Microsoft® Windows Server 2003

Active Directory

운영 가이드

Microsoft®


Microsoft
Windows Server 2003

저자의 글

인증과 보안 인프라로써 많은 기업들이 Active Directory를 구축하여 운영하고 있습니다. 만일 관리자가 Active Directory를 잘못 관리할 경우에는 사용자가 인증을 하지 못하여 업무에 지장을 초래할 수도 있고, 보안상의 허점이 발생할 수도 있습니다.
이에 본 포켓 가이드는 Microsoft Windows Server 2003 Active Directory를 구축, 관리, 문제 해결 하는 일련에 작업들에 대한 How-to 가이드를 제공합니다. 본 가이드의 내용을 기반으로 Active Directory의 가용성과 안정성을 확보하여 사용자들에게 신뢰할 수 있는 컴퓨팅 환경을 제공할 수 있기를 바랍니다.

저자 약력

최철원 / ㈜필라넷 수석 컨설턴트

- Active Directory 인프라 컨설팅 (삼성생명, 삼성토탈, 알리안츠생명, 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 관리자들에게 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)

기획자의 글

Microsoft Windows Server에서 제공하는 Directory Service는 어떤 모습으로 변해 왔을까요? Cairo에서 3가지 기능(Distributed File System, Object oriented File System, Kerberos Security) 제공을 시작으로, NT4.0에서 LDAP을 적용하고 Windows 2000 Server에 이르러 산업 표준 기술을 수용한 Active Directory가 첫 선을 보였으며, Windows Server 2003에서는 좀더 확장된 개념의 Active Directory를 선보이게 되었습니다. 이후 2005년 12월 출시된 Windows Server 2003 R2에서는 Management의 효율성을 강화한 ADFS (Active Directory Federation Service)를 제공하게 되었습니다.

혼돈된 IT 인프라에 체계성을 갖춰 관리, 보안, 상호 운영성의 이익을 갖도록 하는 것이 Active Directory 도입의 가장 큰 이유이며, 새로운 Windows Server 제품이 나올 때 마다 가장 중점을 둬서 발전시킨 것이 Active Directory Service입니다.

최근 국내에서 Active Directory의 도입이 급격히 증가하면서 IT 관리자 분들이 Active Directory를 좀더 효과적으로 구축하고 관리하는데 조금이나마 도움을 드리고자 "Active Directory 운영 가이드"를 기획 제작하게 되었습니다. 모쪼록 본 가이드가 인프라 개선을 통한 귀사의 기업 경쟁력 강화에 큰 도움이 되었으면 합니다.

김영진 / 한국마이크로소프트,
Windows Server Product Marketing Manger

목차

Active Directory 설치

Active Directory를 구성하는 실행 파일들과 데이터베이스 파일들은 모두 도메인 컨트롤러에 저장됩니다. 따라서 Active Directory를 안정적으로 운영하기 위해서는 해킹과 같은 보안 위협으로부터 도메인 컨트롤러를 보호해야 합니다. 만약 회사내의 인증 및 권한 부여를 위해 사용하는 인프라로써 Active Directory를 구성하는 도메인 컨트롤러가 보안 위협에 노출되면 회사 전체에 치명적인 위협이 될 수 있습니다.

Active Directory 설치 마법사를 이용해서 시스템에 Active Directory를 설치함으로써, 관리자는 새 포리스트나 도메인을 생성할 수 있고, 또는 기존 도메인에 추가 도메인 컨트롤러를 생성할 수 있습니다.

Active Directory를 설치하는 과정은 운영 체제 설치 후 도메인 컨트롤러를 생성하고, 보안 위협으로부터 도메인 컨트롤러를 보호하기 위해 다양한 보안을 설정하는 다음과 같은 순서로 이루어집니다.

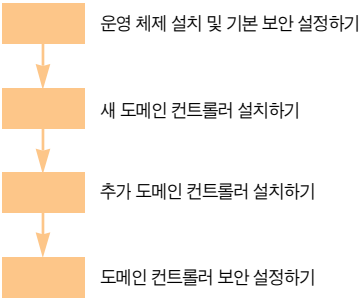

그림 1 Active Directory 설치 프로세스

운영 체제 설치 및 기본 보안 설정하기

Active Directory를 설치하여 도메인 컨트롤러로 운영할 시스템에 Windows Server 2003 운영 체제를 설치합니다. 운영 체제를 설치할 때, 도메인 컨트롤러로 사용될 시스템임을 고려해서 DNS 서비스를 미리 설치하고, 로컬 Administrator 계정의 암호로 복잡성을 만족하는 강력한 암호를 설정합니다.

운영 체제 설치 후에는 최신 서비스 팩과 핫픽스를 설치하여 알려진 운영 체제의 보안 위협으로부터 시스템을 보호하며, 또한 추가적으로 시스템을 보안 위협으로부터 보호하기 위해 몇 가지 기본 보안을 설정합니다.
16 비트용 응용 프로그램을 위해 자동으로 생성되는 8.3 파일 이름 생성 기능

을 정지하여 16 비트로 만들어진 해킹 프로그램이 파일에 접근하는 것을 차단합니다. 또한 Virus Scanning 소프트웨어를 설치하여 바이러스로부터 시스템을 보호합니다. 마지막으로 Windows Server 2003 운영 체제가 부팅하면 자동으로 시작하는 서비스 중에서 도메인 컨트롤러로 동작하는 시스템에서는 불필요한 서비스들을 모두 동작 안 함으로 설정하여 시스템 리소스 절약 및 보안 위협을 감소시킵니다.

Windows Server 2003 운영 체제 설치 및 기본 보안 설정은 다음과 같은 순서로 이루어집니다.

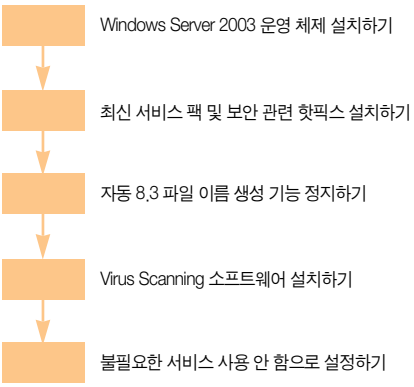

그림 2 운영 체제 설치 및 기본 설정 프로세스

Windows Server 2003 운영 체제 설치하기

도메인 컨트롤러로 사용될 시스템에 Windows Server 2003 운영 체제를 설치할 때는 다음과 같은 사항들을 적용할 것을 권장합니다.

- **모든 파티션은 NTFS로 포맷** : FAT는 파일 및 폴더 단위에 보안 설정을 지원하지 않기 때문에 도메인 컨트롤러로 사용할 시스템의 모든 파티션은 NTFS 보안 설정을 위해 NTFS로 포맷합니다.

- **TCP/IP 프로토콜만 설치** : 도메인 컨트롤러는 TCP/IP 프로토콜만으로도 정상 동작이 가능합니다. 필요 없는 다른 프로토콜은 시스템에 설치하지 않음으로써 보안 위협을 감소시킬 수 있습니다.

- **DNS 설치 함** : 도메인 컨트롤러가 DNS 서버 기능도 수행할 경우에는 운영 체제 설치할 때 DNS를 설치합니다.

- **IIS 설치 안 함** : 도메인 컨트롤러에서 IIS를 운영하는 것은 권장하지 않습니다. IIS와 관련한 다양한 보안 위협이 존재하기 때문에 시스템에 IIS를 설치하지 마십시오.

- **Active Directory 복제에서 SMTP를 사용하지 않으면 SMTP 설치 안 함** : 사이트 간에 메일 기반의 Active Directory 복제를 사용하지 않는다면 일반적인 도메인 컨트롤러에서 SMTP는 필요하지 않습니다.

- **강력한 로컬 Administrator 암호 설정** : 운영 체제를 설치할 때 로컬 Administrator의 암호는 복잡성을 만족하는 암호를 사용합니다. 포리스트의 첫 번째 도메인 컨트롤러를 설치 할 때, 로컬 Administrator 계정의 암

호가 포리스트 루트 도메인의 Administrator 계정의 암호가 됩니다. 다음 조건을 만족하도록 로컬 Administrator 계정의 암호를 설정할 것을 권장합니다.

- 암호의 최소 길이는 9자 이상
- 대문자, 소문자, 특수문자, 숫자를 모두 사용
- 암호의 앞 7자 안에 특수문자를 포함
- 암호에 계정 이름, 관리자 이름, 회사 이름 사용 금지
- 암호 변경 시 이전 암호와 유사한 체계의 암호 설정 금지

최신 서비스 팩 및 보안 관련 핫픽스 설치하기

운영 체제와 관련해 알려진 보안 위협과 내부 버그를 수정한 최신 서비스 팩과 핫픽스를 Microsoft 웹 사이트에서 다운로드 해서 설치합니다.

자동 8.3 파일 이름 생성 기능 정지하기

NTFS 파티션에 생성된 긴 파일 이름을 사용하는 파일들은 16 비트 응용 프로그램과의 하위 호환성을 위해, 자동으로 DOS의 FAT 파티션에서 사용하던 짧은 8.3 파일 이름이 자동으로 생성됩니다.

많은 바이러스나 해킹 관련 도구들은 16 비트 응용 프로그램으로, NTFS 파티션의 파일에 접근할 때 짧은 8.3 파일 이름을 사용합니다. 정상적으로 운영되는 도메인 컨트롤러에서 16 비트 응용 프로그램을 로컬에서 직접 실행하는 경우는 없습니다. 따라서 자동 8.3 파일 이름 생성 기능을 정지함으로써 바이러스나 16 비트 해킹 프로그램이 도메인 컨트롤러의 NTFS 파티션에 접근하는 것을 차단할 수 있습니다.

[따라하기]

자동 8.3 파일 이름 생성 기능 정지하기

레지스트리 편집기를 이용해서 자동 8.3 파일 이름 생성 기능을 정지하는 과정은 다음과 같습니다.

1. 시작 → 실행 메뉴를 선택한 후, regedit를 입력하여 레지스트리 편집기를 실행합니다.
2. 레지스트리 편집기에서 다음 서브키로 이동합니다.
   HKLM\SYSTEM\CurrentControlSet\Control\FileSystem
3. 레지스트리 편집기의 오른쪽 창에서 NtfsDisable8dot3NameCreation를 더블 클릭합니다.
4. 값 데이터 입력창에 1을 입력 한 후, 확인 버튼을 클릭합니다.
5. 레지스트리 편집기를 종료합니다.

Virus Scanning 소프트웨어 설치하기

Windows Server 2003 운영 체제를 설치한 후, 도메인 컨트롤러로 설치하기 전에 먼저 Virus Scanning 소프트웨어를 설치합니다.

최신 바이러스 검사 목록을 다운로드 받은 후에, 바이러스 검사를 실행하여 운영 체제 설치 중에 바이러스의 감염 여부를 점검합니다. 또한 Virus Scanning 소프트웨어가 최신 바이러스를 점검할 수 있도록 바이러스 검사 목록 다운로드와 시스템에 대한 바이러스 검사를 주기적으로 수행하도록 일정을 설정합니다.

불필요한 서비스 사용 안 함으로 설정하기

도메인 컨트롤러에서 동작하는 모든 서비스는 네트워크 공격 대상이 되어 도메인 컨트롤러의 보안을 위협하는 요소가 될 수 있습니다. 보안 위협 요소를 줄이기 위해 도메인 컨트롤러가 정상적으로 동작하는데 꼭 필요한 서비스를 제외한 나머지 서비스는 사용 안 함으로 설정하여, 도메인 컨트롤러를 부팅할 때 동작하지 않도록 합니다.

〈표 1〉은 Windows Server 2003 도메인 컨트롤러로 동작하는 시스템에서 보안을 강화 하기 위해 시작 유형을 사용 안 함으로 설정할 것을 권장하는 서비스 목록입니다.

표 1 시작 유형을 사용 안 함으로 설정할 것을 권장하는 서비스

서비스 이름	기본 시작 유형	권장 시작 유형	용도
Application Management	수동	사용 안함	프로그램 설치 및 제거를 이용해서 배포되는 응용 프로그램을 위한 소프트웨어 설치 서비스를 제공합니다. 도메인 컨트롤러에 임의적으로 소프트웨어가 설치되는 것을 제한하기 위해서 사용 안 함으로 설정합니다.
Automatic Updates	자동	사용 안함	중요한 Windows 업데이트를 다운로드하고 설치할 수 있도록 합니다. 도메인 컨트롤러와 같이 주요한 서버의 경우 관리자가 검증된 핫픽스를 수동으로 설치할 것을 권장합니다.
Background Intelligent Transfer Service	수동	사용 안함	유휴 상태의 네트워크 대역폭을 사용하여 백그라운드에서 파일을 전송합니다. 서비스를 중지하면, Windows Update나 MSN Explorer 등에서 자동으로 프로그램이나 다른 정보를 다운로드할 수 없습니다. 도메인 컨트롤러에서 Automatic Updates 서비스를 사용 안 함으로 설정한 경우에는 이 서비스도 사용 안 함으로 설정합니다.

서비스 이름	기본 시작 유형	권장 시작 유형	용도
Computer Browser	자동	사용 안함	네트워크에 있는 모든 컴퓨터의 목록을 업데이트하고 관리하며, 이 목록을 브라우저로 지정된 컴퓨터에 제공합니다. 도메인 컨트롤러에서 네트워크 컴퓨터 목록을 업데이트되거나 관리하지 않도록 사용 안 함으로 설정합니다.
Distributed Link Tracking Client	수동	사용 안함	클라이언트 프로그램이 NTFS 볼륨이나 동일한 컴퓨터의 다른 NTFS 볼륨, 다른 컴퓨터의 NTFS 볼륨에 있는 링크된 파일을 추적하도록 설정합니다. 서비스를 중지하면 컴퓨터에 있는 링크를 추적하거나 관리할 수 없습니다. 도메인 컨트롤러로 사용하는 서버에서는 사용 안 함으로 설정할 것을 권장합니다.
Error Reporting Service	자동	사용 안함	예상치 못한 응용 프로그램 오류를 모으고 저장하거나 Microsoft에 보고합니다. 도메인 컨트롤러에 발생한 오류 정보를 Microsoft에 보고 할 계획이 없다면 사용 안 함으로 설정합니다.
Portable Media Serial Number Service	수동	사용 안함	컴퓨터에 연결된 Portable Media Player의 시리얼 번호를 검색합니다. 이 서비스가 정지되면, 보호되는 콘텐트가 PMP에 다운로드 되지 않습니다. 도메인 컨트롤러에 PMP를 연결하여 사용하지는 않기 때문에 사용 안 함으로 설정합니다.
Print Spooler	자동	사용 안함	모든 로컬 및 네트워크 프린터 큐를 관리하고 모든 인쇄 작업을 컨트롤합니다. 서비스를 중지하면 로컬 컴퓨터에서 인쇄할 수 없습니다. 도메인 컨트롤러에서 인쇄 작업을 하지 않으면 사용 안 함으로 설정합니다.

서비스 이름	기본 시작 유형	권장 시작 유형	용도
Remote Access Auto Connection Manger	수동	사용 안함	원격 네트워크 또는 컴퓨터에 실패한 연결 시도를 검색하고 대체 연결 방법을 제공합니다. 서비스를 중지하면 사용자가 수동으로 연결해야 합니다. VPN이나 전화 접속을 사용하지 않는 도메인 컨트롤러에서는 사용 안 함으로 설정합니다.
Remote Access Connection Manger	수동	사용 안함	인터넷 또는 다른 원격 네트워크로의 전화 접속 및 가상 사설망(VPN) 연결을 관리합니다. VPN이나 전화 접속을 사용하지 않는 도메인 컨트롤러에서는 사용 안 함으로 설정합니다.
Shell Hardware Detection	자동	사용 안함	자동 실행 하드웨어 이벤트에 대해 알림을 제공합니다. 도메인 컨트롤러에서는 사용 안 함으로 설정할 것을 권장합니다.
Special Administrator Console Helper	수동	사용 안함	관리자가 응급 관리 서비스를 사용하여 명령 프롬프트에 원격으로 액세스합니다. 도메인 컨트롤러에서는 사용 안 함으로 설정할 것을 권장합니다.
Telephony	수동	사용 안함	전화 통신 장치와 IP 기반의 음성 연결을 제어하는 프로그램을 사용하여 클라이언트에 대한 TAPI 지원을 제공합니다. TAPI를 지원하는 응용 프로그램을 사용하지 않는 도메인 컨트롤러에서는 사용 안 함으로 설정합니다.
Uninterruptible Power Supply	수동	사용 안함	컴퓨터에 연결되어 있는 무정전 전원 장치(UPS)를 관리합니다. 무정전 전원 장치(UPS)를 사용하지 않는 도메인 컨트롤러에서는 사용 안 함으로 설정합니다.
Wireless Configuration	자동	사용 안함	IEEE 802.11 어댑터를 자동으로 구성할 수 있도록 합니다. 무선 네트워크나 802.11 인증 프로토콜을 지원하지 않는 도메인 컨트롤러에서는 사용 안 함으로 설정합니다.

[따라하기]

불필요한 서비스 사용 안 함으로 설정하기

불필요한 서비스를 사용 안 함으로 설정하는 과정은 다음과 같습니다.

1. 시작 → 실행 메뉴를 선택한 후, services.msc를 입력하여 서비스 스냅인을 실행합니다.
2. 서비스 목록에서 시작 유형을 사용 안 함으로 설정할 서비스를 마우스 오른 쪽 버튼으로 클릭한 후, 속성 메뉴를 선택합니다.
3. 시작 유형 목록에서 사용 안 함을 선택한 후, 확인 버튼을 클릭합니다.

새 도메인 컨트롤러 설치하기

첫 번째 도메인 컨트롤러를 설치함으로써 포리스트와 도메인이 생성됩니다. 포리스트에 첫 번째 도메인은 포리스트 루트 도메인이라고도 부릅니다.
새 도메인 컨트롤러를 설치하여 기존의 포리스트에 새로운 트리를 생성하거나 하위 도메인을 생성할 수도 있습니다.
Active Directory 논리적 구조에 따라 다양한 도메인으로 구성된 포리스트를 생성할 수 있으며, 포리스트를 생성하고 도메인을 구성하는 첫 걸음은 도메인 컨트롤러를 설치하는 작업입니다.

Active Directory 설치 마법사를 이용해서 새 도메인 컨트롤러 설치하기

Active Directory 설치 마법사를 이용해서 새 도메인 컨트롤러를 설치합니다. 예제에서는 nwtraders.msft 도메인의 첫 번째 도메인 컨트롤러를 설치하여 새 포리스트를 생성합니다.

[따라하기]

Active Directory 설치 마법사를 이용해서 새 도메인 컨트롤러 설치하기

1. 시작 → 실행 메뉴를 선택한 후, dcpromo를 입력하여 Active Directory 설치 마법사를 실행합니다.
2. Active Directory 설치 마법사가 실행됩니다. 간단한 도움말을 읽은 후에 다음 버튼을 클릭합니다.
3. 운영 체제 호환성 페이지가 나타납니다. 도움말을 읽은 후 다음 버튼을 클릭합니다.
4. 서버를 새 도메인의 첫 번째 도메인 컨트롤러나, 기존 도메인의 추가 도메인 컨트롤러로 설정할 것인지를 선택합니다.
   예제에서는 새 포리스트를 생성하기 위해 새 도메인의 도메인 컨트롤러 옵션을 선택한 후, 다음 버튼을 클릭합니다.

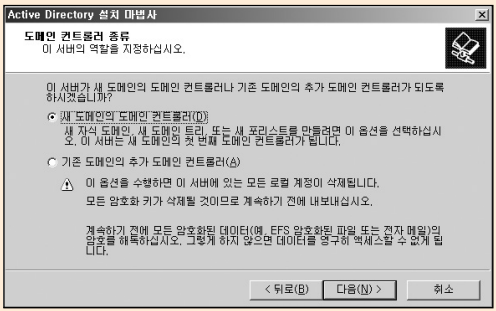

그림 3 도메인 컨트롤러의 종류 지정

5. 새로 생성할 도메인의 유형을 선택한 후, 다음 버튼을 클릭합니다.
   포리스트 루트 도메인을 생성하기 위해서는 새 포리스트에 있는 도메인 옵션을 선택합니다. 기존에 운영중인 도메인의 하위 도메인을 생성하기 위해서는 기존 도메인 트리에 있는 자식 도메인 옵션을 선택합니다. 기존에 운영중인 포리스트에 새로운 트리를 생성하기 위해서는 기존 포리스트에 있는 도메인 트리 옵션을 선택합니다. 예제에서는 새 포리스트 루트 도메인을 생성하기 위해 새 포리스트에 있는 도메인 옵션을 선택합니다.

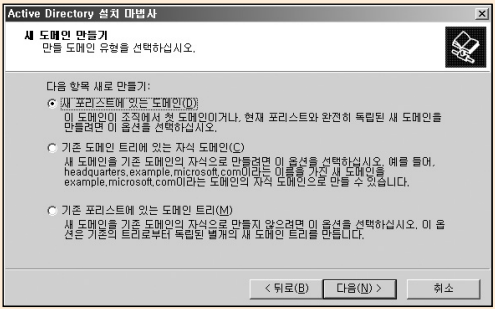

그림 4 새로 생성할 도메인 유형 지정

6. 새 도메인이 사용할 전체 DNS 이름을 〈그림 5〉와 같이 입력한 후, 다음 버튼을 클릭합니다.

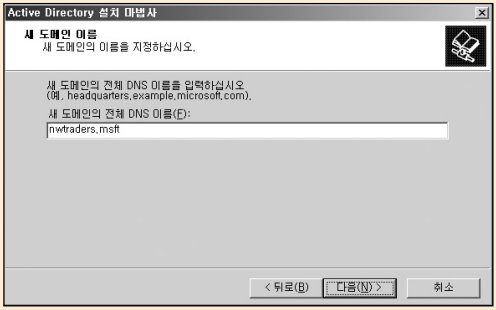

그림 5 새 도메인의 전체 DNS 이름 입력

7. Windows 2000 이전 운영 체제를 사용하는 시스템에서 사용할 NetBIOS 도메인을 입력한 후, 다음 버튼을 클릭합니다.

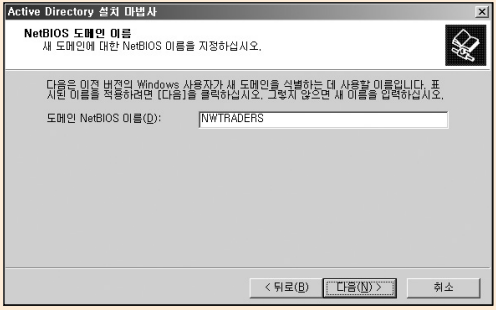

그림 6 새 도메인의 NetBIOS 이름 입력

8. Active Directory 데이터베이스와 로그 파일을 저장할 폴더 경로를 입력한 후, 다음 버튼을 클릭합니다.

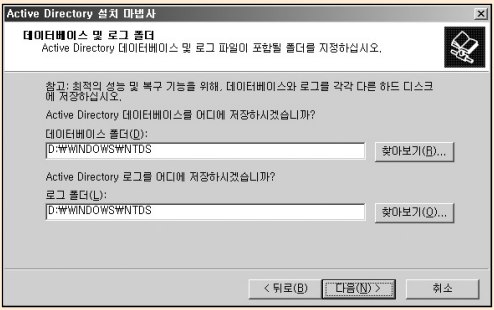

그림 7 데이터베이스 및 로그 폴더 경로 지정

9. 그룹 정책 파일을 저장할 SYSVOL 폴더의 경로를 입력한 후, 다음 버튼을 클릭합니다.

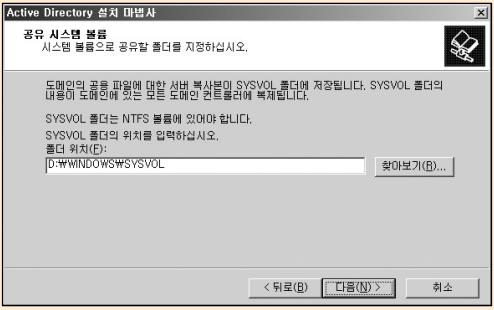

그림 8 SYSVOL 폴더 경로 지정

10. Active Directory가 동작하기 위해 필요한 DNS 구성 여부를 선택합니다. Windows Server 2003 운영 체제를 설치할 때 DNS 서버를 설치 했으므로, Active Directory 설치 마법사가 Active Directory를 운영하기 위해 필요한 DNS 구성을 자동으로 하도록 이 컴퓨터에 DNS 서버를 설치하여 구성하고 이 DNS 서버를 컴퓨터의 기본 DNS 서버로 설정 옵션을 선택한 후, 다음 버튼을 클릭합니다.

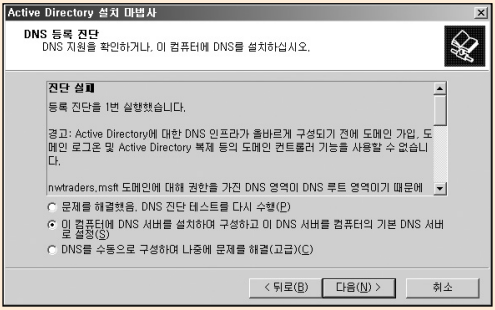

그림 9 DNS 등록 진단

11. 익명 사용자가 도메인의 정보를 읽을 수 있도록 Active Directory 사용 권한을 부여할 것 인지를 선택합니다. Windows 2000 이전의 서버 운영 체제와 호환되는 사용 권한 옵션을 선택하면, Active Directory에 인증 받지 않은 사용자들도 Active Directory의 내용을 읽을 수 있기 때문에 보안이 취약해집니다. Windows 2000 또는 Windows Server 2003 운영 체제와만 호환되는 사용 권한 옵션이 선택되어 있는지 확인한 후, 다음 버튼을 클릭합니다.

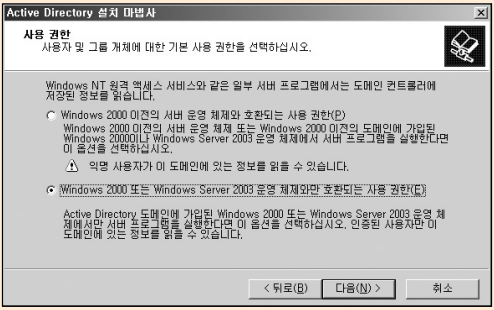

그림 10 사용 권한 설정

12. 디렉터리 서비스 복원 모드로 시스템을 시작했을 때 사용할 로컬 Administrator 계정의 암호를 입력 한 후, 다음 버튼을 클릭합니다.

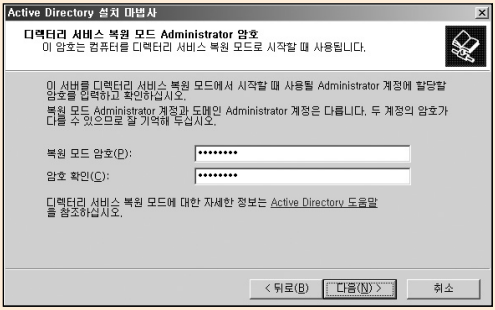

그림 11 디렉터리 서비스 복원 모드 Administrator 암호

13. 요약 페이지에서 선택한 옵션의 내용을 검토한 후, Active Directory를 설치하기 위해 다음 버튼을 클릭합니다.
14. Active Directory 설치가 완료되면, 마침 버튼을 클릭하여 Active Directory 설치 마법사를 종료합니다.
15. Active Directory 설치 마법사에 의해 변경된 내용을 적용하기 위해 지금 다시 시작 버튼을 클릭하여 시스템을 재시작합니다.

무인 설치를 이용해서 새 도메인 컨트롤러 설치하기

Answer 파일을 이용해서 도메인 컨트롤러를 무인 설치하는 것이 가능합니다. Active Directory 설치 마법사를 이용해서 관리자가 필요한 정보를 입력하면서 Active Directory를 설치하면, Active Directory 데이터베이스 경로를 잘못 지정하는 것과 같은 관리자의 실수가 발생할 수 있습니다. 따라서 관리자의 실수를 미연에 방지하고, 작업 속도를 높일 수 있는 무인 설치를 이용해서 새 도메인 컨트롤러를 설치할 것을 권장합니다.

다음은 nwtraders.msft 도메인의 첫 번째 도메인 컨트롤러를 설치하여 새 포리스트를 생성하는 Answer 파일 예제입니다.

```
[DCINSTALL]
ReplicaOrNewDomain=Domain
TreeOrChild=Tree
CreateOrJoin=Create
NewDomainDNSName=nwtraders.msft
DomainNetbiosName=NWTRADERS
DNSOnNetwork=yes
AutoConfigDNS=yes
AllowAnonymousAccess=no
DatabasePath=d:\Windows\NTDS
LogPath= d:\Windows\NTDS
SYSVOLPath= d:\Windows\SYSVOL
SafeModeAdminPassword=Pa$$w0rd
CriticalReplicationOnly=No
RebootOnSuccess=yes
```

[DCINSTALL]

섹션 아래에 Active Directory를 무인 설치하기 위해 필요한 다양한 정보들을 설정합니다. 위 예제에서 사용한 정보들의 상세한 설명은 〈표 2〉를 참고하십시오.

엔트리	설명
ReplicaOrNewDomain	새 도메인을 생성할 것인지(Domain) 또는 도메인에 추가 도메인 컨트롤러를 생성할 것인지(Replica)를 지정합니다.
TreeOrChild	새 도메인을 트리 루트 도메인으로 생성할 것인지(Tree) 또는 기존 도메인에 하위 도메인으로 생성할 것인지(Child)를 지정합니다.
CreateOrJoin	트리 루트 도메인을 새로운 포리스트의 포리스트 루트 도메인으로 생성할 것인지(Create) 또는 기존 포리스트에 추가할 것인지(Join)를 지정합니다.
NewDomainDNSName	새 도메인이 사용할 전체 DNS 이름을 지정합니다.
DomainNetbiosName	Windows 2000 이전 운영 체제를 사용하는 시스템에서 사용할 NetBIOS 도메인을 지정합니다.
DNSOnNetwork	DNS 서버의 IP 주소를 자동으로 설정할 것인지를 지정(Yes 또는 No)합니다.
AutoConfigDNS	Active Directory가 동작하기 위해 필요한 DNS 구성 여부를 지정(Yes 또는 No)합니다.
AllowAnonymousAccess	익명 사용자가 도메인의 정보를 읽을 수 있도록 Active Directory 사용 권한을 부여할 것인지를 지정(Yes 또는 No)합니다.

엔트리	설명
DatabasePath	Active Directory 데이터베이스 파일을 저장할 폴더 경로를 지정합니다.
LogPath	Active Directory 로그 파일을 저장할 폴더 경로를 지정합니다.
SYSVOLPath	그룹 정책 파일을 저장할 SYSVOL 폴더의 경로를 지정합니다.
SafeModeAdminPassword	디렉터리 서비스 복원 모드로 시스템을 시작했을 때 사용할 로컬 Administrator 계정의 암호를 지정합니다.
CriticalReplicationOnly	Active Directory 복제 시에 중요 복제만 수행할 것인지 (Yes) 또는 전체 복제를 수행할 것인지(No)를 지정합니다.
RebootOnSuccess	Active Directory 설치를 성공적으로 완료한 후, 시스템을 재시작 여부를 지정합니다.

표 2 [DCINSTALL] 엔트리 설명

[따라하기]

무인 설치를 이용해서 새 도메인 컨트롤러 설치하기

Answer 파일을 이용해서 새 도메인 컨트롤러를 설치하는 과정은 다음과 같습니다.

1. 시작 → 실행 메뉴를 선택한 후, 다음 명령을 입력하여 Active Directory 설치 마법사를 실행합니다.

   dcpromo /answer:*answerfile*

   *answerfile*에 무인 설치 파일이 저장된 경로를 지정합니다.

추가 도메인 컨트롤러 설치하기

기존에 운영중인 도메인에 도메인 컨트롤러를 추가하는 이유는 여러 가지가 있습니다. 도메인 사용자가 늘어날 경우에는 도메인 컨트롤러를 추가하여 사용자 인증 부하를 분산합니다. 또는 원격 사이트가 생성되어 사이트의 사용자들이 보다 빠르게 인증을 받을 수 있도록 원격 사이트에 도메인 컨트롤러를 추가합니다.

Active Directory 설치 마법사를 이용해서 추가 도메인 컨트롤러 설치하기

Active Directory 설치 마법사를 이용해서 추가 도메인 컨트롤러를 설치합니다. 예제에서는 nwtraders.msft 도메인에 추가 도메인 컨트롤러를 설치합니다.

[따라하기]

Active Directory 설치 마법사를 이용해서 추가 도메인 컨트롤러 설치하기

1. 시작 → 실행 메뉴를 선택한 후, dcpromo를 입력하여 Active Directory 설치 마법사를 실행합니다.
2. Active Directory 설치 마법사가 실행됩니다. 간단한 도움말을 읽은 후에 다음 버튼을 클릭합니다.
3. 운영 체제 호환성 페이지가 나타납니다. 도움말을 읽은 후 다음 버튼을 클릭합니다.
4. 서버를 새 도메인의 첫 번째 도메인 컨트롤러나, 기존 도메인의 추가 도메인 컨트롤러로 설정할 것인지를 선택합니다. 추가 도메인 컨트롤러를 설치하기 위해 기존 도메인의 추가 도메인 컨트롤러 옵션을 선택한 후, 다음 버튼을 클릭합니다.

5. 컴퓨터에 Active Directory를 설치할 수 있는 권한을 가진 계정의 사용자 이름, 암호, 도메인을 입력한 후, 다음 버튼을 클릭합니다.
6. 도메인 컨트롤러를 추가할 도메인 이름을 입력한 후, 다음 버튼을 클릭합니다.
7. Active Directory 데이터베이스와 로그 파일을 저장할 폴더 경로를 입력한 후, 다음 버튼을 클릭합니다.
8. 그룹 정책 파일을 저장할 SYSVOL 폴더의 경로를 입력한 후, 다음 버튼을 클릭합니다.
9. 디렉터리 서비스 복원 모드로 시스템을 시작했을 때 사용할 로컬 Administrator 계정의 암호를 입력 한 후, 다음 버튼을 클릭합니다.
10. 요약 페이지에서 선택한 옵션의 내용을 검토한 후, Active Directory를 설치하기 위해 다음 버튼을 클릭합니다.
11. Active Directory 설치가 완료되면, 마침 버튼을 클릭하여 Active Directory 설치 마법사를 종료합니다.
12. Active Directory 설치 마법사에 의해 변경된 내용을 적용하기 위해 지금 다시 시작 버튼을 클릭하여 시스템을 재시작합니다.

무인 설치를 이용해서 추가 도메인 컨트롤러 설치하기

Answer 파일을 이용해서 도메인 컨트롤러를 기존 운영중인 도메인에 추가하는 것이 가능합니다. Active Directory 설치 마법사를 이용해서 관리자가 필요한 정보를 입력하면서 Active Directory를 설치하면, Active Directory 데이터베이스 경로를 잘못 지정하는 것과 같은 관리자의 실수가 발생할 수 있습니다. 따라서 관리자의 실수를 미연에 방지하고, 작업 속도를 높일 수 있는 무인 설치를 이용해서 추가 도메인 컨트롤러를 설치할 것을 권장합니다.

다음은 nwtraders.msft 도메인에 추가 도메인 컨트롤러를 설치하는 Answer 파일 예제입니다.

```
[DCINSTALL]
ReplicaOrNewDomain=Replica
ReplicaDomainDNSName=nwtraders.msft
ReplicationSourceDC=dc01.nwtraders.msft
UserName=administrator
Password=Pa$$w0rd
UserDomain=nwtraders.msft
DatabasePath=d:\Windows\NTDS
LogPath= d:\Windows\NTDS
SYSVOLPath= d:\Windows\SYSVOL
SafeModeAdminPassword=Pa$$w0rd
CriticalReplicationOnly=no
RebootOnSuccess=yes
```

[DCINSTALL]
섹션 아래에 Active Directory를 무인 설치하기 위해 필요한 다양한 정보들을 설정합니다. 위 예제에서 사용한 정보들의 상세한 설명은 〈표 3〉을 참고하십시오.

엔트리	설명
ReplicaOrNewDomain	새 도메인을 생성할 것인지(Domain) 또는 도메인에 추가 도메인 컨트롤러를 생성할 것인지(Replica)를 지정합니다.
ReplicaDomainDNSName	추가 도메인 컨트롤러를 설치할 도메인의 이름을 지정합니다.
ReplicationSourceDC	추가 도메인 컨트롤러가 복제 할 Active Directory 원본을 가지고 있는 도메인 컨트롤러를 지정합니다. 이 정보를 제공하지 않으면 Active Directory 설치 마법사는 가장 가까운 도메인 컨트롤러를 이용해서 Active Directory를 복제합니다.
UserName	도메인에 도메인 컨트롤러를 추가할 수 있는 권한을 가진 사용자 계정을 지정합니다. 도메인에 추가 도메인 컨트롤러를 설치하기 위해서 Domain Admins 그룹의 구성원이어야 합니다.
Password	도메인에 도메인 컨트롤러를 추가할 수 있는 권한을 가진 사용자 계정의 암호를 지정합니다.
UserDomain	도메인에 도메인 컨트롤러를 추가할 수 있는 권한을 가진 사용자 계정이 저장되어 있는 도메인을 지정합니다.
DatabasePath	Active Directory 데이터베이스 파일을 저장할 폴더 경로를 지정합니다.
LogPath	Active Directory 로그 파일을 저장할 폴더 경로를 지정합니다.
SYSVOLPath	그룹 정책 파일을 저장할 SYSVOL 폴더의 경로를 지정합니다.
SafeModeAdminPassword	디렉터리 서비스 복원 모드로 시스템을 시작했을 때 사용할 로컬 Administrator 계정의 암호를 지정합니다.

