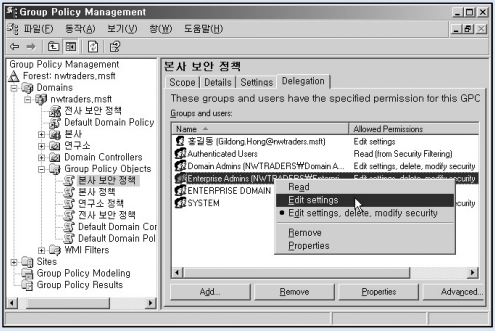

그림 48 사용 권한 변경

SOM에 대한 권한 위임

관리자는 GPMC를 이용해서 SOM과 관련된 다음과 같은 세 종류의 권한을 손쉽게 위임할 수 있습니다.

- SOM에 GPO 연결
- SOM에 대한 그룹 정책 모델링 작업 수행

- SOM에 대한 그룹 정책 결과 집합 정보 수집

이와 관련된 사용 권한 정보는 해당 SOM의 Delegation 탭에서 확인할 수 있습니다. 관리자는 Add 버튼을 이용해서 새로운 그룹이나 사용자에게 원하는 권한을 위임할 수 있고, Remove 버튼을 이용해서 권한을 제거할 수 있습니다.

SOM에 GPO 연결

SOM(사이트, 도메인, 조직 구성 단위)에 GPO를 연결함으로써, 해당 SOM에 존재하는 컴퓨터와 사용자에게 GPO에 설정된 정책들이 적용됩니다. 관리자는 다른 관리자에 의해 생성되고 정책이 설정된 GPO를 SOM에 연결할 수 있도록 개별 SOM 별로 권한을 위임할 수 있습니다.

GPMC 이전에는 SOM의 gPLink와 gPOption 속성에 읽기와 쓰기 권한을 부여함으로써 해당 SOM에 GPO를 연결할 수 있는 권한을 위임 했습니다.
하지만 GPMC에서는 SOM의 속성에 직접 권한을 부여하지 않고, "Link GPOs" 라 정의한 단일 사용 권한을 그룹이나 사용자에게 부여함으로써 보다 손쉽게 권한 위임이 가능합니다.

"Link GPOs" 권한을 위임 받은 관리자는 연결된 GPO 순서, 상속 금지, 무시 안 함과 같은 SOM에 연결된 GPO의 관련 정보도 관리할 수 있습니다.

[따라하기] SOM에 GPO 연결 권한 위임하기

GPMC를 이용해서 특정 SOM에 GPO를 연결 할 수 있는 권한을 위임하는 과정은 다음과 같습니다.

1. GPMC에서 권한을 위임할 SOM(사이트, 도메인, 조직 구성 단위)을 클릭합니다.
2. Delegation 탭을 클릭합니다.
3. Permission 목록에 Link GPOs 권한이 선택되어 있는지 확인합니다. 선택한 SOM에 GPO를 연결할 수 있는 사용 권한이 위임된 그룹이나 사용자 계정 목록이 출력됩니다.
4. 권한을 위임할 그룹이나 사용자 계정을 선택하기 하기 위해 Add 버튼을 클릭합니다.
5. 사용자, 컴퓨터 또는 그룹 선택 대화 상자에서 권한을 위임할 그룹이나 사용자 계정을 입력한 후, 확인 버튼을 클릭합니다.
6. GPO 연결 권한을 하위 컨테이너에게 상속할 것인지를 선택합니다. 선택된 그룹이나 사용자 계정에게 현재 SOM에 대해서만 GPO를 연결할 수 있는 권한을 위임 하기 위해서는 Permission 목록에서 This Container only 옵션을 선택합니다. 현재 SOM과 하위 컨테이너에 대해서도 GPO를 연결할 수 있는 권한을 위임한다면 Permission 목록에서 This Container and all child containers 옵션을 선택합니다. 적절한 옵션을 선택한 후, OK 버튼을 클릭합니다.

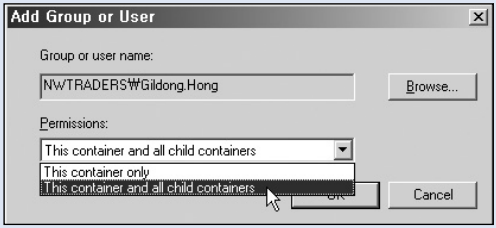

그림 49 권한 상속 여부 선택

7. GPO를 연결할 수 있는 권한을 이미 위임한 그룹이나 사용자 계정의 권한 상속 설정을 변경하기 위해서는 〈그림 50〉와 같이 권한 상속 설정을 변경할 그룹이나 사용자 계정을 마우스 오른쪽 버튼으로 클릭한 후, 메뉴에서 원하는 옵션을 선택합니다.

그림 50 권한 상속 설정 변경

SOM에 대한 그룹 정책 모델링 작업 수행

그룹 정책 모델링을 이용해서 관리자는 OU나 도메인에 존재하는 컴퓨터나 사용자에게 적용될 정책 설정을 미리 시뮬레이션 하여 확인할 수 있습니다. 그룹 정책 모델링 작업은 디폴트로 Domain Admins 그룹의 구성원만 가능하지만, 권한 위임을 통해 다른 관리자들도 수행이 가능합니다.

GPMC 이전에는 도메인이나 OU에서 "정책 결과 집합 생성(계획)" 권한을 그룹이나 사용자에게 부여함으로써 그룹 정책 모델링 작업을 수행할 수 있는 권한을 위임했습니다. 이 권한은 Windows Server 2003 스키마를 가지고 있는 모든 포리스트에 존재합니다.

하지만 GPMC에서는 도메인이나 OU의 속성에 직접 권한을 부여하지 않고, Delegation 탭의 Permission 목록에서 "Perform Group Policy Modeling Analyses"를 선택한 후, 원하는 그룹이나 사용자를 추가함으로써 보다 손쉽게 권한 위임이 가능합니다.

[따라하기] SOM에 대한 그룹 정책 모델링 작업 수행 권한 위임하기

GPMC를 이용해서 개별 SOM에 대한 그룹 정책 모델링 작업을 수행할 수 있는 권한을 위임하는 과정은 다음과 같습니다.

1. GPMC에서 권한을 위임할 도메인이나 조직 구성 단위를 클릭 합니다.
2. Delegation 탭을 클릭한 후, Permission 목록에 Perform Group Policy Modeling Analyses 권한을 선택합니다. 선택한 도메인이나 조직 구성 단위에서 그룹 정책 모델링 작업을 수행할 수 있는 권한이 위임된 그룹이나 사용자 계정 목록이 출력됩니다.

3. 권한을 위임할 그룹이나 사용자 계정을 선택하기 하기 위해 Add 버튼을 클릭합니다.
4. 사용자, 컴퓨터 또는 그룹 선택 대화 상자에서 권한을 위임할 그룹이나 사용자 계정을 입력한 후, 확인 버튼을 클릭합니다.
5. 그룹 정책 모델링 작업을 수행할 수 있는 권한을 하위 컨테이너에게 상속할 것인지를 선택합니다. 선택된 그룹이나 사용자 계정에게 현재 도메인이나 조직 구성 단위에 대해서만 그룹 정책 모델링 작업을 수행할 수 있는 권한을 위임 하기 위해서는 Permission 목록에서 This Container only 옵션을 선택합니다. 현재 도메인이나 조직 구성 단위의 하위 컨테이너에 대해서도 그룹 정책 모델링 작업을 수행할 수 있는 권한을 위임한다면 Permission 목록에서 This Container and all child containers 옵션을 선택합니다. 적절한 옵션을 선택한 후, OK 버튼을 클릭합니다.

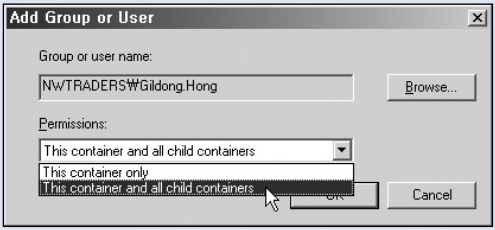

그림 51 권한 상속 여부 선택

6. 그룹 정책 모델링 작업을 수행할 수 있는 권한을 이미 위임한 그룹이나 사용자 계정의 권한 상속 설정을 변경하기 위해서는 권한 상속 설정을 변경할 그룹이나 사용자 계정을 마우스 오른쪽 버튼으로 클릭한 후, 메뉴에서 This container only나 This Container and children 옵션을 선택합니다.

