HP CIFS Server 3.0d 관리자 설명서
버전 A.02.02

HP-UX 11i v1 및 v2

제4판

제품 제조 번호: B8725-90096

E0306

알림

이 설명서의 내용은 예고 없이 변경될 수 있습니다.

HP는 이 자료에 대해 상업성이나 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여 어떤 종류의 보증도 하지 않습니다. HP는 설명서의 오류나 이 제품의 공급, 수행, 또는 사용에 따른 직접, 간접, 특별, 부수적, 파생적 손해에 대해 책임을 지지 않습니다.

보증서 HP 제품에 적용되는 특정 보증서 사본과 교체 부품은 지역 대리점이나 서비스 센터에서 구할 수 있습니다.

제한된 권한 설명 미합중국 정부에 의한 사용, 복제 또는 공개는 미국방성 정부 기관의 경우 DFARS 2 52.227-7013의 Rights in Technical Data and Software 부속 조항 (c) (1) (ii)에 기술된 제한이 적용됩니다. 그리고 기타 기관의 경우 FAR 52.227-19의 Commercial Computer Software Restricted Rights 부속 조항 (c) (1) 및 (c) (2)에 기술된 제한이 적용됩니다.

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto, California 94304 U.S.A.

함께 제공된 설명서, 플로피 디스크 또는 테이프 카트리지는 본 제품에서만 사용 가능합니다.

HP CIFS Server는 Open Source Samba 제품을 기반으로 하며 GPL 라이센스를 따릅니다.

상표권 UNIX는 The Open Group의 등록 상표입니다.

목차

1. HP CIFS Server 소개

2. HP CIFS Server 설치 및 구성

목차

3. Windows NT/XP/2000에서 HP-UX 파일 액세스 권한 관리

4. NT 스타일 도메인

5. Windows 2000/2003 도메인

6. LDAP 통합 지원

목차

7. Winbind 지원

8. HP CIFS Server A.01에서 A.02로 업데이트

9. HP CIFS 배포 모델

목차

10. HP CIFS Server 보안

11. HA HP CIFS 구성

12. HP CIFS용 HP-UX 구성

설명서 정보

이 설명서에서는 HP CIFS Server 제품을 설치, 구성 및 관리하는 방법에 대해 설명합니다. HP CIFS Server 제품과 함께 제공된 *The Samba HowTo Collection* 및 *Using Samba, 2nd* 서적의 내용을 보충하고 추가 HP-UX 고유의 변형, 기능 및 권장 사항에 대해 설명합니다. 이 설명서와 함께 이전에 릴리즈된 설명서도 *http://www.docs.hp.com*에서 온라인으로 구할 수 있습니다.

대상 독자

이 설명서는 HP CIFS Server 제품을 사용한 경험이 있는 사용자를 대상으로 합니다. HP CIFS Server에 대한 자세한 내용은 *http://www.docs.hp.com*에서 온라인으로 제공되는 기타 HP CIFS Server 설명서를 참조하십시오.

설명서의 새로운 내용

새로운 설명서에는 HP CIFS Server 3.0d 버전 A.02.02의 변경 사항이 다음과 같이 들어 있습니다.

- MS Windows 2000/2003 ADS 도메인의 프린터 발행 지원
- winbind를 이용한 `idmap_rid` 기능 지원
- samba 하위 스키마 변경 사항 지원
- `smb.conf` 파일의 구성 매개 변수 변경 사항 지원

표기법

표 1 **설명서 표기법**

정보 유형	글꼴	예제
화면에 표시되는 내용, 프로그램/스크립트 코드 및 명령 이름 또는 매개 변수	Monotype	> user logged in.
텍스트 강조 표현, 한글 설명서 제목	**고딕체**	보드를 제거하기 **전에** 전원이 꺼져 있는지 확인해야 합니다.
제목 및 하위 제목	**굵은체**	**관련 설명서**

발행 정보

표 2 **자세한 발행 정보**

설명서 제품 번호	지원되는 운영 체제	지원되는 제품 버전	발행 날짜
B8725-90023	11.0, 11i v1	A.01.08	2002년 3월
B8725-90060	11.0, 11i v1, v2	A.01.10	2003년 9월
B8725-90061	11.0, 11i v1, v2	A.01.11	2004년 2월
B8725-90066	11.0, 11i v1, v2	A.01.11.01	2004년 6월
B8725-90074	11i v1, v2	A.02.01	2004년 12월
B8725-90088	11i v1, v2	A.02.01.01	2005년 2월
B8725-90096	11i v1, v2	A.02.02	2005년 10월

설명서 내용

이 설명서에서는 HP CIFS Server 제품을 설치, 구성, 관리 및 사용하는 방법을 설명합니다. 이 설명서의 구성은 다음과 같습니다.

표 3 **설명서 구성**

장	설명
HP CIFS Server 소개	HP CIFS Server, Samba 및 HP CIFS Server를 기반으로 하는 Open Source Software 제품군을 설명합니다.
HP CIFS Server 설치 및 구성	HP CIFS Server 제품의 설치 및 구성 방법을 설명합니다.
Windows/NT/XP/2000에서 HP-UX 파일 액세스 권한 관리	Windows NT, XP 및 2000 클라이언트에서 HP CIFS Server의 UNIX 파일 사용 권한 및 POSIX 액세스 제어 목록(ACL)을 확인 및 변경하는 방법을 설명합니다.
NT 스타일 도메인	HP CIFS Server를 PDC 또는 BDC로 설정하고 구성하는 방법을 설명합니다. 그리고 HP CIFS Server를 Windows 2000 이전 버전과 호환되는 컴퓨터로 NT 스타일 도메인, Samba 도메인 또는 Windows 2000/2003 도메인에 참여시키는 프로세스를 설명합니다.
Windows 2000/2003 도메인	Kerberos 보안을 사용하여 Windows 200x 도메인에 HP CIFS Server를 참여시키는 프로세스를 설명합니다.
LDAP 통합 지원	HP Netscape Directory, HP LDAP-UX 통합 제품 및 LDAP 기능이 지원되는 HP CIFS Server 소프트웨어의 설치, 구성 및 검증 방법을 설명합니다.
Winbind 지원	`winbind`가 지원되는 HP CIFS Server를 설정 및 구성하는 방법을 설명합니다.

표 3 **설명서 구성(계속)**

장	설명
HP CIFS Server A.01에서 A.02로 업데이트	Samba 2.2가 기반이 되는 HP CIFS Server A.01.* 버전과 Samba 3.0이 기반이 되는 HP CIFS Server A.02.* 버전 간의 차이에 대해 설명합니다. 사용자가 CIFS를 사용하는 네트워크를 계획하고 업그레이드할 수 있도록 업데이트 절차를 설명합니다.
HP CIFS 배포 모델	세 가지 HP CIFS 배포 모델인 Samba 도메인, Windows 도메인 및 통합 도메인을 설치, 설정 및 구성하는 절차를 설명합니다.
HP CIFS Server 보안	HP CIFS Server를 보호하는 데 사용하는 네트워크 보안 방법을 설명합니다.
HA HP CIFS 구성	활성-대기 또는 활성-활성 고가용성 구성에 필요한 절차를 설명합니다.
HP CIFS용 HP-UX 구성	HP CIFS Server의 HP-UX 조정 절차를 설명합니다.
GNU GPL 라이센스	GNU GPL(General Public License)을 설명합니다.

사용자 의견 접수

HP에서는 이 설명서와 관련된 사용자의 의견과 제안을 받습니다. HP는 사용자 요구를 충족하는 설명서를 만들기 위해 최선을 다할 것입니다. 의견이 있으시면 netinfo_feedback@cup.hp.com으로 보내 주십시오.

의견을 보내실 때 다음 정보를 함께 적어주십시오.

- 설명서의 전체 제목 및 제품 번호. 제품 번호는 인쇄본 설명서와 PDF 버전 설명서의 제목 페이지에 나와 있습니다.

- 의견과 관련된 내용의 절과 페이지 번호
- 사용 중인 HP-UX 버전

1 HP CIFS Server 소개

이 장에서는 본 설명서, HP CIFS, HP CIFS Server의 기반이 되는 Open Source Software 제품군인 Samba 정보, Samba 소스에 대한 HP의 개선 사항 등에 대한 일반

적인 소개와 아울러 HP CIFS에 사용할 수 있는 다양한 설명서 자료를 제공합니다.

HP CIFS 소개

HP CIFS는 HP-UX에 Microsoft CIFS(일반 인터넷 파일 시스템) 프로토콜에 기반한 분산 파일 시스템을 제공합니다. HP CIFS는 HP-UX에 CIFS 프로토콜의 서버 및 클라이언트 구성 요소를 모두 구현합니다.

최신 HP CIFS Server(A.02.01 버전)는 검증된 개방형 소스 소프트웨어인 Samba 버전 3.0.7을 기반으로 하며 Windows NT, XP, 2000 및 HP-UX 컴퓨터를 포함하여 HP CIFS Client 소프트웨어를 실행하는 CIFS Client에 파일 및 인쇄 서비스를 제공합니다.

HP CIFS Client를 사용하면 HP-UX 사용자가 HP CIFS Server를 실행 중인 Windows 서버 및 HP-UX 컴퓨터를 포함한 CIFS 파일 서버를 UNIX 파일 시스템 공유로 마운트할 수 있습니다. HP CIFS Client는 Windows NTLM 인증 프로토콜을 구현하는 선택적인 PAM(Pluggable Authentication Module)도 제공하므로, HP-UX의 PAM 시스템 내에 설치하고 구성할 경우, PAM NTLM은 HP-UX 사용자가 Windows 인증 서버에 대해 인증되도록 합니다.

CIFS 프로토콜의 개념

CIFS(일반 인터넷 파일 시스템)는 원격 파일 액세스를 위한 Windows 사양입니다.

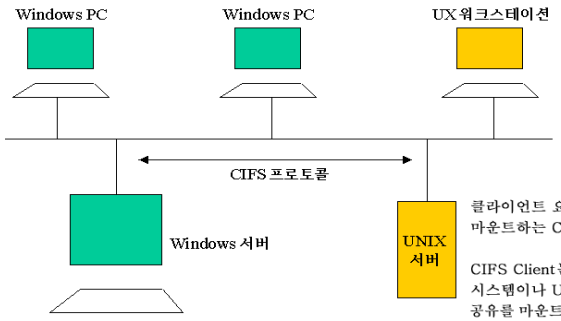
CIFS는 1980년대 후반에 막 태동하던 LAN 기술(예: 이더넷)을 통해 PC간에 파일을 공유하기 위해 개발된 서버 메시지 블록(SMB) 프로토콜이라고도 하는 네트워킹 프로토콜에서 시작되었습니다. SMB는 Microsoft Windows 95, Windows NT, XP 및 OS/2 운영 체제의 기본 파일 공유 프로토콜이며 수백만의 PC 사용자가 회사 인트라넷을 통해 파일을 공유하는 데 사용하는 표준 방식입니다.

CIFS는 SMB에서 이름만 바꾼 것이며 CIFS와 SMB는 모든 실제 용도에 있어서 동일합니다. 현재 Microsoft에서는 "CIFS"를 사용하도록 권장하지만 "SMB"도 여전히 사용되고 있습니다. 또한 CIFS는 UNIX, VMS(tm), Macintosh 및 다른 플랫폼에서도 폭넓게 사용됩니다.

CIFS는 실제로 파일 시스템은 아닙니다. 엄밀하게 말하자면 CIFS는 원격 파일 액세스 프로토콜이며 원격 시스템의 파일에 대한 액세스를 제공합니다. CIFS는 호스트 시스템의 파일 시스템 상단에 위치하여 호스트 시스템의 파일 시스템과 작동합니다. CIFS는 서버와 클라이언트 모두를 정의합니다. CIFS Client는 CIFS Server의 파일에 액세스하는 데 사용됩니다.

HP CIFS는 HP-UX 컴퓨터에서 CIFS 프로토콜을 사용하여 HP-UX 서버의 디렉토리가 Windows 컴퓨터에 마운트되도록 하며 반대의 경우도 가능합니다.

CIFS 패러다임



CIFS Server가 설치되어 있으면 UNIX 시스템은 네트워크에서 또 다른 Windows 서버 역할을 할 수 있습니다. 네트워크상의 UNIX 워크스테이션은 CIFS Client를 사용하여 UNIX 서버에서 CIFS 공유를 액세스할 수도 있습니다. 따라서, UNIX 환경에서는 CIFS로 NFS를 대체할 수 있습니다.

Open Source Software(OSS) Samba 제품군

HP CIFS Server 소스는 1991년에 호주의 Andrew Tridgell이 개발한 Open Source Software(OSS) 프로젝트인 Samba에 기반을 두고 있습니다. 이 절에서는 Samba 제품에 대해 매우 간략히 소개합니다. 웹 사이트나 대부분의 서점에서 Samba 관련 서적을 많이 찾아볼 수 있습니다. 이 중에서 일부는 Samba 팀 구성원이 작성한 것입니다. 따라서 이 제품에 대한 자세한 정보를 보려면 이러한 자료를 사용하는 것이 좋습니다.

Open Source Software

Samba는 GNU Public License(GPL) 조항에 의거하여 HP와 다른 사용자가 사용할 수 있게 되었습니다. 이는 Samba가 "무료 소프트웨어", 즉 어떠한 저작권의 제약도 받지 않음을 의미합니다. 이러한 유형의 소프트웨어는 새로운 소프트웨어를 협력하여 개발하도록 장려하는 목적을 갖고 있습니다.

GNU Public License에 대한 자세한 내용을 보려면 http://www.fsf.org 웹 사이트를 참조하십시오.

Samba 서버 설명 및 기능

Samba 제품군 프로그램을 사용하면 UNIX 및 UNIX와 유사한 운영 체제를 실행하는 시스템에서 Microsoft 네트워킹 프로토콜을 사용하여 서비스를 제공할 수 있습니다. 이 기능을 통해 Microsoft에서 제공하는 기본 네트워킹 클라이언트를 사용하는 DOS 및 Windows 컴퓨터에서 UNIX 파일 시스템 및/또는 프린터에 액세스할 수 있습니다.

사용자는 "네트워크 환경"에서 UNIX 파일 시스템을 드라이브 문자 또는 아이콘으로 보게 되며 마치 사용자의 로컬 시스템에 저장된 것처럼 Windows 프로그램에서 파일을 열 수 있습니다.

이를 위해 Samba는 TCP/IP 상의 NetBios 상단에 서버 메시지 블록(SMB) 네트워킹 프로토콜을 구현합니다.

Samba 및 해당 프로토콜에 대한 자세한 내용은 Robert Eckstein, David Collier-Brown 및 Peter Kelly가 쓴 *Using Samba*의 1장과 2장을 참조하십시오.

Samba 웹 사이트에 액세스하려면 http://www.samba.org로 이동하십시오.

Samba 설명서: 서적 및 온라인

HP CIFS 제품 사용 시 `/opt/samba/docs` 디렉토리에 있는 제품과 함께 제공된 *The Samba HOWTO Collection* 및 *Samba-3 by Example*을 참조하는 것이 좋습니다. 참고 서적 *Using Samba, 2nd Edition*은 `/opt/samba/swat/using_samba`에서도 찾을 수 있습니다. 세 권의 참고 서적 모두 SWAT(Samba 웹 관리 도구)를 통해 사용할 수 있습니다.

중요

*Using Samba, 2nd Edition*은 이전 버전의 Samba(V.2.0.4)에 대해 설명합니다. 하지만 **이 책**의 대부분의 내용은 현재 버전의 CIFS Server에도 적용할 수 있습니다. HP CIFS Server에 관하여 가장 정확한 정보를 보려면 HP에서 제공한 Samba 맨페이지나 SWAT 도움말 기능을 사용해야 합니다.

HP CIFS Server 관리자 설명서는 *http://www.docs.hp.com* 웹 사이트에서도 볼 수 있습니다.

다음은 현재 HP에서 공급하지 않은 Samba 설명서의 목록입니다.

- Official Samb-3 HOWTO and Reference Guide by John H. Terpstra and Jelmer R. Vernooij, Editors, ISBN: 0-13-145355-6.
- Samb-3 By Example Practical exercises to Successful Deployment by John H. Terpstra, ISBN: 0-13-147221-6.
- Using Samba, 2nd Edition Robert Eckstein, David Collier-Brown, Peter Kelly and Jay Ts. (O'Reilly, 2000), ISBN: 0-596-00256-4.
- Samba, Integrating UNIX and Windows by John D Blair (Specialized Systems Consultants, Inc., 1998), ISBN: 1-57831-006-7.
- Samba 웹 사이트: http://www.samba.org/samba/docs.

참고

HP에서 공급하지 않은 Samba 설명서에는 종종 Samba의 이후 릴리즈에 예정된 기능에 대한 설명이 포함되어 있습니다. 이러한 책의 저자가 어떤 기능이 기존 릴리즈에 존재하고 어떤 기능이 Samba의 이후 릴리즈에서 사용할 수 있는지에 대한 정보를 항상 제공하지는 않습니다.

HP CIFS Server의 향상된 기능

HP CIFS Server A.02.01에는 여러 가지 향상된 기능이 통합되었습니다. 다음 절에서는 각각의 향상된 부분에 대해 전반적으로 설명합니다. 다음과 같은 절이 있습니다.

- 백업 도메인 컨트롤러(BDC) 기능(버전 A.02.01의 새 기능)
- Winbind 기능(버전 A.02.01의 새 기능)
- HP CIFS 배포 모델(버전 A.02.01의 새 기능)
- 새로운 인증 시스템 지원(버전 A.02.01의 새 기능)

참고

HP CIFS Server A.02.* 버전에서는 LDAP-UX 통합 제품인 J4269AA를 설치해야 합니다.

백업 도메인 컨트롤러(BDC) 기능(버전 A.02.01)

HP CIFS Server 버전 A.02.01은 주 도메인 컨트롤러(PDC) 역할을 수행하는 도메인에서 BDC를 지원할 수 있게 다음과 같은 향상된 기능을 제공합니다.

- HP CIFS Server PDC에 대해 BDC로 사용할 수 있는 기능
- Windows NT, XP, SP2 및 Windows 200x를 포함한 Windows 클라이언트에서 BDC로 사용할 수 있는 기능
- Windows NT 로그온 스크립트 지원
- Microsoft의 "Server manager for Domain" 도구를 사용하여 Samba BDC의 자원 보기
- 로컬 및 로밍 프로파일 지원
- Samba 서버에 대한 특정 로그온 홈 공유 지원

BDC 지원 설정 및 구성에 대한 자세한 내용은 이 설명서의 5장을 참조하십시오.

Winbind 기능(버전 A.02.01)

Winbind는 Windows 사용자 및 그룹을 HP-UX UID 및 GID로 확인하는 Samba 제품군 프로그램의 구성 요소입니다. Winbind는 NSS 루틴인 /etc/lib/libnss_winbind.1을 제공합니다. 이 루틴은 winbind 데몬, winbindd에 연결하여 ID 매핑을 수행합니다.

Winbind는 HP-UX UID/GID 및 Windows SID(보안 ID) 간에 데이터 매핑을 저장하는 winbind_idmap.tdb라고 하는 데이터베이스를 유지 관리합니다. idmap backend를 ldapsam:ldap://<ldap server name>으로 지정한 경우 winbind는 로컬 매핑 파일을 사용하는 대신에 LDAP 디렉토리 서버에서 이 정보를 가져옵니다.

HP CIFS Server가 Windows NT 또는 Windows 2000/2003 도메인 컨트롤러를 사용하여 구성원 서버로 Windows 도메인에 참여하는 경우 HP CIFS Server에서는 Windows 사용자를 위한 UID 및 GID를 생성하고 매핑할 수 있도록 winbind를 지원합니다.

winbind 지원을 사용하는 HP CIFS Server 설정 및 구성 방법에 대한 자세한 내용은 이 설명서의 9장을 참조하십시오.

HP CIFS 배포 모델(버전 A.02.01)

HP CIFS Server A.02.01에서는 세 가지 배포 도메인 모델인 Samba 도메인 모델, Windows 도메인 모델 및 통합 도메인 모델을 제공합니다. 이러한 세 가지 모델은 일반적인 네트워크 환경을 나타내며 HP CIFS Server의 융통성을 보여 줍니다.

Samba 도메인 모델, Windows 도메인 모델 및 Unified 도메인 모델에 대한 설정 및 구성 방법에 대한 자세한 내용은 이 설명서의 11장을 참조하십시오.

새로운 인증 시스템(버전 A.02.01)

smbpasswd 및 LDAP 인증 백엔드에 대한 지속적인 지원과 함께 새로운 계정 저장 장치 데이터베이스인 ldapsam 및 tdbsam을 지원합니다. HP CIFS Server A.02.01 인증 백엔드는 다음으로 구성됩니다.

- smbpasswd: A.01.* 버전과 호환되는 플랫 파일 형식이며 기본 구성입니다.
- tdbsam: 독립형 서버의 smbpasswd 대체로 사용되며 다양한 속성을 지닌 데이터베이스입니다.

- ldapsam: 다양한 속성을 지니고 있으며 LDAP 디렉토리를 사용하는 계정 저장 장치 및 검색 백엔드입니다. A.01.* 버전과 함께 제공된 것과는 다른 스키마를 사용합니다.
- ldapsam_compat : LDAP 디렉토리를 사용하는 LDAP 저장 장치 및 검색 백엔드로서 A.01.* 버전과 호환됩니다. 이 백엔드는 A.01.* 버전과 함께 제공된 스키마를 사용합니다.

새로운 계정 관리 도구(버전 A.02.01)

HP CIFS Server A.02.01에서는 사용자 계정 정보를 관리할 pdbedit, net 명령, smbldap 도구 및 smbpasswd를 포함하여 새 유틸리티 및 변경된 유틸리티를 지원합니다. net 명령은 새롭고 다양한 유틸리티 작업을 제공하고 기존의 다른 작업을 변경합니다. 새 pdbedit 및 net 명령을 사용하는 방법에 대한 자세한 내용은 SWAT 도움말 텍스트를 참조하십시오.

HP CIFS Server 설명서: 서적 및 온라인

HP CIFS Server의 전체 설명서는 대부분의 기술 서적 전문 서점에서 구할 수 있는 HP에서 공급하지 않는 책 3권(HP가 발행하지 않음)과 이 HP CIFS Server 설명서(서적 및 온라인 형태)로 구성됩니다.

HP에서 발행하는 설명서는 **HP CIFS Server 관리자 설명서**입니다.

Samba-3 HOWTO 및 Reference Guide and Samba-3 by Example은 이 제품과 함께 제공되며 `/opt/samba/docs` 디렉토리에 들어 있습니다. 참고 서적 Using Samba, 2nd Edition도 /opt/samba/swat/using_samba에 있습니다. 3권의 서적 모두 SWAT 유틸리티를 통해 액세스할 수 있습니다.

HP에서 발행하지 않는 책은 Using Samba, Edition 2 by Robert Eckstein, David Collier-Brown and Peter Kelly (O'Reilly, 2000), ISBN: 1-56592-449-5, The official Samba-3 HOWTO and Reference Guide by John H. Terpstra and Jelmer R. Vernooij, Editors, ISBN 및 0-13-145355-6 and Samba-3 by Example입니다.

참고

HP에서 공급하지 않은 Samba 설명서에는 종종 Samba의 이후 릴리즈에 예정된 기능에 대한 설명이 포함되어 있습니다. 이러한 책의 저자가 어떤 기능이 기존 릴리즈에 존재하고 어떤 기능이 Samba의 이후 릴리즈에서 사용할 수 있는지에 대한 정보를 항상 제공하지는 않습니다.

HP CIFS Server에 대한 가장 정확한 정보를 보려면 HP에서 제공한 Samba 맨페이지나 SWAT 도움말 기능을 사용하십시오.

사용 가능한 설명서(항목별)

이 절에서는 주요 Samba 항목에 대해 간단히 설명합니다.

HP CIFS 기초

HP CIFS 기초 절에는 서버에서의 파일의 위치, HP CIFS 설치, HP CIFS 구성 및 HP CIFS 시작 및 중지에 대한 정보가 포함되어 있습니다.

서버에서의 파일의 위치

HP CIFS의 기본 위치는 */opt/samba*입니다. 이 경우 Samba 디렉토리에 *bin/*, *docs/*, *script/*, *examples /*, *HA/*, *man/* 및 *swat/* 디렉토리가 있어야 합니다. 2장의 개요 절에서 HP CIFS Server 파일 및 디렉토리의 전체 목록을 참조하십시오.

HP CIFS 구성 파일은 */etc/opt/samba*에 들어 있습니다. HP CIFS 로그 파일 및 임시 파일은 */var/opt/samba*에 만들어집니다.

HP CIFS 파일 및 디렉토리에 관한 자세한 내용은 이 설명서의 2장을 참조하십시오.

HP CIFS Server 설치

HP CIFS Server 제품은 *swinstall* 유틸리티를 사용하여 설치합니다. 제품 설치 단계는 이 설명서의 2장에 나옵니다.

HP CIFS Server 구성

HP CIFS 구성 스크립트를 실행하는 데 필요한 모든 정보는 이 설명서의 2장에서 제공됩니다.

다른 구성 옵션을 포함할 수도 있습니다. 이러한 옵션에는 전역 구성 옵션, 서비스 구성 옵션 및 브라우저 구성 옵션이 포함됩니다.

HP CIFS Server는 Samba 도메인 모델, Windows 도메인 모델 및 통합 도메인 모델의 세 가지 배포 모델을 지원합니다. 이러한 세 가지 모델은 일반적인 네트워크 환경을 나타내며 HP CIFS Server의 융통성을 보여 줍니다. 자세한 내용은 9장, 213페이지의 “HP CIFS 배포 모델”을 참조하십시오.

HP CIFS 시작 및 중지

`winbind` 지원을 사용하지 않는 경우 다음 명령을 사용하여 HP CIFS Server를 시작 또는 중지합니다.

/opt/samba/bin/startsmb

/opt/samba/bin/stopsmb

`winbind` 지원을 사용하도록 HP CIFS Server를 구성하는 경우 다음 명령을 사용하여 HP CIFS Server를 시작 또는 중지합니다.

/opt/samba/bin/startsmb -w

또는 */opt/samba/bin/startsmb --winbind*

/opt/samba/bin/stopsmb -w

또는 */opt/samba/bin/stopsmb --winbind*

다음 명령을 사용하면 smbd 및 nmbd 실행에 영향을 미치지 않고도 Winbind 실행을 제어할 수 있습니다.

winbind만 시작하려면 다음 명령을 실행합니다.

/opt/samba/bin/startwinbind

winbind만 중지하려면 다음 명령을 실행합니다.

/opt/samba/bin/stopwinbind

위 명령은 이 설명서의 2장에서 설명합니다.

기타 HP CIFS 항목

기타 HP CIFS 항목 절에는 HP CIFS 스크립트, 프린터 추가 및 제거, 유틸리티, SWAT 구성 도구, 브라우저 설명, 문제 해결 및 NIS와 HP CIFS 관련 정보가 포함되어 있습니다.

HP CIFS 스크립트

smbd, nmbd, smbstatus 및 smbclient와 같은 Samba 프로그램의 명령줄 매개 변수에 관한 자세한 내용은 *Using Samba*의 부록 D에 나오는 "Summary of Samba Daemons and Commands"를 참조하십시오. 4장 및 5장에도 사용자 스크립트에 관한 정보가 있습니다.

프린터 설정

HP CIFS Server에서의 인쇄 과정, 인쇄 명령, 인쇄 변수 및 최소 인쇄 설정에 대한 설명은 Samba HOWTO and Reference Guide 17장, "Classic Printing Support"를 참조하십시오. 이 장에는 Samba 인쇄 옵션 및 Windows 클라이언트 프린터로 인쇄에 관한 자세한 정보도 포함되어 있습니다.

SWAT 구성 도구

Samba 웹 관리 도구(SWAT)는 *smb.conf* 파일의 Samba 구성을 설정하거나 변경하는 데 사용할 수 있는 GUI입니다. globals, shares, printers, status, view(smb.conf), 및 password 영역의 정보를 변경할 수 있습니다.

SWAT에 대한 자세한 내용은 *Samba HOWTO and Reference Guide* 30장, "SWAT - The Samba Web Administration Tool"을 참조하십시오.

검색

검색 기능을 통해 네트워크의 서버와 공유를 볼 수 있습니다. Samba는 14가지 이상의 다양한 검색 옵션을 제공합니다. 하지만 기본값으로 시작하는 것이 좋습니다.

검색 기능 및 모든 검색 옵션에 대한 설명은 Samba HOWTO and Reference Guide 9장 "Network Browsing"을 참조하십시오.

문제 해결

Samba HOWTO and Reference Guide 5부 "Troubleshooting"에서는 Samba 문제 해결 방법에 대해 설명하는 유용한 세 단원을 참조할 수 있습니다. 여기에는 Samba의 문제점을 해결할 때 사용하는 도구 목록이 포함되어 있습니다. 이 도구에는 *trace* 및 *tcpdump*와 같은 Unix 유틸리티 및 Samba 로그 파일이 포함되어 있습니다. 여기에는 Samba 설치 또는 재구성 중에 발생하는 문제를 해결할 수 있는 장애 트리도 포함됩니다.

또한 HP 시스템에서 문제점을 해결하는 데 매우 유용한 여러 도구가 있습니다. 예를 들면, `nettl` 및 `netfmt`는 특별히 HP-UX 시스템에서 활동을 추적하는 데 사용됩니다. Microsoft의 `NetMon`은 Windows 2000 서버용 도구로 널리 사용되고 있습니다.

NIS 및 HP CIFS 이제 HP CIFS는 NIS 및 NIS+에서도 작동합니다. 특정 옵션에 대한 자세한 내용은 *Samba HOWTO and Reference Guide*를 참조하십시오.

HP CIFS 설명서 정보

다음 정보를 사용하여 필요한 Samba 및 HP CIFS 설명서를 찾을 수 있습니다.

표 1-1

HP CIFS 제품	설명서 제목: 장: 절
서버 설명	HP CIFS Server 설치 및 관리: 1장, "HP CIFS Server 소개" Samba Meta FAQ No. 2, "General Information about Samba" Samba FAQ No. 1, "General Information" Samba 서버 FAQ: No. 1, "What is Samba" *Using Samba*: 1장, "Learning the Samba"
클라이언트 설명	Samba 맨페이지: samba(7) HP CIFS Client 설치 및 관리: 1장, "HP CIFS Client 소개"
HP 추가 기능	HP CIFS Server 설치 및 관리: 1장, "HP CIFS Server 소개" 절: "Samba 서버 소스에 대한 HP CIFS의 개선" 및 3장, "액세스 제어 목록(ACL)" HP CIFS Client 설치 및 관리: 1장, "HP CIFS Client 소개" 절: "HP CIFS 확장" 및 "ACL 매핑"

표 1-1 **(계속)**

HP CIFS 제품	설명서 제목: 장: 절
서버 설치	HP CIFS Server 설치 및 관리: 2장, "HP CIFS Server 설치 및 구성" Samba FAQ: No 2, "Compiling and Installing Samba on a UNIX Host."
클라이언트 설치	HP CIFS Client 설치 및 관리: 2장, "HP CIFS Client 설치 및 구성"
Samba GUI 관리 도구	*Samba HOWTO and Reference Guide:* 31장, "SWAT - The Samba Web Administration Tool" 또는 *Using Samba*: 2장, "Unix 시스템에 Samba 설치"
서버 구성	HP CIFS Server 설치 및 관리: 2장, "HP CIFS Server 설치 및 구성"
클라이언트 구성	HP CIFS Client 설치 및 관리: 2장, "HP CIFS Client 설치 및 구성"
구성: PAM	HP CIFS Client 설치 및 관리: 6장, "인증" HP-UX 맨페이지: pam(3) HP-UX 맨페이지: pam.conf
서버: 시작 및 중단 클라이언트: 시작 및 중단	HP CIFS Server 설치 및 관리, 2장 HP CIFS Client 설치 및 관리, 2장

표 1-1 **(계속)**

HP CIFS 제품	설명서 제목: 장: 절
서버: Samba 스크립트	*Using Samba:* 부록 D, "Summary of Samba Daemons and Commands"
SMB 및 CIFS 파일 프로토콜	이 설명서의 11장, "HP CIFS 배포 도메인 모델"
SMB 및 CIFS 네트워크 설계	*Using Samba:* 1장, "Learning the Samba" Samba Meta FAQ No. 4, "Designing an SMB and CIFS Network"
Samba 맨페이지	SWAT에서 맨페이지 참조
서버 유틸리티	*Samba HOTO and Reference Guide*
클라이언트 유틸리티	HP CIFS Client 설치 및 관리: 4장, "HP CIFS Client 유틸리티"
서버 인쇄	*Samba HOWTO and Reference Guide:* 17장, "classic Printing Support"
서버 검색	검색 기능 및 모든 검색 옵션에 대한 설명은 *Samba HOWTO and Reference Guide* 9장 "Network Browsing"을 참조하십시오.
서버 보안	이 설명서의 12장 "CIFS Server 보안"

표 1-1 **(계속)**

HP CIFS 제품	설명서 제목: 장: 절
서버 문제 해결	HP CIFS Server 설치 및 관리: 3장, "HP CIFS Server 문제 해결" Samba HOWTO and Reference Guide의 5부 "Troubleshooting" *Using Samba* "9장, Troubleshooting Samba" Samba FAQs No. 4, "Specific Client Application Problems" 및 No 5, "Miscellaneous"
클라이언트 문제 해결:	*/opt/samba/*docs 디렉토리의 DIAGNOSIS.txt Samba 맨페이지: debug2html(1), smbd(8), nmbd(8), smb.conf(5)
	HP CIFS Client 설치 및 관리: 3장, "HP CIFS Client 문제 해결"

HP CIFS Server 파일 및 디렉토리 정보

이 절에서는 CIFS Server를 구성하는 주요 디렉토리 및 파일을 간략하게 설명합니다.

표 1-2 **HP CIFS Server 파일 및 디렉토리**

파일/디렉토리	설명
/opt/samba	HP CIFS Server 대부분의 기본 디렉토리입니다.

표 1-2 HP CIFS Server 파일 및 디렉토리(계속)

파일/디렉토리	설명
/opt/samba_src	HP CIFS Server의 소스 코드를 포함하는 디렉토리입니다(소스 번들이 설치된 경우).
/opt/samba/bin	데몬 및 유틸리티를 포함하여 HP CIFS Server의 바이너리 파일을 포함하는 디렉토리입니다.
/opt/samba/docs	html(htmldocs) 및 텍스트(textdocs)를 포함하여 다양한 형식의 설명서를 포함하는 디렉토리입니다.
/opt/samba/examples	이 디렉토리에는 *smb.conf* 예제 파일, 예제 스크립트 및 기타 유틸리티 등이 들어 있습니다.
/opt/samba/man	이 디렉토리는 HP CIFS Server의 맨 페이지를 포함합니다.
/opt/samba/script	이 디렉토리는 HP CIFS Server의 유틸리티인 다양한 스크립트를 포함합니다.
/opt/samba/swat	이 디렉토리는 Samba 웹 관리 도구(SWAT)에서 필요로 하는 html 및 이미지 파일을 포함합니다.
/opt/samba/HA	이 디렉토리는 고가용성 예제 스크립트, 구성 파일 및 README 파일을 포함합니다.

표 1-2 HP CIFS Server 파일 및 디렉토리(계속)

파일/디렉토리	설명
/var/opt/samba	이 디렉토리는 HP CIFS Server 로그 파일과, lock 파일과 같이 HP CIFS Server가 사용하는 기타 동적 파일을 포함합니다.
/etc/opt/samba	이 디렉토리는 HP CIFS Server가 사용하는 구성 파일(기본적으로 *smb.conf* 파일)을 포함합니다.
/etc/opt/samba/smb.conf	이 파일은 HP CIFS Server의 주 구성 파일이며 다음에 자세히 설명합니다.
/etc/opt/samba/smb.conf.default	이 파일은 HP CIFS Server와 함께 제공되는 기본 *smb.conf* 파일입니다. 사용자의 필요에 맞도록 수정할 수 있습니다.
/opt/samba/LDAP3	이 디렉토리에는 HP CIFS Server에서 LDAP 통합 지원용으로 사용하는 파일이 들어 있습니다.
/opt/samba/COPYING, */opt/samba_src/COPYING,* */opt/samba_src/samba/COPYING*	이 파일은 HP CIFS Server에 적용되는 GNU Public License입니다.
/sbin/init.d/samba	이 스크립트는 HP CIFS Server를 컴퓨터가 부팅될 때 시작하고 종료할 때 중단합니다(이렇게 구성된 경우).
/etc/rc.config.d/samba	이 텍스트 파일은 HP CIFS Server가 컴퓨터 부팅 시 자동으로 시작할지 여부를 구성합니다.

표 1-2 HP CIFS Server 파일 및 디렉토리(계속)

파일/디렉토리	설명
/sbin/rc2.d/S900samba, */sbin/rc1.d/K100samba*	컴퓨터가 부팅되고 종료될 때 자동으로 실행되어 HP CIFS Server를 시작 및 중단하는(이렇게 구성된 경우) */sbin/init.d/samba*에 대한 링크입니다.

2 HP CIFS Server 설치 및 구성

이 장에서는 HP CIFS Server 소프트웨어를 설치하고 구성하는 절차를 설명합니다. 이 장의 구성은 다음과 같습니다.

- HP CIFS Server 요구 사항 및 제한
- 1단계: HP CIFS Server 소프트웨어 설치
- 2단계: 구성 스크립트 실행
- 3단계: 구성 수정
- 4단계: HP CIFS Server 시작

중요

HP CIFS Server A.02.01 이상에서는 LDAP-UX 통합 제품인 J4269AA를 설치해야 합니다.

참고

HP CIFS Server 소프트웨어가 시스템에 미리 설치되어 있는 경우에는 위의 1단계를 건너뛰고 "2단계: 구성 스크립트 실행"으로 이동하십시오.

참고

www.software.hp.com 웹 사이트에서 최신 버전의 소프트웨어를 다운로드할 수 있습니다.

참고

www.docs.hp.com(영문 설명서) 및 **www.docs.hp.com/ko(한글 설명서)** 웹 사이트에서 가장 완벽한 최신 버전의 HP CIFS 설명서를 볼 수 있습니다.

참고

HP는 HP CIFS Server를 시작하기 위해 `inetd` 구성을 지원하지 않습니다.

HP CIFS Server 요구 사항 및 제한

HP CIFS 제품을 설치하기 전에 시스템이 다음의 제품 요구 사항과 제한 사항에 맞는지 확인하십시오.

HP-UX 11.x 메모리 및 디스크 요구 사항

11.x 32비트 및 64비트 HP-UX 시스템은 최소 64MB RAM과 1GB의 디스크 공간으로 부팅할 수는 있지만 이러한 구성의 성능은 너무 떨어집니다. HP의 권장 최소 사양은 다음과 같습니다.

- 11.x 32비트: 128MB RAM, 1GB-2GB 디스크
- 11.x 64비트: 512MB RAM, 2GB-3GB 디스크

HP CIFS Server A.02.01 설치 요구 사항

HP CIFS Server A.02.01 설치하려면 11i v1 PA 시스템의 경우 약 86.7MB의 디스크 공간이 필요하며 11i v2 IA 및 PA 시스템의 경우 약 156.7MB의 디스크 공간이 필요합니다. HP CIFS Server 제품의 구성은 다음과 같습니다.

- CIFS Server 소스 코드 파일/HP-UX 11i v1−3.4MB
- CIFS Server 파일 및 인쇄 서비스/HP-UX 11i v1−83.3MB
- CIFS Server 소스 코드 파일/HP-UX 11i v2 IA−3.4MB
- CIFS Server 파일 및 인쇄 서비스/HP-UX 11i v2 IA−153.3MB
- CIFS Server 소스 코드 파일/HP-UX 11i v2 PA−3.4MB
- CIFS Server 파일 및 인쇄 서비스/HP-UX 11i v2 PA−153.3MB

HP CIFS Server 메모리 및 디스크 요구 사항

A.0.201 버전의 업데이트된 HP CIFS Server 메모리 요구사항

버전 A.02.01에서는 smbd 프로세스당 1000KB 시스템 메모리가 필요합니다. HP CIFS Server는 이전에 smbd 프로세스당 600KB였던 시스템 메모리의 기본 사용량을 400KB를 늘려 약 70퍼센트가 증가했습니다. 메모리 사용량이 증가된 이유는 새로

운 기능이 추가되었기 때문입니다.

기본 메모리가 증가된 것 외에도, smbd 프로세스는 이제 필요에 따라 세분화된 캐싱 요구 사항에 맞게 메모리를 할당할 수도 있습니다. 이 메모리 할당의 크기와 타이밍은 클라이언트의 종류와 액세스 중인 리소스에 따라 크게 달라집니다. 단일 smbd 프로세스는 일시적으로 최대 4MB의 메모리 스왑 공간을 사용할 수 있습니다. 그러나 대부분의 클라이언트 액세스 패턴은 그처럼 전문화된 캐싱 작업을 시작하지 않습니다. 시스템 관리자는 이 새로운 동적 메모리 기능을 평가하기 위해 메모리 이용률을 정기적으로 모니터링해야 합니다.

이전 버전에서 업그레이드할 때, 이러한 변경 내용에 대응하기 위해 HP-UX 서버 메모리 구성을 조정해야 할 수도 있습니다.

자세한 내용은 이 설명서의 12장 "HP CIFS용 HP-UX 구성"을 참조하십시오.

1단계: HP CIFS Server 소프트웨어 설치

HP CIFS Server 업그레이드:

기존 HP CIFS Server 구성을 업그레이드할 경우 현재 환경의 백업 복사본을 만드는 것이 좋습니다. SD 설치 중에 현재 구성 파일이 변경되거나 대체될 것입니다. 현재 구성으로 다시 돌아올 필요가 있으면 */var/opt/samba, /etc/opt/samba* 및 */opt/samba* 디렉토리 아래의 모든 파일을 저장해야 합니다. 예를 들면 다음과 같습니다.

```
$ stopsmb
```

또는 winbind가 사용 중인 경우 다음을 수행합니다.

```
$ stopsmb -w
$ mkdir /tmp/cifs_save
$ tar -cvf /tmp/cifs_save/var_backup.tar /var/opt/samba
$ tar -cvf /tmp/cifs_save/etc_backup.tar /etc/opt/samba
$  tar -cvf /tmp/cifs_save/optsamba_backup.tar /opt/samba
```

`-o` 옵션은 `tar` 명령과 함께 사용하지 마십시오. 그래야 파일 소유권이 제대로 설정됩니다.

업그레이드 중 문제가 발생하면 SD를 사용하여 전체 HP CIFS Server 제품을 제거한 다음 이전 백업 버전을 복원합니다. 이 작업이 끝나면 저장된 구성 파일과 HP CIFS Server를 복원할 수 있습니다. 예를 들면 다음과 같습니다.

```
$ tar -xvf /tmp/cifs_save/var_backup.tar
$ tar -xvf /tmp/cifs_save/etc_backup.tar
$  tar -xvf /tmp/cifs_save/optsamba_backup.tar
```

이 절차가 사용자 데이터 파일을 포함하는 포괄적인 백업 전략을 대체하는 것은 아닙니다.

개요:

HP CIFS Server 소프트웨어를 설치하는 과정에는 *swinstall(1M)* 유틸리티를 사용하여 HP CIFS Server 파일 세트를 로드하는 단계, HP CIFS 구성 절차, 그리고 *startsmb* 스크립트를 사용하여 Samba를 시작하는 단계가 포함됩니다.

절차:

아래의 단계에 따라 HP-UX *swinstall* 프로그램을 사용하여 HP CIFS Server 소프트웨어를 설치하십시오.

1. **root**로 로그인합니다.
2. 소프트웨어 매체(디스크)를 적당한 드라이브에 넣습니다.
3. 다음 명령을 사용하여 *swinstall* 프로그램을 실행합니다.

   ```
   swinstall
   ```

   소프트웨어 선택 창과 소스 지정 창이 열립니다.
4. 필요하면 소스 호스트 이름을 변경하고, 소스 저장소 경로 필드에 드라이브의 마운트 지점을 입력한 다음 **확인** 단추를 활성화하여 소프트웨어 선택 창으로 돌아갑니다. 추가 정보를 보려면 도움말 단추를 활성화합니다.

   이제 소프트웨어 선택 창에 설치에 사용할 수 있는 소프트웨어 번들 목록이 표시됩니다.
5. 사용자의 시스템 유형에 맞는 HP CIFS Server 소프트웨어를 강조 표시합니다.
6. "Actions" 메뉴에서 `Mark for Install`을 선택하여 설치할 제품을 선택합니다. 맨페이지 및 사용자 설명서를 제외하곤 전체 HP CIFS 제품을 설치해야 합니다.
7. "Actions" 메뉴에서 `Install`을 선택하여 제품 설치를 시작하고 설치 분석 창을 엽니다.
8. 상태 필드에 준비 완료 메시지가 표시되면 설치 분석 창에서 **확인** 단추를 활성화합니다.
9. 확인 창에서 **예** 단추를 활성화하여 소프트웨어 설치를 계속합니다. *swinstall*에 의해 설치 창이 표시됩니다.