엔트리	설명
CriticalReplicationOnly	Active Directory 복제 시에 중요 복제만 수행할 것인지(Yes) 또는 전체 복제를 수행할 것인지(No)를 지정합니다.
RebootOnSuccess	Active Directory 설치를 성공적으로 완료한 후, 시스템을 재시작 여부를 지정합니다.

표 3 [DCINSTALL] 엔트리 설명

[따라하기]

무인 설치를 이용해서 새 도메인 컨트롤러 설치하기

Answer 파일을 이용해서 새 도메인 컨트롤러를 설치하는 과정은 다음과 같습니다.

2. 시작 → 실행 메뉴를 선택한 후, 다음 명령을 입력하여 Active Directory 설치 마법사를 실행합니다.

   dcpromo /answer:*answerfile*

   *answerfile*에 무인 설치 파일이 저장된 경로를 지정합니다.

도메인 컨트롤러 보안 설정하기

도메인 컨트롤러를 정상적으로 설치한 후에는, Active Directory와 파일 복제 서비스가 정상 동작하도록 Virus Scanning 소프트웨어에 관련 파일들에 대한 예외 처리를 설정합니다. 또한 도메인 컨트롤러에 대한 보안을 강화하기 위해 그룹 정책을 설정합니다.

Virus Scanning 소프트웨어 설정하기

도메인 컨트롤러가 된 후에도 안티바이러스 소프트웨어 회사로부터 최신 바이러스 검사 목록을 다운로드 받아 주기적으로 바이러스 검사를 수행해야 합니다. 하지만, 일부 오래된 Virus Scanning 소프트웨어의 경우 정상적인 도메인 컨트롤러 운영에 영향을 미칠 수 있습니다. 따라서 Active Directory와 파일 복제 서비스가 정상적으로 동작할 수 있도록 다음 권장 사항을 준수하십시오.

- 모든 도메인 컨트롤러에 반드시 Virus Scanning 소프트웨어를 설치합니다. 물론 가장 좋은 방안은 도메인 컨트롤러로 바이러스가 유포되는 것을 미연에 방지하기 위해, 모든 서버와 클라이언트에 Virus Scanning 소프트웨어를 설치하여 바이러스가 처음 접근하는 경로(방화벽이나 첫 감염된 클라이언트)에서 바로 제거하는 것입니다.
- Active Directory와 파일 복제 서비스에서 사용하는 파일과 문제를 유발하지 않는 Virus Scanning 소프트웨어 버전을 사용합니다. 일부 오래된 Virus Scanning 소프트웨어 버전의 경우 바이러스 검사를 수행할 때, 파일의 메타데이터를 수정하여 대량의 파일 복제를 유발시킵니다.
- 바이러스에 감염될 수 있는 행위를 도메인 컨트롤러에서 수행하지 않도록 도메인 컨트롤러를 클라이언트 용도로 사용하지 마십시오.
- 가능하면 도메인 컨트롤러를 파일 서버 용도로 사용하지 마십시오. Virus Scanning 소프트웨어는 공유에 수정되는 모든 파일에 대해 바이러스 검사를 수행해야 하기 때문에 도메인 컨트롤러에 부하를 줍니다.

파일 복제 서비스에 대량 복제를 유발하지 않는 Virus Scanning 소프트웨어에 대한 정보는 Antivirus, backup, and disk optimization programs that are compatible with the File Replication service(KB815263) 문서를 참고하기 바

랍니다.

Active Directory와 파일 복제 서비스가 정상적으로 동작하기 위해서 다음 폴더와 파일들은 바이러스 검사에서 제외합니다. 바이러스 검사에 예외 처리하는 파일들은 실행 파일들이 아니기 때문에 바이러스에 감염되지 않습니다. 하지만 만약 예외 처리하지 않으면 파일 락킹 때문에 성능 이슈가 발생할 수 있습니다. Virus Scanning 소프트웨어를 이용해서 아래에 폴더들과 파일들을 바이러스 검사에서 예외 처리할 것을 권장합니다.

〈표 4〉는 예외 처리해야 하는 Active Directory 관련 파일들로, 파일들이 존재하는 폴더의 경로는 두 번째 칼럼의 레지스트리 값을 참조합니다.

예외 처리	HKLM\System\CurrentControlSet\Services\NTDS\Parameters
NTDS.dit	DSADatabaseFile
EDB*.log Res1.log Res2.log	Database Log Files Path
Temp.edb Edb.chk	DSA Working Directory

표 4 예외 처리해야 하는 Active Directory 관련 파일들

〈표 5〉는 예외 처리해야 하는 파일 복제 서비스 관련 파일들로, 파일들이 존재하는 폴더의 경로는 두 번째 칼럼의 레지스트리 값을 참조합니다.

예외 처리	HKLM\System\CurrentControlSet\Services\NtFrs\Parameters
jet\sys\edb.chk jet\ntfrs.jdb jet\log*.log	Working Directory
log*.log	DB Log File Directory
예외 처리	**HKLM\System\CurrentControlSet\Services\NtFrs\Parameters\ReplicaSets\GUID**
%systemroot%\sysvol\sysvol	Replica Set Root
%systemroot%\sysvol\staging areas	Replica Set Stage
%systemroot%\sysvol\sysvol\DO_NOT_REMOVE_NtFrs_PreInstall_Directory	

표 5 예외 처리해야 하는 파일 복제 서비스 관련 파일들

〈표 5〉에서 제시한 파일 복제 서비스가 정상적으로 동작하도록 예외 처리해야 할 SYSVOL 폴더의 경로를 정리하면 〈표 6〉과 같습니다.

폴더	예외 처리 여부
%systemroot%\sysvol	예외 처리
%systemroot%\sysvol\domain	바이러스 검사
%systemroot%\sysvol\domain\DO_NOT_REMOVE_NtFrs_PreInstall_Directory	예외 처리
%systemroot%\sysvol\domain\Policies	바이러스 검사
%systemroot%\sysvol\domain\Scripts	바이러스 검사
%systemroot%\sysvol\staging	예외 처리
%systemroot%\sysvol\staging areas	예외 처리
%systemroot%\sysvol\sysvol	예외 처리

표 6 예외 처리해야 하는 Active Directory 관련 파일들

도메인 컨트롤러 그룹 보안 설정하기

새 Windows Server 2003 도메인에는 자동으로 생성된 다음 두 그룹 정책에 의해 전체 도메인 및 도메인 컨트롤러에 기본적인 보안 설정이 적용됩니다.

- Default Domain Policy : 전체 도메인 사용자 및 컴퓨터에 적용되며, 계정 정책을 이용해서 사용자 인증 및 암호와 관련된 보안 정책이 설정되어 있습니다.
- Default Domain Controller Policy : 도메인 컨트롤러에만 적용되는 정책이 설정되어 있습니다.

일반적인 환경에서, 두 기본 그룹 정책만으로 도메인과 도메인 컨트롤러를 보안 위협으로부터 보호할 수 있습니다. 하지만 두 기본 그룹 정책을 수정하여 보다 강력한 보안 설정이 가능하며, 특히 해킹의 주 대상이 되는 도메인 컨트롤러는 더욱 보안을 강화할 필요가 있습니다.

전체 도메인의 보안 정책을 강화하기 위해 Default Domain Policy의 계정 잠금 정책을 〈표 7〉과 같이 설정할 것을 권장합니다.

정책	기본 설정	권장 설정	설명
계정 잠금 기간	정의되지 않음	0 분	계정이 잠기면 관리자에 의해 계정 잠금을 수동으로 해제하도록 설정합니다.
계정 잠금 임계값	0 번의 잘못된 로그온 시도	20번의 잘못된 로그온 시도	기본 설정인 0 번의 잘못된 로그온 시도는 계정 잠금이 동작하지 않습니다. 값을 지정하여 연속 암호가 실패하면 계정이 잠기도록 설정합니다.
다음 시간 후 계정 잠금 수를 원래대로 설정	정의되지 않음	30 분	30분 안에 계정 잠금 임계값을 초과하여 로그온에 실패하면 계정이 잠기도록 설정합니다.

표 7 계정 잠금 정책의 보안 강화 설정

도메인 컨트롤러의 보안 정책을 강화하기 위해 Default Domain Controller Policy의 사용자 권한 할당 정책을 〈표 8〉과 같이 적용할 것을 권장합니다.

정책	기본 설정	권장 설정	설명
로컬 로그온 허용	Account operators Administrators Backup Operators Print Operators Server Operators	Administrators Backup Operators Server Operators	Account Operator와 Print Operator는 도메인 컨트롤러에 로컬 로그온 할 필요가 없습니다.
시스템 종료	Account operators Administrators Backup Operators Print Operators Server Operators	Administrators Backup Operators Server Operators	Account Operator와 Print Operator는 도메인 컨트롤러에 로컬 로그온 할 필요가 없습니다.

표 8 사용자 권한 할당 정책의 보안 강화 설정

도메인 컨트롤러의 보안 정책을 강화하기 위해 Default Domain Controller Policy의 보안 옵션 정책을 〈표 9〉와 같이 적용할 것을 권장합니다.

정책	기본 설정	권장 설정	설명
감사: 글로벌 시스템 개체에 대한 액세스 감사	정의되지 않음	사용 안 함	이벤트, MS-DOS 디바이스와 같은 시스템 개체에 대한 감사 기능을 사용하지 않도록 설정합니다.
감사: 백업 및 복원 권한 사용을 감사	정의되지 않음	사용 안 함	백업 및 복원을 포함해서 사용자 권한에 대한 감사 기능을 사용하지 않도록 설정합니다.
감사: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료	정의되지 않음	사용 안 함	보안 로그가 꽉 차더라도 도메인 컨트롤러를 종료하지 않도록 설정합니다.

정책	기본 설정	권장 설정	설명
네트워크 액세스: 네트워크 인증에 대한 자격 증명의 저장소나 .NET Passport 허용 안 함	정의되지 않음	사용	도메인 컨트롤러에서는 필요 없는 기능입니다.
네트워크 액세스: 명명된 파이프와 공유에 대한 익명 액세스 제한	정의되지 않음	사용	네트워크 공유 폴더와 명명된 파이프에 인증 받지 않은 사용자가 접근하는 것을 차단하도록 설정합니다.
대화형 로그온: 마지막 사용자 이름 표시 안 함	정의되지 않음	사용	마지막 로그온 한 사용자 계정이 Windows 로그온 대화 상자에 출력되지 않도록 설정합니다.
대화형 로그온: [CTRL+ALT+DEL]을 사용할 필요 없음	정의되지 않음	사용 안 함	로그온 하기 위해 사용자는 반드시 [CTRL+ALT+DEL]을 누르도록 설정합니다.
대화형 로그온: 캐시할 로그온의 회수(도메인 컨트롤러가 사용 불가능 할 경우)	정의되지 않음	0 번 로그온	0 번 로그온으로 설정하면 이전 로그온에 대한 캐시를 하지 않습니다. 인증을 받아야만 도메인 컨트롤러에 로그온이 가능합니다.
대화형 로그온: 암호 만료 전에 사용자에게 암호를 변경하도록 프롬프트	정의되지 않음	14 일	복잡성을 만족하는 암호를 생각하고 다시 설정할 충분한 시간을 제공하기 위해 설정합니다.

정책	기본 설정	권장 설정	설명
대화형 로그온: 워크스테이션 잠금 해제를 위해 도메인 컨트롤러 인증 필요	정의되지 않음	사용	캐시된 사용자 계정 정보로 잠금을 해제하면 사용자의 변경된 그룹 정책, 그룹 구성원 등이 적용되지 않습니다. 변경된 사용자 정책이 바로 적용 될 수 있도록 잠금 해제를 위해 도메인 컨트롤러 인증을 사용하도록 설정합니다.
도메인 구성원: 컴퓨터 계정 암호 변경 사용 안함	정의되지 않음	사용 안 함	보안 강화를 위해 주기적으로 컴퓨터 계정의 암호를 변경하도록 설정합니다.
도메인 구성원: 컴퓨터 계정 암호 최대 사용 기간	정의되지 않음	30 일	보안 강화를 위해 주기적(30일)으로 컴퓨터 계정의 암호를 변경하도록 설정합니다.
도메인 구성원: 고급 세션 키 요청 (Windows 2000 또는 그 이상)	정의되지 않음	사용	도메인 컨트롤러 상호간에 가장 보안성이 높은 연결을 사용하도록 설정합니다.
도메인 컨트롤러: Server Operator가 작업을 스케줄하도록 허용	정의되지 않음	사용 안 함	Administrators 그룹의 구성원이 작업을 스케줄하도록 설정합니다.
도메인 컨트롤러: 컴퓨터 계정 암호 변경 거부	정의되지 않음	사용 안 함	보안 강화를 위해 주기적으로 컴퓨터 계정의 암호를 변경하도록 설정합니다.
복구 콘솔: 모든 드라이브 및 폴더에 플로피 복사 및 액세스 허용	정의되지 않음	사용 안 함	인증 받지 못한 사용자가 도메인 컨트롤러의 파일에 접근하지 못하도록 설정합니다.

정책	기본 설정	권장 설정	설명
복구 콘솔: 자동 관리로그온 허용	정의되지 않음	사용 안 함	복구 콘솔을 이용해서 도메인 컨트롤러에 로그온 할 때, Administrator의 암호가 필요하도록 설정합니다.
시스템 개체: 내부 시스템 개체(예:심볼 링크)에 대한 기본 사용 권한을 강화	정의되지 않음	사용	Administrators 그룹의 구성원이 아닌 사용자는 내부 시스템 개체의 내용을 읽을 수 만 있고, 수정할 수 없도록 설정합니다.
시스템 종료: 가상 메모리 페이지 파일 지움	정의되지 않음	사용	시스템 종료 시에 프로세스 메모리 데이터를 페이지 파일에서 삭제합니다.
시스템 종료: 로그온하지 않고 시스템 종료 허용	정의되지 않음	사용 안 함	인증 받고 권한 있는 관리자만이 시스템을 종료 할 수 있도록 설정합니다.
장치: 로그온할 필요 없이 도킹 해제 허용	정의되지 않음	사용 안 함	도메인 컨트롤러로 노트북을 사용하지 않기 때문에 사용 안 함으로 설정합니다.
장치: 로컬로 로그온 한 사용자만이 플로피 드라이브에 액세스 가능	정의되지 않음	사용	로컬로 로그온 한 관리자만이 플로피 드라이브를 사용할 수 있도록 설정합니다. 네트워크에서는 도메인 컨트롤러의 플로피 드라이브를 사용할 수 없습니다.
장치: 로컬로 로그온 한 사용자만이 CD-ROM에 액세스 가능	정의되지 않음	사용	로컬로 로그온 한 관리자만이 CD-ROM을 사용할 수 있도록 설정합니다. 네트워크에서는 도메인 컨트롤러의 CD-ROM을 사용할 수 없습니다.

정책	기본 설정	권장 설정	설명
장치: 사용자가 프린터 드라이버를 설치할 수 없게 함	정의되지 않음	사용	Administrators와 Server Operators 그룹의 구성원만이 프린터 드라이버를 설치할 수 있도록 설정합니다.
장치: 서명되지 않은 드라이버 설치 동작	정의되지 않음	설치 허용 안 함	도메인 컨트롤러에 신뢰할 수 없는 장치 드라이버가 설치되지 않도록 설정합니다.
장치: 이동식 미디어 포맷 및 꺼내기 허용	정의되지 않음	Administrators	Administrators 그룹의 구성원만이 NTFS로 포맷된 이동식 미디어를 꺼낼 수 있도록 설정합니다.
Microsoft 네트워크 서버: 세션 연결을 중단하기 위해 필요한 유휴 시간	정의되지 않음	15 분	일정 시간(15분) 동안 사용하지 않는 SMB 세션 연결을 중단하도록 설정합니다.
Microsoft 네트워크 서버: 로그온 시간이 만료되면 클라이언트 연결 끊기	정의되지 않음	사용	사용자의 로그온 시간이 만료되면 도메인 컨트롤러에 연결된 SMB 세션을 강제 종료 하도록 설정합니다.
Microsoft 네트워크 클라이언트: 타사 SMB 서버에 암호화되지 않은 암호를 보냄	정의되지 않음	사용 안 함	도메인 컨트롤러가 non-Microsoft SMB 서버와 통신할 필요가 없다면, 텍스트 형식으로 암호를 전송하지 않도록 설정합니다.

표 9 보안 옵션 정책의 보안 강화 설정

Windows Time Service 관리

LOB 어플리케이션과 많은 Windows 서비스가 정상적으로 동작하기 위해서 시간 동기화는 매우 중요합니다. 도메인 안에 모든 도메인 컨트롤러와 클라이언트가 시간 동기화를 통해 정확히 동일한 시간을 유지해야만 Kerberos 인증 및 복제가 정상적으로 이루어질 수 있습니다.

Microsoft Windows Server 2003 Windows Time Service(W32Time)는 Network Time Protocol(NTP)을 이용해서 네트워크에서 동작중인 모든 컴퓨터의 날짜와 시간을 지정된 시간 원본을 이용해서 동기화 합니다. Network Time Protocol은 UDP 123 포트를 사용하기 때문에 클라이언트와 시간 원본 사이에 방화벽이 존재할 경우에는 해당 포트를 열어 놓아야만 정상적인 시간 동기화가 이루어집니다.

Windows Time Service는 자동으로 다음과 같은 Active Directory 구조 기반을 이용해서 효율적인 시간 동기화를 수행합니다.

- 모든 클라이언트 컴퓨터는 도메인 컨트롤러를 시간 원본으로 사용합니다.
- 모든 멤버 서버는 클라이언트와 마찬가지로 도메인 컨트롤러를 시간 원본으로 사용합니다.
- 도메인 컨트롤러는 자신이 속한 도메인의 PDC 에뮬레이터로 동작하는 도메인 컨트롤러나 상위 도메인의 도메인 컨트롤러를 시간 원본으로 사용합니다.

- 하위 도메인의 PDC 에뮬레이터는 포리스트 루트 도메인의 PDC 에뮬레이터로 동작하는 도메인 컨트롤러나 그 외 도메인 컨트롤러를 시간 원본으로 사용합니다.

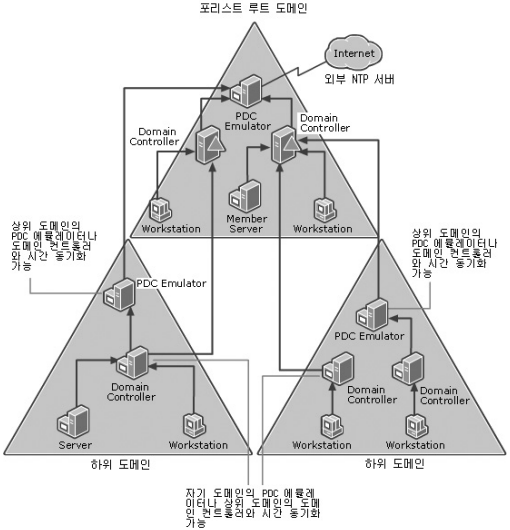

그림 12 Active Directory 구조 기반의 시간 동기화

이와 같은 구조로 시간 동기화가 이루어지기 때문에 결국 포리스트 루트 도메인의 PDC 에뮬레이터로 동작하는 도메인 컨트롤러가 전체 포리스트의 시간 원본이 됩니다. 포리스트 루트 도메인의 PDC 에뮬래아터의 시간을 정확하게 설정하기 위해서 인터넷에 존재하는 외부 NTP 서버와 시간 동기화를 하도록 설정할 수 있습니다. 현재 인터넷에는 표준 시간을 제공하는 많은 수의 NTP 서버가 존재합니다. 사용 가능한 외부 NTP 서버의 목록은 A List of the Sample Network Time Protocol Time Servers That are Available on the Internet(KB262680) 문서를 참고하시기 바랍니다.

만일 인터넷에 존재하는 외부 NTP 서버에 접속할 수 없는 환경에서 정확한 시간 원본이 필요할 경우에는 GPS 디바이스와 같이 시간 동기화 기능을 제공하는 하드웨어 제품을 사용할 것을 권장합니다.

도메인 컨트롤러의 시간 원본 설정하기

Active Directory 구축 후에 관리자는 다음과 같은 두 가지 경우에 도메인 컨트롤러의 시간 원본 설정을 변경합니다.

- 포리스트 루트 도메인을 구축한 후, PDC 에뮬레이터로 동작하는 도메인 컨트롤러가 인터넷에 존재하는 외부 NTP 서버와 시간 동기화를 하도록 설정합니다.
- 포리스트 루트 도메인에서 PDC 에뮬레이터의 역할을 다른 도메인 컨트롤러로 이전했을 경우에는 두 가지 작업을 수행해야 합니다. 첫 번째는 새로이 PDC 에뮬레이터로 동작하는 도메인 컨트롤러가 인터넷에 존재하는 외부 NTP 서버와 시간 동기화를 하도록 설정합니다. 두 번째 작업은 기존에

PDC 에뮬레이터로 동작하던 도메인 컨트롤러가 외부 NTP 서버가 아닌 Active Directory 구조 기반의 시간 동기화를 수행하도록 Windows Time Service 기본 설정으로 복원합니다.

PDC 에뮬레이터의 시간 원본을 외부 NTP 서버로 변경하기

새 포리스트 루트 도메인을 생성하거나, 다른 도메인 컨트롤러로 PDC 에뮬레이터 역할을 이전하였을 경우에는 새로이 PDC 에뮬레이터로 동작하는 도메인 컨트롤러의 시간 원본을 외부 NTP 서버로 설정해야 합니다.

PDC 에뮬레이터의 시간 원본을 변경하기 전에 외부 NTP 서버와 정상적으로 통신이 되는지 테스트를 수행할 것을 권장하며, 또한 PDC 에뮬레이터의 시간 원본을 변경한 후에는 이벤트 뷰어의 시스템 로그에 W32Time 서비스와 관련한 오류가 기록되어 있는지를 모니터링 합니다.

아래 작업을 PDC 에뮬레이터의 로컬에서 실행하기 위해서 관리자는 Administrators 그룹의 멤버 계정으로 로그온 해야 합니다. 원격에서 작업을 수행한다면 관리자는 Domain Admins 그룹의 멤버이어야 합니다.

[따라하기]

PDC 에뮬레이터의 시간 원본을 외부 NTP 서버로 변경하기

PDC 에뮬레이터의 외부 NTP 서버로 time.nuri.net을 설정하는 과정은 다음과 같습니다.

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행하여 외부 NTP 서버와 PDC 에뮬레이터간의 정상 통신 여부와 상호 시간 차이를 점검합니다.

   w32tm /stripchart /computer:time.nuri.net /samples:1 /dataonly

computer에 외부 NTP 서버의 DNS 이름이나 IP 주소를 입력합니다. 지정한 외부 NTP 서버와 정상 통신이 가능하면 〈그림 13〉의 윗 부분과 같이 PDC 에뮬레이터와의 시간 차이를 출력합니다.

3. 다음 명령을 실행하여 PDC 에뮬레이터의 시간 원본을 지정한 외부 NTP 서버로 변경합니다.

   w32tm /config /manualpeerlist:time.nuri.net /syncfromflags:manual /reliable:yes /update

   manualpeerlist에 외부 NTP 서버의 DNS 이름이나 IP 주소를 입력합니다. 〈그림 13〉과 같이 명령이 성공적으로 완료되었습니다. 메시지가 출력되면 PDC 에뮬레이터의 시간 원본 변경에 성공한 것입니다.

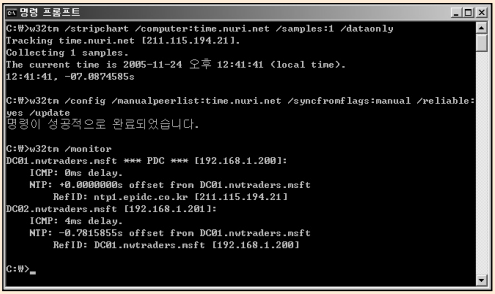

그림 13 외부 NTP 서버 설정

4. 다음 명령을 실행하여 모든 도메인 컨트롤러의 시간 동기화 설정 상태를 점검합니다.

   w32tm /monitor

〈그림 13〉의 아랫부분을 보면 예제 도메인인 nwtraders.msft에는 DC01과 DC02 두 대의 도메인 컨트롤러가 동작 중입니다. 그 중에 DC01이 PDC 에뮬레이터로 동작 중이며, RefID를 보면 외부 NTP 서버가 시간 원본으로 설정되어 있는 것을 확인할 수 있습니다. 반면에 DC02는 도메인 구조 기반에 따라 기본 설정으로 PDC 에뮬레이터인 DC01이 시간 원본으로 설정되어 있는 것을 DC02의 RefID를 보면 확인할 수 있습니다.

Note

w32tm 명령어에 대한 보다 자세한 정보를 원하면, 명령 프롬프트에서 w32tm /? 을 입력합니다.
또는 Microsoft 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=42984)의 Windows Time Service Tools and Settings를 참조하시기 바랍니다.

기존 PDC 에뮬레이터의 시간 동기화 방식을 도메인 구조 기반으로 복원하기

포리스트 루트 도메인에서 PDC 에뮬레이터의 역할을 다른 도메인 컨트롤러로 이전했을 경우에는 기존에 PDC 에뮬레이터로 동작하던 도메인 컨트롤러가 외부 NTP 서버가 아닌 Active Directory 구조 기반의 시간 동기화를 수행하도록 Windows Time Service 기본 설정으로 복원해야 합니다.

[따라하기]

기존 PDC 에뮬레이터의 시간 동기화 방식을 도메인 구조 기반으로 복원하기

기존 PDC 에뮬레이터의 시간 원본을 외부 NTP 서버에서 도메인 구조 기반으로 설정하는 과정은 다음과 같습니다.

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행하여 도메인 구조 기반의 시간 동기화를 수행하도록 설정합니다.

   w32tm /config /syncfromflags:domhier /reliable:no /update

   명령어가 실행되면 기존 PDC 에뮬레이터의 시간 원본으로 이전된 PDC 에뮬레이터가 설정 됩니다.
3. 변경 사항을 반영하기 위해 Windows Time Service를 재시작합니다. 다음 명령을 입력하여 Windows Time Service를 종료합니다.

   net stop w32time
4. 다음 명령을 실행하여 Windows Time Service를 시작합니다.

   net start w32time

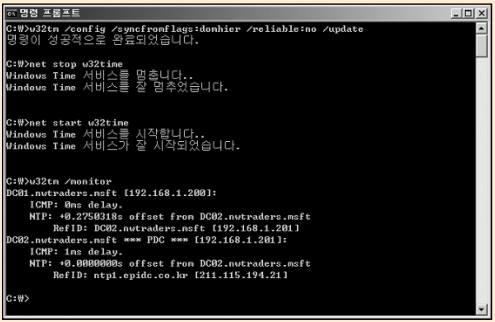

그림 14 도메인 구조 기반으로 복원

5. 다음 명령을 입력하여 모든 도메인 컨트롤러의 시간 동기화 설정 상태를 점검합니다.
   w32tm /monitor
   〈그림 14〉의 예제는 DC02로 PDC 에뮬레이터를 이전하고, 외부 NTP 서버를 시간 원본으로 이미 설정한 상태에서 이전 PDC 에뮬레이터인 DC01의 Windows Time Service 설정을 기본 설정으로 복원하는 과정입니다. 〈그림 14〉 아랫부분에 DC01의 RefID를 보면 시간 원본으로 새 PDC 에뮬레이터인 DC02가 설정된 것을 확인할 수 있습니다.

Windows Time Service 사용 안 함으로 설정하기

NTP 프로토콜을 사용하는 다른 시간 동기화 제품을 사용할 경우에는 Windows Time Service를 사용 안 함으로 설정해야 합니다.

[따라하기]

Windows Time Service 사용 안 함으로 설정하기

Windows Time Service를 사용 안 함으로 설정하는 과정은 다음과 같습니다.

1. 시작 → 실행 메뉴를 선택한 후, services.msc를 입력하여 서비스 스냅인을 실행합니다.
2. 서비스 목록에서 Windows Time을 마우스 오른 쪽 버튼으로 클릭한 후, 속성 메뉴를 선택합니다.
   Windows Time 속성 대화 상자가 실행됩니다.
3. 시작 유형 목록에서 사용 안 함을 선택한 후, 확인 버튼을 클릭합니다.

Windows 기반 클라이언트의 시간 원본 설정하기

Active Directory 도메인 환경하에서 동작하는 Windows 기반 클라이언트들은 도메인 구조 기반에 의해 자동으로 도메인 컨트롤러와 시간 동기화를 수행하기 때문에, 관리자는 클라이언트의 시간 원본 설정을 따로 할 필요가 없습니다. 하지만 다음과 같은 환경에서 동작하는 Windows 기반 클라이언트의 경우에는 자동 시간 동기화가 이루어지지 않습니다.

- Windows 2000 이전 도메인 환경하에서 동작하는 클라이언트 컴퓨터
- UNIX 환경하에서 동작하는 클라이언트 컴퓨터
- 도메인에 가입하지 않은 클라이언트 컴퓨터

이와 같은 클라이언트들의 정확한 시간 설정을 위해 Active Directory 도메인 컨트롤러를 시간 원본으로 설정할 것을 권장합니다. 만약 시간 원본 설정을 하지 않을 경우에 클라이언트는 각자 내부 하드웨어 시계를 이용해서 시간 동기화를 합니다. 이런 경우에는 클라이언트간에 시간이 상이할 수 있으며, 시간 정보를 사용하는 클라이언트의 업무용 어플리케이션이 있을 경우에는 오류를 유발할 수 있습니다.

특정 클라이언트의 시간 원본 설정하기

도메인 구조 기반의 자동 시간 동기화가 이루어지지 않는 클라이언트일 경우에는 관리자가직접 시간 원본을 설정할 수 있습니다. 클라이언트의 시간 원본으로 외부 NTP 서버를 지정할 수도 있고, 회사 내에 Windows 2000 이상의 Active Directory 도메인을 운영 중이라면 도메인 컨트롤러를 클라이언트의 시간 원본으로 지정할 수 있습니다. 클라이언트의 시간 원본을 변경하기 전에 시간 원본과 정상적으로 통신이 되는지 테스트를 수행할 것을 권장하며, 또한 클

라이언트의 시간 원본을 변경한 후에는 이벤트 뷰어의 시스템 로그에 W32Time 서비스와 관련한 오류가 기록되어 있는지를 모니터링 합니다.
아래 작업을 클라이언트의 로컬에서 실행하기 위해서 관리자는 Administrators 그룹의 멤버 계정으로 로그온 해야 합니다.

[따라하기]

특정 클라이언트의 시간 원본 설정하기

특정 클라이언트의 시간 원본을 설정하는 과정은 다음과 같습니다. 예제에서는 기존 운영중인 nwtraders.msft 도메인의 DC01, DC02 두 도메인 컨트롤러를 도메인에 가입하지 않은 클라이언트의 시간 원본으로 설정합니다.

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행하여 시간 원본과 클라이언트간의 정상 통신 여부와 상호 시간 차이를 점검합니다.
   w32tm /stripchart /computer:dc01.nwtraders.msft /samples:1 /dataonly
   computer에 시간 원본으로 지정할 NTP 서버의 DNS 이름이나 IP 주소를 입력합니다.
3. 다음 명령을 입력하여 클라이언트의 시간 원본을 변경합니다.
   w32tm /config /manualpeerlist:" dc01.nwtraders.msft dc02.nwtraders.msft" /syncfromflags:manual /update
   manualpeerlist에 시간 원본으로 지정할 NTP 서버의 DNS 이름이나 IP 주소를 입력합니다. 시간 원본을 두 개 이상 지정할 경우에는 예제와 같이 각 시간 원본을 스페이스로 분리하고, 전체를 큰 따옴표로 묶습니다.
   명령이 성공적으로 완료되었습니다. 메시지가 출력되면 클라이언트의 시간 원본 변경에 성공한 것입니다.

Note

w32tm 명령어에 대한 보다 자세한 정보를 원하면, 명령 프롬프트에서 w32tm /? 을 입력합니다.

또는 Microsoft 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=42984)의 Windows Time Service Tools and Settings를 참조하시기 바랍니다.

클라이언트의 시간 동기화 방식을 도메인 구조 기반으로 복원하기

어떤 목적에 의해 관리자는 도메인에 가입된 클라이언트의 시간 원본으로 특정 NTP 서버를 사용하도록 지정하는 것이 가능합니다. 그 후 다시 클라이언트의 시간 동기화 방식을 도메인 구조 기반의 자동 시간 동기화로 복원할 수 있습니다.

[따라하기]

클라이언트의 시간 동기화 방식을 도메인 구조 기반으로 복원하기

다른 NTP 서버를 시간 원본으로 사용하던 도메인에 가입된 클라이언트의 시간 원본을 도메인 구조 기반으로 복원하는 과정은 다음과 같습니다.

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행하여 도메인 구조 기반의 시간 동기화를 수행하도록 설정합니다.

   w32tm /config /syncfromflags:domhier /update

   명령어가 실행되면 클라이언트의 시간 원본으로 도메인 구조 기반에 따라 적절한 도메인 컨트롤러가 설정 됩니다.

3. 변경 사항을 반영하기 위해 Windows Time Service를 재시작합니다. 다음 명령을 입력하여 Windows Time Service를 종료합니다.
   net stop w32time
4. 다음 명령을 입력하여 Windows Time Service를 시작합니다.
   net start w32time

Windows Time Service를 최초 기본 설정으로 복원하기

만일 로컬 컴퓨터의 Windows Time Service 설정에 오류가 있을 경우에는 문제 해결을 시도하는 것보다 Windows Time Service를 최초 기본 설정으로 복원하는 것이 더 효율적입니다.

[따라하기]

Windows Time Service를 최초 기본 설정으로 복원하기

설정에 오류가 있는 로컬 컴퓨터의 Windows Time Service를 최초 기본 설정으로 복원하는 과정은 다음과 같습니다.

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행하여 Windows Time Service를 종료합니다.
   net stop w32time
3. 다음 명령을 실행하여 로컬 컴퓨터에서 Windows Time Service의 등록을 해제하고, 모든 구성 정보를 레지스트리에서 제거합니다.
   w32tm /unregister

4. 다음 명령을 실행하여 로컬 컴퓨터에서 Windows Time Service가 실행되도록 등록하고, 모든 구성 정보를 기본 설정으로 레지스트리에 추가합니다.
   w32tm /register
5. 다음 명령을 실행하여 Windows Time Service를 시작합니다.
   net start w32time

SYSVOL 관리

Windows Server 2003 System Volume(SYSVOL)은 모든 도메인 컨트롤러의 하드 디스크에 존재하는 폴더로 그룹 정책 파일과 스크립트 파일을 저장하는 표준 저장소로 동작합니다. SYSVOL에 저장된 파일들은 파일 복제 서비스(FRS)에 의해 같은 도메인의 다른 도메인 컨트롤러로 복제됩니다.

SYSVOL에 저장되는 파일들은 그룹 정책 템플릿(GPT)으로 컴퓨터와 사용자에게 적용할 그룹 정책을 저장하는 파일입니다. 반면에 그룹 정책의 버전이나 링크 정보와 같은 그룹 정책 컨테이너(GPC)는 Active Directory에 저장되어 Active Directory 복제에 의해 도메인의 모든 도메인 컨트롤러로 복제됩니다. 따라서 그룹 정책이 정상적으로 컴퓨터와 사용자에게 적용되기 위해서는 모든 도메인 컨트롤러에 그룹 정책 템플릿과 그룹 정책 컨테이너가 복제되어야 합니다.

파일 복제 서비스는 SYSVOL을 모니터링 하여 SYSVOL에 저장되어 있는 파일에 변경이 발생하면, 자동으로 같은 도메인에 다른 도메인 컨트롤러로 변경된 파일을 복제합니다.

SYSVOL 관리

SYSVOL을 관리한다는 것은 SYSVOL이 파일들을 저장하기 위해 충분한 저장 공간이 있는지 점검하고, 파일 복제 서비스에 의해 SYSVOL 안에 파일들이 정상적으로 복제하는지 모니터링 하는 것입니다. 또한 도메인 컨트롤러에 하드 디스크를 추가하거나 제거하는 경우에 필요하다면 SYSVOL과 관련된 관리 작업을 수행해야 합니다. 관리자가 SYSVOL을 관리하기 위해 고려해야 할 사항은 다음과 같습니다.

[저장 공간]

도메인의 구성 환경에 따라, SYSVOL은 정상적인 동작을 위해 많은 양의 저장 공간을 필요로 합니다. 초기 설치 환경에서는 SYSVOL에 할당된 저장 공간만으로도 충분하겠지만, Active Directory가 점점 커지고 복잡해진다면 초기 SYSVOL에 할당된 저장 공간이 부족할 수 있습니다.

이벤트 로그에 SYSVOL의 저장 공간이 부족하다는 이벤트가 기록된다면 관리자는 SYSVOL을 포함하고 있는 하드 디스크의 저장 공간을 늘릴 것인지 아니면 레지스트리에 설정된 SYSVOL 복제 준비(Staging) 영역의 크기 제한 값을 변경할 것인지를 결정해야 합니다. 레지스트리 설정을 변경하는 함으로써 SYSVOL 복제 준비 영역에 더 많은 저장 공간을 할당할 수 있습니다. 이 방법은 SYSVOL를 다른 하드 디스크로 이동하는 것보다는 더 빠르고 작업이 용이합니다.

[성능]

SYSVOL에 저장된 파일에 변경이 발생하며 자동으로 같은 도메인의 다른 도메인 컨트롤러로 복제됩니다. 만약 SYSVOL에 저장된 파일에 변경이 자주 발생한다면, 복제에 의해 SYSVOL을 포함하고 있는 하드 디스크의 I/O가 증가합니다. 예를 들어, 관리자가 GPO를 자주 수정한다면 SYSVOL에 저장된

그룹 정책 파일은 다른 도메인 컨트롤러의 SYSVOL로 복제되기 때문에 각 도메인 컨트롤러의 SYSVOL을 포함하고 있는 하드 디스크 I/O를 증가시킵니다. 만일 SYSVOL을 포함하는 하드 디스크가 Active Directory 데이터베이스나 페이지 파일과 같은 다른 시스템 파일을 역시 포함하고 있다면, 하드 디스크의 I/O를 증가시켜 도메인 컨트롤러의 성능에 영향을 미칠 수 있습니다.