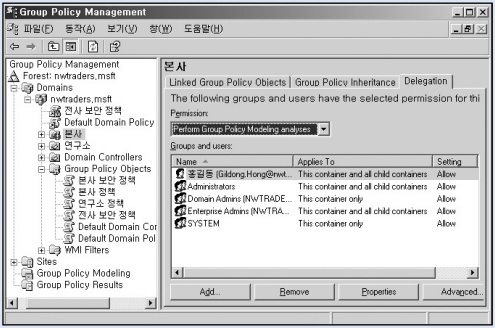

그림 52 그룹 정책 모델링 작업 수행 권한 위임

SOM에 대한 그룹 정책 결과 집합 정보 수집

그룹 정책 결과 집합을 이용해서 관리자는 도메인이나 조직 구성 단위에 존재하는 컴퓨터나 사용자에게 적용된 정책 설정을 확인할 수 있습니다. 디폴트로 대상 컴퓨터의 로컬 Administrator 권한을 가지고 있어야만 원격에서 대상 컴퓨터의 그룹 정책 결과 집합 정보를 수집할 수 있지만, 권한 위임을 통해 다른 관리자들도 정보 수집이 가능합니다.

GPMC 이전에는 도메인이나 OU에서 "정책 결과 집합 생성(로깅)" 권한을 그룹이나 사용자에게 부여함으로써 그룹 정책 결과 집합 정보를 수집할 수 있는 권한을 위임했습니다. 이 권한은 Windows Server 2003 스키마를 가지고 있는 모든 포리스트에 존재합니다.

하지만 GPMC에서는 도메인이나 OU의 속성에 직접 권한을 부여하지 않고, Delegation 탭의Permission 목록에서 "Read Group Policy Results Data"를 선택한 후, 원하는 그룹이나 사용자를 추가함으로써 보다 손쉽게 권한 위임이 가능합니다.

[따라하기] SOM에 대한 그룹 정책 결과 집합 정보 수집 권한 위임하기

GPMC를 이용해서 개별 SOM에 대한 그룹 정책 결과 집합 정보를 수집할 수 있는 권한을 위임하는 과정은 다음과 같습니다.

1. GPMC에서 권한을 위임할 도메인이나 조직 구성 단위를 클릭 합니다.
2. Delegation 탭을 클릭한 후, Permission 목록에 Read Group Policy Results Data 권한을 선택합니다. 선택한 도메인이나 조직 구성 단위에서 그룹 정책 결과 집합 정보를 수집할 수 있는 권한이 위임된 그룹이나 사용자 계정 목록이 출력됩니다.
3. 권한을 위임할 그룹이나 사용자 계정을 선택하기 하기 위해 Add 버튼을 클릭합니다.
4. 사용자, 컴퓨터 또는 그룹 선택 대화 상자에서 권한을 위임할 그룹이나 사용자 계정을 입력한 후, 확인 버튼을 클릭합니다.
5. 그룹 정책 결과 집합 정보를 수집할 수 있는 권한을 하위 컨테이너에게 상속할 것인지를 선택합니다. 선택된 그룹이나 사용자 계정에게 현재 도메인이나 조직 구성 단위에 대해서만 그룹 정책 결과 집합 정보를 수집할 수 있는 권한을 위임 하기 위해서는 Permission 목록에서 This Container only 옵션을 선택합니다. 현재 도메인이나 조직 구성 단위의 하위 컨테이너에 대해서도 그룹 정책 결과 집합 정보를 수집할 수 있는 권한을 위임한다면 Permission 목록에서 This Container and all child containers 옵션을 선택

합니다. 적절한 옵션을 선택한 후, OK 버튼을 클릭합니다.

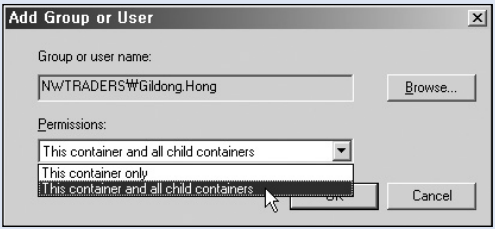

그림 53 권한 상속 여부 선택

6. 그룹 정책 결과 집합 정보를 수집할 수 있는 권한을 이미 위임한 그룹이나 사용자 계정의 권한 상속 설정을 변경하기 위해서는 권한 상속 설정을 변경할 그룹이나 사용자 계정을 마우스 오른쪽 버튼으로 클릭한 후, 메뉴에서 This container only나 This Container and children 옵션을 선택합니다.

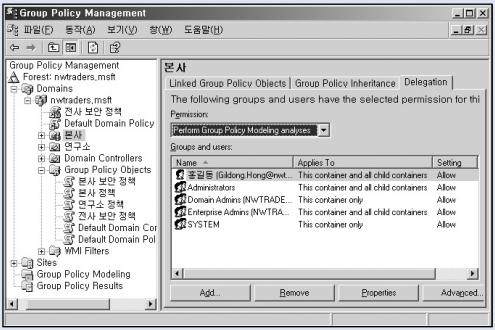

그림 54 그룹 정책 결과 집합 정보 수집 권한 위임

WMI 필터에 대한 권한 위임

WMI 필터는 Windows Server 2003 Active Directory에서 새로이 소개된 기능입니다. 관리자는 GPMC를 이용해서 WMI 필터와 관련된 다음과 같은 두 종류의 권한을 손쉽게 위임할 수 있습니다.

- WMI 필터 생성
- WMI 필터 수정

WMI 필터 생성

새로 생성된 WMI 필터는 Active Directory 도메인의 System 컨테이너 아래 WMIPolicy 컨테이너에 저장됩니다. GPMC 이전에 관리자는 WMIPolicy 컨테이너에 직접 사용 권한을 설정함으로써 WMI 필터를 생성, 수정, 삭제 할 수 있는 권한을 위임할 수 있습니다.

GPMC에서는 WMI Filter 노드의 Delegation 탭에서 원하는 그룹이나 사용자에게 Create Owner 또는 Full Control 권한을 부여함으로써 손쉽게 권한 위임이 가능합니다.

GPMC에서는 다음과 같은 두 종류의 사용 권한을 제공하여 관리자가 보다 쉽게 WMI 필터를 생성하는 권한을 위임할 수 있습니다.

- Creator owner : 새 WMI 필터를 생성할 수 있는 권한을 위임합니다. 이 권한을 위임 받은 관리자는 새 WMI 필터를 생성할 수 있지만, 오직 본인이 생성한 WMI 필터에 대해서만 모든 권한을 가집니다.

- Full control : 새 WMI 필터를 생성할 수 있는 권한을 위임합니다. 이 권한을 부여 받은 관리자는 새 WMI 필터를 생성할 수 있고, 또한 관리자 본인이 생성한 WMI 필터뿐만 아니라, 다른 관리자에 의해 생성된 도메인의 모든 WMI 필터에 대해 모든 권한을 가집니다.

디폴트로 Domain Admins 그룹과 Enterprise Admins 그룹에는 Full control 권한이 부여되어 있고, Group Policy Creator Owners 그룹에는 Creator owner 권한이 부여되어 있습니다.

[따라하기] WMI 필터 생성 권한 위임하기

GPMC를 이용해서 WMI 필터를 생성할 수 있는 권한을 위임하는 과정은 다음과 같습니다.

1. GPMC에서 WMI Filters 노드를 클릭한 후, Delegation 탭을 클릭합니다.
2. 권한을 위임할 그룹이나 사용자 계정을 선택하기 하기 위해 Add 버튼을 클릭합니다.
3. 사용자, 컴퓨터 또는 그룹 선택 대화 상자에서 권한을 위임할 그룹이나 사용자 계정을 입력한 후, 확인 버튼을 클릭합니다.
4. 선택한 그룹이나 사용자 계정에게 위임할 사용 권한을 선택합니다. 〈그림 55〉와 같이 두 종류의 사용 권한 중에 위임할 사용 권한을 선택한 후, OK 버튼을 클릭합니다.

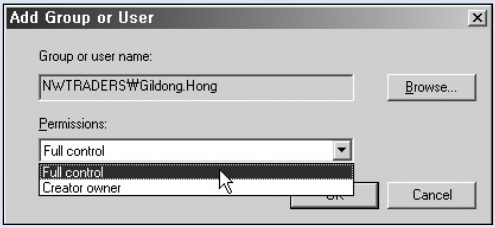

그림 55 위임할 권한 선택

5. 목록에 이미 추가되어 있는 그룹이나 사용자 계정의 권한을 변경하기 위해서는 사용 권한을 변경할 그룹이나 사용자 계정을 마우스 오른쪽 버튼으로 클릭한 후, 메뉴에서 Full control이나 Create owner 옵션을 선택합니다.