   소프트웨어를 설치하는 동안 설치 창을 통해 데이터가 처리되는 것을 볼 수 있습니다. 상태 필드에 준비 완료 표시가 나타나고 참고 창이 열립니다.

   *swinstall*은 파일 세트를 로드하고 파일 세트에 대해 제어 스크립트를 실행합니다. 예상 처리 시간은 3분 ~ 5분입니다.
10. */var/adm/sw/swinstall.log* 및 */var/adm/sw/swagent.log*에서 로그 파일을 확인하여 설치가 성공했는지 확인합니다.

2단계: 구성 스크립트 실행

samba_setup 구성 스크립트는 새 설치용으로만 제공됩니다. HP CIFS Server A.01에서 A.02로의 업데이트 방법에 대한 자세한 절차는 8장, 199페이지의 “HP CIFS Server A.01에서 A.02로 업데이트”를 참조하십시오.

samba_setup 구성 스크립트를 실행하기 전에 기본 구성 정보를 알고 있어야 하며 사용하는 HP CIFS 배포 도메인 모델에 따라 추가 소프트웨어를 설치해야 할 수도 있습니다. `samba_setup` 스크립트를 실행하기 전에 다음을 수행해야 합니다.

- HP CIFS를 WINS 서버로 사용할지를 결정합니다.
- HP CIFS에서 기존 WINS 서버에 액세스하는 경우 WINS IP 주소를 가져옵니다.
- LDAP 백엔드를 사용하기로 선택한 경우 다음과 같은 전역 LDAP 매개 변수 정보를 제공합니다.
  - LDAP 디렉토리 서버의 정규화된 고유 이름
  - ldap SSL
  - ldap suffix
  - ldap user suffix
  - ldap group suffix
  - ldap admin dn

  LDAP 매개 변수를 구성하는 방법에 대한 자세한 내용은 6장, 131페이지의 “LDAP 통합 지원”을 참조하십시오.
- HP CIFS Server 이름을 가져옵니다.
- Windows NT4 도메인을 사용하기로 선택한 경우 다음 정보를 제공합니다.
  - 도메인 이름
  - 주 도메인 컨트롤러(PDC)의 이름
  - 백업 도메인 컨트롤러(BDC)의 이름

— 관리자 사용자 이름 및 암호

자세한 내용은 4장, 97페이지의 “NT 스타일 도메인”을 참조하십시오.

- Windows ADS(Active Directory Server) 영역을 사용하기로 선택한 경우 다음 정보를 제공합니다.

  — 영역 이름

  — 도메인 컨트롤러 이름

  — 관리자 사용자 이름 및 암호

  — LDAP-UX 통합 제품을 설치되어 있어야 합니다.

  — Kerberos 라이브러리를 사용할 수 있어야 합니다.

  Kerberos 보안을 사용하여 HP CIFS Server를 Windows 2000/2003 도메인에 참여시키는 방법에 대한 자세한 내용은 5장, 123페이지의 “Windows 2000/2003 도메인”을 참조하십시오.

- 작업 그룹 환경을 사용하려는 경우 다음 인증 보안 유형을 선택합니다.

  — 서버 수준 보안: 이 보안 유형이 지정된 경우 다른 SMB 암호 서버에 의해 암호 인증이 처리됩니다. 클라이언트가 특정 공유에 액세스하려 할 경우, Samba는 사용자에게 해당 공유에 대한 액세스가 허용되었는지 확인합니다. 그런 다음 Samba에서 SMB 암호 서버.영역 이름을 통해 암호를 확인합니다.

  — 사용자 수준 보안: 이 보안 유형이 지정된 경우 각 공유가 특정 사용자에게 할당됩니다. 액세스 요청이 있을 경우 Samba는 허용된 로컬 사용자 목록에서 사용자의 사용자 이름과 암호를 확인하고 일치하는 경우에만 액세스를 허용합니다.

  — 공유 수준 보안: 이 보안 유형이 지정된 경우 각 공유(디렉토리)에는 관련된 암호가 최소한 하나씩 있습니다. 암호를 가진 사용자는 누구나 공유에 액세스할 수 있으며 다른 액세스 제한은 없습니다.

- 다음 명령을 사용하여 Samba 구성 스크립트를 실행합니다.

  ```
  /opt/samba/bin/samba_setup
  ```

이 스크립트는 입력한 정보에 따라 *smb.conf* 파일을 수정합니다.

3단계: 구성 수정

HP CIFS Server가 다음 기능을 제공하려면 구성을 수정해야 합니다.

- ACL 지원
- 클라이언트 및 서버에서 UNIX 확장자의 대/소문자 구분
- DOS 속성 매핑
- 인쇄 서비스(최신 버전인 A.02.01 버전)
- 분산 파일 시스템(DFS) 지원
- MC/ServiceGuard 고가용성(HA) 구성

ACL 지원 구성(A.01.07 버전)

현재 HP-UX에서는 *unix* UNIX 파일 사용 권한과 *hpux_posix* VxFS POSIX ACL의 두 가지 ACL 체계를 지원합니다.

아래에는 예제 값이 표시됩니다.

- 예제 1:

  ```
  acl schemes = unix
  ```

  이것은 기본 ACL 스키마로서 UNIX ACL 기능을 무시하고 UNIX 파일 사용 권한을 사용합니다.

- 예제 2:

  ```
  acl schemes = none
  ```

  이 예제는 공유의 모든 ACL 지원을 해제하며 클라이언트가 공유의 임의의 파일 시스템에 대한 ACL 정보를 가져오거나 설정하려 할 때마다 오류가 반환됩니다.

- 예제 3:

  ```
  acl schemes = hpux_posix
  ```

  이 예제는 전체 공유에서 VxFS POSIX ACL만 지원합니다. 클라이언트에서 ACL을 가져오거나 설정하려 할 경우 해당 파일 시스템에서 VxFS POSIX ACL을 지원하는 경우에만 성공합니다. UNIX 사용 권한만 지원되는 경우 클라이언트에서 ACL을 가져오거나 설정하려고 시도하면 실패합니다.

- 예제 4:

  ```
  acl schemes = hpux_posix unix
  ```

  HP CIFS는 VxFS POSIX ACL을 사용하려고 시도합니다. ACL이 없는 경우 UNIX 사용 권한을 사용할 것입니다.

ACL 지원 구성(A.01.08 버전)

HP CIFS Server 버전 A.01.08은 "nt acl support"라고 하는 공유 수준의 변수를 제공합니다. 이 변수에 사용할 수 있는 값은 "yes"와 "no"입니다. 이 변수의 기본값은 "yes"입니다. 사용자는 이 변수를 사용하면 공유별로 ACL 지원을 설정/해제할 수 있습니다. ACL에 관한 자세한 내용은 이 설명서의 3장을 참조하십시오.

대/소문자 구분 구성

기본적으로 HP CIFS Server는 DOS 및 NT와 마찬가지로 대/소문자를 구분하도록 구성되어 있습니다.

참고

UNIX에서 CIFS 확장자를 사용할 때는 CIFS Client와 Server 모두 대/소문자를 구분하도록 구성하는 것이 좋습니다.

CIFS Server의 경우 서버 구성 파일 */etc/opt/samba/smb.conf*를 다음과 같이 편집합니다.

```
case sensitive = yes
```

CIFS Client의 경우, */etc/opt/cifsclient/cifsclient.cfg* 파일에서 다음 기본값이 설정되어 있는지 확인합니다.

```
caseSensitive = yes
```

DOS 속성 매핑 구성

Samba에서 DOS 파일 속성을 UNIX 파일 시스템의 *owner, group* 및 *other* 실행 비트에 매핑하기 위해 구성될 수 있는 세 가지 매개 변수로 *map system, map hidden* 및 *map archive*가 있습니다.

CIFS Client를 사용할 경우 이 세 가지 매개 변수를 모두 해제합니다. *map archive* 매개 변수가 설정된 경우 사용자가 파일에 데이터를 쓸 때마다 owner 실행 권한이 설정됩니다. 이는 일반적으로 HP CIFS Client 또는 UNIX 클라이언트에 적합하지 않은 동작입니다.

기본적으로 *map system* 및 *map hidden*은 해제되어 있고 *map archive*는 활성화되어 있습니다.

*map archive*를 해제하려면 다음과 같이 */etc/opt/samba/smb.conf*를 수정합니다.

```
map archive = no
```

HP CIFS 버전 A.02.02용 인쇄 서비스 구성

이 절에서는 HP CIFS 버전 A.02.02를 실행하는 시스템에서의 인쇄 서비스 구성에 관한 정보를 제공합니다. 이제 HP CIFS Server에서는 다음과 같은 NT 인쇄 기능을 제공합니다.

- 프린터 드라이버 파일이 없는 Windows NT, 2000 및 XP 클라이언트로 파일을 다운로드할 수 있습니다.
- Windows NT/XP/2000 **프린터 추가** 마법사를 사용하여 프린터 드라이버 파일을 업로드할 수 있습니다.
- 프린터 개체에 대한 NT 액세스 제어 목록(ACL)을 지원합니다.

각 인쇄 서비스(ACL 제외) 설치 및 구성에 관한 정보는 다음 절에서 제공합니다. ACL 지원 구성에 관한 정보는 이전 절에서 설명했습니다.

[printers] 공유 구성

다음은 최소한의 인쇄 설정입니다. 다음 두 절차 중 **하나**를 사용하여 [printers] 공유를 만듭니다.

1. SWAT(Samba 관리 도구)

   또는

2. */etc/opt/samba/smb.conf* 파일에 [printers] 공유를 만듭니다. 다음 예제를 참조하십시오.

   ```
   [hpdeskjet]
     path = /tmp
     printable = yes
   ```

   여기서 "hpdeskjet"은 추가할 프린터의 이름입니다.

[printers] 공유 만들기

/etc/opt/samba/smb.conf 파일에서 [printers] 공유를 구성합니다. 다음 예제를 참조하십시오.

```
[printers]
  path = /tmp
  printable = yes
  browseable = no
```

smb.conf 파일에는 정의되지 않았지만 HP CIFS Server에 존재하는 SWAT에 프린터 목록을 표시하려면 이 공유가 필요합니다. 이 공유가 정의되지 않은 경우에는 프린터 목록은 *smb.conf* 파일에 정의된 프린터 공유만 표시합니다.

프린터 드라이버 파일을 자동으로 업로드하도록 서버 설정

A.02.01 버전의 소프트웨어를 사용하여 Samba 호스트에 새 드라이버를 추가하려면 다음 두 조건 중 하나가 참이어야 합니다.

1. Samba 호스트에 연결하는 데 사용된 계정의 uid가 0(즉 root 계정)입니다.
2. Samba 호스트에 연결하는 데 사용된 계정이 프린터 관리자 목록의 구성원입니다. 이 경우 다음과 같은 `[global]` *smb.conf* 매개 변수가 필요합니다.

   ```
   printer admin = netadmin
   ```

연결된 계정이 계속 액세스를 소유하고 있어야 파일을 [print$] 아래의 하위 디렉토리에 추가할 수 있습니다. 모든 파일은 기본적으로 '읽기 전용'으로 설정되며 `'printer admin =' 매개 변수에 'netadmin'뿐만 아니라 드라이버를 서버로 업로드할 수 있도록 허용된 모든 사용자 또는 그룹의 이름도 포함되어야 합니다.

다음은 필요한 다른 매개 변수의 예제입니다.

1. *smb.conf* 파일에 HP CIFS Server의 "/etc/opt/samba/printers" 빈 디렉토리를 가리키는 [print$] 공유를 다음과 같이 만듭니다. 다음 예제를 참조하십시오.

   ```
   [print$]
     path = /etc/opt/samba/printers
     browseable = yes
     guest ok = yes
     read only = yes
     write list = netadmin
   ```

이 예제에서, "write list" 매개 변수는 관리자 수준의 사용자 계정에 공유에서 파일 업데이트를 하기 위한 쓰기 액세스 권한을 지정합니다.

2. 지원해야 할 각 아키텍처에 대해 [print$] 공유 아래에 하위 디렉토리 트리를 만듭니다. 다음 예제를 참조하십시오.

```
cd /etc/opt/samba/printers
mkdir W32X86
mkdir Win40
```

드라이버 파일을 보관할 위치(하위 디렉토리)는 두 곳이며, 파일이 사용될 Windows의 버전에 따라 달라집니다.

Windows NT, XP 또는 Windows 2000 드라이버 파일의 경우, 파일은 */etc/opt/samba/printers/W32X86* 하위 디렉토리에 저장됩니다.

Windows 9x 드라이버 파일의 경우, 파일은 */etc/opt/samba/printers/Win40/0* 하위 디렉토리에 저장됩니다.

프린터 드라이버를 자동으로 업로드하도록 클라이언트 설정

디스크에서 HP CIFS Server의 프린터로 프린터 드라이버 파일을 자동으로 업로드할 수 있습니다. 업로드 단계는 다음과 같습니다.

1. `\\[server name]` 명령을 실행하여 CIFS Server로 연결하거나 **네트 워크 환경**에서 CIFS Server로 이동합니다. 프린터 관리 목록 구성으로 연결되었는지 확인합니다.
2. CIFS Server에서 "프린터"를 두 번 클릭하거나 "프린터 및 팩스" 폴더를 클릭합니다. CIFS Server에서 사용할 수 있는 프린터의 목록이 폴더에 표시됩니다. 프린터 속성을 보면 다음과 같은 오류 메시지가 표시됩니다.

   장치 설정을 표시할 수 없습니다. 지정된 프린터의 드라이버가 설치되지 않았으므로 스풀러 등록 정보만 표시됩니다. 지금 드라이버를 설치하시겠습니까?

3. 오류 대화 상자에서 "아니오"를 클릭하면 프린터 속성 창이 표시됩니다.
4. '고급' 탭을 클릭하고 나서 '새 드라이버...' 단추를 클릭합니다.

5. 프린터 드라이버(예제: hp LaserJet 5i)를 선택합니다. 사용자에게 드라이버 파일을 요청하게 됩니다. 드라이버 파일이 있는 경로를 제공합니다. 드라이버 파일이 디스크에서 업로드되어 [print$] 공유 아래의 하위 디렉토리에 저장됩니다.

MS Windows 2000/2003 ADS 도메인에 프린터 발행

프린터를 발행하면 HP CIFS Server 프린터를 Microsoft Windows 2000/2003 ADS 도메인에서 검색할 수 있습니다. Windows 클라이언트가 ADS 도메인의 도메인 구성원인 경우 해당 클라이언트는 프린터를 검색하여 설치할 수 있습니다.

프린터 발행 지원을 위한 HP CIFS Server 설정

다음 절차에 따라 프린터 발행 지원을 위한 HP CIFS Server 설정을 수행합니다.

단계 **1.** 각 프린터의 프린터 공유와 smb.conf 파일의 [printers] 공유를 만듭니다. 다음은 [printers] 공유의 예제입니다.

```
[printers]
  path = /tmp
  printable = yes
  browseable = yes
```

특정 프린터 공유를 설정하는 경우의 예제는 다음을 참조하십시오. 여기서 lj1005는 프린터의 이름입니다.

```
[lj1005]
  path = /tmp
  printable = yes
```

단계 **2.** smb.conf 파일에 [print$] 공유를 만들고 path 매개 변수를 /etc/opt/samba/printers라는 디렉토리로 설정합니다. 다음 예제를 참조하십시오.

```
[print$]
  path = /etc/opt/samba/printers
 use client driver = no
  browseable = yes
  guest ok = yes
  read only = yes
  write list = netadmin
```

위 예제에서 write list 매개 변수는 관리자 수준의 사용자 계정이 이 공유에서 파일 업데이트를 위한 쓰기 액세스를 가짐을 지정합니다. use client driver 매개 변수는 No로 설정해야 합니다.

단계 **3.** HP CIFS Server에 연결할 수 있는 도메인 사용자의 목록을 지정하려면 printer admin 매개 변수를 구성합니다. 다음 예제를 참조하십시오.

```
[global]
  printer admin = cifsuser1, cifsuser2
```

단계 **4.** HP CIFS Server가 ADS 도메인의 구성원이 아닌 경우에는 net ads join -U Administrator%password 명령을 사용하여 HP CIFS Server를 ADS 도메인에 도메인 구성원 서버로 참여하게 합니다. 자세한 내용은 5장, 123페이지의 “Windows 2000/2003 도메인”에 있는 "HP CIFS Server가 Windows 2000/2003 도메인에 ADS 구성원 서버로 참여" 절을 참조하십시오.

Windows 클라이언트에서 프린터 발행

ADS 도메인의 도메인 구성원인 Windows 클라이언트에서 프린터를 발행하려면 다음 절차를 수행합니다.

단계 **1.** Windows 클라이언트에 프린터 관리 목록의 구성원인 사용자로 로그인합니다. 예를 들어, 사용자 이름 cifsuser1을 사용할 수 있습니다.

단계 **2.** start를 클릭합니다.

단계 **3.** run 탭을 클릭합니다.

단계 **4.** open 상자에 \\<HP CIFS Server name>을 입력하여 HP CIFS Server에 연결합니다. 예를 들어, \\hpserverA를 입력할 수 있습니다. hpserverA는 HP CIFS Server의 이름입니다.

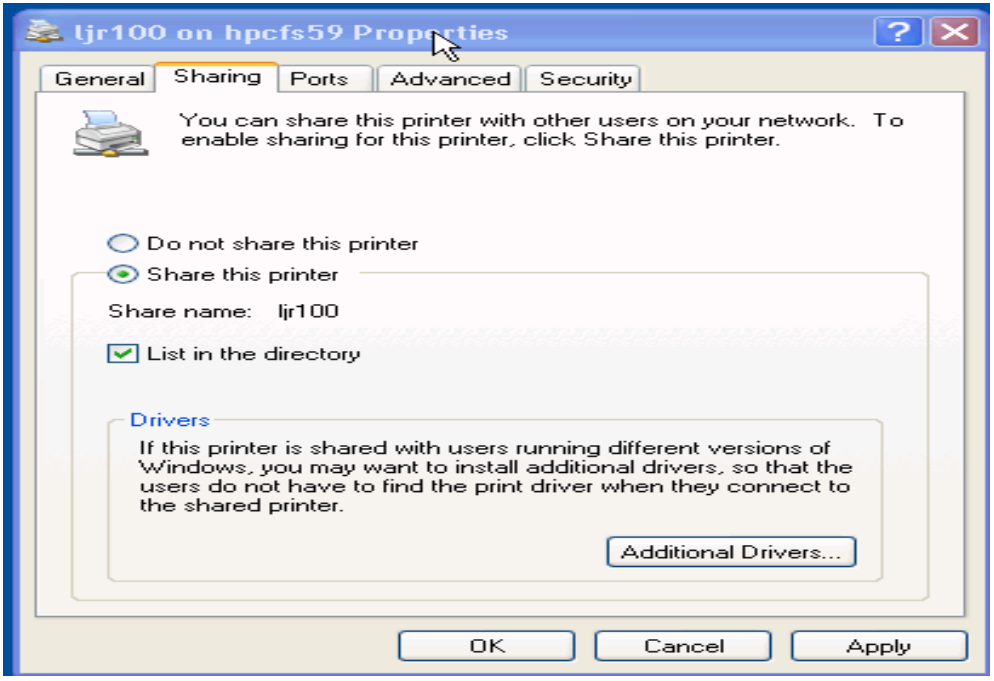
단계 **5.** printers 폴더를 클릭합니다.

단계 **6.** 프린터를 두 번 클릭하고 프린터를 선택한 다음 properties 탭을 선택합니다.

단계 **7.** properties 창 화면에서 sharing 탭을 클릭합니다.

단계 **8.** 공유 창 화면에서 `list in the directory` 확인란을 선택합니다. 다음 화면 스냅샷 예제를 참조하십시오.

그림 2-1 **프린터 발행 화면**



프린터가 발행되었는지 확인

HP CIFS Server 시스템에서 `net ads printer search` 명령을 실행하여 프린터가 발행되었는지 확인할 수 있습니다. 예를 들어, 프린터 `hpdesklj2`가 발행되었는지 확인하려면 다음을 입력합니다.

```
$ net ads printer search hpdesklj2
```

위 명령을 실행한 후의 출력은 다음과 같습니다.

```
objectClass: top
objectClass:leaf
objectClass:connectionPoint
objectClass:printQuene
printerName:hpdesklj2
serverName:HPSERVERA
```

Windows 클라이언트에서는 다음 단계에 따라 프린터가 발행되었는지 확인할 수도 있습니다.

단계 **1.** Windows 클라이언트에 프린터 관리 목록의 구성원인 사용자로 로그인합니다. 예를 들어, 사용자 이름 `cifsuser1`을 사용할 수 있습니다.

단계 **2.** `start`를 클릭합니다.

단계 **3.** `search` 탭을 클릭합니다.

단계 **4.** 단추를 클릭하여 네트워크 프린터를 찾습니다.

단계 **5.** `In` 상자에서 ADS 도메인의 이름을 선택합니다.

단계 **6.** `find now` 탭을 클릭합니다.

프린터 발행에 사용되는 명령

이 절에서는 HP CIFS Server에서 프린터 발행 지원에 사용되는 `net ads printer` 명령에 대해 설명합니다.

프린터 검색

Windows 2000/2003 ADS 도메인 전체에서 프린터를 검색하려면 다음 명령을 실행합니다.

```
$ net ads printer search <printer_name>
```

프린터 이름을 지정하지 않으면 이 명령은 ADS 도메인에서 사용 가능한 모든 프린터를 검색합니다.

예를 들어, 다음 명령은 ADS 도메인에서 사용할 수 있는 모든 프린터를 검색합니다.

```
$ net ads printer search
```

위 명령을 실행한 후의 출력은 다음과 같습니다.

```
objectClass: top
objectClass:leaf
objectClass:connectionPoint
objectClass:printQuene
printerName:hpdesklj2
serverName:HPSERVERA

objectClass: top
objectClass:leaf
objectClass:connectionPoint
```

```
objectClass:printQuene
printerName:lj1005
serverName:HPSERVERA

objectClass: top
objectClass:leaf
objectClass:connectionPoint
objectClass:printQuene
printerName:lj3200
serverName:HPSERVERB
```

프린터 제거

ADS 도메인에서 프린터를 제거하려면 다음 명령을 실행합니다.

```
$ net ads printer remove <printer_name>
```

예를 들어, 다음 명령은 프린터 lj1005를 ADS 도메인에서 제거합니다.

```
$ net ads printer remove lj1005
```

프린터 다시 발행

프린터를 처음으로 발행하려면 "Windows 클라이언트에서 프린터 발행" 절에 있는 절차를 수행해야 합니다. 프린터를 제거한 경우에는 다음 명령을 사용하여 다시 발행할 수 있습니다.

```
$ net ads printer publish <printer_name>
```

예를 들어, 다음 명령은 프린터 lj1005를 ADS 도메인에 다시 발행합니다.

```
$ net ads printer publish lj1005
```

분산 파일 시스템(DFS) 지원 설정

이 절에서는 다음을 위한 절차를 제공합니다.

- HP CIFS Server에 DFS 트리 설정
- HP CIFS Server의 DFS root 디렉토리에 DFS 링크 설정

참고

root 디렉토리의 파일은 공유하지 않는 것이 좋습니다. root 디렉토리 아래의 하위 디렉토리에 대해서만 파일 공유를 설정해야 합니다.

HP CIFS Server에 DFS 트리 설정

이 절차를 통해 DFS 트리를 설정하고 나면 DFS 클라이언트의 사용자는 HP CIFS Server의 *servername**DFS*에 위치한 DFS 트리를 검색할 수 있습니다.

1. 분산 파일 시스템(DFS) root 디렉토리로 작동할 HP CIFS Server를 선택합니다.
2. 매개 변수 `host msdfs`가 `yes`로 설정되도록 *smb.conf* 파일을 수정하여 HP CIFS Server를 DFS 서버로 구성합니다. 예를 들면 다음과 같습니다.

   ```
   [global]
     host msdfs = yes
   ```

3. HP CIFS 분산 파일 시스템(DFS) 서버에서 DFS root로 작동할 디렉토리를 만듭니다.
4. 공유를 만들고 *smb.conf* 파일의 매개 변수 `path = DFS root directory`로 정의합니다. 예를 들면 다음과 같습니다.

   ```
   [DFS]
     path = /export/dfsroot
   ```

5. *smb.conf* 파일을 수정하고 `msdfs root` 매개 변수를 `yes`로 설정합니다. 예를 들면 다음과 같습니다.

   ```
   [DFS]
     path = /export/dfsroot
     msdfs root = yes
   ```

HP CIFS Server의 DFS root 디렉토리에 DFS 링크 설정

HP CIFS Server의 분산 파일 시스템(DFS) root 디렉토리는 DFS 링크를 다른 서버를 가리키는 심볼릭 링크 형태로 보관할 수 있습니다.

DFS root 디렉토리에 DFS 링크를 설정하기 전에, root 디렉토리의 사용 권한과 소유권을 설정해야 지정된 사용자만 DFS 링크를 작성, 삭제 또는 수정할 수 있습니다.

심볼릭 링크 이름은 모두 소문자여야 합니다. DFS 공유에 액세스하는 모든 클라이언트는 동일한 사용자 이름과 암호를 가져야 합니다.

다음은 DFS 링크 설정의 예제입니다.

1. `ln` 명령을 사용하여 */export/dfsroot* 디렉토리에서 "linka" 및 "linkb"의 DFS 링크를 설정합니다. "linka" 및 "linkb"는 모두 네트워크의 다른 서버를 가리킵니다. 다음은 명령의 예제입니다.

```
cd /export/dfsroot
chown root /export/dfsroot
chmod 775 /export/dfsroot
ln -S msdfs:serverA\\shareA linka
ln -S msdfs:serverB\\shareB serverC\\shareC linkb
```

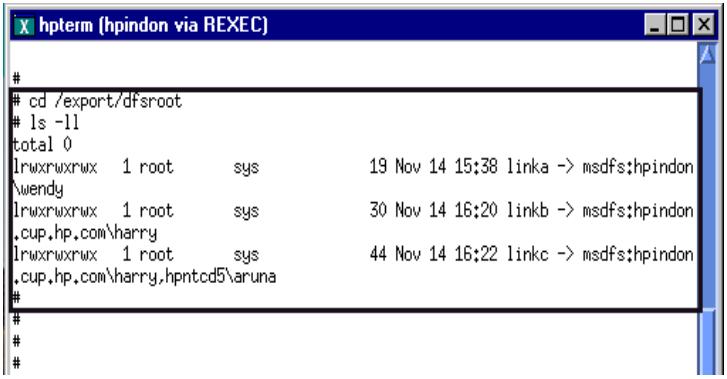
2. */export/dfsroot* 디렉토리에서 `ls -l` 명령을 사용하면 다음과 비슷한 출력 결과가 표시됩니다.

```
lrwxrwxrwx 1 root sys 24 Oct 30 10:20
linka -> msdfs:serverA\\shareA
lrwxrwxrwx 1 root sys 30 Oct 30 10:25
linkb -> msdfs:serverB\\shareB, serverC\\shareC
```

이 예제에서 "serverC"는 "linkb"의 대체 경로입니다. 따라서 "serverB"의 작동이 중단되어도 "linkb"는 여전히 "serverC"를 통해 액세스할 수 있습니다. "linka" 및 "linkb"는 공유 이름입니다. 사용자는 둘 중 한 쪽에만 액세스되면 네트워크의 적절한 공유로 이동할 수 있습니다.

다음 화면 스냅샷 예제를 참조하십시오.

그림 2-2 **링크 공유 이름 예제**



MC/ServiceGuard 고가용성 지원

고가용성 HP CIFS Server에서는 HP CIFS Server 제품을 노드의 MC/ServiceGuard 클러스터에서 실행할 수 있습니다. MC/ServiceGuard를 사용하면

HP 9000 서버 컴퓨터의 고가용성 클러스터를 만들 수 있습니다.

A.01.08 버전의 템플릿 파일이 개선된 결과, 클러스터 노드 수에 제한받지 않으며 이전 스키마에 비해 다른 여러 이점을 얻게 되었습니다.

6장에서 제공하는 구성 절차를 따릅니다.

4단계: HP CIFS Server 시작

winbind 지원을 사용하지 않는 경우에는 아래 스크립트를 실행하여 Samba를 시작합니다.

```
/opt/samba/bin/startsmb
```

winbind 지원을 사용하도록 HP CIFS Server를 구성하는 경우에는 아래 스크립트를 실행하여 Samba를 시작합니다.

```
/opt/samba/bin/startsmb -w
```

또는 `/opt/samba/bin/startsmb --winbind`

이 명령으로 Samba가 성공적으로 시작된 경우, 시작된 특정 프로세스를 나타내는 메시지가 표시됩니다. 스크립트가 성공적으로 수행된 경우 종료 값은 0입니다. 스크립트가 실패하면 종료 값은 1입니다.

Samba 설치 및 구성이 끝났습니다.

winbind 지원을 사용하지 않는 경우에는 아래 스크립트를 실행하여 Samba를 중지합니다.

```
/opt/samba/bin/stopsmb
```

winbind 지원을 사용하는 경우에는 아래 스크립트를 실행하여 Samba를 중지합니다.

```
/opt/samba/bin/stopsmb -w
```

또는 `/opt/samba/bin/stopsmb --winbind`

스크립트가 성공적으로 수행된 경우 종료 값은 0입니다. 스크립트가 실패하면 종료 값은 1입니다.

다음 명령을 사용하면 smbd 및 nmbd 실행에 영향을 미치지 않고도 Winbind 실행을 제어할 수 있습니다.

winbind만 시작하려면 다음 명령을 실행합니다.

```
/opt/samba/bin/startwinbind
```

winbind만 중지하려면 다음 명령을 실행합니다.

```
/opt/samba/bin/stopwinbind
```

개별적으로 데몬 시작 및 중지

startsmb 및 stopsmb 스크립트에는 데몬을 개별적으로 시작 및 중지하는 두 가지 새 옵션 -n(nmbd만) 및 -s(smbd만)가 추가되었습니다. startsmb -s 명령은 smbd 데몬을 시작합니다. stopsmb -s 명령은 smbd 데몬을 중지합니다. -n 옵션은 nmbd 데몬을 같은 방식으로 시작 및 중지합니다.

시스템 부팅 시 자동 시작 구성

HP CIFS Server를 처음으로 설치하면 부팅 시에 자동으로 시작되지 않습니다. 이 때 */etc/rc.config.d/samba* 파일을 편집하면 HP CIFS Server 및 관련 데몬이 부팅 시에 자동으로 시작되도록 만들 수 있습니다. 이 구성 파일에는 다음 두 변수가 있습니다.

```
RUN_SAMBA=0
RUN_WINBIND=0
```

RUN_SAMBA 변수는 시스템을 시작할 때 HP CIFS Server 데몬 smbd 및 nmbd가 시작되는지 여부를 결정합니다. RUN_WINBIND 변수는 시스템을 시작할 때 winbind 데몬 winbindd가 시작되는지 여부를 결정합니다. 두 변수는 독립적으로 작동합니다.

HP CIFS Server가 자동으로 시작되도록 구성하려면 RUN_SAMBA를 0이 아닌 값으로 설정합니다. Winbind가 자동으로 시작되도록 구성하려면 RUN_WINBIND를 0이 아닌 값으로 설정합니다. 예를 들어, 시스템을 시작할 때 HP CIFS Server 및 Winbind가 자동으로 시작되게 하려면 */etc/rc.config.d/samba* 파일의 변수를 다음과 같이 편집합니다.

```
RUN_SAMBA=1
RUN_WINBIND=1
```

데몬을 중지했다가 다시 시작하여 새 설정 적용

smb.conf 구성 파일은 변경되면 매분 자동으로 다시 로드됩니다. SIGHUP를 CIFS 서버로 보내면 강제로 다시 로드를 실행할 수 있습니다. 구성 파일을 다시 로드해도 이미 연결된 서비스에는 영향을 주지 않습니다.

하지만 smb.conf에 있는 다음 매개 변수의 새 설정을 적용하려면 CIFS 서버 데몬을 중지했다가 다시 시작해야 합니다.

- netbios aliases

- interfaces
- auth methods
- passdb backend
- invalid users
- valid users
- admin users
- read list
- write list
- printer admin
- hosts allow
- hosts deny
- hosts equiv
- preload modules
- wins server
- vfs objects
- idmap backend

기타 Samba 구성 문제

개방 모드 잠금을 HP-UX로 변환

HP CIFS Server A.01.07 이후 버전은 개방 모드 잠금을 HP-UX로 변환할 수 있습니다. 이 기능을 사용하면 HP-UX 프로세스는 CIFS Client의 개방 모드 잠금과 충돌하는 경우 파일에서 자문 잠금을 얻지 않습니다. 즉, HP-UX 프로세스의 자문 잠금과 충돌하는 경우 CIFS Client는 파일을 열 수 없습니다.

개방 모드 잠금을 HP-UX로 바꾸려면 `smb.conf`의 `map share modes` 설정을 **yes**로 변경해야 합니다. `map share modes`의 기본 설정은 **no**입니다.

변경 알림을 사용한 성능 조정

이 절에서는 **변경 알림** 기능 및 국제화를 사용한 성능 조정에 대해 설명합니다.

Samba Server에서는 **변경 알림**이라고 하는 새 기능을 지원합니다. **변경 알림** 기능을 사용하면 클라이언트는 매핑된 파일 공유의 디렉토리 아래에 있는 파일 또는 하위 디렉토리에 변경이 있을 경우 서버로부터 알림을 요청할 수 있습니다. 지정된 디렉토리 내에 포함된 파일 또는 디렉토리가 수정된 경우 서버는 클라이언트에게 이 사실을 알립니다. 이 기능의 목적은 클라이언트 화면의 Windows 탐색기가 최신 정보를 유지하도록 하는 것입니다. 그 결과, 사용자가 Windows 탐색기를 통해 보고 있는 파일이 변경되면 이는 즉시 화면에 반영됩니다.

Samba에서 이 기능을 구현하는 유일한 방법은 해당 디렉토리 아래의 모든 파일과 하위 디렉토리를 주기적으로 검색하고 마지막 검색 이후에 변경이 있었는지 확인하는 것입니다. 이 작업은 리소스를 많이 사용하므로 Samba뿐 아니라 시스템에서 실행되는 다른 응용 프로그램의 성능에 영향을 끼칠 수 있습니다. 검색의 리소스 사용량에 영향을 주는 주요 요소는 변경 알림 요청이 있는 디렉토리 수와 해당 디렉토리 크기의 두 가지입니다. Windows 탐색기(또는 다른 파일 브라우저)를 실행하는 클라이언트가 많거나 공유 디렉토리에 파일 및/또는 하위 디렉토리가 많은 경우 각 검색 주기에서는 CPU 사용량이 많아집니다.

성능상의 영향을 줄이기 위해, 모니터링하도록 요청된 디렉토리에서 Samba의 변경 검색 주기를 조절할 수 있습니다. Samba의 변경 검색 주기를 조절하는 매개 변수는 *Change Notify Timeout*입니다. 매개 변수 값은 각 검색 주기 시작 사이의 초를 나타냅니다. 기본값은 60입니다. 따라서 시스템이 **변경 알림 요청**이 있는 모든 디렉토리를 검색하는 데 55초가 걸린다면 항상 높은 부하가 걸리게 됩니다.

Change Notify Timeout 값을 더 큰 값으로 늘리면 **변경 알림** 디렉토리 검색 주기를 줄일 수 있습니다. 이 방법의 문제는 클라이언트가 변경 알림을 요청한 디렉토리 내의 변경을 **보는** 시간이 늦어진다는 점입니다. 성능 감소라는 문제와 클라이언트 파일 브라우저의 업데이트가 늦어지는 문제 사이에서 적절하게 선택해야 합니다.

CFS(Clustered File System)에서 HP CIFS Server를 사용하는 경우의 특수 고려 사항

CFS를 사용하면 여러 시스템에서 데이터에 액세스하면서도 파일 시스템의 장점을 활용할 수 있습니다. 하지만 HP CIFS Server를 포함한 응용 프로그램이 항상 클러스터를 인식할 수 있는 것은 아닙니다. Veritas CFS 환경에서 HP CIFS Server를 사용하는 경우에는 다음에 유의해야 합니다.

- 여러 노드에서 동시에 실행되는 CIFS Server가 Veritas CFS를 사용하여 `smb.conf` 구성을 공유하면 안 됩니다.

  이름/IP 등록 충돌 등 여러 노드에서 구성 파일을 공유하면 안 되는 실무적인 이유가 여러 가지 있습니다. 또한 `smb.conf` 파일을 공유하면 CIFS Server 시스템 데이터도 공유되어 동시 파일 액세스가 늘어나고 CIFS Server가 손상될 가능성도 커집니다.

- A.02.02에서는 다른 마스터 데몬이 Veritas CFS를 통해 다른 노드의 데몬 PID를 공유하는 경우 HP CIFS Server가 시작되지 않습니다. (구성 데몬 PID 파일이 같은 노드에서 공유되는 경우 HP CIFS Server는 같은 노드에서 여러 마스터 데몬을 시작할 수 없습니다. 기본적으로 PID 파일은 `/var/opt/samba/lock` 경로에 있습니다.) CIFS에서 이렇게 하는 이유는 위에서 설명한 것과 같은 CIFS Server 구성의 공유 문제를 방지하기 위해서입니다.

- HP CIFS Server를 사용하여 여러 노드에서 동시에 Veritas CFS 디렉토리를 공유하지 말아야 합니다.

  Veritas CFS에서는 클러스터의 여러 노드를 통해 같은 파일을 동시에 읽고 쓸 수 있기 때문에 클러스터 시스템의 여러 노드에서 HP CIFS Server를 구성하는 경우에는 특히 주의해야 합니다. 동시 파일 액세스를 사용하면 여러 작성자가 서로의 작업을 덮어써서 데이터가 손상될 수 있습니다.

- smb.conf 매개 변수 `strict locking`을 `yes`로 설정하면 데이터 손상을 방지할 수 있지만 이 경우 성능이 저하될 수 있습니다.

  기본적으로 HP CIFS Server는 여러 클라이언트(그리고 Veritas CFS를 공유하는 여러 노드)에서 파일에 액세스할 수 있게 해 주기 때문에 동시 파일 액세스가 발생할 수 있고, 따라서 데이터가 손상될 가능성도 약간 있습니다. 그래서 HP CIFS Server은 동시 파일 액세스를 방지하는 "strict locking" 메커니즘을 제공합니다. `smb.conf`에서 `strict locking`이 `yes`로 설정되어 있으면 서버는 파일의 모든 읽기 및 쓰기 액세스에 대해 파일 잠금을 확인하고 잠금이 있으면 액세스를 거부합니다. 일부 시스템에서 이 확인이 느리게 실행되고, 중요한 경우에는 클라이언트에서 잠금 확인을 요청하는 경우가 많기 때문에 대부분의 환경에서는 `smb.conf`의 `strict locking`을 `no`로 설정하는 것이 좋습니다.

3 Windows NT/XP/2000에서 HP-UX 파일 액세스 권한 관리

소개

이 장에서는 Windows NT, XP 및 2000 클라이언트를 사용하여 HP CIFS Server의 표준 UNIX 파일 사용 권한 및 VxFS POSIX 액세스 제어 목록(ACL)을 확인 및 변경하는 방법을 설명합니다. 또한 새 구성 옵션인 acl_schemes도 소개합니다.

UNIX 파일 사용 권한 및 POSIX ACL

HP CIFS Server는 Windows NT, XP 또는 Windows 2000 클라이언트에서 UNIX 파일 사용 권한 또는 VxFS POSIX ACL을 조작할 수 있도록 합니다. 이 기능을 사용하면 친숙한 Windows 탐색기 인터페이스로 UNIX 파일 사용 권한 또는 POSIX ACL을 관리하는 대부분의 작업을 수행할 수 있습니다.

참고

파일 ACL의 개념은 Windows와 HP-UX 플랫폼에서 비슷하긴 하지만 UNIX ACL을 Windows ACL로 대체할 수 없다는(즉 완벽한 에뮬레이션이 제공되지 않는다는) 기능상의 중요한 차이가 있습니다. 예를 들어, Windows 응용 프로그램이 HP CIFS Server에 있는 파일의 ACL 데이터를 변경할 경우 예상하지 못한 동작이 발생하게 됩니다.

Windows NT에서 UNIX 사용 권한 보기

NT와 UNIX의 파일 사용 권한 및 VxFS POSIX간의 ACL 데이터가 서로 다르므로 Samba는 UNIX에서 NT로, NT에서 UNIX로 데이터를 매핑해야 합니다.

다음 표는 UNIX 파일 사용 권한을 Windows NT ACL 액세스 유형으로 변환하는 방법을 보여줍니다.

표 3-1

UNIX 사용 권한	NT 액세스 유형
r--	특별 액세스(R)
-w-	특별 액세스(W)
--x	특별 액세스(X)
rw-	특별 액세스(RW)
r-x	읽기(RX)
-wx	특별 액세스(WX)
rwx	특별 액세스(RWX)

표 3-1 **(계속)**

UNIX 사용 권한	NT 액세스 유형
r--	특별 액세스

위에 표시된 사용 권한 모드 외에도, UNIX 파일 사용 권한은 파일 소유자, 파일 소유 그룹 및 기타(다른 모든 사용자 및 그룹)를 구분합니다.

NT ACL에서 UNIX 파일 소유자 변환

UNIX 파일 시스템 소유자는 다른 사용자에게 없는 추가 사용 권한을 갖습니다. 예를 들어, 소유자는 파일에 대한 자신의 소유권을 전달하거나 파일을 삭제하거나, 파일의 이름을 변경하거나 파일의 사용 권한 모드를 변경할 수 있습니다. 이러한 기능은 Windows NT 클라이언트의 삭제(D), 변경 권한(P) 및 소유권 가져오기(O) 권한과 비슷합니다. Samba는 Windows NT 탐색기 인터페이스에서 UNIX 파일 소유권을 표시하기 위해 *DPO* 권한을 추가하였습니다.

예를 들어, UNIX 파일 시스템의 파일이 UNIX 사용자 *john*의 소유이고 *john*은 이 파일에 대해 읽기 및 쓰기(rw-) 권한을 가진 경우 Windows NT 클라이언트는 사용자 *john*의 이러한 권한을 다음과 같이 표시합니다.

특별 액세스(RWDPO)

또한 Windows NT 탐색기 인터페이스에서 UNIX 소유자를 표시할 수 있습니다. **파일 등록 정보** 대화 상자에서 보안 탭을 선택한 다음 **소유권 단추**를 누르면 소유자인 UNIX 사용자의 이름이 표시됩니다.

NT ACL에서 UNIX 소유 그룹 변환

UNIX 파일 시스템의 **소유 그룹**은 Windows NT 클라이언트에서 **소유권 가져오기**(O) 권한으로 표시됩니다. NT에서 **소유권 가져오기** 권한의 의미가 UNIX 파일 시스템에서의 소유 그룹의 의미와 정확히 일치하지는 않지만 그래도 이 권한은 소유권 **가져오기** 권한으로 변환됩니다.

UNIX 파일 시스템의 개별 파일에 서로 다른 사용 권한을 가진 그룹이 여럿 있을 수 있으므로 이러한 표현은 VxFS POSIX ACL을 변환할 때 더욱 중요해집니다. 이러한 사용 권한 유형이 없으면 소유 그룹 항목과 다른 그룹 항목을 구분할 수 없게 됩니다.

예를 들어, UNIX 파일 시스템의 *sales*라는 소유 그룹이 파일에 대해 **읽기** 및 **실행**(r-x) 사용 권한을 가진 경우 Windows NT 클라이언트는 *sales* 그룹의 사용 권한을 다음과 같이 표시합니다.

특별 액세스(RXO)

NT ACL에서 UNIX 기타 사용 권한 변환

UNIX에서 기타 사용 권한 항목은 **소유자**가 아니며 **소유 그룹**에 속하지 않는 모든 사용자 또는 그룹을 나타냅니다. 이 항목은 Windows NT 클라이언트에서 **모두** 액세스 제어 항목으로 매핑됩니다.

NT 디렉토리 및 파일 사용 권한 변환

Windows NT 클라이언트는 디렉토리 항목에 **디렉토리** 권한과 **파일** 권한의 두 가지 권한이 표시됩니다. 디렉토리 사용 권한은 디렉토리 자체에 대한 사용 권한입니다. 파일 사용 권한은 해당 디렉토리에서 작성된 파일 및 하위 디렉토리로부터 상속한 사용 권한입니다. Samba는 디렉토리에 대한 UNIX 사용 권한을 Windows NT 디렉토리 사용 권한으로 변환하며 반대의 경우도 마찬가지입니다. UNIX 사용 권한으로/에서 변환되는 경우 Windows NT **파일 사용 권한**이 지원되지 않습니다.

그러나 NT **파일 사용 권한**은 VxFS POSIX ACL의 경우에는 지원됩니다(다음 절에서 설명).