[하드 디스크 관리]

하드 디스크 추가나 제거와 같은 관리 작업을 수행하면서 필요에 따라 SYSVOL의 위치를 변경할 수 있습니다. 비록 SYSVOL을 포함하는 하드 디스크와 상관없는 다른 하드 디스크에 대한 관리 작업을 수행했다 하더라도 SYSVOL에 미치는 영향이 없는지 점검해야 합니다.

드라이브 문자는 하드 디스크를 추가하거나 제거할 경우에 변경 될 수도 있습니다. 파일 복제 서비스는 Active Directory와 레지스트리에 저장된 드라이브 문자를 포함하는 폴더 경로를 이용해서 SYSVOL의 위치를 파악하기 때문에, 만약 드라이브 문자가 변경되면 파일 복제 서비스는 정상적으로 동작할 수 없습니다.

[그룹 정책 백업]

SYSVOL의 그룹 정책 파일들이 파일 복제 서비스에 의해 정상적으로 모든 도메인 컨트롤러에 복제되어 있어야만 그룹 정책이 컴퓨터와 사용자에게 적용됩니다. SYSVOL은 그룹 정책 템플릿(GPT)으로 컴퓨터와 사용자에게 적용할 그룹 정책 파일을 저장하고 있고, 반면에 Active Directory는 그룹 정책 컨테이너(GPC)로 그룹 정책의 버전이나 링크 정보를 저장하고 있습니다. 이 두 정보가 모든 도메인 컨트롤러에 복제되어야만 정상적으로 그룹 정책이 동작합니다. 따라서, SYSVOL의 파일들만 백업하는 것은 완벽한 그룹 정책의 백업이 아닙니다. 그룹 정책 관리 콘솔(GPMC)는 UI 기반이나 스크립트 기반

으로 그룹 정책을 백업할 수 있는 기능을 제공합니다. 정기적인 백업 및 재해 복구 프로세스의 일부분으로 그룹 정책을 백업 하는 것은 관리자의 주요 관리 작업입니다.

SYSVOL 폴더 구조 이해하기

SYSVOL의 위치를 변경하는 작업을 수행하기 위해서 관리자는 SYSVOL의 폴더 구조, 각 폴더들의 상관 관계, 레지스트리나 폴더 자체에 저장된 폴더 경로에 대한 정확한 이해가 필요합니다. SYSVOL를 다른 하드 디스크로 이동하는 작업을 수행하기 위해서는 레지스트리나 폴더에 저장된 각종 폴더 경로를 새 위치로 변경해야 합니다.

SYSVOL 전체를 이동하거나 복제 준비(Staging) 폴더만 이동할 때, 상호 연관성이 있는 폴더와 정션 포인트(Junction Point), 레지스트리 설정에 일관성을 유지해야 합니다. 만일 잘못 설정하면 파일 복제 서비스는 엉뚱한 폴더에 저장된 파일들을 복제하거나, 또는 심각한 오류를 발생시키며 복제를 중단합니다.

SYSVOL에서 사용하는 폴더 중에는 정션 포인트(Junction Point)라는 기능을 사용하는 폴더가 존재합니다. 정션 포인트는 폴더처럼 생겼고 동작도 폴더와 동일하게 동작하지만 엄밀히 말해 폴더는 아닙니다. 사용자는 Windows 탐색기에서 일반 폴더와 정션 포인트를 구분할 수 없습니다. 정션 포인트는 다른 폴더의 링크 정보를 저장하고 있습니다. 만일 사용자가 Windows 탐색기와 같은 어플리케이션을 이용해서 정션 포인트를 클릭하면, 정션 포인트는 자동으로 정션 포인트가 링크하는 폴더로 리디렉션 하여 링크 된 폴더의 파일들을 보여 줍니다.

Note

정션 포인트를 생성하거나 수정하기 위해서는 Windows Server 2003 Resource Kit에서 제공하는 Linkd.exe가 필요합니다. Linkd.exe를 이용해서 정션 포인트에 저장된 링크 정보를 확인하고 또한 정션 포인트를 생성, 수정, 삭제 할 수 있습니다.

예를 들어 C: 루트 하위에 Folder1과 Folder2 두 폴더를 생성하고, 〈그림 15〉와 같이 linkd.exe를 이용해서 Folder3은 C:\Folder1을 링크하는 정션 포인트로 설정한다면, 사용자는 Windows 탐색기에서 다음과 같이 세 개의 폴더를 확인할 수 있습니다.

\Folder1

\Folder2

\Folder3

만일 Folder3을 클릭하면, Windows 탐색기는 자동으로 Folder1로 리디렉션하여 Folder1의 파일들을 보여 줍니다. 리디렉션은 운영체제에서 내부적으로 동작하기 때문에, 사용자나 Windows 탐색기는 리디렉션 되어 링크 된 다른 폴더의 정보를 본다는 아무런 메시지도 제공 받지 않습니다. 결국 사용자는 Folder1을 클릭하거나 Folder3을 클릭했을 때 모두 동일한 파일들을 보게 됩니다. 명령 프롬프트에서 C: 루트 하위 폴더를 출력하면 〈그림 15〉와 같이 Folder1과 Folder2는 〈DIR〉로 표시되고, Folder3은 〈JUNCTION〉으로 나타나는 것을 확인 할 수 있습니다.

그림 15 정션 포인트 생성 및 폴더 목록 보기

SYSVOL을 이동할 때는 숨김 폴더를 포함해서 SYSVOL 하위의 모든 파일과 폴더를 이동해야 합니다. 특히 파일 복제 서비스에 의해 사용되는 폴더 정보를 수정하기 위해서는 다음과 같은 SYSVOL 하위 3 단계까지의 폴더 구조에 대해 파악 할 필요가 있습니다.

%systemroot%\SYSVOL

%systemroot%\SYSVOL\Domain

%systemroot%\SYSVOL\Domain\Policies

%systemroot%\SYSVOL\Domain\Scripts

%systemroot%\SYSVOL\Staging

%systemroot%\SYSVOL\Staging\Domain

%systemroot%\SYSVOL\Staging Areas

%systemroot%\SYSVOL\Staging Areas\Domain FQDN

%systemroot%\SYSVOL\Sysvol

%systemroot%\SYSVOL\Sysvol\Domain FQDN

Note

만일 Windows 탐색기에서 SYSVOL 하위의 일부 폴더가 보이지 않으면, 도구 → 폴더 옵션 메뉴를 선택한 후, 보기 탭에서 숨김 파일 및 폴더 표시 옵션을 선택하십시오.

SYSVOL은 네 개의 하위 폴더를 가지고 있습니다. 이중에서 Domain과 Staging 폴더는 하위에 실제 데이터를 저장하고 있는 폴더이고, 반면에 Staging Areas와 sysvol 폴더는 하위에 정션 포인트가 설정되어 있습니다. %systemroot%\SYSVOL\Domain 폴더는 그룹 정책 템플릿(GPT)으로 컴퓨터와 사용자에게 적용할 그룹 정책 파일을 저장하는 용도로 사용합니다. %systemroot%\SYSVOL\Staging 폴더는 복제할 파일을 압축하고 복제 된 파일의 압축을 해제하는 용도인 복제 준비 폴더로 사용합니다. %systemroot%\SYSVOL\Staging Areas와 %systemroot%\SYSVOL\Sysvol 폴더 하위에 도메인 FQDN을 폴더 이름으로 사용하는 폴더는 정션 포인트입니다. %systemroot%\SYSVOL\Staging Areas\Domain FQDN 정션 포인트는 복제 준비 폴더인 %systemroot%\SYSVOL\Staging\Domain 폴더를 링크하고 있습니다, %systemroot%\SYSVOL\Sysvol\Domain FQDN 정션 포인트는 그룹 정책 파일을 저장하는 %systemroot%\SYSVOL\Domain 폴더를 링크합니다. 따라서 SYSVOL을 이동하여 정션 포인트가 링크하고 있는 폴더의 경로가 변경되면 정션 포인트의 링크 정보를 수정해야 합니다.

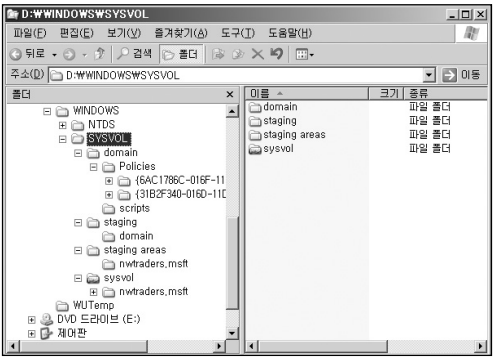

그림 16 SYSVOL 폴더 구조

SYSVOL을 이동하면 정션 포인트뿐만 아니라 Active Directory와 레지스트리에 저장되어 있는 SYSVOL 관련 폴더 정보도 수정해야 합니다.

파일 복제 서비스는 Active Directory에 SYSVOL 폴더 위치와 관련해서 두 값을 저장합니다. 첫 번째는 fRSRootPath에 그룹 정책 파일과 스크립트 파일을 저장하고 있는 SYSVOL 폴더 경로를 저장합니다. 기본 설정으로 이 폴더는 %systemroot%\SYSVOL\Domain 폴더입니다.

두 번째는 fRSStagingPath에 복제 준비로 사용되는 SYSVOL 폴더 경로를 저장합니다.

기본 설정으로 이 폴더는 %systemroot%\SYSVOL\Staging\Domain 폴더입니다. Net Logon 서비스는 HKLM\SYSTEM\CurrentControlSet\Services\NetLogon\Parameters의 SysVol 값에 SYSVOL과 NETLOGON 공유를 생성할 폴더의 경로를 저장합니다. 기본 설정으로 이 폴더는 %systemroot%\SYSVOL\Sysvol 폴더입니다. 따라서 SYSVOL을 이동하여 폴더의 위치가 변경되면 파일 복제 서비스와

Net Logon 서비스가 정상적으로 동작할 수 있도록 Active Directory와 레지스트에 관련 폴더 경로를 수정해야 합니다.
SYSVOL 전체를 이동할 경우에는 먼저 SYSVOL 전체 폴더를 새 위치로 이동합니다. 그 후 정션 포인트의 링크 정보를 수정하고, 관련 서비스들이 사용하는 Active Directory와 레지스트리 정보를 수정합니다.
때에 따라서 SYSVOL 전체를 이동하지 않고, 복제 준비 폴더만 이동하는 것도 가능합니다. 이런 경우에는 먼저 Active Directory의 fRSStagingPath와 %systemroot%\SYSVOL\Staging Areas\Domain FQDN 정션 포인트의 링크 정보를 수정한 후, 복제 준비 폴더를 새 위치로 이동합니다.

복제 준비 폴더의 최대 크기 늘리기

복제 준비 폴더(Staging Area)는 다른 도메인 컨트롤러로 복제할 파일이나 다른 도메인 컨트롤러로부터 복제 된 파일을 임시로 저장하는 폴더입니다. 파일 복제 서비스는 파일을 복제하기 전에 복제할 파일을 복제 준비 폴더에 복사한 후 압축합니다. 그리고 압축된 파일을 다른 도메인 컨트롤러로 복제함으로써 복제 준비 폴더가 사용하는 공간을 절약하고, 복제 시 네트워크 트래픽을 최소화 합니다. 압축된 파일을 복제 받은 도메인 컨트롤러는 역시 복제 준비 폴더에서 압축을 해제한 후, SYSVOL 하위의 적절한 경로에 파일을 복사합니다.
복제 준비 폴더의 최대 크기는 기본 설정으로 660 MB이며, 레지스트리 설정을 수정하여 최소 10 MB에서 최대 2 TB까지 변경할 수 있습니다. 만일 SYSVOL에 많은 파일들이 변경되어 복제 준비 폴더가 660 MB 이상의 저장 공간을 사용하게 되면, 파일 복제 서비스는 이벤트 로그에 이벤트 ID 13522를 기록하여 저장소 공간이 부족할 것을 기록하고, 복제 준비 폴더가 사용할

수 있는 공간이 확보 될 때까지 복제를 중단합니다.
SYSVOL을 포함하고 있는 하드 디스크의 사용 가능한 공간이 충분한 상태에서, 복제 준비 폴더가 사용하는 저장 공간이 레지스트리에 설정된 최대 크기를 초과하여 파일 복제 서비스가 중단된 경우에는 레지스트리를 수정해서 복제 준비 폴더의 최대 크기를 확장해야 합니다.

[따라하기]

복제 준비 폴더의 최대 크기 늘리기

복제 준비 폴더의 최대 크기를 늘리기 위해서는 다음 레지스트리 값을 필요한 용량만큼 변경합니다.

키 위치 : HKLM\SYSTEM\CurrentControlSet\Services\Ntfrs\Parameters
이름 : Staging Space Limit in KB
데이터 종류: REG_DWORD
기본 설정 값: 0xA5000 (660000 KB = 660 MB)

예를 들어 1.2 GB 용량의 데이터를 복제해야 한다면, 사전에 복제에 참여하는 모든 도메인 컨트롤러의 복제 준비 폴더가 사용할 수 있는 저장 공간의 최대 크기를 1.5 GB로 수정할 것을 권장합니다. 복제 준비 폴더의 최대 크기를 설정하는 과정은 다음과 같습니다.

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행하여 파일 복제 서비스를 종료합니다.
   net stop ntfrs
3. 시작 → 실행 메뉴를 선택한 후, regedit를 입력하여 레지스트리 편집기를 실행합니다.
4. 레지스트리 편집기에서 다음 서브키로 이동합니다.
   HKLM\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters

5. 레지스트리 편집기의 오른쪽 창에서 Staging Space Limit in KB를 더블 클릭합니다.
6. 단위 목록에서 10진수를 선택한 후, 값 데이터 입력창에 임시 저장소의 최대 크기를 입력합니다.
   임시 저장소의 최대 크기를 1.5 GB로 확장한다면 1500000를 입력한 후, 확인 버튼을 클릭합니다.
7. 레지스트리 편집기를 종료합니다.
8. 명령 프롬프트를 실행합니다.
9. 다음 명령을 실행하여 파일 복제 서비스를 시작합니다.
   net start ntfrs
10. 이벤트 뷰어를 실행하여 파일 복제 서비스가 정상적으로 재시작 했는지를 점검합니다. 파일 복제 서비스가 정상적으로 재시작 했으면 이벤트 ID 13516이 기록됩니다.

복제 준비 폴더 이동하기

기본 설정으로 Active Directory 설치 마법사는 SYSVOL 아래에 복제 준비 폴더를 생성합니다. Active Directory 설치 마법사는 복제할 파일을 압축하고, 복제 받은 파일의 압축을 해제하는 용도로 사용할 복제 준비 폴더로 두 폴더(Staging과 Staging Area)를 생성합니다. 복제 준비 폴더를 이동할 경우에는 이 두 폴더의 이름을 변경하는 것도 가능합니다. 만일 파일 복제 서비스가 기가 바이트 이상의 파일을 복제해야 한다면 다음과 같은 이유에 따라 복제 준비 폴더의 위치를 다른 하드 디스크로 이동할 것을 권장합니다.

- 복제 준비 폴더가 운영 체제나 다른 응용 프로그램이 필요로 하는 하드 디스크 공간을 모두 사용하는 것을 방지
- 복제 준비 폴더를 다른 물리적 하드 디스크로 이동함으로써, 디스크 I/O를 분산시켜 운영 체제나 다른 응용 프로그램의 성능 향상
- 복제 준비 폴더 최대 크기를 늘려서 복제에 필요한 충분한 사용 공간 제공

복제 준비 폴더를 이동하면 복제 준비 폴더의 경로를 저장하고 있는 두 곳을 업데이트 해야 합니다. 하나는 파일 복제 서비스가 복제 준비 폴더의 위치를 파악하기 위해 사용하는 Active Directory의 fRSStagingPath입니다. 또 다른 하나는 파일 복제 서비스가 압축된 파일을 임시로 저장하는 폴더 경로를 링크하고 있는 SYSVOL의 Staging Area 정션 포인트입니다.
복제 준비 폴더의 이동은 다음과 같은 순서로 진행합니다.

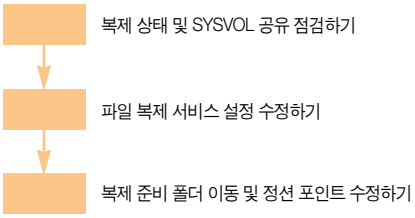

그림 17 복제 준비 폴더 이동 프로세스

복제 상태 및 SYSVOL 공유 점검하기

복제 준비 폴더를 이동하기 전에 먼저 파일 복제 서비스의 정상 동작 여부를 점검합니다. 그리고 복제 토폴로지에 의해 복제가 정상적으로 이루어지는지를 점검하고, 또한 SYSVOL과 NetLogon 공유가 정상적으로 생성되어 있는지도 점검합니다.

[따라하기]

복제 상태 및 SYSVOL 공유 점검하기

1. 시작 → 관리 도구 → 이벤트 뷰어 메뉴를 선택하여, 이벤트 뷰어를 실행합니다.
2. 파일 복제 서비스와 관련한 이벤트를 점검하기 위해, 이벤트 뷰어 왼쪽 창에서 파일 복제 서비스를 클릭합니다.
3. 가장 최근에 서버를 재시작한 이후에 이벤트 ID 13516이 기록되어 있는지 점검합니다.
   이벤트 ID 13516은 파일 복제 서비스가 정상적으로 시작 되었고, SYSVOL과 NetLogon 공유가 정상적으로 생성 되었으며, 도메인 컨트롤러가 정상적으로 동작함을 알려줍니다.
4. 다음 명령을 실행하여 복제가 정상적으로 이루어지는지를 점검합니다.
   dcdiag /test:replications
5. 〈그림 18〉과 같이 computername passed test Replications 메시지가 출력되는지 확인합니다.

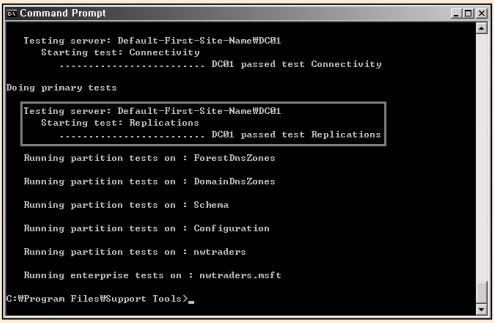

그림 18 복제 점검

6. 명령 프롬프트를 실행합니다.
7. 다음 명령을 실행하여 도메인 컨트롤러에 SYSVOL과 NetLogon 공유가 생성되어 있는지 점검합니다.
   net share
8. 다음 명령을 실행하여 복제가 정상적으로 동작하기 위해 SYSVOL 공유에 로그온 할 수 있는 권한이 적절히 설정되어 있는지 점검합니다.
   dcdiag /test:netlogons
9. 〈그림 19〉와 같이 computername passed test NetLogons 메시지가 출력되는지 확인합니다. 만일 test에 실패했다는 메시지가 출력되면, SYSVOL과 NetLogon 공유 권한이 적절히 설정되었는지 점검합니다.

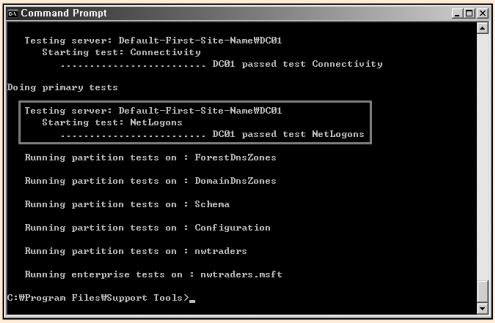

그림 19 SYSVOL 공유 권한 점검

파일 복제 서비스 설정 수정하기

도메인 컨트롤러의 파일 복제 서비스에 의해 복제가 정상적으로 동작하는 것을 점검한 후에는, 파일 복제 서비스가 복제 준비 폴더의 위치를 파악하기 위해 사용하는 Active Directory의 fRSStagingPath와 레지스트리 정보를 수정합니다.

[따라하기]

파일 복제 서비스 설정 수정하기

예제에서는 nwtraders.msft 도메인의 DC01 도메인 컨트롤러의 복제 준비 폴더를 D:\Windows\SYSVOL\Staging\Domain에서 F:\FrsStaging로 이동합니다. 파일 복제 서비스의 설정을 수정하는 과정은 다음과 같습니다.

1. 시작 → 실행 메뉴를 선택한 후, adsiedit.msc를 입력하여 ADSI Edit를 실행합니다.
2. 〈그림 20〉과 같이 ADSI Edit의 왼쪽 창에서 Domain[DC01.nwtraders.msft]\DC=nwtraders,DC=msft\OU=Domain Controllers\CN=DC01\CN=NTFRS Subscriptions로 이동합니다.

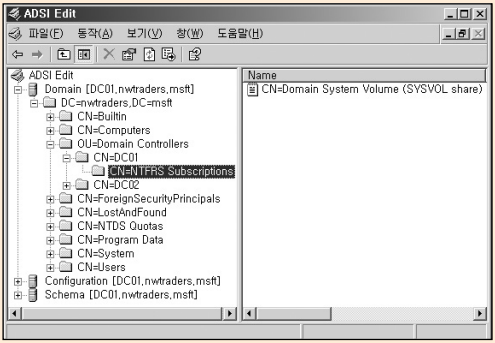

그림 20 ADSI Edit를 이용해서 fRSStagingPath 수정

3. ADSI Edit의 왼쪽 창에서 CN=Domain System Volume (SYSVOL share)를 마우스 오른쪽 버튼으로 클릭한 후, 메뉴에서 속성을 선택합니다.
4. Attribute Editor 탭에서 show mandatory attributes 옵션이 선택되어 있는지 확인합니다. 만약 옵션이 선택되어 있지 않으면 show mandatory attributes 옵션을 선택합니다.
5. Attributes 목록에서 fRSStagingPath를 더블 클릭 합니다.
6. 〈그림 21〉과 같이 이동할 복제 준비 폴더의 경로를 입력한 후, OK 버튼을 클릭합니다.

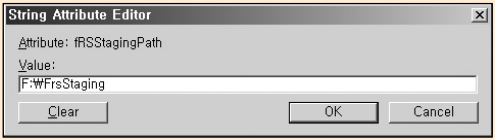

그림 21 복제 준비 폴더 경로 설정

7. 확인 버튼을 클릭하여 속성 대화 상자를 닫은 후, ADSI Edit를 종료합니다.
8. 레지스트리에 저장된 복제 준비 폴더의 경로를 업데이트하기 위해 시작 → 실행 메뉴를 선택한 후, regedit를 입력하여 레지스트리 편집기를 실행합니다.
9. 레지스트리 편집기에서 다음 서브키로 이동합니다.
   HKLM\System\CurrentControlSet\Services\NtFrs\Parameters\Replica Sets
10. Replica Sets 하위에 복제 세트의 GUID로 서브키들이 존재합니다. 복제 준비 폴더의 경로를 변경하기 위해 GUID 서브키를 클릭합니다.
11. 레지스트리 편집기의 왼쪽 창에서 Replica Set Stage의 값이 이전 복제 준비 폴더 경로와 일치하는지 확인합니다. 일치하지 않을 경우에는 일치할 때까지 GUID 서브키들을 검색합니다.
    〈그림 22〉와 같이 Replica Set Stage의 값으로 기존의 복제 준비 폴더인 d:\windows\sysvol\staging\domain이 설정되어 있으면, 이동할 복제 준비 폴더 경로로 수정하기 위해 Replica Set Stage를 더블 클릭합니다.

그림 22 Replica Set Stage 수정

12. 이동할 복제 준비 폴더의 경로를 입력한 후, 확인 버튼을 클릭합니다.
13. 레지스트리 편집기를 종료합니다.

복제 준비 폴더 이동 및 정션 포인트 수정하기

지금까지의 과정을 정상적으로 수행하였으면, 파일 복제 서비스는 복제 준비 폴더의 경로가 변경된 것을 인지하여 아래와 같이 이벤트 ID 13563를 기록합니다.

파일 복제 서비스는 DOMAIN SYSTEM VOLUME (SYSVOL SHARE) 복제본 세트의 준비 경로가 변경되었음을 검색했습니다.

현재 준비 경로 = d:\windows\sysvol\staging\domain
새 준비 경로 = f:\frsstaging

서비스가 다시 시작된 후에는 새 준비 경로를 사용하게 됩니다. 서비스는 컴퓨터를 다시 부팅할 때 마다 다시 시작되도록 설정되어 있습니다. 준비 디렉터리의 데이터 손실을 막기 위해 수동으로 서비스를 다시 시작하는 것이 좋습니다. 수동으로 서비스를 다시 시작하려면 다음을 수행하십시오.

[1] "net stop ntfrs"를 실행하거나 서비스 스냅인을 사용하여 파일 복제 서비스를 중지하십시오.
[2] 복제본 세트 DOMAIN SYSTEM VOLUME (SYSVOL SHARE)에 대응하는 모든 준비 파일을 새 준비 위치로 이동하십시오. 하나 이상의 복제본 세트가 현재 준비 디렉터리를 공유하고 있으면 준비 파일을 새 준비 디렉터리로 복사하는 것이 좋습니다.
[3] "net start ntfrs"를 실행하거나 서비스 스냅인을 사용하여 파일 복제 서비스를 시작하십시오. ("net start ntfrs"에 뒤따라)

이벤트 설명과 같이 복제 준비 폴더를 새 위치로 이동한 후, 정션 포인트를 수정합니다.

[따라하기]

복제 준비 폴더 이동 및 정션 포인트 수정하기

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행하여 파일 복제 서비스를 종료합니다.
   net stop ntfrs
3. 기존 복제 준비 폴더 아래의 모든 파일들을 새로운 복제 준비 폴더로 복사합니다.

4. 다음 명령을 실행하여 파일 복제 서비스를 시작합니다.
   net start ntfrs
5. 정션 포인트를 변경하기 위해, 명령 프롬프트에서
   %systemroot%\SYSVOL\staging areas
   폴더로 디렉터리를 변경합니다.
6. dir 명령을 실행하여 〈JUCNTION〉으로 출력되는 정션 포인트를 확인합니다. 예제에서는 〈그림 23〉과 같이 nwtraders.msft가 정션 포인트임을 확인할 수 있습니다.
7. 정션 포인트가 링크하고 있는 폴더 경로를 확인하기 위해 다음과 같은 명령을 실행합니다.
   Linkd "정션 포인트 경로"
   〈그림 23〉의 중간을 보면 정션 포인트가 이전의 복제 준비 폴더를 링크하고 있는 것을 확인 할 수 있습니다.

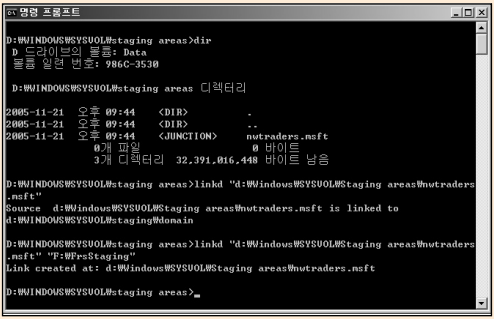

그림 23 정션 포인트 수정

8. 이동한 복제 준비 폴더를 링크하도록 정션 포인트를 업데이트하기 위해 다음과 같은 명령을 실행합니다.
   Linkd "정션 포인트 경로" "이동한 복제 준비 폴더 경로"

SYSVOL 이동하기

복제 준비 폴더만 이동하는 것이 아니라 SYSVOL 전체를 이동한다면, 수작업을 통해 이동이 가능합니다. SYSVOL 이동을 자동화 해 주는 관리 도구는 없기 때문에 관리자는 SYSVOL 복사, 파일 복제 서비스 및 Net Logon 서비스 설정 수정, 보안 설정, 정션 포인트 수정과 같은 일련의 작업을 주의 깊게 수행해야 합니다.

SYSVOL을 다른 하드 디스크로 이동하는 방법으로 Active Directory 설치 마법사를 이용할 수 있습니다. 하지만 이 방법은 먼저 도메인 컨트롤러에서 Active Directory를 제거한 후, 다시 Active Directory 설치 마법사를 이용해서 SYSVOL을 다른 위치로 지정해서 도메인 컨트롤러를 설치하기 때문에 일반적으로 권장하지는 않습니다. SYSVOL 이동은 다음과 같은 순서로 진행합니다.

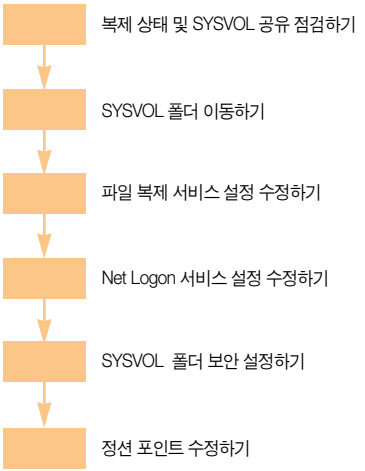

그림 24 SYSVOL 이동 프로세스

복제 상태 및 SYSVOL 공유 점검하기

복제 준비 폴더를 이동하기 전에 먼저 파일 복제 서비스의 정상 동작 여부를 점검합니다.

그리고 복제 토폴로지에 의해 복제가 정상적으로 이루어지는지를 점검하고 또한 SYSVOL과 NetLogon 공유가 정상적으로 생성되어 있는지도 점검합니다.

[따라하기]

복제 상태 및 SYSVOL 공유 점검하기

복제 준비 폴더 이동하기의 [따라하기] 복제 상태 및 SYSVOL 공유 점검하기를 참조하기 바랍니다.

SYSVOL 폴더 이동하기

SYSVOL 폴더를 이동하기 위해서는 %systemroot%\SYSVOL과 그 하위 모든 폴더 및 파일을 이동해야 합니다. %systemroot%\SYSVOL의 하위 폴더 중에는 sysvol이라는 동일한 폴더 이름을 사용하는 폴더가 있습니다. SYSVOL을 이동하기 위해서는 하위 폴더 (%systemroot%\SYSVOL\sysvol)가 아닌 %systemroot%\SYSVOL을 이동하도록 주의하십시오.

[따라하기]

SYSVOL 폴더 이동하기

예제에서는 nwtraders.msft 도메인의 DC02 도메인 컨트롤러의 SYSVOL를 D:\Windows\SYSVOL에서 F:\SYSVOL로 이동합니다. SYSVOL 폴더를 이동하는 과정은 다음과 같습니다.

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행하여 파일 복제 서비스를 종료합니다.
   net stop ntfrs
3. Windows 탐색기를 이용해서 SYSVOL(D:\Windows\SYSVOL)의 모든 내용들을 새로 이동할 폴더(F:\SYSVOL)로 복사합니다.

파일 복제 서비스 설정 수정하기

SYSVOL 폴더를 새 위치로 복사한 후에는, 파일 복제 서비스가 SYSVOL의 위치를 파악하기 위해 사용하는 Active Directory의 fRSRootPath와 fRSStagingPath 값을 수정합니다.

[따라하기]

파일 복제 서비스 설정 수정하기

1. 시작 → 실행 메뉴를 선택한 후, adsiedit.msc를 입력하여 ADSI Edit를 실행합니다.
2. ADSI Edit의 왼쪽 창에서 Domain[DC02.nwtraders.msft]\DC=nwtraders,DC=msft\OU=Domain Controllers\CN=DC02\CN=NTFRS Subscriptions로 이동합니다.

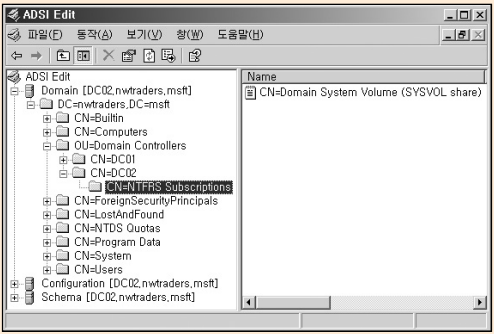

그림 25 ADSI Edit를 이용해서 fRSRootPath와 fRSStagingPath 수정

3. ADSI Edit의 왼쪽 창에서 CN=Domain System Volume (SYSVOL share)를 마우스 오른쪽 버튼으로 클릭한 후, 메뉴에서 속성을 선택합니다.
4. Attribute Editor 탭에서 show mandatory attributes 옵션이 선택되어 있는지 확인합니다. 만약 옵션이 선택되어 있지 않으면, show mandatory attributes 옵션을 선택합니다.
5. 파일 복제 서비스에 의해 복제되는 SYSVOL 폴더를 수정하기 위해 Attributes 목록에서 fRSRootPath를 더블 클릭 합니다.
6. SYSVOL 폴더의 경로를 입력한 후, OK 버튼을 클릭합니다. 경로명을 입력할 때는 〈그림 26〉과 같이 그룹 정책 템플릿 파일들이 저장되는 SYSVOL 폴더 하위에 Domain 폴더명까지 입력합니다.

그림 26 SYSVOL 복제 경로 설정

7. 복제 준비 폴더를 수정하기 위해 Attributes 목록에서 fRSStagingPath를 더블 클릭 합니다.
8. 이동할 복제 준비 폴더의 경로를 입력한 후, OK 버튼을 클릭합니다. 복제 준비 폴더의 경로명을 입력할 때는 〈그림 27〉과 같이 SYSVOL 폴더 하위의 staging\domain 폴더명까지 입력합니다.

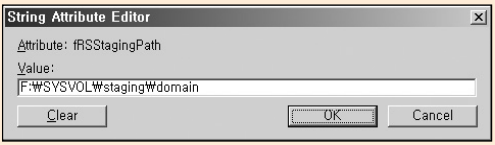

그림 27 복제 준비 폴더 경로 설정

9. 확인 버튼을 클릭하여 속성 대화 상자를 닫은 후, ADSI Edit를 종료합니다.
10. 파일 복제 서비스가 신뢰할 수 없는 복원(non-authoritative restore)을 수행하여 SYSVOL 폴더를 복원하기 위해 시작 → 실행 메뉴를 선택한 후, regedit를 입력하여 레지스트리 편집기를 실행합니다.
11. 레지스트리 편집기에서 다음 서브키로 이동합니다.
    HKLM\System\CurrentControlSet\Services\NtFrs\Parameters\Backup/Restore\Process at Startup
12. 레지스트리 편집기의 오른쪽 창에서 BurFlags을 더블 클릭합니다.
13. 파일 복제 서비스가 신뢰할 수 없는 복원을 수행하도록 D2를 입력한 후, 확인 버튼을 클릭합니다.
14. 레지스트리 편집기를 종료합니다.

Net Logon 서비스 설정 수정하기

Net Logon 서비스는 HKLM\SYSTEM\CurrentControlSet\Services\NetLogon\Parameters의 SysVol 값에 SYSVOL과 NETLOGON 공유를 생성할 폴더의 경로를 저장합니다. 따라서 SYSVOL을 이동하여 폴더의 위치가 변경되면 Net Logon 서비스가 이동한 SYSVOL 경로에 공유를 생성하도록 관련 레지스트리 값을 수정해야 합니다.

[따라하기]

Net Logon 서비스 설정 수정하기

Net Logon 서비스가 SYSVOL 폴더를 공유하기 위해 사용하는 SYSVOL 경로를 수정하는 과정은 다음과 같습니다.

1. 시작 → 실행 메뉴를 선택한 후, regedit를 입력하여 레지스트리 편집기를 실행합니다.
2. 레지스트리 편집기에서 다음 서브키로 이동합니다.
   HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
3. 레지스트리 편집기의 오른쪽 창에서 sysvol을 더블 클릭합니다.
4. 이동한 SYSVOL 경로에 SYSVOL 공유가 생성되도록 경로를 수정한 후, 확인 버튼을 클릭합니다. 경로명을 입력할 때는 SYSVOL 폴더 하위에 sysvol 폴더명까지 입력합니다.
   예제에서는 f:\SYSVOL\sysvol을 입력합니다.
5. SYSVOL 공유 경로가 적절히 수정되었는지 확인한 후, 레지스트리 편집기를 종료합니다.

SYSVOL 폴더 보안 설정하기

이동한 SYSVOL 폴더에 처음 Active Directory 설치 마법사에 의해 설정되었던 보안 설정과 동일한 보안 설정 적용이 필요합니다.

[따라하기]

SYSVOL 폴더 보안 설정하기

SYSVOL 폴더에 적절한 보안 설정을 하는 과정은 다음과 같습니다.

1. 시작 → 실행 메뉴를 선택한 후, notepad를 입력하여 메모장을 실행합니다.
2. 메모장에 아래 내용을 입력한 후, Unicode 인코딩 방식으로 %systemroot%\security\templates 폴더에 sysvol.inf 파일명으로 저장합니다.

```
[Unicode]
Unicode=yes
[Version]
signature=" $CHICAGO$"
Revision=1
[Profile Description]
Description=default perms for sysvol
[File Security]
;" %SystemRoot%\SYSVOL" ,0," D:AR(A;OICI;FA;;;BA)"
 "%Sysvol%" ,2,"
D:P(A;CIOI;GRGX;;;AU)(A;CIOI;GRGX;;;SO)(A;CIOI;GA;;;BA)
(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
 "%Sysvol%\domain\policies" ,2,"
D:P(A;CIOI;GRGX;;;AU)(A;CIOI;GRGX;;;SO)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;
SY)(A;CIOI;GA;;;CO)(A;CIOI;GRGWGXSD;;;PA)"
```

3. 명령 프롬프트를 실행합니다.

4. 새 SYSVOL 폴더에 보안 설정을 하기 위해 다음 명령을 실행합니다.
   secedit /configure /cfg %systemroot%\security\templates\sysvol.inf
   /db %systemroot%\security\templates\sysvol.db /overwrite
5. %systemroot%\ security\logs 폴더의 scesrv.log 파일의 내용을 점검하여 이동한 SYSVOL 폴더에 성공적으로 보안 설정이 되었는지 점검합니다.