WMI 필터 수정

GPMC에서는 개별 WMI 필터에 대해 권한 위임이 가능합니다. GPMC에서는 다음과 같은 두 종류의 사용 권한을 제공하여 보다 쉽게 개별 WMI 필터를 관리하는 권한을 위임합니다.

- Edit : WMI 필터를 수정할 수 있는 권한을 위임합니다.
- Full control : WMI 필터를 수정, 삭제, 권한 설정할 수 있는 권한을 위임합니다.

[따라하기] WMI 필터 수정 권한 위임하기

GPMC를 이용해서 WMI 필터를 수정할 수 있는 권한을 위임하는 과정은 다음과 같습니다.

1. GPMC에서 WMI Filters 노드 아래에 권한을 위임할 WMI 필터를 클릭합니다.
2. Delegation 탭을 클릭합니다.
3. 권한을 위임할 그룹이나 사용자 계정을 선택하기 하기 위해 Add 버튼을 클릭합니다.
4. 사용자, 컴퓨터 또는 그룹 선택 대화 상자에서 권한을 위임할 그룹이나 사용자 계정을 입력한 후, 확인 버튼을 클릭합니다.
5. 선택한 그룹이나 사용자 계정에게 위임할 사용 권한을 선택합니다. 〈그림 56〉과 같이 두 종류의 사용 권한 중에 위임할 사용 권한을 선택한 후, OK 버튼을 클릭합니다.

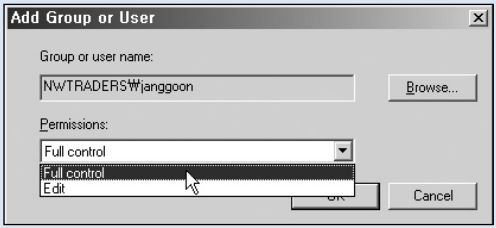

그림 56 위임할 권한 선택

6. 목록에 이미 추가되어 있는 그룹이나 사용자 계정의 권한을 변경하기 위해서는 사용 권한을 변경할 그룹이나 사용자 계정을 마우스 오른쪽 버튼으로 클릭한 후, 메뉴에서 Full control이나 Edit 옵션을 선택합니다.

그룹 정책 관리

관리자는 그룹 정책을 관리하기 위해 다음과 같은 작업을 수행해야 합니다.

- **백업** : GPO 백업은 GPO의 모든 설정 정보를 파일 시스템에 저장합니다. 백업된 GPO는 향후에 복원이나 가져오기 작업에서 사용할 수 있습니다.

- **복원** : GPO 복원은 백업된 GPO를 이용해서 GPO가 백업된 시점으로 GPO 설정들을 돌려 놓습니다. GPO 복원은 백업된 GPO의 도메인 및 GUID 정보를 이용해서 복원 작업을 수행하기 때문에, 다른 도메인에 GPO를 복원하는 작업은 수행할 수 없습니다.

- **가져오기** : GPO 가져오기는 기존 GPO에 백업된 GPO의 설정 값을 가져옵니다. GPO 복원과 달리 가져오기 작업은 같은 도메인, 다른 도메인, 다른 포리스트에서도 수행할 수 있습니다. 가져오기 작업을 이용하여 관리자는 테스트 도메인에서 테스트 한 GPO를 백업하여 운영 환경의 GPO에 가져오기로 동일한 설정 값을 구성할 수 있습니다.

- **복사** : GPO 복사는 GPO 설정 값을 파일 시스템에 저장하지 않고, GPO 설정 값을 복사하여 새로운 GPO를 생성합니다.

백업

GPO 백업은 Active Directory와 Sysvol에 저장하는 GPO와 관련된 다음과 같은 데이터를 지정한 파일 시스템 경로에 저장합니다.

- GPO의 도메인과 GUID 정보
- GPO 정책 설정 값
- GPO의 DACL
- GPO에 연결된 WMI 필터

백업은 GPO와 별개로 저장되는 WMI 필터, GPO가 연결된 SOM 정보, IPSec 정책과 같은 정보는 백업하지 않습니다. 이런 정보들은 자체적으로 사용 권한을 가지는 별도의 개체들입니다. WMI 필터나 IPSec 정책은 백업된 GPO 뿐만 아니라 다른 GPO에도 다중으로 연결될 수 있기 때문에, GPO를 복원 할 때 이런 개체들이 같이 복원되는 것은 적절치 못할 수 있습니다.

GPO의 WMI 필터 연결 정보는 GPO의 속성 중에 하나이기 때문에 GPO 백업과 복원에 포함되지만, WMI 필터 자체는 GPO와 별개의 개체입니다. 따라서 WMI 필터 자체를 백업하거나 복원하기를 원한다면, GPMC의 WMI Filter 노드에서 Import 또는 Export 기능을 이용하면 됩니다.

마찬가지로 IPSec 정책도 GPO와 별개로 저장되어 있기 때문에, GPO 백업

은 IPSec 정책 연결 정보만 백업됩니다. 따라서 IPSec 정책 자체를 백업하거나 복원하기를 원한다면, IP 보안 관리 스냅인에서 정책 내보내기 또는 정책 가져오기 기능을 이용하면 됩니다.

각 GPO 백업에 유일한 ID를 부여함으로써, 같은 파일 시스템 경로에 여러 GPO의 백업을 저장하거나 또는 동일 GPO의 여러 백업을 같이 저장하는 것이 가능합니다.

관리자는 다음과 같은 다양한 방법을 이용해서 GPO를 백업할 수 있습니다.

- Group Policy objects 노드 아래에서 백업할 GPO를 마우스 오른쪽 버튼으로 클릭한 후, Back up 메뉴를 선택합니다.

- Group Policy objects 노드의 Contents 탭 아래에서 백업할 GPO를 마우스 오른쪽 버튼으로 클릭한 후, Back up 메뉴를 선택합니다.

- Group Policy objects 노드를 마우스 오른쪽 버튼으로 클릭한 후, Back up All 메뉴를 선택합니다. 이 메뉴를 선택하면 도메인의 모든 GPO를 백업합니다.

- GPMC에서 제공하는 BackupGPO.wsf와 BackupAllGPOs.wsf 스크립트를 이용해서 GPO를 백업합니다.

GPO를 백업하기 위해서 백업을 수행하는 관리자는 GPO에 읽기 권한을 가지고 있어야 하고, 백업을 저장할 파일 시스템 경로에 쓰기 권한을 가지고 있어야 합니다.

[따라하기] GPO 백업하기

GPMC를 이용해서 GPO를 백업하는 과정은 다음과 같습니다.

1. GPMC의 Group Policy objects 노드 아래에서 백업을 수행할 GPO를 마우스 오른쪽 버튼으로 클릭한 후, Back up 메뉴를 선택합니다.
2. Browse 버튼을 클릭하여 GPO 백업을 저장할 파일 시스템 경로를 지정합니다. 백업에 대한 설명이 필요하면 Description 입력창에 적절한 설명을 입력한 후, Back up 버튼을 클릭합니다.

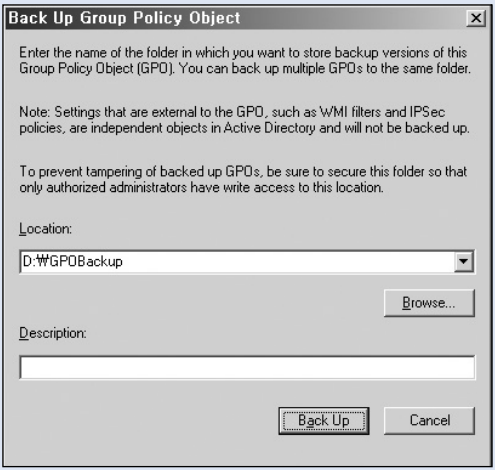

그림 57 GPO 백업

3. 지정한 GPO에 대한 백업이 진행됩니다. 백업이 완료되면 OK 버튼을 클릭합니다.

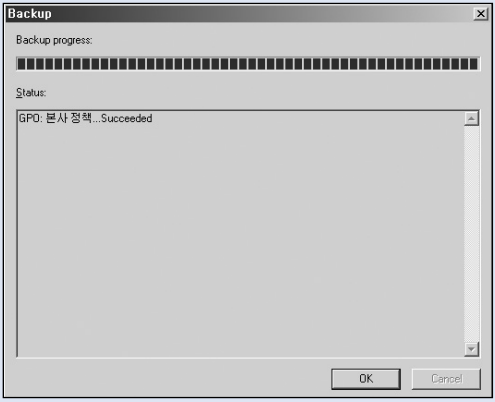

그림 58 GPO 백업 완료

백업 GPO 관리

GPMC는 백업된 GPO를 관리할 수 있는 다음과 같은 두 가지 방법을 제공합니다.