Windows NT에서 UNIX 사용 권한 설정

위에서 설명한 UNIX에서 NT로의 변환을 반대로 수행하는 작업은 한 가지 예외를 제외하면 항상 성공합니다. 그러나 클라이언트에서 사용자나 그룹에 **특별 액세스(DPO)** 또는 **특별 액세스(O)**를 추가해도 **소유자** 또는 **소유 그룹**을 변경할 수는 없습니다.

읽기, 쓰기 및 실행을 제외한 모든 NT 사용 권한은 Samba 서버의 파일에 적용될 때 무시됩니다. 이러한 사용 권한으로는 삭제(D), 변경 권한(P) 및 소유권 가져오기(O) 등이 있습니다.

다음 표는 NT 액세스 유형을 UNIX 사용 권한으로 매핑하는 방법을 보여줍니다.

표 3-2

NT 액세스 유형	UNIX 사용 권한
특별 액세스(R)	r--
특별 액세스(W)	-w-
특별 액세스(X)	--x

표 3-2 **(계속)**

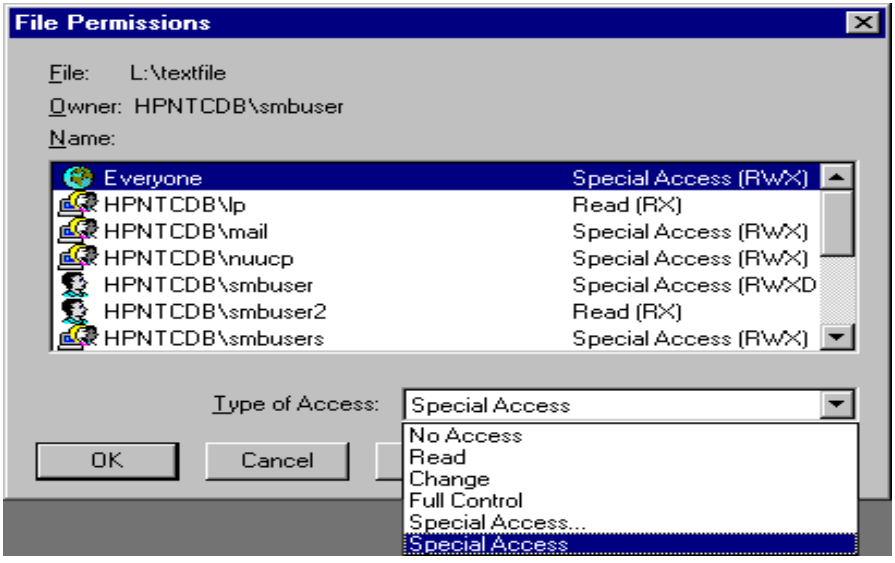
NT 액세스 유형	UNIX 사용 권한
특별 액세스(RW)	rw-
읽기(RX)	r-x
특별 액세스(WX)	-wx
특별 액세스(RWX)	rwx
특별 액세스	r--

NT에서 UNIX 파일 사용 권한으로 매핑할 경우에는 새로운 NT ACL 항목을 추가할 수 없는데, 그 이유는 UNIX 사용 권한에서는 **소유자**, **소유 그룹** 및 **기타** ACL 항목만 지원되기 때문입니다. UNIX는 알 수 없는 항목을 무시합니다. 반대로 위에 나열한 세 항목은 UNIX에서 필요한 것이므로 삭제할 수 없습니다.

미리 정의된 NT 사용 권한

Windows NT 탐색기 ACL 인터페이스를 사용하면 사용자 정의 특별 액세스 사용 권한을 만들 수 있을 뿐만 아니라 **변경** 및 **모든 권한**과 같은 미리 정의된 사용 권한을 선택할 수도 있습니다.

그림 3-1 **Windows NT 탐색기 ACL 인터페이스**



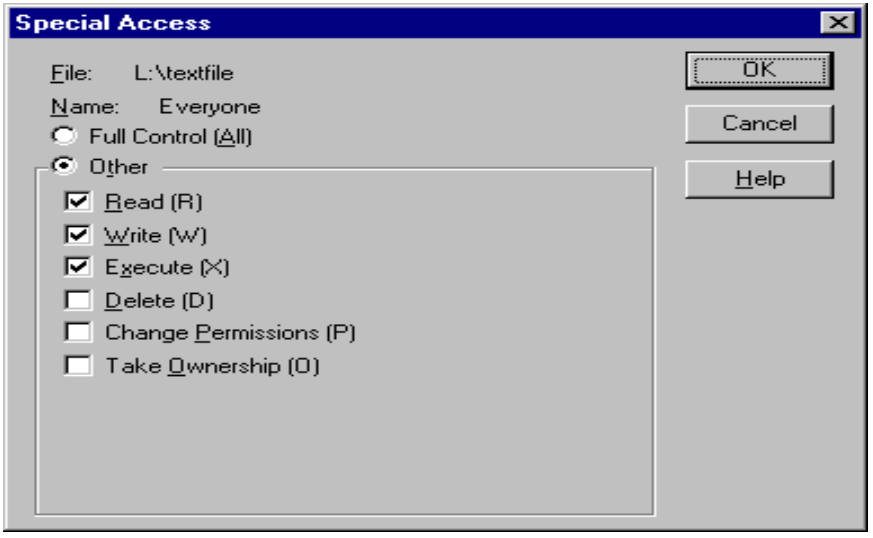
미리 정의된 NT 액세스 유형을 사용하여 Samba 공유의 사용 권한을 설정하면 나중에 표시되는 사용 권한이 NT에서 설정한 사용 권한과 일치하지 않게 됩니다.

예를 들어, **모든 권한**은 Samba 서버에서 *rwx*가 되며 Windows NT 클라이언트에서 표시될 때는 **특별 액세스(RWX)**로 표시됩니다.

표 3-3

NT 액세스 유형	UNIX 사용 권한
권한 없음	---
읽기	r-x
바꾸기	rwx
모든 권한	rwx

그림 3-2 **Windows NT 특별 액세스 사용 권한**



VxFS POSIX ACL 파일 사용 권한

VxFS POSIX ACL은 UNIX 파일 사용 권한의 상위 집합입니다. VxFS POSIX ACL은 다음 세 가지 방식으로 UNIX 파일 사용 권한의 개념을 확장합니다.

- VxFS POSIX ACL은 기본 소유자, 그룹 및 기타 UNIX 파일 사용 권한보다 많은 항목을 허용합니다.
- VxFS POSIX ACL은 디렉토리 사용 권한에 대해 기본적인 액세스 제어 항목(ACE)을 지원합니다. 이는 이 디렉토리에서 만들어진 모든 파일은 자동으로 부모 디렉토리의 기본 ACE를 상속한다는 것을 의미합니다. 또한 디렉토리 사용 권한에 상속 사용 권한 유형이 추가됩니다.
- *class* ACE라고 하는 특별 ACE가 사용됩니다. class *ACE*의 역할은 다른 ACE를 제한하는 것입니다. 기본 UNIX 사용 권한은 영향을 받지 않습니다.

  예를 들어, 파일에 *class ACE*가 읽기(**r--**)로 설정되면 ACE에서 일부 사용자 및 그룹에 **쓰기** 및 **실행** 액세스 권한을 주더라도 실제로는 이 권한이 부여되지 않습니다. *class ACE*는 비 class ACE의 사용 권한을 걸러 내는 마스크 역할을 합니다. *class ACE*가 (**---**) 또는 권한 없음으로 설정된 경우, 다른 ACE가 존재할 수는 있지만 실제 사용 권한이 변경되지는 않습니다.

VxFS POSIX ACL을 NT ACL로 변환

그 밖의 VxFS POSIX ACL 기능은 다음과 같이 NT ACL로의 변환 및 NT ACL로부터의 변환에 영향을 줍니다.

- 기타 *VxFS POSIX ACE*는 Windows NT 클라이언트에서 *NT ACE*로 나타납니다. 사용 권한 모드는 UNIX 사용 권한 모드처럼 변환됩니다. 이 기능을 사용하여 Windows NT 클라이언트에서 새로운 사용자 및 그룹 항목을 추가할 수도 있습니다. 이 기능에 대한 제한 사항은 다음 절에서 설명합니다.
- 디렉토리에서 상속을 위해 지원하는 **기본 ACE**는 NT의 디렉토리에서 **파일 사용 권한**으로 변환됩니다. Windows NT 클라이언트에서 표시되는 파일 사용 권한은 Samba 서버의 UNIX 파일 시스템에서 **기본 ACE**를 나타냅니다. 파일 사용 권한이 NT 클라이언트의 디렉토리에 설정된 경우 이에 대응하는 **기본 ACE**가 UNIX 파일 시스템의 디렉토리에 설정됩니다.
- 다른 ACE를 제한하는 데 사용되는 *class ACE*는 무시됩니다. 이 ACE는 Windows NT 클라이언트에서 표시되지 않으며 NT 클라이언트에서 설정할 수 있는 방법은 없습니다. Windows NT에는 *class ACE*와 유사한 것이 없으므로 클라이언트 측에서 지원하기가 어렵습니다.

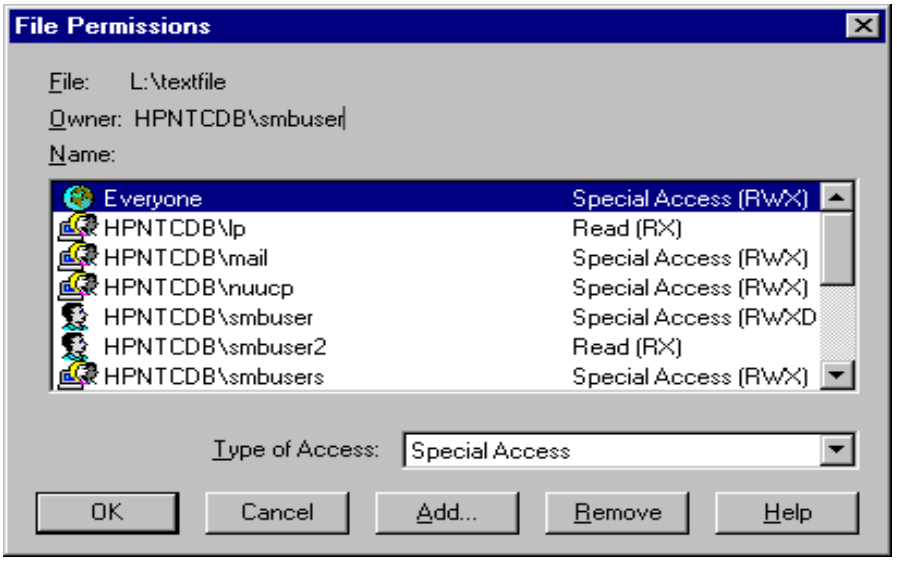
NT 탐색기 GUI를 사용한 ACL 작성

Windows NT 탐색기 GUI를 사용하여 새 ACL을 설정합니다.

이 절에서는 ACE 목록에 새 항목을 추가하는 방법을 설명합니다.

- Windows NT GUI의 파일/디렉토리 사용 권한 대화 상자에서 추가 단추를 클릭하여 사용자 및 그룹 추가 대화 상자를 엽니다.

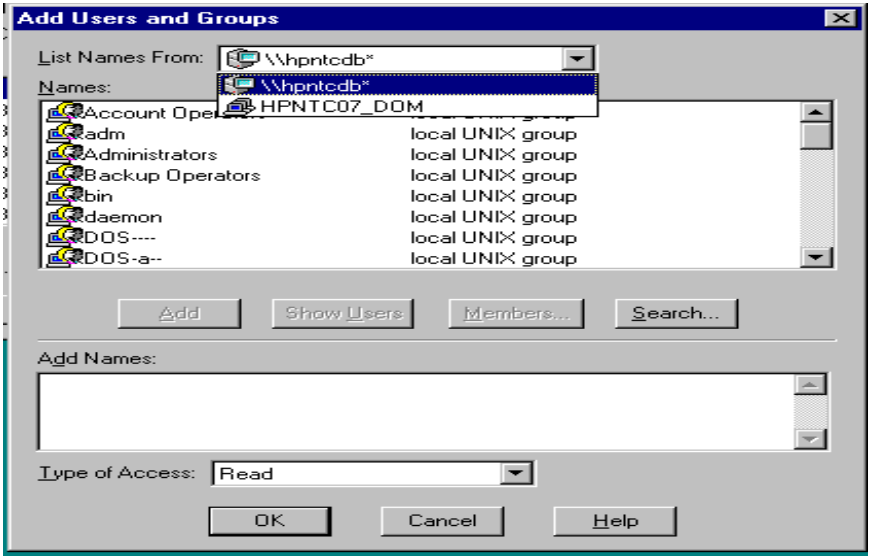
그림 3-3 **Windows NT 탐색기 파일 사용 권한**



참고

도메인 선택 필드는 그룹 이름 목록을 찾을 곳을 표시합니다. 여기에는 사용자의 도메인 이름도 표시됩니다. 새 ACL을 추가하는 데 도메인 목록을 사용하지 마십시오.

그림 3-4 Windows NT 탐색기가 필드에서 이름 나열

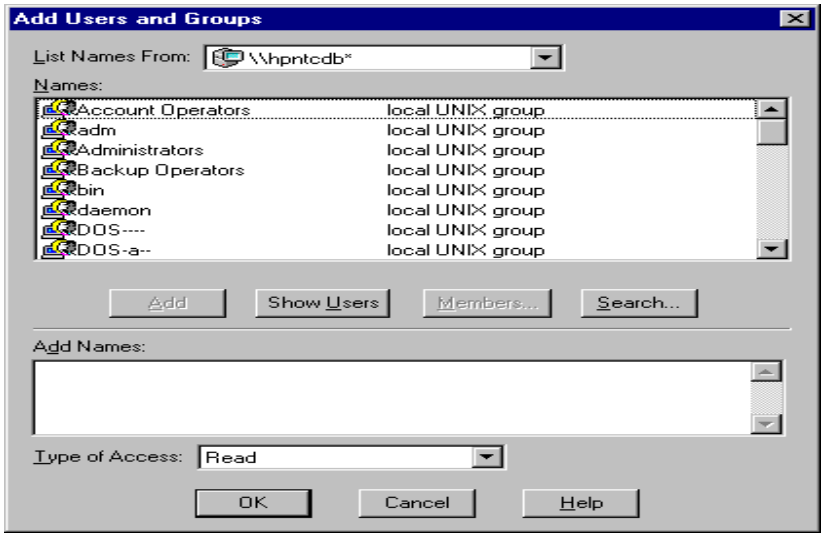


그 대신, 기본 UNIX 파일 시스템에서 인식할 수 있는 그룹 및 사용자의 목록이 필요합니다.

실제 ACL은 최종 형태의 UNIX 파일 사용 권한 또는 VxFS POSIX ACL이기 때문에 유효한 그룹 및 사용자는 Samba 서버가 알고 있는 UNIX 그룹 및 사용자입니다.

- **사용자 및 그룹 추가** 대화 상자의 **도메인 선택** 드롭다운 목록으로 이동합니다. 화면에서는 Samba 서버에 이름을 나열하는 작업만 수행해야 합니다. 이는 HP 권장 목록입니다.

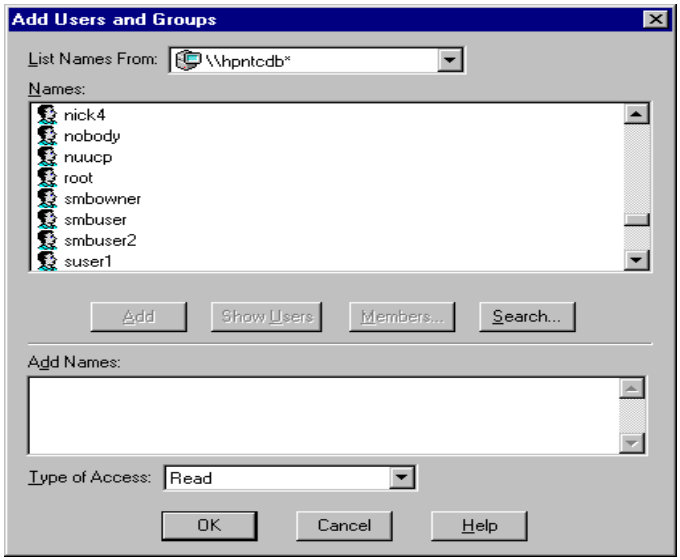
그림 3-5 Windows NT 탐색기 사용자 및 그룹 추가 대화 상자



- *local UNIX group*이라는 이름의 목록에서 임의의 이름을 선택합니다. 이들 그룹은 Samba 서버에 있는 실제 UNIX 그룹입니다.

- 원하는 경우 **사용자 표시** 단추를 클릭하면 Samba 서버상의 모든 UNIX 사용자가 목록에 추가됩니다. 언제든 *local Unix groups* 및 사용자의 ACE를 목록에 추가할 수 있습니다.

그림 3-6 **UNIX 그룹 및 사용자 추가**



- **이름 추가** 텍스트 필드에 사용자 및 그룹 이름을 입력하여 사용자 및 그룹을 추가할 수 있습니다. 이름이 올바른 UNIX 그룹 또는 사용자 이름일 경우 사용자 및 그룹이 추가됩니다.
- 선택적으로 사용자 또는 그룹 이름 앞에 Samba 서버 이름과 역슬래시를 덧붙여 추가할 수도 있습니다(예를 들면, *server1\users1*). 이름 목록에서 이름을 선택하면 GUI에서 해당 이름이 텍스트 목록에 입력되고 서버 이름이 자동으로 추가됩니다.
- 선택적으로 사용자 이름 매핑 기능을 사용하여 NT 사용자 이름(또는 도메인 이름)에서 UNIX 사용자 이름으로 매핑을 정의할 수 있습니다. 예를 들어, NT 사용자 이름 administrator와 admin을 UNIX 사용자 이름 *root*로 매핑할 수 있습니다. 매핑은 일대일 또는 다대일이 될 수 있습니다.

  Samba는 UNIX 사용자 이름으로 매핑된 NT 사용자 이름에 대한 ACE 작성을 지원합니다.

위 예제에 이어 NT 클라이언트에서 *administrator* 사용자에 대한 ACE를 작성하면 Samba 서버에서는 *root* 사용자에 대한 ACE가 작성됩니다. 클라이언트는 해당 ACE를 *administrator* 사용자가 아닌 *root* 사용자에 대한 것으로 표시합니다.

*administrator*와 같은 한 사용자 이름에 대해 ACE를 추가한 다음 ACE 목록을 표시하고 다른 사용자 이름(root)에 대한 새 ACE를 볼 경우 혼란이 생깁니다. 여러 NT 사용자 이름이 한 UNIX 사용자 이름으로 매핑될 수 있기 때문에 Samba는 한 UNIX 사용자 이름만 표시합니다. UNIX 사용자 이름으로 매핑된 NT 이름은 표시할 수 없습니다.

또한 한 UNIX 사용자에 대해 충돌을 일으키는 여러 ACE를 작성하지 않도록 조심해야 합니다. 예를 들어 NT GUI에서 *administrator, admin* 및 *root* 사용자에 대한 ACE를 추가할 수 있습니다. 그러나 Samba는 이러한 변경을 적용할 때 *administrator* 및 *admin*을 UNIX 사용자 *root*로 매핑하며, 그 결과 서로 다른 세 ACE를 모두 사용자 *root*로 한 파일에 추가하려고 합니다. 이는 잘못된 것이며 Samba는 세 ACE 중 두 ACE를 무시합니다.

Samba 이름 목록에서 이름 선택

UNIX 사용자에 매핑된 NT 사용자 이름은 **사용자 및 그룹 추가** 대화 상자의 **사용자 표시** 단추를 누를 때도 표시됩니다. ACE에 추가한 모든 유효한 이름이 Samba 서버의 이름 목록에 있습니다(**사용자 표시** 단추를 누를 경우). 이름을 입력하거나 NT 도메인 목록에서 이름을 선택할 필요가 없습니다. 그러나 NT 도메인 목록에서 선택한 이름이 Samba 서버의 UNIX 사용자 이름이면 이 이름이 추가됩니다. 이는 Samba에서 사용자 이름 매핑이 있는 이름에도 적용됩니다.

이름을 직접 입력하는 대신 Samba 서버의 이름 목록에서 이름을 선택하도록 권장하는 또 다른 이유가 있습니다. 즉, 동일한 이름의 UNIX 그룹과 UNIX 사용자가 있을 수 있기 때문입니다. 목록에서 이름을 선택할 경우 Samba는 그것이 사용자인지 그룹인지 알 수 있습니다. 직접 이름을 입력할 경우 사용자 또는 그룹인지 지정할 방법이 없고, UNIX 그룹 이름을 입력한 경우에도 Samba는 동일한 이름의 사용자에 대해 ACE를 추가하게 됩니다.

POSIX ACL 및 Windows 2000/XP 클라이언트

HP CIFS Server A.01.07 이후 버전을 사용하면 Windows 2000 클라이언트에서 POSIX ACL 사용 권한을 보고 설정할 수 있습니다. 이 절에서는 Windows 2000/XP 사용 권한을 잘 알고 있다는 가정 하에 설명합니다. 이 절의 목적은 HP CIFS Server가 Windows 2000/XP 사용 권한을 해석하는 방법과 Windows 2000/XP 클라이언트가 HP-UX 사용 권한을 해석하고 표시하는 방법을 설명하는 것입니다.

Windows 2000/XP 클라이언트는 Windows NT 클라이언트와 비슷한 방식으로 POSIX ACL과 상호 작용하며 약간의 차이점은 다음 절에서 설명합니다. 이 장의 다음 절에서 ACL 및 Windows 2000/XP 클라이언트에 대해 배울 수 있습니다. 또한 `man aclv`를 실행하여 POSIX ACL에 대해 더 자세히 배울 수 있습니다.

Windows 2000/XP 클라이언트에서 UNIX 사용 권한 보기

다음 표는 HP CIFS Server의 UNIX 사용 권한이 Windows 2000/XP 클라이언트의 기본 및 고급 ACL 보기에 대한 사용 권한에 매핑되는 방식을 보여줍니다.

표 3-4 UNIX 사용 권한의 Windows 2000/XP 클라이언트 사용 권한 매핑

UNIX 사용 권한	Windows 2000/XP 클라이언트에 표시되는 사용 권한	
	기본	고급
r--	읽기	특성 읽기, 확장 특성 읽기, 데이터 읽기, 사용 권한 읽기
-w-	쓰기	특성 쓰기, 확장 특성 쓰기, 데이터 추가, 데이터 쓰기, 사용 권한 읽기
--x	없음	실행 또는 폴더 트래버스, 특성 읽기, 사용 권한 읽기

표 3-4 UNIX 사용 권한의 Windows 2000/XP 클라이언트 사용 권한 매핑(계속)

UNIX 사용 권한	Windows 2000/XP 클라이언트에 표시되는 사용 권한	
r-x	읽기 및 실행	첫 번째 셀의 모든 읽기 사용 권한과 동일 실행 또는 폴더 트래버스
rw-	읽기, 쓰기	첫 번째 셀의 모든 읽기 사용 권한과 동일 두 번째 셀의 모든 쓰기 사용 권한과 동일
rwx	모든 권한	모든 권한 및 모든 사용 권한 정보가 전달됨
---	어떤 권한도 전달되지 않음	없음

참고

위 표에서 **고급**이라고 표시된 사용 권한은 ACL 대화 상자에서 고급, 보기/편집을 차례로 클릭하면 볼 수 있습니다.

파일 소유자 ACE의 경우, 소유권 가져오기, 삭제 및 권한 변경 플래그가 표시됩니다. 파일의 소유 그룹 ACE의 경우, 소유권 가져오기 사용 권한 플래그가 표시됩니다.

그러나 파일 사용 권한이 '모든 권한'인 경우에는 Windows ACE 고급 및 기본 보기의 모든 사용 권한이 전달됩니다.

Windows 2000/XP 클라이언트에서 사용 권한 설정

다음 표는 클라이언트에서 사용 권한을 설정할 때 각 Windows 2000/XP 클라이언트 사용 권한이 UNIX 사용 권한으로 매핑되는 방식을 보여줍니다.

표 3-5 Windows 2000/XP 사용 권한의 UNIX 사용 권한 매핑

Windows 2000/XP	UNIX 사용 권한
모든 권한	rwx
쓰기	-w-
수정	rwx
읽기 및 실행	r-x
읽기	r--
폴더 목록 / 데이터 읽기(**고급**)	r--
특성 읽기(**고급**)	r--
확장 특성 읽기(**고급**)	r--
읽기 사용 권한(**고급**)	r--
파일 만들기 / 데이터 쓰기(**고급**)	-w-
폴더 만들기 / 데이터 추가(**고급**)	-w-
쓰기 특성(**고급**)	-w-
쓰기 확장 특성(**고급**)	-w-
폴더 트래버스 / 파일 실행(**고급**)	--x
하위 폴더 및 파일 삭제(**고급**)	HP-UX에서 의미 없음
삭제(**고급**)	* 설명은 다음 표 참조
변경 권한(**고급**)	* 설명은 다음 표 참조

표 3-5 **Windows 2000/XP 사용 권한의 UNIX 사용 권한 매핑(계속)**

Windows 2000/XP	UNIX 사용 권한
소유권 가져오기(**고급**)	* 설명은 다음 표 참조

* 삭제, 변경 권한 및 소유권 가져오기 사용 권한은 파일 및 그룹 소유권을 나타냅니다. Windows 2000/XP 클라이언트에서는 이러한 권한을 볼 수 있지만 설정할 수는 없습니다.

파일 사용 권한이 모든 권한으로 설정되지 않으면 삭제, 변경 및 소유권 가져오기 사용 권한이 파일 소유자에 대해 표시됩니다. 소유권 가져오기 사용 권한은 파일 소유 그룹에 대해 표시됩니다. 모든 사용자 및 다른 ACE의 경우, 사용 권한이 모든 권한으로 설정되지 않은 한 이러한 사용 권한이 표시되지 않습니다.

참고

위 표에서 **고급**이라고 표시된 Windows 2000 사용 권한은 ACL 대화 상자에서 고급, 보기/편집을 차례로 클릭하면 볼 수 있습니다.

참고

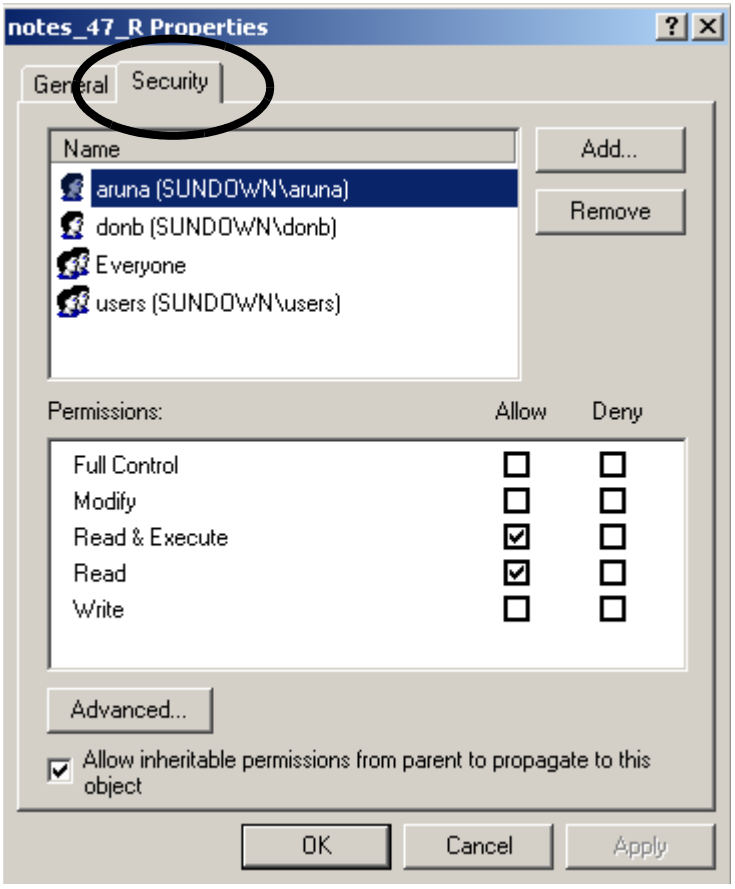
CIFS Server는 파일 소유자에게 적어도 "읽기" 사용 권한이 설정되도록 합니다. 예를 들어, 사용자가 파일의 사용 권한을 "- - -"로 설정하려 할 경우, CIFS Server는 실제 권한을 "r - -"로 설정합니다.

Windows 2000 클라이언트에서 ACL 보기

단계

1. 파일을 마우스 오른쪽 단추로 클릭한 다음 등록 정보를 선택합니다.

단계 **2.** 보안 탭을 클릭합니다.



파일 소유자 표시

단계 **1.** 고급을 클릭합니다.

단계 **2.** 액세스 컨트롤 설정 대화 상자에서 소유자 탭을 클릭합니다.

HP CIFS Server 디렉토리 ACL 및 Windows 2000/XP 클라이언트

디렉토리 ACL 유형

POSIX 아래의 ACL 디렉토리에는 액세스 및 기본 ACE가 포함되어 있습니다. 액세스 ACE는 디렉토리 자체에 대한 액세스를 제어합니다. 기본 ACE는 현재 디렉토리 아래에 만들어진 새 파일 및 하위 디렉토리에 대해 어떤 사용 권한이 설정될 것인지 지정합니다.

Windows 2000 클라이언트에서 ACL 보기

Windows 2000 또는 XP에서 파일 또는 디렉토리에 대한 ACL은 기본 및 고급 보기에 표시됩니다.

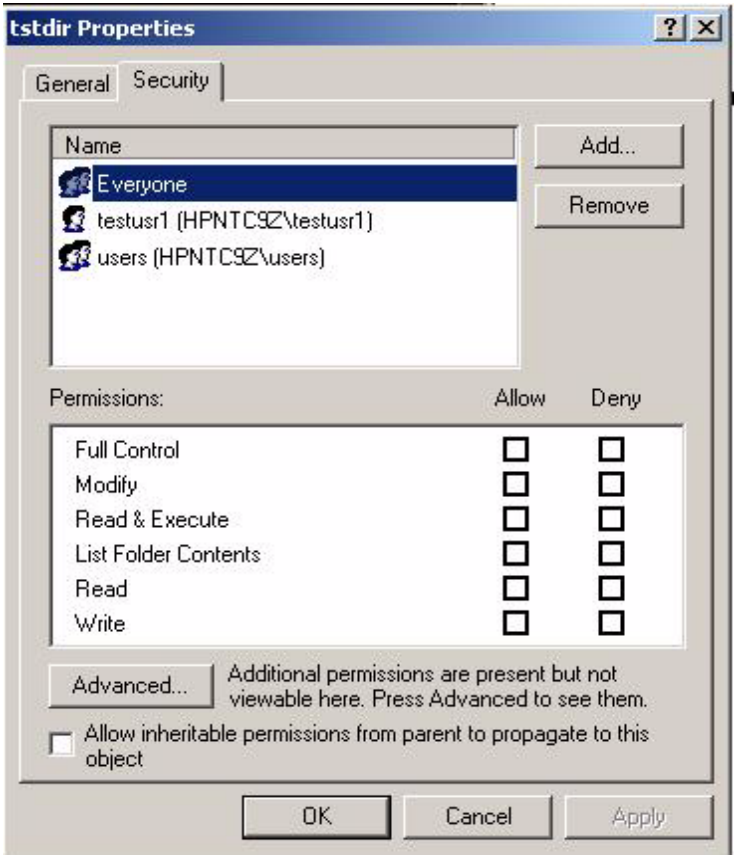
Windows 2000 클라이언트에서 기본 ACL 보기

단계

1. 파일 또는 디렉토리를 마우스 오른쪽 단추로 클릭한 다음 등록 정보를 선택합니다.

단계 **2.** 보안 탭을 클릭합니다.

그림 3-7 **기본 ACL 보기**



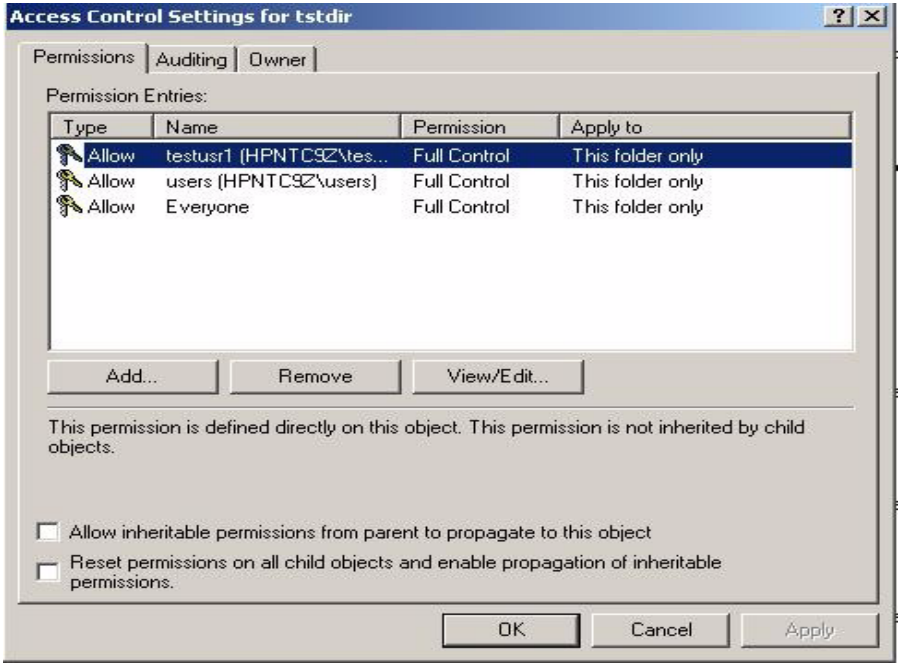
Windows 2000 클라이언트에서 고급 ACL 보기

단계 **1.** 파일 또는 디렉토리를 마우스 오른쪽 단추로 클릭한 다음 등록 정보를 선택합니다.

단계 **2.** 보안 탭을 클릭합니다.

단계 **3.** 고급 단추를 클릭합니다.

그림 3-8 **고급 ACL 보기**



POSIX에 Windows 2000/XP 디렉토리 상속 값 매핑

POSIX 아래에서 기본 ACE는 파일 및 하위 디렉토리 모두에 적용될 수 있습니다. Windows 2000 또는 XP 환경에서 디렉토리 ACE 항목은 POSIX와 다르며 다음의 Windows **상속 값**(Windows 고급 ACE 화면의 **적용 대상** 값)을 사용하여 **액세스**와 **기본** 동작을 구분합니다.

- 이 폴더만
- 이 폴더, 하위 폴더 및 파일
- 이 폴더 및 하위 폴더
- 이 폴더 및 파일

- 하위 폴더 및 파일만
- 하위 폴더만
- 파일만

Windows 고급 ACE 화면에서 디렉토리 ACE를 변경하거나 추가할 때 HP CIFS Server는 Windows **상속 값**을 해당 POSIX ACE 유형에 매핑합니다.

다음 표는 Windows **상속 값**이 POSIX에 매핑되는 방식을 보여줍니다.

표 3-6 **상속 값의 POSIX 매핑 표**

상속 값	HP CIFS Server에 의한 POSIX 매핑
이 폴더만	액세스 ACE로 매핑
이 폴더, 하위 폴더 및 파일	이 유형의 ACE는 액세스 및 기본 ACE 모두로 매핑됨
이 폴더 및 하위 폴더	이 디렉토리에 대한 액세스 ACE**로만** 매핑됨
이 폴더 및 파일	이 디렉토리에 대한 액세스 ACE**로만** 매핑됨
하위 폴더 및 파일만	이 디렉토리에 대한 기본 ACE로만 매핑됨
하위 폴더만	이 유형은 지원되지 않으며 이 유형의 ACE는 HP CIFS Server에서 무시됨
파일만	이 유형은 지원되지 않으며 이 유형의 ACE는 HP CIFS Server에서 무시됨

Windows 2000/XP 클라이언트에서 디렉토리 ACL 수정

참고

HP-UX 디렉토리 ACL은 Windows 2000 또는 XP 클라이언트에서 ACL 기본 사용 권한 화면을 통해 일관성 없이 설정됩니다.

POSIX 디렉토리 ACL을 보거나 변경하려면 Windows 고급 사용 권한 화면(**디렉토리 ->등록 정보 ->보안 탭->고급 단추**)을 사용해야 합니다.

이번 절에서는 Widnows 2000 또는 XP 클라이언트에서 디렉토리 ACE를 수정하는 방법을 설명합니다.

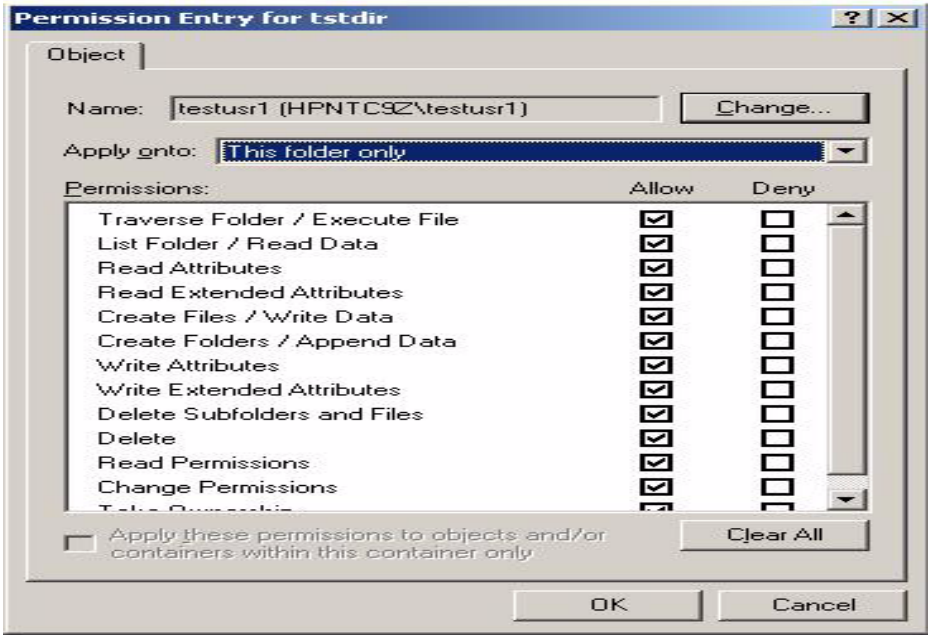
단계 **1.** 디렉토리를 마우스 오른쪽 단추로 클릭한 다음 등록 정보를 선택합니다.

단계 **2.** 보안 탭을 클릭합니다.

단계 **3.** 고급 단추를 클릭합니다.

단계 **4.** ACE를 선택한 다음 보기/편집 탭을 클릭합니다.

그림 3-9 **ACE 사용 권한 수정**



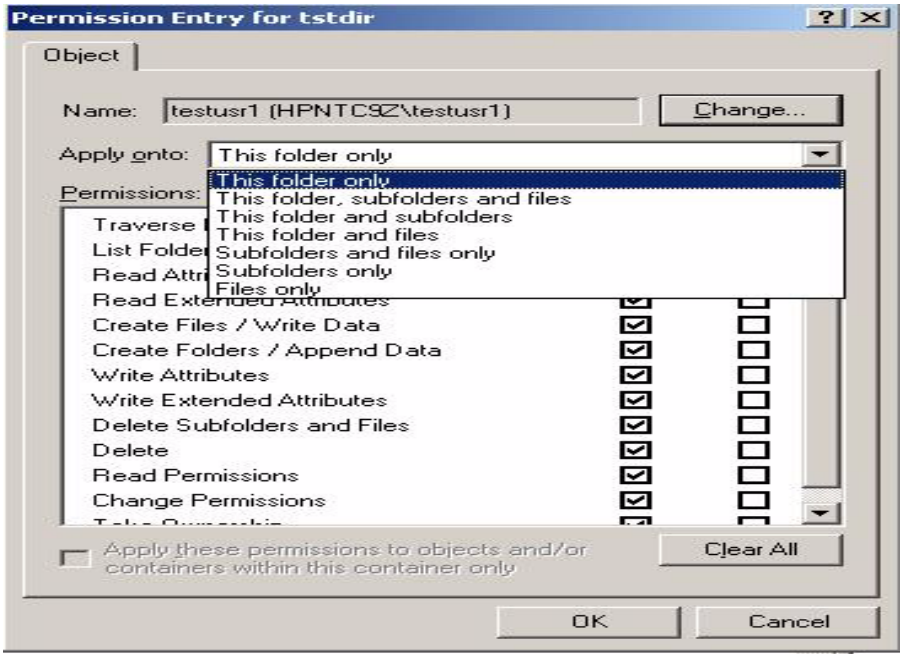
단계 **5.** 각 사용 권한 옆의 확인란을 선택하거나 선택 취소하여 원하는 사용 권한을 추가하거나 제거합니다. 이 창의 각 사용 권한이 UNIX 사용 권한에 어떻게 매핑되는지 자세히 알려면 "Windows 2000/XP 사용 권한의 UNIX 사용 권한 매핑 표"를 참조하십시오.

단계 **6.** 대화 상자의 **적용 대상** 드롭다운 목록에서 해당 ACE 유형을 선택합니다. 각 ACE가 POSIX ACE에 매핑되는 방식에 따라 적절히 선택합니다. 자세한 내용은 "상속 값의 POSIX 매핑 표"를 참조하십시오.

단계 **7.** 확인을 클릭하면 고급 ACE 화면으로 돌아갑니다. 4단계에서 6단계까지 반복하여 다른 ACE를 수정합니다.

단계 **8.** 고급 ACE 화면에서 확인 또는 적용 단추를 클릭합니다.

그림 3-10 **적용 대상 값과 함께 ACE 유형 수정**



중요

동일한 사용자 또는 그룹의 기본 및 액세스 ACE에 대해 서로 다른 사용 권한을 설정하려면 **확인** 단추를 클릭하기 전에 **고급 ACE 보기** 대화 상자에서 두 개의 다른 ACE 항목을 선택해야 합니다.

ACE 항목을 수정하고 **허용** 및 **거부** 확인란을 모두 선택 취소하면 Windows 2000 또는 XP 클라이언트는 해당 ACE를 제거하고 HP CIFS Server에 전달하지 않습니다.

디렉토리 소유자가 액세스 권한을 잃지 않으려면 해당 소유자에 대한 액세스 및 기본 ACE에는 모두 **모든 권한**이 설정되어야 합니다.

Windows 2000/XP 클라이언트에서 ACE 항목 제거

필수 ACL(사용자, 소유 그룹, 모두)의 경우, 고급 Windows 사용 권한 화면에서 ACE 항목을 제거해도 UNIX 시스템에서 해당 ACE 항목은 제거되지 않습니다. HP CIFS Server는 파일에 대한 기존 액세스 ACE로부터 없어진 ACE를 생성합니다.

다른 사용자 또는 그룹 ACE의 경우, 고급 Windows 화면에서 ACE 항목을 제거하면 HP CIFS Server에서 해당 ACE 항목이 제거됩니다.

예제

다음 세 가지 예제는 Windows 2000/XP 클라이언트에서 ACE 항목이 제거될 때 HP CIFS Server에서 디렉토리 ACE가 변경되는 경우를 보여줍니다.

예제 1:

예제 1에서 HP CIFS Server의 `testdir`에 대한 기존 디렉토리 ACE는 다음과 같습니다.

```
# file:testdir
# owner:testuser
# owning group:users
access:owner:rwx
access:owning group:rwx
access:other:rwx
default:owner:rwx
default:owning group:r-x
default:other:r-x
```

예제 1에서, 고급 Windows ACE 화면에서 기본 소유 그룹 ACE 항목인 r-x가 제거되면 HP CIFS Server는 기존 액세스 소유 그룹 ACE인 rwx에 기반하여 없어진 기본 소유 그룹 ACE 항목을 생성합니다. 다음은 HP CIFS Server에서 디렉토리 ACE에 대한 변경 결과를 보여줍니다.

```
# file:testdir

# owner:testuser

# owning group:users

access:owner:rwx

access:owning group:rwx

access:othere:rwx

defualt:owner:rwx

default:owning group:rwx

default:other:r-x
```

예제 2:

예제 2에서 HP CIFS Server의 testdir에 대한 기존 디렉토리 ACE는 다음과 같습니다.

```
# file:testdir

# owner:testuser

# owning group:users

access:owner:rwx

access:owning group:r-x

access:other:rwx

defualt:owner:rwx

default:owning group:r--

default:other:r--
```

예제 2에서, 고급 Windows ACE 화면에서 액세스 소유 그룹 ACE 항목인 r-x와 기본 소유 그룹 ACE 항목인 r--이 고급 Windows ACE 화면에서 제거되면 HP CIFS Server는 기존 액세스 소유 그룹 ACE에 기반하여 없어진 소유 그룹 ACE 항목을 생성합니다. 다음은 HP CIFS Server에서 디렉토리 ACE에 대한 변경 결과를 보여줍니다.

```
# file:testdir
# owner:testuser
# owning group:users
access:owner:rwx
access:owning group:r-x
access:other:rwx
defualt:owner:rwx
default:owning group:r-x
default:other:r--
```

예제 3:

예제 3에서 HP CIFS Server의 testdir에 대한 기존 디렉토리 ACE는 다음과 같습니다.

```
# file:testdir
# owner:testuser
# owning group:users
# other group:testgroup
access:owner:rwx
access:owning group:r-x
access:other group:rw-
defualt:owner:rwx
default:owning group:r--
default:other group:r-w
```

예제 3에서, 고급 Windows ACE 화면에서 액세스 기타 그룹 ACE 항목인 rw-와 기본 기타 그룹 ACE 항목인 r--x가 제거되면 HP CIFS Server는 액세스 기타 그룹 및 기본 기타 그룹 ACE 항목을 모두 제거합니다. 다음은 HP CIFS Server에서 디렉토리 ACE에 대한 변경 결과를 보여줍니다.

```
# file:testdir
# owner:testuser
# owning group:users
```

```
# other group:testgroup
access:owner:rwx
access:owning group:r-x
defualt:owner:rwx
default:owning group:r--
```

Windows 2000/XP 클라이언트에서 디렉토리 ACL 추가

이번 절에서는 Widnows 2000 또는 XP 클라이언트에서 디렉토리 ACE를 추가하는 방법을 설명합니다.