정션 포인트 수정하기

SYSVOL에서 사용하는 두 개의 정션 포인트가 이동한 SYSVOL의 경로를 링크하도록 수정합니다. 정션 포인트를 수정한 후에는 파일 복제 서비스를 시작하여 정상적으로 동작하는지 점검합니다.

[따라하기]

정션 포인트 수정하기

1. Windows 탐색기를 이용해서 SYSVOL을 복사하면서 정션 포인트에 복사된 파일이 있는지 점검하여 모두 삭제합니다.
   예제에서는 다음 폴더 하위에 모든 폴더와 파일을 삭제합니다.
   F:\SYSVOL\Sysvol
   F:\SYSVOL\Staging areas
2. 명령 프롬프트를 실행합니다.
3. 그룹 정책 템플릿이 저장되는 폴더를 링크하는 정션 포인트를 수정합니다. 예제에서는 F:\SYSVOL 폴더로 이동하였으므로 다음 명령을 실행하여 수정합니다.
   Linkd "F:\SYSVOL\Sysvol\nwtraders.msft" "F:\SYSVOL\Domain"
4. 복제 준비 폴더를 링크하는 정션 포인트를 수정합니다. 예제에서는 F:\SYSVOL 폴더로 이동하였으므로 다음 명령을 실행하여 수정합니다.

Linkd “F:\SYSVOL\ Staging areas \nwtraders.msft”
“F:\SYSVOL\Staging\Domain”

5. 다음 명령을 실행하여 파일 복제 서비스를 시작합니다.
   net start ntfrs
6. 다음 명령을 실행하여 SYSVOL 공유와 NetLogon 공유가 이동한 SYSVOL 경로에 생성되었는지 점검합니다. 만일 두 공유가 생성되어 있지 않을 경우에는 Net Logon 서비스를 재시작합니다.
   net share
7. 이벤트 뷰어를 실행하여 파일 복제 서비스가 정상적으로 재시작 했는지를 점검합니다.
   파일 복제 서비스가 정상적으로 재시작 했으면 이벤트 ID 13516이 기록됩니다.

글로벌 카탈로그 관리

글로벌 카탈로그는 포리스트에 있는 모든 Active Directory 개체의 정보를 저장하고 있는 도메인 컨트롤러를 말합니다. 글로벌 카탈로그는 글로벌 카탈로그를 호스팅하고 있는 도메인 컨트롤러가 속한 도메인의 모든 개체의 전체 정보를 저장하고, 포리스트에 있는 다른 모든 도메인에 대해서는 모든 개체의 부분 정보를 저장합니다.

글로벌 카탈로그에 포함되는 모든 도메인 개체의 부분 정보는 사용자 검색 작업에 가장 일반적으로 사용되는 정보들입니다. 개체의 정보 중에 글로벌 카탈로그로 복제하여 저장할 것인지에 대한 여부는 스키마 정의를 통해서 가능합니다. 도메인 개체의 특성 중 가장 일반적으로 검색되는 특성을 글로벌 카탈로그에 저장하면, 개체에 대한 정보를 검색할 때 포리스트를 구성하는 도메인 컨트롤러들을 불필요하게 조회하지 않아도 되므로 네트워크 성능에 영향을 주지 않고 효율적이고 빠른 검색이 가능합니다.

포리스트의 첫 번째 도메인 컨트롤러는 자동으로 글로벌 카탈로그로 동작합니다. 관리자는 글로벌 카탈로그를 관리하기 위해 다른 도메인 컨트롤러에 글로벌 카탈로그 기능을 추가하거나, 글로벌 카탈로그 기능을 제거 할 수 있습니다.

Active Directory 환경하에서 글로벌 카탈로그는 다음과 같은 역할을 수행합니다.

- **개체 검색** : 글로벌 카탈로그를 사용하면 데이터가 저장된 도메인의 위치에 관계없이 모든 도메인의 디렉터리 정보를 검색할 수 있습니다. 시작 → 검색 메뉴에서 사람이나 프린터를 검색하거나 쿼리에서 전체 디렉터리 옵션을 선택하면, 글로벌 카탈로그를 이용해서 검색합니다. 검색 요청을 입력하면 요청이 기본 글로벌 카탈로그 포트 3268로 라우팅 되어 글로벌 카탈로그로 보내집니다.
- **UPN 인증 제공** : Windows 로그온 대화 상자에 사용자가 UPN을 입력하여 인증을 요청하면, 도메인 컨트롤러는 글로벌 카탈로그를 검색하여 입력한 UPN과 일치하는 사용자 계정이 존재하는 도메인을 찾습니다. 그 후 사용자 계정이 존재하는 도메인의 도메인 컨트롤러를 이용해서 사용자 인증을 완료합니다.
- **다중 도메인 환경에서 유니버설 그룹 구성원 자격 정보 제공** : 각 도메인에 저장되는 글로벌 그룹 구성원 정보와 달리 유니버설 그룹 구성원 정보는 글로벌 카탈로그에만 저장됩니다. 예를 들어 유니버설 그룹에 속해 있는 사용자가 Windows 2000 기본 도메인 기능 수준 이상으로 설정된 도메인에 로그온 하면, 글로벌 카탈로그를 검색하여 로그온 사용자 계정이 속한 유니버설 그룹 정보를 제공합니다.

Windows 2000 기본 이상의 기능 수준으로 설정된 도메인에 사용자가 로그온할 때 글로벌 카탈로그를 사용할 수 없는 경우, 이 사용자가 이전에 이 도메인에 로그온 한 적이 있으면 컴퓨터는 캐시된 자격 증명을 사용하여 사용자의 로그온을 허용합니다. 사용자가 이전에 이 도메인에 로그온 한 적이 없었다면, 이 사용자는 로컬 계정으로 컴퓨터에 로그온 해야 합니다. 그러나 사용자가 Domain Admins 그룹의 구성원인 경우에는 글로벌 카탈로그를 사용할 수 없을 때도 항상 컴퓨터에 로그온 할 수 있습니다.

포리스트에 도메인이 하나만 있을 경우에는 사용자가 로그온 할 때 글로벌 카탈로그에서 유니버설 그룹 구성원 자격을 검색할 필요가 없습니다. Active Directory가 해당 포리스트에 다른 도메인이 없음을 감지하여 유니버설 그룹 구성원에 대해 글로벌 카탈로그에 검색을 요청하지 않기 때문입니다.

글로벌 카탈로그 서버 추가

포리스트 루트 도메인의 첫 번째 도메인 컨트롤러는 자동으로 글로벌 카탈로그 서버로 설정됩니다. 그 후 포리스트의 규모가 커짐에 따라, 도메인 컨트롤러를 글로벌 카탈로그 서버로 설정할 필요가 발생합니다. 사용자 로그온 및 검색 속도를 향상시키기 위해 사이트 마다 최소 한 대의 글로벌 카탈로그 서버를 운영해야 하며, 만약 사이트 내에 다수의 도메인 컨트롤러가 존재할 경우에는 최소 두 대의 글로벌 카탈로그 서버를 운영하는 것을 권장합니다.

만약 사이트 내에 세 대 이상의 도메인 컨트롤러를 운영할 경우에는, 사이트 내에서 운영중인 도메인 컨트롤러의 과반수 도메인 컨트롤러를 글로벌 카탈로그 서버로 운영하는 것이 가장 좋습니다.

포리스트가 단일 도메인으로 구성되어 있는 경우에는 모든 도메인 컨트롤러를 글로벌 카탈로그 서버로 설정하는 것도 좋은 방안입니다.

글로벌 카탈로그 서버 제거

도메인 컨트롤러에서 글로벌 카탈로그 기능을 제거하면, 도메인 컨트롤러는 DNS에 등록된 글로벌 카탈로그 서버 관련 SRV 레코드를 삭제합니다. KCC는 글로벌 카탈로그 기능이 제거된 도메인 컨트롤러에서 기존에 복제 된 다른 도메인의 개체 정보를 삭제합니다. Windows Server 2003 도메인 컨트롤러에서는 우선 순위가 높은 서비스에 영향을 미치지 않도록, 백그라운드에서 Active Directory의 글로벌 카탈로그 파티션을 삭제합니다. 도메인 컨트롤러에서 글로벌 카탈로그 기능을 제거하는 이유 중에 하나로 Windows Server 2003에서 제

공하는 유니버설 그룹 구성원 캐쉬 기능입니다. 유니버설 그룹 구성원 캐쉬 기능을 이용함으로써 사용자의 수가 적은 사이트에서 동작중인 도메인 컨트롤러는 타 사이트의 글로벌 카탈로그 서버를 이용하면서도 로그온 속도를 향상할 수 있습니다.

글로벌 카탈로그 서버 설정하기

사이트 내에 글로벌 카탈로그 서버가 필요한 경우에는 기존의 도메인 컨트롤러를 글로벌 카탈로그 서버로 설정합니다. NTDS Settings 개체의 글로벌 카탈로그 옵션을 선택하면 KCC는 복제 토폴로지를 업데이트합니다. 복제 토폴로지가 업데이트 된 후에 글로벌 카탈로그 서버로 설정된 도메인 컨트롤러에 다른 도메인의 도메인 파티션의 일부분이 복제됩니다. 복제가 사이트 간에 이루어진다면 사이트 링크 일정에 따라 복제가 발생합니다.

[따라하기]

글로벌 카탈로그 서버 설정하기

예제에서는 DC02.nwtraders.msft 도메인 컨트롤러를 글로벌 카탈로그 서버로 설정합니다. Active Directory 사이트 및 서비스 관리 도구를 이용해서 글로벌 카탈로그 서버를 설정하는 과정은 다음과 같습니다.

1. 시작 → 관리 도구 → Active Directory 사이트 및 서비스 메뉴를 선택하여, Active Directory 사이트 및 서비스 관리 도구를 실행합니다.
2. 콘솔 트리에 Sites를 클릭하여 확장 한 후, 글로벌 카탈로그 서버로 설정할 도메인 컨트롤러가 속해 있는 사이트 개체를 클릭하여 확장합니다.
3. Servers를 클릭하여 확장 한 후, 글로벌 카탈로그 서버로 설정할 도메인 컨트롤러의 서버 개체를 클릭하여 확장합니다.

그림 28 Active Directory 사이트 및 서비스

4. NTDS Settings를 마우스 오른쪽 버튼을 클릭한 후, 속성 메뉴를 선택합니다.
5. NTDS Settings 등록 정보 대화 상자에서 글로벌 카탈로그 옵션을 선택하여, 도메인 컨트롤러를 글로벌 카탈로그 서버로 설정합니다.

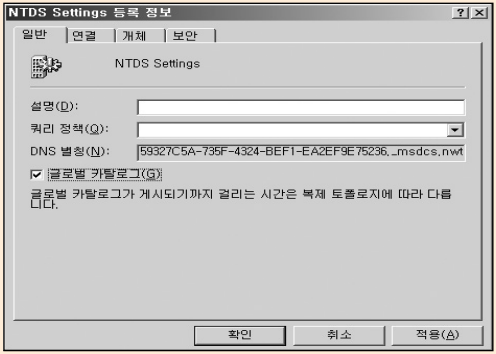

그림 29 글로벌 카탈로그 설정

6. 확인 버튼을 클릭한 후, Active Directory 사이트 및 서비스 관리 도구를 종료합니다.

글로벌 카탈로그 서버 제거하기

NTDS Settings 개체의 글로벌 카탈로그 옵션을 선택 해제함으로써 도메인 컨트롤러에서 글로벌 카탈로그 기능을 제거할 수 있습니다. 옵션 선택을 해제하면 더 이상 클라이언트가 글로벌 카탈로그 검색을 위해 도메인 컨트롤러에 접근하지 않도록, Net Logon 서비스는 DNS 서버에 등록된 글로벌 카탈로그 관련 SRV 레코드를 제거합니다. 또한 3268과 3269 포트로 LDAP 쿼리를 더 이상 받아들이지 않습니다.

[따라하기]

글로벌 카탈로그 서버 제거하기

예제에서는 DC02.nwtraders.msft 도메인 컨트롤러에서 글로벌 카탈로그 서버를 제거합니다. Active Directory 사이트 및 서비스 관리 도구를 이용해서 글로벌 카탈로그 서버를 제거하는 과정은 다음과 같습니다.

1. 시작 → 관리 도구 → Active Directory 사이트 및 서비스 메뉴를 선택하여, Active Directory 사이트 및 서비스 관리 도구를 실행합니다.
2. 콘솔 트리에 Sites를 클릭하여 확장 한 후, 글로벌 카탈로그 서버를 제거할 도메인 컨트롤러가 속해 있는 사이트 개체를 클릭하여 확장합니다.
3. Servers를 클릭하여 확장 한 후, 글로벌 카탈로그 서버를 제거할 도메인 컨트롤러의 서버 개체를 클릭하여 확장합니다.
4. NTDS Settings를 마우스 오른쪽 버튼을 클릭한 후, 속성 메뉴를 선택합니다.
5. NTDS Settings 등록 정보 대화 상자에서 글로벌 카탈로그 옵션이 선택되어 있으면, 선택을 해제하여 도메인 컨트롤러에서 글로벌 카탈로그 서버를 제거합니다.

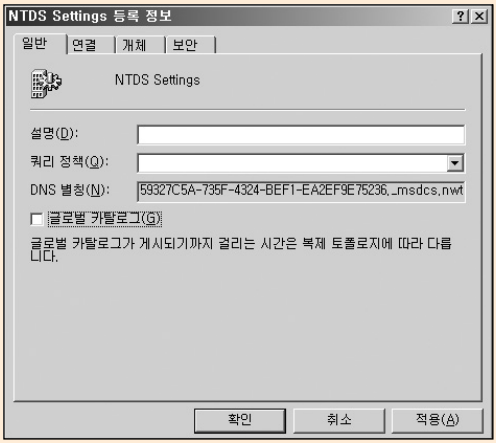

그림 30 글로벌 카탈로그 제거

6. 확인 버튼을 클릭한 후, Active Directory 사이트 및 서비스 관리 도구를 종료합니다.

작업 마스터 관리

포리스트에서 다른 도메인 컨트롤러가 수행하지 않는 특별한 역할을 수행하는 도메인 컨트롤러를 작업 마스터 또는 FSMO 역할 홀더라고 부릅니다. 포리스트에는 다음과 같은 두 종류의 포리스트 레벨 작업 마스터가 존재합니다. 이러한 역할은 포리스트에서 고유성을 유지해야 하며, 이는 전체 포리스트에 걸쳐 스키마 마스터 및 도메인 명명 마스터는 각각 하나씩만 존재할 수 있다는 뜻입니다.

- **스키마 마스터** : 스키마 마스터는 포리스트 전체에서 스키마에 대한 모든 업데이트와 변경 내용을 제어합니다. 포리스트의 스키마를 업데이트하려면 스키마 마스터에 액세스할 수 있어야 합니다. 전체 포리스트에 걸쳐 스키마 마스터 역할을 담당하는 도메인 컨트롤러는 하나만 존재할 수 있습니다.
- **도메인 명명 마스터** : 도메인 명명 마스터는 포리스트에 도메인을 추가하거나 제거하는 것을 제어합니다. 또한 응용 프로그램 파티션을 추가하거나 제거하는 역할도 담당합니다. 전체 포리스트에 걸쳐 도메인 명명 마스터 역할을 담당하는 도메인 컨트롤러는 하나만 존재할 수 있습니다.

포리스트 안에 각 도메인에는 다음과 같은 세 종류의 도메인 레벨 작업 마스터가 존재합니다. 이러한 역할은 각 도메인에서 고유성을 유지해야 하며, 이는 포리스트에 있는 각 도메인마다 RID 마스터, PDC 에뮬레이터 및 인프라 마스터를 각각 하나씩만 가질 수 있다는 뜻입니다.

- **RID 마스터** : RID 마스터는 일련의 RID를 같은 도메인에 있는 각 도메인 컨트롤러에 할당합니다, 각 도메인 컨트롤러에 할당된 RID는 도메인 컨트롤러가 사용자, 그룹 또는 컴퓨터 개체를 만들 때 개체의 고유 SID(보안 식별자)를 생성할 때 사용됩니다. 포리스트의 각 도메인에서 RID 마스터 역할을 담당하는 도메인 컨트롤러는 하나만 존재할 수 있습니다.
- **PDC 에뮬레이터** : 도메인에 Windows 2000 이전 운영 체제를 사용하는 클라이언트나 Windows NT BDC(백업 도메인 컨트롤러)가 있는 경우에 PDC 에뮬레이터가 Windows NT PDC(주 도메인 컨트롤러)로 동작합니다. PDC 에뮬레이터는 클라이언트의 암호 변경을 처리하고, 다른 도메인 컨트롤러의 시간 원본으로써 시간을 동기화하는 역할도 맡고 있습니다. 포리스트의 각 도메인에서 PDC 에뮬레이터 역할을 담당하는 도메인 컨트롤러는 하나만 존재할 수 있습니다.
- **인프라 마스터** : 인프라 마스터는 도메인 간에 참조되는 개체의 SID 특성 및 고유 이름 특성을 업데이트 하는 역할을 담당합니다. 인프라 마스터는 자신이 가지고 있는 데이터와 글로벌 카탈로그의 데이터를 비교합니다. 모든 도메인에 있는 개체의 업데이트는 복제를 통해 글로벌 카탈로그에 주기적으로 전달되기 때문에 글로벌 카탈로그 데이터는 언제나 최신 상태를 유지합니다. 따라서 인프라 마스터는 오래된 데이터를 발견하면 글로벌 카탈로그로부터 최신 데이터를 업데이트 한 후, 업데이트된 데이터를 도메인에 있는 다른 도메인 컨트롤러로 복제합니다. 포리스트의 각 도메인에서 인프라 마스터 역할을 담당하는 도메인 컨트롤러는 하나만 존재할 수 있습니다.

도메인 컨트롤러에 할당된 작업 마스터 역할은 Active Directory가 정상적으로 동작하기 위해 항상 고유성을 유지하며 동작해야 합니다. 포리스트 내에 새로운 도메인 및 사이트를 생성하는 경우에 작업 마스트 역할의 할당은 매우 중요합니다.

작업 마스터 역할 할당

작업 마스터 역할을 부적절하게 할당하였을 경우에, 사용자들은 암호 변경을 실패할 수 있고, 관리자는 도메인에 새로운 사용자나 그룹과 같은 개체를 생성하는데 실패할 수 있습니다. 또한 스키마를 업데이트 하는데 실패하거나, 사용자 계정 이름을 변경하였을 때 그룹 멤버쉽에서 여전히 변경전의 사용자 계정 이름이 출력될 수 있습니다. 포리스트 내에 새로운 도메인 및 사이트를 생성하는 경우에, 관리자는 다른 도메인 컨트롤러로 작업 마스터 역할을 전송하는 관리 작업이 필요할 수 있습니다. 포리스트 레벨 작업 마스터와 도메인 레벨 작업 마스터 역할은 포리스트와 도메인 안에 어떤 도메인 컨트롤러에도 할당할 수 있지만, 잘못된 작업 마스터 역할 할당은 Active Directory의 정상적인 동작을 방해하고, 관리적인 부하를 유발합니다.

Active Directory의 성능을 향상하고 관리적인 부하를 줄이기 위해 다음과 같이 작업 마스터 역할을 할당할 것을 권장합니다.

- 세 개의 도메인 레벨 작업 마스터는 같은 도메인 컨트롤러에 할당합니다.
- 글로벌 카탈로그 서버에 도메인 레벨 작업 마스터 역할을 할당하지 않습니다.
- 도메인 레벨 작업 마스터 역할은 고성능의 도메인 컨트롤러에 할당합니다.

[포리스트 루트 도메인에서 포리스트 레벨 역할 할당]

포리스트에서 첫 번째 도메인 컨트롤러에는 스키마 마스터와 도메인 명명 마스터 역할이 할당됩니다. 또한 포리스트의 첫 번째 도메인 컨트롤러는 글로벌 카탈로그 역할도 수행합니다. 관리 및 백업/복원을 용이하게 수행하기 위해 포리스트 레벨 작업 마스터 역할을 포리스트 루트 도메인의 첫 번째 도메인 컨트롤러에 그대로 유지 할 것을 권장합니다. 이 역할을 다른 도메인 컨트롤러로 전송하는 것은 큰 성능 향상을 기대할 수 없으며, 오히려 관리 및 백업/복원과 관련한 추가적인 관리 부하를 발생합니다. PDC 에뮬레이터와 달리

포리스트 레벨 작업 마스터 역할은 도메인 컨트롤러에 큰 부하를 주지 않기 때문에, 포리스트의 첫 번째 도메인 컨트롤러에 두 작업 마스터 역할을 그대로 유지합니다.

[같은 도메인 컨트롤러에 도메인 레벨 역할 할당]

새 도메인의 첫 번째 도메인 컨트롤러에 세 종류의 도메인 레벨 작업 마스터 역할이 할당됩니다. 포리스트 루트 도메인의 경우를 제외하면, 도메인의 첫 번째 도메인 컨트롤러에 할당 된 세 종류의 도메인 레벨 작업 마스터 역할을 그대로 유지할 것을 권장합니다.

Windows 2000 이전 클라이언트는 PDC 에뮬레이터로 업데이트를 전송하기 때문에, PDC 에뮬레이터는 많은 수의 RID가 필요합니다. 따라서 PDC 에뮬레이터와 RID 마스터 역할이 보다 효율적으로 상호 동작할 수 있도록, 두 역할은 같은 도메인 컨트롤러에 할당할 것을 권장합니다.

만약 도메인 레벨 역할을 여러 도메인 컨트롤러로 분산할 경우에는 백업과 복원이 더욱 복잡해집니다. 작업 마스터 역할을 담당하는 도메인 컨트롤러를 복원할 경우에는 추가적인 고려 사항들이 발생하기 때문에, 같은 도메인 컨트롤러에 모든 도메인 레벨 역할을 할당함으로써 복원 시에 필요한 관리 부하를 줄일 수 있습니다.

[고성능 도메인 컨트롤러에 도메인 레벨 역할 할당]

5 종류의 작업 마스터 중에서 PDC 에뮬레이터 역할을 담당하는 도메인 컨트롤러에 가장 많은 부하가 발생합니다. PDC 에뮬레이터는 매일 Active Directory를 구성하는 다른 시스템으로부터 전송되는 다양한 요구 사항을 처리해야 하기 때문에, 가용성 및 빠른 응답성을 제공하기 위해 PDC 에뮬레이터 역할은 고성능의 도메인 컨트롤러에 할당할 것을 권장합니다.

Windows 2000 이전의 운영 체제를 사용하는 클라이언트와 Windows NT

4.0 도메인 컨트롤러가 네트워크에 존재할 경우에는 Windows 2000 이상의 운영 체제를 사용하는 클라이언트와 Windows 2000 Server 이상의 운영 체제를 사용하는 도메인 컨트롤러로 구성된 Active Directory 환경에 비해 더 많은 부하를 PDC 에뮬레이터에 가하게 됩니다. 이런 환경하에서 동작하는 PDC 에뮬레이터의 경우에는 부하를 분산하는 작업이 필요할 수 있습니다.
만약 작업 마스터로 동작하는 도메인 컨트롤러가 과부하로 인해 성능이 하락한다면, 관리자는 덜 사용되는 도메인 컨트롤러로 부하를 분산하도록 Active Directory 환경을 재구성할 수 있습니다.
DNS에 등록되는 도메인 컨트롤러의 가중치를 조절함으로써, 과부하로 성능이 저하되는 작업 마스터에게 다른 도메인 컨트롤러보다 적은 사용자의 패킷이 전송되도록 구성할 수 있습니다.

작업 마스터 오류

일부 작업 마스터 역할은 정상적인 Active Directory 운영에 반드시 필요합니다. 일반적으로 작업 마스터 역할을 담당하는 도메인 컨트롤러에 오류가 발생하면 사용자나 관리자는 바로 오류 사실을 인지 할 수 없습니다. 특정 작업 마스터가 담당하는 기능을 사용하려 했을 때 오류가 발생함으로써, 관리자나 사용자는 작업 마스터 역할을 담당하는 도메인 컨트롤러가 사용 불가능한 상태라는 것을 인지 하게 됩니다.
시스템 고장이나 네트워크 문제로 인해 작업 마스터를 사용할 수 없는 경우, 관리자는 먼저 시스템 또는 네트워크 고장의 원인 및 예상 지속 기간을 파악해야 합니다. 곧 해결될 네트워킹 문제나 시스템 고장이 원인인 경우에는 작업 마스터를 다시 사용할 수 있을 때까지 기다립니다.
만약 고장 난 현재의 작업 마스터를 절대 다시 사용할 수 없는 경우에는 작업 마스터의 역할을 다른 도메인 컨트롤러가 점유(Role Seize)할 수 있습니다. 역할을 다른 도메인 컨트롤러가 점유할 것인지에 대한 결정은 역할의 종류 및

역할을 수행중인 도메인 컨트롤러의 사용 불능 기간에 따라 달라집니다.
네트워킹 문제나 시스템 고장이 해결되어 다시 작업 마스터가 동작을 시작하였어도 동일한 문제가 자주 반복되거나, 부하를 분산하는 차원에서 관리자는 작업 마스터 역할을 다른 도메인 컨트롤러로 전송(Role Transfer)할 수 있습니다.
각 작업 마스터에 오류가 발생했을 때 미치는 영향은 다음과 같습니다.

[스키마 마스터 오류]

스키마 마스터 역할을 담당하는 도메인 컨트롤러에 오류가 발생해 기능이 정지되어도 사용자는 스키마 마스터를 사용할 수 없다는 것을 알 수 없습니다. 스키마를 수정하거나 설치 과정에서 스키마를 수정하는 응용 프로그램을 설치하려고 하지 않는 한 관리자도 이를 알 수 없습니다.
따라서 긴급히 스키마를 업데이트하는 작업을 수행할 일이 없다면, 장기간 스키마 마스터 역할을 담당하는 도메인 컨트롤러가 정지되어 있어도 Active Directory 운영 환경에 큰 영향을 미치지는 않습니다.
하지만 너무 오랫동안 스키마 마스터를 사용할 수 없는 경우, 관리자는 스키마 마스터 역할을 다른 도메인 컨트롤러가 점유할 것인지를 고려해야 합니다. 일단 역할이 다른 도메인 컨트롤러에 점유된 후에는 기존 스키마 마스터 역할이 중단된 도메인 컨트롤러를 절대로 다시 네트워크에 연결하면 안 됩니다.

[도메인 명명 마스터 오류]

도메인 명명 마스터 역할을 담당하는 도메인 컨트롤러에 오류가 발생해 기능이 정지되어도 사용자는 도메인 명명 마스터를 사용할 수 없다는 것을 알 수 없습니다. 포리스트에 도메인을 추가하거나 제거하려고 시도하지 않는 한 관리자도 이를 알 수 없습니다.
따라서 도메인을 추가하거나 제거하는 작업을 수행할 일이 없다면, 장기간 도메인 명명 마스터 역할을 담당하는 도메인 컨트롤러가 정지되어 있어도

Active Directory 운영 환경에 큰 영향을 미치지는 않습니다.
하지만 너무 오랫동안 도메인 명명 마스터를 사용할 수 없는 경우, 관리자는 도메인 명명 마스터 역할을 다른 도메인 컨트롤러가 점유할 것인지를 고려해야 합니다. 일단 역할이 다른 도메인 컨트롤러에 점유된 후에는 기존 도메인 명명 마스터 역할이 중단된 도메인 컨트롤러를 절대로 다시 네트워크에 연결하면 안 됩니다.

[RID 마스터 오류]

RID 마스터 역할을 담당하는 도메인 컨트롤러에 오류가 발생해 기능이 정지되어도 사용자는 RID 마스터를 사용할 수 없다는 것을 알 수 없습니다. 대량의 개체를 생성할 때 도메인 컨트롤러에 할당된 RID를 모두 사용하여 더 이상 개체를 생성할 수 없는 경우에만, 관리자는 RID 마스터를 사용할 수 없다는 것을 인지 할 수 있습니다.따라서 도메인에 대량의 개체를 생성하는 작업을 수행할 일이 없다면, 장기간 RID 마스터 역할을 담당하는 도메인 컨트롤러가 정지되어 있어도 Active Directory 운영 환경에 큰 영향을 미치지는 않습니다.
하지만 너무 오랫동안 RID 마스터를 사용할 수 없는 경우, 관리자는 RID 마스터 역할을 다른 도메인 컨트롤러가 점유할 것인지를 고려해야 합니다. 일단 역할이 다른 도메인 컨트롤러에 점유된 후에는 기존 RID 마스터 역할이 중단된 도메인 컨트롤러를 절대로 다시 네트워크에 연결하면 안 됩니다.

[PDC 에뮬레이터 오류]

PDC(주 도메인 컨트롤러) 에뮬레이터 역할을 담당하는 도메인 컨트롤러에 오류가 발생해 기능이 정지되면 사용자들은 직접적인 영향을 받습니다. 따라서 PDC 에뮬레이터를 장시간 사용할 수 없는 경우에 즉시 역할을 다른 도메인 컨트롤러가 점유해야 할 수도 있습니다.

[인프라 마스터 오류]
인프라 마스터 역할을 담당하는 도메인 컨트롤러에 오류가 발생해 기능이 정지되어도 사용자는 인프라 마스터를 사용할 수 없다는 것을 알 수 없습니다. 최근에 대량의 계정을 이동하거나 이름을 변경하지 않은 한, 관리자도 이를 알 수 없습니다.
따라서 도메인에 대량의 계정을 이동하거나 이름을 변경하는 작업을 수행할 일이 없다면, 장기간 인프라 마스터 역할을 담당하는 도메인 컨트롤러가 정지되어 있어도 Active Directory 운영 환경에 큰 영향을 미치지는 않습니다.
하지만 너무 오랫동안 인프라 마스터를 사용할 수 없는 경우, 관리자는 RID 마스터 역할을 다른 도메인 컨트롤러가 점유할 것인지를 고려해야 합니다.

작업 마스터 역할 전송(Role Transfer)과 점유(Role Seize)
작업 마스터 역할 전송은 작업 마스터 역할을 하나의 도메인 컨트롤러에서 다른 도메인 컨트롤러로 이동하는 적합한 방법입니다. 역할 전송이 된 후에는 이전 작업 마스터는 더 이상 작업 마스터 역할을 수행하지 않습니다. 반면에 역할을 전송 받은 도메인 컨트롤러는 작업 마스터로써 역할을 수행합니다. 이는 네트워크에 같은 작업 마스터 역할을 담당하는 도메인 컨트롤러에 의해 Active Directory가 비정상적으로 동작할 수 있는 가능성을 제거합니다.
따라서 역할 전송은 현재 작업 마스터 역할을 담당하는 도메인 컨트롤러와 역할을 전송 받을 도메인 컨트롤러가 모두 정상적으로 동작하고 네트워크 액세스가 가능할 때 사용합니다.
반면에 역할 점유는 장시간 고장 난 현재의 작업 마스터를 절대 다시 사용할 수 없어, 역할전송이 불가능한 경우에 사용합니다.
작업 마스터 역할 전송이나 점유를 하기 위해서 관리자는 다음 그룹의 구성원이어야 합니다.

작업 마스터	그룹
스키마 마스터	Enterprise Admins
도메인 명명 마스터	Enterprise Admins
RID 마스터	Domain Admins
PDC 에뮬레이터	Domain Admins
인프라 마스터	Domain Admins

표 10 역할 전송 및 점유에 필요한 그룹 구성원

작업 마스터 역할 전송하기

새로운 포리스트를 생성할 때, Active Directory 설치 마법사는 포리스트 루트 도메인의 첫 번째 도메인 컨트롤러에 두 포리스트 레벨 작업 마스터 역할을 할당합니다. 또한 새로운 도메인을 생성할 때, Active Directory 설치 마법사는 도메인의 첫 번째 도메인 컨트롤러에 세 도메인 레벨 작업 마스터 역할을 할당합니다. 이렇게 자동으로 할당된 작업 마스터 역할은 성능 최적화 및 관리 차원에서 다른 도메인 컨트롤러로 전송할 수 있습니다.

스키마 마스터 역할 전송하기

스키마 마스터는 포리스트 레벨 작업 마스터로, 포리스트 전체에서 오직 하나의 도메인 컨트롤러만이 역할을 수행합니다. 스키마 마스터 역할을 전송하기 위해서 Active Directory 스키마 스냅인이나 Ntdsutil.exe를 사용합니다. Active Directory 스키마 스냅인이 시스템에 등록되어 있지 않다면 등록 작업을 먼저 수행해야 합니다.

[따라하기]

스키마 마스터 역할 전송하기

예제에서는 스키마 마스터 역할을 DC01.nwtraders.msft에서 DC02.nwtraders.msft 도메인 컨트롤러로 전송합니다. Active Directory 스키마 스냅인을 이용해서 스키마 마스터 역할을 전송하는 과정은 다음과 같습니다.

1. 시작 → 실행 메뉴를 선택한 후, Active Directory 스키마 스냅인을 등록하기 위해 다음 명령을 실행합니다.
   Regsvr32 schmmgmt.dll
   이미 Active Directory 스키마 스냅인을 시스템에 등록하였다면 이 과정은 생략합니다.
2. 시작 → 실행 메뉴를 선택한 후, 다음 명령을 실행합니다.
   mmc
3. 파일 → 스냅인 추가/제거 메뉴를 선택합니다.
4. 스냅인 추가/제거 대화 상자가 나타나면, 추가 버튼을 클릭합니다.
5. 실행 가능한 독립 실행형 스냅인 목록에서 Active Directory 스키마 스냅인을 선택한 후, 추가 버튼을 클릭합니다.
6. 닫기 버튼을 클릭한 후, 확인 버튼을 클릭하여 스냅인 추가/제거 대화 상자를 종료합니다.
7. 콘솔 루트 아래에 Active Directory 스키마를 마우스 오른쪽 버튼으로 클릭한 후, 도메인 컨트롤러 변경 메뉴를 선택합니다.
8. 도메인 컨트롤러 변경 대화 상자에서 이름 지정 옵션을 클릭합니다. 〈그림 31〉와 같이 새로 스키마 마스터 역할을 전송 받을 도메인 컨트롤러의 이름을 입력한 후, 확인 버튼을 클릭합니다.

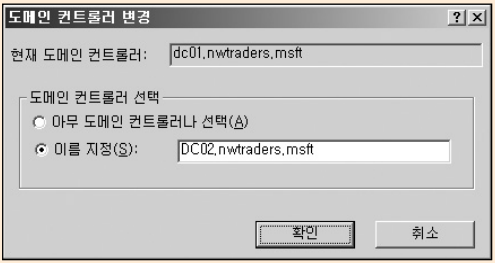

그림 31 도메인 컨트롤러 변경

9. 콘솔 루트 아래에 Active Directory 스키마를 마우스 오른쪽 버튼으로 클릭한 후, 작업 마스터 메뉴를 선택합니다.
10. 스키마 마스터 변경 대화 상자에 현재 스키마 마스터 역할을 수행하는 도메인 컨트롤러와 역할을 전송 받을 도메인 컨트롤러 이름을 확인한 후, 변경 버튼을 클릭합니다.

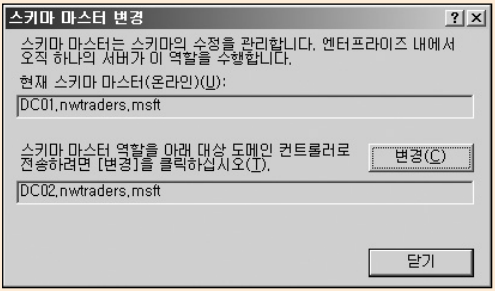

그림 32 스키마 마스터 변경

11. 작업 마스터 변경을 확인하는 대화 상자가 나타납니다. 예 버튼을 클릭하여 스키마 마스터 역할을 전송합니다.
12. 작업 마스터 전송이 성공했음을 알리는 대화 상자가 나타납니다. 확인 버튼을 클릭합니다.
13. 닫기 버튼을 클릭하여 스키마 마스터 변경 대화 상자를 종료한 후, MMC를 종료합니다.

[따라하기]

Ntdsutil.exe를 이용해서 스키마 마스터 역할 전송하기

Ntdsutil.exe를 이용해서 스키마 마스터 역할을 전송하는 과정은 다음과 같습니다.

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행해서 Ntdsutil.exe를 실행합니다.
   ntdsutil
3. ntdsutil: 프롬프트에서 roles를 입력하고, Enter 키를 누릅니다.
4. fsmo maintenance: 프롬프트에서 connections를 입력하고, Enter 키를 누릅니다.
5. server connections: 프롬프트에서 다음 명령을 실행합니다.
   connect to server *servername*
   *servername*에 새로 스키마 마스터 역할을 전송 받을 도메인 컨트롤러의 이름을 입력합니다.
6. server connections: 프롬프트에서 quit를 실행합니다.
7. 스키마 마스터 역할을 5 단계에서 연결한 도메인 컨트롤러로 전송하기 위해 fsmo maintenance: 프롬프트에서 다음 명령을 실행합니다.
   transfer schema master

8. 역할 전송을 확인하기 위해 역할 전송 확인 대화 상자가 나타납니다. 예 버튼을 클릭합니다.
9. 스키마 마스터 역할 전송이 완료되면, 〈그림 33〉과 같이 현재 각 작업 마스터 역할을 담당하고 있는 도메인 컨트롤러의 정보를 출력합니다.

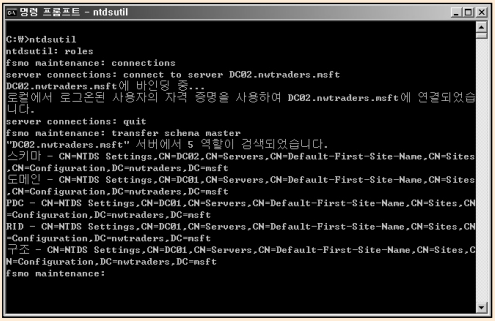

그림 33 스키마 마스터 전송

10. fsmo maintenance: 프롬프트에서 quit를 실행합니다.
11. ntdsutil.exe를 종료하기 위해서 ntdsutil: 프롬프트에서 quit를 실행합니다.