- Domains 노드를 마우스 오른쪽 버튼으로 클릭한 후, Manage Backups 메뉴를 선택합니다. 이 메뉴를 선택하면 지정한 파일 시스템 경로에 백업된 모든 도메인과 포리스트의 GPO 목록을 출력합니다.

- Group Policy objects 노드를 마우스 오른쪽 버튼으로 클릭한 후, Manage Backups 메뉴를 선택합니다. 이 메뉴를 선택하면 지정한 파일 시스템 경로에 백업된 해당 도메인의 GPO 목록만을 출력합니다.

Manage Backups 메뉴를 선택하면 〈그림 59〉와 같이 지정한 파일 시스템 경로에 백업된 GPO 목록이 출력됩니다.

Manage Backups 대화 상자에서는 GPO를 저장하고 있는 도메인 이름, GPO 이름, GPO를 백업한 시간, GPO 백업 때 입력한 설명 그리고 GPO의 GUID 정보를 출력합니다. Show only the latest version of each GPO 옵션을 선택하면 각 GPO의 가장 최신 백업만 목록에 출력합니다.

Manage Backups 대화 상자에서 관리자는 View Settings 버튼을 클릭하여 백업된 GPO의 설정을 웹 브라우저를 통해 볼 수 있고, Restore나 Delete 버튼을 이용해서 원하는 GPO 백업을 복원하거나 삭제할 수 있습니다.

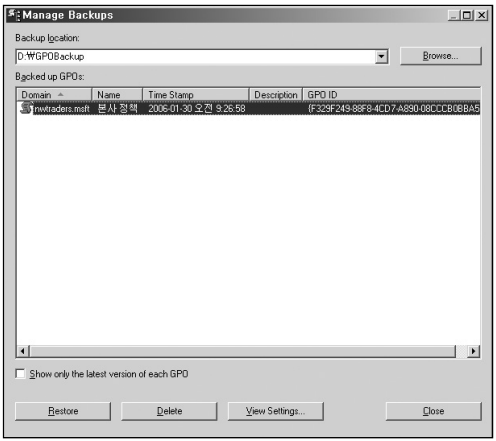

그림 59 GPO 백업 관리

복원

GPO 복원은 백업된 GPO를 이용해서 GPO가 백업된 시점으로 GPO 설정들을 돌려 놓습니다. 관리자는 GPO가 삭제 되었거나, GPO를 백업된 시점으로 돌려 놓고 싶을 때 복원을 사용할 수 있습니다. 복원을 이용하면 백업된 GPO의 GUID를 이용해서 GPO가 복원됩니다. 이는 삭제된 GPO를 복원할 때도 동일하게 적용됩니다. 백업된 GPO의 GUID가 동일하게 복원 되는 것은 복원 작업이 가져오기나 복사 작업과 구분되는 점입니다.

GPO 복원 작업을 수행하면 다음과 같은 데이터들이 복원됩니다.

- GPO 정책 설정 값
- GPO의 DACL
- GPO에 연결된 WMI 필터

GPO 복원은 SOM 연결 정보는 복원하지 않습니다. GPO 백업에서 설명했듯이 WMI 필터, IPSec 정책과 함께 SOM 연결 정보는 백업되지 않기 때문에 당연히 복원도 되지 않습니다. 관리자가 존재하는 GPO를 복원했다면, 기존에 SOM에 연결된 정보를 그대로 사용할 수 있습니다. 하지만 삭제된 GPO를 복원하면 GPO는 복원되지만 SOM에 대한 연결 정보는 복원되지 않기 때문에, 관리자는 직접 적절한 SOM(사이트, 도메인, 조직 구성 단위)에 복원한 GPO를 연결해야 합니다. 복원한 GPO의 연결 정보는 〈그림 60〉와 같이 백업된 GPO의 리포트(General\Links 항목)에서 확인할 수 있습니다.

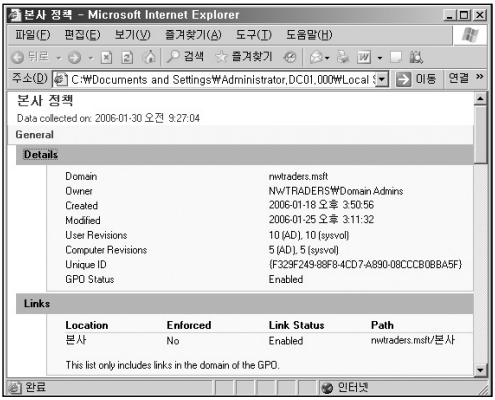

그림 60 백업 리포트

관리자는 다음과 같은 다양한 방법을 이용해서 GPO를 복원할 수 있습니다.

- 존재하는 GPO를 복원하기 위해서, Group Policy objects 노드 아래에서 복원할 GPO를 마우스 오른쪽 버튼으로 클릭한 후, Restore from Backup 메뉴를 선택합니다.

- 삭제된 GPO를 복원하기 위해서는 Group Policy objects 노드를 마우스 오른쪽 버튼으로 클릭한 후, Manage Backups 메뉴를 선택합니다. Manage Backups 대화 상자에서 복원할 GPO를 선택한 후, Restore 버튼을 클릭합니다.

- GPMC에서 제공하는 RestoreGPO.wsf와 RestoreAllGPOs.wsf 스크립트를 이용해서 GPO를 복원합니다.

존재하는 GPO를 복원하는 경우와 삭제된 GPO를 삭제하는 경우에 복원 작업을 성공적으로 수행하기 위해 관리자에게 필요한 사용 권한에 차이가 있습니다. 각각의 경우에 관리자는 〈표 9〉와 같이 적절한 권한을 가지고 있어야 합니다.

GPO 상태	필요한 사용 권한
존재하는 GPO	관리자는 존재하는 GPO에 대해 Edit settings, delete, and modify security 권한이 필요합니다. 또한 백업된 GPO가 저장된 파일 시스템 경로에 대해 읽기 권한이 필요합니다.
삭제된 GPO	관리자는 GPO를 복원할 도메인에 GPO를 생성할 수 있는 권한이 필요합니다. 또한 백업된 GPO가 저장된 파일 시스템 경로에 대해 읽기 권한이 필요합니다.

표 9 GPO 복원에 필요한 사용 권한

GPO를 복원할 때, GPMC는 GPO의 상태에 따라 다음과 같이 GPO 버전을 다르게 설정합니다.

- **존재하는 GPO 복원** : 복원된 GPO가 클라이언트에 재적용 되도록 GPO를 복원하면서 존재하는 GPO의 버전을 증가시킵니다.

- **삭제된 GPO 복원** : 백업된 GPO에 저장된 버전을 그대로 복원합니다.

도메인 이름을 변경하면, 도메인 이름을 변경하기 전에 백업한 GPO를 이용해서 복원 작업을 수행 할 수 없습니다. 따라서 도메인 이름 변경 후에 가급적 빠른 시간 안에 전체 GPO를 백업 할 것을 권장합니다.

[따라하기] GPO 복원하기

GPMC를 이용해서 존재하는 GPO를 복원하는 과정은 다음과 같습니다.

1. GPMC의 Group Policy objects 노드 아래에서 복원을 수행할 GPO를 마우스 오른쪽 버튼으로 클릭한 후, Restore form Backup 메뉴를 선택합니다.
2. Restore Group Policy Object Wizard가 실행됩니다. 간단한 도움말을 읽은 후에 다음 버튼을 클릭합니다.
3. Browse 버튼을 클릭하여 복원할 GPO 백업이 저장된 파일 시스템 경로를 지정한 후, 다음 버튼을 클릭합니다.

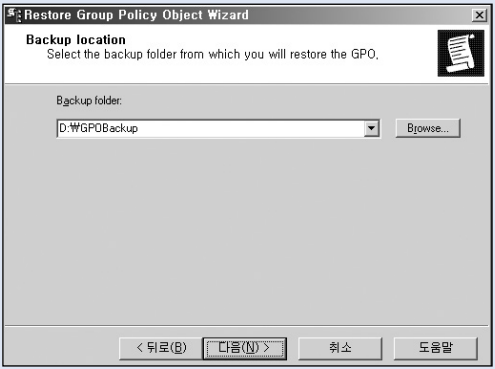

그림 61 복원할 GPO가 저장된 파일 시스템 경로 지정

4. 지정한 파일 시스템 경로에 저장된 GPO 백업들이 Backed up GPOs 목록이 출력됩니다. View Settings 버튼을 클릭하여 선택한 GPO의 설정을 확인할 수 있습니다.
   복원할 GPO 백업을 선택한 후, 다음 버튼을 클릭합니다.