단계 **1.** 디렉토리를 마우스 오른쪽 단추로 클릭한 다음 등록 정보를 선택합니다.

단계 **2.** 보안 탭을 클릭합니다.

단계 **3.** 고급 단추를 클릭합니다.

단계 **4.** 추가 단추를 클릭하면 사용자 또는 그룹 선택 창이 나타납니다.

단계 **5.** 원하는 사용자 또는 그룹을 선택합니다.

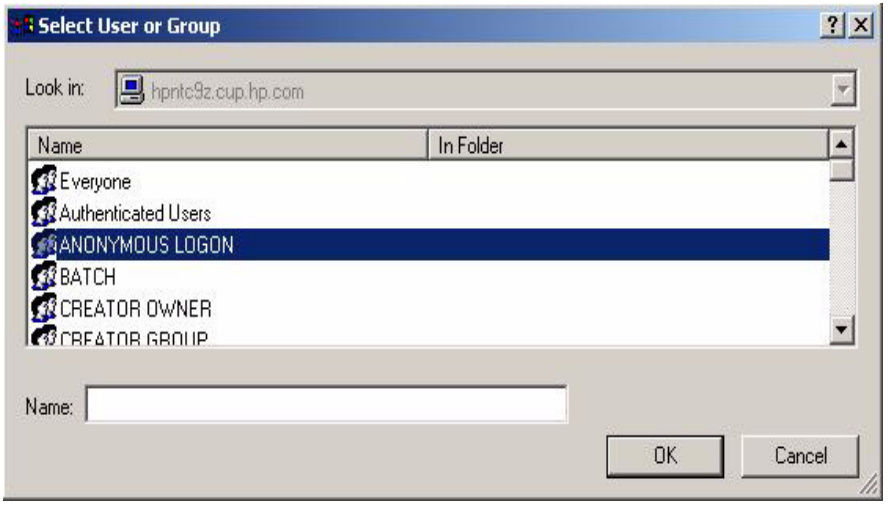
단계 **6.** 확인을 클릭하면 ACE 사용 권한 및 ACE 유형을 입력하라는 메시지가 표시됩니다.

단계 **7.** 원하는 사용 권한을 입력한 다음 확인을 클릭합니다.

단계

8. ACE 고급 보기 화면으로 돌아간 후 확인 또는 **적용** 단추를 클릭하여 새 ACE를 추가합니다.

그림 3-11 **새 ACE 사용자 또는 그룹 선택**



중요

사용 권한이 설정되지 않은 POSIX ACE는 해당 사용자 또는 그룹에 대해 ACE를 추가하고 원하는 사용 권한을 설정하면 수정할 수 있습니다. Windows ACL 인터페이스에서 **추 가** 단추를 클릭하면 새 ACE를 추가할 수 있습니다.

POSIX 기본 소유자 및 소유 그룹 ACL

HP CIFS Server A.01.10 버전의 경우 POSIX 기본 소유자 및 기본 소유 그룹 ACE는 Windows 인터페이스에 `Creator Owner` 및 `Creator Group`으로 표시됩니다.

HP CIFS Server A.01.09 버전 이하의 경우, 해당 액세스 및 기본 ACE에 대한 사용 권한이 서로 동일하면 소유자, 소유 그룹 및 모두에 대해 하나의 ACE만 표시됩니다.

HP CIFS Server A.01.10 버전의 경우, 액세스 및 기본 ACE에 대한 사용 권한이 서로 동일하더라도 POSIX 기본 소유자 및 기본 소유 그룹 ACE는 Windows 인터페이스에 `Creator Owner` 및 `Creator Group`으로 표시됩니다. 그러나 액세스 및 기본 사용 권한이 서로 동일하면 모든 사용자는 오직 하나의 ACE로만 표시됩니다.

Windows `Creator Owner` 및 `Creator Group` ACE에 대한 사용 권한을 변경하면 HP CIFS Server의 POSIX 기본 소유자 및 소유 그룹 ACE만 수정됩니다.

사용 권한이 설정되지 않은 POSIX ACE

사용 권한이 설정되지 않은 POSIX 소유 그룹 및 모든 사용자 ACE는 Windows 인터페이스에 표시되지 않습니다. 예를 들어, HP CIFS Server에서 디렉토리 소유 그룹에 사용 권한이 설정되지 않은 경우 해당 소유 그룹에 대한 ACE는 Windows 인터페이스에 표시되지 않습니다. 사용 권한이 설정되지 않은 다른 사용자나 그룹에 대한 ACE는 Windows 인터페이스에서 사용 권한이 없는 것으로 표시됩니다.

사용 권한이 설정되지 않은 POSIX ACE는 해당 사용자 또는 그룹에 대해 ACE를 추가하고 원하는 사용 권한을 설정하면 수정할 수 있습니다. Windows ACL 인터페이스에서 **추 가** 단추를 클릭하면 새 ACE를 추가할 수 있습니다.

Samba ACL 지원 구성

HP CIFS A.01.07 버전

비 HP Samba 버전에서는 서버별로 Samba의 **NT ACL 지원**을 설정하거나 해제할 수만 있었습니다. 설정될 경우 모든 Samba 공유에 대해 UNIX 파일 사용 권한 지원 기능이 활성화되었습니다. VxFS POSIX ACL을 포함하여 어떤 ACL 체계도 지원하지 않았으며, 대신 *smb.conf* **변수**인 *nt acl support*를 통해 이전 **NT ACL 지원**을 구성했습니다. 이 기능은 HP CIFS 제품에서 계속 지원됩니다.

하지만 HP CIFS에는 Samba ACL 지원을 구성하는 데 사용할 수 있는 새로운 *smb.conf* 변수가 있습니다. 또한 이 Samba 버전에서는 Samba 서버의 모든 공유를 서로 다르게 구성할 수 있습니다.

Samba 공유의 root 아래에 많은 UNIX 파일 시스템이 있을 수 있으므로 한 Samba 공유에 HFS 파일 시스템, VxFS 3.3 파일 시스템, NFS 파일 시스템 및 이전 VxFS 파일 시스템의 파일이 있을 수 있습니다. 공유에 한 유형의 ACL 지원을 할당할 경우 해당 위치에 있는 각 파일 시스템의 기능을 충분히 활용하지 못할 수 있습니다. 따라서 이 버전의 Samba에서는 각 공유에 대해 ACL 스키마 목록을 만들 수 있게 되었습니다.

ACL 스키마의 목록은 해당 공유에 있는 파일에 ACL 스키마를 시도하는 순서를 지정합니다. 현재는 ACL 스키마인 *unix*(UNIX 파일 사용 권한을 의미) 및 *hpux_posix*(HP-UX의 VxFS POSIX ACL을 의미)가 지원됩니다.

다음 예제에서는 HP-UX HFS ACL 또한 지원되며 이 스키마를 *hpux_hfs*라고 가정합니다. *smb.conf*에서 공유별 변수의 이름은 *acl_schemes*입니다.

예제:

다음은 ACL 스키마의 다섯 가지 예제입니다.

예제 1:

acl schemes = hpux_posix hpux_hfs unix

공유가 이 acl 스키마 매개 변수를 설정한 경우 Samba는 VxFS POSIX ACL의 사용을 시도합니다. 이 스키마가 지원되지 않는 경우, HFS ACL을 시도합니다. 이 스키마도 지원되지 않는 경우, UNIX 파일 사용 권한을 사용합니다.

Windows 클라이언트가 이 공유에서 HFS 파일 시스템의 파일에 대한 ACL을 보려고 요청한 경우 Samba는 POSIX ACL 시스템 호출을 사용합니다. 하지만 이 시도는 실패하고 해당 파일에는 ACL 스키마가 지원되지 않음을 나타내는 오류가 반환됩니다. 그런 다음 Samba는 HFS ACL 시스템 호출을 시도하며 이 시도는 성공합니다. 사용자는 이 예제에서 설명한 처음의 실패를 볼 수 없습니다.

예제 2:

acl schemes = unix

이것은 기본 ACL 스키마로서 이전 버전의 Samba와 마찬가지로 기본적으로 UNIX ACL 기능을 무시하고 UNIX 파일 사용 권한을 사용합니다.

예제 3:

acl schemes = none

이 ACL 예제에서는 공유에 대한 모든 ACL 지원을 해제하며 클라이언트가 공유의 임의의 파일 시스템에 있는 ACL 정보를 가져오거나 설정하려 할 때마다 반환될 오류를 생성합니다.

예제 4:

acl schemes = hpux_posix

이 ACL 예제에서는 전체 공유에서 VxFS POSIX ACL만 지원합니다. NFS, HFS 또는 VxFS 3.3 이전 파일 시스템의 파일에 대해 ACL을 가져오거나 설정하려는 클라이언트의 모든 시도는 실패합니다. 이 예제에서는 UNIX 파일 사용 권한을 사용하지 않습니다. ACL 지원은 POSIX ACL을 지원하는 파일 시스템의 파일에 대해서만 작동합니다(현재 VxFS 3.3 이상).

예제 5:

acl schemes = unix hpux_posix

UNIX 파일 사용 권한은 모든 UNIX 파일 시스템 유형에서 지원되므로 이 ACL 예제는 acl scheme을 unix로 설정하는 것과 같습니다(예제 2). 이는 스키마가 목록의 다음 ACL 스키마로 넘어가지 않음을 의미합니다. 각 경우에 시도되는 처음이자 마지막 스키마는 unix 스키마가 됩니다.

위에서 설명한 예제는 Samba 공유에서 임의의 ACL 스키마 조합이 지원되는 방식을 보여줍니다.

ACL 체계 목록에 여러 체계를 두고자 할 경우 효율을 최대화하는 순서를 설정하는 것이 좋습니다. 예를 들어, 가장 많이 액세스되는 파일이 모두 VxFS 3.3 파일 시스템상

의 파일일 경우, *hpux_posix*를 해당 공유의 ACL 스키마 목록에서 맨 앞에 둡니다. 그렇지 않으면 Samba는 올바른 스키마를 찾기까지 다른 ACL 스키마에 대해 여러 번 시스템 호출을 수행하게 됩니다. 이렇게 우선 순위를 설정하는 것은 Samba가 더 많은 ACL 유형을 지원할수록 더욱 중요해집니다.

HP CIFS A.01.08 버전

HP CIFS Server A.01.08 버전의 경우, "nt acl support" 구성 변수가 공유 수준이 됩니다. 이 변수는 전에 전역 수준 변수였습니다. 이 변수의 기본값은 "yes"입니다. 이 변수를 사용하면 공유별로 ACL 지원을 제어할 수 있습니다.

위의 변수를 설정하는 것 외에 ACL 지원에 필요한 다른 특별한 구성은 없습니다.

NT ACL을 지원하는 공유에 대해, CIFS Server는 항상 UNIX 파일 시스템에서 POSIX ACL을 가져오거나 설정하려고 시도합니다. 해당 파일 시스템에서 POSIX ACL을 지원하지 않을 경우 CIFS Server는 Unix 파일 사용 권한을 사용합니다. 이 경우 사용자는 세 가지 기본 ACE(소유자, 그룹 및 모두)만 가져오거나 설정할 수 있습니다. 다른 ACE는 무시됩니다.

CIFS Server A.01.08 버전에서는 구성 변수 "acl schemes"(A.01.07 이하 버전에서 존재)가 지원되지 **않습니다.** 하지만 구성 파일에 이 변수를 넣어도 CIFS Server는 정상적으로 작동합니다.

혼동을 피하려면 구성 파일(*smb.conf*)에서 이 변수를 제거하거나 주석 처리하는 것이 좋습니다.

결론

Samba ACL 지원 기능은 Windows NT/XP/2000 클라이언트에서 UNIX 파일 사용 권한 또는 UNIX ACL을 조작하는 데 사용됩니다.

이 기능을 사용하면 UNIX 사용 권한 또는 VxFS POSIX ACL에 대한 거의 모든 수정 작업을 NT/XP/2000 클라이언트에서 수행할 수 있습니다(VxFS POSIX ACL의 *clas* 항목은 예외).

Windows NT/XP/2000 클라이언트에서 실행되는 Windows 응용 프로그램에서는 완벽한 NT/XP/2000 ACL 지원을 기대할 수 없습니다. 대부분의 NT/XP/2000 ACL 정보는 Samba 서버에 의해 유지되거나 검색되지만, 일부 정보는 손실되거나 변경될 수도 있습니다.

ACL 지원은 NT/XP/2000 ACL 에뮬레이션이 아니며 NT/XP/2000 클라이언트를 통해 UNIX ACL에 액세스하는 것입니다. 따라서 완벽한 NT/XP/2000 ACL 지원을 요구하는 Windows 응용 프로그램은 실행할 수 없습니다.

4 NT 스타일 도메인

소개

이 장에서는 HP CIFS Server 단독으로 구성되는 Samba 도메인인지 여부에 따라 NT 스타일 도메인에서 또는 Microsoft NT 주 도메인 컨트롤러(PDC)를 사용하는 NT 도메인으로서 HP CIFS Server가 수행하는 역할을 구성하는 방법에 대해 설명합니다. 여기서는 NT 스타일 도메인이나 Windows 2000 이전 버전과 호환되는 컴퓨터로서 Windows 2000/2003 도메인에 참여하는 구성원 서버를 구성하는 작업에 대해 설명합니다. Windows 2000/2003 도메인을 컨트롤러를 ADS 구성원 서버로 사용하는 도메인에 참여하는 구성원 서버의 구성에 대해서는 5장, **Windows 2000/2003 도메인**을 참조해야 합니다. 9장, **HP CIFS 배포 모델**에서는 일반적인 네트워크 배포에서 서버 역할을 어떻게 사용할 수 있는지에 대해 자세히 설명합니다.

NT 스타일 도메인 모델에서 다음과 같은 다양한 역할을 수행하도록 HP CIFS Server를 구성할 수 있습니다.

- Microsoft NT PDC를 사용하는 NT 도메인의 구성원 서버
- HP CIFS Server를 PDC로 사용하는 Samba 도메인의 PDC
- HP CIFS Server에서 PDC 역할을 하는 Samba 도메인의 백업 도메인 컨트롤러(BDC)
- HP CIFS Server에서 PDC 역할을 하는 Samba 도메인의 구성원 서버

Samba 도메인 모델의 장점

HP CIFS Server PDC 도메인 모델은 다음과 같은 많은 장점을 제공합니다.

- HP CIFS Server PDC 도메인 관리자는 도메인 컨트롤러의 권한 하에서 워크스테이션 및 서버를 그룹화할 수 있습니다.
- 관련 시스템을 도메인으로 그룹화하여 도메인 구성원을 중앙 집중식으로 관리할 수 있습니다. 이 경우 한 가지 장점은 동일한 사용자 계정을 여러 시스템에서 사용할 수 있다는 것입니다. 사용자가 암호를 한 번만 변경하면 해당 사용자가 액세스하는 모든 시스템에 변경 사항이 적용됩니다. 또 다른 장점은, 각 시스템마다 별도로 계정을 관리해야 할 필요가 없으므로 IT 관리 작업이 줄어든다는 것입니다.

- HP CIFS BDC는 HP CIFS PDC 인증 작업 중 일부를 넘겨받도록 구성할 수 있으며 PDC가 실패하거나 작동을 중지해야 하는 경우 PDC로 승격시킬 수 있습니다.

주 도메인 컨트롤러

주 도메인 컨트롤러(PDC)는 도메인 안에서 다음과 같은 여러 작업을 수행합니다. 여기에는 다음과 같은 작업이 포함됩니다.

- 도메인의 구성원인 사용자 및 워크스테이션의 사용자 로그온 인증
- 도메인의 사용자 계정 및 그룹 정보 관리를 위한 중앙 지점 역할
- 주 도메인 컨트롤러(PDC)에 도메인 관리자로 로그온한 사용자는 도메인에 속한 컴퓨터의 Windows 도메인 계정 정보를 추가, 삭제 또는 수정 가능

백업 도메인 컨트롤러

백업 도메인 컨트롤러의 장점

BDC를 사용하는 HP CIFS Server를 사용하면 다음과 같은 이점이 있습니다.

- BDC는 WAN에 PDC 연결이 끊긴 경우, 도메인의 구성원인 사용자 및 워크스테이션에 대해 사용자 로그온을 인증할 수 있습니다. BDC는 도메인 보안 및 네트워크 통합 모두에서 중요한 역할을 담당합니다.
- PDC의 로컬 네트워크 처리량이 많을 때 BDC가 네트워크 로그온 요청을 받아서 사용자를 인증할 수 있습니다. 따라서 네트워크 서비스의 안정성을 향상시킬 수 있습니다.
- PDC가 사용 불가능하게 되거나 실패하는 경우 BDC는 PDC로 승격될 수 있습니다. 이 기능은 도메인 컨트롤러 관리의 중요한 기능입니다. HP CIFS Server에서 BDC를 PDC로 승격시키려면 `domain master` 매개 변수를 "no"에서 "yes"로 변경해야 합니다.

제한 사항

다음은 BDC 지원에 대한 제한 목록입니다.

- HP CIFS Server는 HP CIFS PDC에 대한 BDC로만 작동할 수 있습니다.

- HP CIFS Server 및 MS Windows 서버는 각 고유의 PDC 유형에 대해 BDC로 작동할 수 있습니다.
- HP CIFS Server는 보안 계정 관리(SAM) 업데이트 델타 파일을 만들 수 없습니다. PDC와 상호 운용이 불가능하므로 BDC에서 유지되는 델타 파일에서 SAM을 동기화할 수 없습니다.
- Samba 3.0 BDC는 PDC에 대한 복제를 지원하지 않습니다. 비 LDAP 백엔드에서 Samba 3.0 BDC를 실행하는 경우 SAM 데이터베이스를 동기화하기가 어려울 수 있습니다. PDC/BDC 하부 구조에 사용할 수 있는 설계 구성에 대한 자세한 내용은 *Official Samba HOWTO and Reference Guide*에서 **표 5.1**, Domain Backend Account Distribution Option을 참조하십시오.

도메인 구성원

- 다음의 구성원 서버를 지원합니다.
  - Windows NT
  - Windows 2000 및 Windows 2003
  - HP CIFS Server
- 도메인 구성원 컴퓨터의 사용자는 도메인 내의 네트워크 리소스에 액세스할 수 있습니다. 이러한 리소스의 예제로는 파일 및 프린터 공유와 응용 프로그램 서버 등을 들 수 있습니다.
- 도메인 구성원은 사용자 로그온에 대해 사용자 인증을 수행하지 않습니다. 그 대신 구성원은 보안 채널을 통해 자격 증명을 도메인 컨트롤로 보냅니다. 도메인 컨트롤러는 이 자격 증명을 데이터베이스에 있는 자격 증명과 비교하여 그 결과를 구성원 서버로 반환합니다. 반환된 결과를 토대로 액세스가 허용됩니다.

HP CIFS Server를 PDC로 구성

주 도메인 컨트롤러(PDC)로 구성된 HP CIFS Server는 Windows 클라이언트(구성원 서버)용 컴퓨터 계정을 만들어야 합니다. 이 기능을 사용하려면 samba_setup 실행 시 "주 도메인 컨트롤러"를 선택한 후 다음 사항을 확인하십시오.

1. PDC 역할을 하는 HP CIFS Server에서 LDAP 백엔드를 사용하지 않는 경우 smb.conf 파일의 내용은 다음과 같습니다.

```
[global]
  workgroup = SAMBADOM #Samba Domain
  security = user
  domain logon = yes
  domain master = yes
  encrypt passwords = yes

[netlogon]
  comment = The domain logon service
  path = /var/opt/samba/netlogon
  writeable = no
  guest ok = no

[profiles]

  comment = profiles Service
  path = /etc/opt/samba/profiles
  read only = no
  create mode = 600
  directory mode =770
```

2. PDC 역할을 하는 HP CIFS Server에서 LDAP 백엔드를 사용하여 UNIX 및 Samba 계정 데이터베이스를 저장하는 경우 smb.conf 파일의 내용은 다음과 같습니다.

```
[global]
  workgroup = SAMBADOM #Samba Domain
  security = user
  domain logon = yes
  domain master = yes
  encrypt passwords = yes
  passdb backend = ldapsam:ldap://ldapserver:389
```

3. 도메인 로그온 서비스에 대한 /var/opt/samba/netlogon 하위 디렉토리가 존재합니다.

참고

security: Windows 사용자, 클라이언트 시스템 계정 및 암호가 smbpasswd 파일이나 LDAP 백엔드에 저장되고 관리되도록 하려면 이 매개 변수를 user로 설정합니다.

domain master: HP CIFS Server가 PDC 역할을 하도록 하려면 이 매개 변수를 yes로 설정합니다.

domain logon: netlogon 서비스를 제공하려면 이 매개 변수를 yes로 설정합니다.

Encrypt passwords: 사용자를 인증하는 데 사용되는 암호를 암호화하려면 이 매개 변수를 yes로 설정합니다. HP CIFS Server가 PDC 역할을 하도록 구성하는 경우 이 매개 변수를 yes로 설정해야 합니다.

HP CIFS Server를 BDC로 구성

HP CIFS Server를 백업 도메인 컨트롤러(BDC) 역할을 하도록 구성하는 경우에는 SWAT 도구나 편집기를 사용하여 /etc/opt/samba/smb.conf 파일에서 상대 도메인 컨트롤러 매개 변수를 구성해야 합니다. smb.conf 파일의 내용은 다음과 같습니다.

- BDC 역할을 하는 HP CIFS Server에서 LDAP 백엔드를 사용하지 않는 경우 smb.conf 파일의 내용은 다음과 같습니다.

```
[global]
  workgroup = SAMBADOM    #Samba Domain
  security = user
  domain logon = yes
  domain master = no
  encrypt passwords = yes
  security = user


[netlogon]
  comment = The domain logon service
  path = /var/opt/samba/netlogon
  writeable = no
  guest ok = no
```

- BDC 역할을 하는 HP CIFS Server에서 LDAP 백엔드를 사용하여 UNIX 및 Samba 계정 데이터베이스를 저장하는 경우 smb.conf 파일의 내용은 다음과 같습니다.

```
[global]
  workgroup = SAMBADOM #Samba Domain
  security = user
  domain logon = yes
  domain master = no
  encrypt passwords = yes
  passdb backend = ldapsam:ldap://ldapserver:389
```

- 상대 도메인 컨트롤러 매개 변수를 구성하는 경우 도메인 로그온 서비스의 /var/opt/samba/netlogon 하위 디렉토리가 있어야 합니다.

HP CIFS에서는 실제 SAM 데이터베이스는 물론 해당 복제도 구현하지 않습니다. BDC의 HP CIFS 구현은 한 가지 중요한 차이점을 제외하고는 PDC와 매우 유사합니다. BDC는 PDC와 거의 비슷하지만, `smb.conf` 매개 변수인 `domain master`를 `no`로 설정해야 한다는 점이 다릅니다.

참고

`security`: Windows 사용자, 클라이언트 컴퓨터 계정 및 암호가 `smbpasswd` 파일이나 LDAP 백엔드에 저장되고 관리되도록 하려면 이 매개 변수를 `user`로 설정합니다.

`domain master`: HP CIFS Server를 BDC로 사용하려면 이 매개 변수를 `no`로 설정합니다.

`domain logon`: netlogon 서비스를 제공하려면 이 매개 변수를 `yes`로 설정합니다.

`Encrypt passwords`: 사용자를 인증하는 데 사용되는 암호를 암호화하려면 이 매개 변수를 `yes`로 설정합니다. HP CIFS Server가 BDC 역할을 하도록 구성하는 경우에는 이 매개 변수를 `yes`로 설정해야 합니다.

Samba 도메인에서 BDC를 PDC로 승격

PDC가 실패하거나 중지되어야 하는 경우에는 BDC에서 `"domain master = yes"`를 설정하기만 하면 됩니다. 이렇게 하면 해당 NetBIOS 이름이 등록되고 PDC 역할을 하는 것으로 간주됩니다.

도메인 구성원 서버

HP CIFS Server를 구성원 서버로 구성

HP CIFS Server가 백업 도메인 컨트롤러로 작동하도록 구성하는 경우에는 SWAT 도구나 편집기를 사용하여 /etc/opt/samba/smb.conf 파일에서 상대 도메인 매개 변수를 구성해야 합니다. smb.conf 파일의 내용은 다음과 같습니다.

- 구성원 서버로 작동하는 HP CIFS Server에서 LDAP 백엔드를 사용하지 않는 경우 smb.conf 파일의 내용은 다음과 같습니다.

```
[global]
  workgroup = NTDOM
  security = domain
  password server = DOMPDA
  encrypt passwords = yes
  netbios name = myserver
```

- 구성원 서버로 작동하는 HP CIFS Server에서 Unix 및 Samba 계정 데이터베이스를 저장하기 위해 LDAP 백엔드를 사용하는 경우 smb.conf file 파일의 내용은 다음과 같습니다

```
[global]
  workgroup = NTDOM
  security = domain
  encrypt passwords = yes
  passdb backend = ldapsam:ldap://ldapserver:389
   netbios name = myserver
```

참고

workgroup: 이 매개 변수는 HP CIFS Server가 구성원으로 참여하는 도메인 이름을 지정합니다.

security: HP CIFS Server가 도메인에 구성원으로 참여하는 경우 이 매개 변수는 "domain"으로 설정해야 합니다.

`password server`: 이 매개 변수는 사용자 이름 인증 및 유효성 검사를 수행하는 PDC 시스템의 NetBIOS 이름을 정의합니다.

`encrypt passwords`: 이 매개 변수를 `yes`로 설정하면 사용자를 인증하는 데 사용되는 암호가 암호화됩니다.

`netbios`: 이 매개 변수는 구성원 서버를 알고 있는 NetBIOS 이름으로 설정합니다.

HP CIFS Server를 NT 도메인, Windows 2000/2003(Windows 2000 이전 버전 컴퓨터로서) 또는 Samba 도메인에 참여

이 절에서는 HP CIFS Server를 NT 도메인, Windows 2000/2003(Windows 2000 이전 버전 컴퓨터로서) 또는 Samba 도메인에 구성원 서버로 참여시키는 절차에 대해 설명합니다.

단계별 절차

1. `samba_setup`을 실행할 때 "도메인 구성원 서버"를 선택합니다. 메시지에 따라 도메인 구성원 서버 컴퓨터 계정을 PDC에 추가해야 합니다.

   Windows NT: Windows NT PDC로 이동한 후 다음 단계를 수행하여 HP CIFS 구성원 서버의 시스템 계정을 만듭니다.

   a. "시작"을 클릭하고 "프로그램", "관리", "도구"를 차례로 선택한 다음 "서버 관리자" 도구를 엽니다.

   b. "컴퓨터"를 클릭한 후 "도메인에 추가" 아이콘을 선택하고 HP CIFS Server의 호스트 이름을 입력합니다.

   c. 컴퓨터 유형을 선택하라는 메시지가 표시되면 "Windows NT Workstation 또는 Server" 옵션을 선택합니다.

   Windows 2000: Windows 2000 PDC로 이동한 후 Active Directory Controller Wizard를 사용하여 HP CIFS 구성원 서버의 시스템 계정을 만듭니다.

   "`Windows 2000 이전 버전 컴퓨터에서 이 계정을 사용`" 확인란을 선택하고 컴퓨터 이름을 추가합니다.

   Samba(HP CIFS 포함): PDC 역할을 하는 Samba Server로 이동한 후 4장, "컴퓨터 트러스트 계정 만들기" 절에 나와 있는 단계를 수행하여 HP CIFS Member

Server의 컴퓨터 계정을 만듭니다. 그리고 나면 samba_setup에서 "net rpc join -U Administrator%password" 명령을 자동으로 수행합니다.

컴퓨터 트러스트 계정 만들기

PDC 역할을 하는 HP CIFS Server에서 Windows 클라이언트(클라이언트=구성원 서버) 시스템의 트러스트 계정은 컴퓨터에 대해 만들어진 사용자 목록입니다. 이 계정은 시스템 이름 뒤에 "$"가 붙습니다.

LDAP(기본값)를 사용하지 않는 PDC의 경우 컴퓨터 계정은 */etc/passwd* (Unix 사용자 계정) 및 */var/opt/samba/private/smbpasswd*(Windows 사용자 계정)에 항목이 들어 있습니다.

LDAP를 사용하는 PDC의 경우 컴퓨터 계정은 디렉토리 서버 데이터베이스에 posixAccount 및 sambaSamAccount 객체 클래스 항목이 들어 있습니다.

주 도메인 컨트롤러(PDC) 기능을 하는 HP CIFS Server에 Windows 클라이언트용 컴퓨터 계정을 만드는 순서는 다음과 같습니다.

1. Windows 클라이언트의 UNIX 또는 POSIX 계정을 만듭니다.

   - LDAP를 사용하지 않는 경우 다음 명령을 사용하여 */etc/passwd* 파일에서 Windows 클라이언트의 POSIX 계정을 만듭니다.

     ```
     $ useradd -c NT_workstation -d /home/temp -s \
     /bin/false client1$
     ```

     예를 들어, "client1"이라는 클라이언트 컴퓨터 이름에 대한 */etc/passwd* 파일의 결과 항목은 다음과 같습니다.

     ```
     client1$:*:801:800:NT_Workstation: \
     /home/temp:/bin/false
     ```

     여기서 801은 uid이며 800은 "machines" 그룹의 그룹 ID입니다. uid 또는 그룹 id는 고유 번호입니다. 0부터 100까지의 UID 값은 특수한 값이거나 각 서버에 고유한 값일 수 있습니다. 이는 각 시스템에 따라 다릅니다.

     시스템 계정은 뒤에 달러 기호 문자("$")가 붙은 시스템의 이름입니다. 홈 디렉토리는 /home/temp로 설정할 수 있습니다. */etc/passwd* 파일의 셸 필드는 사용되지 않으며 /bin/false로 설정할 수 있습니다.

   - LDAP를 사용할 수 있는 경우 다음 명령을 사용하여 LDAP 디렉토리에서 Windows 클라이언트의 posixAccount 항목을 만듭니다.

```
$ /opt/samba/LDAP3/smbldap-tools/smbldap-useradd.pl \
client1$
```

예를 들어, "client1"이라는 클라이언트 컴퓨터에 대한 LDAP 디렉토리 서버의 결과 항목은 다음과 같습니다.

```
objectClass: posixAccount
cn: client1$
uid: client1$
uidNumber: 1000
gidNumber: 200
homeDirectory: /home/temp
loginShell: /bin/false
userPassword: {crypt}x
pwdLastSet: 1076466492
logonTime: 0
logofftime: 2147483647
kickoffTime: 2147483647
pwdCanChange: 0
pwdMustChange: 2147483647
rid: 1206
primaryGroupID: 1041
acctFlags: [W          ]
displayName: client1$
```

2. Samba PDC 서버에서 smbpasswd 프로그램을 실행하여 Windows 계정을 만듭니다.

   - LDAP를 사용할 수 없는 경우 다음 명령을 사용하여 Windows 클라이언트의 Windows 계정을 */var/opt/samba/private/smbpasswd* 파일에 추가합니다.

     ```
     $ smbpasswd -a -m client1
     ```

     예를 들어, "client1"이라는 클라이언트 컴퓨터에 대한 */etc/opt/samba/private/smbpasswd* 파일의 관련 컴퓨터 항목은 다음과 같습니다.

     ```
     client1$:*801:800:ED816800D0393DAAD3B435B51404EE:321ABE
     EFE10EC431B9AAFF1A1D0D47:[W       ]:LCT-0000000:
     ```

   - LDAP를 사용할 수 있는 경우 다음 명령을 사용하여 Windows 클라이언트용 sambaAccount 항목을 LDAP 디렉토리 서버에 추가합니다.

     ldapsam_compat 백엔드의 경우:

     ```
     $ /opt/samba/bin/smbpasswd -a -m client1
     ```

ldapsam 백엔드의 경우:

```
$ /opt/samba/bin/smbpasswd -a -m client1
```

예를 들어, "client1"이라는 클라이언트 컴퓨터에 대한 LDAP 디렉토리 서버의 관련 컴퓨터 항목은 다음과 같습니다.

```
objectClass: posixAccount
objectClass: sambaSamAccount
cn: client1$
uid: client1$
uidNumber: 1000
gidNumber: 200
homeDirectory: /home/temp
loginShell: /bin/false
gecos: Samba_Server
description: Samba_Server
userPassword: {crypt}x
pwdLastSet: 1076466492
logonTime: 0
logofftime: 2147483647
kickoffTime: 2147483647
pwdCanChange: 0
pwdMustChange: 2147483647
rid: 1206
primaryGroupID: 1041
lmPassword: E0AFF63989B8FA6576549A685C6AFAF1
ntPassword: E0AFF63989B8FA6576549A685C6AFAF1
acctFlags: [W          ]
displayName: client1$
```

참고

pdbedit, net 명령을 비롯한 여러 유틸리티를 사용하여 컴퓨터 트러스트 계정을 만들 수도 있습니다. net 명령은 다양한 새 유틸리티 작업을 제공합니다. pdbedit 및 net 명령을 사용하여 컴퓨터 트러스트 계정을 만드는 방법에 대한 자세한 내용은 pdbedit, net 명령에 대한 SWAT 도움말 텍스트를 참조하십시오.

도메인 사용자 구성

다음 예제는 PDC로 구성된 HP CIFS Server에 도메인 사용자, 도메인 관리자 및 도메인 게스트를 구성하는 명령의 예제입니다.

- root 수준의 사용자인 경우 */sbin/sh* 디렉토리에 있는 "user" 그룹에 도메인 사용자를 만듭니다. 예를 들면 다음과 같습니다.

  ```
  useradd -g users -c "Domain Users" -s /sbin/sh domuser
  ```

  root 수준의 사용자가 **아닌** 경우 */usr/bin/sh* 디렉토리에 있는 "users" 그룹에 도메인 사용자를 만듭니다. 예를 들면 다음과 같습니다.

  ```
  useradd -g users -c "Domain Users" -s /usr/bin/sh domuser
  ```

  여기서 domuser는 도메인 사용자의 이름입니다.

- root 수준의 사용자인 경우 /sbin/sh 디렉토리에 있는 "adm" 그룹에 도메인 관리자를 만듭니다. 예를 들면 다음과 같습니다.

  ```
  useradd -g adm -c "Domain Administrators" -s /sbin/sh
  domadmin
  ```

  root 수준의 사용자가 **아닌** 경우 */usr/bin/sh* 디렉토리에 있는 "adm" 그룹에 도메인 관리자를 만듭니다. 예를 들면 다음과 같습니다.

  ```
  useradd -g adm -c "Domain Administrators" -s /usr/bin/sh
  domadmin
  ```

  여기서 domadmin은 도메인 관리자의 이름입니다.

- root 수준의 사용자인 경우 */sbin/sh* 디렉토리에 있는 "users" 그룹에 도메인 게스트를 만듭니다. 예를 들면 다음과 같습니다.

  ```
  useradd -g users -c "Domain Guest" -s /sbin/sh domguest
  ```

  root 수준의 사용자가 **아닌** 경우 */usr/bin/sh* 디렉토리에 있는 "users" 그룹에 도메인 게스트를 만듭니다. 예를 들면 다음과 같습니다.

  ```
  useradd -g users -c "Domain Guest" -s /usr/bin/sh domguest
  ```

  여기서 domguest는 도메인 게스트의 이름입니다.

사용자를 만든 다음에는(앞의 예제 참조) 모든 사용자가 */etc/passwd* 파일에 추가되었는지 확인하십시오.

Windows 클라이언트의 Samba 도메인 참여

1. *smb.conf* 파일에서 다음 매개 변수를 확인합니다.

   `security` 매개 변수를 "user"로 설정합니다.

   `workgroup` 매개 변수를 도메인의 이름으로 설정합니다.

   `encrypt passwords` 매개 변수를 "yes"로 설정합니다.

   ```
   [global]
     security = user
     workgroup = SAMBADOM #SAMBA Domain name
     domain logon = yes
     encrypt passwords = yes
   ```

2. Windows 클라이언트의 UNIX 또는 POSIX 계정을 만듭니다.

   - `passdb backend` 옵션을 `smbpasswd`로 설정하는 경우 다음 명령을 사용하여 */etc/passwd* 파일에서 Windows 클라이언트의 POSIX 계정을 만듭니다.

     ```
     $ useradd -c NT_workstation -d /home/temp -s \
     /bin/false client1$
     ```

     예를 들어, "`client1`"이라는 클라이언트 컴퓨터 이름에 대한 */etc/passwd* 파일의 결과 항목은 다음과 같습니다.

     ```
     client1$:*:803:808:NT_Workstation: \
     /home/temp:/bin/false
     ```

     여기서 `803`은 uid이며 `808`은 "machines" 그룹의 그룹 ID입니다. uid 또는 그룹 id는 고유 번호입니다. 0부터 100까지의 UID 값은 특수한 값이거나 각 서버에 고유한 값일 수 있습니다. 이는 각 시스템에 따라 다릅니다.

     시스템 계정은 뒤에 달러 기호 문자("$")가 붙은 시스템의 이름입니다. 홈 디렉토리는 `/home/temp`로 설정할 수 있습니다. */etc/passwd* 파일의 셸 필드는 사용되지 않으며 `/bin/false`로 설정할 수 있습니다.

   - `passdb backend` 옵션을 `ldapsam` 또는 `ldapsam_compat`로 설정하는 경우 다음 명령을 사용하여 LDAP 디렉토리에 Windows 클라이언트용 posixAccount 항목을 만듭니다.

```
$ /opt/samba/LDAP/smbldap-tools/smbldap-useradd.pl \
client1$
```

예를 들어, "client1"이라는 클라이언트 컴퓨터에 대한 LDAP 디렉토리 서버의 결과 항목은 다음과 같습니다.

```
dn: uid=client1, ou=people,dc=org, dc=hp, dc=com
objectClass: top,
inetOrgPerson,posixAccount,organizationPerson, person
cn: client1$
sn: client1$
uid: client1$
uidNumber: 1002
gidNumber: 202
homeDirectory: _HOMEPREFIX_/client1$
loginShell: _LOGINSHELL_
userPassword: {crypt}x
pwdLastSet: 1076466300
logonTime: 0
logofftime: 2147483650
kickoffTime: 2147483650
pwdCanChange: 0
pwdMustChange: 2147483650
rid: 1206
primaryGroupID: 1041
acctFlags: [W          ]
displayName: client1$
```

3. Samba PDC 서버에서 smbpasswd 프로그램을 실행하여 Windows 계정을 만듭니다.

   - passdb backend 옵션을 smbpasswd로 설정하는 경우 다음 명령을 사용하여 Windows 클라이언트용 Windows 계정을 */var/opt/samba/private/smbpasswd* 파일에 추가합니다.

     ```
     $ smbpasswd -a -m client1$
     ```

     예를 들어, "client1"이라는 클라이언트 컴퓨터에 대한 */etc/opt/samba/private/smbpasswd* 파일의 관련 컴퓨터 항목은 다음과 같습니다.

     ```
     client1$:*803:808:ED816822D0393DAAD3B435B51404DD:321ABE
     EFE10EC431B9BBFF1A1C0C047:[W       ]:LCT-0000000:
     ```

   - passdb backend 옵션을 ldapsam 또는 ldapsam_compat로 설정하는 경우 다음 명령을 사용하여 Windows 클라이언트용 sambaSamAccount 항목을 LDAP 디렉토리 서버에 추가합니다.

```
$ smbpasswd -a -m client1
```

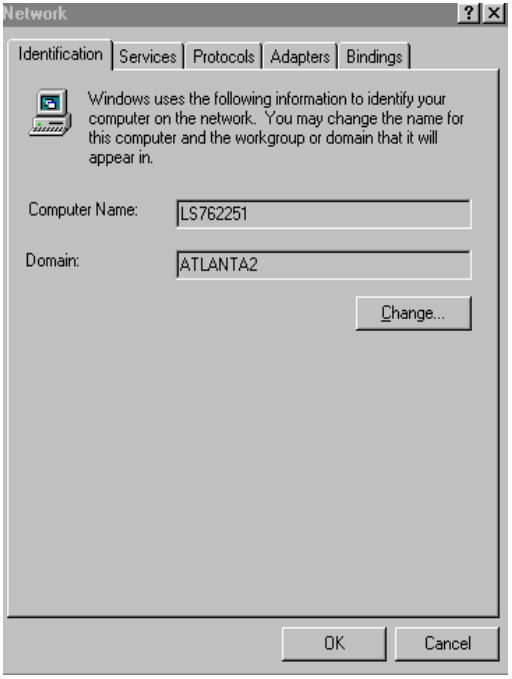
예를 들어, "client1"이라는 클라이언트 컴퓨터에 대한 LDAP 디렉토리 서버의 관련 컴퓨터 항목은 다음과 같습니다.

```
objectClass: posixAccount
objectClass: sambaSamAccount
cn: client1$
uid: client1$
uidNumber: 1002
gidNumber: 202
homeDirectory: /home/temp
loginShell: /bin/false
gecos: Samba_Server
description: Samba_Server
userPassword: {crypt}x
pwdLastSet: 1076466300
logonTime: 0
logofftime: 2147483650
kickoffTime: 2147483650
pwdCanChange: 0
pwdMustChange: 2147483650
rid: 1206
primaryGroupID: 1041
lmPassword: E0AFF63989B8FA6576549A685C6ADFC1
ntPassword: E0AFF63989B8FA6576549A685C6ADFC1
acctFlags: [W          ]
displayName: client1$
```

4. Windows NT에 로컬 관리자로 로그온합니다.
5. Windows NT 바탕 화면에서 '시작', '설정' 및 '제어판'을 순서대로 클릭합니다. 제어판 창이 열리면 '네트워크' 아이콘을 두 번 클릭합니다. '네트워크' 창이 열리면 '확인' 탭을 클릭합니다. 아래의 그림 4-1을 참조하십시오.

6. '도메인' 필드에 Samba 도메인 이름을 입력하고 '변경' 단추를 누릅니다. 아래의 그림 4-3을 참조하십시오.

그림 4-1 **Samba PDC 도메인 이름 입력**



로밍 프로파일

PDC로 구성된 HP CIFS Server는 다음 기능을 갖춘 로밍 프로파일을 지원합니다.

- 사용자의 환경, 기본 설정, 바탕 화면 설정 등이 HP CIFS Server에 저장됩니다.
- 로밍 프로파일을 공유 파일로 만들어 Windows 클라이언트 간에 공유할 수 있습니다.
- 사용자가 도메인의 워크스테이션에 로그온하면, PDC로 구성된 HP CIFS Server의 공유에 있는 로밍 프로파일이 로컬 시스템으로 다운로드됩니다. 로그아웃하면 프로파일은 다시 서버로 복사됩니다.

로밍 프로파일 구성

다음 절차에 따라 로밍 프로파일을 구성합니다.

1. *smb.conf* 파일의 `logon path` 전역 매개 변수를 사용해 로밍 프로파일을 수정하거나 사용 가능하게 합니다. 예를 들면 다음과 같습니다.

```
[global]
  logon path = \\%L\profile\%U
  workgroup = SAMBADOM
  security = user
  encrypt passwords = yes
  domain logon = yes
```

2. 로밍 프로파일에 사용할 `[profiles]` 공유를 만듭니다. 사용자 프로파일 파일에 사용되는 프로파일 공유에 `profile acls = yes`를 설정합니다. 일반 공유에 `profile acls = yes`를 설정하면 해당 공유에서 만들어지는 파일의 소유권이 잘못될 수 있습니다. 다음은 `[profiles]` 공유의 구성 예제입니다.

```
[profiles]
   profile acls = yes
  path = /etc/opt/samba/profiles
  read only = no
  create mode = 600
  directory mode = 770
```

```
writeable = yes
browseable = no
guest ok = no
```

사용자 로그온 스크립트 구성

로그온 스크립트 구성은 다음 조건을 만족해야 합니다.