도메인 명명 마스터 역할 전송하기

도메인 명명 마스터는 포리스트 레벨 작업 마스터로, 포리스트 전체에서 오직 하나의 도메인 컨트롤러만이 역할을 수행합니다. 도메인 명명 마스터 역할을 전송하기 위해서 Active Directory 도메인 및 트러스트 관리 도구나 Ntdsutil.exe를 사용합니다.

[따라하기]

도메인 명명 마스터 역할 전송하기

예제에서는 도메인 명명 마스터 역할을 DC01.nwtraders.msft에서 DC02.nwtraders.msft 도메인 컨트롤러로 전송합니다. Active Directory 도메인 및 트러스트 관리 도구를 이용해서 도메인 명명 마스터 역할을 전송하는 과정은 다음과 같습니다.

1. 시작 → 관리 도구 → Active Directory 도메인 및 트러스트 메뉴를 선택하여, Active Directory 도메인 및 트러스트 관리 도구를 실행합니다.
2. 콘솔 트리에 Active Directory 도메인 및 트러스트를 마우스 오른쪽 버튼으로 클릭한 후, 도메인 컨트롤러에 연결 메뉴를 선택합니다.
3. 도메인 컨트롤러에 연결 대화 상자의 사용할 수 있는 도메인 컨트롤러 선택 목록에서 새로 도메인 명명 마스터 역할을 전송 받을 도메인 컨트롤러의 이름을 선택 한 후, 확인 버튼을 클릭합니다.

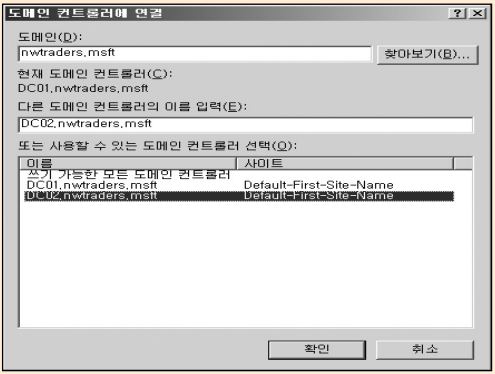

그림 34 도메인 컨트롤러에 연결

4. 콘솔 트리에 Active Directory 도메인 및 트러스트를 마우스 오른쪽 버튼으로 클릭한 후, 작업 마스터 메뉴를 선택합니다.
5. 작업 마스터 변경 대화 상자에 현재 도메인 명명 마스터 역할을 수행하는 도메인 컨트롤러와 역할을 전송 받을 도메인 컨트롤러 이름을 확인한 후, 변경 버튼을 클릭합니다.

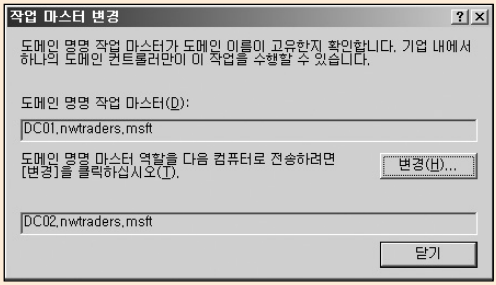

그림 35 도메인 명명 마스터 변경

6. 작업 마스터 변경을 확인하는 대화 상자가 나타납니다. 예 버튼을 클릭하여 도메인 명명 마스터 역할을 전송합니다.
7. 작업 마스터 전송이 성공했음을 알리는 대화 상자가 나타납니다. 확인 버튼을 클릭합니다.
8. 닫기 버튼을 클릭하여 작업 마스터 변경 대화 상자를 종료한 후, Active Directory 도메인 및 트러스트 관리 도구를 종료합니다.

[따라하기]

Ntdsutil.exe를 이용해서 도메인 명명 마스터 역할 전송하기

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행해서 Ntdsutil.exe를 실행합니다.
   ntdsutil
3. ntdsutil: 프롬프트에서 roles를 입력하고, Enter 키를 누릅니다.
4. fsmo maintenance: 프롬프트에서 connections를 입력하고, Enter 키를 누릅니다.
5. server connections: 프롬프트에서 다음 명령을 실행합니다.
   connect to server *servername*
   *servername*에 새로 도메인 명명 마스터 역할을 전송 받을 도메인 컨트롤러의 이름을 입력합니다.
6. server connections: 프롬프트에서 quit를 실행합니다.
7. 도메인 명명 마스터 역할을 5 단계에서 연결한 도메인 컨트롤러로 전송하기 위해 fsmo maintenance: 프롬프트에서 다음 명령을 실행합니다.
   transfer domain naming master
8. 역할 전송을 확인하기 위해 역할 전송 확인 대화 상자가 나타납니다. 예 버튼을 클릭합니다.
9. 도메인 명명 마스터 역할 전송이 완료되면, 〈그림 36〉과 같이 현재 각 작업 마스터 역할을 담당하고 있는 도메인 컨트롤러의 정보를 출력합니다.

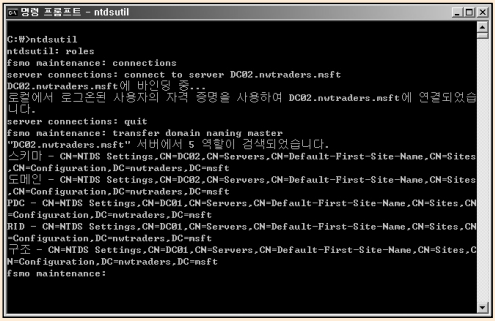

그림 36 도메인 명명 마스터 전송

10. fsmo maintenance: 프롬프트에서 quit를 실행합니다.
11. ntdsutil.exe를 종료하기 위해서 ntdsutil: 프롬프트에서 quit를 실행합니다.

도메인 레벨 작업 마스터 역할 전송하기

도메인 레벨 작업 마스터(RID 마스터, PDC 에뮬레이터, 인프라 마스터) 역할을 전송하기 위해서 Active Directory 사용자 및 컴퓨터 관리 도구나 Ntdsutil.exe를 사용합니다.

[따라하기]

도메인 레벨 작업 마스터 역할 전송하기

예제에서는 도메인 레벨 작업 마스터 역할을 DC01.nwtraders.msft에서 DC02.nwtraders.msft 도메인 컨트롤러로 전송합니다. Active Directory 사용자 및 컴퓨터 관리 도구를 이용해서 도메인 레벨 작업 마스터 역할을 전송하

는 과정은 다음과 같습니다.

1. 시작 → 관리 도구 → Active Directory 사용자 및 컴퓨터 메뉴를 선택하여, Active Directory 사용자 및 컴퓨터 관리 도구를 실행합니다.
2. 콘솔 트리에 Active Directory 사용자 및 컴퓨터를 마우스 오른쪽 버튼으로 클릭한 후, 도메인 컨트롤러에 연결 메뉴를 선택합니다.
3. 도메인 컨트롤러에 연결 대화 상자의 사용할 수 있는 도메인 컨트롤러 선택 목록에서 새로 도메인 레벨 작업 마스터 역할을 전송 받을 도메인 컨트롤러의 이름을 선택 한 후, 확인 버튼을 클릭합니다.

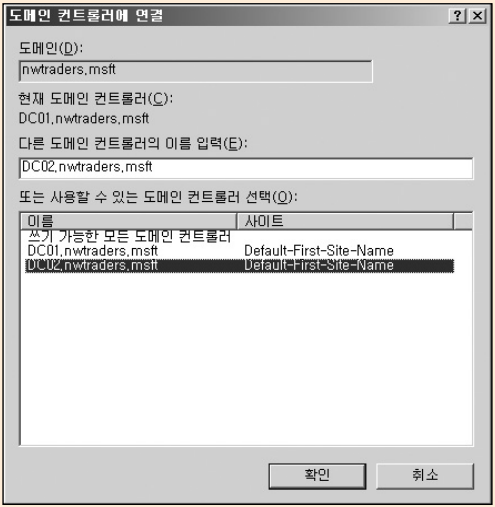

그림 37 도메인 컨트롤러에 연결

4. 콘솔 루트에 Active Directory 도메인 및 트러스트를 마우스 오른쪽 버튼으로 클릭한 후, 모든 작업 → 작업 마스터 메뉴를 선택합니다.
5. 작업 마스터 대화 상자에 나타납니다. 전송하고자 하는 도메인 명명 마스터 역할에 해당하는 탭(RID, PDC, 인프라)을 클릭합니다.
6. 현재 도메인 레벨 작업 마스터 역할을 수행하는 도메인 컨트롤러와 역할을 전송 받을 도메인 컨트롤러 이름을 확인한 후, 변경 버튼을 클릭합니다.

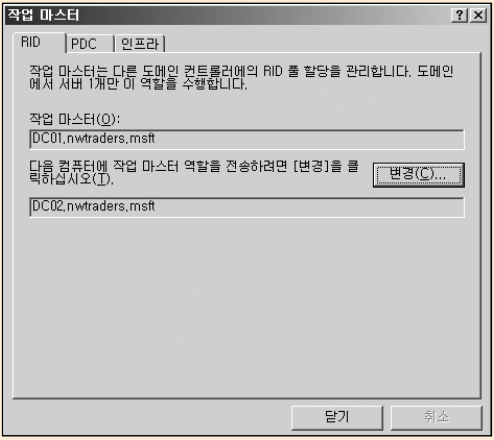

그림 38 도메인 레벨 작업 마스터 변경

7. 작업 마스터 변경을 확인하는 대화 상자가 나타납니다. 예 버튼을 클릭하여 도메인 레벨 작업 마스터 역할을 전송합니다.
8. 작업 마스터 전송이 성공했음을 알리는 대화 상자가 나타납니다. 확인 버튼을 클릭합니다.
9. 닫기 버튼을 클릭하여 작업 마스터 대화 상자를 종료한 후, Active Directory 사용자 및 컴퓨터 관리 도구를 종료합니다.

[따라하기]

Ntdsutil.exe를 이용해서 도메인 레벨 작업 마스터 역할 전송하기

Ntdsutil.exe를 이용해서 도메인 레벨 작업 마스터 역할을 전송하는 과정은 다음과 같습니다.

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행해서 Ntdsutil.exe를 실행합니다.

   ntdsutil
3. ntdsutil: 프롬프트에서 roles를 입력하고, Enter 키를 누릅니다.
4. fsmo maintenance: 프롬프트에서 connections를 입력하고, Enter 키를 누릅니다.
5. server connections: 프롬프트에서 다음 명령을 실행합니다.

   connect to server *servername*

   *servername*에 새로 도메인 레벨 작업 마스터 역할을 전송 받을 도메인 컨트롤러의 이름을 입력합니다.
6. server connections: 프롬프트에서 quit를 실행합니다.
7. 도메인 레벨 작업 마스터 역할 중에 RID 마스터 역할을 5 단계에서 연결한 도메인 컨트롤러로 전송하려면, fsmo maintenance: 프롬프트에서 다음 명령을 실행합니다.

   transfer RID master

   도메인 레벨 작업 마스터 역할 중에 PDC 에뮬레이터 역할을 5 단계에서 연결한 도메인 컨트롤러로 전송하려면, fsmo maintenance: 프롬프트에서 다음 명령을 실행합니다.

   transfer PDC

   도메인 레벨 작업 마스터 역할 중에 인프라 마스터 역할을 5 단계에서 연결한 도메인 컨트롤러로 전송하려면, fsmo maintenance: 프롬프트에서 다음

명령을 실행합니다.
transfer infrastructure master
8. 역할 전송을 확인하기 위해 역할 전송 확인 대화 상자가 나타납니다. 예 버튼을 클릭합니다.
9. 도메인 명명 마스터 역할 전송이 완료되면, 현재 각 작업 마스터 역할을 담당하고 있는 도메인 컨트롤러의 정보를 출력합니다.
10. fsmo maintenance: 프롬프트에서 quit를 실행합니다.
11. ntdsutil.exe를 종료하기 위해서 ntdsutil: 프롬프트에서 quit를 실행합니다.

작업 마스터 역할 점유하기

역할 점유(Role Seize)는 현재 작업 마스터 역할을 담당하는 도메인 컨트롤러에서 역할을 제거하지 않고 다른 도메인 컨트롤러에 역할을 할당합니다. 역할 점유는 기존의 작업 마스터가 하드웨어 오류에 의해 더 이상 정상적인 동작이 불가능한 상황에서 사용합니다.

역할 점유는 Active Directory에 두 가지 문제를 유발할 수 있습니다. 첫 번째, 기존의 작업 마스터가 동작하지 않은 상태에서 다른 도메인 컨트롤러에 강제로 작업 마스터 역할을 할당하여 동작하기 때문에, 기존의 작업 마스터에서 변경된 데이터를 미처 복제 받지 못했을 수 있습니다. 이는 데이터 유실이나 Active Directory 데이터베이스의 무결성을 손상시킬 수 있습니다.

두 번째, 기존의 작업 마스터는 자신이 정지해 있을 때 다른 도메인 컨트롤러가 역할을 점유했기 때문에, 자신이 더 이상 작업 마스터로 동작하면 안 된다는 것을 알지 못합니다. 기존의 작업 마스터가 하드웨어 오류로 더 이상 사용할 수 없다면 상관 없지만, 하드웨어 복구나 백업을 통해 복원이 되어 다시 정상적으로 부팅되면 다시 이전의 작업 마스터 역할을 수행합니다.
이런 상황에서는 서로 다른 도메인 컨트롤러가 같은 작업 마스터 역할을 수행하기 때문에 Active Directory 운영 환경에 치명적인 오류를 유발할 수 있습니다. 따라서 역할을 점유한 후에는 기존 작업 마스터 역할을 담당하던 도메인 컨트롤러는 절대로 다시 네트워크에 연결하면 안 됩니다.

작업 마스터 역할을 점유하기 위해서는 Ntdsutil.exe를 사용해야 합니다. Ntdsutil.exe를 이용해서 작업 마스터 역할을 점유할 때, Ntdsutil.exe는 먼저 작업 마스터 역할 전송을 시도합니다. 만약 현재 작업 마스터와 통신이 불가능하면, Ntdsutil.exe는 작업 마스터 역할 점유를 수행합니다.

Ntdsutil.exe를 이용해서 작업 마스터 역할을 점유하는 과정은 모든 작업 마스터에 대해 동일합니다.

[따라하기]

작업 마스터 역할 점유하기

Ntdsutil.exe를 이용해서 작업 마스터 역할을 점유하는 과정은 다음과 같습니다.

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행해서 Ntdsutil.exe를 실행합니다.
   ntdsutil
3. ntdsutil: 프롬프트에서 roles를 입력하고, Enter 키를 누릅니다.

4. fsmo maintenance: 프롬프트에서 connections를 입력하고, Enter 키를 누릅니다.
5. server connections: 프롬프트에서 다음 명령을 실행합니다.
   connect to server *servername*
   *servername*에 작업 마스터 역할을 점유할 도메인 컨트롤러의 이름을 입력합니다.
6. server connections: 프롬프트에서 quit를 실행합니다.
7. 포리스트 레벨 작업 마스터 역할 중에 스키마 마스터 역할을 5 단계에서 연결한 도메인 컨트롤러에 점유하려면, fsmo maintenance: 프롬프트에서 다음 명령을 실행합니다.
   seize schema master
   포리스트 레벨 작업 마스터 역할 중에 도메인 명명 마스터 역할을 5 단계에서 연결한 도메인 컨트롤러에 점유하려면, fsmo maintenance: 프롬프트에서 다음 명령을 실행합니다.
   seize domain naming master
   도메인 레벨 작업 마스터 역할 중에 RID 마스터 역할을 5 단계에서 연결한 도메인 컨트롤러에 점유하려면, fsmo maintenance: 프롬프트에서 다음 명령을 실행합니다.
   seize RID master
   도메인 레벨 작업 마스터 역할 중에 PDC 에뮬레이터 역할을 5 단계에서 연결한 도메인 컨트롤러에 점유하려면, fsmo maintenance: 프롬프트에서 다음 명령을 실행합니다.
   seize PDC
   도메인 레벨 작업 마스터 역할 중에 인프라 마스터 역할을 5 단계에서 연결

한 도메인 컨트롤러에 점유하려면, fsmo maintenance: 프롬프트에서 다음 명령을 실행합니다.

seize infrastructure master

8. 역할 점유를 확인하기 위해 역할 점유 확인 대화 상자가 나타납니다. 예 버튼을 클릭합니다.
9. 작업 마스터 역할 점유가 완료되면, 현재 각 작업 마스터 역할을 담당하고 있는 도메인 컨트롤러의 정보를 출력합니다.

〈그림 39〉는 DC01.nwtraders.msft 도메인 컨트롤러가 스키마 마스터 역할을 점유한 예제입니다. 먼저 역할 전송을 시도하고, 기존 스키마 마스터와 통신에 실패하자 점유를 수행하는 것을 확인 할 수 있습니다.

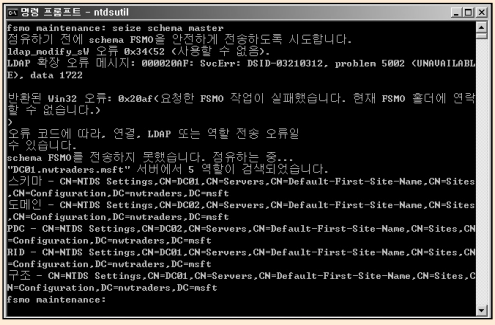

그림 39 작업 마스터 점유하기

10.fsmo maintenance: 프롬프트에서 quit를 실행합니다.

11.ntdsutil.exe를 종료하기 위해서 ntdsutil: 프롬프트에서 quit를 실행합니다.

Active Directory 데이터베이스 관리

Active Directory는 NTDS.dit 데이터베이스 파일에 저장됩니다. 데이터베이스 파일과 함께 트랜잭션을 저장하는 로그 파일도 사용합니다. 성능 향상을 위해 데이터베이스 파일과 트랜잭션 로그 파일은 서로 다른 하드 디스크에 저장할 것을 권장합니다. 평상시 운영 환경하에서 주기적인 백업을 수행하는 것 이외에는 Active Directory 데이터베이스를 관리하기 위해 매일 정기적으로 수행해야 할 관리 작업을 없습니다. 하지만 다음과 같은 상황이 발생하면 적절한 관리 작업을 수행해야 합니다.

- 저장 공간 부족
- 하드 디스크 오류
- 대량의 개체 삭제나 글로벌 카탈로그 서버 기능 제거 후에 사용하지 않는 공간 반납의 필요성

관리자는 Active Directory 데이터베이스 파일과 로그 파일을 저장하는 파티션의 남은 저장 공간을 주기적으로 모니터링 해야 합니다. Active Directory 데이터베이스 파일과 로그 파일을 저장하는 파티션의 사용 가능한 저장 공간 크기에 대한 권장 사항은 다음과 같습니다.

- NTDS.dit를 저장하는 파티션 : 현재 NTDS.dit 파일 크기의 20% 이상 또는 500 MB
- 로그 파일을 저장하는 파티션 : 현재 로그 파일 크기의 20% 이상 또는 500 MB

- NTDS.dit와 로그 파일을 모두 저장하는 파티션 : 현재 NTDS.dit 파일과 로그 파일 합의 20% 이상 또는 1 GB

대규모 퇴사나 조직 통폐합과 같은 인사 명령이 발생하면, Identity 관리 차원에서 Active Directory에 관련 개체들이 삭제됩니다. 개체들이 삭제될 때, Active Directory 데이터베이스 파일에는 빈 공간들이 생깁니다. 정기적인 온라인 조각 모음은 개체 삭제에 의해 생긴 빈 공간들을 모아서 하나의 큰 빈 공간으로 만듭니다. 향후 새로운 개체가 Active Directory에 생성될 때, Active Directory 데이터베이스 파일의 크기를 늘리지 않고 온라인 조작 모음에 의해 생성된 빈 공간을 저장 공간으로 할당됩니다.

정기적인 온라인 조각 모음은 개체 삭제에 의해 Active Directory 데이터베이스 파일 내에 생성된 빈 공간들을 모아 하나의 큰 빈 공간을 생성하지만, 생성한 빈 공간을 Windows 파일 시스템에 반납하지는 않습니다. 따라서 대량의 개체 삭제나 글로벌 카탈로그 서버 기능 제거와 같은 관리 작업을 수행해도 Active Directory 데이터베이스 파일 크기는 줄어들지 않습니다.

비록 이런 환경이 Active Directory 운영에 큰 영향을 미치지는 않지만, Active Directory 데이터베이스 안에 사용하지 않는 큰 빈 공간이 계속 남게 됩니다. Active Directory 데이터베이스가 사용하지 않는 빈 공간을 Windows 파일 시스템에 반납하기 위해서는 오프라인 조각 모음을 수행합니다.
그 외에 관리자는 관리 작업으로는 데이터베이스 파일이나 로그 파일을 저장하는 하드 디스크를 교체하거나 다른 하드 디스크로 이동하는 Active Directory 데이터베이스 관리 작업을 수행할 수 있습니다.
Active Directory 데이터베이스 관리 작업을 수행하기 전에, 관리자는 반드시 시스템 상태 백업을 수행해야 합니다. 그 후 도메인 컨트롤러를 디렉터리 서

비스 복원 모드로 부팅한 후, Ntdsutil.exe를 이용해서 관리 작업을 수행합니다. Active Directory 데이터베이스 관리 작업을 수행한 후에는 데이터베이스 무결성 점검을 수행할 것을 권장합니다. 데이터베이스 무결성 점검은 Ntdsutil.exe의 integrity 명령을 이용해서, Active Directory 데이터베이스 파일의 모든 바이트를 읽어 바이너리 레벨의 데이터베이스 손상 여부를 점검합니다. 또한 데이터베이스 헤더의 정상 유무와 모든 테이블의 무결성을 점검합니다.

따라서 데이터베이스 무결성 점검은 Active Directory 데이터베이스 파일의 크기와 도메인 컨트롤러의 성능에 따라 많은 시간이 소요될 수 있습니다. 테스트 환경하에서 2 GB당 한 시간의 시간이 소요되었습니다.

Active Directory 데이터베이스 파일 이동하기

다음과 같은 경우에 Active Directory 데이터베이스 파일을 이동합니다.

- **하드 디스크 관리** : 만약 Active Directory 데이터베이스 파일이나 로그 파일을 저장하고 있는 하드 디스크를 교체하는 작업을 수행해야 한다면, 데이터베이스 파일을 임시로 또는 완전히 다른 하드 디스크로 이동합니다.
- **저장 공간 부족** : Active Directory 데이터베이스 파일이나 로그 파일을 저장하는 하드 디스크의 저장 공간이 부족할 경우에는, 먼저 Active Directory와 관련 없는 다른 파일이 많은 공간을 사용하고 있는지를 점검합니다. 만일 Active Directory 데이터베이스 파일이나 로그 파일이 많은 공간을 사용하기 때문이라면, 관리자는 다음과 같은 두 가지 관리 작업 중에 하나를 선택하여 수행합니다.
  - 현재 Active Directory 데이터베이스 파일이나 로그 파일을 저장하고 있는 파티션의 크기를 확장합니다. 이 방법은 파일의 경로가 변하지 않기

때문에 Ntdsutil.exe를 이용한 추가적인 관리 작업을 수행할 필요가 없습니다.

- Ntdsutil.exe를 이용해서 Active Directory 데이터베이스 파일이나 로그 파일을 저장 공간이 충분한 다른 파티션으로 이동합니다.

Active Directory 데이터베이스 파일이나 로그 파일을 이동하기 위해서는 반드시 Ntdsutil.exe를 이용해서 변경된 경로가 레지스트리에 수정되도록 합니다. 이동이 완료된 후에는 향후 복원이 필요한 경우를 대비해, 이동한 경로로 Active Directory 데이터베이스 파일이나 로그 파일이 복원되도록 다시 한번 시스템 상태 백업을 수행합니다. 또한 이동한 Active Directory 데이터베이스 파일이나 로그 파일의 NTFS 권한이 적절히 설정되어 있는지도 점검합니다. Active Directory 데이터베이스 파일을 이동하면 Ntdsutil.exe는 HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters 서브키에 다음 값들을 수정합니다.

- Database backup path
- Digital Signature Algorithm (DSA) database file
- DSA working directory

로그 파일을 이동하면 Ntdsutil.exe는 HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters 서브키에 다음 값들을 수정합니다.

- Database log files path

Active Directory 데이터베이스 파일 이동은 다음과 같은 순서로 진행합니다.

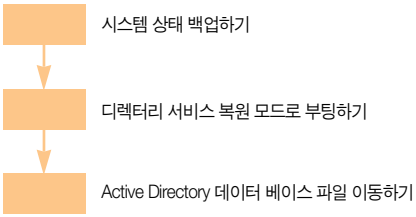

그림 40 Active Directory 데이터베이스 파일 이동 프로세스

시스템 상태 백업하기

Active Directory 데이터베이스 관리 작업을 수행하기 전에, 관리자는 반드시 시스템 상태 백업을 수행해야 합니다. 시스템 상태 백업은 Active Directory 데이터베이스 파일이나 로그 파일을 이동하는 중에 오류가 발생 했을 때, 이전 상태로 복원하기 위해서 반드시 필요합니다.

시스템 상태 백업을 수행하는 자세한 과정은 Active Directory 백업과 복원 파트를 참조하기 바랍니다.

디렉터리 서비스 복원 모드로 부팅하기

Active Directory 데이터베이스 파일과 로그 파일을 이동하기 위해서는 도메인 컨트롤러를 디렉터리 서비스 복원 모드로 부팅해야 합니다. 디렉터리 서비스 복원 모드로 도메인 컨트롤러를 부팅하면 더 이상 도메인 컨트롤러로 동작하지 않습니다.

디렉터리 서비스 복원 모드로 도메인 컨트롤러를 부팅하면 더 이상 도메인 계정을 사용해서 인증을 할 수 없기 때문에, 관리자는 로컬 SAM 데이터베이

스에 저장된 로컬 Administrator 계정과 암호로 도메인 컨트롤러에 로그온 합니다. 로컬 Administrator 계정의 암호는 Active Directory 설치 마법사를 이용해서 Active Directory를 설치할 때 지정합니다.

도메인 컨트롤러를 물리적으로 접근이 가능한 경우에는 시스템을 재시작하면서 F8 키를 눌러서 디렉터리 서비스 복원 모드로 부팅하는 것이 가능합니다. 만약 관리자가 원격에서 관리 작업을 수행하는 경우에는 Boot.INI를 수정해서 도메인 컨트롤러를 디렉터리 서비스 복원 모드로 부팅합니다.

[따라하기]

디렉터리 서비스 복원 모드로 부팅하기

도메인 컨트롤러를 디렉터리 서비스 복원 모드로 부팅하는 과정은 다음과 같습니다.

1. 도메인 컨트롤러를 재시작합니다.
2. 운영 체제를 선택하는 메뉴가 나타나면 F8 키를 누릅니다.
3. Windows 고급 옵션 메뉴에서 디렉터리 서비스 복원 모드 (Windows 도메인 컨트롤러만 가능)을 선택합니다.
4. Windows 로그온 대화 상자가 나타나면 로컬 Administrator 계정과 암호를 입력해서 로그온 합니다.

[따라하기]

Boot.INI를 수정하여 디렉터리 서비스 복원 모드로 부팅하기

BOOT.INI를 수정해서 도메인 컨트롤러를 디렉터리 서비스 복원 모드로 부팅하는 과정은 다음과 같습니다.

1. 시작 → 제어판 메뉴를 선택한 후, 시스템 아이콘을 더블클릭 합니다.
2. 시스템 등록정보 대화 상자에서 고급 탭을 클릭한 후, 시작 및 복구의 설정 버튼을 클릭합니다.

3. BOOT.INI 파일을 수정하기 위해 편집 버튼을 클릭합니다.
4. 〈그림 41〉과 같이 운영 체제 부팅 정보의 마지막 부분에 /SAFEBOOT:DSREPAIR를 추가합니다.

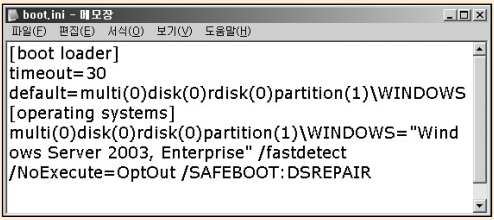

그림 41 BOOT.INI 수정

5. 수정된 BOOT.INI 파일을 저장 한 후, 메모장을 종료합니다.
6. 도메인 컨트롤러를 재시작합니다.
7. Windows 로그온 대화 상자가 나타나면 로컬 Administrator 계정과 암호를 입력해서 로그온 합니다.
8. 시작 → 제어판 메뉴를 선택한 후, 시스템 아이콘을 더블클릭 합니다.
9. 시스템 등록정보 대화 상자에서 고급 탭을 클릭한 후, 시작 및 복구의 설정 버튼을 클릭합니다.
10. BOOT.INI 파일을 수정하기 위해 편집 버튼을 클릭합니다.
11. 운영 체제 부팅 정보의 마지막 부분에 /SAFEBOOT:DSREPAIR를 삭제합니다.
12. 수정된 BOOT.INI 파일을 저장 한 후, 메모장을 종료합니다.

Active Directory 데이터베이스 파일 이동하기

Active Directory 데이터베이스 파일이나 로그 파일을 저장하는 하드 디스크의 저장 공간이 부족하거나, 성능 향상을 위해 Active Directory 데이터베이스 파일이나 로그 파일을 다른 하드 디스크로 이동하는 과정은 다음과 같습니다.

[따라하기]

Active Directory 데이터베이스 파일 이동하기

1. 명령 프롬프트를 실행합니다.
2. Change Directory(CD) 명령을 이용해서 Active Directory 데이터베이스 파일이나 로그 파일이 저장된 폴더로 이동합니다.
3. 다음 명령을 실행해서 Ntdsutil.exe를 실행합니다.
   ntdsutil
4. ntdsutil: 프롬프트에서 files를 입력하고 Enter 키를 누릅니다.
5. Active Directory 데이터베이스 파일을 이동하기 위해서 file maintenance: 프롬프트에서 다음 명령을 실행합니다.
   move db to *drive:\directory*
   *drive:\directory*에 Active Directory 데이터베이스 파일을 이동할 폴더 경로를 지정합니다. 지정한 폴더가 존재하지 않을 경우에는 Ntdsutil.exe이 폴더를 생성합니다. 만일 폴더 경로가 공간을 포함하고 있을 경우에는 다음과 같이 큰 따옴표를 사용해야 합니다.
   move db to "f:\NTDS folder"
   로그 파일을 이동하기 위해서 file maintenance: 프롬프트에서 다음 명령을 실행합니다.
   move logs to *drive:\directory*
   *drive:\directory*에 로그 파일을 이동할 폴더 경로를 지정합니다. 지정한 폴더가 존재하지 않을 경우에는 Ntdsutil.exe이 폴더를 생성합니다.

6. Active Directory 데이터베이스 파일에 대한 무결성을 점검하기 위해 file maintenance:
   프롬프트에서 다음 명령을 실행합니다.
   integrity

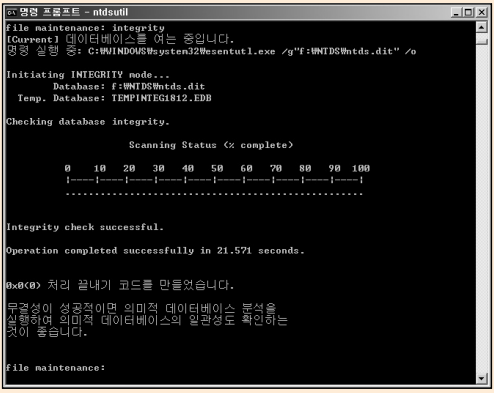

그림 42 Active Directory 데이터베이스 무결성 점검

7. 〈그림 42〉와 같이 이동한 Active Directory 데이터베이스 파일에 대한 무결성 점검이 오류 없이 완료 되면, file maintenance: 프롬프트에서 quit를 실행합니다.
8. ntdsutil.exe를 종료하기 위해서 ntdsutil: 프롬프트에서 quit를 실행합니다.
9. 도메인 컨트롤러를 정상적으로 재시작 합니다.

사용하지 않는 공간 반납하기

일상적인 운영 환경하에서, Active Directory 데이터베이스 파일은 개체 생성과 삭제에 의해 내부적으로 빈 공간들이 산재하게 됩니다. Active Directory는 가비지 컬렉션 프로세스의 일부로 온라인 조각 모음을 특정 시간 간격(기본적으로 12시간 간격)으로 자동 수행합니다. 온라인 조각 모음은 Active Directory 데이터베이스 파일 크기를 줄이지는 않지만, 대신 내부 데이터 저장소에 대한 최적화를 수행합니다.

관리자는 Active Directory 데이터베이스 파일 내에 더 이상 사용하지 않는 빈 공간을 Windows 파일 시스템에 반납하기 위해서 오프라인 조각 모음을 수행합니다. 대량의 개체 삭제나 글로벌 카탈로그 서버 기능 제거 후에 사용하지 않는 빈 공간을 반납하고자 한다면 오프라인 조각 모음을 수행하여 Active Directory 데이터베이스 파일(NTDS.dit)의 크기를 줄일 수 있습니다.

레지스트리에 가비지 콜렉션 로그 레벨을 설정함으로써, 관리자는 오프라인 조각 모음을 수행했을 때 Windows 파일 시스템에 반납 가능한 빈 공간의 크기에 대한 정보를 얻을 수 있습니다.

다음과 같이 가비지 콜렉션 로그 레벨을 0에서 1로 변경하면, 관리자는 디렉터리 서비스 로그에서 이벤트 ID 1646이 기록 되는 것을 확인할 수 있습니다.

키 위치 :
HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics
이름 : Garbage Collection
데이터 종류: REG_DWORD
기본 설정 값: 0
변경 값: 1

이 이벤트는 현재 Active Directory 데이터베이스가 사용하는 총 용량과 오프라인 조각 모음을 통해 Windows 파일 시스템에 반납 가능한 용량에 대한 정보를 제공합니다. 가비지 콜렉션 로그 레벨이 기본 설정인 0으로 되어 있으면, 오류에 관련된 이벤트만이 디렉터리 서비스 로그에 기록됩니다. 관리자는 온라인 조각 모음과 관련한 다음과 같은 이벤트를 디렉터리 서비스 로그에서 확인할 수 있습니다.

- 이벤트 ID 700, 701 : 온라인 조작 모음의 시작과 끝을 기록합니다.
- 이벤트 ID 1646 : 오프라인 조각 모음을 통해 Windows 파일 시스템에 반납 가능한

용량에 대한 정보와 Active Directory 데이터베이스가 사용하는 총 용량을 기록합니다.
〈그림 43〉의 이벤트 설명을 참조하면, 현재 Active Directory 데이터베이스의 크기는 44 MB이고 온라인 조각 모음에 의해 생성된 빈 공간은 14 MB가 됩니다. 따라서 향후 오프라인 조각 모음을 수행하면 14 MB를 Windows 파일 시스템에 반납하여, Active Directory 데이터베이스의 크기는 30 MB로 최적화 됩니다.

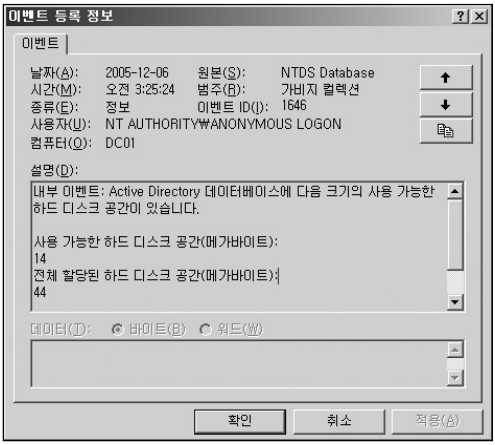

그림 43 이벤트 ID 1646

Active Directory 데이터베이스의 사용하지 않는 빈 공간을 Windows 파일 시스템에 반납하는 오프라인 조각 모음은 다음과 같은 순서로 진행합니다.

그림 44 사용하지 않는 공간 반납 프로세스

시스템 상태 백업하기

Active Directory 데이터베이스 관리 작업을 수행하기 전에, 관리자는 반드시 시스템 상태 백업을 수행해야 합니다. 시스템 상태 백업은 Active Directory 데이터베이스 파일이나 로그 파일을 이동하는 중에 오류가 발생 했을 때, 이전 상태로 복원하기 위해서 반드시 필요합니다.

시스템 상태 백업을 수행하는 자세한 과정은 Active Directory 백업과 복원 파트를 참조하기 바랍니다.

디렉터리 서비스 복원 모드로 부팅하기

Active Directory 데이터베이스 파일과 로그 파일을 이동하기 위해서는 도메인 컨트롤러를 디렉터리 서비스 복원 모드로 부팅해야 합니다. 디렉터리 서비스 복원 모드로 도메인 컨트롤러를 부팅하면 더 이상 도메인 컨트롤러로 동작하지 않습니다.

디렉터리 서비스 복원 모드로 도메인 컨트롤러를 부팅하면 더 이상 도메인 계정을 사용해서 인증을 할 수 없기 때문에, 관리자는 로컬 SAM 데이터베이스에 저장된 로컬 Administrator 계정과 암호로 도메인 컨트롤러에 로그온 합니다. 로컬 Administrator 계정의 암호는 Active Directory 설치 마법사를 이용해서 Active Directory를 설치할 때 지정합니다.

도메인 컨트롤러를 물리적으로 접근이 가능한 경우에는 시스템을 재시작하면서 F8 키를 눌러서 디렉터리 서비스 복원 모드로 부팅하는 것이 가능합니다. 만약 관리자가 원격에서 관리 작업을 수행하는 경우에는 Boot.INI를 수정해서 도메인 컨트롤러를 디렉터리 서비스 복원 모드로 부팅합니다.