그림 62 복원할 GPO 백업 선택

5. 요약 정보를 확인한 후, 마침 버튼을 클릭합니다.

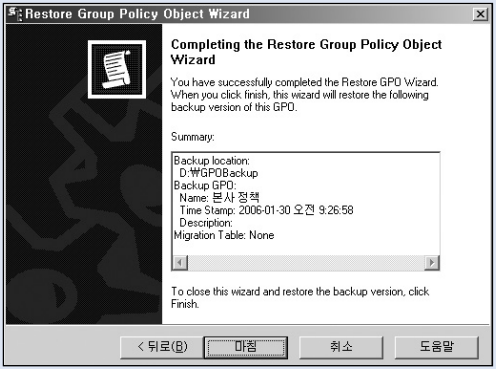

그림 63 요약 정보 출력

6. 지정한 GPO에 대한 복원이 진행됩니다. 복원이 완료되면 OK 버튼을 클릭합니다.

가져오기

GPO 가져오기는 기존 GPO에 파일 시스템에 백업된 GPO의 설정 값을 가져옵니다. GPO 복원과 달리 가져오기 작업은 같은 도메인, 다른 도메인, 다른 포리스트에서도 수행할 수 있습니다. 따라서 가져오기는 트러스트 관계가 없는 도메인으로 GPO를 마이그레이션 하는 용도로 사용하면 유용합니다.

예를 들어 가져오기 작업을 이용하여 관리자는 테스트 도메인에서 테스트 한 GPO를 백업하여 트러스트 관계가 없는 운영 환경 도메인의 GPO에 가져오기로 동일한 설정 값을 구성할 수 있습니다.

기존에 존재하는 GPO를 대상으로 가져오기 작업을 수행할 수 있으며, 가져오기 작업 중에 GPO의 ACL, SOM 연결 정보, WMI 필터 정보는 수정되지 않습니다.

관리자는 다음과 같은 방법을 이용해서 가져오기 작업을 수행할 수 있습니다.

- Group Policy objects 노드 아래에서 GPO를 마우스 오른쪽 버튼으로 클릭한 후, Import 메뉴를 선택합니다.

- GPMC에서 제공하는 ImportGPO.wsf와 ImportAllGPOs.wsf 스크립트를 이용해서 GPO를 백업합니다.

가져오기 작업을 수행하는 관리자는 대상 GPO에 Edit settings, delete, and modify security 권한을 가지고 있어야 합니다.

복사

복사는 새로운 GPO를 생성한 후, Active Directory에 존재하는 원본 GPO의 설정을 복사합니다. 복사 작업은 같은 도메인, 같은 포리스트의 다른 도메인, 다른 포리스트에서도 수행할 수 있습니다. 따라서 복사는 테스트 도메인에서 테스트가 완료된 GPO를 운영 환경의 도메인으로 마이그레이션 하는 용도로 사용하면 유용합니다

GPO를 복사할 때, 관리자는 대상 GPO의 DACL 설정과 관련한 다음 두 옵션을 선택할 수 있습니다.

- 새 GPO를 생성할 때 적용하는 디폴트 DACL 설정

- 원본 GPO의 DACL을 새로 생성되는 GPO에 설정

GPO를 복사할 때, 같은 도메인에 복사할 경우와 다른 도메인으로 복사할 경우에 다음과 같은 차이점이 발생합니다.

- 같은 도메인에서 GPO를 복사할 경우에는 WMI 필터 연결 정보도 복사됩니다. 하지만 다른 도메인으로 GPO를 복사할 경우에는 대상 도메인에 WMI 필터가 존재하지 않기 때문에 WMI 필터 연결 정보는 복사되지 않습니다.

- 같은 도메인에서 GPO를 복사할 경우에는 원본 GPO의 IPSec 정책 정보가 대상 GPO에도 복사됩니다. 하지만 다른 도메인으로 GPO를 복사할 경우에는 대상 도메인에 IPSec 정책이 존재하지 않기 때문에 IPSec 정책 정보는 복사되지 않습니다.

관리자는 다음과 같은 다양한 방법을 이용해서 GPO를 백업할 수 있습니다.

- Group Policy objects 노드 아래에서 복사할 원본 GPO를 마우스 오른쪽 버튼으로 클릭한 후, Copy 메뉴를 선택합니다. 그리고 대상 도메인의 Group Policy objects 노드를 아래에서 마우스 오른쪽 버튼으로 클릭한 후, Paste 메뉴를 선택합니다.

- GPMC에서 제공하는 CopyGPO.wsf 스크립트를 이용해서 GPO를 복사합니다.

복사 작업을 수행하는 관리자는 대상 도메인에 대해서는 GPO를 생성 할 수 있는 권한이 필요하고, 원본 GPO에 대해서는 읽기 권한이 필요합니다.

마이그레이션

관리자는 GPMC의 가져오기나 복사 기능을 이용해서 손쉽게 도메인 간에 GPO를 마이그레이션 할 수 있습니다. 하지만 GPO에 원본 도메인과 직접적으로 연관된 정보를 포함하고 있을 경우에는 마이그레이션이 원활하게 진행될 수 없습니다. 예를 들어 원본 GPO에 도메인의 특정 사용자나 그룹에게 사용 권한을 부여하는 정책이 존재 할 경우에, GPO를 마이그레이션 하는 대상 도메인에는 해당 사용자나 그룹에 대한 정보가 없기 때문에 완벽한 마이그레이션이 불가능합니다.

이런 문제를 해결하기 위해 GPMC에서는 마이그레이션 테이블을 제공하여 도메인과 직접 연관된 정보를 변환하여 마이그레이션이 가능하도록 지원합니다.

변환이 필요한 정책 값

다른 도메인으로 GPO를 마이그레이션 할 때, 모든 정책 설정 값을 변환 할 필요는 없습니다. 예를 들어 관리 템플릿에 설정 된 값들은 모두 변환 없이 그대로 마이그레이션이 가능합니다.

변환이 필요한 대표적인 정책 설정 값들은 두 가지로, 바로 계정과 UNC 경로입니다. 원본 GPO의 정책 설정 값에 컴퓨터, 사용자, 그룹 계정이 포함되어 있다면, 다른 도메인으로 마이그레이션 될 때 적절히 대상 도메인에 존재하는 컴퓨터, 사용자, 그룹 계정으로 변환되어야 합니다.

UNC 경로의 경우에는 마이그레이션 하는 대상 도메인의 클라이언트에서는 원본 도메인의 서버에 접근이 불가능할 수 있기 때문에 접근 가능한 서버의 UNC 경로로 변환해야 합니다. 물론 대상 도메인의 클라이언트들도 원본 도메인의 서버에 접근이 가능한 경우에는 굳이 UNC 경로를 변환할 필요는 없습니다.

다음과 같은 정책들은 계정을 설정 값으로 가지기 때문에, 복사나 가져오기를 이용해서 GPO를 마이그레이션 할 때, GPMC의 마이그레이션 테이블을 이용해서 값을 변환해야 합니다.

- 보안 설정
  - 사용자 권한 할당
  - 제한된 그룹
  - 시스템 서비스
  - 레지스트리
  - 파일 시스템

- GPO DACL

- 소프트웨어 설치 개체의 DACL

다음과 같은 정책들은 UNC 경로를 설정 값으로 가지기 때문에, 복사나 가져오기를 이용해서 GPO를 마이그레이션 할 때, GPMC의 마이그레이션 테이블을 이용해서 값을 변환해야 합니다.

- 폴더 리디렉션
- 소프트웨어 설치
- 스크립트(시작/종료, 로그온/로그오프)

마이그레이션 테이블

GPMC는 복사와 가져오기 작업을 수행할 때 마이그레이션 테이블을 이용해서 계정 및 UNC 경로를 변환하는 기능을 제공합니다. 마이그레이션 테이블은 〈그림 64〉와 같이 변환할 데이터 타입, 원본 값 그리고 대상 값을 지정하는 간단한 테이블입니다.