- 사용자 로그온 스크립트는 HP CIFS Server의 `[netlogon]` 파일 공유에 저장되어야 합니다.
- 이 스크립트에는 UNIX 실행 권한이 설정되어야 합니다.
- 모든 로그온 스크립트에 포함된 명령은 Windows 클라이언트에서 인식할 수 있는 유효한 명령이어야 합니다.
- 로그온 사용자는 로그온 스크립트를 실행할 수 있는 적절한 액세스 사용 권한을 갖고 있어야 합니다.

다음은 사용자 로그온 스크립트의 구성 예제입니다.

```
[global]
  logon script = %U.bat

[netlogon]
  path = /etc/opt/samba/netlogon
  writeable = yes
  browseable = no
  guest ok = no
```

이 예제에서는 배치 파일(.bat)이 PDC로 구성된 HP CIFS Server의 [netlogon]이라는 파일 공유에서 실행됩니다.

로그온 시 로그온 스크립트 실행

PDC로 구성된 HP CIFS Server에서는 사용자가 로그온할 때 로그온 스크립트가 실행될 수 있습니다. 이 기능을 사용하려면 다음을 수행해야 합니다.

- 사용자 로그온 스크립트는 HP CIFS Server의 `[netlogon]` 파일 공유에 저장되어야 합니다.
- HP CIFS Server는 *smb.conf* 파일의 `logon script` 전역 매개 변수를 설정하여 로그인 스크립트가 실행되게 합니다.
- Windows 클라이언트에서 실행될 로그온 스크립트의 형식은 모두 DOS 텍스트 형식이어야 하며 **실행** 사용 권한을 포함해야 합니다.

홈 드라이브 매핑 지원

HP CIFS Server에서는 *smb.conf* 파일에 다음 두 가지 전역 매개 변수를 사용하여 사용자 홈 디렉토리 및 홈 드라이브 매핑 기능을 사용할 수 있습니다.

- `login home`
- `logon drive`

예를 들면 다음과 같습니다.

```
[global]
  logon drive = H:
  logon home = \\%L\%U
```

도메인 간 트러스트 관계

트러스트 관계를 사용하면 하나의 도메인에서 다른 도메인의 사용자에 대한 인증을 통과할 수 있습니다. 트러스팅 도메인은 트러스트된 도메인의 사용자에 대한 로그온 인증을 허용합니다.

HP CIFS Server에서는 다음과 같은 트러스트 관계를 지원합니다.

- HP CIFS PDC Samba 도메인은 NT 도메인을 사용하는 트러스팅 도메인, 트러스트된 도메인 또는 양방향 트러스트(트러스팅 및 트러스트됨 또는 "2웨이") 도메인입니다.
- HP CIFS PDC Samba 도메인은 다른 Samba 도메인을 사용하는 트러스팅 도메인, 트러스트된 도메인 또는 양방향 트러스트 도메인입니다.
- NT 도메인이나 Windows 2000/2003 도메인의 HP CIFS 구성원 서버는 도메인 컨트롤러에서 설정한 트러스트 관계를 존중합니다.

HP CIFS PDC Samba 도메인에서는 Window 2000/2003 도메인을 사용하는 트러스트된 도메인이든 트러스팅 도메인이든 트러스트를 허용하지 않습니다. HP CIFS Samba 도메인에서는 도메인 A가 도메인 B를 트러스트하고, 도메인 B가 도메인 C를 트러스트함으로써 도메인 A가 도메인 C를 트러스트하는 과도적 트러스트를 허용하지 않습니다.

트러스트된 사용자를 위한 Smb.conf 구성

HP CIFS Server에서는 모든 Samba 사용자가 HP-UX 로컬 로그온을 수행해야 합니다. 따라서 다른 도메인의 트러스트된 Samba 사용자라도 일치하는 로컬 POSIX 사용자가 필요합니다. POSIX 사용자를 즉석에서 추가할 수 있도록 하려면 `add user script` `smb.conf` 구성 매개 변수를 설정합니다. 예를 들면, 다음과 같습니다.

```
add user script = /usr/sbin/useradd  -g users -c \
"Auto_Account" -s /bin/false %u
```

다른 Samba 도메인을 사용하여 HP CIFS PDC에서 트러스트 관계 설정

이 절에서는 다른 Samba 도메인을 사용하여 HP CIFS PDC에서 트러스트 관계를 설정하는 데 사용되는 절차에 대해 설명합니다.

root로 로그온하고 트러스트된 도메인 PDC에서 다음 단계를 실행합니다.

단계 1. 트러스팅 도메인의 트러스트 계정을 /etc/passwd에 추가합니다. 다음과 같이 useradd 명령을 사용하여 도메인 이름과 "$"를 추가합니다.

```
$ useradd <trusting domain name>$
```

useradd 명령의 이름 길이 제한으로 /etc/passwd를 편집하여 트러스팅 도메인 이름 계정을 추가해야 할 수도 있습니다.

단계 2. smbpasswd를 실행하여 트러스팅 도메인 Samba 계정을 트러스트된 도메인 백엔드 데이터베이스에 추가하고 트러스팅 계정의 암호를 만듭니다. 이 암호는 트러스팅 도메인에서 트러스트 관계를 설정할 때 사용됩니다.

```
$ smbpasswd -a -i <trusting domain name>
```

root 로 로그온하고 트러스팅 도메인 PDC에서 다음 단계를 실행합니다.

단계 1. net rpc trustdom을 실행하여 트러스트를 설정하고 트러스트된 도메인 PDC에서 smbpasswd 명령을 사용하여 만든 암호를 입력합니다.

```
$ net rpc trustdom establish <trusted domain name>
```

NT 도메인을 사용하여 HP CIFS PDC에서 트러스트 관계 설정

Samba 도메인에서 NT 도메인 트러스트

다음 단계에 따라 Samba 도메인에서 NT 도메인을 트러스트합니다.

단계 1. NT 도메인 컨트롤러에서 User Manager 유틸리티를 실행합니다. 정책/트러스트 관계로 이동한 후 CIFS Server의 트러스팅 Samba 도메인 계정을 추가하고 암호를 설정합니다.

단계 2. 트러스팅 Samba 도메인 PDC에서 root로 로그온합니다. net rpc trustdom을 실행하여 트러스트를 설정하고 트러스트된 NT 도메인 PDC에서 User Manager 유틸리티를 사용하여 만든 암호를 입력합니다.

```
$ net rpc trustdom establish <trusted domain name>
```

NT 도메인에서 Samba 도메인 트러스트

root로 로그온하고 트러스트된 Samba 도메인 PDC에서 다음 단계를 실행합니다.

단계 **1.** 트러스팅 NT 도메인의 트러스트 계정을 /etc/passwd에 추가합니다. 다음과 같이 useradd 명령을 사용하여 도메인 이름과 "$"를 추가합니다.

```
$ useradd <trusting NT domain name>$
```

useradd 명령의 이름 길이 제한으로 /etc/passwd를 편집하여 트러스팅 NT 도메인 이름 계정을 추가해야 할 수도 있습니다.

단계 **2.** smbpasswd를 실행하여 트러스팅 NT 도메인 Samba 계정을 트러스트된 Samba 도메인 백엔드 데이터베이스에 추가하고 트러스팅 계정의 암호를 만듭니다. 이 암호는 트러스팅 NT 도메인에서 트러스트 관계를 설정할 때 사용됩니다.

```
$ smbpasswd -a -i <trusting domain name>
```

단계 **3.** NT 도메인 컨트롤러에서 User Manager 유틸리티를 실행합니다. 정책/트러스트 관계로 이동합니다. CIFS Server의 트러스트된 Samba 도메인 계정을 추가하고 Samba 도메인 PDC에서 smbpasswd 명령을 통해 설정된 암호를 입력합니다.

NT 도메인 또는 Windows 2000/2003 도메인의 HP CIFS 구성원 서버에서 트러스트 관계 설정

HP CIFS Member Server는 도메인 컨트롤러에 대한 도메인 인증을 통과하므로 HP CIFS Server에 대한 별도의 구성이 필요하지 않습니다. HP CIFS 구성원 서버는 도메인 컨트롤러에서 설정된 트러스트 관계를 존중합니다.

5 Windows 2000/2003 도메인

이 장에서는 HP CIFS Server가 Windows 2000/2003 도메인에 ADS 구성원 서버로 참여하는 프로세스에 대해 설명합니다. Windows 2000 이전 버전의 컴퓨터로 참여하려면 4장 "NT 스타일 도메인"의 105페이지의 “도메인 구성원 서버”를 참조하십시오.

HP CIFS Server가 Windows 2000/2003 도메인에 ADS 구성원 서버로 참여

Kerberos 클라이언트 및 패치 요구 사항

HP CIFS Server A.02.02의 경우 Windows 2003 ADS Domain Controller(DC)와의 HP CIFS Server 통합을 지원하려면 1.3.5.03 버전이 있는 새 버전의 Kerberos v5 클라이언트가 필요합니다. Windows 2003 ADS DC에서 작동하도록 구성된 HP CIFS Server가 있는 경우에는 Kerberos Client를 버전 1.3.5 이상으로 업데이트해야 합니다. Kerberos Client 버전 1.0은 원래 HP-UX 11i v1 및 v2에 번들로 제공된 것이며, 이 버전은 Windows 2003 ADS DC 환경에서 작동하는 HP CIFS Server 버전 A.02.02와 호환되지 않습니다.

Kerberos v5 Client(KRB5CLIENT) 제품은 다음 Software Depot 웹 사이트 http://www.hp.com/go/softwaredepot에서 다운로드할 수 있습니다.

검색 필드에 `KRB5CLIENT`를 입력합니다.

Kerberos v5 Client 제품을 사용하려면 HP-UX 11i v1 및 v2 시스템에 패치를 설치해야 합니다. 자세한 패치 정보는 **HP CIFS Server 3.0d 릴리즈 노트 버전 A.02.02**를 참조하십시오.

단계별 절차

다음 절차를 통해 HP CIFS Server를 Windows 200x 도메인에 ADS 기본 구성원 서버로 참여시킵니다.

참고

HP CIFS Server에서는 다음과 같은 Kerberos 암호화 유형만 지원합니다.

- DES-CBC-CRC
- DES-CBC-MD5

`/etc/krb5.conf` 파일에서 이러한 암호화 유형 중 하나를 구성해야 합니다.

단계 **1.** HP CIFS Server에 설치된 LDAP-UX 통합 제품을 확인합니다.

```
swlist | grep J4269AA
```

필요할 경우 6장, "LDAP 통합 지원"의 143페이지의 “HP CIFS Server에 LDAP-UX Client Services 설치”를 참조하십시오.

단계 **2.** HP CIFS Server에서 Kerberos 구성 파일 /etc/krb5.conf를 만들어 이 파일에서 기본 영역, KDC(Key Distribution Center) 서버 및 로깅 파일 이름을 지정합니다. Kerberos 클라이언트는 영역의 KDC를 저장하는 구성에 따라 다릅니다. 다음은 영역 MYREALM.XYZ.COM과 KDC로 컴퓨터 adsdc.myrealm.xyz.com이 지정되어 있는 /etc/krb5.conf의 예제를 보여 줍니다.

```
# Kerberos Configuration                                          #
#                                                                 #
# This krb5.conf file is intended as an example only.             #
# See krb5.conf(4) for more details.                              #
#
# Please verify that you have created the directory /var/log.#
#                                                                 #
# Replace MYREALM.XYZ.COM with your kerberos Realm.               #
# Replace adsdc.myrealm.xyz.com with your Windows ADS DC full#
# domain name.                                                    #
#                                                                 #
[libdefaults]
default_realm = MYREALM.XYZ.COM
default_tkt_enctypes = DES-CBC-CRC
default_tgs_enctypes = DES-CBC-CRC
ccache_type = 2


[realms]
MYREALM.XYZ.COM = {
kdc = adsdc.myrealm.xyz.com:88
admin_server = adsdc.myrealm.xyz.com
}
[domain_realm]
.xyz.com = MYREALM.XYZ.COM
```

참고

서버 필드에 :88이 필요합니다.

```
[logging]
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmin.log
default = FILE:/var/log/krb5lib.log
```

/etc/krb5.conf 파일 구성 방법에 대한 자세한 내용은 krb5.conf(4) 맨페이지를 참조하십시오.

단계 **3.** 다음 명령을 실행하여 Kerberos 구성을 확인합니다.

```
login as root
run kinit <user e.g. Administrator@myrealm.xyz.com>
(필요할 경우 사용자 및 암호를 Windows ADS DC에 추가)
```

확인 중에 다음과 같은 오류가 발생할 수도 있습니다.

- Pre-Authentication Failed는 암호를 잘못 입력했음을 의미합니다.
- Clock skew too great는 HP-UX 컴퓨터의 시간이 Windows 도메인 컨트롤러와 동기화되지 않았음을 나타냅니다. date 명령을 실행하여 데이터를 재설정하거나 TZ=GMT를 설정하고 다시 시도합니다.
- kinit: KDC has no support for encryption type while getting initial credentials라는 경고 메시지가 표시될 수 있습니다. Windows 2000/2003 도메인을 설치할 때 관리자에 대해 사용했던 원래의 암호에서 적어도 한 번은 관리자 암호를 변경해야 합니다.
- 그 밖의 오류는 /etc/krb5.conf 파일의 오류일 수 있습니다. (:88을 /etc/krb5.conf 파일의 서버 필드에 추가해야 합니다.)

단계 **4.** 다음 절차에 따라 HP CIFS Server를 구성합니다.

- 새로운 설치의 경우, /opt/samba/bin/samba_setup을 실행하고 ADS 구성원 서버를 선택할 수 있습니다.

  새로운 설치의 경우, samba_setup 명령을 완료하고 다음 smb.conf 구성 항목을 확인합니다. 그리고 나면 samba_setup이 "net ads join -U Administrator%password" 명령을 수행하여 ADS 도메인을 자동으로 참여시킵니다.

```
[global]
  workgroup = MYREALM     # Domain Name
  realm = MYREALM.XYZ.COM
  security = ADS
  domain master = no
  encrypt passwords = yes
  netbios name = MYSERVER
  password server = adsdc.myrealm.xyz.com
```

- 기존 설치의 경우, smb.conf 구성 항목을 다음과 같이 수정합니다.

```
[global]
  workgroup = MYREALM     # Domain Name
  realm = MYREALM.XYZ.COM
  security = ADS
  domain master = no
  encrypt passwords = yes
  netbios name = MYSERVER
  password server = adsdc.myrealm.xyz.com
```

그런 다음 "net ads join -U Administrator%password" 명령을 수동으로 실행하여 ADS 도메인을 참여시킵니다.

경고

Windows Server Manager를 사용하여 ADS Server에 시스템 이름을 추가하지 마십시오. 이렇게 하면 "userAccountControl"의 값이 KDC가 CIFS 지원 유형이 아닌 구성원 서버를 위한 RC4-HMAC 티켓을 실행하게 만들도록 설정됩니다. Kerberos 인증이 실패하고, NTLM으로 넘어가고, 사용자에게 사용자 암호 요청 프롬프트가 표시됩니다.

시스템이 이미 Windows Server Manager GUI를 사용하여 ADS에 추가된 경우에는 Window Server Manager를 사용하여 시스템 계정을 삭제하면 됩니다. 그리고 해당 지침에 따라 "kinit" 및 "net ads join" 명령을 실행합니다.

이 문제를 해결하는 다른 방법은 ADS에서 ADS_UF_USE_DES_KEY_ONLY (2097152 또는 0x200000) 플래그가 있는 CIFS 구성원 서버의 "userAccountControl" 속성 값을 *AND*로 설정하는 것입니다. 이 작업은

Windows 2000 또는 2003 CD의 "adsiedit.msc" 도구나 ldapmodify 명령을 사용하여 수행할 수 있습니다.

참고

HP CIFS Server가 도메인에 Windows 2000 이전 버전의 서버로 현재 참여하고 있는 경우 HP CIFS Server를 Windows 도메인에 ADS 구성원 서버로 추가하기 전에 먼저 도메인에서 서버를 제거하십시오.

참고

`realm`: 이 매개 변수는 정규화된 도메인 이름을 가진 ADS Kerberos 영역의 이름을 지정합니다. 이 이름은 `krb5.conf`의 Kerberos 영역 값과 동일하게 설정해야 합니다.

`workgroup`: 이 매개 변수는 HP CIFS Server가 도메인 구성원 서버인 도메인의 이름을 지정합니다.

`security`: HP CIFS Server가 Windows 200x에 ADS 기본 구성원 서버로 참여하는 경우에는 이 매개 변수를 `ADS`로 설정해야 합니다.

`password server`: 이 매개 변수는 사용자 이름 인증 및 유효성 검사를 수행하는 Windows ADS PDC 컴퓨터의 NetBIOS 이름을 정의합니다.

`encrypt passwords`: 이 매개 변수를 `yes`로 설정하면 사용자를 인증하는 데 사용되는 암호가 암호화됩니다.

`netbios name`: 이 매개 변수를 구성원 서버를 알고 있는 NetBIOS 이름으로 설정합니다.

단계 **5.** 다음 명령을 사용하여 HP CIFS Server를 시작합니다.

```
/opt/samba/bin/startsmb
```

단계 **6.** 다음 명령을 실행하여 Kerberos 인증을 확인합니다. 이 명령에서 Kerberos 보안을 사용하도록 강제로 설정하려면 `-k` 옵션을 사용해야 합니다.

```
smbclient -W <Window Domain> -U <user name in domain> -k //<HP CIFS
Server name>/<share> <password for user>
```

smbclient 명령을 실행하면 HP CIFS Server의 공유에 연결할 수 있습니다.

6 LDAP 통합 지원

이 장에서는 LDAP 통합을 지원하는 HP CIFS Server에 대해 설명합니다. 이 장에는 LDAP의 장점과 HP Netscape Directory Server, HP LDAP-UX Integration 제품 및 HP CIFS Server 소프트웨어의 설치, 구성 및 확인 절차에 대한 내용이 포함되어 있습니다. 이 장의 구성은 다음과 같습니다.

개요

LDAP(Lightweight Directory Access Protocol)는 중앙 집중식 관리 하부 구조 개발을 위한 프레임워크를 제공합니다. LDAP에서는 응용 프로그램, 서비스, 사용자 계정, Windows 계정 및 구성 정보를 중앙 LDAP 디렉토리로 통합하여 디렉토리 사용 가능 컴퓨팅을 지원합니다.

사용자와 서버 수가 많은 Samba 고객 사이트에서는 LDAP 지원과 HP CIFS Server를 통합하고자 할 수도 있습니다. LDAP 디렉토리 서버와 통신하도록 여러 HP CIFS Server를 구성하면 사용자 데이터베이스의 확장 가능한 중앙 집중식 관리를 제공할 수 있습니다. HP-UX에서 LDAP-UX Integration 제품과 HP CIFS Server를 통합하면 HP CIFS Server에서 Netscape Directory Server에 사용자 계정 정보를 저장할 수 있습니다. LDAP 데이터베이스는 `/etc/passwd` 또는 NIS와 `smbpasswd` 또는 NT 서버 사용자 데이터베이스로 대체할 수 있습니다.

이전에 `smbpasswd` 파일에 저장한 LDAP 디렉토리에 Windows 사용자 정보를 저장할 수 있습니다. LDAP 통합을 사용하면 `SMBD` 프로그램에서 LDAP 디렉토리를 사용하여 인증 및 권한 부여 프로세스 중에 Windows 사용자 정보를 조회합니다. 또한 Windows 사용자 정보를 추가, 삭제 또는 변경하기 위해 `smbpasswd` 프로그램을 호출하는 경우 `smbpasswd` 파일이 아니라 LDAP 사용자 데이터베이스가 업데이트됩니다.

HP CIFS Server에서 제공하는 구성 매개 변수를 통해 LDAP 지원을 활성화할 수 있습니다. `smb.conf passwd backend` 매개 변수를 `ldapsam` 또는 `ldapsam_compat`로 지정하는 경우 HP CIFS Server는 암호, 사용자, 그룹 및 기타 데이터의 디렉토리 서버에 액세스합니다.

HP CIFS Server A.02.* 버전은 여러 가지 면에서 A.01.* 버전과 다릅니다. A.01.*에 사용된 `sambaAccount` 객체 클래스를 교체할 새로운 객체 클래스 `sambaSamAccount`가 사용되었습니다. A.02.*로 업데이트하는 경우 A.01.* 호환 백엔드인 `ldapsam_compat`를 지정하면 기존 설치가 계속 작동됩니다. 마이그레이션 스크립트를 사용할 수 있으며 새로운 설치에서 암호 백엔드로 `ldapsam`을 선택합니다. HP CIFS Server A.01.* 버전에서 A.02.* 버전으로 LDAP를 업그레이드하는 방법에 대한 자세한 절차는 178페이지의 “LDAP를 HP CIFS Server A.01.*에서 A.02.*로 업그레이드”를 참조하십시오.

smb.conf 파일에 지정된 ldap ssl 매개 변수를 구성하여 SSL(Secure Sockets Layer) 지원을 활성화할 수 있습니다. SSL이 지원되면 HP CIFS Server는 SSL이 활성화된 LDAP 디렉토리에 대한 액세스를 허용하므로 네트워크상에서 암호가 보호되고 CIFS Server와 SSL 사용 LDAP 디렉토리 서버 간에 기밀성 및 데이터 무결성이 보장됩니다. passdb backend = ldapsam:ldaps://<fully qualitied name of NDS server>을 설정하여 SSL 지원을 활성화할 수 있습니다.

참고

HP CIFS Server는 다른 LDAP 제품과 함께 잘 작동되지만 HP에서는 HP CIFS Server를 HP LDAP-UX Integration, J4269AA 및 HP Netscape Directory Server, J4258CA, 제품 구성과 함께 사용하는 경우에만 LDAP 지원을 제공합니다.

HP CIFS Server 장점

LDAP를 지원하는 HP CIFS Server는 고객에게 다음과 같은 이점을 제공합니다.

- LDAP는 중앙 집중식 사용자 데이터베이스 관리를 제공하므로 여러 HP CIFS Server에서 사용자 계정 정보를 유지 관리해야 하는 필요성이 감소됩니다.
- 여러 HP CIFS Server 또는 사용자를 LDAP 디렉토리 환경에 쉽게 추가할 수 있습니다. 따라서 HP CIFS Server의 확장성이 크게 향상됩니다.
- LDAP 디렉토리에서 사용자 계정 정보를 저장 및 조회할 수 있습니다. 따라서 순차 검색보다는 색인화된 검색을 제공하므로 대형 데이터베이스 사용 시 사용자 조회 시간이 감소됩니다.
- smbpasswd 파일에 저장된 정보의 경우 추가 속성을 위한 공간이 없습니다. LDAP 지원을 사용하면 스키마를 확장할 수 있으므로 LDAP 디렉토리에 추가 사용자 정보를 저장할 수 있습니다. 따라서 추가적인 직원 및 사용자 데이터베이스가 필요하지 않습니다.

네트워크 환경

HP CIFS Server에서는 다양한 네트워크 환경을 지원합니다. WINS, 브라우저 제어, 도메인 로그온, 로밍 프로파일 등 다양한 기능을 사용하여 다양한 네트워크 환경 범위를 계속 지원할 수 있습니다. LDAP 통합은 Samba 사용자 인증을 위한 또 하나의 대체 솔루션을 제공합니다.

도메인 모델 네트워크

주 도메인 컨트롤러(PDC)로 사용되는 CIFS Server

PDC는 Windows 인증을 담당하므로 PDC로 구성된 HP CIFS Server는 Windows 인증을 위해 `smbpasswd`를 LDAP 사용 디렉토리 서버로 변경합니다. 그 밖의 Samba 구성 항목은 변경되지 않은 상태로 유지됩니다. 새 LDAP 구성의 관리자는 HP LDAP-UX 통합 소프트웨어를 설치하고 LDAP 클라이언트도 구성해야 합니다. 이 경우 LDAP 디렉토리 서버에서 Posix 및 Windows 사용자의 통합도 허용합니다.

구성원 서버로 사용되는 CIFS Server

Samba 구성을 변경되지 않은 상태로 유지하면 도메인 모델 네트워크 환경에서 구성원 서버로 사용되는 HP CIFS Server를 구성원 서버로 계속 사용할 수 있습니다. Windows 인증 요청은 LDAP 또는 `smbpasswd`를 통해 PDC에서 계속 관리됩니다. 새 LDAP 구성의 관리자는 HP LDAP-UX 통합 소프트웨어를 설치하고 LDAP 디렉토리 서버에서 Posix 및 Windows 사용자를 통합하도록 LDAP 클라이언트를 구성할 수 있습니다.

구성원 서버(`security = domain`)가 LDAP를 사용하도록 구성된 경우에는 PDC를 통해 인증하려고 합니다. PDC 인증이 실패하면 고유 `smb.conf` 구성 파일에 설정된 LDAP 디렉토리 서버를 통해 직접 인증합니다.

Samba PDC의 백업 도메인 컨트롤러(BDC)로 사용되는 CIFS Server

BDC도 Windows 인증을 담당하므로 BDC로 구성된 HP CIFS Server는 사용자 인증을 위해 LDAP 디렉토리에 액세스할 수 있습니다. BDC 구성은 `master browser`와 `domain master`를 모두 no로 설정한다는 점을 제외하고는 PDC 구성과 거의 같습니다.

ADS(Active Directory Service) 구성원 서버로 사용되는 CIFS Server

ADS 구성원 서버는 LDAP 라이브러리 및 Kerberos 보안을 사용하여 ADS 도메인 컨트롤러의 인증 서비스에 액세스합니다. 따라서 LDAP-UX Integration 및 HP Kerberos Client Library 제품이 필요합니다. 자세한 내용은 5장, 123페이지의 “Windows 2000/2003 도메인”을 참조하십시오.

UNIX/9000(ASU) 서버용 고급 서버

LDAP 통합을 사용하면 중앙 집중식 사용자 데이터 관리를 통해 ASU를 CIFS Server로 쉽게 마이그레이션할 수 있습니다. ASU PDC 서버는 마이그레이션 도움말 패키지(*http:// software.hp.com*)를 사용하여 사용자를 `/etc/passwd` 항목으로 마이그레이션할 수 있습니다. HP CIFS Server는 `smbpasswd` 파일에 항목을 만드는 `/opt/samba/bin/syncsmbpasswd` 도구를 제공합니다. `/etc/passwd` 및 `smbpasswd` 파일의 항목을 사용하면 이 장 뒷부분에서 설명하는 마이그레이션 스크립트를 사용하여 LDAP 디렉토리에 ASU 사용자와 UNIX 사용자를 모두 통합할 수 있습니다.

작업 그룹 모델 네트워크

서버 모드 보안으로 구성된 HP CIFS Server는 지정된 서버에서 Windows 사용자를 인증합니다. LDAP를 사용하는 경우에는 서버 모드 인증이 실패할 경우 인증 작업이 LDAP 서버에게 넘겨집니다.

공유 모드 보안으로 구성된 HP CIFS Server는 `smbpasswd`를 LDAP 디렉토리 서버로 변경할 수 있습니다.

독립형 사용자 모드 서버로 구성된 HP CIFS Server는 `smbpasswd`를 LDAP 디렉토리 서버로 변경할 수 있습니다.

UNIX 사용자 인증 - /etc/passwd, NIS 마이그레이션

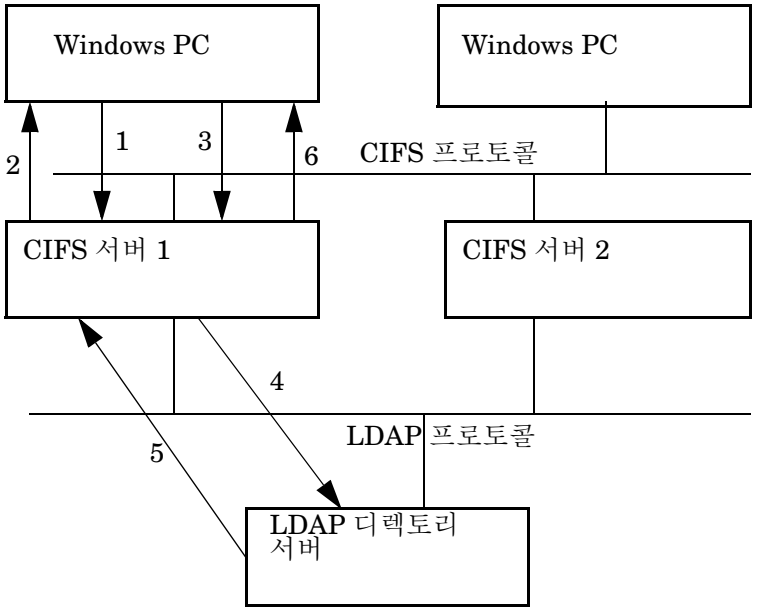
HP CIFS 로그온 시 Samba(Windows) 사용자 인증 외에 HP UNIX 사용자 인증도 필요합니다. Samba 및 UNIX 서버를 단일 LDAP 디렉토리 서버 데이터베이스로 통합할 수 있습니다. 그러나 원한다면 UNIX 사용자에 대해 `/etc/passwd` 파일 또는 NIS 데이터베이스 파일을 계속 사용할 수도 있습니다.

HP에서 제공한 마이그레이션 스크립트를 사용하면 `/etc/passwd` 파일 및 NIS 데이터베이스 파일을 LDAP 디렉토리 서버로 마이그레이션할 수 있습니다. 마이그레이션 스크립트에 대한 자세한 내용은 152페이지의 “Netscape Directory에 데이터 마이그레이션” 및 178페이지의 “LDAP를 HP CIFS Server A.01.*에서 A.02.*로 업그레이드”를 참조하십시오.

LDAP 통합을 사용한 CIFS 인증

LDAP 통합을 사용하면 여러 HP CIFS Server에서 중앙 집중식 사용자 데이터베이스 관리를 위해 단일 LDAP 디렉토리 서버를 공유할 수 있습니다. HP CIFS Server에서는 LDAP 디렉토리에 액세스하여 사용자 인증을 위해 Windows 사용자 정보를 조회할 수 있습니다. 그림 6-1은 LDAP 네트워크 환경의 CIFS 인증을 보여줍니다.

그림 6-1 LDAP 통합을 사용한 CIFS 인증



다음은 그림 6-1에 표시된 사용자 인증을 위한 Windows PC, CIFS Server 및 LDAP 디렉토리 서버 간 메시지 교환을 설명합니다.

1. Windows 사용자가 연결을 요청합니다.

2. CIFS Server에서 `challenge`를 Windows PC 클라이언트로 전송합니다.

3. Windows PC 클라이언트에서 사용자 암호 및 `challenge` 정보를 기초로 하여 `response` 패킷을 CIFS Server로 전송합니다.

4. CIFS Server가 LDAP 디렉토리 서버에서 사용자 데이터를 조회하고 암호 정보를 포함한 데이터 속성을 요청합니다.

5. CIFS Server는 LDAP 디렉토리 서버에서 암호 정보를 비롯하여 데이터 속성을 받습니다. 암호와 `challenge` 정보가 클라이언트 `response` 패키지의 정보와 일치하면 Samba 사용자 인증이 성공적으로 수행됩니다.

6. Samba 사용자가 인증되고 유효한 posix 사용자로 매핑되면 CIFS Server는 사용자 토큰 세션 ID를 Windows PC 클라이언트로 반환합니다.

설치 및 구성 요약

다음 내용에서는 LDAP를 지원하는 HP CIFS Server를 설치, 구성, 확인 및 활성화하기 위한 절차를 간략하게 설명합니다.

- Netscape Directory Server(아직 설치되지 않은 경우)를 설치합니다. 141페이지의 “Netscape Directory Server 설치”를 참조하십시오.
- Netscape Directory Server(아직 구성되지 않은 경우)를 구성합니다. 141페이지의 “Netscape Directory Server 구성”을 참조하십시오.
- HP CIFS Server에 LDAP-UX 클라이언트 서비스(아직 설치되지 않은 경우)를 설치합니다. 143페이지의 “HP CIFS Server에 LDAP-UX Client Services 설치”를 참조하십시오.
- HP CIFS Server에 LDAP-UX 클라이언트 서비스(아직 구성되지 않은 경우)를 구성합니다. 144페이지의 “LDAP-UX Client Services 구성”을 참조하십시오.
- SSL(Secure Sockets Layer)을 사용하려는 경우에는 SSL을 활성화합니다. 149페이지의 “SSL(Secure Sockets Layer) 사용”을 참조하십시오.
- 데이터를 Netscape Directory Server로 마이그레이션합니다. 152페이지의 “Netscape Directory에 데이터 마이그레이션”을 참조하십시오.
- Samba 하위 스키마를 Netscape Directory Server로 확장합니다. 157페이지의 “Samba 하위 스키마를 Directory Server로 확장”을 참조하십시오.
- LDAP를 지원하도록 HP CIFS Server를 구성합니다. 160페이지의 “HP CIFS Server 구성”을 참조하십시오.
- Samba 사용자를 Netscape Directory Server에 설치합니다. 163페이지의 “디렉토리에 Samba 사용자 설치”를 참조하십시오.

LDAP를 지원하는 HP CIFS Server 설치 및 구성에 대한 자세한 내용은 이어지는 절의 내용을 참조하십시오.

Netscape Directory Server 설치 및 구성

이 절에서는 Netscape Directory Server를 설치하고 LDAP-UX 클라이언트 서비스 및 HP CIFS Server를 사용하도록 구성하는 방법을 설명합니다.

디렉토리 구성에 대한 자세한 내용은 *http://docs.hp.com/hpux/internet*의 *Preparing Your LDAP Directory for HP-UX Integration*을 참조하십시오.

Netscape Directory Server 설치

Netscape Directory Server(아직 설치되지 않은 경우)를 설치해야 합니다. HP에서는 HP Netscape Directory Server 제품(J4258CA)의 설치를 권장합니다. 이 제품은 *http://software.hp.com*에서 다운로드할 수 있습니다. HP-UX 버전 6.02 이상용 Netscape Directory Server 제품으로 설치해야 합니다.

HP-UX 버전 6.02 이상용 Netscape Directory Server를 설치한 경우에는 posix 스키마가 이미 설치되어 있습니다. 이 스키마는 `/opt/ldapux/ypldapd/etc/slapd-v3.nis.conf` 파일에 들어 있습니다. Posix 스키마(RFC2307)에 대한 자세한 내용은 *http://www/ietf.org/rfc.html*을 참조하십시오. RFC 2307은 `posixAccount`, `posixGroup` 등의 객체 클래스로 구성됩니다. `posixAccount`는 `/etc/passwd` 파일의 사용자 항목을 나타내며 `posixGroup`은 `/etc/group` 파일의 그룹 항목을 나타냅니다.

Netscape Directory Server 구성

Netscape Directory Server(아직 구성되지 않은 경우)를 구성해야 합니다. 이 절에서는 HP-UX용 Netscape Directory Server를 구성하는 방법에 대한 주요 작업을 설명합니다.

대부분의 구성 매개 변수에 대해 기본값을 선택하면 Netscape Directory Server를 신속히 구성할 수 있습니다. 다음은 주요 구성 작업을 보여줍니다.

단계

1. `root`로 로그인하고 `setup` 프로그램을 실행합니다.

```
$ cd /var/opt/netscape/servers/setup
$ ./setup
```

단계 **2.** 사용자 데이터를 저장할 Netscape Directory Server의 호스트 이름을 입력합니다.

단계 **3.** 이전에 지정한 디렉토리 서버의 포트 번호를 입력합니다. 기본 포트 번호는 389입니다.

단계 **4.** 관리자의 고유 이름(DN)과 암호를 입력합니다. 이 사용자는 운영자 권한을 가지고 있습니다. 예를 들면, "admin"을 관리자 DN으로 입력할 수 있습니다.

단계 **5.** 기본 DN을 입력합니다. 이 DN은 Netscape Directory Server의 정규화된 호스트 이름 중 DNS 부분입니다. 예를 들어, 디렉토리 서버의 호스트 이름이 "hostA.org.hp.com"이면 기본 DN은 "dc=org, dc=hp, dc=com"입니다.

단계 **6.** 모든 권한을 가진 디렉토리 관리자의 고유 이름(DN)과 암호를 입력합니다. 예를 들어, "Directory Manager"를 디렉토리 관리자 DN으로 입력할 수 있습니다.

단계 **7.** 관리 도메인(Netscape Directory Server의 정규화된 호스트 이름 중 DNS 도메인 부분)을 지정합니다.

단계 **8.** 관리 포트 번호를 지정합니다. 이 포트 번호는 1024와 65535 사이의 임의 번호입니다. 이 포트 번호를 사용하여 Netscape Directory Server 관리를 위해 디렉토리 서버에 연결합니다.

단계 **9.** 디렉토리 서버를 구성한 후에는 관리 콘솔 데몬이 자동으로 시작되어 선택한 포트 상에서 수신합니다.

Netscape Directory Server 확인

다음 명령을 실행하여 Netscape Directory Server를 올바르게 설치 및 구성했는지 확인하고 Netscape Directory Server 데몬이 실행되고 있는지 확인합니다.

```
$ ps -ef | grep ns-
```

이 명령의 출력은 다음과 같습니다.

```
root 17289  17288 0  18:54:34 ? 0:00  ns-httpd -d
/var/opt/netscape/servers/admin-serv/config
www 17230      1 0 18:53:54 ? 0:03 ./ns-slapd -D
/var/opt/netscape/servers/slapd-hpcif57 -i /var/o
```

HP CIFS Server에 LDAP-UX Client Services 설치

swinstall(1M)을 사용하여 NativeLdapClient 하위 제품인 LDAP-UX 클라이언트 서비스 소프트웨어를 HP CIFS Server에 설치합니다. 설치 절차에 대한 자세한 내용은 **LDAP-UX Client Services B.03.20 릴리즈 노트**를 참조하십시오. LDAP-UX 클라이언트 서비스 소프트웨어는 *http://www.software.hp.com*에서 제공합니다. LDAP-UX 클라이언트 서비스 버전 B.03.20 이상을 설치해야 합니다. 제품을 설치한 후에는 시스템을 다시 부팅할 필요가 없습니다.

LDAP-UX Client Services 구성

LDAP-UX 클라이언트 서비스가 아직 구성되지 않은 경우에는 구성해야 합니다. 이 절에서는 Netscape Directory Server 버전 6.02 이상으로 LDAP-UX 클라이언트 서비스를 구성하는 주요 단계를 설명합니다. LDAP-UX 클라이언트 서비스를 구성하는 방법에 대한 자세한 내용은 *http://www.docs.hp.com*에 있는 *LDAP-UX Client Services B.03.20 Administrator's Guide*의 "*Configure the LDAP-UX Client Services*"를 참조하십시오.

`setup` 프로그램을 실행하여 LDAP-UX 클라이언트 서비스를 구성해야 합니다. 이 요구 사항을 반드시 준수해야 합니다. 그렇지 않으면, LDAP를 지원하는 HP CIFS Server가 올바르게 작동하지 않습니다.

`setup` 프로그램을 실행하여 클라이언트 시스템에 LDAP-UX 클라이언트 서비스를 구성할 경우에는 `setup`에서 다음 주요 작업을 자동으로 수행합니다.

- Netscape 디렉토리 스키마를 posixAccount objectclass 및 속성으로 확장합니다(아직 확장되지 않은 경우).
- 사용자가 제공하는 정보에서 Netscape Directory의 구성 프로파일 항목을 작성합니다. 프로파일에는 클라이언트가 디렉토리의 사용자 및 그룹 데이터에 액세스하는 데 필요한 정보가 들어 있습니다. 예를 들면, 다음과 같습니다.
  - 디렉토리 서버 호스트
  - 디렉토리 서버 네트워크 포트
  - 디렉토리에서 사용자, 그룹 및 기타 정보 위치
- 로컬 클라이언트의 시작 파일을 디렉토리 및 구성 프로파일 위치로 업데이트합니다.
- 디렉토리에서 LDAP 클라이언트 시스템으로 구성 프로파일을 다운로드합니다.
- 사용자 및 그룹 검색을 위한 LDAP 접미사로 기본 DN을 할당합니다.
- 제품 데몬 `ldapclientd`를 시작합니다(시작하도록 선택한 경우). LDAP-UX Client B.03.20의 경우 LDAP-UX 기능이 작동하도록 하려면 클라이언트 데몬을 시작해야 합니다.

빠른 구성

다음과 같이 대부분의 구성 매개 변수에 대해 기본값을 선택하면 LDAP-UX 클라이언트 서비스를 신속히 구성할 수 있습니다.

단계 **1.** Samba 조직 단위 기본값과의 일관성을 유지하려면 `/opt/ldapux/migrate/migrate_common.ph` 파일을 편집하여 `ou=Group` `$RFC2307BIS` 구조의 기본 그룹 objectclass를 `ou=Groups`로 변경해야 합니다.

단계 **2.** root로 로그인한 후 `setup` 프로그램을 실행합니다.

```
$ cd /opt/ldapux/config
$ ./setup
```

`setup` 프로그램에서 몇 가지 질문과 기본 응답을 제공합니다. **Enter** 키를 눌러 기본값을 사용하거나 값을 변경한 다음 **Enter** 키를 누릅니다. 설치 중에 언제든지 **Ctrl+b**를 눌러 백업하거나 **Ctrl+c**를 눌러 설치 프로그램을 종료합니다.

단계 **3.** Netscape Directory를 LDAP 디렉토리 서버(옵션 1)로 선택합니다.

단계 **4.** 프로파일이 있는 디렉토리 서버 또는 새 프로파일을 작성할 디렉토리 서버의 호스트 이름 또는 IP 주소를 입력합니다.

단계 **5.** 프로파일을 저장할 이전에 지정한 디렉토리 서버의 포트 번호를 입력합니다. 기본 포트 번호는 389입니다.

`Setup` 프로그램에서 스키마가 `posixAccount` objectclass와 속성으로 확장되었는지 디렉토리를 검사합니다. 이 검사를 반드시 수행해야 하지만 한 번만 수행하면 됩니다.

단계 **6.** 스키마가 이미 확장된 경우에는 `setup` 프로그램에서 이 단계를 건너뜁니다. 그렇지 않으면, 스키마를 확장하기 위해 디렉토리 스키마를 확장할 수 있는 디렉토리 사용자의 고유 이름(DN)과 암호를 입력합니다. 예를 들어, 디렉토리 관리자의 디렉토리 관리자 DN과 암호로 "`Directory Manager`"를 입력할 수 있습니다.

스키마를 확장하려면 다음을 입력해야 합니다.

1. 디렉토리 사용자의 DN을 입력합니다. 기본값이 표시됩니다. 기본값을 사용하려면 **Enter** 키를 누르고, 그렇지 않으면 DN 이름을 입력합니다.
2. 암호를 입력합니다.

단계 **7.** 새 프로파일을 작성할 경우에는 디렉토리에 프로파일 DN의 모든 상위 항목(있는 경우)을 추가합니다. 새 프로파일을 작성하려 하지만 프로파일의 상위 항목이 디렉토리에 아직 존재하지 않는 경우에는 설치가 수행되지 않습니다. 예를 들어, 프로파일을 **cn=ldapuxprofile, dc=org, dc=hp, dc=com**으로 지정하려는 경우 기본 경로인 **org.hp.com**이 디렉토리에 있어야 합니다. 그렇지 않으면 설치가 수행되지 않습니다.

새 프로파일을 작성하는 중에 프로파일 DN의 모든 상위 항목을 디렉토리에 추가합니다. 모든 상위 항목 없이 새 프로파일을 작성할 경우 **설치**가 수행되지 않습니다.

단계 **8.** 다음에는 사용할 기존 프로파일의 DN 또는 새 프로파일의 DN을 입력합니다.

디렉토리의 모든 프로파일을 표시하려면 다음과 같은 명령을 사용합니다.

```
$ ldapsearch -b o=org.hp.com objectclass=DUAConfigProfile dn
```

기존 프로파일을 사용할 경우 setup 프로그램이 클라이언트를 구성하고 프로파일을 다운로드한 후 종료됩니다. 이 경우 아래 단계 11을 계속 진행합니다.

단계 **9.** 새 프로파일을 작성할 경우에는 새 프로파일을 만들 수 있는 디렉토리 사용자의 디렉토리 관리자 DN 및 암호를 입력합니다.

단계 **10.** 다음에는 이름 서비스 데이터를 저장할 디렉토리의 호스트 이름과 포트 번호를 입력합니다. 가용성을 높이기 위해 각 LDAP-UX 클라이언트는 최대 세 개의 서로 다른 디렉토리 호스트에서 이름 서비스 데이터를 검색할 수 있습니다. 순서대로 검색할 최대 세 개의 호스트를 입력할 수 있습니다.

단계 **11.** passwd, group, hosts, services 등과 같이 클라이언트가 사용자 이름 서비스 데이터를 검색해야 할 기본 DN을 입력합니다.

단계 **12.** 프롬프트가 표시될 때 나머지 기본 구성 매개 변수를 그대로 적용하면 Netscape 디렉토리와 첫 번째 클라이언트를 신속히 구성할 수 있습니다.