[따라하기]

디렉터리 서비스 복원 모드로 부팅하기

도메인 컨트롤러를 디렉터리 서비스 복원 모드로 부팅하는 과정은 다음과 같습니다.

1. 도메인 컨트롤러를 재시작합니다.
2. 운영 체제를 선택하는 메뉴가 나타나면 F8 키를 누릅니다.
3. Windows 고급 옵션 메뉴에서 디렉터리 서비스 복원 모드 (Windows 도메인 컨트롤러만 가능)을 선택합니다.
4. Windows 로그온 대화 상자가 나타나면 로컬 Administrator 계정과 암호를 입력해서 로그온 합니다.

[따라하기]

Boot.INI를 수정하여 디렉터리 서비스 복원 모드로 부팅하기

BOOT.INI를 수정해서 도메인 컨트롤러를 디렉터리 서비스 복원 모드로 부팅하는 과정은 다음과 같습니다.

1. 시작 → 제어판 메뉴를 선택한 후, 시스템 아이콘을 더블클릭 합니다.
2. 시스템 등록정보 대화 상자에서 고급 탭을 클릭한 후, 시작 및 복구의 설정 버튼을 클릭합니다.
3. BOOT.INI 파일을 수정하기 위해 편집 버튼을 클릭합니다.
4. 〈그림 45〉와 같이 운영 체제 부팅 정보의 마지막 부분에 /SAFEBOOT:DSREPAIR를 추가합니다.

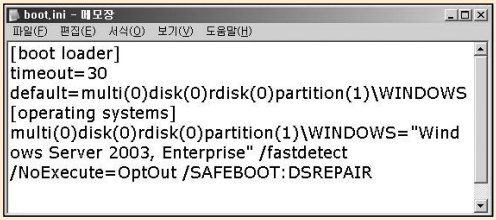

그림 45 BOOT.INI 수정

5. 수정된 BOOT.INI 파일을 저장 한 후, 메모장을 종료합니다.
6. 도메인 컨트롤러를 재시작합니다.
7. Windows 로그온 대화 상자가 나타나면 로컬 Administrator 계정과 암호를 입력해서 로그온 합니다.
8. 시작 → 제어판 메뉴를 선택한 후, 시스템 아이콘을 더블클릭 합니다.
9. 시스템 등록정보 대화 상자에서 고급 탭을 클릭한 후, 시작 및 복구의 설정 버튼을 클릭합니다.
10. BOOT.INI 파일을 수정하기 위해 편집 버튼을 클릭합니다.
11. 운영 체제 부팅 정보의 마지막 부분에 /SAFEBOOT:DSREPAIR를 삭제합니다.
12. 수정된 BOOT.INI 파일을 저장 한 후, 메모장을 종료합니다.

오프라인 조각 모음 수행하기

오프라인 조각 모음을 수행하면 지정한 다른 폴더에 최적화된 새로운 Active Directory 데이터베이스 파일이 생성됩니다. 새로운 Active Directory 데이터베이스 파일을 생성하는 위치로 도메인 컨트롤러 로컬 하드 디스크나 네트워크 맵핑 드라이브를 지정하는 것이 가능합니다.

하지만 네트워크와 관련된 잠재적인 오류가 발생하는 것을 막기 위해, 새로운 Active Directory 데이터베이스 파일은 도메인 컨트롤러의 로컬 하드 디스크에 생성할 것을 권장합니다.

지정된 위치에 새로운 Active Directory 데이터베이스 파일이 생성된 후에는, 원래 위치로 최적화 된 파일을 복사합니다. 도메인 컨트롤러가 최적화 된 새 Active Directory 데이터베이스 파일을 이용해서 성공적으로 재시작 될 때까지, 원본 NTDS.dit 파일은 원래 위치에서 이름을 변경해 놓거나 다른 위치에 저장해 둘 것을 권장합니다.

[따라하기]

오프라인 조각 모음 수행하기

Active Directory 데이터베이스의 사용하지 않는 빈 공간을 Windows 파일 시스템에 반납하는 오프라인 조각 모음을 수행하는 과정은 다음과 같습니다.

1. 명령 프롬프트를 실행합니다.
2. Change Directory(CD) 명령을 이용해서 Active Directory 데이터베이스 파일이나 로그 파일이 저장된 폴더로 이동합니다.
3. 다음 명령을 실행해서 Ntdsutil.exe를 실행합니다.
   ntdsutil
4. ntdsutil: 프롬프트에서 files를 입력하고 Enter 키를 누릅니다.

5. Active Directory 데이터베이스 파일 및 로그 파일의 경로와 크기에 대한 현재 정보를 수집하기 위해 file maintenance: 프롬프트에서 다음 명령을 실행합니다.

   Info

   출력된 Active Directory 데이터베이스 파일 및 로그 파일의 경로를 적어 둡니다. 〈그림 46〉의 예제에서 Active Directory 데이터베이스 파일 및 로그 파일이 모두 f:\NTDS 폴더에 저장된 것을 확인 할 수 있습니다.

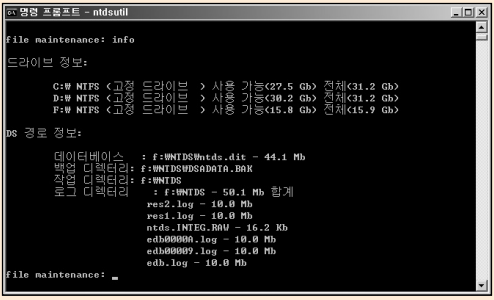

그림 46 Active Directory 데이터베이스 파일 및 로그 파일의 경로 정보

6. Active Directory 데이터베이스 파일을 이동하기 위해서 file maintenance: 프롬프트에서 다음 명령을 실행합니다.

   compact to *drive:\directory*

   *drive:\directory*에 최적화된 새 Active Directory 데이터베이스 파일이 생성될 폴더 경로를 지정합니다. 지정한 폴더가 존재하지 않을 경우에는 Ntdsutil.exe이 폴더를 생성한 후 최적화된 Active Directory 데이터베이스 파일을 생성합니다.

만일 폴더 경로가 공간을 포함하고 있을 경우에는 다음과 같이 큰 따옴표를 사용해야 합니다.

compact to “f:\temp folder”

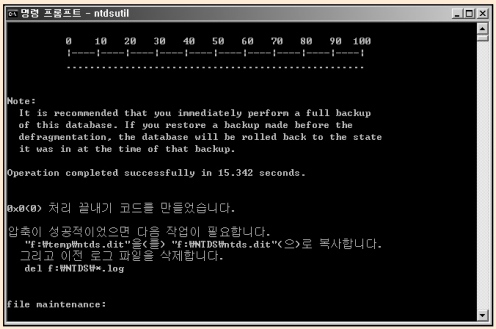

그림 47 오프라인 조각 모음 실행

7. 오프라인 조각 모음이 오류 없이 완료되면, file maintenance: 프롬프트에서 quit를 실행합니다.
8. ntdsutil.exe를 종료하기 위해서 ntdsutil: 프롬프트에서 quit를 실행합니다.
9. 5 단계에서 기록했던 로그 파일 폴더에 저장되어 있는 로그 파일들을 다음과 같은 명령을 실행하여 모두 삭제합니다. Edb.chk 파일을 삭제할 필요는 없습니다.

   del drive:\pathToLogFiles*.log
10. 도메인 컨트롤러가 최적화 된 새 Active Directory 데이터베이스 파일을 이용해서 성공적으로 재시작 될 때까지 원본 NTDS.dit 파일을 보존할 것을 권장합니다.

원본 NTDS.dit 파일을 원래 위치에서 이름을 변경해 놓거나, 다른 위치에 복사합니다.

11. 5 단계에서 기록했던 Active Directory 데이터베이스 파일을 저장하는 폴더에 최적화 된 새 Active Directory 데이터베이스 파일을 복사합니다.
12. 다음 명령을 실행해서 Ntdsutil.exe를 실행합니다.
    ntdsutil
13. ntdsutil: 프롬프트에서 files를 입력하고 Enter 키를 누릅니다.
14. Active Directory 데이터베이스 파일에 대한 무결성을 점검하기 위해 file maintenance: 프롬프트에서 다음 명령을 실행합니다.
    integrity
15. 최적화 된 Active Directory 데이터베이스 파일에 대한 무결성 점검이 오류 없이 완료 되면, file maintenance: 프롬프트에서 quit를 실행합니다.
16. ntdsutil.exe를 종료하기 위해서 ntdsutil: 프롬프트에서 quit를 실행합니다.
17. 도메인 컨트롤러를 정상적으로 재시작 합니다.

도메인 컨트롤러 관리

이미 설치되어 운영중인 도메인 컨트롤러에 대한 관리 작업은 적지만, 일반적인 운영 환경에서 관리자는 다음과 같은 도메인 컨트롤러와 관련된 작업을 수행할 수 있습니다.

도메인 컨트롤러 추가 및 제거

운영중인 도메인에 새로운 도메인 컨트롤러를 추가하기 위해, Windows Server 2003이나 Windows Server 2003 SP1이 설치된 컴퓨터에 Active Directory 설치 마법사를 이용해서 Active Directory를 설치합니다. 새로운 도메인 컨트롤러를 생성함으로써 새로운 포리스트나 도메인을 생성할 수 있으며, 기존에 운영중인 도메인에 도메인 컨트롤러를 추가할 수 있습니다.

새로운 도메인 컨트롤러를 추가하는 이유는 여러 가지가 있습니다. 도메인 사용자가 늘어날 경우에는 도메인 컨트롤러를 추가하여 사용자 인증 부하를 분산합니다. 또는 원격 사이트가 생성되어 사이트의 사용자들이 보다 빠르게 인증을 받을 수 있도록 원격 사이트에 도메인 컨트롤러를 추가합니다.

더 이상 도메인 컨트롤러가 필요 없는 경우에는 Active Directory를 설치하는 과정과 유사하게 Active Directory 설치 마법사를 이용해서 Active Directory를 제거합니다. 만일 도메인 컨트롤러에 오류가 발생해서 더 이상 동작이 불가능한 경우에는 로컬의 Active Directory를 강제로 제거하고, 포리스트의 Active Directory에 남아 있는 강제 제거한 도메인 컨트롤러의 메타데이터 정보를 삭제합니다.

도메인 컨트롤러 이름 변경

관리적인 측면이나 다른 이유에 의해 도메인 컨트롤러의 이름을 변경할 필요가 있습니다.

Windows Server 2003으로 구성된 도메인 컨트롤러는 쉽게 이름을 변경할 수 있으며, 변경된 도메인 컨트롤러 이름은 DNS에 자동으로 반영됩니다. 도메인 컨트롤러의 이름을 변경한 후에 관리자는 복제가 정상적으로 동작하도록 파일 복제 서비스 구성원 개체의 이름을 변경합니다.

원격 사이트에 도메인 컨트롤러 추가

만약 느린 WAN 구간으로 연결된 원격 사이트에 사용자가 늘어난다면, 사용자 로그온과 검색 속도를 향상하기 위해 원격 사이트에 도메인 컨트롤러를 추가할 필요가 있습니다. 원격 사이트에 도메인 컨트롤러를 추가 하기 위해 관리자는 미리 도메인 컨트롤러를 설치한 후 원격 사이트로 배송하여 운영할 것인지, 또는 원격 사이트에서 직접 도메인 컨트롤러를 설치할 것인지를 결정해야 합니다.

원격 사이트에서 직접 도메인 컨트롤러를 설치한다면, 다음 두 가지 중에 하나를 Active Directory 복제 방식으로 선택합니다.

- WAN 구간을 통해 Active Directory 복제
- 시스템 상태 백업을 복원

Active Directory 설치 마법사는 도메인 컨트롤러 설치 중에 다른 도메인 컨트롤러로부터 Active Directory 전체를 복제하는 작업을 수행합니다. 만약 원격 사이트에 도메인 컨트롤러가 존재하지 않는다면 Active Directory 설치 마법사는 느린 WAN 구간을 경유 해서 다른 사이트의 도메인 컨트롤러로부터 Active Directory를 복제해야 합니다. Active Directory의 크기에 따라 느린

WAN 구간에 병목현상을 유발하고, 복제로 인해 장시간 동안 작업을 수행해야 하는 부담이 발생합니다.
이런 경우에는 기존 도메인 컨트롤러에서 백업한 시스템 상태 백업을 복원함으로써 원격 사이트에 도메인 컨트롤러를 빠르게 추가할 수 있습니다. 시스템 상태 백업을 복원하여 도메인 컨트롤러를 추가하기 위해서는, 시스템 상태를 백업한 도메인 컨트롤러와 새로 추가하는 도메인 컨트롤러가 Windows Server 2003 또는 Windows Server 2003 SP1 이상의 동일한 운영 체제를 사용해야 합니다. 또한 하드웨어 플랫폼(32 비트 또는 64 비트)도 반드시 동일해야 합니다.

원격 사이트에 도메인 컨트롤러 설치하기

시스템 상태 백업을 이용해서 원격 사이트에 도메인 컨트롤러를 설치하는 주 목적은 도메인, 정보, 스키마 파티션과 추가적으로 글로벌 카탈로그 파티션, DNS 응용 프로그램 파티션의 복제 원본으로 로컬에 복원한 시스템 상태 파일들을 이용하기 위해서입니다.
로컬에 복원한 시스템 상태 파일들을 이용해서 Active Directory를 생성하고, 시스템 상태 백업 이후에 변경된 내용은 다른 사이트의 도메인 컨트롤러를 통해 복제함으로써 최소한의 WAN 구간 트래픽을 발생하면서 새로운 도메인 컨트롤러를 생성합니다. 복원된 시스템 상태 파일들로 도메인 컨트롤러를 설치하기 위해 다음과 같은 방법을 사용할 수 있습니다.

- 복원된 시스템 상태 파일들이나 unrestored.bkf 파일을 외장 하드 디스크, CD 또는 DVD와 같은 이동식 저장 장치에 복사 한 후, 도메인 컨트롤러로 설치할 시스템과 함께 원격 사이트로 배송

- 도메인 컨트롤러로 설치할 시스템의 로컬 하드디스크에 시스템 상태 백업을 복원한 후, 원격 사이트에 배송

복원된 시스템 상태 파일을 이동식 저장 장치에 복사 한 경우에는 여러 도메인 컨트롤러를 설치할 때 사용할 수 있다는 장점이 있습니다.
원격 사이트에서 DCPromo /adv 옵션을 이용하여 Active Directory 설치 마법사를 실행하면, 복원된 시스템 상태 파일들을 이용해서 도메인 컨트롤러를 설치합니다.원격 사이트에 시스템 상태 백업을 이용해서 도메인 컨트롤러를 설치할 때는 다음과 같은 사항을 준수할 것을 권장합니다.

- **Windows Server 2003 서비스 팩 1 설치** : 도메인 컨트롤러에 응용 프로그램 디렉터리 파티션을 사용할 경우에는 Active Directory를 설치하기 전에 Windows Server 2003 서비스 팩 1을 설치할 것을 권장합니다. Windows Server 2003 서비스 팩 1이 설치되지 않은 시스템에 시스템 상태 백업을 복원하면 응용 프로그램 디렉터리 파티션이 복원되지 않습니다. 따라서 DNS와 같은 응용 프로그램 디렉터리 파티션을 사용할 경우에는, Active Directory 설치 중에 WAN 구간의 복제 트래픽이 발생합니다.
- **동일한 기능이 동작중인 도메인 컨트롤러의 시스템 상태 백업** : 시스템 상태 백업은 설치할 도메인 컨트롤러와 동일한 기능이 동작중인 도메인 컨트롤러에서 수행합니다. 만일 원격 사이트에 글로벌 카탈로그 서버로 동작할 도메인 컨트롤러를 설치하기 위해서는 글로벌 카탈로그 서버로 동작중인 도메인 컨트롤러에서 시스템 상태 백업을 수행합니다.
- **시스템 상태 백업과 도메인 컨트롤러 설치 시간 간격의 최소화** : 시스템 상태 백업을 수행한 후, 빠른 시일 안에 복원한 시스템 상태 파일들을 이용해서 도메인 컨트롤러를 설치합니다. 이 간격이 길어지면 Active Directory를 설치한 후, 시스템 상태 백업 이후에 변경된 내용을 업데이트

하기 위해 WAN 구간에 많은 트래픽이 발생합니다.

- **원격 사이트에 시스템을 배송 하기 전에 운영 체제 설치 완료** : 도메인 컨트롤러로 설치할 시스템을 원격 사이트에 배송하기 전에, 다른 도메인 컨트롤러와 동일하게 운영 체제를 설치합니다. 파티션, 드라이브 문자 지정, 최신 패치 및 서비스 팩 적용등과 같이 표준화 된 운영 체제 설치를 완료합니다.

복원한 시스템 상태 파일들을 이용해서 원격 사이트에 도메인 컨트롤러를 설치하는 순서는 다음과 같습니다.

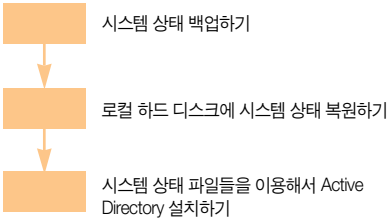

그림 48 원격 사이트에 도메인 컨트롤러 설치 프로세스

시스템 상태 백업하기

설치할 도메인 컨트롤러와 동일한 기능이 동작중인 도메인 컨트롤러에서 시스템 상태 백업을 수행합니다. 만일 원격 사이트에 글로벌 카탈로그 서버로 동작할 도메인 컨트롤러를 설치하기 위해서는 글로벌 카탈로그 서버로 동작중인 도메인 컨트롤러에서 시스템 상태 백업을 수행합니다. 설치할 도메인 컨트롤러에 DNS 서버를 운영할 계획이면, 역시 DNS 서버가 동작중인 도메인 컨트롤러에서 시스템 상태 백업을 수행합니다.

시스템 상태 백업을 수행하는 자세한 과정은 Active Directory 백업과 복원 파트를 참조하기 바랍니다.

로컬 하드 디스크에 시스템 상태 복원하기

원격 사이트에 설치할 도메인 컨트롤러의 로컬 하드 디스크에 다른 도메인 컨트롤러에서 백업한 시스템 상태 백업을 복원합니다. 도메인 컨트롤러를 설치한 후에는 로컬에 복원한 시스템 상태 파일들은 삭제합니다.

[따라하기]

로컬 하드 디스크에 시스템 상태 복원하기

로컬 하드 디스크에 시스템 상태 백업을 복원하는 과정은 다음과 같습니다.

1. 시작 → 실행 메뉴를 선택한 후, ntbackup를 입력하여 백업 및 복원 마법사를 실행합니다.
2. 백업 및 복원 마법사 시작 페이지가 나타납니다. 다음 버튼을 클릭합니다.
3. 시스템 상태 백업을 복원하기 위해 파일 및 설정 복원 옵션을 선택한 후, 다음 버튼을 클릭합니다.
4. 복원 할 시스템 상태 백업을 선택하기 위해 찾아보기 버튼을 클릭합니다.
5. 백업한 파일을 열기 위해 찾아보기 버튼을 클릭합니다. 복원할 시스템 상태 백업 파일을 선택한 후, 확인 버튼을 클릭합니다.

6. 복원할 항목 목록에서 복원할 시스템 상태 백업을 확장합니다. System State 항목을 클릭한 후, 다음 버튼을 클릭합니다.

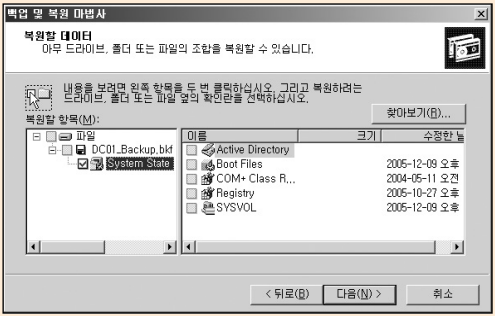

그림 49 복원할 시스템 상태 백업 선택

7. 백업 및 복원 마법사 완료 페이지에서 고급 버튼을 클릭합니다.
8. 파일을 복원할 위치 목록에서 대체 위치를 선택합니다.
9. 대체 위치 입력창에 시스템 상태 백업을 복원할 폴더 경로를 입력한 후, 다음 버튼을 클릭합니다.
   도메인 컨트롤러를 설치할 때 Active Directory 데이터베이스 파일을 저장할 파티션에 〈그림 50〉과 같이 NTDSRestore 폴더 이름을 사용할 권장합니다.

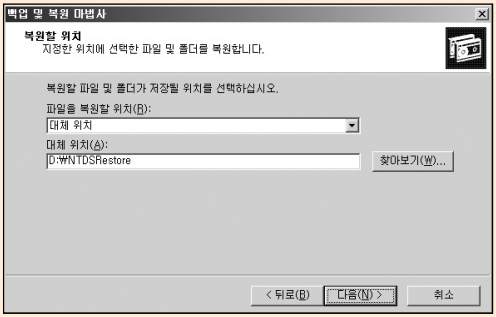

그림 50 복원할 위치 지정

10. 복원 방법으로 기본 설정을 사용합니다. 기본 파일을 보존함(권장) 옵션이 선택되어 있는지 확인한 후, 다음 버튼을 클릭합니다.
11. 고급 복원 옵션으로 기본 설정을 사용합니다. 보안 설정 복원과 기본 볼륨 탑재 지점 유지 옵션이 선택되어 있는지 확인한 후, 다음 버튼을 클릭합니다.
12. 마침 버튼을 클릭합니다. 지정한 대체 위치로 시스템 상태 백업이 복원됩니다.
13. 복원이 완료되면 닫기 버튼을 클릭합니다.

시스템 상태 파일들을 이용해서 Active Directory 설치하기

원격 사이트에서 DCPromo /adv 옵션을 이용하여 Active Directory 설치 마법사를 실행하면, 복원된 시스템 상태 파일들을 이용해서 도메인 컨트롤러를 설치합니다.

[따라하기]

시스템 상태 파일들을 이용해서 Active Directory 설치하기

시스템 상태 파일들을 이용해서 원격 사이트에 Active Directory를 설치하는 과정은 다음과 같습니다.

1. 시작 → 실행 메뉴를 선택한 후, dcpromo /adv를 입력하여 Active Directory 설치 마법사를 실행합니다.
2. Active Directory 설치 마법사 시작 페이지가 나타납니다. 다음 버튼을 클릭합니다.
3. 운영 체제 호환성 페이지가 나타납니다. 도움말을 읽은 후 다음 버튼을 클릭합니다.
4. 도메인 컨트롤러 종류 페이지에서 기존 도메인의 추가 도메인 컨트롤러 옵션을 선택한 후, 다음 버튼을 클릭합니다.
5. 추가 도메인 컨트롤러의 Active Directory 정보를 동기화 할 도메인 정보의 위치를 지정합니다. 복원된 다음 백업 파일에서 옵션을 선택한 후, 시스템 상태 백업을 복원한 폴더 경로를 입력합니다. 폴더 경로를 확인한 후 다음 버튼을 클릭합니다.

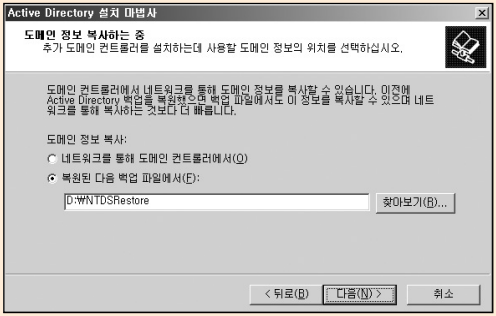

그림 51 도메인 정보의 위치 지정

6. 시스템 상태 백업을 수행한 도메인 컨트롤러가 글로벌 카탈로그 서버일 경우에는 새로 추가하는 도메인 컨트롤러를 글로벌 카탈로그 서버로 구성할 것인지를 묻습니다. 구성 여부에 따라 적절히 예 또는 아니오 옵션을 선택한 후, 다음 버튼을 클릭합니다.

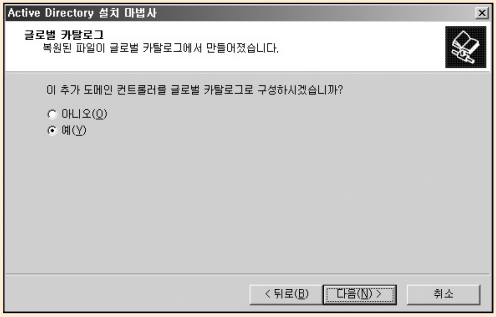

그림 52 글로벌 카탈로그 구성 여부 선택

7. Active Directory를 설치할 수 있는 권한을 가진 도메인 계정과 암호를 입력한 후, 다음 버튼을 클릭합니다.
8. Active Directory 데이터베이스와 로그 파일을 저장할 경로를 입력한 후, 다음 버튼을 클릭합니다.
9. SYSVOL 폴더의 경로를 입력한 후, 다음 버튼을 클릭합니다.
10. 디렉터리 서비스 복원 모드로 시스템을 시작했을 때 사용할 로컬 Administrator 계정의 암호를 입력 한 후, 다음 버튼을 클릭합니다.
11. 요약 페이지에서 선택한 옵션의 내용을 검토한 후, 다음 버튼을 클릭합니다.
12. Active Directory 설치가 완료되면, 마침 버튼을 클릭하여 Active Directory 설치 마법사를 종료합니다.
13. Active Directory 설치 마법사에 의해 변경된 내용을 적용하기 위해 지금 다시 시작 버튼을 클릭하여 시스템을 재시작합니다.

도메인 컨트롤러의 이름 변경하기

Windows Server 2003으로 구성된 도메인 컨트롤러는 Windows 2000 Server로 구성된 도메인 컨트롤러와 달리 쉽게 이름을 변경할 수 있습니다. 클라이언트나 멤버 컴퓨터에서 컴퓨터 이름을 변경하는 과정과 동일하게 도메인 컨트롤러의 이름을 변경합니다. 도메인 컨트롤러의 이름을 변경한 후에 관리자는 복제가 정상적으로 동작하도록 파일 복제 서비스 구성원 개체의 이름도 변경해야 합니다. 도메인 컨트롤러의 이름 변경은 다음과 같은 순서로 진행합니다.

그림 53 도메인 컨트롤러 이름 프로세스

도메인 컨트롤러 이름 변경하기

클라이언트나 멤버 컴퓨터에서 컴퓨터 이름을 변경하는 과정과 동일하게 제어판의 시스템 등록 정보를 이용해서 도메인 컨트롤러의 이름을 변경합니다.

[따라하기]

도메인 컨트롤러 이름 변경하기

1. 시작 → 제어판 → 시스템 아이콘을 더블클릭 합니다.
2. 시스템 등록 정보 대화 상자가 나타납니다. 컴퓨터 이름 탭을 클릭한 후, 변경 버튼을 클릭합니다.
3. 컴퓨터 이름 변경 확인 대화 상자가 나타납니다. 확인 버튼을 클릭합니다.

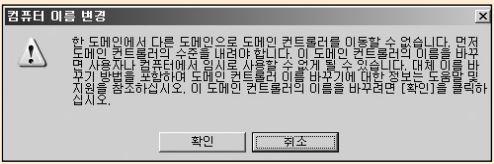

그림 54 컴퓨터 이름 변경 확인

4. 컴퓨터 이름 입력창에 도메인 컨트롤러의 새 이름을 입력한 후, 확인 버튼을 클릭합니다.
5. 도메인 컨트롤러의 이름을 변경할 수 있는 권한을 가진 계정과 암호를 입력 한 후, 확인 버튼을 클릭합니다.
6. 변경된 내용을 적용하기 위해 컴퓨터를 재시작 할 것을 알리는 대화 상자가 나타납니다. 확인 버튼을 클릭합니다.
7. 확인 버튼을 클릭하여 시스템 등록 정보 대화 상자를 종료합니다.
8. 시스템 설정 변경을 적용하기 위해 시스템 재시작이 필요합니다. 예 버튼을 클릭하여 시스템을 재시작합니다.

파일 복제 서비스 구성원 개체 이름 변경하기

도메인 컨트롤러의 이름을 변경한 후에는 Active Directory 사용자 및 컴퓨터를 이용해서 파일 복제 서비스 구성원 개체의 정보를 변경합니다.

[따라하기]

파일 복제 서비스 구성원 개체 이름 변경하기

파일 복제 서비스 개체의 정보를 업데이트 하는 과정은 다음과 같습니다. 아래 예제에서는 DC03 도메인 컨트롤러의 이름을 DC02로 변경한 후에, 파일 복제 서비스 구성원 개체의 이름을 변경합니다.

1. 시작 → 관리 도구 → Active Directory 사용자 및 컴퓨터 메뉴를 선택하여, Active Directory 사용자 및 컴퓨터 관리 도구를 실행합니다.
2. Active Directory 사용자 및 컴퓨터 관리 도구의 왼쪽 창에서 Active Directory 사용자 및 컴퓨터를 마우스 오른쪽 버튼으로 클릭한 후, 보기 → 고급 기능 메뉴를 선택합니다.

3. 콘솔 트리의 도메인 이름 하위에, System → File Replication Service → Domain System Volume (SYSVOL Share)까지 확장합니다.
4. Domain System Volume (SYSVOL Share) 하위의 파일 복제 서비스 구성원 개체 중에서 변경전의 도메인 컨트롤러 이름을 사용하는 것을 찾습니다. 〈그림 55〉의 오른쪽 창을 보면, 컴퓨터 칼럼은 현재 도메인 컨트롤러의 이름을 사용하는데, 이름 칼럼은 변경하기 전의 도메인 컨트롤러 이름을 사용하는 구성원 개체를 찾을 수 있습니다.

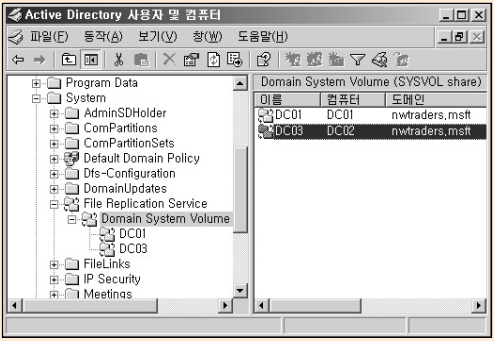

그림 55 파일 복제 서비스 구성원 개체

5. 변경전의 도메인 컨트롤러 이름을 사용하는 구성원 개체를 마우스 오른쪽 버튼으로 클릭한 후, 이름 바꾸기 메뉴를 선택합니다.
6. 구성원 개체의 이름을 도메인 컨트롤러의 새 이름으로 변경한 후, Active Directory 사용자 및 컴퓨터를 종료합니다.

도메인 컨트롤러 제거하기

도메인 컨트롤러 제거 작업은 Active Directory 마법사에 의해 이루어지며, 시스템에서 Active Directory 데이터베이스 및 SYSVOL에 관련된 모든 파일을 삭제한 후, 도메인 컨트롤러를 멤버 서버로 설정합니다.
더 이상 필요 없는 도메인 컨트롤러의 제거는 다음과 같은 순서로 진행합니다.

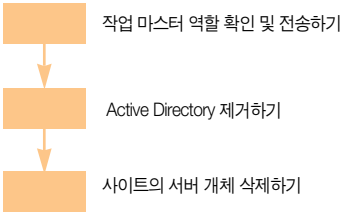

그림 56 도메인 컨트롤러 제거 프로세스

작업 마스터 역할 확인 및 전송하기

Active Directory 설치 마법사는 도메인 컨트롤러를 제거할 때, 먼저 제거할 도메인 컨트롤러가 작업 마스터 역할을 담당하고 있는지 점검합니다. 만약 제거할 도메인 컨트롤러가 작업 마스터 역할을 담당하고 있으면, 임의의 다른 도메인 컨트롤러로 작업 마스터 역할을 전송합니다. 임의의 도메인 컨트롤러로 역할을 전송하기 때문에 과부하가 발생하거나 추가 관리 작업이 필요할 수 있습니다.

따라서 Active Directory를 제거하기 전에 먼저 도메인 컨트롤러가 작업 마스터 역할을 담당하고 있는지 점검하고, 적절한 도메인 컨트롤러로 작업 마스터 역할을 전송할 것을 권장합니다.

[따라하기]

작업 마스터 역할 확인 및 전송하기

5 종류의 작업 마스터 역할을 담당하는 도메인 컨트롤러를 확인하는 과정은 다음과 같습니다.

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행해서 ntdsutil.exe를 실행합니다.
   ntdsutil
3. ntdsutil: 프롬프트에서 roles를 입력하고 Enter 키를 누릅니다.
4. fsmo maintenance: 프롬프트에서 connections를 입력하고, Enter 키를 누릅니다.
5. server connections: 프롬프트에서 다음 명령을 실행합니다.
   connect to server *servername*
   *servername*에 제거할 도메인 컨트롤러의 이름을 입력합니다.
6. server connections: 프롬프트에서 quit를 실행합니다.
7. fsmo maintenance: 프롬프트에서 select operation target를 입력하고, Enter 키를 누릅니다.
8. 5 종류의 작업 마스터 역할을 담당하는 도메인 컨트롤러의 정보를 확인하기 위해 select operation target: 프롬프트에서 다음 명령을 실행합니다.
   list roles for connected server
   〈그림 57〉과 같이 5 종류의 작업 마스터 역할을 담당하고 있는 도메인 컨트롤러가 출력됩니다. 제거할 도메인 컨트롤러가 작업 마스터 역할을 담당하고 있는 지 확인합니다.

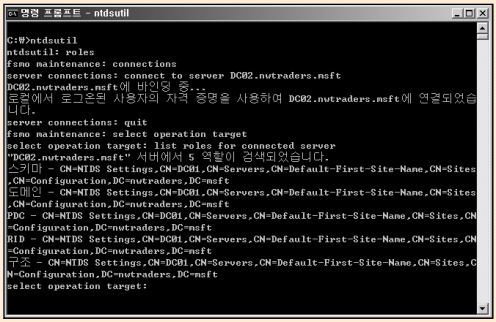

그림 57 작업 마스터 역할 확인하기

9. 제거할 도메인 컨트롤러가 작업 마스터 역할을 담당하고 있으면 적절한 도메인 컨트롤러로 역할을 전송합니다.
   작업 마스터 역할을 전송하는 과정은 작업 마스터 관리 파트를 참조하기 바랍니다.

Active Directory 제거하기

Active Directory 설치 마법사를 이용해서 Active Directory를 제거합니다.

[따라하기]

Active Directory 제거하기

1. 시작 → 실행 메뉴를 선택한 후, dcpromo를 입력하여 Active Directory 설치 마법사를 실행합니다.

2. Active Directory 설치 마법사가 실행됩니다. 간단한 도움말을 읽은 후에 다음 버튼을 클릭합니다.
3. 제거할 도메인 컨트롤러가 글로벌 카탈로그 서버로 동작하고 있으면, 〈그림 58〉과 같이 다른 글로벌 카탈로그가 존재하는지 확인할 것을 알려주는 메시지가 출력됩니다. 확인 버튼을 클릭합니다.

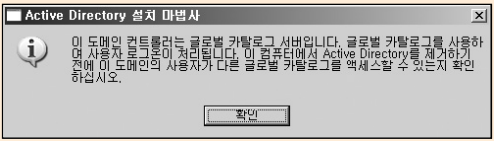

그림 58 글로벌 카탈로그 서버 경고 메시지

4. 제거할 도메인 컨트롤러가 도메인의 마지막 도메인 컨트롤러인지 여부를 선택합니다.
   제거할 도메인 컨트롤러가 도메인의 마지막 도메인 컨트롤러이면 이 서버가 도메인의 마지막 도메인 컨트롤러입니다. 옵션을 선택합니다. 마지막 도메인 컨트롤러이면 도메인이 제거되고, 독립 실행형 서버로 바뀝니다.
   도메인의 마지막 도메인 컨트롤러인지 여부에 따라 옵션을 선택한 후, 다음 버튼을 클릭합니다.

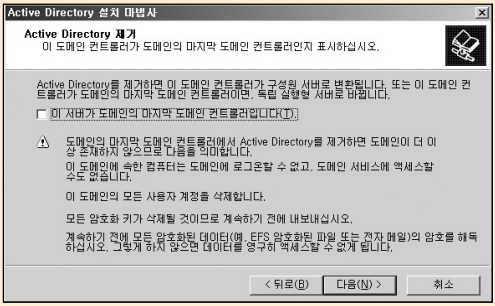

그림 59 Active Directory 제거

5. 로컬 Administrator 계정의 암호를 설정합니다. 암호를 두 번 입력 후 다음 버튼을 클릭합니다.
6. 선택한 옵션을 요약한 화면이 나타납니다. Active Directory를 제거하기 위해 다음 버튼을 제거합니다.
7. Active Directory를 구성하는 요소들을 제거하는 화면이 나타납니다. Active Directory 제거가 완료되면 마침 버튼을 클릭하여 Active Directory 설치 마법사를 종료합니다.
8. Active Directory 설치 마법사에 의해 변경된 내용을 적용하기 위해 지금 다시 시작 버튼을 클릭하여 시스템을 재시작합니다.

사이트의 서버 개체 삭제하기

도메인 컨트롤러가 생성되면, 사이트 하위에 도메인 컨트롤러의 서버 개체가 생성됩니다. 서버 개체는 하위에 NTDS Settings 개체를 생성합니다. 도메인 컨트롤러에서 동작하는 다른 응용 프로그램 역시 동작하는데 필요한 개체를 서버 개체 하위에 생성할 수 있습니다. 도메인 컨트롤러를 제거한 후에 사이트 하위에 서버 개체를 삭제해야 합니다. 하지만 서버 개체를 삭제하기 전에 서버 개체 하위에 개체가 존재하는 지 확인 한 후, 하위 개체가 없는 경우에만 서버 개체를 삭제합니다.

[따라하기]

사이트의 서버 개체 삭제하기

Active Directory 사이트 및 서비스 관리 도구를 이용해서 서버 개체를 삭제하는 과정은 다음과 같습니다.