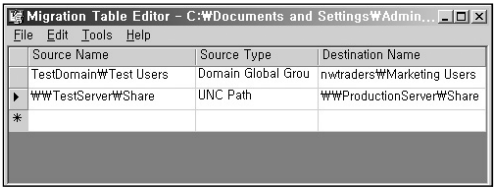

그림 64 예제 마이그레이션 테이블

테스트 도메인(TestDomain)에서 GPO를 테스트한 후, 운영 도메인(nwtraders)으로 GPO를 마이그레이션 한다고 가정하겠습니다. 테스트 도메인에서는 Test Users 그룹에 사용자 계정을 포함하여 GPO에 대한 정책을 테스트 한 후, 운영 도메인에서는 Marketing Users 그룹으로 변환하기 위해서 〈그림 64〉와 같이 마이그레이션 테이블을 구성합니다.

마찬가지로 테스트 도메인에서 사용자의 폴더 리디렉션을 위해 지정한 UNC 경로(\\TestServer\Share)를 운영 도메인에서는 \\ProductionServer\Share로 변환합니다.

마이그레이션 테이블을 생성하고 수정하기 위해서는 GPMC의 Domain 노드나 Group Policy Objects 노드를 마우스 오른쪽 버튼으로 클릭한 후, Open Migration Table Editor 메뉴를 선택합니다. 수정한 마이그레이션 테이블은 XML 파일로 저장되면, .migrable 확장명을 가집니다.

마이그레이션 테이블에서는 변환할 대상 값을 직접 지정하는 대신, 다음과 같은 옵션을 지정할 수 있습니다.

- Same As Source : 원본 값을 변환 없이 그대로 복사합니다
- No Destination : 값 변환 없이 마이그레이션 대상 GPO에서 계정을 제거합니다.
- Map By Relative Name : 마이그레이션 대상 도메인에서 원본 계정 이름과 동일한 계정 이름을 찾아서 맵핑합니다.

GPO 마이그레이션 하기

GPO 마이그레이션은 〈그림 65〉와 같은 순서로 진행합니다.

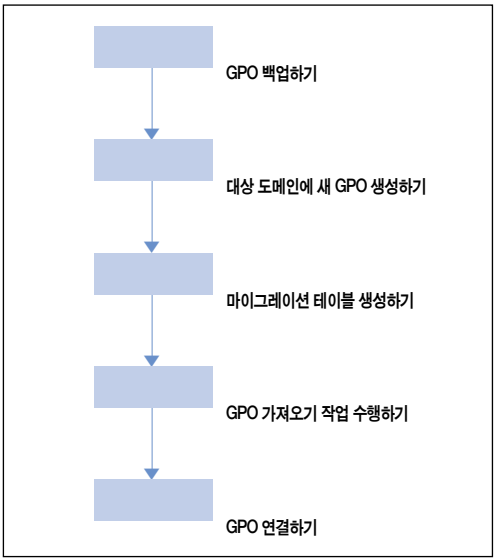

그림 65 GPO 마이그레이션 프로세스

[Step 1 - GPO 백업하기]

GPO 마이그레이션을 수행하기 위해 제일 먼저 원본 GPO를 백업하여 파일 시스템에 저장합니다. 관리자는 Group Policy objects 노드 아래에서 마이그레이션 할 GPO를 마우스 오른쪽 버튼으로 클릭한 후, Back up 메뉴를 선택하여 GPO를 백업합니다.

[Step 2 - 대상 도메인에 새 GPO 생성하기]

가져오기 작업을 수행하기 위해서는 대상 도메인에 새 GPO를 생성해야 합니다. 관리자는 Group Policy objects 노드를 마우스 오른쪽 버튼으로 클릭한 후, New 메뉴를 선택하여 새 GPO를 생성합니다.

[Step 3 - 마이그레이션 테이블 생성하기]

대상 도메인으로 GPO를 마이그레이션 하기 위해 필요한 마이그레이션 테이블을 생성합니다. 마이그레이션 할 GPO의 설정 값에 계정이나 UNC 경로가 포함되어 있지 않다면 마이그레이션 테이블이 필요 없습니다. 하지만 GPO의 설정 값에 계정이나 UNC 경로가 포함되어 있다면 정상적인 마이그레이션을 위해 관리자는 가져오기 작업을 수행하기 전에 마이그레이션 테이블을 생성해야 합니다.

관리자는 GPMC의 Domain 노드나 Group Policy Objects 노드를 마우스 오른쪽 버튼으로 클릭한 후, Open Migration Table Editor 메뉴를 선택하여 마이그레이션 테이블을 생성합니다.

Migration Table Editor는 GPO의 설정 값에 계정이나 UNC 경로를 검색하는 기능을 제공합니다. Tools의 Populate from GPO 메뉴를 선택한 후, GPO 목록에서 마이그레이션 할 원본 GPO를 선택하면, 변환이 필요한 계정이나 UNC 경로를 검색하여 자동으로 마이그레이션 테이블을 생성합니다. 관리자는 몇몇 필요한 값만 변경함으로써 보다 쉽고 빠르게 작업을 완료할 수 있습니다.

[Step 4 - GPO 가져오기 작업 수행하기]

관리자는 백업된 원본 GPO를 이용해서 가져오기 작업을 수행합니다. Group Policy objects 노드 아래에서 대상 GPO를 마우스 오른쪽 버튼으로 클릭한 후, Import 메뉴를 선택합니다. GPO Import Wizard가 실행되면 GPO 설정을 가져올 백업된 GPO와 마이그레이션 테이블을 지정하여 가져오기 작업을 완료합니다.

[Step 5 - GPO 연결하기]

가져오기 작업이 완료되면, GPO는 원본 GPO와 동일한 설정으로 복원됩니다. 하지만 SOM에 대한 GPO 연결 정보는 복원 되지 않기 때문에, 관리자는 대상 도메인이나 조직 구성 단위에 마이그레이션 한 GPO를 목적에 맞게 적절히 연결합니다.

스크립트를 이용한 관리

GPMC는 그룹 정책 관련 작업을 스크립팅 할 수 있는 COM 인터페이스를 제공합니다. 이 COM 인터페이스는 Jscript나 VBScript와 같은 스크립트뿐만 아니라 Visual Basic이나 VC++과 같은 프로그래밍 언어에서도 사용할 수 있습니다. GPMC에서 제공하는 COM 인터페이스에 대한 자세한 설명은 GPMC가 설치된 시스템의 %programfiles%\gpmc\scripts\gpmc.chm 도움말 파일에서 제공합니다.

GPMC를 설치하면 %programfiles%\gpmc\scripts 폴더에 COM 인터페이스의 사용법을 보여 주는 실제 운영 환경에서도 유용한 다양한 예제 스크립트를 제공합니다. 예제 스크립트는 모두 .wsf 확장자를 가지며, 일부 Jscript로 작성된 스크립트를 제외하고 모두 VBScript로 작성되어 있습니다. 스크립트

는 모두 명령 프롬프트에서 CScript.exe를 이용해서 실행해야 합니다. (예: "c:\program files\gpmc\scripts〉cscript ListAllGPOs.wsf")

관리자는 예제 스크립트를 이용해서 다양한 관리 작업을 배치, 자동화 할 수 있습니다. 〈표 10〉는 GPMC에서 제공하는 예제 스크립트에 대해 설명하고 있습니다.

스크립트	관리 작업	설명
BackupAllGPOs.wsf	도메인에 있는 모든 GPO 백업	도메인에 있는 모든 GPO를 지정한 폴더에 백업합니다.
BackupGPO.wsf	GPO 백업	GPO 이름이나 GUID를 지정하면 해당 GPO를 지정한 폴더에 백업합니다.
CopyGPO.wsf	GPO 복사	새 GPO를 생성하고 원본 GPO의 설정을 새 GPO에 복사합니다.
CreateEnvironment FromXML.wsf	XML을 이용해서 도메인에 GPO 동작 환경 생성	GPO가 동작하는데 필요한 환경 (예: 조직 구성 단위, GPO, 연결 및 보안 그룹)을 저장한 XML 파일을 읽어 들여, 도메인에 스크립트로 개체들을 만들어 GPO 동작 환경을 생성합니다.
CreateGPO.wsf	GPO 생성	지정된 이름의 새 GPO를 생성합니다.
CreateMigration Table.wsf	마이그레이션 테이블 생성	도메인 간에 GPO 복사 및 가져오기 작업을 할 경우에 사용자 계정 매핑 하는데 필요한 마이그레이션 테이블을 생성합니다.