표 6-1에서는 구성 매개 변수와 해당 기본값을 보여줍니다.

표 6-1 구성 매개 변수 및 기본값

매개 변수	기본값
클라이언트 바인딩 유형	Anonymous
바인딩 시간 제한	5초
검색 시간 제한	제한 없음
조회 사용	예
프로파일 TTL(지속 시간)	0 - 무한
지원되는 서비스에 대해 표준 RFC-2307 객체 클래스 속성 사용	예
지원되는 서비스에 대해 기본 검색 설명 사용	예
인증 방법	Simple

표 6-1에 있는 구성 매개 변수에 대한 자세한 내용은 *http://www.docs.hp.com*에 있는 **LDAP-UX Client Services B.03.20 관리 설명서**의 "**부록 B: LDAP-UX Client Services Object Classes**"를 참조하십시오.

단계 13. 구성 정보를 입력한 후에는 `setup` 프로그램에서 스키마를 확장하고 새 프로파일을 만든 후 디렉토리를 사용하도록 클라이언트를 구성합니다.

단계 14. NSS(Name Service Switch)를 구성합니다.

`/etc/nsswitch.conf` 파일의 사본을 저장하고 소스를 편집하여 사용할 ldap 이름 서비스 및 기타 이름 서비스를 지정합니다. 예제는 `/etc/nsswitch.ldap` 파일을 참조하십시오. `/etc/nsswitch.ldap`를 `/etc/nsswitch.conf`로 복사할 수 있습니다. 자세한 내용은 *nsswitch.conf*(4)를 참조하십시오.

단계 15. 클라이언트 데몬 `/opt/ldapux/bin/ldapclientd`를 시작할지 여부를 묻는 메시지가 표시됩니다. LDAP 기능이 작동되도록 하려면 클라이언트 데몬을 시작해야 합니다.

단계 16. 다음 명령을 실행하여 구성을 확인합니다.

```
$ /opt/ldapux/bin/ldapsearch -T -b "cn=schema" -s base \
"(objectclass=*)"|grep -i posix
```

ldapsearch 명령을 실행할 때 posixAccount objectclass가 출력에 표시되는지 확인합니다. 출력은 다음과 같습니다.

```
objectClasses: ( 1.3.6.1.1.1.2.0 NAME "posixAccount" DESC
"Standard LDAP objectclass" SUP top AUXILIARY MUST ( cn $ uid $
uidNumber $ gidNumber $ homeDirectory) MAY ( userPassword $
loginShell $ gecos $ description ) X-ORIGIN "RFC 2307" )
```

```
objectClasses: ( 1.3.6.1.1.1.2.2 NAME "posixGroup" DESC
"Standard LDAP objectclass" SUP top STRUCTURAL MUST ( cn $
gidNumber ) MAY ( userPassword $ memberUid $description ) X-
ORIGIN "RFC 2307" )
```

참고

ldapsearch 명령줄 유틸리티를 사용하면 LDAP 디렉토리 항목을 찾아서 가져올 수 있습니다. 이 유틸리티는 지정한 고유 이름(DN)과 암호를 사용하여 지정된 서버와의 연결을 열고 지정한 검색 필터에 기초하여 항목을 검색합니다. 자세한 내용은 *Netscape Directory Server 6.02 for HP-UX Administrator's Guide (http://www.docs.hp.com/hpux/internet)*를 참조하십시오.

SSL(Secure Sockets Layer) 사용

HP CIFS Server는 CIFS Server와 SSL 활성 LDAP 디렉토리 서버 간에 안전하게 통신할 수 있도록 SSL(Secure Sockets Layer)을 지원합니다.

SSL을 사용할 계획이지만 아직 LDAP에 SSL을 사용하지 않는 경우에는 Netscape Directory Server 및 LDAP-UX 클라이언트에서 이를 활성화해야 합니다. LDAP 서버 및 클라이언트를 활성화한 경우에는 SSL을 사용하도록 HP CIFS Server를 구성할 수 있습니다.

LDAP에서 SSL 통신을 활성화하려면 우선 CS(Certification Authority) Server를 제대로 설정해야 합니다.

LDAP 디렉토리 서버, LDAP-UX 클라이언트 및 SSL을 지원하는 HP CIFS Server 구성에 대한 자세한 내용은 다음 하위 절을 참조하십시오.

SSL을 사용하도록 Netscape Directory Server 구성

다음 단계에 따라 LDAP 상에서 SSL 통신을 활성화하도록 Netscape Directory Server를 구성합니다.

단계 **1.** Netscape Directory Server에 대한 인증서를 확보하여 설치하고 CA(Certification Authority)를 신뢰하도록 Netscape Directory Server를 구성합니다.

자세한 내용은 *http://docs.hp.com*에 있는 *Netscape Directory Server 6.1 Administrator's Guide*에서 "*Managing SSL*" 장의 "*Obtaining and Installing Server Certificates*" 절을 참조하십시오.

단계 **2.** 디렉토리에서 SSL을 활성화합니다.

디렉토리 서버에서 SSL을 활성화하는 방법에 대한 자세한 내용은 *http://docs.hp.com*에 있는 *Netscape Directory Server 6.1 Administrator's Guide*에서 "*Managing SSL*" 장의 "*Activating SSL*" 절을 참조하십시오.

단계 **3.** SSL 사용 가능 디렉토리 서버에 연결하도록 관리 서버를 구성합니다.

SSL 사용 가능 디렉토리 서버에 연결하도록 관리 서버를 구성하는 방법에 대한 자세한 지침은 *http://docs.hp.com*에 있는 *Managing Servers with Netscape Console*을 참조하십시오.

SSL을 사용하도록 LDAP-UX Client 구성

SSL을 사용하려는 경우에는 LDAP-UX 클라이언트에 CA(Certification Authority) 인증서를 설치하고 SSL을 사용하도록 LDAP-UX 클라이언트를 구성해야 합니다.

다음 단계에 따라 LDAP 클라이언트 시스템에서 SSL을 활성화합니다.

단계 **1.** 선택적으로 디렉토리 서버의 각 사용자가 모든 LDAP 클라이언트에 대해 SSL을 사용하여 인증할 개인용 인증서를 확보하고 설치했는지 확인하십시오.

Netscape Communicator에서 인증서 데이터베이스를 다운로드하여 인증서 데이터베이스를 사용자의 LDAP-UX 클라이언트에 설치하는 것도 하나의 방법입니다.

인증서 데이터베이스 파일 `cert7.db` 및 `key3.db`는 사용 중인 Netscape Communicator의 버전에 따라 클라이언트 시스템에서 `/.netscape` 또는 `/.mozilla/default/*.slt` 디렉토리에 다운로드됩니다. Netscape Communicator 7.0을 사용하여 Certification Authority 인증서를 다운로드하는 경우에는 인증서 데이터베이스 파일 `cert7.db` 및 `key3.db`가 `/.mozilla/default/*.slt` 디렉토리로 다운로드됩니다.

Netscape Communicator 4.75를 사용하여 Certificate Authority 인증서를 다운로드하면 인증서 데이터베이스 파일 `cert7.db` 및 `key3.db`는 `/.netscape` 디렉토리로 다운로드됩니다.

인증서 데이터베이스 파일 `cert7.db` 및 `key3.db`를 클라이언트에 다운로드한 후에는 `cert7.db`를 가리키는 `/etc/opt/ldapux/cert7.db` 및 `key3.db`를 가리키는 `/etc/opt/ldapux/key3.db` 심볼릭 링크를 만들어야 합니다.

LDAP-UX 클라이언트 시스템에 Certification Authority 인증서를 설치하는 방법에 대한 자세한 내용은 *http://docs.hp.com*에 있는 *LDAP-UX Client Services B.03.20 Administrator's Guide*에서 "*Installing LDAP-UX Client Services*" 장의 "*Configuring LDAP Clients to Use SSL*" 절을 참조하십시오.

단계 **2.** `setup` 프로그램을 실행하여 LDAP-UX 클라이언트 서비스가 SSL을 사용하도록 구성합니다. LDAP-UX 클라이언트 서비스에서 SSL을 활성화하기 위해 설치 프로그램을 실행하는 방법에 대한 자세한 내용은 *http://docs.hp.com*에 있는 *LDAP-UX*

*Client Services B.03.20 Administrator's Guide*에서 *Installing LDAP-UX Client Services* 장의 *Custom Configuration* 하위 절을 참조하십시오.

LDAP-UX 클라이언트 서비스가 이미 설치되어 있으면 다음과 같이 `/etc/opt/ldapux/ldapux_profile` 파일에서 `authenticationMethod` 및 `preferredServerList` 속성을 수정하십시오.

- `authenticationMethod` 속성을 수정하여 전송 계층 보안 인증 방법 `tls:`를 소스 인증 방법 `simple` 앞에 추가합니다.

  예를 들어, SSL을 활성화하지 않은 상태에서는 원래 `authenticationMethod` 항목은 **authenticationMethod: simple**입니다. SSL을 활성화하면 `authenticationMethod` 항목은 **authenticationMethod: tls:simple**이 됩니다.

- `preferredServerList` 속성을 수정하여 일반 LDAP 포트 번호 389를 SSL 포트 번호 636으로 변경합니다.

  예를 들어, SSL을 활성화되지 않은 상태에서는 원래 `preferredServerList` 항목은 다음과 같습니다. **preferredServerList: 1.2.5.20:389.** With SSL을 활성화하면 `preferredServerList` 항목은 **preferredServerList: 1.2.5.20:636**이 됩니다.

SSL을 사용하도록 HP CIFS Server 구성

HP CIFS Server A.02.* 버전의 경우, SSL을 지원할 수 있도록 `smb.conf`에서 `passwd backend = ldapsam:ldaps://<fully qualitied name of NDS server>`을 설정합니다. 이전 버전과 호환되는 A.01.* 버전의 LDAP 계정 백엔드를 사용하려는 경우에는 `smb.conf`에서 `passwd backend = ldapsam_compat://ldaps:< ldap server name>,ldap ssl = yes` 및 `ldap port = 636`을 설정하여 SSL을 활성화합니다.

HP CIFS Server에서 SSL을 활성화하는 방법에 대한 자세한 내용은 160페이지의 “LDAP 구성 매개 변수”를 참조하십시오.

Netscape Directory에 데이터 마이그레이션

/etc/passwd 파일 또는 NIS 데이터베이스 파일의 모든 UNIX 사용자 계정을 Netscape Directory Server로 마이그레이션하는 것이 좋습니다. LDAP-UX Integration 제품에서는 이 작업을 자동으로 수행하는 마이그레이션 스크립트를 제공합니다. 이 스크립트는 /opt/ldapux/migrate 디렉토리에 있습니다. migrate_all_online.sh 및 migrate_all_nis_online.sh라는 두 가지 셸 스크립트는 /etc 디렉토리 또는 NIS 맵의 모든 소스 파일을 마이그레이션합니다. 반면 perl 스크립트 migrate_passwd.pl, migrate_group.pl 및 migrate_hosts.pl은 개별 파일을 마이그레이션합니다. 셸 스크립트는 perl 스크립트를 호출합니다. 마이그레이션 스크립트의 기능 및 사용 방법에 대한 자세한 내용은 */opt/ldapux/README* 파일 또는 *http://docs.hp.com*에 있는 *LDAP-UX Client Services B.03.20 Administrator's Guide*의 "*Name Service Migration Scripts*" 절을 참조하십시오.

모든 파일 마이그레이션

migrate_all_online.sh 및 migrate_all_nis_online.sh라는 두 가지 셸 스크립트는 모든 이름 서비스 데이터를 LDIF(LDAP Data Interchange Format) 파일 또는 디렉토리로 직접 마이그레이션합니다. migrate_all_online.sh 셸 스크립트는 /etc/passwd, /etc/group 및 /etc/hosts와 같은 소스 파일에서 정보를 가져옵니다. migrate_all_nis_online.sh 스크립트는 *ypcat(1)* 명령을 사용하여 NIS 맵에서 정보를 가져옵니다. 이 스크립트는 매개 변수를 사용하지 않지만 필요한 정보를 입력하라는 메시지가 표시됩니다. 또한 출력을 LDIF로 그대로 둘지 또는 항목을 디렉토리에 추가할지 묻는 프롬프트가 표시됩니다.

참고

root 사용자인 IT 관리자와 같은 일부 사용자를 /etc/passwd 파일에 보관하는 것이 좋습니다. 이렇게 하면 HP-UX 시스템에서 root 사용자가 다른 암호를 사용할 수 있습니다. 또한 LDAP 디렉토리 서버를 사용할 수 없는 경우에도 여전히 시스템에 로그인할 수 있습니다.

참고

마이그레이션 스크립트를 실행하기 전에 /opt/ldapux/migrate/migrate_common.ph 파일을 편집하여 $RFC2307BIS 구조의 기본 그룹 objectclass를 ou=Group에서 ou=Groups로 변경합니다. 이렇게 하면 Samba 조직 단위 기본값과 일치시킬 수 있습니다.

예제

다음 예제에서 마이그레이션 스크립트인 migrare_all_online.sh를 사용하여 데이터를 LDAP 디렉토리로 가져오는 데 필요한 단계를 보여줍니다.

단계 1. LDAP_BASEDN인 환경 변수를 설정하여 데이터를 저장할 위치를 지정합니다.

예를 들면, 다음 명령은 LDAP 기본 DN을 org.hp.com으로 설정합니다.

```
$ export LDAP_BASEDN="dc=org, dc=hp, dc=com"
```

단계 2. 다음 스크립트 migrate_all_online.sh를 실행하여 /etc 파일의 모든 이름 서비스 데이터 파일을 LDIF 파일로 마이그레이션합니다.

```
$ migrate_all_online.sh
```

스크립트에 적절히 응답합니다. 이 예제에서는 cn=Directory Manager 및 credentials to bind를 디렉토리 관리자 암호와 함께 사용합니다.

참고

이 경우 LDAP 디렉토리 서버에는 pam 및 nsswitch의 백엔드로 사용하는 데 필요한 모든 항목이 포함되어 있습니다. HP CIFS Server에서 sambaSamAccount objectclass와 posixAccount objectclass의 일부 속성을 공유하므로 우선 이 디렉토리 서버가 필요합니다.

개별 파일 마이그레이션

다음의 perl 스크립트는 /etc 디렉토리에서 각 소스 파일을 LDIF로 마이그레이션합니다. 이 스크립트는 152페이지의 "모든 파일 마이그레이션" 절에 설명된 셸 스크립트를 통해 호출됩니다. perl 스크립트는 입력 소스 파일과 출력 LDIF에서 정보를 가져옵니다.

환경 변수

perl 스크립트를 사용하여 개별 파일을 마이그레이션하는 경우 다음 환경 변수를 설정해야 합니다.

LDAP_BASEDN 데이터를 저장할 기본 고유 이름입니다.
예를 들어, 다음 명령은 기본 DN을 DC=org, DC=hp, DC=com으로 설정합니다.

```
export LDAP_BASEDN="DC=org, DC=hp, DC=com"
```

Perl 마이그레이션 스크립트의 일반 구문

모든 perl 마이그레이션 스크립트에서는 다음과 같은 일반 구문을 사용합니다.

scriptname inputfile [outputfile]

여기서 각 항목에 대한 설명은 다음과 같습니다.

scriptname 이 이름은 사용하려는 특정 스크립트의 이름입니다. 표 6-2는 마이그레이션 스크립트 목록을 제공합니다.

inputfile 이 이름은 사용하려는 스크립트에 해당하는 해당 이름 서비스 소스 파일의 이름입니다.

outputfile 이 매개 변수는 선택적인 매개 변수로 LDIF가 저장되는 파일의 이름입니다. stdout은 기본 출력입니다.

마이그레이션 스크립트

아래 표 6-2에서는 마이그레이션 스크립트를 설명합니다.

표 6-2 마이그레이션 스크립트

스크립트 이름	설명
migrate_base.pl	기본 DN 정보를 만듭니다.

표 6-2 마이그레이션 스크립트(계속)

스크립트 이름	설명
migrate_group.pl	/etc/group 파일의 그룹을 마이그레이션합니다.
migrate_hosts.pl [a]	/etc/hosts 파일의 호스트를 마이그레이션합니다.
migrate_networks.pl	/etc/networks 파일의 네트워크를 마이그레이션합니다.
migrate_passwd.pl[b]	/etc/passwd 파일의 사용자를 마이그레이션합니다.
migrate_protocols.pl	/etc/protocols 파일의 프로토콜을 마이그레이션합니다.
migrate_rpc.pl	/etc/rpc 파일의 RPC를 마이그레이션합니다.
migrate_services.pl[c]	/etc/services 파일의 서비스를 마이그레이션합니다.
migrate_common.ph	모든 perl 스크립트에서 사용하는 루틴 및 구성 정보를 지정합니다.

a. 시스템이 동일한 호스트 이름으로 구성된 경우에는 마이그레이션 스크립트 migrate_host.pl에서 각 IP 주소의 호스트 이름에 대해 동일한 고유 이름을 사용하여 만든 LDIF 파일에 여러 항목을 만듭니다. 고유 이름은 LDAP 디렉토리에서 고유해야 하므로 먼저 지정된 호스트 레코드와 IP 주소를 수동으로 병합하고 LDIF 파일에서 중복된 레코드를 삭제해야 합니다. 그 결과 다음과 같은 형태로 병합됩니다.

. . . .
dn: cn=machineA, ou=hosts, ou=unix, dc=org, dc=hp, dc=com
objectClass: top
objectClass: ipHost
ipHostNumber: 1.3.5.72
ipHostNumber: 1.3.8.4
ipHostNumber: 1.5.8.76
cn: hostA
cn: hostA.org.hp.com
. . . .

b. Netgroup
- NIS 최적화 맵 "byuser" 및 "byhost"는 사용되지 않습니다.
-세 쌍씩 단일 문자열로 저장됩니다.
-세 쌍씩 괄호로 묶어야 합니다. 예를 들어, "machine, user, domain"은 유효하지 않지만 "(machine, user, domain)"은 유효한 세 쌍입니다.

c. 서비스 데이터를 LDAP 디렉토리로 마이그레이션하는 경우 여러 프로토콜이 여러 서비스 포트가 **아닌** 하나의 서비스 이름에만 연결될 수 있습니다.

예제

다음 단계를 수행하여 /etc/passwd 파일을 LDIF 파일로 마이그레이션합니다.

단계 1. 환경 변수인 LDAP_BASEDN을 설정하여 데이터를 저장할 위치를 지정합니다.

예를 들면, 다음 명령은 LDAP 기본 DN을 org.hp.com으로 설정합니다.

```
$ export LDAP_BASEDN="dc=org, dc=hp, dc=com"
```

단계 2. 다음 스크립트 migrate_passwd.pl을 실행하여 /etc/passwd 파일의 모든 데이터를 /tmp/passwd.ldif 파일로 마이그레이션합니다.

```
$ migrate_passwd.pl /etc/passwd /tmp/passwd.ldif
```

출력 중 일부는 다음과 같습니다.

```
dn: uid=johnl,ou=People,dc=org,dc=hp,dc=com
objectclass: top
objectclass: account
objectclass: posixAccount
objectclass: Account
loginShell: /usr/bin/ksh
uidNumber: 8662
gidNumber: 8200
homeDirectory: /home/johnl
gecos: John Louie, 48S-020, 447-1890
userPassword: {crypt}aOACGvt0T, 1fo
acctFlags: UX
pwdLastSet: 1063301239
```

Samba 하위 스키마를 Directory Server로 확장

이제 Samba 하위 스키마가 있는 Netscape Directory Server 스키마를 HP CIFS Server의 sambaSamAccount 하위 스키마에서 Netscape Directory Server로 확장해야 합니다. 스키마를 확장하기 전에 LDAP 디렉토리 및 LDAP-UX 클라이언트 서비스를 구성했으며 데이터를 LDAP 디렉토리로 마이그레이션했는지 확인합니다.

Samba 하위 스키마는 HP CIFS Server A.02.*에서 향상되었습니다. LDAP 백엔드를 사용하는 경우에는 버전 A.01.*의 스키마를 계속 사용할 것인지 업데이트된 버전 A.02.*의 스키마를 사용할 것인지 선택해야 합니다. 사용할 스키마를 선택하려면 `smb.conf`의 매개 변수를 다음과 같이 설정합니다.

- 버전 A.02.*의 업데이트된 스키마를 사용하려면 `passwd backend` 매개 변수를 `ldapsam:ldap://<ldap server name>`으로 설정합니다.
- 버전 A.01.*의 스키마를 사용하려면 `passwd backend` 매개 변수를 `ldapsam_compat:ldap://<ldap server name>`으로 설정합니다.

HP CIFS Server A.02.01.*와 A.02.02 사이의 Samba 하위 스키마 차이점

Samba 하위 스키마는 HP CIFS Server A.02.02에서 수정되었습니다. 이 절에서는 HP CIFS Server A.02.02에서 제거된 속성 및 objectclass와 새로운 속성 및 objectclass의 목록을 보여줍니다.

제거된 속성 및 Objectclass

다음은 HP CIFS Server A.02.02에서 제거된 속성 및 objectclass의 목록입니다.

- `sambaPrivName` 속성
- `sambaPrivilegeList` 속성
- `sambaPrivilege` objectclass

더 이상 사용되지 않는 위 속성 및 objectclass는 HP CIFS Server A.02.01.*에서 사용된 적이 없습니다.

새로운 속성 및 Objectclass

다음은 새로운 속성 및 objectclass의 목록입니다.

- `sambaAccountPolicyName` 속성
- `sambaAccountPolicyValue` 속성
- `sambaAccountPolicy` objectclass

위의 새로운 속성 및 objectcalss는 현재 HP CIFS Server A.02.02에서 사용되지 않습니다.

참고

업데이트된 Samba 하위 스키마는 HP CIFS A.02.01.*에서 사용할 수 있는 하위 스키마와 호환됩니다. 디렉토리 서버에 버전 A.02.01.*의 Samba 하위 스키마를 사용한 경우에는 HP CIFS Server A.02.02로 업그레이드한 후에도 계속 사용할 수 있습니다.

Samba 하위 스키마를 디렉토리로 확장하는 절차

HP CIFS Server A.02.*의 Samba 하위 스키마 `/opt/samba/LDAP3/98samba3.ldif`를 Netscape Directory Server로 확장하려면 다음 단계를 수행합니다.

단계

1. `ftp` 명령을 실행하여 HP CIFS Server에서 `/opt/samba/LDAP3/98samba3.ldif` 파일을 가져와서 Netscape Directory Server에 저장합니다.

   예를 들어, 다음 명령은 `/opt/samba/LDAP3/98samba3.ldif` 파일을 HP CIFS Server에서 Netscape Directory Server(hostA.hp.com)의 `/var/opt/netscape/servers/sldapd-hostA.hp.com/config/schema/98samba3.ldif` 파일로 복사합니다.

   ```
   cd /opt/samba/LDAP3
   ftp hostA.org.hp.com
   user root
   rootpasswd
   cd /var/opt/netscape/servers/sldapd-hostA.hp.com/config/schema
   bin
   put 98samba3.ldif
   quit
   ```

단계 **2.** Netscape Directory Server에 로그인하고 데몬 `slapd`를 다시 시작합니다. 이렇게 하면 LDAP 디렉토리에서 `sambaSamAccount` 하위 스키마를 인식할 수 있습니다.

```
$ /var/opt/netscape/servers/slapd-<server name>/restart-slapd
```

예를 들면 다음과 같습니다.

```
$ /var/opt/netscape/servers/slapd-hostA.hp.com/restart-slapd
```

단계 **3.** 다음의 `ldapsearch` 명령을 사용하여 Netscape Directory Server의 스키마를 Samba 하위 스키마로 업데이트했는지 확인합니다.

```
$ /opt/ldapux/bin/ldapsearch -T -b "cn=schema" -s base \
"(objectclass=*)"|grep -i samb
```

`ldapsearch` 명령을 실행할 때 출력에 `sambaSamAccount` objectclass가 표시되는지 확인해야 합니다.

```
objectClasses: ( 1.3.6.1.4.1.7165.2.2.6 NAME
'sambaSamAccount' DESC 'Samba 3.0 Auxilary SAM Account'
STRUCTURAL MUST ( uid $ sambaSID )
```

HP CIFS Server 구성

LDAP 기능을 지원하도록 HP CIFS Server를 설치 및 구성해야 합니다.

LDAP 구성 매개 변수

다음은 LDAP 기능을 사용하도록 HP CIFS Server를 구성하는 데 사용할 수 있는 새로운 전역 매개 변수의 목록입니다. 이러한 매개 변수는 전역 매개 변수 아래 있는 `/etc/opt/samba/smb.conf` 파일에서 설정됩니다.

[global] 여기에 정의된 전역 설정은 LDAP 지원 기능이 있는 HP CIFS Server에서 사용합니다.

표 6-3 전역 매개 변수

매개 변수	설명
`ldap port`	LDAP 디렉토리 서버에 연결하는 데 사용되는 TCP 포트 번호를 지정합니다. 기본적으로 이 매개 변수는 389로 설정되어 있습니다.
`ldap server`	데이터를 저장할 Netscape Directory Server의 호스트 이름을 지정합니다.
`ldap suffix`	사용자 및 컴퓨터 계정 정보를 추가할 디렉토리 트리의 기본 위치를 지정합니다. 이 위치는 항목의 검색을 시작할 위치를 LDAP에 알려주는 검색 기준의 고유 이름(DN)으로 사용되기도 합니다. 예를 들어, 기본 DN이 "dc=org, dc=hp, dc=com"이면 `ldap suffix = "dc= org, dc=hp, dc=com"`의 값을 설정해야 합니다.
`ldap user suffix`	사용자 정보를 추가할 디렉토리 트리의 기본 위치를 지정합니다. 이 매개 변수를 지정하지 않으면 HP CIFS Server에서는 `ldap suffix`의 값을 사용합니다. 예를 들면, `ldap user suffix = "ou=People"` 입니다.

표 6-3 전역 매개 변수(계속)

매개 변수	설명
ldap group suffix	그룹 정보를 추가할 디렉토리 트리의 기본 위치를 지정합니다. 이 매개 변수를 지정하지 않으면 HP CIFS Server에서는 ldap suffix의 값을 대신 사용합니다. 예를 들면, ldap group suffix = "ou=Groups"입니다.
ldap filter	RPC 2254를 준수하는 LDAP 검색 필터를 지정합니다. 기본값은 sambaAccount objectclass와 일치하는 모든 항목의 uid 속성과 로그인 이름을 일치시키는 것입니다. 예를 들면, ldap filter = (&(uid=%u)(objectclass=sambaAccount))입니다.
ldap admin dn	사용자 계정 정보를 검색할 때 HP CIFS Server에서 LDAP 디렉토리 서버에 연결하는 데 사용하는 사용자 고유 이름(DN)을 지정합니다. ldap admin dn은 /var/opt/samba/private/secrets.tdb 파일에 저장된 admin dn password와 함께 사용됩니다. 예를 들면, ldap admin dn = "cn = directory manager"입니다.
ldap ssl	SSL(Secure Sockets Layer) 지원을 지정합니다. HP CIFS Server는 ldap ssl = start tls 옵션을 지원하지 않습니다. LDAP에 대해 디렉토리 서버에서 SSL을 사용하는 경우 이 기능을 활성화하려면 **Yes**를 지정하고 SSL을 비활성화하려면 **No**를 지정합니다. 기본적으로 이 매개 변수는 **No**로 설정되어 있습니다.

smbpasswd 프로그램 매개 변수

다음은 smbpasswd 프로그램의 새 매개 변수입니다.

smbpasswd -w ldap admin password 정보를 변경하기 위해 새 매개 변수인 -w가 smbpasswd 프로그램에 추가되었습니다.

LDAP 기능 지원 구성

HP CIFS Server를 설치한 후에는 기존 구성이 현재 구성된 대로 계속 작동합니다. LDAP 지원을 활성화하려면 SWAT 도구 또는 편집기를 사용하여 `/etc/opt/samba/smb.conf` 파일에서 상대적인 LDAP 구성 매개 변수를 구성해야 합니다.

참고

새로 설치하는 고객은 `samba_setup` 프로그램을 실행하여 HP CIFS Server를 설치 및 구성하는 것이 좋습니다.

다음과 같이 `samba_setup` 프로그램을 신속히 실행하여 LDAP 기능을 지원하는 HP CIFS Server를 구성할 수 있습니다.

단계 1. LDAP 기능을 사용하려면 다음 명령을 실행합니다.

```
$ export PATH=$PATH:/opt/samba/bin
$ samba_setup
```

`samba_setup` 프로그램을 실행할 경우 LDAP를 사용할지 묻는 메시지가 표시됩니다. LDAP를 사용하려면 **Yes**를 누르고 LDAP를 비활성화하려면 **No**를 누릅니다.

단계 2. `samba_setup` 프로그램에 응답하여 `/etc/opt/samba/smb.conf` 파일에서 다음 전역 LDAP 매개 변수를 구성합니다.

- `ldap server`
- `ldap suffix`
- `ldap admin dn`
- `ldap ssl`
- `ldap user suffix`
- `ldap group suffix`
- `ldap idmap suffix`
- `ldap machine suffix`

이러한 새 매개 변수에 대한 자세한 내용은 160페이지의 “LDAP 구성 매개 변수”를 참조하십시오.

디렉토리에 Samba 사용자 설치

이 절에서는 LDAP 다렉토리에 Samba 사용자를 설치 및 확인하는 방법을 설명합니다.

자격 증명 추가

LDAP 기능을 지원하는 HP CIFS Server를 사용하는 경우에는 `smbpasswd` 명령이 `/var/opt/samba/private/smbpasswd` 파일보다는 LDAP 디렉토리의 사용자 계정 정보를 조작합니다. LDAP 디렉토리에 Samba 사용자를 설치하기 전에 디렉토리 관리자 자격 증명을 `/var/opt/samba/private/secrets.tdb` 파일에 추가해야 합니다.

Samba 정보용 LDAP 디렉토리를 수정할 수 있는 사용자에 대해 LDAP 자격 증명을 저장하려면 다음 명령을 실행합니다.

```
$ smbpasswd -w <password of the LDAP Directory Manager>
```

예를 들면, 다음 명령은 LDAP 디렉토리 관리자의 자격 증명을 저장합니다.

```
$ smbpasswd -w dmpasswd
```

여기서 `dmpasswd`는 LDAP 디렉토리 관리자의 암호입니다.

참고

암호가 ldap admin 디렉토리 관리자의 암호와 정확히 일치하는지 확인해야 합니다. 이 암호는 사용자 관리용이며 나중에 사용할 수 있도록 저장됩니다. 암호가 틀려도 오류 메시지는 표시되지 않지만 사용자 관리를 수행할 수 없습니다.

Samba 사용자 확인

`ldapsearch` 명령줄 유틸리티를 사용하면 LDAP 디렉토리 항목을 찾아서 가져올 수 있습니다. 이 유틸리티는 지정한 고유 이름(DN)과 암호를 사용하여 지정된 서버와의 연결을 열고 지정한 검색 필터에 기초하여 항목을 검색합니다.

구문

ldapsearch [*option*]

옵션

-b 검색/삽입 기준

-s 검색 범위

-D 디렉토리 로그인

-w 디렉토리 관리자의 암호

예제

다음 예제에서는 ldapsearch 유틸리티를 사용하여 사용자 항목인 johnl에 sambaAccount objectclass가 들어 있는지 확인합니다.

```
$ /opt/ldapux/bin/ldapsearch -b "dc=org,dc=hp, dc=com" -ssub \
-D "cn=Directory Manager" -w dmpasswd "uid=johnl"
```

출력은 다음과 같습니다.

```
dn: uid=johnl,ou=People,dc=org,dc=hp,dc=com
objectclass: top
objectclass: account
objectclass: posixAccount
objectclass: sambaAccount
loginShell: /usr/bin/ksh
uidNumber: 8662
gidNumber: 8200
homeDirectory: /home/johnl
gecos: John Louie, 48S-020, 447-1890
userPassword: {crypt}aOACGvt0T, 1fo
lmPassword: 0AED71B7494489AG2ED50F26D3C5EB07
NTPassword: 7C46DE22B8963EAA3F9F90BE4E0F661
acctFlags: UX
pwdLastSet: 1063301239
```

LDAP 관리 도구

HP CIFS Server에서 Netscape Directory Server에서 사용자, 그룹 및 암호를 관리할 수 있는 LDAP 관리 도구를 제공합니다. Perl 스크립트를 사용하려면 HP-UX 11i(PA-RISC) 및 HP-UX 11i(IA) 버전 5.6.1.E 이상에서 perl이 필요합니다. *http://software.hp.com*에서는 무료 다운로드 소프트웨어를 제공합니다.

HP CIFS Server LDAP 도구

LDAP-UX Integration 제품 도구 외에도, `smbpasswd`, `net` 명령, `pdbedit` 및 CIFS 스크립트를 비롯하여 LDAP 디렉토리의 CIFS 데이터 관리에 많은 HP CIFS Server 관리 도구를 사용할 수 있습니다.

Smbpasswd 도구

HP CIFS passdb 백엔드가 `ldapsam` 또는 `ldapsam_compat`인 경우 `smbpasswd`는 LDAP 디렉토리에서 작업을 수행합니다.

`smbpasswd -a` 명령을 실행하여 해당 posix 사용자에 sambaSamAccount 정보를 추가하기 전에 POSIX 사용자가 LDAP에 있는지 확인해야 합니다.

POSIX 사용자가 LDAP 디렉토리에 없으면 `smbldap-useradd.pl` 스크립트를 실행하여 POSIX 및 Samba 사용자 계정을 LDAP 디렉토리에 추가할 수 있습니다.

구문

도움말 메시지를 보려면 다음 명령을 실행하십시오.

```
$smbpasswd -h
```

root로 실행한 경우:

```
$smbpasswd [options] [username]
```

그렇지 않은 경우:

```
$ smbpasswd [options]
```

네트워크 명령

LDAP 구성에 사용할 수 있는 네트워크 명령에는 몇 가지가 있습니다.

구문

도움말 메시지를 보려면 다음 명령을 실행하십시오.

```
$ net help
```

Pdbedit

Pdbedit는 LDAP 디렉토리를 사용하는 사용자 관리에 사용할 수 있습니다. pdbedit는 smbpasswd에서 ldapsam으로의 이동을 비롯하여 하나의 passdb 백엔드를 다른 백엔드로 마이그레이션하는 작업을 지원합니다.

구문

도움말 메시지를 보려면 다음 명령을 실행하십시오.

```
$ pdbedit -h
```

Smbldap 도구

다음은 Netscape Directory Server에서 사용자 및 그룹 데이터를 관리하는 데 사용할 수 있는 HP CIFS Server smbldap 도구 목록입니다. HP CIFS Server A.01.* 버전의 경우 이 도구는 /opt/samba/LDAP/smbldap-tools 디렉토리에 있습니다. HP CIFS Server A.02.* 버전의 경우 이 도구는 /opt/samba/LDAP3/smbldap-tools 디렉토리에 있습니다.

smbldap-groupadd.pl	새 그룹(objectclass: posixGroup)을 추가합니다.
smbldap-groupdel.pl	그룹(objectclass: posixGroup)을 삭제합니다.
smbldap-groupmod.pl	그룹(objectclass: posixGroup)을 수정합니다.
smbldap-groupshow.pl	그룹(objectclass: posixGroup)을 표시합니다.
smbldap_conf.pm	전역 구성 파일
smbldap-useradd.pl	새 사용자(objectclass: 사용 도구 옵션에 따라 posixAccount, sambaAccont 또는 둘 다)를 추가합니다.
smbldap-userdel.pl	사용자(objectclass: 사용 도구 옵션에 따라 posixAccount, sambaAccount 또는 둘 다)를 삭제합니다.

smbldap-usermod.pl	사용자 데이터(objectclass: 사용 도구 옵션에 따라 posixAccount, sambaAccount 또는 둘 다)를 수정합니다.
smbldap-usershow.pl	사용자 데이터(objectclass: 사용 도구 옵션에 따라 posixAccount, sambaAccont 또는 둘 다)를 표시합니다.
smbldap-passwd.pl	samba 암호, posix 암호 또는 두 암호 모두를 추가하거나 수정합니다.
smbldap-migrate-accounts.pl	사용자 계정을 smbpasswd 파일에서 LDAP 디렉토리로 마이그레이션합니다.
smbldap-migrate-groups.pl	Windows NT 그룹을 LDAP 디렉토리에서 또는 LDAP 디렉토리로 마이그레이션합니다.
smbldap-populate.pl	LDAP 디렉토리에 잘 알려진 RID를 가진 일부 사용자 및 그룹을 추가하거나 그러한 사용자 및 그룹으로 채웁니다.

HP CIFS Server A.02.* 버전의 경우, 이러한 도구를 실행하기 전에 해당 구성 값이 들어 있는 /opt/samba/LDAP3/smbldap-tools/smbldap_conf.pm 구성 파일을 편집해야 합니다. 각 도구의 사용과 관련된 자세한 정보를 보려면 도구 옵션 -?를 사용하면 됩니다. 이러한 도구의 사용 방법에 대한 자세한 내용은 */opt/samba/LDAP3/smbldap-tools/FILES* 및 */opt/samba/LDAP3/smbldap-tools/README*를 참조하십시오. HP CIFS Server A.01.* 버전의 경우, smbldap_conf.pm 파일은 /opt/samba/LDAP/smbldap-tools 디렉토리에 들어 있습니다.

참고

이러한 관리 도구를 실행하려면 HP-UX 11i(PA-RISC) 및 HP-UX 11i(IA) 버전 5.6.1.E 이상에서 perl이 필요합니다. *http://software.hp.com*에서는 무료 다운로드 소프트웨어를 제공합니다.

smbldap_conf.pm

Samba 관리 도구를 실행하기 전에 스크립트 구성 파일인 /opt/samba/LDAP3/smbldap-tools/smbldap_conf.pm을 편집하여 $SID, $masterLDAP, $suffix, $binddn 및 $bindpasswd 로컬 사이트 변수를

LDAP 디렉토리 서버 이름, LDAP 기본 고유 이름(DN), 디렉토리 관리자 이름 및 암호로 설정할 수 있습니다. `startsmb`를 사용하여 실행 중이 아니면 먼저 samba 데몬을 시작합니다. 구성 파일 전체에서 환경 변수를 환경에 적합한 값($SID 포함)으로 설정합니다. 현재의 SID 기본값은 SID="S-1-5-21-3516781642-1962875130-3438800523"입니다. `net rpc getsid` 명령을 실행하여 해당 SID를 가져와야 합니다. 그렇지 않으면, LDAP 디렉토리에 추가하는 모든 계정에 올바르지 않은 SID가 지정되어 계정이 유효하지 않게 됩니다.

OU(조직 단위)가 LDAP 하위 스키마, 특히 세 단위, `usersou`, `groupsou` 및 `computersou`와 일치하는지 확인합니다. 이 세 단위의 값은 다음과 같습니다.

- $usersou = q (People);
- $groupsou = q (Groups);
- $computersou = q (Computers).

LDAP 디렉토리 서버 이름을 `"hostA.org.hp.com"`으로, SID를 `"S-1-5-21-1415721273-4291299877-1153850723"`으로, LDAP 기본 DN을 `"org.hp.com"`으로, 디렉토리 관리자 이름을 `"Directory Manager"`로, 그리고 암호를 `"dmpasswd"`로 설정하는 다음 예제를 살펴보겠습니다.

- $SID="S-1-5-21-1415721273-4291299877-1153850723"
- $masterLDAP="dc=org, dc=hp, dc=com"
- $suffix="org.hp.com"
- $binddn="cn=Directory Manager"
- $bindpasswd="dmpasswd"

참고

`-w` 옵션을 사용하면 LDAP 관리 도구를 실행할 때 LDAP 디렉토리 관리 암호를 지정할 수 있습니다. `-w` 옵션을 사용하지 않는 경우 HP CIFS Server는 `/opt/samba/LDAP3/smbldap-tools/smbldap_conf.pm` 구성 파일에서 `$bindpasswd` 속성의 암호 값을 조회합니다.

smbldap-groupadd.pl 도구

이 도구를 사용하면 posixGourp objectclass라는 새 그룹 항목을 Netscape Directory Server에 추가할 수 있습니다.

구문

smbldap-groupadd.pl [*options*] *groupname*

여기서 ***options***은 다음 중 하나입니다.

-a	자동 그룹 매핑 항목을 추가합니다.
-g	그룹 ID(GID)를 지정합니다.
-w	LDAP 디렉토리 관리자 암호를 지정합니다.
-r	그룹 RID를 지정합니다.
-s	그룹 SID를 지정합니다.
-t	그룹 유형을 지정합니다.
-p	GID 번호를 stdout로 출력합니다.
-?	도움말 메시지를 표시합니다.

groupname

그룹 이름을 지정합니다. 그룹 데이터 정보가 LDAP 디렉토리에 추가됩니다.

예제

다음 명령은 그룹 ID가 "200"인 새 그룹 이름 "group1"을 Netscape Directory Server에 추가합니다.

```
cd /opt/samba/LDAP3/smbldap-tools
./smbldap-groupadd.pl -g 200 group1
```

smbldap-groupdel.pl 도구

이 도구를 사용하면 Netscape Directory Server에서 그룹 항목을 삭제할 수 있습니다. 이 도구는 posixGroup 정보를 삭제합니다.

구문

smbldap-groupdel.pl [*option*] *groupname*

여기서 ***option***은 다음과 같습니다.

-w	LDAP 디렉토리 관리자 암호를 지정합니다.

-? 도움말 메시지를 표시합니다.

groupname

그룹 이름을 지정합니다. 그룹 데이터 항목이 LDAP 디렉토리에서 삭제됩니다.

예제

다음 명령은 Netscape Directory Server에서 그룹 이름 "group1"을 삭제합니다.

```
cd /opt/samba/LDAP3/smbldap-tools
./smbldap-groupdel.pl group1
```

smbldap-groupshow.pl 도구

이 도구를 사용하면 Netscape Directory Server에서 posixGroup 정보를 가진 그룹 항목을 볼 수 있습니다.

구문

smbldap-groupshow.pl [*option*] *groupname*

여기서 ***option***은 다음 중 하나입니다.

-w LDAP 디렉토리 관리자 암호를 지정합니다.

-? 도움말 메시지를 표시합니다.

groupname

그룹 이름을 지정합니다. 디렉토리의 그룹 서비스 데이터가 표시됩니다.

예제

다음 명령은 Netscape Directory Server에서 그룹 이름 "group2"를 표시합니다.

```
cd /opt/samba/LDAP3/smbldap-tools
./smbldap-groupshow.pl group2
```

smbldap-useradd.pl 도구

smblcap-useradd.pl 도구를 사용하면 Netscape Directory Server에 새 사용자를 추가할 수 있습니다. 지정하는 도구 옵션에 따라 posixAccount 및/또는 sambaAccount 정보를 디렉토리에 추가할 수 있습니다.

참고

도구 옵션 -a 또는 -W를 지정하면 posixAccount 정보 외에도 sambaAccount 정보를 LDAP 디렉토리에 추가할 수 있습니다. 도구 옵션 -a 또는 -W를 지정하지 않는 경우에는 posixAccount 정보만 추가할 수 있습니다.

구문

smbldap-useradd.pl [*options*] *username*

여기서 ***options***은 다음 중 하나입니다.

-a	Windows 사용자를 지정합니다. 이 옵션을 사용하면 posixAccont 및 sambaAccount가 LDAP 디렉토리에 추가됩니다. 이 옵션을 사용하지 않으면 사용자의 posixAccount 정보만 추가됩니다.
-W	Windows 워크스테이션을 지정합니다. 이 옵션을 사용하면 posixAccont 및 sambaAccount가 모두 LDAP 디렉토리에 추가됩니다. 이 옵션을 사용하지 않으면 posixAccount 정보만 추가됩니다.
-x	rid 및 primaryGroupID를 10진수 대신에 16진수로 작성합니다.
-u	사용자 ID(UID)를 지정합니다.
-g	그룹 ID(GID)를 지정합니다.
-n	그룹을 만들지 않습니다.
-d	홈 디렉토리를 지정합니다.
-s	셸 정보를 지정합니다.
-m	홈 디렉토리를 만들고 /etc/skel을 복사합니다.
-k	-m 옵션과 함께 사용되는 기초 디렉토리를 만듭니다.
-c	gecos
-w	LDAP 디렉토리 관리자 암호를 지정합니다.
-P	사용자 암호를 추가하는 smbldap-passwd.pl 도구를 호출합니다.
-A	사용자 암호를 변경할 수 있습니다.
-B	사용자 암호를 변경해야 합니다.

-C	\\PDC-SRC\homes와 같은 SMB 홈 공유를 지정합니다.
-D	H와 같은 홈 공유와 관련된 홈 드라이브 문자를 지정합니다.
-E	스크립트 경로(로그인할 때 실행할 DOS 스크립트)를 지정합니다.
-F	프로파일 디렉토리를 지정합니다.
-H	Samba 계정 제어 비트를 지정합니다.
-N	기본 이름을 지정합니다.
-S	성을 지정합니다.
-?	도움말 메시지를 표시합니다.

username

새 사용자 이름을 지정합니다. 사용자 서비스 데이터가 LDAP 디렉토리에 추가됩니다.