1. 시작 → 관리 도구 → Active Directory 사이트 및 서비스 메뉴를 선택하여, Active Directory 사이트 및 서비스 관리 도구를 실행합니다.
2. 콘솔 트리에 Sites를 클릭하여 확장 한 후, 제거한 도메인 컨트롤러가 속해 있는 사이트 개체를 클릭하여 확장합니다.
3. Servers를 클릭하여 확장 한 후, 제거한 도메인 컨트롤러의 서버 개체를 클릭하여 확장합니다.
   제거한 도메인 컨트롤러의 서버 개체 하위에 개체가 없는 것을 확인합니다.
4. 서버 개체를 삭제하기 위해 서버 개체를 마우스 오른쪽 버튼으로 클릭한 후, 삭제 메뉴를 선택합니다.
   〈그림 60〉의 예제에서는 DC02가 제거된 도메인 컨트롤러입니다. 다른 도메인 컨트롤러의 서버 개체는 하위에 NTDS Settings 개체가 존재하지만, 제거된 DC02는 하위에 개체가 존재하지 않는 것을 확인할 수 있습니다.

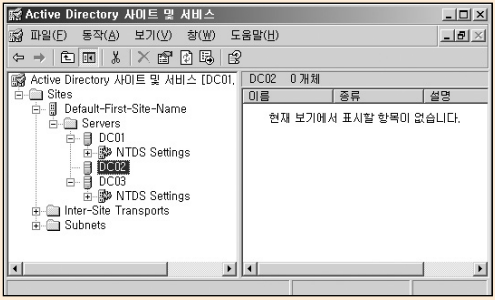

그림 60 하위 개체 유무 확인

5. 개체를 삭제할 것인지를 확인하는 대화 상자가 나타납니다. 예를 버튼을 클릭합니다.
6. 서버 개체가 삭제된 것을 확인 한 후, Active Directory 사이트 및 서비스 관리 도구를 종료합니다.

도메인 컨트롤러 강제 제거하기

기존에 동작중인 도메인 컨트롤러와 정상적으로 네트워크 통신을 하면서 도메인 컨트롤러를 제거할 수 없는 환경에서는 도메인 컨트롤러를 강제로 제거해야 합니다.

예를 들어 스키마 마스터로 동작 중이던 도메인 컨트롤러가 장시간 하드웨어 오류로 인해 중지된 상태에서, 다른 도메인 컨트롤러가 스키마 마스터 역할을 점유했습니다. 그 후 하드웨어 오류가 고쳐졌다고 해도 이전에 스키마 마스터로 동작 중이던 도메인 컨트롤러를 네트워크에 연결해서 사용하거나, 또는 dcpromo를 이용해서 정상적으로 도메인 컨트롤러를 제거할 수 없습니다. 만약 이전에 도메인 컨트롤러를 네트워크에 연결하면 포리스트에 두 개의 스키마 마스터가 동작하기 때문에 Active Directory 운영에 심각한 오류를 발생합니다. 따라서 이럴 경우에는 먼저 dcpromo /forceremoval 옵션을 이용해서 도메인 컨트롤러를 강제로 제거 한 후, 네트워크에 연결하여 다시 사용합니다.

dcpromo /forceremoval 옵션을 이용해서 도메인 컨트롤러를 강제 제거하는 것과 별개로 관리자는 추가적으로 Active Directory에 남아있는 강제 제거된 도메인 컨트롤러의 메타데이터를 삭제해야 합니다.

Active Directory에는 도메인 컨트롤러와 관련된 많은 양의 메타데이터가 저장됩니다. 정상적으로 도메인 컨트롤러를 제거하면, 이 메타데이터는 Active Directory에서 삭제됩니다. 하지만 도메인 컨트롤러 강제 제거는 도메인에 연결 없이 시스템에서만 Active Directory 관련 파일들을 삭제한 것이기 때문에 Active Directory에는 메타데이터가 그대로 남아 있습니다.

따라서 강제로 제거된 도메인 컨트롤러의 메타데이터는 ntdsutil.exe를 이용해서 제거합니다.

도메인 컨트롤러 강제 제거는 다음과 같은 순서로 진행합니다.

그림 61 도메인 컨트롤러 강제 제거 프로세스

Active Directory 강제 제거하기

dcpromo /forceremoval 옵션을 이용해서 도메인 컨트롤러에서 Active Directory를 강제로 제거 할 수 있습니다.

[따라하기]

Active Directory 강제 제거하기

1. 시작 → 실행 메뉴를 선택한 후, dcpromo /forceremoval를 입력하여 Active Directory 설치 마법사를 실행합니다.
2. Active Directory 설치 마법사가 실행됩니다. 다음 버튼을 클릭합니다.
3. 강제로 Active Directory 제거 페이지가 나타납니다. 간단한 도움말을 읽은 후, 다음 버튼을 클릭합니다.

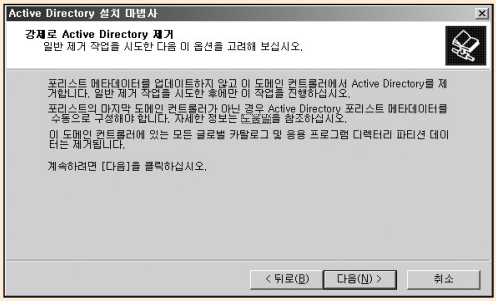

그림 62 Active Directory 강제 제거

4. 로컬 Administrator 계정의 암호를 설정합니다. 암호를 두 번 입력 후 다음 버튼을 클릭합니다.
5. 포리스트 메타데이터를 업데이트 하지 않고 이 컴퓨터에서 Active Directory를 제거한다는 요약 화면이 나타납니다. Active Directory를 제거하기 위해 다음 버튼을 제거합니다.
6. Active Directory를 구성하는 요소들을 제거하는 화면이 나타납니다. Active Directory 제거가 완료되면 마침 버튼을 클릭하여 Active Directory 설치 마법사를 종료합니다.
7. Active Directory 설치 마법사에 의해 변경된 내용을 적용하기 위해 지금 다시 시작 버튼을 클릭하여 시스템을 재시작합니다.

메타데이터 제거하기

도메인 컨트롤러를 강제로 제거한 경우에는 Active Directory에 남아 있는 도메인 컨트롤러의 메타데이터를 제거해야 합니다. 메타데이터는 ntdsutil.exe를 이용해서 제거할 수 있습니다.

Windows Server 2003 서비스 팩 1이 설치된 도메인 컨트롤러에서 ntdsutil.exe를 이용해서 메타데이터를 제거하면 자동으로 작업 마스터를 전송하거나 점유하는 작업을 수행합니다.

또한 파일 복제 서비스와 관련된 정보도 자동으로 제거합니다.

[따라하기]

메타데이터 제거하기

ntdsutil.exe를 이용해서 메타데이터를 제거하는 과정은 다음과 같습니다.

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행해서 Ntdsutil.exe를 실행합니다.
   ntdsutil
3. ntdsutil: 프롬프트에서 metadata cleanup를 입력하고 Enter 키를 누릅니다.
4. metadata cleanup: 프롬프트에서 connection를 입력하고 Enter 키를 누릅니다.
5. server connections: 프롬프트에서 다음 명령을 실행합니다.
   connect to server *servername*
   *servername*에 강제 제거한 도메인 컨트롤러의 메타데이터를 삭제하기 위해 연결할 도메인 컨트롤러의 이름을 입력합니다.
6. server connections: 프롬프트에서 quit를 실행합니다.
7. metadata cleanup: 프롬프트에서 select operation target를 입력하고 Enter 키를 누릅니다.

8. select operation target: 프롬프트에서 list sites를 입력하고 Enter 키를 누릅니다.
9. 현재 Active Directory에 구성되어 있는 사이트 목록이 출력됩니다. 메타데이터를 제거할 도메인 컨트롤러가 속해 있는 사이트를 선택하기 위해 select operation target: 프롬프트에서 다음 명령을 실행합니다.

   select site *sitenumber*

   *sitenumber*에는 출력된 사이트 목록에서 메타데이터를 제거할 도메인 컨트롤러가 속해 있는 사이트의 번호를 입력합니다.

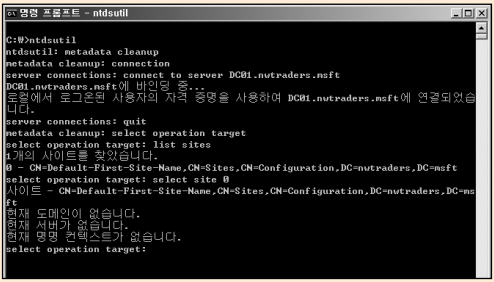

그림 63 사이트 선택

10. select operation target: 프롬프트에서 list domains in site를 입력하고 Enter 키를 누릅니다.
11. 9 단계에서 연결한 사이트에 존재하는 도메인의 목록이 출력됩니다. 메타데이터를 제거할 도메인 컨트롤러가 속해 있는 도메인을 선택하기 위해 select operation target: 프롬프트에서 다음 명령을 실행합니다.

    select domain *domainnumber*

    *domainnumber*에는 출력된 도메인 목록에서 메타데이터를 제거할 도메

인 컨트롤러가 속해 있는 도메인의 번호를 입력합니다.

12. select operation target: 프롬프트에서 list servers in site를 입력하고 Enter 키를 누릅니다.
13. 11 단계에서 연결한 도메인에 존재하는 도메인 컨트롤러의 목록이 출력됩니다. 메타데이터를 제거할 도메인 컨트롤러을 선택하기 위해 select operation target: 프롬프트에서 다음 명령을 실행합니다.

    select server *servernumber*

    *servernumber*에는 출력된 도메인 컨트롤러 목록에서 메타데이터를 제거할 도메인 컨트롤러의 번호를 입력합니다.
14. select operation target: 프롬프트에서 quit를 실행합니다.
15. 선택한 사이트에 속한 도메인의 도메인 컨트롤러의 메타데이터를 제거하기 위해 metadata cleanup: 프롬프트에서 다음 명령을 실행합니다.

    remove selected server
16. 〈그림 64〉와 같이 선택된 도메인 컨트롤러의 메타데이터를 제거할 것인지 확인하는 대화 상자가 나타납니다. 예 버튼을 클릭합니다.

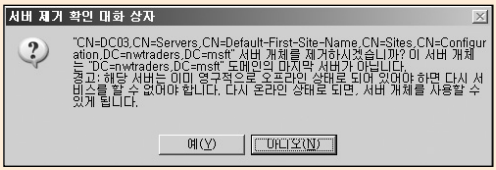

그림 64 서버 제거 확인 대화 상자

17. 메타데이터 제거가 완료되면, metadata cleanup: 프롬프트에서 quit를 실행합니다.
18. ntdsutil.exe를 종료하기 위해서 ntdsutil: 프롬프트에서 quit를 실행합니다.

사이트의 서버 개체 삭제하기

도메인 컨트롤러가 생성되면, 사이트 하위에 도메인 컨트롤러의 서버 개체가 생성됩니다.

서버 개체는 하위에 NTDS Settings 개체를 생성합니다. 도메인 컨트롤러에서 동작하는 다른 응용 프로그램 역시 동작하는데 필요한 개체를 서버 개체 하위에 생성할 수 있습니다. 도메인 컨트롤러를 제거한 후에 사이트 하위에 서버 개체를 삭제해야 합니다. 하지만 서버 개체를 삭제하기 전에 서버 개체 하위에 개체가 존재하는 지 확인 한 후, 하위 개체가 없는 경우에만 서버 개체를 삭제합니다. 사이트의 서버 개체를 삭제하는 자세한 과정은 도메인 컨트롤러 제거하기 파트를 참조하기 바랍니다.

Active Directory 백업과 복원

Active Directory 백업은 정기적인 관리 작업의 일환으로 모든 도메인 컨트롤러에서 주기적으로 수행해야 합니다. 반면에 Active Directory 복원은 정기적인 관리 작업은 아니지만, 오류가 발생한 도메인 컨트롤러를 이전 상태로 복원하기 위해 꼭 필요한 경우에 수행합니다.

시스템 상태 백업

Active Directory는 시스템이 정상적으로 동작하기 위해 서로 연관성이 있는 시스템 컴포넌트들의 모음인 시스템 상태의 일부분으로 백업됩니다. 시스템 상태를 구성하는 컴포넌트들은 모두 같이 백업되고 같이 복원되어야 합니다. 도메인 컨트롤러에서 시스템 상태 백업을 수행할 때 백업되는 시스템 컴포넌트는 다음과 같습니다.

- **시스템 시작(부팅) 파일들** : Windows Server 2003 운영 체제가 부팅하기 위해 필요한 파일들입니다.
- **레지스트리** : 운영 체제와 응용 프로그램이 시작하고 동작하는데 필요한 정보를 저장합니다.
- **클래스 등록 데이터베이스** : COM 개체들의 등록 정보를 저장하는 데이터베이스입니다.
- **시스템 볼륨(SYSVOL)** : 그룹 정책을 저장하는 파일들이 저장되어 있는 폴더로, 도메인 컨트롤러의 SYSVOL 폴더에는 다음과 같은 폴더와 파일들이 저장됩니다.
  - NETLOGON 공유 폴더
  - 사용자 로그온 스크립트

- 시스템 정책
- 그룹 정책 설정들
- 파일 시스템 정션
- 도메인 컨트롤러들과 복제를 위해 사용하는 파일 복제 준비 폴더들

• Active Directory : 다음과 같은 파일들이 저장됩니다.
- Active Directory 데이터베이스 파일 (NTDS.dit)
- 검사점 파일 (Edb.chk)
- 트랜젝션 로그 파일 (Edb*.log, Res*.log))

도메인 컨트롤러에 서버 클러스터나 인증서 서비스를 설치하면, 역시 시스템 상태 백업의 일부분으로 백업됩니다.

백업을 수행하는 목적

다음과 같은 이유 때문에 관리자는 도메인 컨트롤러의 시스템 상태 백업을 주기적으로 수행해야 합니다.

- 소프트웨어나 하드웨어 오류에 의해 부팅이나 정상적인 동작이 불가능한 도메인 컨트롤러를 복원합니다.
- 삭제된 Active Directory 개체를 복원합니다. 신뢰할 만한 복원(Authoritative Restore)을 이용해서, 개별 개체나 OU 또는 디렉터리 파티션에 모든 개체를 삭제 상태에서 복원할 수 있습니다.
- 원격 사이트에 복원한 시스템 상태 파일들을 이용해서 추가 도메인 컨트롤러를 설치합니다. Dcpromo /adv 옵션을 이용해서 대용량의 Active Directory 데이터베이스를 가진 도메인의 원격 사이트에 최소한의 WAN 구간 트래픽만을 유발하여 추가 도메인 컨트롤러를 설치할 수 있습니다.

백업 가이드라인

안정적인 Active Directory 복원을 위해 다음과 같은 가이드라인에 따라 백업을 수행할 것을 권장합니다.

- 일반 백업을 수행합니다. Windows Server 2003 백업 도구는 일반, 복사, 증분, 차등, 매일과 같은 다양한 백업 방식을 제공합니다. 하지만 Active Directory는 시스템 상태의 일부분으로 백업되기 때문에 일반 백업을 사용해야 합니다.
- 매일 도메인 안에 최소 두 대의 도메인 컨트롤러에서 백업을 수행합니다.
- 백업 미디어는 안전한 장소에 보관합니다.

시스템 상태 백업은 백업을 수행한 도메인 컨트롤러를 복원할 때만 사용 가능합니다. 또는 복원한 시스템 상태 파일들을 이용해서 같은 도메인의 추가 도메인 컨트롤러를 설치할 때도 사용할 수 있습니다.
시스템 상태 백업을 수행한 도메인 컨트롤러가 아닌 다른 도메인 컨트롤러를 복원할 수는 없습니다. 당연히, Windows 2000 Server 도메인 컨트롤러의 시스템 상태 백업으로 Windows Server 2003 도메인 컨트롤러를 복원할 수 없습니다.

백업 주기

얼마나 자주 백업을 수행할 것인지는 Active Directory 구성 환경에 따라 매우 다양합니다. 일반적인 Active Directory 환경에서 사용자나 컴퓨터 계정의 정보는 매일 수정됩니다. 예를 들어, 도메인 컨트롤러 계정을 포함해서 컴퓨터 계정은 30일마다 암호를 변경합니다. 따라서 매일 일정 퍼센트의 컴퓨터들은 암호를 변경합니다. 또한 사용자 계정의 암호도 만료되기 때문에 매일 일정 퍼센트의 사용자 암호도 변경됩니다. 따라서 도메인 컨트롤러를 자주 백업

할수록 복원할 때 문제가 적게 발생합니다. Active Directory 개체나 도메인 컨트롤러가 많을수록 더 자주 백업 할 것을 권장합니다.

예를 들어 대규모 포리스트에서 많은 개체가 들어 있는 OU를 삭제해서 복원해야 할 경우, 일주일 전에 생성한 백업으로 복원을 하면 복원한 OU에 최근 일주일 동안 생성되거나 수정된 개체는 다시 관리자가 수작업으로 일일이 복원을 해야 합니다. 따라서 복원 후에 개체를 생성하거나 수정하는 수작업을 최소화하기 위해서는 최신의 시스템 상태 백업이 항상 존재하도록 백업 주기를 설정합니다. Active Directory의 Tombstone lifetime 값은 도메인 컨트롤러가 삭제된 개체의 정보를 저장하는 기간을 지정합니다. 이 값은 또한 시스템 상태 백업의 유효 기간이기도 합니다. Active Directory는 Tombstone lifetime 값보다 오래된 시스템 상태 백업을 복원하는 것을 차단합니다. 따라서 Tombstone lifetime에서 정의한 기간 안에 최소한 하나 이상의 시스템 상태 백업을 수행해야만 복원이 가능합니다.

주기적인 시스템 상태 백업과 별개로 Active Directory를 구성하는 주요 환경에 변화가 발생하면, 바로 시스템 상태 백업을 수행합니다. 주기적인 시스템 상태 백업과 함께 다음과 같은 경우에 바로 시스템 상태 백업을 수행할 것을 권장합니다.

- Active Directory 데이터베이스 및 로그 파일을 이동
- 서비스 팩 설치나 운영 체제 업그레이드
- Active Directory 데이터베이스를 수정하는 핫픽스 설치
- 복원된 시스템 상태 파일들을 이용해서 추가 도메인 컨트롤러를 설치해야 할 경우
- 관리자에 의해 Tombstone lifetime이 값을 수정

백업 파일 명명 규칙

백업을 주기적으로 수행하면 많은 백업 파일이 생성되기 때문에, 복원시에 적절한 백업 파일을 빨리 찾을 수 있도록 백업 파일 이름에는 다음과 같은 정보들을 포함할 것을 권장합니다.

- 백업을 수행한 도메인 컨트롤러의 FQDN
- 도메인 컨트롤러의 빌드넘버와 서비스 팩 정보
- 글로벌 카탈로그 서버 유무
- Tombstone lifetime(TSL) 값
- 백업을 수행한 날짜

위에 정보를 포함한 백업 파일의 명명 규칙은 다음과 같습니다.
FQDN.Build_Number.Service_Pack, [No]GC.TSL.YYYYMMDD.bkf
예를 들어, 2005년 12월 01일에 Tombstone lifetime 값이 60일로 설정된 nwtraders.msft 도메인의 Windows Server 2003 SP1이 설치된 DC01 도메인 컨트롤러에서 수행한 백업 파일의 이름은 다음과 같습니다.
DC01.nwtraders.msft.3709.SP1.NoGC.60.20051201.bkf
만약 동일한 환경에서 DC01이 글로벌 카탈로그 서버로 동작 중이라면 백업 파일의 이름은 다음과 같습니다.
DC01.nwtraders.msft.3709.SP1.GC.60.20051201.bkf

시스템 상태 백업하기

소프트웨어나 하드웨어 오류에 의해 부팅이나 정상적인 동작이 불가능한 도메인 컨트롤러나 삭제된 Active Directory 개체를 복원하기 위해서는 시스템 상태 백업이 필요합니다. 또한 복원된 시스템 상태 파일들을 이용해서 원격 사이트에 추가 도메인 컨트롤러를 생성할 때도 시스템 상태 백업이 필요합니다.

시스템 상태 백업을 수행하기 위해 사용하는 Ntbackup.exe는 Active Directory 컴포넌트를 백업하기 위해 다양한 옵션을 제공합니다. 시스템 상태를 백업할 때, 시스템 보호 파일들을 포함 할 것인지 여부를 선택할 수 있습니다. 시스템 보호 파일들은 복원된 시스템 파일들을 이용해서 추가 도메인 컨트롤러를 생성할 때는 필요하지 않습니다. 만약 추가 도메인 컨트롤러를 생성하기 위해 시스템 상태 백업을 수행 한다면, 고급 옵션을 이용해서 시스템 보호 파일을 백업하지 않도록 설정할 수 있습니다. 시스템 보호 파일을 백업하지 않으면, 백업 파일의 크기가 줄어들고 또한 백업 및 복원 시간도 단축됩니다.

소프트웨어나 하드웨어 오류에 의해 부팅이나 정상적인 동작이 불가능한 도메인 컨트롤러나 삭제된 Active Directory 개체를 복원하기 위한 시스템 상태 백업은 반드시 시스템 보호 파일들을 백업해야 합니다.

시스템 상태 백업 수행하기

소프트웨어나 하드웨어 오류에 의해 부팅이나 정상적인 동작이 불가능한 도메인 컨트롤러나 삭제된 Active Directory 개체를 복원하기 위해 시스템 보호 파일을 포함하는 시스템 상태 백업을 수행하는 과정은 다음과 같습니다.

[따라하기]

시스템 상태 백업 수행하기

1. 시작 → 실행 메뉴를 선택한 후, ntbackup을 입력하여 백업 및 복원 마법사를 실행합니다.
2. 백업 및 복원 마법사가 실행됩니다. 다음 버튼을 클릭합니다.
3. 백업을 수행하기 위해 파일 및 설정 백업 옵션을 선택한 후, 다음 버튼을 클릭합니다.
4. 시스템 백업을 수행하기 위해 백업할 내용을 사용자가 선택 옵션을 선택한 후, 다음 버튼을 클릭합니다.
5. 백업할 항목에서 바탕화면 폴더를 확장한 후, 내 컴퓨터 폴더를 확장합니다. 〈그림 65〉와 같이 System State 항목을 선택 한 후, 다음 버튼을 클릭합니다.

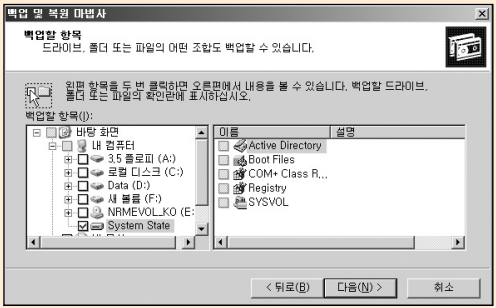

그림 65 백업할 항목 선택

6. 백업 파일을 저장할 폴더 경로를 입력합니다. 명명 규칙에 맞게 백업 이름을 입력한 후, 다음 버튼을 클릭합니다.

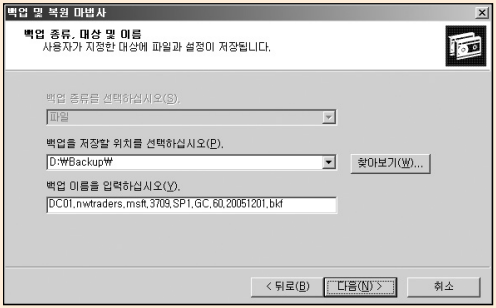

그림 66 백업 저장 경로 및 이름 지정

7. 백업 및 복원 마법사 완료 페이지가 나타납니다. 고급 버튼을 클릭합니다.
8. 백업 종류 목록에 일반이 선택되어 있는지 확인한 후, 다음 버튼을 클릭합니다.
9. 백업한 시스템 상태의 무결성을 확인하기 위해 백업 후 데이터 확인 옵션을 선택한 후, 다음 버튼을 클릭합니다.

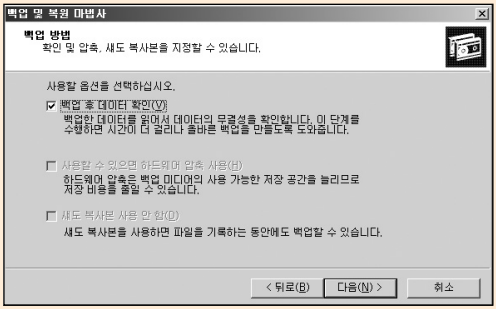

그림 67 백업 후 데이터 확인 옵션 선택

10. 데이터를 덮어쓰고, 백업 데이터에 소유자 및 관리자만이 접근할 수 있도록 설정할 지 여부를 선택합니다. 상황에 따라 적절한 옵션을 선택한 후, 다음 버튼을 클릭합니다.
11. 백업을 언제 수행할 지를 선택합니다. 지금 바로 시스템 상태 백업을 수행하기 위해 지금 시작 옵션을 선택한 후, 다음 버튼을 클릭합니다.
12. 설정한 옵션들이 모두 맞는지 확인 한 후, 시스템 상태 백업을 수행하기 위해 마침 버튼을 클릭합니다.

시스템 보호 파일을 제외한 시스템 상태 백업 수행하기

시스템 보호 파일을 백업하지 않으면, 백업 파일의 크기가 줄어들고 또한 백업 및 복원 시간도 단축됩니다. 추가 도메인 컨트롤러를 생성하기 위해 시스템 보호 파일을 제외한 시스템 상태 백업을 수행하는 과정은 다음과 같습니다.

[따라하기]

시스템 보호 파일을 제외한 시스템 상태 백업 수행하기

1. 시작 → 실행 메뉴를 선택한 후, ntbackup을 입력하여 백업 및 복원 마법사를 실행합니다.
2. 백업 및 복원 마법사 시작 페이지에서 고급 모드 링크를 클릭합니다.
3. 백업 유틸리티가 실행됩니다. 시스템 백업을 수행하기 위해 백업 탭을 클릭합니다.
4. 백업할 항목에서 System State 항목을 선택합니다.
5. 찾아보기 버튼을 클릭하여 백업을 저장할 경로 및 이름을 지정한 후, 백업 시작 버튼을 클릭합니다.

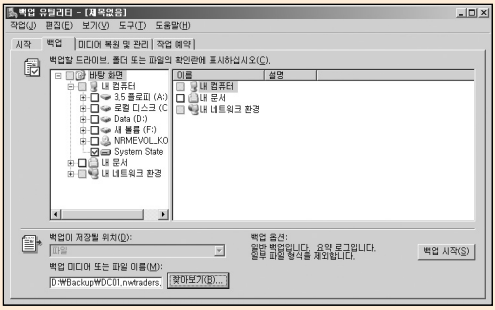

그림 68 백업 유틸리티

6. 백업 작업 정보 대화 상자가 나타납니다. 고급 버튼을 클릭합니다.

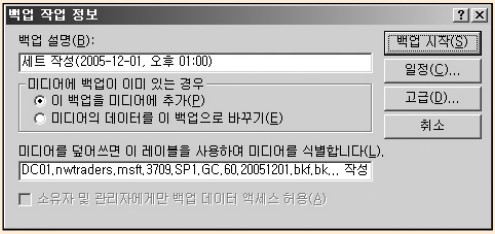

그림 69 백업 작업 정보

7. 고급 백업 옵션 대화 상자에서 시스템 상태를 포함하여 시스템 보호 파일을 자동으로 백업 옵션의 선택을 해제 한 후, 확인 버튼을 클릭합니다.

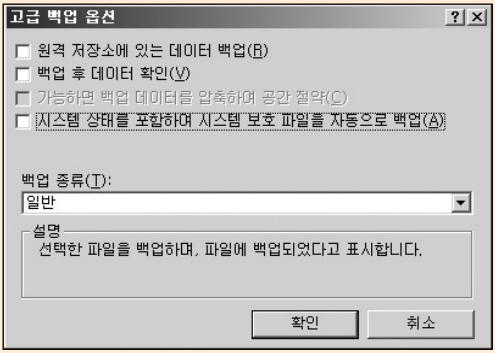

그림 70 고급 백업 옵션

8. 백업 시작 버튼을 클릭하여 시스템 상태 백업을 시작합니다.

9. 백업이 완료되면 닫기 버튼을 클릭한 후, 백업 유틸리티를 종료합니다.

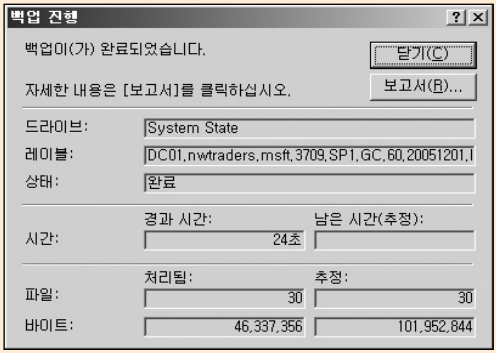

그림 71 백업 완료

도메인 컨트롤러에 신뢰할 수 없는 복원 수행하기

신뢰할 수 없는 복원(Non-Authoritative Restore)은 Active Directory를 복원하는 가장 기본적인 방법입니다. 신뢰할 수 없는 복원은 비정식 복원이라고도 부릅니다. 신뢰할 수 없는 복원을 수행하기 위해서는 도메인 컨트롤러를 디렉터리 서비스 복원 모드로 부팅해야 합니다.

Active Directory를 복원한 후에는 복제 파트너에 의해 복원된 백업이 수행된 후에 변경된 데이터들이 복제됩니다.

신뢰할 수 없는 복원은 도메인 컨트롤러를 백업을 수행했던 시점으로 돌려 놓습니다. 따라서 백업을 수행했던 시점 이후에 변경된 Active Directory 데이터는 다른 복제 파트너(도메인 컨트롤러)로부터 받아 동기화합니다.

신뢰할 수 없는 복원은 소프트웨어나 하드웨어 오류에 의해 도메인 컨트롤러가 더 이상 정상적인 동작이 불가능할 때 사용합니다. 신뢰할 수 없는 복원을 수행하여 오류가 발생한 도메인 컨트롤러를 백업을 수행한 시점으로 돌려 놓고, 복제를 통해 최신 Active Directory 데이터를 동기화 합니다.

만약 실수로 삭제된 특정 개체를 복원하길 원한다면, 신뢰할 수 없는 복원이 아닌 신뢰할 만한 복원을 수행해야 합니다. 신뢰할 수 없는 복원을 수행하면 복원된 도메인 컨트롤러에는 삭제된 특정 개체가 존재하지만, 복제 파트너와의 동기화를 통해 다시 삭제가 되기 때문에 원하는 목적을 달성할 수 없습니다.

도메인 컨트롤러에 신뢰할 수 없는 복원은 다음과 같은 순서로 진행합니다.

그림 72 신뢰할 수 없는 복원 프로세스

디렉터리 서비스 복원 모드로 부팅하기

신뢰할 수 없는 복원을 수행하기 위해서는 도메인 컨트롤러를 디렉터리 서비스 복원 모드로 부팅해야 합니다. 디렉터리 서비스 복원 모드로 도메인 컨트롤러를 부팅하면 더 이상 도메인 컨트롤러로 동작하지 않습니다.

디렉터리 서비스 복원 모드로 도메인 컨트롤러를 부팅하면 더 이상 도메인 계정을 사용해서 인증을 할 수 없기 때문에, 관리자는 로컬 SAM 데이터베이스에 저장된 로컬 Administrator 계정과 암호로 도메인 컨트롤러에 로그온 합니다. 로컬 Administrator 계정의 암호는 Active Directory 설치 마법사를 이용해서 Active Directory를 설치할 때 지정합니다.
도메인 컨트롤러를 물리적으로 접근이 가능한 경우에는 시스템을 재시작하면서 F8 키를 눌러서 디렉터리 서비스 복원 모드로 부팅하는 것이 가능합니다. 만약 관리자가 원격에서 관리 작업을 수행하는 경우에는 Boot.INI를 수정해서 도메인 컨트롤러를 디렉터리 서비스 복원 모드로 부팅합니다.
도메인 컨트롤러를 디렉터리 서비스 보원 모드로 부팅하는 자세한 과정은 Active Directory 데이터베이스 관리 파트를 참고하십시오.

시스템 상태 복원하기

소프트웨어나 하드웨어 오류에 의해 정상 동작이 불가능한 도메인 컨트롤러를 신뢰할 수 없는 복원을 이용해서 복구하기 위해 시스템 상태를 복원합니다. 시스템 상태 복원이 완료된 후에는 도메인 컨트롤러를 정상 상태로 재시작하면, 복제 파트너에 의해 최신 Active Directory 데이터가 동기화 됩니다.

[따라하기]

시스템 상태 복원하기

도메인 컨트롤러에 시스템 상태를 복원하는 과정은 다음과 같습니다.

1. 시작 → 실행 메뉴를 선택한 후, ntbackup을 입력하여 백업 및 복원 마법사를 실행합니다.
2. 백업 및 복원 마법사가 실행됩니다. 다음 버튼을 클릭합니다.
3. 복원을 수행하기 위해 파일 및 설정 복원 옵션을 선택한 후, 다음 버튼을 클릭합니다.

4. 복원할 항목에서 복원한 백업 파일을 확장합니다. 〈그림 73〉과 같이 System State를 선택한 후, 다음 버튼을 클릭합니다.

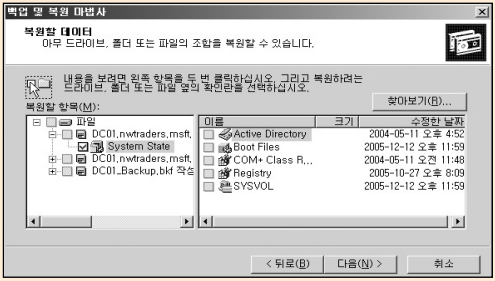

그림 73 복원할 데이터 선택

5. 백업 및 복원 마법사 완료 페이지가 나타납니다. 고급 버튼을 클릭합니다.
6. 복원할 위치를 지정합니다. 파일을 복원할 위치 목록에 원래 위치가 선택되어 있는지 확인 한 후, 다음 버튼을 클릭합니다.

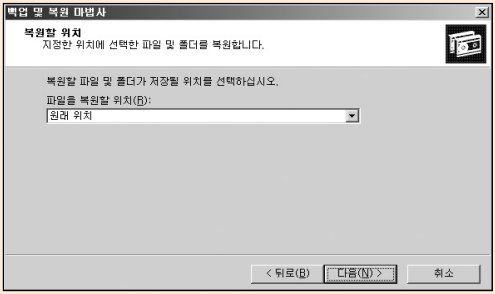

그림 74 복원할 위치 선택

7. 대체 위치로 복구하지 않으면 시스템 상태가 복구될 때 현재 시스템 상태를 덮어쓴다는 경고 메시지가 출력됩니다. 확인 버튼을 클릭합니다.
8. 컴퓨터에 이미 있는 파일을 복원하는 방법을 선택합니다. 기존 파일을 보존함(권장) 옵션이 선택되어 있는지 확인한 후, 다음 버튼을 클릭합니다.

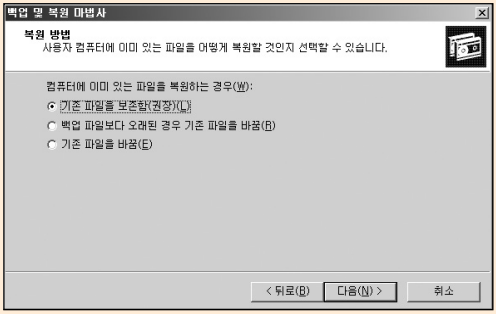

그림 75 복원 방법 선택

9. 고급 복원 옵션을 선택합니다. 〈그림 76〉과 같이 세 개의 고급 복원 옵션이 선택되어 있는지 확인한 후, 다음 버튼을 클릭합니다.

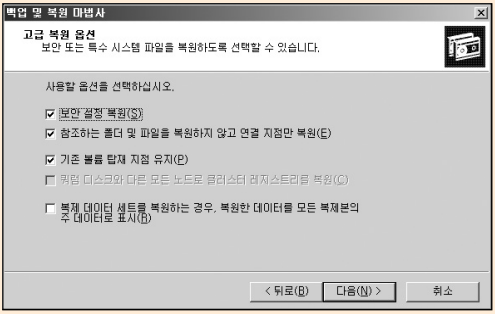

그림 76 고급 복원 옵션 선택

10. 설정한 옵션들이 모두 맞는지 확인 한 후, 시스템 상태 복원을 시작하기 위해 마침 버튼을 클릭합니다.
11. 복원이 완료되면 닫기 버튼을 클릭합니다.
12. 일부 파일 및 설정의 복원을 완료하기 위해 시스템을 재시작 할 것을 묻는 대화 상자가 나타납니다. 예 버튼을 클릭하여 도메인 컨트롤러를 재시작합니다. 도메인 컨트롤러가 정상 상태로 재시작하면, 복제 파트너에 의해 최신 Active Directory 데이터가 동기화 됩니다.

Active Directory 개체에 신뢰할 만한 복원 수행하기

신뢰할 만한 복원은 정식 복원이라고도 부릅니다. 신뢰할 만한 복원(Authoritative Restore)은 지정된 개체나 OU를 백업된 시점으로 복원합니다. 예를 들어, 관리자가 실수로 삭제한 OU를 복원해야 한다면 신뢰할 만한 복원을 수행합니다. 만약 신뢰할 수 없는 복원을 수행한다면, 시스템 상태 복원으로 복구된 OU는 동기화 과정을 거치면서 다시 삭제됩니다.
신뢰할 만한 복원을 수행하기 위해 관리자는 신뢰할 수 없는 복원과 마찬가지로 시스템 상태 백업을 도메인 컨트롤러에 복원합니다. 시스템 상태 복원 후에 바로 도메인 컨트롤러를 재시작하지 않고, 복원할 OU에 마킹 작업을 수행합니다. 마킹 된 OU는 도메인 컨트롤러를 재시작하여 동기화 작업이 수행될 때 다른 도메인 컨트롤러로 복제 되어 복구 됩니다.
복원할 개체에 마킹을 하면, 다른 도메인 컨트롤러에 존재하는 삭제된 개체의 버전보다 높은 버전이 설정되기 때문에, 동기화 할 때 시스템 상태를 복원한 도메인 컨트롤러의 마킹한 개체가 다른 도메인 컨트롤러로 복제되어 복구됩니다.