CreateXMLFrom Environment.wsf	GPO 동작 환경을 저장하는 XML 파일 생성	조직 구성 단위, GPO, GPO 연결 그리고 GPO 보안 설정에 관한 정보를 저장하는 XML 파일을 생성합니다. 생성된 XML 파일과 CreateEnvironmentFromXML.wsf 스크립트를 함께 사용하면 동일한 GPO 동작 환경을 가지는 도메인을 구성할 수 있습니다.
DeleteGPO.wsf	GPO 삭제	GPO 이름이나 GUID를 지정하면 해당 GPO를 삭제합니다. 또한 SOM의 연결도 삭제합니다.
GrantPermission OnAllGPOs.wsf	모든 GPO에 대해 사용 권한 설정	도메인의 모든 GPO에 대해 지정한 사용 권한을 설정합니다.
ImportGPO.wsf	GPO의 정책 설정 가져오기	지정된 백업에서 도메인에 있는 기존의 GPO로 정책 설정을 가져옵니다.
ImportAllGPOs.wsf	여러 GPO의 정책 설정을 가져오기	새 GPO를 생성한 후, 지정한 경로에 저장된 각 GPO의 백업으로부터 정책 설정을 새 GPO로 가져옵니다.
RestoreGPO.wsf	GPO 복원	백업된 GPO를 복원합니다.
RestoreAllGPOs.wsf	모든 GPO 복원	지정한 경로에 저장된 모든 GPO를 복원합니다.
SetGPOPermissions BySOM.wsf	도메인, 조직 구성 단위 또는 사이트에 연결되어 있는 GPO의 사용 권한 설정	특정 도메인, 조직 구성 단위 또는 사이트에 연결되어 있는 모든 GPO에 대해 지정한 사용 권한을 설정합니다.
SetGPOPermissions .wsf	GPO 사용 권한 설정	지정한 GPO에 대해 사용 권한을 설정합니다.
SetGPOCreation Permissions.wsf	GPO 생성 권한 위임	지정한 그룹이나 사용자에게 GPO를 생성할 수 권한을 위임하거나 제거합니다.

SetSOM Permissions.wsf	SOM에 그룹 정책에 관련된 사용 권한 설정	지정한 사이트, 도메인 또는 조직 구성 단위에 그룹 정책에 관련된 사용 권한을 설정합니다.
FindDisabled GPOs.wsf	사용할 수 없는 GPO 목록 출력	지정한 도메인에서 전체 또는 부분적으로 사용할 수 없는 GPO를 모두 출력합니다.
DumpGPOInfo.wsf	GPO 정보 출력	만든 시간, 수정 시간, 소유자, 상태, 버전, GPO를 필터링 하는 보안 그룹, 모든 권한, 편집, 읽기 또는 사용자 지정 권한을 가진 보안 그룹 및 연결 정보 등 지정한 GPO에 대한 정보를 출력합니다.
DumpSOMInfo.wsf	SOM에 대한 정보 출력	GPO 연결 및 정책 관련 사용 권한 등 지정한 사이트, 도메인 또는 조직 구성 단위에 대한 정보를 출력합니다.
FindGPOsByPolicy Extension.wsf	특정 정책이 설정된 GPO 목록 출력	특정 정책이 설정된 GPO를 모두 출력합니다. 예를 들어 소프트웨어 설치 또는 폴더 리디렉션 정책이 설정된 GPO를 모두 출력합니다.
FindGPOsBy SecurityGroup.wsf	특정 사용자에게 사용 권한이 설정된 GPO 목록 출력	지정한 사용자에게 사용 권한이 설정되어 있는 GPO를 모두 출력합니다. 사용 권한으로 읽기, 적용, 편집 또는 전체 편집을 지정할 수 있습니다.
FindDuplicate NamedGPOs.wsf	중복된 이름이 있는 GPO 목록 출력	지정한 도메인 내에서 중복된 이름을 가진 GPO를 모두 출력합니다.
FindGPOsWith NoSecurity Filtering.wsf	적용 권한이 없는 GPO 목록 출력	지정한 도메인에서 GPO에 적용 권한이 설정되지 않아 아무에게도 적용되지 않는 GPO를 모두 출력합니다.
FindOrphaned GPOsInSYSVOL.wsf	SYSVOL에서 고아가 된 GPO 목록 출력	SYSVOL에서 Active Directory에 해당 구성 요소가 없는 모든 GPO를 찾아 출력합니다.

FindSOMsWith ExternalGPO Links.wsf	외부 GPO가 연결된 SOM 목록 출력	지정한 도메인에서 다른 도메인에 있는 GPO가 연결된 모든 도메인, 조직 구성 단위 및 사이트를 출력합니다.
FindUnlinked GPOs.wsf	SOM에 연결되지 않은 GPO 목록 출력	지정한 도메인에서 SOM에 연결이 없는 모든 GPO를 출력합니다.
GetReports ForAllGPOs.wsf	모든 GPO에 대한 보고서 생성	지정한 도메인에 있는 모든 GPO에 대한 XML 및 HTML 보고서를 생성합니다.
GetReportsFor GPO.wsf	GPO에 대한 보고서 생성	지정한 GPO에 대한 XML 및 HTML 보고서를 생성합니다.
ListAllGPOs.wsf	도메인에 있는 모든 GPO 목록 출력	지정한 도메인에 있는 모든 GPO를 출력합니다.
ListSOMPolicy Tree.wsf	SOM 및 연결 GPO 목록 출력	지정한 도메인에 있는 모든 SOM 목록을 SOM에 연결된 GPO 목록과 함께 출력합니다.
QueryBackup Location.wsf	백업 GPO의 정보 출력	지정한 폴더에 저장된 모든 GPO 백업에 대한 정보를 출력합니다.

표 10 GPMC에서 제공하는 스크립트들

그룹 정책 문제 해결

그룹 정책은 정상적으로 동작하기 위해 많은 서비스들과 상호 의존하고 있습니다. Active Directory부터 그룹 정책 설정 값의 충돌까지 다양한 그룹 정책과 관련한 오류가 발생할 수 있고, 관리자는 오류를 감지하여 문제 해결을 시도해야 합니다.

본 가이드에서는 클라이언트에 적용되는 그룹 정책과 관련한 문제 해결 방안에 대해 설명하겠습니다.

클라이언트의 그룹 정책 현황 파악하기

클라이언트에 적용된 GPO와 적용 되지 않은 GPO에 대한 정보를 파악할 때, 가장 손쉬운 방법은 gpresult.exe를 이용하는 것입니다. 컴퓨터와 사용자에게 적용된 상세한 정책 설정 값 보다는 클라이언트의 전반적인 그룹 정책 적용 현황에 대해 파악할 때 유용합니다.

그룹 명령 프롬프트에서 gpresult를 실행하면 다음 예제와 같은 정보가 출력됩니다.

Microsoft (R) Windows (R) XP Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

2006-01-30 오후 9:19:43에 만듦

NWTRADERS\Gildong.Hong(COMA에 있는)에 대한 RSOP : 로깅 모드

운영 체제 종류: Microsoft Windows XP Professional
운영 체제 구성: 구성원 워크스테이션
운영 체제 버전: 5.1.2600
도메인 이름: NWTRADERS
도메인 종류: Windows 2000
사이트 이름: AsiaSite
로밍 프로필:
로컬 프로필: C:\Documents and Settings\Gildong.Hong
느린 링크에 연결됨: 아니오

컴퓨터 설정

CN=COMA,OU=본사,DC=nwtraders,DC=msft
그룹 정책을 마지막 적용한 시간: 2006-01-30 at 오후 9:17:53
적용한 그룹 정책 원본: DC01.nwtraders.msft
그룹 정책 느린 연결 임계값: 500 kbps

적용된 그룹 정책 개체

N/A

다음 그룹 정책 개체(GPO)는 필터되었기 때문에 적용되지 않았습니다.

Default Domain Policy

필터링: 적용 안 됨(알 수 없는 이유)

본사 보안 정책

필터링: 적용 안 됨(비어 있음)

전사 보안 정책

필터링: 적용 안 됨(비어 있음)

로컬 그룹 정책

필터링: 적용 안 됨(비어 있음)

컴퓨터가 다음 보안 그룹에 소속되어 있습니다.

BUILTIN\Administrators

Everyone

BUILTIN\Users

NT AUTHORITY\NETWORK

NT AUTHORITY\Authenticated Users

COMA$

Domain Computers

사용자 설정

CN=홍길동,OU=본사,DC=nwtraders,DC=msft
그룹 정책을 마지막 적용한 시간: 2006-01-30 at 오후 9:17:53
적용한 그룹 정책 원본: DC01.nwtraders.msft
그룹 정책 느린 연결 임계값: 500 kbps

적용된 그룹 정책 개체

본사 정책
본사 보안 정책

다음 그룹 정책 개체(GPO)는 필터되었기 때문에 적용되지 않았습니다.