참고

사용자 이름과 -a 옵션은 마지막 매개 변수로 지정해야 합니다. -a 옵션 뒤에 지정되는 모든 매개 변수는 smbldap-useradd.pl 도구에서 무시됩니다.

예제

다음 명령은 사용자 ID가 "102"이고 그룹 ID가 "1005"인 "johnl"이라는 새 사용자 이름을 Netscape Directory Server에 추가합니다. "johnl"에 대한 posixAccount와 sambaAccount 정보가 모두 추가됩니다.

```
cd /opt/samba/LDAP3/smbldap-tools
./smbldap-useradd.pl -u 102 -g 1005 -a johnl
```

smbldap-usermod.pl 도구

smblcap-usermod.pl 도구를 사용하면 Netscape Directory Server에서 사용자 항목을 수정할 수 있습니다. 지정하는 도구 옵션에 따라 디렉토리에서 posixAccount 및/또는 sambaAccount 정보를 수정할 수 있습니다.

구문

smbldap-usermod.pl [*options*] *username*

여기서 ***options***은 다음 중 하나입니다.

-u	사용자 ID(UID)를 수정합니다.
-o	고유하지 않은 UID도 사용할 수 있도록 지정합니다.
-g	그룹 ID(GID)를 수정합니다.
-l	로그인 이름을 수정합니다.
-s	셸 정보를 수정합니다.
-c	gecos
-d	홈 디렉토리를 수정합니다.
-a	sambaSamAccount objectclass를 추가합니다.
-w	LDAP 디렉토리 관리자 암호를 지정합니다.
-A	사용자 암호를 변경할 수 있습니다.
-B	사용자 암호를 변경해야 합니다.
-C	\\PDC-SRC\homes와 같은 SMB 홈 공유를 지정합니다.
-D	H와 같은 홈 공유와 관련된 홈 드라이브 문자를 지정합니다.
-E	스크립트 경로(로그인할 때 실행할 DOS 스크립트)를 수정합니다.
-F	프로파일 디렉토리를 수정합니다.
-H	Samba 계정 제어 비트를 수정합니다.
-I	사용자를 비활성화합니다.
-J	사용자를 활성화합니다.
-N	기본 이름을 지정합니다.
-P	smbldap-passwd.pl을 호출하여 종료합니다.
-?	도움말 메시지를 표시합니다.

username

사용자 이름을 지정합니다. LDAP 디렉토리의 사용자 정보가 수정됩니다.

예제

다음 명령은 사용자 ID가 "200"인 사용자 이름 "johnI"을 Netscape Directory Server에서 수정합니다.

```
cd /opt/samba/LDAP3/smbldap-tools
./smbldap-usermod.pl -u 200 johnl
```

smbldap-userdel.pl 도구

smbldap-userdel.pl 도구를 사용하면 Netscape Directory Server에서 사용자 항목을 삭제할 수 있습니다. 이 도구는 LDAP 디렉토리에서 posixAccout와 sambaAccount 정보를 모두 삭제합니다.

구문

smbldap-userdel.pl [*options*] *username*

여기서 ***options***은 다음 중 하나입니다.

-r 홈 디렉토리를 제거합니다.

-w LDAP 디렉토리 관리자 암호를 지정합니다.

-? 도움말 메시지를 표시합니다.

username

사용자 항목의 이름입니다. 사용자 항목 데이터가 LDAP 디렉토리에서 삭제됩니다.

예제

다음 명령은 "michael"이라는 사용자 이름을 Netscape Directory Server에서 삭제합니다.

```
cd /opt/samba/LDAP3/smbldap-tools
./smbldap-userdel.pl michael
```

smbldap-usershow.pl 도구

smbldap-usershow.pl 도구를 사용하면 Netscape Directory Server의 사용자 항목 정보를 표시할 수 있습니다.

구문

smbldap-usershow.pl [*option*] *username*

여기서 ***option***은 다음 중 하나입니다.

-w LDAP 디렉토리 관리자 암호를 지정합니다.

-? 도움말 메시지를 표시합니다.

username

사용자 항목의 이름을 지정합니다.

예제

다음 명령은 Netscape Directory Server의 "johnl" 사용자의 사용자 항목 데이터를 표시합니다.

```
cd /opt/samba/LDAP3/smbldap-tools
./smbldap-usershow.pl johnl
```

smbldap-migrate-accounts.pl 도구

smbldap-migrate-accounts.pl 도구를 사용하면 smbpasswd 파일의 사용자 계정 정보를 Netscape Directory Server로 마이그레이션할 수 있습니다.

이 도구에서는 pwdump 유틸리티를 사용하여 모든 사용자를 Windows 서버에서 PDC로 사용되는 HP CIFS Server로 마이그레이션할 수 있습니다. 자세한 내용은 "Windows 서버에서 PDC로 사용되는 HP CIFS Server로 사용자 마이그레이션"을 참조하십시오.

구문

smbldap-migrate-accounts.pl [*option*]

여기서 ***option***은 다음 중 하나입니다.

-a people만 처리합니다.

-c computers만 처리합니다.

-w LDAP 디렉토리 관리자 암호를 지정합니다.

-A <opts> 사용자에 대해 smbldap-useradd에 축어로 전달된 옵션 문자열

-W <opts> 컴퓨터에 대해 smbldap-useradd에 축어로 전달된 옵션 문자열

-C 항목을 찾을 수 없는 경우 항목을 만들지 않으며 stdout에 기록하지 않습니다.

-U 항목을 찾을 수 없는 경우 항목을 업데이트하지 않으며 stdout에 기록하지 않습니다.

-? 도움말 메시지를 표시합니다.

예제

다음 명령은 smbpasswd 파일의 모든 "people" 계정을 Netscape Directory Server로 마이그레이션합니다.

```
cd /opt/samba/LDAP3/smbldap-tools
./smbldap-migrate-accounts.pl -a
```

Windows 서버에서 PDC로 사용되는 HP CIFS Server로 사용자 마이그레이션

모든 사용자를 Windows 서버에서 PDC로 작동하는 HP CIFS Server로 마이그레이션하려면 다음 단계를 수행합니다.

단계 1. 다음 웹 사이트에서 Windows 서버로 pwdump.exe를 다운로드합니다.

http://de.samba/org/samba/ftp/pwdump/

단계 2. pwdump.exe를 실행하여 모든 사용자 데이터가 포함된 dumpfile 파일을 실행합니다.

```
pwdump.exe > <dumpfile>
```

단계 3. 단계 2에서 만든 dumpfile 파일을 PDC로 사용되는 HP CIFS 서버 시스템으로 전달합니다.

단계 4. HP CIFS 서버 시스템에서 다음 명령을 실행하여 사용자 데이터를 디렉토리 서버로 마이그레이션합니다.

```
cd /opt/samba/LDAP3/smbldap-tools
./smbldap-migrate-accounts.pl <options> < dumpfile
```

smbldap-migrate-groups.pl 도구

smbldap-migrate-groups.pl 도구를 사용하면 Windows NT 그룹 정보를 Netscape Directory Server로 마이그레이션할 수 있습니다.

구문

```
smbldap-migrate-groups.pl [option]
```

여기서 ***option***은 다음 중 하나입니다.

-C 그룹이 없는 경우 그룹을 만들지 않습니다.

-U 그룹이 있는 경우 그룹을 업데이트하지 않습니다.

-r 그룹을 재귀적으로 처리합니다.

-w LDAP 디렉토리 관리자 암호를 지정합니다.

Windows 서버에서 PDC로 작동하는 HP CIFS Server로 그룹 마이그레이션

Windows 서버에서 PDC로 작동하는 HP CIFS Server로 모든 그룹을 마이그레이션 하려면 다음 단계를 수행합니다.

단계 **1.** Windows 서버에서 `net group` 명령을 실행하여 그룹 데이터가 포함된 파일을 만듭니다.

```
net group <groupname> > <groupdump>
```

단계 **2.** 단계 1에서 만든 `groupdump` 파일을 PDC로 사용되는 HP CIFS 서버 시스템으로 전달합니다.

단계 **3.** HP CIFS 서버 시스템에서 다음 명령을 실행하여 그룹 데이터를 디렉토리 서버로 마이그레이션합니다.

```
cd /opt/samba/LDAP3/smbldap-tools
./smbldap-migrate-groups.pl < groupdump
```

smbldap-passwd.pl 도구

`smbldap-passwd.pl` 도구를 사용하면 사용자의 samba 암호와 posix 암호를 모두 Netscape Directory Server에 추가하거나 수정할 수 있습니다.

구문

```
smbldap-passwd.pl [option] username
```

여기서 ***option***은 다음 중 하나입니다.

-w LDAP 디렉토리 관리자 암호를 지정합니다.

-? 도움말 메시지를 표시합니다.

username

사용자 이름 항목을 지정합니다. 사용자 암호가 LDAP 디렉토리에 추가되거나 수정됩니다.

예제

다음 명령은 "`johnl`"이라는 사용자 이름의 samba 암호와 posix 암호를 Netscape Directory Server에 추가하거나 수정합니다.

```
cd /opt/samba/LDAP3/smbldap-tools
./smbldap-passwd.pl johnl
```

LDAP를 HP CIFS Server A.01.*에서 A.02.*로 업그레이드

기존 HP CIFS Server 버전 A.01.* LDAP 구성을 버전 A.02.*로 업그레이드하는 경우 `smb.conf` 구성 파일을 다음과 같이 변경합니다.

- `smb.conf`에서 `passwd backend = ldapsam_compat://ldaps:< ldap server name>`, `ldap ssl = yes` 및 `ldap port = 636`을 설정하여 SSL을 활성화합니다.
- 선택적으로 더 이상 사용되지 않는 매개 변수 `ldap enable`을 제거할 수도 있습니다.
- 선택적으로 기본 `ldap suffix`에서 people과 group을 제거하고 people을 `ldap user suffix`에 추가하며 group을 `ldap group suffix`에 추가할 수도 있습니다. 예를 들어, `ldap suffix = "ou=People,dc=org,dc=hp,dc=com"`은 `ldap suffix = "dc=org,dc=hp,dc=com"` 및 `ldap user suffix = "ou=People"`이 됩니다.

LDIF 파일 업데이트를 비롯하여 A.01 스타일의 LDAP를 A.02 스타일 LDAP로 변환하려면 다음 단계를 수행하십시오.

단계 **1.** `ftp` 명령을 실행하여 HP CIFS Server에서 `/opt/samba/LDAP/98samba.ldif` 파일을 가져와서 Netscape Directory Server에 저장합니다.

예를 들어, 다음 명령은 HP CIFS Server의 `/opt/samba/LDAP/98samba.ldif` 파일을 Netscape Directory Server(hostA.hp.com)의 `/var/opt/netscape/servers/sldapd-hostA.hp.com/config/schema/98samba.ldif` 파일로 복사합니다.

```
cd /opt/samba/LDAP
ftp hostA.org.hp.com
user root
rootpasswd
cd /var/opt/netscape/servers/sldapd-hostA.hp.com/config/schema
bin
put 98samba.ldif
quit
```

단계 **2.** 다음 `ldapsearch` 명령을 사용하여 Netscape Directory Server에서 하위 스키마가 `sambaAccount`인 스키마를 검색하여 출력을 LDIF 파일에 저장합니다.

```
$ /opt/ldapux/bin/ldapsearch -h <NDS Server name> -p 389 -l \
-b <whole cdn> -s sub "objectClass= sanbaAccount" > \ output file
```

예를 들어, 다음 명령은 하위 스키마가 sambaAccount인 Netscape Directory Server(hostA.org.hp.com)의 스키마를 찾아서 출력을 /tmp/old.ldif 파일에 저장합니다.

```
$ /opt/ldapux/bin/ldapsearch -h hostA.org.hp.com -p 389 -l \
-b <whole cdn> -s sub "objectClass= sanbaAccount" > \ /tmp/old.ldif
```

단계 **3.** net 명령을 실행하여 Netscape Directory Server의 도메인 SID를 가져옵니다.

```
$ /opt/samba/bin/net getlocalsid [<NDS Server>]
```

예를 들어, 다음 명령은 Netscape Directory Server(hostA.org.hp.com)의 도메인 SID를 가져옵니다.

```
$ /opt/samba/bin/net getlocalsid hostA.org.hp.com
```

단계 **4.** convertSambaAccount 스크립트를 실행하여 기존 Samba 하위 스키마를 Samba 3.0에서 지원하는 업데이트된 하위 스키마로 변환합니다.

```
$ cd /opt/samba/LDAP3
```

```
$ ./convertSambaAccount --sid <sid from step3> --input file
<ldif file from step2> --output file
```

예를 들어, 다음 명령은 hostA.org.hp.com에 대해 도메인 SID가 210인 경우 기존 ldif 파일인 /tmp/old.ldif를 업데이트된 samba3.0 ldif 파일인 new.ldif로 변환합니다.

```
$ ./convertSambaAccount --210 --/tmp/old.ldif --/tmp/new.ldif
```

단계 **5.** ldifdiff 스크립트를 실행하여 두 LDIF 파일의 차이를 비교하고 출력을 LDIF 파일에 저장합니다.

예를 들면, 다음 명령은 /tmp/old.ldif와 /tmp/new.ldif의 차이를 비교한 후 출력을 /tmp/mod.ldif 파일에 저장합니다.

```
$ ./opt/ldapux/bin/ldifdiff /tmp/old.ldif /tmp/new.ldif > \
/tmp/mod.ldif
```

단계 **6.** ldapmodify 스크립트를 실행하여 디렉토리 서버에 있는 기존 sambaAccount 하위 스키마를 단계 5에서 가져온 업데이트된 sambaSamAccount 하위 스키마로 수정합니다.

```
$ /opt/ldapux/bin/ldapmodify -c -h hostA.org.hp.com -D
"cn=Directory Manager" -w <password> -f /tmp/mod.ldif
```

단계 **7.** `ldap filter` smb.conf 매개 변수를 `ldap filter= (uid=%u)`로 변경합니다. `(uid=%u)`가 기본값이므로 `ldap filter` 항목은 제거할 수 있습니다.

단계 **8.** `passdb backend` smb.conf 매개 변수를 `passdb backend = ldapsam:ldap://<fully qualified name of NDS Server>` 또는 SSL 사용 가능 LDAP의 경우 `passdb backend = ldapsam:ldaps://<fully qualified name of NDS Server>`로 변경합니다.

LDAP 기능 지원에 대한 제한 사항

HP에서는 HP LDAP-UX Integration 제품 J4269AA와 HP Netscape Directory Server J4258CA에서 작동하는 LDAP 통합 가능 HP CIFS Server만 지원합니다.

7 Winbind 지원

이 장에서는 winbind를 지원하는 HP CIFS Server를 설정 및 구성하는 방법을 설명합니다. 이 장의 구성은 다음과 같습니다.

- 187페이지의 “Winbind를 지원하는 HP CIFS Server 구성”
- 191페이지의 “Winbind 시작 및 중지”
- 193페이지의 “Winbind의 idmap_rid 지원”
- 195페이지의 “wbinfo 유틸리티”

개요

UNIX 및 Microsoft Windows NT/ADS는 사용자 및 그룹 정보를 나타내는 모델이 서로 다르며 이러한 모델을 구현하는 데 있어서 서로 다른 기술을 사용합니다. Winbind는 Windows 사용자 및 그룹을 HP-UX UID 및 GID로 확인하는 Samba 프로그램 제품군의 구성 요소입니다. Winbind는 UNIX 구현 및 NSS(Name Services Switch)를 사용하여 Windows NT 도메인 사용자가 HP-UX 시스템에서 UNIX 사용자로 표시되고 작동할 수 있게 합니다. Winbind는 tdb 파일 또는 LDAP 디렉토리에 ID 매핑 데이터베이스를 저장합니다.

Winbind는 다음 두 가지 기능을 제공합니다.

- NSS(Name Service Switch)를 통한 ID 확인

  NSS(Name Service Switch)는 호스트 이름, 사용자 이름 및 그룹 이름과 같은 시스템 정보를 다양한 소스에서 확인할 수 있도록 하는 기능입니다.

  NSS 응용 프로그래밍 인터페이스를 사용하면 HP-UX 사용자 이름 및 그룹을 확인할 때 winbind가 시스템 정보 소스로 제공될 수 있습니다. Winbind는 NSS 인터페이스를 사용하여 winbind를 실행하는 HP-UX 시스템에서 사용자 및 그룹을 열거하고 Windows 도메인의 모든 사용자 및 그룹을 표시합니다.

  Winbind는 라이브러리 루틴 /etc/lib/libnss_winbind.1을 제공하는데, 이 루틴은 winbind 데몬에 연결하여 ID 매핑을 확인합니다.

- 사용자 및 그룹 ID 할당

  Winbind는 HP-UX UID/GID 및 Windows SID(보안 ID) 간에 데이터 매핑을 저장하는 winbind_idmap.tdb라고 하는 데이터베이스를 유지 관리합니다. 이 루틴은 Windows SID로 매핑된 idmap uid/gid 범위에서 할당된 UID 및 GID를 저장합니다. idmap 백엔드를 ldapsam:ldap://<ldap server name>으로 지정한 경우 winbind는 로컬 매핑 파일을 사용하는 대신에 LDAP 디렉토리 서버에서 이 정보를 가져옵니다.

winbind에 대한 자세한 내용은 다음 웹 사이트에 있는 *Samba 3.0 HOWTO Reference Guide*의 23장 "Winbind:Use of Domain Accounts"를 참조하십시오.

http://us3.samba.org/samba/docs/man/Samba-HOWTO-Collection/

Winbind 작동 방법

Winbind는 Windows 도메인 컨트롤러와 통신하는 winbind 데몬(/opt/samba/bin/winbindd), NSS(Name Service Switch)에서 제공하는 이름 서비스 및 smb.conf 파일의 구성 옵션을 사용하여 작동합니다. Winbind를 지원하는 경우 NSS 구성 파일인 /etc/nsswitch.conf를 설정하여 HP-UX 시스템에서 Windows 도메인에만 존재하는 사용자 및 그룹에 대한 UID 및 GID 매핑을 조회할 수 있도록 해야 합니다.

사용자가 CIFS Server 공유에 연결하는 경우 사용자의 Windows SID(보안 ID)는 smb.conf 파일 안에 지정된 범위 내 UID 및 GID 세트로 매핑됩니다. 사용자가 공유에서 파일을 만들거나 수정하는 경우 이 매핑된 UID 및 GID 쌍은 파일의 소유자 및 그룹 소유자로 기록됩니다.

UNIX 프로세스에서 이러한 UID 및 GID 쌍을 사용자 이름을 변환해야 하는 경우에는 표준 C 라이브러리 함수 getpwname() 및 getgrnam()을 호출하여 UID 및 GID 쌍과 관련된 사용자 이름을 검색합니다. 한편, 이러한 루틴은 /etc/nsswitch.conf 파일의 항목을 사용하여 정보를 가져올 때 사용할 이름 서비스 백엔드를 결정합니다. Winbind 항목이 /etc/nsswitch.conf 파일에 지정된 경우에는 UID 및 GID를 Windows SID로 변환하고 나서 암호 서버에서 이 SID와 관련된 사용자 이름을 조회하기 위해 winbind 데몬인 winbindd와 연결되는 /usr/lib/libnss_winbind.1 루틴이 호출됩니다.

Windows SID를 UNIX UID 및 GID에 매핑하는 다른 방법은 idmap_rid 기능을 사용하는 것입니다. winbind의 idmap_rid 기능은 LDAP 없이도 도메인 전체에 로컬 UNIX UID 및 GID에 고유한 Windows SID 매핑을 제공합니다. Windows NT 또는 Windows 2000/2003 ADS 도메인에서 idmap_rid를 사용할 수 있습니다. 자세한 내용은 193페이지의 “Winbind의 idmap_rid 지원”을 참조하십시오.

Winbind를 지원하는 HP CIFS Server 구성

Winbind 기능을 지원하도록 HP CIFS Server를 설정 및 구성해야 합니다.

Winbind 구성 매개 변수

표 7-1은 winbind의 작동을 제어하는 데 사용되는 새로운 전역 매개 변수의 목록입니다. 이 매개 변수는 /etc/opt/samba/smb.conf 파일의 [global] 섹션 안에 설정됩니다.

표 7-1 전역 매개 변수

매개 변수	설명
winbind separator	이 구분 기호를 지정하여 도메인 이름과 사용자 이름을 구분합니다. 예제: winbind separator = \
idmap uid	도메인 사용자의 UID 범위를 지정합니다.
idmap gid	도메인 그룹의 GID 범위를 지정합니다.
winbind enum users	winbind 사용자의 열거를 허용하려면 **Yes**로 지정하고 winbind 사용자의 열거를 허용하지 않으려면 **No**로 지정합니다. 기본적으로 이 매개 변수는 **No**로 설정되어 있습니다.
winbind enum groups	winbind 그룹의 열거를 허용하려면 **Yes**로 지정하고 winbind 그룹의 열거를 허용하지 않으려면 **No**로 지정합니다. 기본적으로 이 매개 변수는 **Yes**로 설정되어 있습니다.
idmap backend	LDAP 백엔드를 지정하여 로컬 idmap tdb 파일 대신에 공통 LDAP 백엔드에 대한 SID의 UID/GID 매핑을 유지합니다. 이렇게 하면 모든 UID 및 GID가 도메인에서 고유할 수 있습니다. 예제: idmap backend = ldap://ldapserverA.hp.com

표 7-1 **전역 매개 변수(계속)**

매개 변수	설명
`winbind cache time`	Windows NT 서버에 다시 조회하기 전에 `winbindd` 데몬에서 사용자 및 그룹 정보를 캐시하는 시간(초)을 지정합니다. 기본적으로 이 매개 변수는 300으로 설정되어 있습니다.
`winbind enable local accounts`	`winbindd`를 smb.conf의 다양한 계정 관리 후크(예제: 'add user script') 교체 시 표준으로 사용할지 여부를 제어합니다. 사용하는 경우에는 `winbindd`에서 `getpwnam()` 또는 `getgrgid()` 등을 통해 사용 가능한 UNIX 계정 정보의 또 다른 소스로서 로컬 사용자 및 그룹을 생성할 수 있도록 지원합니다. 이 매개 변수는 기본적으로 **No**로 설정되어 있습니다.
`winbind use default domain`	사용자 이름에서 도메인 구성 요소를 사용하지 않고 사용자에 대해 `winbindd` 데몬이 작동하는지 여부를 지정합니다. 도메인 구성 요소가 없는 사용자는 `winbindd` 서버의 고유 도메인의 일부로 처리됩니다. 기본적으로 이 매개 변수는 **No**로 설정되어 있습니다.
`template homedir`	`winbind` 사용자 홈 디렉토리를 지정합니다. 예제: `template homedir = /home/%U`.
`template primary group`	winbindd의 로컬 계정 관리 기능에서 만든 각 사용자에 대한 주 그룹의 기본값을 정의합니다. 기본적으로 이 매개 변수는 **nobody**로 설정되어 있습니다.

smb.conf 예제

다음은 `smb.conf` 파일의 예제입니다.

```
[global]
workgroup = DomainA  # Doamin name
security = domain or ADS

# Winbindd section
winbind separator = \
idmap_backend = ldap:ldap://ldaphost1.company.com
idmap uid = 10000-20000
```

```
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
winbind cache time = 10
winbind enable local accounts = no
winbind use default domain = no
ldap idmap suffix = ou=testdir, dc=depart, dc=company, dc=com

[shareA]
path = /tmp/shareA
guest ok = no
writable = yes
```

Idmap 백엔드

여러 CIFS Server가 Windows NT 또는 Windows ADS 도메인에 참여하고 `winbind`를 사용하는 경우 LDAP 디렉토리에 ID 맵을 저장하도록 여러 CIFS Server를 구성할 수 있습니다. LDAP 서버를 사용하고 `smb.conf`의 `idmap backend` 매개 변수로 CIFS Server를 구성하면 모든 UID 및 GID가 도메인에서 고유할 수 있습니다. 이는 NFS 공유에 대한 Windows 액세스를 지원하는 데 있어서 중요합니다.

다음은 `ldaphostA.hp.com` 컴퓨터가 idmap 백엔드로 지정되어 있는 `/etc/smb.conf` 파일의 예제입니다.

```
idmap uid = 10000-20000
idmap gid = 10000-20000
idmap backend = ldap:ldap://ldaphostA.company.com
ldap idmap suffix = ou=test, dc=depart, dc=company, dc=com
```

NSS(Name Service Switch) 구성

`winbind` 지원을 사용하려면 사용자 또는 그룹 이름 조회용 이름 서비스로 `winbind`를 사용하도록 NSS 제어 파일인 `/etc/nsswitch.conf`를 구성해야 합니다.

예를 들면, `/etc/nsswitch.conf` 파일을 다음과 같이 설정할 수 있습니다.

```
passwd:     files winbind
group:      files winbind
protocols:  files
hosts:       dns files [NOTFOUND=return] wins
```

이 예제에서 NSS는 먼저 /etc/passwd 및 /etc/group 파일을 확인하고 항목이 발견되지 않으면 winbind를 확인합니다.

NSS 구성 방법에 대한 자세한 내용은 *http://docs.hp.com/hpux/netcom/*에 있는 *NFS Services Administrator's Guide*의 "Configuring the Name Service Switch"와 switch(4)를 참조하십시오.

Winbind 사용자의 파일 소유권 예제

다음 예제에서는 /opt/samba/bin/smbclient를 사용하여 도메인 DomA에서 사용자 John으로 HP CIFS Server Server1에 있는 공유 shareA에 연결합니다.

```
$ cd /opt/samba/bin
$ ./smbclient //Server1/shareA -U DomA\\John
```

출력은 다음과 같습니다.

```
Domain=[DomainA] OS=[Unix] Server=[Samba 3.0.7 based HP CIFS \
Server A.02.01]
```

```
$ smb:\>put JohnTest
$ smb:\>quit
```

ll 명령을 사용하여 다음과 같이 /tmp/shareA/JohnTest 파일의 소유권을 표시합니다.

```
$ ll /tmp/shareA/JohnTest
```

ll 명령을 실행할 경우 출력은 다음과 같습니다.

```
-rwxr--r--  1 DomA\John DomA\GroA 290 Nov 0 12:05 \
tmp/shareA/JohnTest
```

위의 출력에서 파일 소유자는 DomA\John이며 그룹 소유자는 DomA\GroA입니다. 소유자 및 그룹 소유자의 첫 번째 부분인 DomA는 도메인 이름이며 \는 winbind 구분 기호입니다. 마지막 부분인 John과 GroA는 Windows 도메인의 실제 사용자 이름과 그룹 이름입니다.

다음과 같이 ll -n명령을 사용하여 파일 소유권의 UID 및 GID를 표시합니다.

```
$ ll -n /tmp/shareA/JohnTest
```

-rwxr--r-- 1 10002 10005 290 Nov 0 12:05 tmp/shareA/JohnTest

ll -n 명령을 실행하면 UID(10002)와 GID(10005)가 출력에 표시됩니다. UID와 GID 모두 winbind에서 사용하기 위해 smb.conf 파일에 지정한 값 범위 안에 속합니다.

Winbind 시작 및 중지

이 절에서는 winbind를 지원하는 HP CIFS Server를 시작하거나 중지하는 방법을 설명합니다.

Winbind 시작

다음과 같이 startsmb -winbind 또는 startsmb -w 명령을 사용하여 HP CIFS Server에서 winbind 데몬을 시작합니다.

```
$ startsmb -winbind
```

또는

```
$ startsmb -w
```

Winbind 중지

다음과 같이 stopsmb -winbind 또는 stopsmb -w 명령을 사용하여 HP CIFS Server에서 winbind 데몬을 중지합니다.

```
$ stopsmb -winbind
```

또는

```
$ stopsmb -w
```

참고

winbind 데몬만 시작 또는 중지하려면 startwinbind 및 stopwinbind 스크립트를 사용합니다. 예를 들면, 다음 명령을 사용하여 winbind 데몬만 시작합니다.

```
$ startwinbind
```

시스템 시작 시 Winbind 자동 시작

/etc/rc.config.d/samba에서 RUN_WINBIND 매개 변수를 지정하여 시스템을 시작할 때 winbind 데몬인 winbindd를 시작할 것인지 여부를 지정할 수 있습니다.

시스템을 시작할 때 winbind를 자동으로 시작하도록 구성하려면 RUN_WINBIND를 1로 설정합니다.

Winbind의 idmap_rid 지원

winbind에서 idmap_rid 기능을 사용하면 Windows SID를 로컬 UNIX UID 및 GID에 고유하게 매핑할 수 있습니다. idmap_rid 기능에서는 사용자 SID의 RID를 사용하여 구성 가능한 기본 값에 RID 번호를 추가하는 방식으로 UID 및 GID를 생성합니다. RID는 중앙에서 관리하는 Windows 도메인 컨트롤러에 의해 할당되기 때문에 이 도구를 사용하면 CIFS winbind 데몬으로 도메인 전체에서 고유한 HP-UX UID 및 GID를 생성할 수 있습니다. 이 기능은 LDAP 디렉토리가 없는 여러 CIFS 서버에서 매핑 동기화에 사용할 수 있습니다. Windows NT 도메인 또는 Windows 2000/2003 ADS 도메인에서는 idmap_rid를 사용할 수 있지만, Windows 트러스트된 도메인에서는 사용할 수 없습니다.

idmap_rid 사용 제한 사항

- idmap_rid 기능은 단일 Windows 도메인에서만 사용됩니다. Windows 트러스트된 도메인에서는 사용할 수 없습니다. idmap_rid를 사용하려면 smb.conf 파일의 allow trusted domains 매개 변수를 No로 설정해야 합니다.
- smb.conf 파일에서 idmap_rid 범위를 idmap uid 및 idmap gid 범위 모두와 같게 설정해야 합니다.
- idmap backend 매개 변수를 idmap_rid로 설정하면 UID 및 GID 매핑 데이터가 로컬로만 저장됩니다.

idmap_rid 설정 및 사용

idmap_rid를 사용하려면 smb.conf 파일에서 idmap backend를 idmap_rid로 설정하고 allow trusted domains를 No로 설정해야 합니다.

다음은 idmap_rid를 사용하는 smb.conf 파일의 예제입니다.

```
[global]
workgroup = DomainA  # Doamin name
security = domain or ADS

# Winbindd section
idmap uid = 50000-60000
idmap gid = 50000-60000
idmap backend = idmap_rid:DomainA=50000-60000
```

```
allow trusted domain= no
winbind cache time = 10
winbind enum users = yes
winbind enum groups = yes
winbind enable local accounts = no
winbind use default domain = no
winbind separator = \
```

idmap_rid 확인

wbinfo -u 및 wbinfo -g 명령을 사용하여 idmap_rid 등록 정보가 설정 및 구성되어 있으며 idmap_rid가 실행 중인지 확인할 수 있습니다.

$ wbinfo -u

다음은 wbinfo -u 명령을 사용한 경우의 출력 예제입니다.

```
DOMAIN_DOM\user1 50004
DOMAIN_DOM\user2 50005
DOMAIN_DOM\user3 50006
DOMAIN_DOM\user4 50007
DOMAIN_DOM\Guest 50008
DOMAIN_DOM\user5 50009
DOMAIN_DOM\ntuser 50010
DOMAIN_DOM\root 50011
DOMAIN_DOM\pcuser 50012
DOMAIN_DOM\winusr 50016
```

$ wbinfo -g

다음은 wbinfo -g 명령을 사용한 경우의 출력 예제입니다.

```
DOMAIN_DOM\Domain Admins 50010
DOMAIN_DOM\Domain Guests 50011
DOMAIN_DOM\Domain Users 50012
DOMAIN_DOM\Domain Computers 50013
DOMAIN_DOM\Domain Controllers 50014
DOMAIN_DOM\Schema Admins 50015
DOMAIN_DOM\Enterprise Admins 50016
DOMAIN_DOM\Cert Publishers 50017
DOMAIN_DOM\Account Operators 50018
DOMAIN_DOM\Group Policy Creator Owners 50020
```

wbinfo 유틸리티

wbinfo 도구를 사용하여 winbind 데몬으로부터 정보를 가져올 수 있습니다. wbinfo를 실행하려면 winbind 데몬인 winbindd를 구성 및 시작해야 합니다.

구문

wbinfo [*option*]

여기서 ***option***은 다음 중 하나입니다.

-l HP-UX 이름 제한 8자를 초과하는 Windows 사용자 및 그룹 이름이 있는 경로 데이터를 표시합니다.

-L HP-UX 이름 제한 8자를 초과하는 Windows 사용자 및 그룹 이름에 정규화된 Windows 도메인 이름이 추가된 경로 데이터를 표시합니다.

-u UID를 사용자 이름과 함께 표시합니다.

-g GID를 그룹 이름과 함께 표시합니다.

-N NetBIOS 이름을 IP 주소로 변환합니다.

-I IP 주소를 NetBIOS 이름으로 변환합니다.

-n 이름을 Windows SID로 변환합니다.

-s Windows SID를 이름으로 변환합니다.

-U 사용자 ID(UID)를 Windows SID로 변환합니다.

-G 그룹 ID(GID)를 Windows SID로 변환합니다.

-S Windows SID를 사용자 ID(UID)로 변환합니다.

-Y Windows SID를 그룹 ID(GID)로 변환합니다.

-A idmap에서 새 RID를 가져옵니다.

-c 로컬 사용자 계정을 만듭니다.

-x 로컬 사용자 계정을 삭제합니다.

-C 로컬 그룹을 만듭니다.

-X 로컬 그룹을 삭제합니다.

-o 사용자를 그룹에 추가합니다.

-O 사용자를 그룹에서 제거합니다.

-D 도메인에 대한 정보를 표시합니다.

-r 사용자 그룹을 가져옵니다.

-V winbind 버전을 표시합니다.

-? 도움말 메시지를 표시합니다.

이 도구를 사용하는 방법에 대한 자세한 내용은 `/opt/samba/man/man1/wbinfo.1` 파일을 참조하십시오.

예제

다음은 `wbinfo -l` 명령을 사용한 경우의 출력 예제입니다.

```
$ wbinfo -l /tmp
```

```
drwxr-xr-x   2  user1  Domain Users      96 Jun 23 16:52 Folder1
drwxr-xr-x   2  user2  Domain Users      96 Jun 23 16:52 Folder2
```

다음은 `wbinfo -L` 명령을 사용한 경우의 출력 예제입니다.

```
$ wbinfo -L /tmp
```

```
drwxr-xr-x   2  DOMAIN_DOM\user1  DOMAIN_DOM\Domain Users
96 Jun 23 16:52 Folder1
drwxr-xr-x   2  DOMAIN_DOM\user2  DOMAIN_DOM\Domain Users
96 Jun 23 16:52 Folder2
```

다음은 `wbinfo -u` 명령을 사용한 경우의 출력 예제입니다.

```
$ wbinfo -u
```

```
DOMAIN_DOM\johnb 10003
DOMAIN_DOM\user1 10004
DOMAIN_DOM\user2 10005
DOMAIN_DOM\user3 10006
DOMAIN_DOM\user4 10007
DOMAIN_DOM\Guest 10008
DOMAIN_DOM\user5 10009
DOMAIN_DOM\ntuser 10010
DOMAIN_DOM\root 10011
DOMAIN_DOM\pcuser 10012
```

```
DOMAIN_DOM\winusr 10016
DOMAIN_DOM\maryw 10017
```

다음은 wbinfo -g 명령을 사용한 경우의 출력 예제입니다.

```
$ wbinfo -g
DOMAIN_DOM\Domain Admins 10010
DOMAIN_DOM\Domain Guests 10011
DOMAIN_DOM\Domain Users 10012
DOMAIN_DOM\Domain Computers 10013
DOMAIN_DOM\Domain Controllers 10014
DOMAIN_DOM\Schema Admins 10015
DOMAIN_DOM\Enterprise Admins 10016
DOMAIN_DOM\Cert Publishers 10017
DOMAIN_DOM\Account Operators 10018
DOMAIN_DOM\Print Operators 10000
DOMAIN_DOM\Group Policy Creator Owners 10020
```

8 HP CIFS Server A.01에서 A.02로 업데이트

HP CIFS Server A.02.*에서는 A.01.* 기능을 지원하며 대부분의 경우 업데이트할 구성 변경 내용이 없거나 최소한으로 변경하면 됩니다. 그러나, Samba 2.2가 기반이 되

는 HP CIFS Server A.01.* 버전과 Samba 3.0이 기반이 되는 HP CIFS Server A.02.* 버전 간에는 많은 차이점이 있습니다. HP CIFS Server versions A.02.*는 광범위한 네트워크 관리 작업을 단순화하기 위해 배포할 수 있는 여러 추가 기능을 제공합니다. 이 장에서는 이러한 차이를 설명하고 사용자가 CIFS 사용 가능 네트워크를 계획하고 업그레이드할 수 있도록 업데이트 절차에 대해 설명합니다.

설명서

HP CIFS Server A.02.* 버전은 다음 문서를 제공합니다. 이 문서는 A.01.* 버전에는 포함되어 있지 않습니다.

- Samba 관련 서적, *The Official Samba HOWTO and Reference Guide*
- Samba 관련 서적, *Samba 3 by Example*
- 구성 매개 변수, 유틸리티 및 도구에 대한 업데이트된 도움말 텍스트
- **HP CIFS Server 관리자 설명서** A.02.* 기능으로 업데이트 및 A.01.*과의 차이점

HP CIFS Server 제품 B8725AA와 함께 제공되는 Samba 관련 서적은 SWAT(Samba Web Administration Tool) 홈 페이지를 통해 또는 `/opt/samba/docs/Samba-HOWTO-Collection.pdf` 및 `/opt/samba/swat/help`에서 액세스할 수도 있습니다. 업데이트를 수행하기 전에 이러한 서적의 내용에 충분히 익숙해져야 합니다. 이러한 서적은 Samba 기능 설명, 배포 전략 및 구성 도움말을 제공하는 훌륭한 정보 자료입니다. 이러한 서적을 HP CIFS Server에 대한 기본 참고서로 사용할 수 있지만, 이 설명서(**HP CIFS Server 관리자 설명서**)에서 설명하는 HP-UX와 HP CIFS Server의 차이를 알고 있어야 합니다.

HP CIFS Server A.02.*의 추가된 기능

HP CIFS Server 버전 A.02.01부터는 Samba 3.0을 기반으로 한 여러 새로운 기능을 사용할 수 있습니다. 다음은 이러한 새로운 기능에 대해 설명합니다.

- Active Directory Server 지원

  HP CIFS Server는 ADS 영역을 구성원 서버로 참여시키고 Kerberos 보안과 LDAP를 사용하여 사용자를 인증할 수 있습니다. Windows 200x 도메인을 참여시키기 전에 5장, 123페이지의 “Windows 2000/2003 도메인”을 참조하십시오.

- 새 인증 시스템

  `smbpasswd` 및 LDAP 인증 백엔드에 대한 지속적인 지원과 함께 HP CIFS Server에서는 새로운 계정 저장 장치 데이터베이스인 `ldapsam`과 `tdbsam`을 지원합니다. 이 기능은 가장 중요한 새로운 기능 중 하나이므로 업데이트하기 전에 새 인증 시스템의 사용에 대해 알아야 합니다. `passdb backend` 매개 변수를 구성하는 방법은 앞에서 설명한 참고 서적과 SWAT 도움말 텍스트를 참조하거나 `man smb.conf` 명령을 실행하십시오. A.01.* 버전을 A.02.* HP CIFS Server 버전으로 업데이트하기 전에 이 장 뒷부분에 나오는 209페이지의 “HP CIFS Server A.01.*를 A.02.*로 업데이트”를 참조하십시오.

- Winbind

  Winbind는 UNIX 사용자 및 그룹(UID 및 GID)을 Windows 사용자 및 그룹에 동적으로 할당하여 Windows 기반 도메인 통합을 지원할 수 있습니다.

- 보다 많아진 계정 관리 도구

  `pdbedit`, `net` 명령, `smbldap` 도구 및 `smbpasswd`와 같은 유틸리티를 사용하여 사용자 계정 정보를 관리할 수 있습니다. `net` 명령은 새롭고 다양한 유틸리티 작업을 제공하고 기존의 다른 작업을 변경합니다.

그 밖의 많은 새로운 기능에 대한 자세한 내용은 `/opt/samba/SAMBA_WHATSNEW.txt`를 참조하십시오.

smb.conf의 매개 변수 변경 사항

표 10-1은 HP CIFS Server A.02.01용 `smb.conf` 파일에서 새로 추가된 매개 변수와 제거된 매개 변수의 목록을 제공합니다.

표 8-1 **smb.conf의 매개 변수 변경 사항**

새로 추가된 매개 변수	제거된 매개 변수
원격 관리 - abort shutdown script - shutdown script 사용자 및 그룹 계정 관리 - add group script - add machine script - add user to group script - algorithmic rid base - delete group script - delete user from group script - passbd backend - set primary group script - passwd chat time out 인증 - auth methods - realm 프로토콜 옵션 - client lanman auth - client NTLMv2 auth - client schannel - client signing - client use spnego - disable netbios - ntlm auth - paranoid server security - server schannel - server signing - smb ports - use spnego 파일 서비스 - get quote command - hide special files - hide unwriteable files - hostname lookups - kernel change notify - mangle prefix - map acl inherit - msdfs proxy - set quota command - use sendfile - vfs objects	- admin log - alternate permissions - character set - client codepage - code page directory - coding system - domain admin group - domain guest group - force unknown acl user - nt smb support - post script - printer driver - printer driver file - print driver location - status - strip dot - total print jobs - use rhosts - valid chars - vfs option - read size(사용 되지 않음) - source environment(사용 되지 않음) - mangled stack - hide local users - groupname map 사용 되지 않음 - only user - mangled map

표 8-1 smb.conf의 매개 변수 변경 사항(계속)

새로 추가된 매개 변수	제거된 매개 변수
인쇄 - cups options - max reported print jobs UNICODE 및 문자 집합 - display charset - unix charset SID를 uid/gid에 매핑 - idmap backend - idmap gid - idmpa uid - winbind enable local accounts - winbind trusted domains only - template primary group - enable rid algorithm LDAP - ldap delete dn - ldap user suffix - ldap group suffix - ldap idmap suffix - ldap passwd sync - ldap trust ids - ldap del only sam attr - ldap replication sleep 일반 구성 - preload modules - private dir 수정된 매개 변수(동작 변경 사항) - encrypt passwords(기본적으로 활성화됨) - mangling method(기본적으로 "hash"로 설정됨) - passwd chat - passwd program - password server - restrict anonymous - security(새로운 "ads" 값) - strict locking(기본적으로 비활성화됨) - unix extensions(기본적으로 비활성화됨) - winbind cache time	

HP CIFS Server A.02.02의 매개 변수 변경 사항

이 절에서는 HP CIFS Server A.02.02의 `smb.conf` 매개 변수 변경 사항을 설명합니다.

새로운 매개 변수

다음은 HP CIFS Server A.02.02의 새로운 구성 매개 변수 목록입니다.

- `enable privileges`
- `allocation roundup size`
- `force printer name`
- `log nt token command`
- `ldap password sync`
- `check password script`

매개 변수 변경 사항

표 8-2는 기본 동작이 변경된 구성 매개 변수의 목록입니다.

표 8-2 매개 변수 변경 사항

매개 변수 이름	A.02.01.*	A.02.02
`strict locking`	`boolean` 유형	`integer` 유형
`dos filetimes`	**비활성화**	**활성화**
`lpq cache time`	10초	30초
`syslog`	1	HPUX의 경우에만 0

제거된 매개 변수

다음은 HP CIFS Server A.02.02에서 더 이상 사용되지 않는 구성 매개 변수입니다.

- `lstat broken symlinks`(`lstat broken symlinks = yes` 동작은 HP CIFS Server 버전 A.02.02에 통합)

HP CIFS Server A.01.*과 A.02.* 간의 동작 차이점

Samba 2.2가 기반이 되는 HP CIFS Server A.01.*과 Samba 3.0이 기반이 되는 HP CIFS Server A.02.* 간의 알려진 여러 가지 차이점은 HP CIFS Server 동작에 영향을 미칠 수 있습니다. 이 절에서는 HP CIFS Server A.02.*의 동작에 대한 주요 변경 사항에 대해 설명합니다. 그 밖의 변경 사항과 자세한 정보는 `/opt/samba/SAMBA_WHATSNEW.txt`를 참조하십시오.

HP CIFS Server A.02.*의 동작에 대한 주요 변경 사항은 다음과 같습니다.

- Windows 도메인의 구성원으로 작동하는 경우 A.01.*은 `getpwnam()` 호출을 통해 UID를 가져올 수 없으면 원격 도메인 컨트롤러에서 인증한 사용자를 `guest account`로 매핑합니다. A.02.*에서는 연결을 단순히 `NT_STATUS_LOGON_FAILURE` 오류로 거부합니다.
- HP CIFS Server 시스템 리소스 요구 사항이 증가되었습니다.