신뢰할 만한 복원은 실수로 삭제된 개체나 OU 전체를 복원할 때 매우 유용합니다. 하지만 도메인 컨트롤러를 복원하는 용도로는 사용하지 않습니다. 도메인 컨트롤러를 복원 해야 한다면 신뢰할 수 없는 복원을 사용합니다.
사용자 계정이 삭제되었을 때, 신뢰할 만한 복원을 이용해서 사용자 계정을 마킹하여 복원이 가능합니다. 하지만 사용자 계정이 복구될 때 사용자 계정이 속해 있는 그룹 구성원 정보는 상황에 따라 자동으로 복구 될 수도 있고, 자동으로 복구가 되지 않아 수동으로 복구 해야 할 수도 있습니다. 사용자 계정이 복구 될 때 그룹 구성원 자동 복구 여부는 그룹이 생성될 때 또는 그룹에 사용자 계정이 구성원으로 포함될 때 포리스트의 기능 수준에 따라 달라집니다.

포리스트 기능 수준이 Windows Server 2003 임시 또는 Windows Server 2003일 때, 생성된 그룹이거나 사용자 계정이 그룹의 구성원으로 추가되면, 신뢰할 수 있는 복원을 이용해서 사용자 계정이 복원 될 때 자동으로 그룹 구성원 정보가 복원됩니다. 반면에 포리스트 기능 수준이 Windows Server 2003 임시 또는 Windows Server 2003이 아닐 때, 생성된 그룹이거나 사용자 계정이 그룹의 구성원으로 추가되면, 신뢰할 수 있는 복원을 이용해서 사용자 계정이 복원 될 때 자동으로 그룹 구성원 정보가 복원되지 않습니다. 따라서 사용자 계정을 복원한 후 추가적으로 그룹 구성원 정보도 복원해야 합니다.

신뢰할 수 있는 복원을 이용해서 개체를 복원할 때 ntdsutil.exe를 사용합니다. Ntdsutil.exe는 개체를 복원할 때 포리스트 기능 수준에 따라 그룹 구성원 정보를 복원할 수 있습니다. 예를 들어, Gildong.Hong 사용자 계정이 삭제되었습니다. 이 계정은 포리스트 기능 수준이 Windows 2000일 때 생성된 그룹 G1의 구성원입니다. 또한 포리스트 기능 수준을 Windows Server 2003으로 올린 후에 생성된 그룹 G2의 구성원이기도 합니다.
신뢰 할 수 있는 복원을 이용해서 Gildong.Hong 사용자 계정을 복원하면, 포리스트 기능 수준이 Windows Server 2003일 때 생성된 그룹 G2의 구성원에 Gildong.Hong 사용자 계정이 자동으로 포함되어 복원됩니다. 반면에 포리스트 기능 수준이 Windows 2000일 때 생성된 그룹 G1의 구성원에 Gildong.Hong 사용자 계정은 복원되지 않습니다.
Windows Server 2003 서비스 팩 1에서 제공하는 ntdsutil.exe는 포리스트 기능 수준이 Windows 2000일 때 생성된 그룹 구성원 정보를 복원할 수 있도록 LDIF 파일을 생성하는 기능을 제공합니다.
삭제된 Active Directory 개체를 복원하기 위한 신뢰할 수 있는 복원은 다음과 같은 순서로 진행합니다.

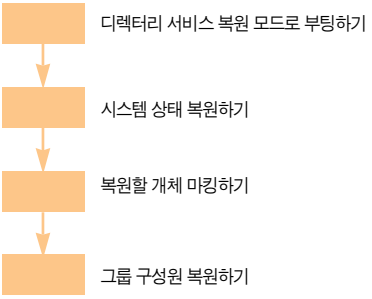

그림 77 신뢰할 수 있는 복원 프로세스

아래 설명하는 신뢰할 수 있는 복원 예제에서는 nwtraders.msft 도메인의 본사 OU에 실수로 삭제된 Gildong.Hong 계정을 복원합니다. Gildong.Hong 계정은 G1 그룹과 G2 그룹의 구성원입니다. G1 그룹은 포리스트 기능 수준이 Windows 2000일 때 생성 되었고, G2 그룹은 포리스트 기능 수준을 Windows Server 2003으로 올린 후에 생성한 그룹입니다.

그림 78 복원 예제

디렉터리 서비스 복원 모드로 부팅하기

신뢰할 수 있는 복원을 수행하기 위해서는 도메인 컨트롤러를 디렉터리 서비스 복원 모드로 부팅해야 합니다. 디렉터리 서비스 복원 모드로 도메인 컨트롤러를 부팅하면 더 이상 도메인 컨트롤러로 동작하지 않습니다.

디렉터리 서비스 복원 모드로 도메인 컨트롤러를 부팅하면 더 이상 도메인 계정을 사용해서 인증을 할 수 없기 때문에, 관리자는 로컬 SAM 데이터베이스에 저장된 로컬 Administrator 계정과 암호로 도메인 컨트롤러에 로그온 합니다. 로컬 Administrator 계정의 암호는 Active Directory 설치 마법사를 이용해서 Active Directory를 설치할 때 지정합니다.

도메인 컨트롤러를 물리적으로 접근이 가능한 경우에는 시스템을 재시작하면서 F8 키를 눌러서 디렉터리 서비스 복원 모드로 부팅하는 것이 가능합니다. 만약 관리자가 원격에서 관리 작업을 수행하는 경우에는 Boot.INI를 수정해서 도메인 컨트롤러를 디렉터리 서비스 복원 모드로 부팅합니다.

도메인 컨트롤러를 디렉터리 서비스 보원 모드로 부팅하는 자세한 과정은 Active Directory 데이터베이스 관리 파트를 참고하십시오.

시스템 상태 복원하기

삭제된 개체를 복원하기 위해서 도메인 컨트롤러에 시스템 상태를 복원합니다. 신뢰할 수 없는 복원을 수행할 경우에는 시스템 상태를 복원한 후에 바로 도메인 컨트롤러를 정상 상태로 재시작합니다.
하지만 신뢰할 수 있는 복원의 경우에는 시스템 상태를 복원한 후, 복원할 개체를 마킹하는 작업이 필요합니다. 마킹 작업 후에 시스템을 재시작합니다.

[따라하기]

시스템 상태 복원하기

도메인 컨트롤러에 시스템 상태를 복원하는 과정은 다음과 같습니다.

1. 시작 → 실행 메뉴를 선택한 후, ntbackup을 입력하여 백업 및 복원 마법사를 실행합니다.
2. 백업 및 복원 마법사가 실행됩니다. 다음 버튼을 클릭합니다.
3. 복원을 수행하기 위해 파일 및 설정 복원 옵션을 선택한 후, 다음 버튼을 클릭합니다.
4. 복원할 항목에서 복원한 백업 파일을 확장합니다. 복원할 백업의 System State를 선택한 후, 다음 버튼을 클릭합니다.
5. 백업 및 복원 마법사 완료 페이지가 나타납니다. 고급 버튼을 클릭합니다.
6. 복원할 위치를 지정합니다. 파일을 복원할 위치 목록에 원래 위치가 선택되어 있는지 확인 한 후, 다음 버튼을 클릭합니다.
7. 대체 위치로 복구하지 않으면 시스템 상태가 복구될 때 현재 시스템 상태를 덮어쓴다는 경고 메시지가 출력됩니다. 확인 버튼을 클릭합니다.

8. 컴퓨터에 이미 있는 파일을 복원하는 방법을 선택합니다. 기존 파일을 보존함(권장) 옵션이 선택되어 있는지 확인한 후, 다음 버튼을 클릭합니다.
9. 고급 복원 옵션을 선택합니다. 〈그림 76〉과 같이 세 개의 고급 복원 옵션이 선택되어 있는지 확인한 후, 다음 버튼을 클릭합니다.
10. 설정한 옵션들이 모두 맞는지 확인 한 후, 시스템 상태 복원을 시작하기 위해 마침 버튼을 클릭합니다.
11. 복원이 완료되면 닫기 버튼을 클릭합니다.
12. 일부 파일 및 설정의 복원을 완료하기 위해 시스템을 재시작 할 것을 묻는 대화 상자가 나타납니다. 복원할 개체에 대한 마킹 작업을 수행하기 위해 아니오 버튼을 클릭합니다.

복원할 개체 마킹하기

관리자의 실수로 삭제된 개체를 마킹하여 복원합니다. 복원할 개체에 마킹을 하면, 다른 도메인 컨트롤러에 존재하는 삭제된 개체의 버전보다 높은 버전이 설정되기 때문에, 동기화 할 때 시스템 상태를 복원한 도메인 컨트롤러의 마킹 한 개체가 다른 도메인 컨트롤러로 복제되어 복구됩니다. Ntdsutil.exe를 이용해서 복원할 개체의 DN을 지정하면, 다른 도메인 컨트롤러로 마킹된 개체가 복제됩니다.

[따라하기]

복원할 개체 마킹하기

ntdsutil.exe를 이용해서 복원할 개체를 마킹하는 과정은 다음과 같습니다.

1. 명령 프롬프트를 실행합니다.

2. 다음 명령을 실행해서 Ntdsutil.exe를 실행합니다.
   ntdsutil
3. ntdsutil: 프롬프트에서 authoritative restore를 입력하고 Enter 키를 누릅니다.
4. 복원할 개체에 마킹을 하기 위해 authoritative restore: 프롬프트에서 다음 명령을 실행합니다.
   restore object *DistinguishedName*
   *DistinguishedName*에 복원할 개체의 DN을 입력합니다.
   본사 OU에 삭제된 Gildong.Hong 계정을 마킹하기 위해서는 다음 명령을 실행합니다.
   restore object "CN=Gildong.Hong,OU=본사,DC=nwtraders,DC=msft"
5. 정식 복원을 수행할 것인지를 묻는 대화 상자가 나타납니다. 예 버튼을 클릭합니다.
6. 〈그림 79〉와 같이 4 단계에서 지정한 개체에 대한 마킹 과정이 수행 됩니다. 예제에서 복원한 Gildong.Hong 계정은 G1, G2 그룹의 구성원입니다. G2 그룹은 포리스트 기능 수준을 Windows Server 2003으로 올린 후 생성한 그룹이기 때문에 Gildong.Hong 계정을 마킹함으로써 구성원 정보도 같이 복원됩니다. 하지만 G1 그룹은 포리스트 기능 수준이 Windows 2000일 때 생성된 그룹이기 때문에 자동으로 구성원 정보가 복원되지 않습니다. 따라서 시스템 재시작 후에 복제가 완료되면 Gildong.Hong 계정은 복원됨과 동시에 G2 그룹의 구성원에 포함되어 있지만, G1 그룹의 구성원에는 포함되어 있지 않습니다.
   Windows Server 2003 서비스 팩 1에서 제공하는 ntdsutil.exe는 포리스트 기능 수준이 Windows 2000일 때 생성된 그룹의 구성원도 복원할 수 있도록 〈그림 79〉와 같이 ldif 파일을 생성해 줍니다.

도메인 컨트롤러를 재시작한 후에 ldif 파일을 이용해서 복원되지 않는 그룹의 구성원 정보도 복원할 수 있습니다.

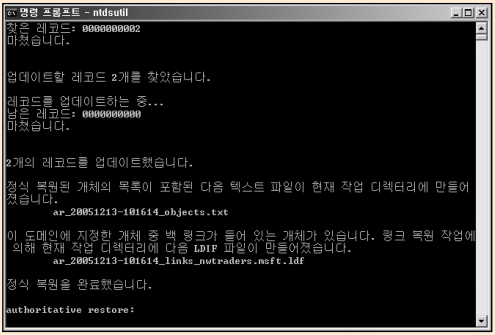

그림 79 복원할 개체에 대한 마킹 작업 수행

7. 복원할 개체에 대한 마킹이 완료되면, authoritative restore: 프롬프트에서 quit를 실행합니다.
8. ntdsutil.exe를 종료하기 위해서 ntdsutil: 프롬프트에서 quit를 실행합니다.
9. 마킹한 개체가 다른 도메인 컨트롤러로 복제되어 복원 되도록 도메인 컨트롤러를 재시작합니다.

그룹 구성원 복원하기

처음 포리스트를 구성했을 때 바로 포리스트 기능 수준을 Windows Server 2003으로 생성한 후 사용자 계정 및 그룹 계정을 생성하고, 그룹 구성원을 추가하는 작업을 수행했다면 그룹 구성원 복원하기 과정은 생략합니다.

왜냐하면 삭제된 계정을 복원할 때, 포리스트 기능 수준이 Windows Server 2003일 때 생성된 그룹의 구성원은 계정을 마킹하여 복원 할 때, 계정이 속한 그룹의 구성원까지도 복원해 주기 때문입니다.

하지만 포리스트 기능 수준이 Windows 2000일 때 생성된 그룹의 구성원은 계정을 마킹하여 복원할 때, 계정이 속한 그룹의 구성원 정보를 복원해 주지 않습니다. 따라서 ntdsutil.exe가 계정을 마킹할 때 생성해 준 LDIF 파일을 Import하여 계정을 그룹의 구성원에 포함시키는 작업을 수행해야 합니다.

[따라하기]

그룹 구성원 복원하기

예제에서는 포리스트 기능 수준이 Windows 2000일 때 생성된 G1 그룹의 구성원 정보는 복원되지 않았습니다. 따라서 ntdsutil.exe가 생성해 준 LDIF(예제에서는 ar_20051213-101614_links_nwtraders.msft.ldf) 파일을 Import 하여 Gildong.Hong 계정을 G1 그룹의 구성원에 포함시킵니다. 포리스트 기능 수준이 Windows 2000일 때 생성된 그룹의 구성원 정보를 복원 하는 과정은 다음과 같습니다.

1. 명령 프롬프트를 실행합니다.
2. 다음 명령을 실행해서 그룹 구성원 정보를 복원합니다.

   ldifde -i -k -f *FileName*

   *FileName*에 복원할 그룹 구성원 정보를 저장하고 있는 LDIF 파일 이름을 입력합니다.

3. 〈그림 80〉과 같이 정상적으로 LDIF 파일의 내용이 Import 된 것을 확인한 후, 명령 프롬프트를 종료합니다.

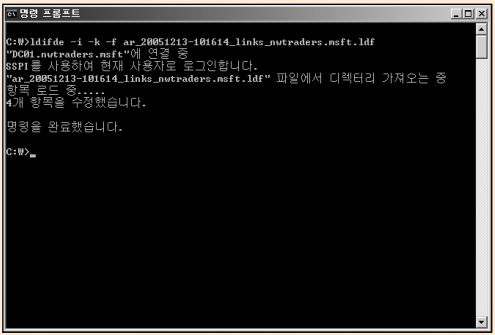

그림 80 LDIF Import

문제 해결

Active Directory는 정상적으로 동작하기 위해 많은 서비스들과 상호 의존하는 분산 시스템입니다. 특정 서비스에 발생한 오류는 Active Directory가 동작하는 데 필요한 다른 서비스에도 영향을 미치며, 사용자 인증 및 권한 부여를 통해 회사의 주요 보안 인프라로써 동작하는 Active Directory가 정상적으로 동작하지 않으면 업무에 치명적인 영향을 미칩니다.
관리자는 컴퓨터나 서비스에 발생한 문제를 인지하고, 오류가 발생한 정확한 Active Directory 구성 요소를 찾아내서 문제를 해결해야 합니다.
일반적인 경우에 관리자는 다음과 같은 상황이 발생하면 문제 해결을 시도합니다.

- 이벤트 로그에 기록된 오류 이벤트
- MOM과 같은 전문 모니터링 서비스에 발생한 경고
- IT 관리자나 사용자에 의해 보고된 이상 증상

오류 메시지에 대한 대응

이벤트 로그에 이벤트가 기록되면, 먼저 이벤트 로그에 오류 메시지를 기록한 Net Logon이나 파일 복제 서비스 같은 원본을 파악합니다. 로그를 기록한 원본과 이벤트 ID를 이용해서 Microsoft Knowledge Base를 검색하면 쉽게 오류의 원인 및 해결 방안을 얻을 수 있습니다.

모니터링 경고에 대한 대응

Active Directory 운영 환경에 따른 적절한 모니터링 시스템을 구축합니다. 모니터링 시스템에서 발생하는 경고는 다양하며, 이벤트 로그에 비해 실시간으

로 오류를 인지하여 즉시 대응할 수 있다는 장점이 있습니다. 모니터링 경고가 발생하면 이벤트 로그에 기록된 오류 메시지와 함께 오류의 원인을 파악하고, 문제 해결을 시도합니다.

보고된 이상 증상에 대한 대응

IT 관리자나 사용자에 의해 보고된 이상 증상을 기반으로 Active Directory 문제 해결을 시도해야 한다면, 정의된 문제 해결 방안을 순차적으로 수행하면서 정확한 오류의 원인을 파악해야 합니다. 아래에 "문제 해결 프로세스"는 오류의 원인을 파악하고 해결할 때까지 문제를 해결하는 단계별 프로세스를 제공합니다.

문제 해결 프로세스

이벤트 로그 또는 Active Directory 시스템을 모니터링 하는 과정이나 IT 관리자 또는 사용자의 이상 증상 보고에 의해 관리자는 운영중인 Active Directory에 오류가 발생한 것을 감지합니다. 이때 다음과 같은 문제 해결 프로세스를 단계적으로 수행하여 오류의 원인을 파악하고, 빠른 시간 안에 문제를 해결할 수 있습니다.

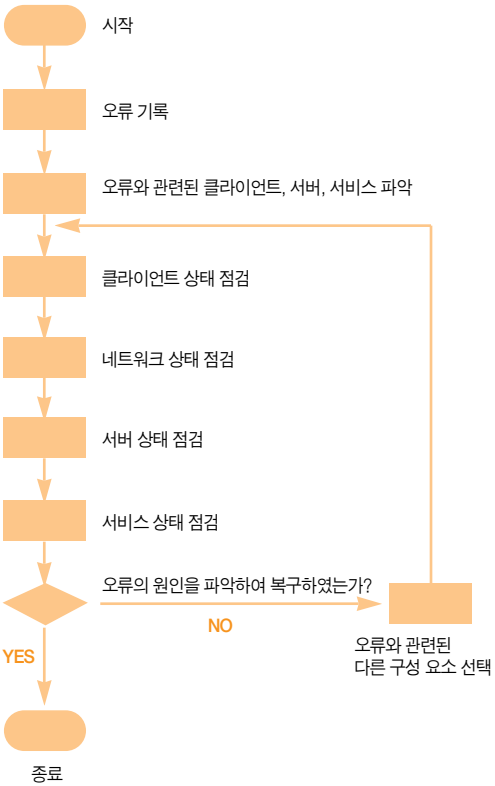

그림 81 문제 해결 프로세스

오류 기록

오류와 관련된 정보를 기록함으로써 오류의 원인을 잘못 파악하는 문제를 제거할 수 있고, 기록된 정보를 이용해서 장애의 원인과 해결 방안을 보다 빠르게 파악할 수 있습니다. 또한 오류에 대한 기록은 향후 유사한 오류에 대해 빠른 문제 해결 방안을 제공합니다. 오류를 Active Directory를 구성하는 시스템의 이벤트 로그나 모니터링 시스템에서 발생한 경고를 통해 파악하였다면 사용자들이 장애를 인지하기 전에 바로 문제 해결을 수행합니다.

오류가 발생했다는 것을 사용자의 이상 증상 보고에 의해 파악하였다면 최대한 빠른 시간 내에 문제를 해결하여 사용자가 업무를 보는데 지장을 받지 않도록 합니다.

정확한 오류 분석 및 문제 해결을 위해 다음과 같은 정보를 기록할 것을 권장합니다.

- 오류가 발생한 날짜와 시간
- 오류 번호와 메시지
- 다음과 같은 클라이언트 정보
  - 컴퓨터 이름
  - 로그온 사용자 계정
  - TCP/IP 구성 정보
  - 클라이언트에 설정되어 있는 DNS 서버 목록
  - 클라이언트 운영체제 및 서비스 팩 정보
- 다음과 같은 서버 정보
  - 컴퓨터 이름
  - TCP/IP 구성 정보
  - 서버 운영체제 및 서비스 팩 정보

- 네트워크 정보
  - 클라이언트 도메인 이름
  - 서버 도메인 이름
- 응용 프로그램 이름과 관련 설정
- 서비스 이름과 관련 설정

추가해서 다음과 같은 정보도 파악하여 기록합니다.

- 오류 재연 가능한가? 재연이 가능하다면 오류를 유발하는 과정
- 클라이언트에 발생한 장애의 경우에 동일 증상이 다른 클라이언트에서도 발생하는가?
- 유사한 장애가 이미 보고 되어, 원인 파악 및 장애 복구 방안 중인가?

오류와 관련된 클라이언트, 서버, 서비스 파악

발생한 오류와 관계가 있는 Active Directory 컴포넌트가 어떤 것인지 파악합니다. 보고된 오류와 연관 관계가 있는 Active Directory 컴포넌트를 파악하는 것이 때에 따라서 쉬울 수도 있고 어려울 수도 있지만, 이를 정확히 파악함으로써 오류의 원인을 찾는데 많은 시간을 절약할 수 있습니다.

클라이언트 상태 점검

클라이언트와 서버 사이에 통신은 대부분 클라이언트에서 먼저 요구 사항을 서버에 전송하기 때문에 문제 해결을 위해 클라이언트의 상태를 점검합니다. 클라이언트는 적절한 환경 설정이 되어 있어야 하고, 네트워크에 정상적으로 연결되어 동작해야 합니다.
다음과 같이 클라이언트의 상태를 점검합니다.

- 네트워크에 정상적으로 연결되어 있는지 점검합니다.
- IP 주소, DNS 서버 주소와 같은 TCP/IP 설정을 점검합니다.

- 시스템 모니터를 이용해서 클라이언트의 CPU 사용률이 높지 않은지 점검합니다.

네트워크 상태 점검

다음과 같이 클라이언트와 서버 사이의 네트워크가 정상 동작 중인지 점검합니다.

- Ping 명령어를 이용해서 클라이언트와 서버 사이에 네트워크가 정상 연결되어 있는지 점검합니다. 클라이언트와 서버 네트워크의 연결에 문제가 있다면 방화벽 설정, IPSec 정책, NAT 구성, Windows XP에 포함되어 있는 개인 방화벽 설정을 점검합니다.
- 기본적인 네트워크 연결에는 이상이 없지만, 클라이언트와 서버 사이의 응용 프로그램에 의한 패킷이 정상적으로 연결되지는 확인하기 위해서 네트워크 모니터를 이용합니다.

서버 상태 점검

서버 상태를 점검하기 위해서, 클라이언트에서 수행했던 점검과 동일한 점검을 수행합니다.

- 네트워크에 정상적으로 연결되어 있는지 점검합니다.
- IP 주소, DNS 서버 주소와 같은 TCP/IP 설정을 점검합니다.
- 시스템 모니터를 이용해서 서버의 CPU 사용률이 높지 않은지 점검합니다.

서비스 상태 점검

앞의 점검을 통해 클라이언트와 서버의 기본적인 설정과 상태에 이상이 없다면, 오류와 관련된 서비스에 대한 점검이 필요합니다.
다음과 같이 서비스의 상태를 점검합니다.

- 서비스가 정상적으로 설치되어 구성되어 있는지 점검합니다.
- 서비스가 정상 동작 중인지 점검합니다.
- 이벤트 로그에 서비스와 관련된 로그가 기록되어 있는지 점검합니다.
- 사용자나 클라이언트가 서비스에 접근하여 명령을 수행할 수 있는 권한을 가지고 있는지 점검합니다.

오류와 관련된 다른 구성 요소 선택

만약 앞의 단계들을 수행하면서 오류의 원인을 파악하지 못했다면, 오류와 관련된 다른 요소가 있는지 파악합니다. 때에 따라서 장애와 직접적인 연관이 없어 보이는 다른 클라이언트나 서버에 의해 장애가 발생할 수도 있기 때문입니다. Active Directory는 논리적, 물리적 구성 요소가 상호 유기적으로 동작을 하기 때문에 한 구성 요소의 작은 오류가 다른 곳에 오류를 유발할 수 있습니다. 따라서 오류의 원인을 찾아 낼 때까지 연관 관계가 있는 Active Directory 구성 요소들을 계속해서 점검합니다.

문제 해결을 위해 도메인 컨트롤러 사전 준비

Active Directory에 발생한 오류의 원인을 파악하고 문제를 해결하기 위해, 도메인 컨트롤러에 적절한 사전 준비를 수행해야 합니다. 사전 준비는 오류의 원인을 파악하고 문제를 해결할 때 사용할 수 있는 다양한 도구들을 설치하는 과정입니다.

문제 해결을 위해 도메인 컨트롤러에 다음과 같은 사전 준비를 수행할 것을 권장합니다.

Windows Server 2003 서비스 팩 1 설치하기

가능하면 모든 도메인 컨트롤러에 Windows Server 2003 서비스 팩 1을 설치합니다. Windows Server 2003 서비스 팩 1을 설치함으로써 ntdsutil.exe의 향상된 기능을 문제 해결 시 사용할 수 있습니다. Windows Server 2003 서비스 팩 1에서 제공하는 ntdsutil.exe는 도메인 컨트롤러의 메타데이터를 제거하고, 삭제된 개체를 복원하기 위해 신뢰할 수 있는 복원을 수행할 때 그룹 멤버쉽 복원하는 새로운 기능이 추가되었습니다.

Windows Support Tools 설치하기

향상된 오류 분석 및 문제 해결을 위해 Windows Server 2003 서비스 팩 1에서 제공하는 Windows Support Tools를 설치합니다. Windows Server 2003 서비스 팩 1에서 제공하는 Windows Support Tools는 향상된 버전의 Dcdiag.exe와 Repadmin.exe 도구를 포함하고 있습니다.

Dcdiag.exe 도구는 DNS 분석 테스트 및 복제 동작 상태에 대한 레포팅 기능을 제공합니다.

Repadmin.exe 도구는 개별 컴퓨터의 레지스트리를 수정하지 않고 다수의 도메인 컨트롤러의 복제 관련 설정을 변경 관리 할 수 있는 기능을 제공합니다.

Windows Server 2003 서비스 팩 1이 설치된 모든 도메인 컨트롤러에 Windows Server 2003 서비스 팩 1에서 제공하는 Windows Support Tools를 설치할 것을 권장합니다.

Windows Server 2003 Resource Kit 설치하기

향상된 오류 분석 및 문제 해결을 위해 Windows Server 2003 Resource Kit을 Microsoft 웹 사이트에서 다운로드 받아 설치할 것을 권장합니다. Windows Server 2003 Resource Kit은 linkd.exe, Ntfrsutl.exe와 같은 오류 분석 및 문제 해결을 위한 도구를 제공합니다.

네트워크 모니터 설치하기

컴퓨터 사이에 네트워크 트래픽을 분석하여 네트워크 연결 이슈 문제를 해결하기 위해 네트워크 모니터를 사용합니다.

로그 레벨 설정하기

만약 이벤트 뷰어의 디렉터리 서비스 로그에 기록된 정보가 문제 해결에 필요한 충분한 정보를 제공하지 못할 경우에는 다음 레지스트리의 엔트리 값을 수정하여 로그 레벨을 설정합니다.

HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics

기본 설정으로 모든 엔트리의 로그 레벨은 최소한의 정보만 기록하는 0으로 설정되어 있습니다. 가장 높은 로그 레벨은 5이며, 로그 레벨을 높일수록 더 상세한 정보가 디렉터리 서비스 로그에 기록됩니다.

오류 분석을 위해 Active Directory 관련 구성 요소에 대한 로그 레벨을 5로 설정합니다. 그 후 문제가 해결되면 상세 로그 기록에 의해 불필요한 부하가 발생하는 것을 막기 위해 다시 로그 레벨을 0으로 설정합니다.

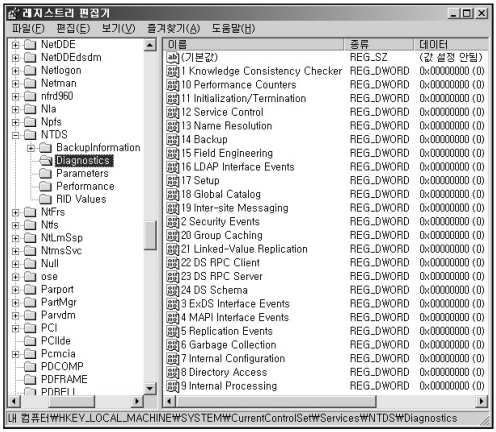

그림 82 로그 레벨 설정 가능한 디렉터리 서비스 엔트리

도메인 컨트롤러의 높은 CPU 사용률 문제 해결하기

도메인 컨트롤러의 CPU 사용률이 높은 것으로 모니터링 되면, 〈그림 83〉의 문제 해결 프로세스를 이용해서 오류 원인 및 문제 해결을 시도합니다.

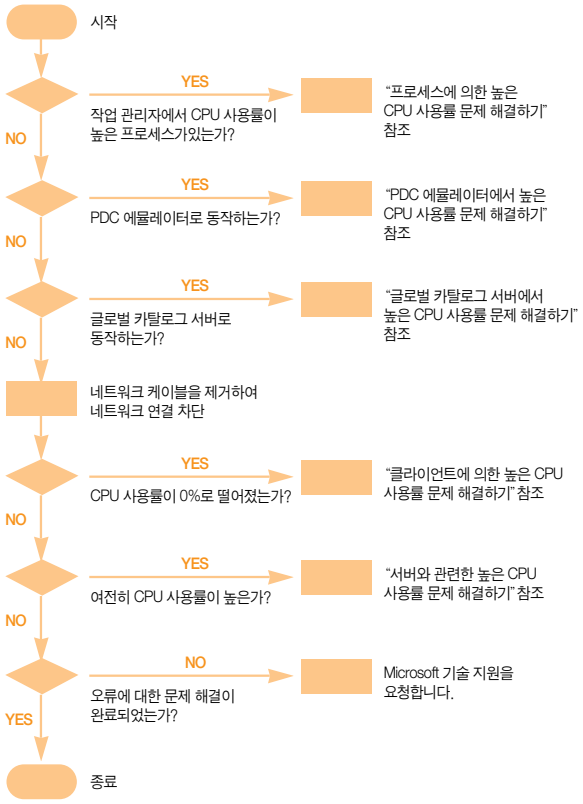

그림 83 도메인 컨트롤러의 높은 CPU 사용률 문제 해결 프로세스

프로세스에 의한 높은 CPU 사용률 문제 해결하기

프로세스나 서비스가 도메인 컨트롤러의 CPU를 많이 사용할 경우에는 〈그림 84〉의 문제 해결 프로세스를 이용해서 오류 원인 및 문제 해결을 시도합니다.

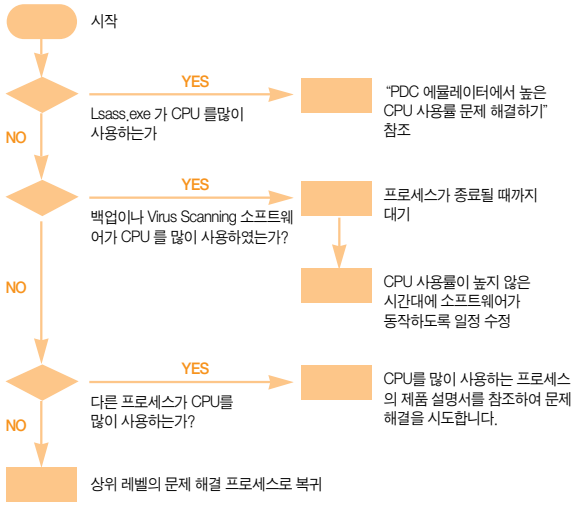

그림 84 프로세스에 의한 높은 CPU 사용률 문제 해결 프로세스

PDC 에뮬레이터에서 높은 CPU 사용률 문제 해결하기

만일 Lsass.exe 프로세스가 CPU를 많이 사용할 경우에는 도메인 컨트롤러가 PDC 에뮬레이터로 동작 중인지 점검합니다. 도메인 컨트롤러가 PDC 에뮬레이터로 동작 중일 경우에는 〈그림 85〉의 문제 해결 프로세스를 이용해서 오류 원인 및 문제 해결을 시도합니다.

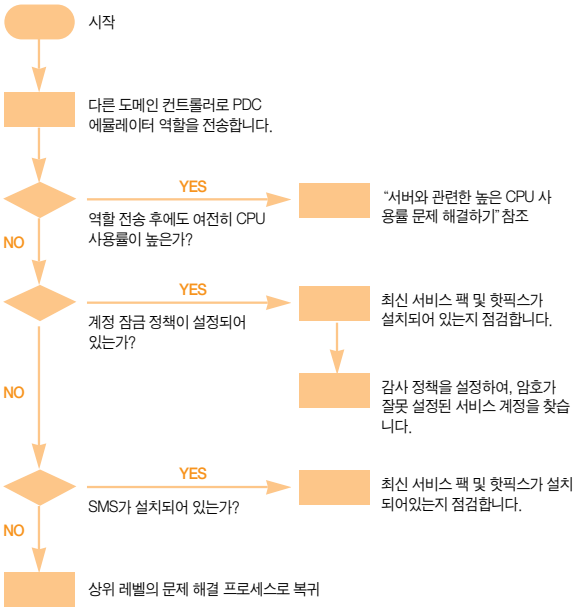

그림 85 PDC 에뮬레이터에서 높은 CPU 사용률 문제 해결 프로세스

글로벌 카탈로그 서버에서 높은 CPU 사용률 문제 해결하기

Lsass.exe 프로세스가 CPU를 많이 사용하는 도메인 컨트롤러가 PDC 에뮬레이터가 아니면, 도메인 컨트롤러가 글로벌 카탈로그 서버로 동작 중인지 점검합니다. 도메인 컨트롤러가 글로벌 카탈로그 서버로 동작 중일 경우에는 〈그림 86〉의 문제 해결 프로세스를 이용해서 오류 원인 및 문제 해결을 시도합니다.

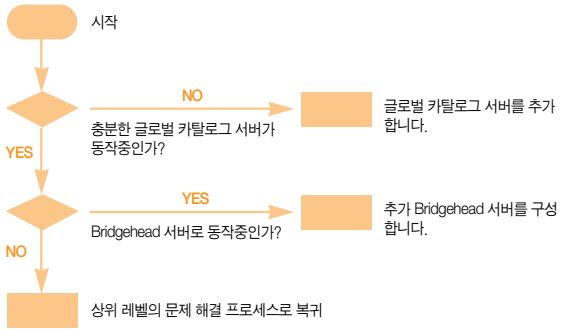

그림 86 글로벌 카탈로그 서버에서 높은 CPU 사용률 문제 해결 프로세스

클라이언트에 의한 높은 CPU 사용률 문제 해결하기

Lsass.exe 프로세스가 CPU를 많이 사용하는 도메인 컨트롤러가 PDC 에뮬레이터나 글로벌 카탈로그 서버로 동작 하지 않는다면, 도메인 컨트롤러에 연결된 네트워크 케이블을 뽑아서 네트워크 연결을 차단합니다. 만일 CPU 사용률이 0%로 떨어지면 높은 CPU 사용률은 클라이언트에 의해 발생한 것이므로 〈그림 87〉의 문제 해결 프로세스를 이용해서 오류 원인 및 문제 해결을 시도합니다. ADPerf.exe를 실행하여 CPU를 많이 사용하는 LDAP 검색 쿼리가 있는지 점검합니다. 또한 특정 클라이언트가 도메인 컨트롤러에 부하를 발생시키면, 부하를 발생시키는 클라이언트에 대한 문제 해결을 시도합니다.

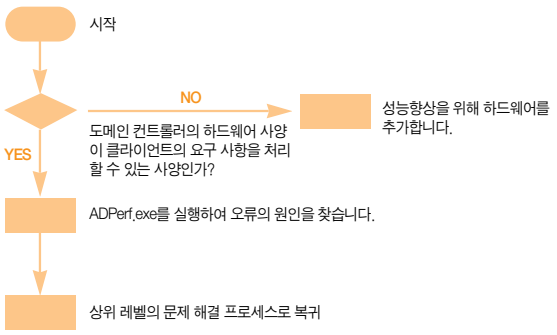

그림 87 클라이언트에 의한 높은 CPU 사용률 문제 해결 프로세스

서버와 관련한 높은 CPU 사용률 문제 해결하기

만일 도메인 컨트롤러를 네트워크에서 분리해도 여전히 CPU 사용률이 높다면 〈그림 88〉의 문제 해결 프로세스를 이용해서 오류 원인 및 문제 해결을 시도합니다. Garbage collection과 Security event에 대한 로그 레벨을 수정하여 ACL을 수정하는 프로세스가 있는지를 점검합니다.

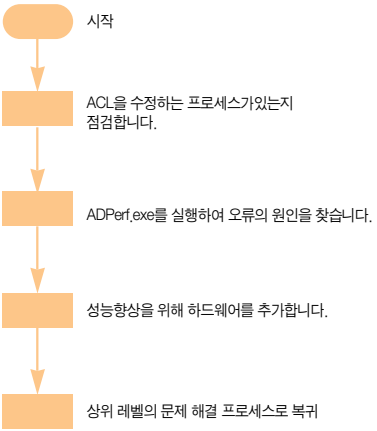

그림 88 서버와 관련한 높은 CPU 사용률 문제 해결 프로세스

마치면서

지면 관계상 Active Directory에 대한 개요 및 설계에 대한 내용을 담지는 못했지만, 본 Active Directory 운영 가이드는 Active Directory를 관리하기 위해 반드시 알아야 할 작업들에 대해 설명하고 있습니다. 비록 작은 포켓 가이드 북이지만 Active Directory를 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