전사 보안 정책
필터링: 적용 안 됨(비어 있음)

로컬 그룹 정책
필터링: 적용 안 됨(비어 있음)

사용자가 다음 보안 그룹에 소속되어 있습니다.

Domain Users
Everyone
BUILTIN\Users
BUILTIN\Administrators

NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Authenticated Users
LOCAL
Domain Admins
본사 임직원

Gpresult는 다음과 같이 세 종류의 정보를 제공합니다.

- **일반 정보** : 클라이언트 운영 체제, 클라이언트가 속해 있는 도메인과 사이트 이름에 대한 정보를 출력합니다. 로밍 및 로컬 프로필에 대한 정보와 저속 네트워크 연결 여부에 대해 출력합니다.

- **컴퓨터 설정** : 컴퓨터 계정이 저장되어 있는 컨테이너 DN 정보, 그룹 정책이 마지막으로 적용된 시간 그리고 그룹 정책을 다운로드 받은 도메인 컨트롤러에 대한 정보를 출력합니다. 컴퓨터 설정을 적용한 GPO와 필터링 되어 적용되지 않은 GPO(필터링 사유) 목록을 출력합니다. 컴퓨터 계정이 구성원으로 포함되어 있는 보안 그룹 목록을 출력합니다.

- **사용자 설정** : 사용자 계정이 저장되어 있는 컨테이너 DN 정보, 그룹 정책이 마지막으로 적용된 시간 그리고 그룹 정책을 다운로드 받은 도메인 컨트롤러에 대한 정보를 출력합니다. 사용자 설정을 적용한 GPO와 필터링 되어 적용되지 않은 GPO(필터링 사유) 목록을 출력합니다. 사용자 계정이 구성원으로 포함되어 있는 보안 그룹 목록을 출력합니다.

적용된 정책 설정 값 확인하기

컴퓨터와 사용자에게 적용된 정책 설정 값을 확인하기 위해서는 정책 결과 집합 스냅인을 사용합니다. 시작 → 실행 메뉴를 선택한 후, rsop.msc를 입력하여 정책 결과 집합 스냅인을 실행합니다.

〈그림 66〉와 같이 클라이언트에 적용된 정책 결과 집합 데이터를 수집합니다.

그림 66 정책 결과 집합 데이터 수집

정책 결과 집합 데이터 수집이 완료되면 정책 결과 집합 스냅인이 실행됩니다. 관리자는 정책 결과 집합 스냅인을 이용해서 컴퓨터와 사용자에게 적용된 최종 정책 설정 값과 그 설정 값을 적용한 GPO의 이름을 확인할 수 있습니다.

〈그림 67〉의 예제는 Gildong.Hong 사용자가 로그온 한 ComA 컴퓨터에서 정책 결과 집합 스냅인을 실행한 것으로 사용자 계정에 본사 정책 GPO에 설정된 화면 보호기 관련 정책들이 적용된 것을 확인할 수 있습니다. 각 정책을 더블 클릭하면 정책의 정확한 설정 값을 확인할 수 있습니다.

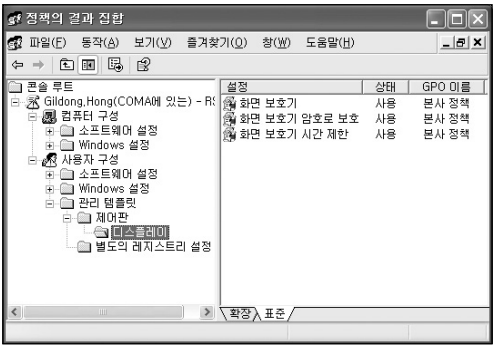

그림 67 정책 결과 집합 스냅인

충돌이 발생한 정책 설정 값 확인하기

관리자가 컴퓨터와 사용자에게 적용하기 위해 설정한 GPO 정책 설정 값이 클라이언트에서 확인한 결과 다른 값으로 설정되어 있을 경우에는 대부분의 경우 다른 GPO에 설정된 정책과 충돌이 발생한 것입니다.

어떤 GPO와 충돌이 발생했고, GPO의 우선 순위에 대해 파악하기 위해서 관리자는 정책 결과 집합 스냅인을 이용할 수 있습니다. 관리자는 시작 → 실행 메뉴를 선택한 후, rsop.msc를 입력하여 정책 결과 집합 스냅인을 실행한 후, 충돌이 발생한 정책을 더블 클릭합니다.

설정 탭에서는 현재 최종적으로 적용된 정책의 설정 값을 확인 할 수 있습니다. 〈그림 68〉은 사용자가 마우스나 키보드를 일정 시간 사용하지 않을 경우에 화면 보호기가 동작하는 시간을 설정하는 정책에 1800초가 설정된 것입니다.

그림 68 최종 적용된 정책 설정 값

우선 순위 탭을 클릭하면 정책이 설정되어 컴퓨터나 사용자에게 적용된 GPO의 목록이 출력됩니다. 〈그림 69〉에서는 사용자 정책인 화면 보호기 시간 제한 정책이 설정되어 현재 로그온 한 사용자에게 적용된 GPO는 본사 정책 GPO와 본사 보안 정책 GPO인 것을 확인 할 수 있습니다.

이 두 GPO에 설정된 화면 보호기 시간 제한 정책의 설정 값이 사용자에게 적용된 것이고, 최종적으로는 우선 순위가 높아 마지막에 적용된 본사 정책 GPO의 설정 값인 1800초가 적용된 것입니다. 따라서 관리자는 GPO의 우선 순위를 변경하는 추가 작업을 수행해서 원하는 GPO의 설정 값이 사용자에게 적용되도록 할 수 있습니다.

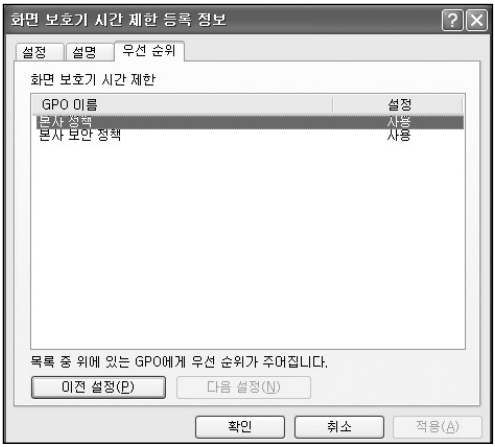

그림 69 정책이 적용된 GPO 우선 순위

그룹 정책 강제 재적용 하기

관리자는 백그라운드 정책 적용 주기와 상관없이 변경된 그룹 정책이 바로 클라이언트에 적용되도록 해야 할 경우가 있습니다. 관리자는 클라이언트 컴퓨터에 gpupdate.exe 명령어를 이용해서 그룹 정책 적용을 강제화 할 수 있습니다.

변경된 정책만 다운로드 받도록 하기 위해서는 명령 프롬프트에서 gpupdate 만 입력하여 실행합니다. 반면에 컴퓨터와 사용자의 모든 정책을 다시 다운로드 받아 적용하기 위해서는 〈그림 70〉와 같이 /force 옵션을 사용합니다. 재 적용한 정책에 따라 사용자 로그오프나 시스템 재시작을 묻는 경우도 있습니다.

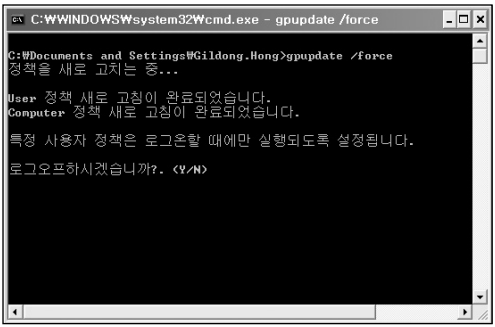

그림 70 gpupdate를 이용한 정책 강제 적용

마치면서

지면 관계상 상세한 내용까지는 담지는 못했지만, 본 그룹 정책 가이드는 그룹 정책의 개요부터 문제 해결까지 그룹 정책을 관리하는 관리자가 반드시 알아두어야 할 내용들에 대해 설명하고 있습니다. 비록 작은 포켓 가이드 북이지만 Active Directory 그룹 정책을 이용해서 사내 보인 인프라를 관리하는 국내 IT Pro에게 큰 도움이 되길 바랍니다.

필라넷 수석 컨설턴트 최철원 저

Microsoft
한국마이크로소프트(유)

서울특별시 강남구 대치동 892번지 포스코센터 서관 5층
전화 : 080-985-2000
www.microsoft.com/korea