  HP CIFS Server A.02.01에서는 smbd 프로세스당 1000KB가 필요합니다.

  기본 메모리 증가 외에도, 단일 smbd 프로세스에서 최대 4MB의 메모리 스왑 공간을 임시로 사용할 수 있습니다.

  `nfile` 값이 smbd 프로세스당 24개에서 28개 항목으로 증가되었습니다.

  자세한 내용은 **HP CIFS Server 관리 설명서**의 2장 "HP CIFS Server 설치 및 구성"과 12장 "HP CIFS용으로 HP-UX 구성"을 참조하십시오.
- HP CIFS Server A.02.01 이상에서는 LDAP-UX 통합 제품인 J4269AA를 설치해야 합니다.
- 도메인 컨트롤러 역할을 하는 HP CIFS Server A.01.*에 컴퓨터 계정을 추가하는 경우 컴퓨터 트러스트 계정의 HP-UX ID를 만들도록 `add user script` 매개 변수가 지정됩니다. HP CIFS Server A.02.01에는 이러한 용도로 지정해야 하는 `add machine script` 매개 변수를 새로 추가했습니다. A.02.*는 `add machine script` 옵션이 없는 경우 `add user script` 옵션을 사용하지 않습니다.
- `join` 도메인 명령

A.02.*에서 도메인을 참여시키는 데 사용되는 "smbpasswd -j domain_name -r PDC_hostname -U administrator%passwd" 명령은 net 명령으로 대체되었습니다.

인증에 Kerberos 프로토콜을 사용하지 않는 Windows NT/2000 도메인은 smb.conf 파일에서 workgroup 매개 변수로 도메인 이름을 지정하여 "net rpc join -U Administrator%passwd" 명령을 사용합니다.

Kerberos가 구성된 Windows 2000 ADS 도메인의 경우는 smb.conf 파일에서 workgroup 매개 변수로 도메인 이름을 지정하여 "net ads join -U Adminitrator%passwd" 명령을 사용합니다.

- LDAP 스키마가 향상되었습니다. LDAP 백엔드를 사용하기로 한 경우에는 현재 스키마를 계속 사용할지 또는 업데이트된 스키마를 사용할지 여부를 선택해야 합니다. 업데이트된 스키마를 사용하기로 한 경우에는 smb.conf 파일에서 passwd backend 매개 변수를 ldapsam://ldapserver로 설정합니다. 현재 스키마를 사용하려는 경우에는 passwd backend 매개 변수를 ldapsam_compat://ldapserver로 설정합니다.
- A.02.* 버전에서는 A.01.* 도메인을 참여시킬 수 없습니다. A.01.* 버전 서버가 A.02.* PDC의 구성원 서버가 될 수 있으므로 A.01.* 버전과 A.02.* 버전의 혼합이 일부 허용되기도 하지만 A.02.*는 BDC 또는 A.01.* PDC의 구성원 서버로 작동할 수 없습니다. A.02.* 버전은 ASU(Advance Server for UNIX) PDC의 구성원 서버로도 사용할 수 없습니다.
- winbind 데몬인 winbindd가 실행되고 있지 않은 경우에는 도메인 사용자가 Windows ADS 또는 NT4 도메인 구성원으로 작동하는 HP CIFS Server 공유에 액세스할 수 있는 로컬 계정을 가지고 있어야 합니다. 로컬 계정이 없으면 HP CIFS Server에서 로그온을 거부합니다. add user script 옵션을 smb.conf 파일에 추가하면 로그온 사용자의 로컬 계정이 서버에 자동으로 생성됩니다. winbind 데몬인 winbindd가 실행 중이면 도메인 사용자에게 로컬 계정이 필요하지 않습니다. Winbindd는 Windows SID를 Unix UID/GIOD로 매핑할 수 있습니다.

HP CIFS Server A.01.*를 A.02.*로 업데이트

2장 "HP CIFS Server 설치 및 구성"의 설치 및 구성 절차는 HP CIFS Server A.02.* 버전과 A.01.* 버전에 모두 적용됩니다. 그러나 HP CIFS Server의 A.01.* 버전에서 A.02.* 버전으로 업데이트하는 경우에는 다음의 추가 사항을 고려해야 하며 아래 절차가 적용됩니다.

- HP CIFS Server A.02.* 버전에서는 A.01.* 버전으로의 다운그레이드 경로를 제공하지 않습니다. 따라서, 2장 HP CIFS Server 설치 및 구성의 39페이지의 “1단계: HP CIFS Server 소프트웨어 설치”에 설명된 백업 절차를 반드시 수행해야 합니다.
- 서버 배포 모델을 결정합니다.

  HP CIFS Server A.02.*는 HP CIFS Server A.01.* 버전 PDC 도메인의 구성원 서버가 될 수 없습니다. HP CIFS Server A.01.* 구성원 서버는 HP CIFS Serer A.02.* PDC 도메인에 참여할 수 있습니다. HP CIFS 배포 도메인 모델에 대한 자세한 내용은 9장, 213페이지의 “HP CIFS 배포 모델”을 참조하십시오.
- 대상 인증 백엔드를 결정합니다.

  선택하는 인증 백엔드는 배포 모델 및 업데이트 절차에 영향을 미칩니다. 업데이트를 진행하기 전에 인증 방법을 알고 있어야 합니다. HP CIFS Server에서 제공하는 Samba 관련 서적 *The Official Samba HOWTO and Reference Guide*와 *Samba 3 by Example*을 참조하십시오.

  HP CIFS Server A.02.* 인증 백엔드는 다음으로 구성됩니다.

  — `smbpasswd`: A.01.* 버전과 호환되는 일반 파일 형식입니다. 이 형식은 기본 구성입니다.

  — `tdbsam`: 독립형 서버의 `smbpasswd` 대체로 사용되며 다양한 속성을 지닌 데이터베이스입니다.

  — `ldapsam`: 다양한 속성을 지니고 있으며 LDAP 디렉토리를 사용하는 계정 저장 장치 및 검색 백엔드입니다. A.01.* 버전과 함께 제공된 것과는 다른 스키마를 사용합니다.

— `ldapsam_compat` : 이전 버전과 호환되는 LDAP 계정 백엔드의 HP CIFS Server A.01.* 버전입니다.

passdb backend 조합을 지정할 수도 있습니다. 다른 백엔드를 지정할 수 있습니다. 예를 들면, 실제 순서는 인증 방법의 `smb.conf` 키워드 순서를 따릅니다.

`passdb backend = smbpasswd tdbsam ldapsam` ldapsam_compat

- 현재 사용되는 대로 LDAP 또는 `smbpasswd`를 계속 사용하려면 HP CIFS PDC 및 독립형 서버의 A.01.* 버전을 업데이트하십시오.

  `passdb backend` 매개 변수를 LDAP 백엔드의 `ldapsam_compat`로 설정하거나 `smbpasswd` 백엔드의 `smbpasswd`로 설정할 수 있습니다.

  `security = domain` 구성을 보존하여 구성원 서버를 도메인 구성원 서버로 유지 관리할 수 있습니다.

  도메인 구성원 서버 설치 및 구성 방법에 대한 자세한 내용은 PDC 변경을 완료한 후 해당되는 105페이지의 “도메인 구성원 서버” 또는 5장, 123페이지의 “Windows 2000/2003 도메인”을 참조하십시오.

- `smb.conf` 매개 변수를 검사하고 203페이지의 “smb.conf의 매개 변수 변경 사항”에 요약된 필수 업데이트를 수행합니다.
- HP CIFS Server 데몬을 시작하고 변경 사항을 확인합니다.
- `pdbedit`와 `-i`, `-e` 및 `-g` 옵션을 사용하여 현재 데이터베이스에서 대상 위치로 이동합니다. `pdbedit`에 대한 자세한 내용은 SWAT 도움말 페이지를 참조하십시오. LDAP 백엔드를 사용하는 경우 자세한 내용은 6장, 131페이지의 “LDAP 통합 지원”을 참조하십시오.
- 대상 인증 백엔드가 적용되도록 `smb.conf` 파일의 `passdb backend` 매개 변수를 업데이트합니다.

버전 A.01.08에서 A.02.*로 프린터 서비스 마이그레이션

HP CIFS Server A.01.08에서 버전 A.02.*로 프린터 서비스를 마이그레이션하려면 다음 절차를 수행합니다.

- smb.conf 매개 변수인 `printer driver file`, `printer driver` 및 `printer driver location`은 A.02.01에서 더 이상 지원되지 않습니다. 프린터 드라이버 업로드에 대한 자세한 내용은 47페이지의 “프린터 드라이버를 자동으로 업로드하도록 클라이언트 설정” 절의 설명을 참조하십시오.

- `printers.def`를 사용하는 경우에는 프린터 드라이버 업로드에 대한 47페이지의 “프린터 드라이버를 자동으로 업로드하도록 클라이언트 설정” 절의 설명을 따르십시오.
- `printers.def`, `printer driver file`, `printer driver` 또는 `printer driver location`을 사용하지 않는 경우 프린터 서비스의 모든 기존 구성 매개변수는 전과 동일하게 작동됩니다.
- 자세한 프린터 마이그레이션 정보는 웹사이트 *http://us3.samba.org/samba/docs/man/Samba-HOWTO-Collection/*에 있는 "*Samba 3.0 HOWTO and Reference Guide*"의 20장, "Migration of Classical Printing to Samba"절을 참조하십시오.

HP CIFS Server A.01.*를 A.02.*로 업데이트

9 HP CIFS 배포 모델

이 장에서는 Samba 도메인, Windows 도메인 및 통합 도메인의 세 가지 HP CIFS 배포 모델에 대해 설명합니다. 참조용으로 각 배포 모델에 대한 구성 파일의 예제가 제공됩니다. 이 장의 구성은 다음과 같습니다.

- 215페이지의 “소개”
- 216페이지의 “Samba 도메인 모델”
- 230페이지의 “Windows 도메인 모델”
- 241페이지의 “통합 도메인 모델”

소개

HP CIFS는 HP-UX에 Microsoft CIFS(일반 인터넷 파일 시스템) 프로토콜에 기반한 분산 파일 시스템을 제공합니다. HP CIFS Server는 Windows NT, Windows 200x, Advanced Server 및 기타 CIFS Server, 클라이언트 등과 상호 운용됩니다. 이 장에는 Samba 도메인 모델, Windows 도메인 모델 및 통합 도메인 모델의 세 가지 배포 모델에 대한 참조 정보가 있습니다. 이러한 세 가지 모델은 일반적인 네트워크 환경을 나타내며 HP CIFS Server의 융통성을 보여 줍니다.

각 모델은 서버 관계를 표시하지만 모든 배포 모델에서는 기본 파일 액세스를 다음 클라이언트와 조합하여 지원합니다.

- Windows 2000, XP SP1 및 XP SP2
- Windows 터미널 서버(NT4 및 2000)
- HP CIFS Client
- UNIX 워크스테이션(NFS가 내보낸 CIFS 디렉토리를 마운트하는 방식 사용)

Samba 도메인 모델

다음과 같은 특성을 가진 환경에서 Samba 도메인 배포 모델을 사용할 수 있습니다.

- 도메인이 HP CIFS Server로 구성되고 Windows 도메인 컨트롤러가 없습니다.
- 서버 수만큼의 사용자에게 파일 및 인쇄 서비스를 제공하는 UNIX 서버를 지원합니다.
- HP CIFS Server를 PDC(주 도메인 컨트롤러)로 구성합니다. 하나 이상의 HP CIFS Server가 BDC(백업 도메인 컨트롤러)의 역할을 합니다.
- PDC 및 BDC는 LDAP 백엔드를 사용하여 일반적인 Posix 및 Windows 계정을 LDAP 디렉토리에 통합합니다. 이렇게 하려면 대규모 배포를 위한 LDAP-UX Integration 소프트웨어가 필요합니다.
- 보다 큰 규모의 배포를 위한 백엔드 저장 장치로 LDAP-UX Netscape Directory Server에 액세스합니다.

Samba 도메인 모델에서는 다음과 같은 이점을 제공합니다.

- 쉬운 확장 기능을 제공합니다.
- BDC 역할을 하는 HP CIFS Server는 네트워크에서 PDC가 사용되는 동안 네트워크 로그온 요청을 선택하고 사용자를 인증합니다. PDC가 사용 불가능하게 되거나 실패하는 경우 BDC는 PDC로 승격될 수 있습니다. PDC-BDC 모델에서는 보다 큰 규모의 네트워크를 위한 인증 로드 균형 조정을 제공합니다.
- PDC, BDC 및 도메인 구성원 서버는 계정 데이터베이스를 LDAP 디렉토리에 저장하여 네트워크 크기에 관계없이 관리를 중앙 집중화합니다.

그림 9-1에서는 로컬 암호 데이터베이스를 사용하여 PDC 역할을 하는 독립형 HP CIFS Server를 보여 줍니다.

그림 9-1 PDC 역할을 하는 독립형 HP CIFS Server

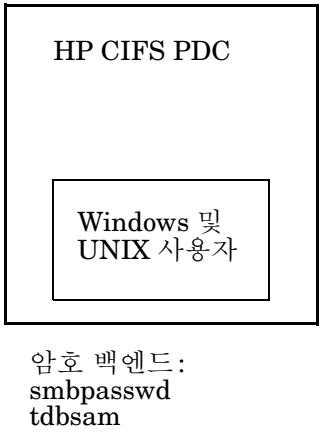


그림 9-2에서는 NDS(Netscape Directory Server)를 LDAP 백엔드로 사용하여 PDC 역할을 하는 독립형 HP CIFS Server를 보여 줍니다.

그림 9-2 NDS 백엔드를 사용하여 PDC 역할을 하는 독립형 HP CIFS Server

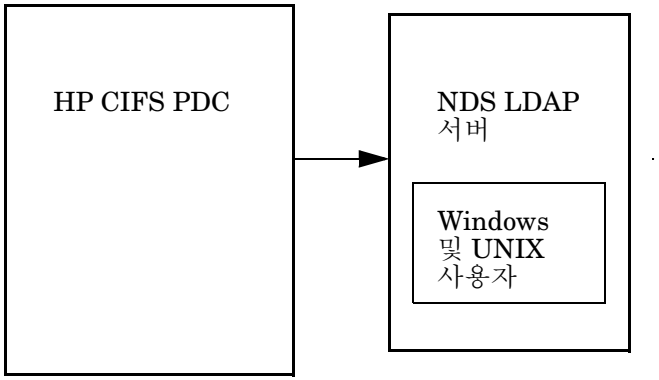


그림 9-3에서는 LDAP 백엔드로 Netscape Directory Server를 사용하는 여러 HP CIFS Server를 보여 줍니다.

그림 9-3 NDS 백엔드를 사용하는 여러 HP CIFS Server

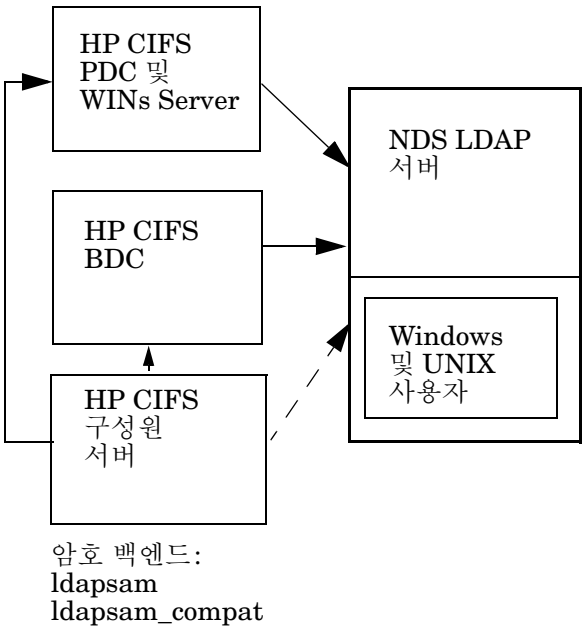
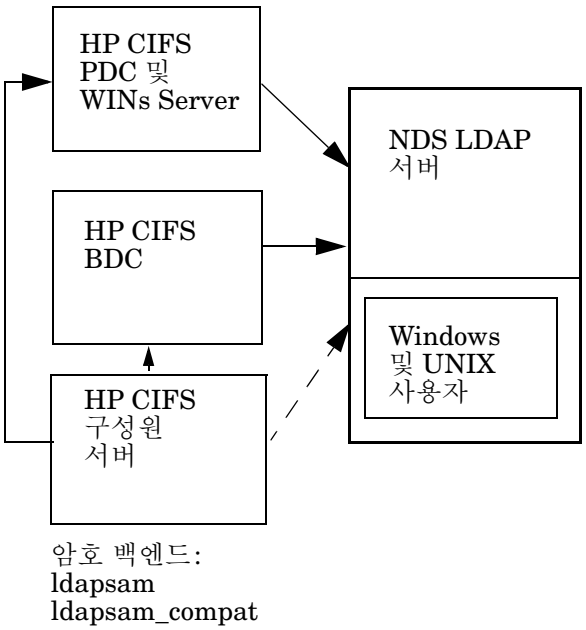


그림 9-4에서는 Samba 도메인 모델을 보여 줍니다.

그림 9-4 Samba 도메인



Samba 도메인 배포 모델은 PDC(주 도메인 컨트롤러)로 구성된 HP CIFS Server 및 BDC(백업 도메인 컨트롤러)의 역할을 하는 하나 이상의 HP CIFS Server로 구성됩니다. PDC, BDC 및 구성원 서버는 중앙 LDAP 백엔드를 사용하여 POSIX 및 Windows 계정을 LDAP 디렉토리에 통합합니다. 이렇게 하려면 보다 큰 규모의 배포를 위해 HP CIFS Server에 설치 및 구성된 HP LDAP-UX 클라이언트 서비스 소프트웨어가 필요합니다.

Samba 도메인 구성 요소

이 모델에서는 여러 서버에 사용하기 위해 디렉토리 서버와 LDAP 액세스를 사용합니다. 모든 노드에 LDAP-UX 클라이언트 서비스 소프트웨어를 설치하고 구성하여 POSIX 및 Windows 사용자 데이터를 모두 중앙 집중화해야 합니다. LDAP 설정 방법에 대한 자세한 내용은 6장, 131페이지의 “LDAP 통합 지원”을 참조하십시오.

WINS는 여러 하위 네트워크로 구성된 환경에서 사용됩니다. 여러 하위 네트워크로 구성된 환경에서 단일 LAN 세그먼트의 브로드캐스트 한계를 초과하려면 이름-IP주소 매핑이 필요합니다. HP CIFS Server는 WINS 서버 기능을 제공하며, 이 WINS 서버는 도메인에 대해 한 노드(일반적으로 PDC)에서 사용할 수 있고 나머지 노드(일반적으로 BDC 및 구성원 서버)의 구성에 주소를 지정해야 합니다. PC 클라이언트 구성에서도 WINS 서버 주소를 지정하여 도메인에 참여할 수 있습니다. WINS 서버가 될 HP CIFS Server의 `smb.conf`에 `wins support = yes`를 설정합니다. 나머지 HP CIFS Server의 `smb.conf`에 "`wins server = <ip address>`"를 설정합니다. Samba 제공 WINS는 복제를 제공하지 않으므로 WINS 서버는 네트워크에서 하나의 장애 요인이 될 수 있습니다. WINS 서버에서 Serviceguard를 사용하여 고가용성 요구 사항이 필요할 경우 DNS 서버에서 NetBIOS 이름의 정적 캐시 또는 클라이언트 호스트 파일을 사용하는 것이 좋습니다.

PDC 역할을 하는 HP CIFS Server

PDC로 구성된 HP CIFS Server는 도메인 전체에서 Windows 인증을 수행합니다. "`security = user`" 및 "`domain logons = yes`" `smb.conf` 매개 변수가 이 동작을 실행합니다.

단일 서버 설치에서는 `smbpasswd` 또는 `tdbsam` 암호 백엔드를 사용할 수 있지만 대규모 설치에서는 LDAP 백엔드를 사용하여 Posix 사용자와 Windows 사용자 모두의 관리를 중앙 집중화해야 합니다. `passdb backend = ldapsam:ldap://<ldap server name>` 또는 `passdb backend = ldapsam_compat:ldap://<ldap server name>`을 사용하여 LDAP를 구성합니다.

검색 제어는 CIFS PDC의 중요한 특징입니다. `domain master = yes` 매개 변수는 서버에서 NetBIOS 이름 <pdc name>1B를 등록하게 합니다. 여기서 1B는 도메인 마스터 브라우저용으로 예약되어 있습니다. 다른 서버에서 이 이름을 인식합니다.

LDAP 디렉토리를 사용하여 PDC 역할을 하는 HP CIFS Server를 통합할 경우 HP LDAP-UX Integration 소프트웨어를 설치하고 LDAP-UX 클라이언트를 구성해야 합니다. 이렇게 하면 POSIX 및 Windows 사용자 계정을 LDAP 디렉토리에 통합할 수 있습니다. LDAP 데이터베이스는 `/etc/passwd` 및 `smbpasswd`를 대체할 수 있고 PDC는 Windows 인증을 위해 LDAP 디렉토리에 액세스할 수 있습니다.

BDC 역할을 하는 HP CIFS Server

BDC 구성은 PDC 구성과 비슷합니다. 따라서 BDC는 대부분의 네트워크 로그온 처리를 수행할 수 있습니다. 로컬 네트워크에서 PDC가 사용되고 있는 경우 로컬 세그먼트의 BDC는 로그온 요청을 처리하고 사용자를 인증합니다. 세그먼트에 부하가 크게 증가하면 이 작업 부하는 다른 세그먼트의 BDC 또는 PDC로 전달됩니다. 따라서 BDC를 네트워크 전체에 배포하면 리소스를 최적화하고 네트워크 서비스에 안정성을 추가할 수 있습니다.

`smb.conf`의 `local master` 매개 변수를 `yes`로 설정하면 검색을 네트워크 전체에 분배할 수도 있습니다.

PDC가 사용 불가능하게 되거나 실패하는 경우 BDC를 PDC로 승격할 수 있습니다. BDC를 PDC로 승격하려면 `domain master` 매개 변수를 `no`에서 `yes`로 변경합니다.

PDC 및 BDC는 중앙 LDAP 디렉토리를 사용하여 일반적인 Posix 및 Windows 계정을 LDAP 디렉토리에 저장합니다. LDAP 디렉토리를 사용하여 BDC 역할을 하는 HP CIFS Server를 통합할 경우 HP LDAP-UX Integration 소프트웨어를 설치하고 LDAP-UX 클라이언트를 구성해야 합니다. BDC는 Windows 인증을 위해 LDAP 디렉토리에 액세스할 수 있습니다.

구성원 서버 역할을 하는 HP CIFS

일반적으로 인증과 로그온 요청을 처리하는 충분한 도메인 컨트롤러를 항상 제공하려면 BDC당 30대 이상의 Windows 클라이언트가 있는 경우에는 구성원 서버 대신 BDC를 구성하십시오.

HP CIFS Server를 Samba 도메인에 참여시킬 수 있습니다. Windows 인증 요청은 LDAP, `smbpasswd` 또는 기타 백엔드를 사용하여 PDC 또는 BDC에서 관리됩니다. HP CIFS Server를 Samba 도메인에 참여시키는 방법에 대한 자세한 내용은 4장, 105 페이지의 “도메인 구성원 서버”를 참조하십시오.

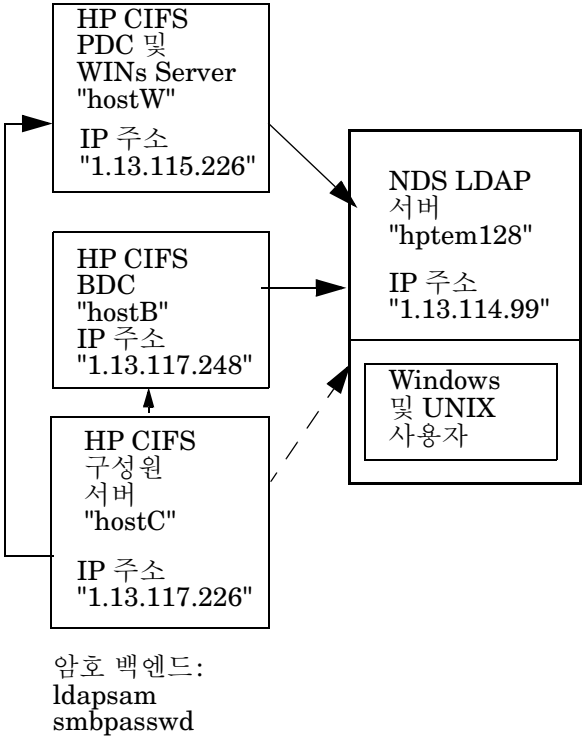
구성원 서버의 smb.conf 구성은 PDC 및 BDC의 구성과 다릅니다. security 매개 변수를 domain으로 설정해야 합니다. 이렇게 하면 구성원 서버는 PDC 또는 BDC를 통해 인증합니다. password server 매개 변수를 PDC 이름으로 설정해야 하며 하나 이상의 BDC 이름을 추가할 수도 있습니다. domain master 매개 변수를 no로 설정하여 PDC에서 제어하도록 합니다.

PDC 및 BDC의 경우 passdb backend 매개 변수를 LDAP 서버 이름으로 설정하여 POSIX 및 Windows 계정 데이터베이스 관리를 중앙 집중화합니다. LDAP를 사용하려면 HP LDAP-UX Integration 소프트웨어를 설치하고 LDAP 클라이언트를 구성하여 POSIX 및 Windows 사용자를 LDAP 디렉토리에 통합해야 합니다.

Samba 도메인 모델의 예제

그림 9-5에서는 PDC 및 WINs 서버 역할을 하는 HP CIFS Server 시스템 `hostW`(IP 주소: `1.13.115.226`), BDC 역할을 하는 HP CIFS Server 시스템 `hostB`(IP 주소: `1.13.117.248`) 및 Netscape Directory Server 시스템 `hptem128`이 있는 Samba 도메인 모델의 예제를 보여 줍니다.

그림 9-5 **Samba 도메인 모델의 예제**



PDC에 대한 샘플 smb.conf 파일

다음은 그림 9-5에 표시된 샘플 Samba 도메인 모델의 PDC 역할을 하는 HP CIFS Server 시스템 `hostW`에 사용되는 샘플 Samba 구성 파일인 /etc/smb.conf입니다.

```
#####################################
#
# Samba config file created using SWAT
# from 1.13.129.217
#
# Global Parameters
[global]
workgroup = SAMBA30_DOMAIN # Domain Name
server string = Samba Server hostW PDC
passdb backed = ldapsam:ldap://hpldap128:389, smbpasswd
log level = 0
security = user
syslog = 0
log fie = /var/opt/samba/log.%m
max log size = 1000
domain logons = Yes
preferred master = Yes
local master = Yes
domain master = Yes
wins support = yes
ldap admin dn = cn=Directory Manager
ldap group suffix = ou=Groups
ldap machine suffix = ou= Computers
ldap suffix = dc=org, dc=hp, dc=com
ldap user suffix = ou= People
read only = No
short preserve case = No
dos filetime resolution = Yes
#
[homes]
comment = Home Directory
browseable = No
[tmp]
comment = Temporary file space
path = /tmp

[netlogon]
comment = The domain logon service
path = /var/opt/samba/netlogon
read only = Yes
```

참고

SSL 활성 LDAP에 대해 `passdb backend = ldapsam:ldaps://<fully qualitied name of NDS Server>`를 설정합니다. `passdb backend =`

ldapsam:ldap://<NDS Server name>을 설정하여 SSL 지원을 비활성화합니다. 이전 버전과 호환되는 A.01.* 버전의 LDAP 계정 백엔드를 사용하려는 경우에는 smb.conf에서 passwd backend = ldapsam_compat://ldaps:< ldap server name>, ldap ssl = yes 및 ldap port = 636을 설정하여 SSL 지원을 활성화합니다.

구성 옵션

- domain master: HP CIFS Server가 PDC 역할을 하도록 하려면 이 매개 변수를 yes로 설정합니다.
- domain logon: netlogon 서비스를 제공하려면 이 매개 변수를 yes로 설정합니다.
- passdb backend: LDAP 데이터베이스의 이전 Samba 하위 스키마를 사용하려면 이 매개 변수를 ldapsam_compat:ldap://<ldap server name>으로 설정해야 합니다. HP CIFS Server A.02.01에서 지원하는 새 하위 스키마를 사용하려면 이 매개 변수를 ldapsam:ldap://<ldap server name>으로 설정해야 합니다.
- WINs support: HP CIFS Server를 WINs 서버로 구성하려면 이 매개 변수를 yes로 설정해야 합니다.

BDC에 대한 샘플 smb.conf 파일

다음은 그림 9-5에 표시된 샘플 Samba 도메인 모델의 BDC 역할을 하는 HP CIFS Server 시스템 hostB에 사용되는 샘플 Samba 구성 파일인 /etc/smb.conf입니다.

```
#######################################
#
# Samba config file created using SWAT
# from 1.13.129.217
#
# Global Parameters
[global]
workgroup = SAMBA30_DOMAIN     # Domain Name
server string = Samba Server hostB BDC
password server =
passdb backend = ldapsam:ldap://hptem128:389, smbpasswd
log level = 0
syslog = 0
log fie = /var/opt/samba/log.%m
max log size = 1000
```

```
domain logons = Yes
security = user
local master = No
domain master = No
wins server = 1.13.115.226 # Set the PDC as WINs Serer
wins support = yes
ldap admin dn = cn=Directory Manager
ldap group suffix = ou=Groups
ldap machine suffix = ou= Computers
ldap suffix = dc=org, dc=hp, dc=com
ldap user suffix = ou= People
read only = No
short preserve case = No
dos filetime resolution = Yes
#
[homes]
comment = Home Directory
browseable = No
[tmp]
comment = temporary file space
path = /tmp
```

구성 옵션

- `passdb backend`: LDAP 데이터베이스의 이전 Samba 하위 스키마를 사용하려면 이 매개 변수를 `ldapsam_compat:ldap://<ldap server name>`으로 설정해야 합니다. HP CIFS Server A.02.01에서 지원하는 새 하위 스키마를 사용하려면 이 매개 변수를 `ldapsam:ldap://<ldap server name>`으로 설정해야 합니다.
- `domain master`: HP CIFS Server를 BDC로 사용하려면 이 매개 변수를 `no`로 설정합니다.
- `WINs Server`: PDC를 WINs 서버로 사용하는 경우 이 매개 변수를 PDC의 시스템 이름으로 설정합니다.
- `domain logon`: netlogon 서비스를 제공하려면 이 매개 변수를 `yes`로 설정해야 합니다.

도메인 구성원 서버에 대한 샘플 smb.conf 파일

구성원 서버 역할을 하도록 HP CIFS Server를 구성하려면 SWAT 도구나 편집기를 사용하거나 `samba_setup`을 실행하여 `/etc/opt/samba/smb.conf` 파일의 관련 도메인 매개 변수를 구성해야 합니다.

다음은 그림 9-5에 표시된 샘플 Samba 도메인 모델의 도메인 구성원 서버 역할을 하는 HP CIFS Server 시스템 hostC에 사용되는 샘플 Samba 구성 파일인 /etc/smb.conf입니다.

```
#####################################
#
# Samba config file created using SWAT
# from 1.13.129.217
#
# Global Parameters
[global]
workgroup = SAMBA30_DOMAIN     # Domain Name
server string = Samba Server hostC Domian Member Server
password server = hostW hostB
security = Domain
netbios aliases = MOONEY
log level = 0
syslog = 0
log fie = /var/opt/samba/log.%m
max log size = 1000
domain logons = Yes
preferred master = No
domain master = No
wins server = 1.13.115.226   # Set the PDC ad Wins Server
wins support = yes
ldap port = 389
ldap admin dn = cn=Directory Manager
ldap group suffix = ou=Groups
ldap machine suffix = ou= Computers
ldap suffix = dc=org, dc=hp, dc=com
ldap ssl = no
ldap user suffix = ou= People
read only = No
short preserve case = No
dos filetime resolution = Yes
#
[homes]
comment = Home Directory
browseable = No
```

구성 옵션

- workgroup: 이 매개 변수는 HP CIFS Server가 도메인 구성원으로 속한 도메인의 이름을 지정합니다.

- `security`: HP CIFS Server가 구성원으로 도메인에 참여할 경우 이 매개 변수를 `domain`으로 설정해야 합니다.
- `WINs Server`: PDC를 Wins 서버로 사용할 경우 이 매개 변수를 PDC의 시스템 이름으로 설정합니다.
- `password server`: 이 매개 변수는 사용자 이름 인증과 유효성 검증을 수행하는 PDC 및 BDC 시스템의 NetBIOS 이름을 정의합니다.

샘플 /etc/nsswich.ldap 파일

LDAP 백엔드 지원을 사용하여 PDC, BDC 및 구성원 서버를 설정할 경우 Netscape Directory Server에서 계정 정보를 검색하도록 `/etc/nsswitch.conf` 파일을 구성해야 합니다. `/etc/nsswitch conf` 파일 사본을 저장하고 원래 파일을 편집하여 LDAP 이름 서비스 및 사용하려는 기타 이름 서비스를 지정할 수 있습니다. `/etc/nsswitch.ldap`를 `/etc/nsswitch.conf`로 복사만 할 수도 있습니다.

다음은 그림 9-5에 표시된 샘플 Samba 도메인 모델에 사용되는 샘플인 `/etc/nsswitch.ldap`입니다.

```
# /etc/nsswitch.ldap                                        #
# You can copy this sample file to /etc/nsswitch.conf.      #
# This sample file uses Lightweigh Directory Access         #
# Protocol(LDAP) in conjunction with dns and files.         #
passwd:     files ldap
group:      files ldap
hosts:      dns [NOTFOUND=return] files ldap
networks:   files ldap
protocols:  files ldap
rpc:        files ldap
publickey:  files
netgroup:   files ldap
automount:  files
aliases:    files
services:   files ldap
```

Windows 도메인 모델

다음과 같은 특성을 가진 환경에서 Windows 도메인 모델을 사용할 수 있습니다.

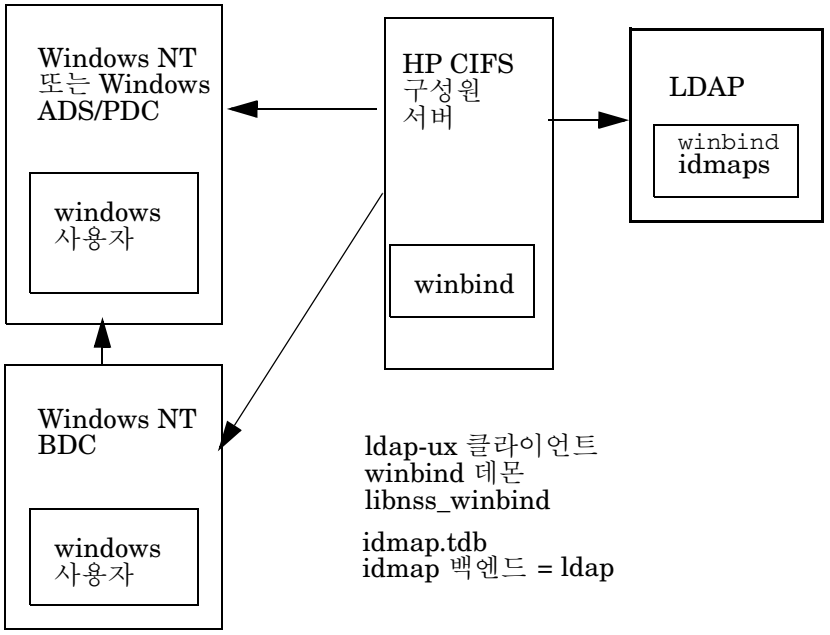
- Windows NT4, Windows 200x 혼합 모드 또는 Windows 200x ADS 서버(NetBIOS 활성화)를 배포합니다.
- 서버 수만큼의 사용자에게 파일 및 인쇄 서비스를 제공하는 HP CIFS Server를 지원합니다. 이렇게 하려면 ADS 도메인 구성원 서버 사용을 위한 HP-UX LDAP Integration 클라이언트 소프트웨어가 필요합니다.
- 보다 큰 규모의 배포를 위한 백엔드 저장 장치로 LDAP-UX Netscape Directory Server에 액세스하여 여러 HP CIFS Server에서 `winbind` ID 맵을 유지 관리합니다.

Windows 도메인 모델에서는 다음과 같은 이점을 제공합니다.

- Windows 도메인 구성원의 단일 사인온, 네트워크 로그온 및 Windows 계정 관리 시스템을 지원합니다.
- `winbind`를 사용하여 여러 HP CIFS Server에서 쉬운 사용자 관리를 지원합니다.
- 쉬운 확장 기능을 제공합니다.

그림 9-6에서는 다음과 같이 Windows 도메인 배포 모델을 보여 줍니다.

그림 9-6 Windows 도메인



Windows 도메인 모델에서 HP CIFS Server는 Windows NT 또는 Windows 200x 도메인 컨트롤러를 사용하여 구성원 서버로 Windows 도메인에 참여할 수 있습니다. HP CIFS Server는 `winbind`를 지원하여 Windows 사용자에게 UID 및 GID 매핑을 제공합니다. 보다 큰 규모의 배포 환경의 경우 LDAP 디렉토리를 사용하여 여러 HP CIFS Server에서 고유 ID 맵을 유지 관리할 수 있습니다.

Windows 도메인 구성 요소

HP CIFS Server는 NT 도메인 구성원에 사용되는 NTLMv1/NTLMv2 보안 및 Windows 2000/2003 기본 구성원에 사용되는 Kerberos 보안을 지원하므로 HP CIFS Server는 Windows 2000/2003 ADS, Windows 200x 혼합 모드 또는 NT 환경에서 관리할 수 있습니다. HP CIFS Server는 실제 SAM 데이터베이스를 지원하지 않으며 도메인 컨트롤러로 Windows NT, Windows 2000 또는 Windows 2003 도메인에 참여할

수 없습니다. HP CIFS는 `winbind`를 지원하며, 이를 사용하여 Windows 사용자 및 그룹 매핑에 POSIX 사용자 및 그룹을 명시적으로 할당하지 않을 수 있습니다. `Winbind`는 Windows 사용자에 대한 UID 및 GID를 생성하고 매핑합니다. `smb.conf` 매개 변수를 `idmap uid = <uid range>` 및 `idmap gid = <gid range>`로 설정합니다. `winbind`에 대한 자세한 내용은 7장, 183페이지의 "Winbind 지원"을 참조하십시오.

여러 HP CIFS Server를 배포할 경우 LDAP 디렉토리를 사용하여 여러 시스템에서 고유한 ID를 유지 관리할 수 있습니다. 그렇지 않으면 HP CIFS Server에 마운트된 NFS 공유를 사용할 때 시스템 간에 사용자 매핑의 일관성이 유지되지 않습니다. LDAP 디렉토리에서 ID 맵의 관리를 중앙 집중화하려면 `smb.conf` 파일에서 `idmap backend` 매개 변수를 `ldapsam:ldap://<ldap server name>`으로 설정합니다.

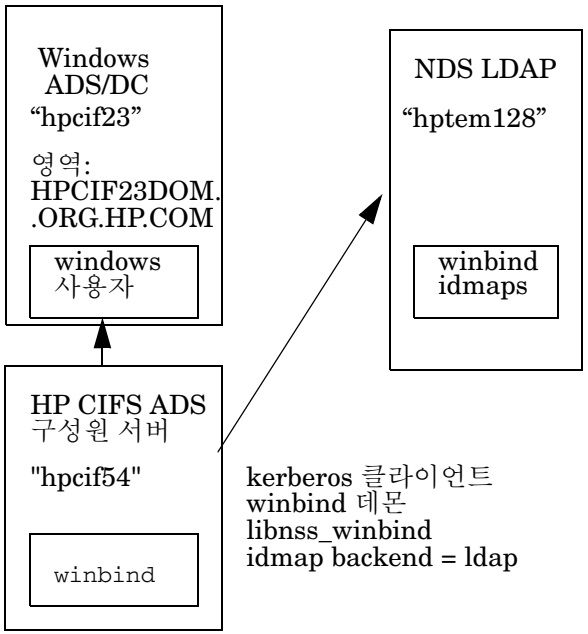
`wins server = <Windows or NT WINS server address>` `smb.conf` 매개 변수를 사용하여 여러 하위 네트워크로 구성된 네트워크 전체에 액세스할 수 있습니다. HP CIFS WINS 서버는 WINS 데이터를 복제할 수 없으므로 Windows 또는 NT WINS 서버를 사용할 수 있는 경우에는 HP CIFS에서 제공하는 WINS 서버를 사용하지 않도록 합니다.

*http://docs.hp.com*에서 사용할 수 있는 "*LDAP-UX Client Service with Micrsoft Windows 2000 Active Directory Administrator's Guide*"에서는 HP-UX ADS 클라이언트 구성에 대한 도움말을 제공합니다.

ADS 도메인 모델의 예제

그림 9-7에서는 HPCIF23DOM.ORG.HP.COM이라는 영역, ADS 도메인 컨트롤러 시스템 hpcif23, 기본 구성원 서버 역할을 하는 HP CIFS Server 시스템 hpcif54 및 Netscape Directory Server 시스템 hptem128이 있는 Windows 2000/2003 ADS 도메인 모델의 예제를 보여 줍니다.

그림 9-7 ADS 도메인 모델의 예제



HP CIFS ADS 구성원 서버에 대한 샘플 smb.conf 파일

다음은 그림 9-7에 표시된 샘플 ADS 도메인 모델의 ADS 구성원 서버 역할을 하는 HP CIFS Server 시스템 hpcif54에 사용되는 샘플 Samba 구성 파일인 /etc/smb.conf입니다.

```
########################################################
#
# An sample smb.conf file for an HP CIFS ADS member server
#
```

```
# Global Parameters
[global]
workgroup = hpcif23_dom    # Domain Name
server string = CIFS Server as a domain member of hpcif23_dom
realm = HPCIF23DOM.ORG.HP.COM
security = ADS
netbios name = hpcif54
encrypt passwords = yes
password server = *
passdb backend = smbpasswd
log level = 0
syslog = 0
log fie = /var/opt/samba/log.%m
max log size = 1000
host msdfs = yes

# For LDAPSAM
# passdb backend = ldapsam:/ldap://hptem128
# ldap port = 389
# ldap admin dn = cn=Directory Manager
# ldap filter = (&(uid=%u)(objectclas=SambaSamAccount))
# ldap user suffix = ou=People
# ldap group suffix = ou=Groups
# ldap machine suffix = ou= Computers
# ldap suffix = dc=org, dc=hp, dc=com
# ldap ssl = no
# ldap user suffix = ou= People
# ldap delete dn = no
# ldap passwd sync = no
# ldap replication sleep = 1000
# ldap timeout = 15

# For idmap configuration of winbind
idmap backend = ldap:ldap://hptem128
idmap uid = 1000-10000
idmap gid = 1000-10000
ldap server = hptem128
ldap admin dn = "cn=Directory Manager"
ldap suffix = dc=org, dc=hp, dc=com
ldap port = 389
ldap idmap suffix = ou=ldmap

#
# For non winbind solution
# add user script = /usr/sbin/useradd -g users -c \
# winbind_create -d /tmp -s /bin/false %u
# For winbind solution
```

```
winbind use default domain =yes
winbind uid = 10000-20000
winbind gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
template homedir = /home/%U
template shell = /bin/false

#
[homes]
comment = Home Directory
browseable = no
writable = yes
valid users = %D\%S
create mode = 0664
directory mode = 0775

[locshare]
path = /tmp
read only = no
browseable = yes
writable = yes

[nfsshare]
path=/mount/tmp
read only = no
browseable = yes
writable = yes

[dfsshare]
path=/dfsroot
read only = no
browseable = yes
writable = yes

[tmp]
path = /tmp
read only = no
browseable = yes
writable = yes
```

샘플 /etc/krb5.conf 파일

ADS 구성원 서버 역할을 하는 HP CIFS Server에서 Kerberos 구성 파일 /etc/krb5.conf를 만듭니다. 이 파일에서 영역 이름, KDC(Key Distribution Center) 서버의 위치 및 로깅 파일 이름을 지정합니다.

다음은 그림 9-7에 표시된 샘플 ADS 도메인 모델에 사용되는 샘플인 /etc/krb5.conf입니다.

```
# Kerberos Configuration                                          #
#                                                                 #
# This krb5.conf file is intended as an example only.             #
# See krb5.conf(4) for more details.                              #
#
# Please verify that you have created the directory /var/log.#
#                                                                 #
# Replace MYREALM.XYZ.COM with your kerberos Realm.               #
# Replace adsdc.myrealm.xyz.com with your Windows ADS DC full#
# domain name.                                                    #
#                                                                 #
[libdefaults]
default_realm = HPCIF23DOM.ORG.HP.COM
default_tkt_enctypes = DES-CBC-MD5
default_tgs_enctypes = DES-CBC-MD5
ccache_type = 2

[realms]
MYREALM.XYZ.COM = {
kdc = hpcif23.org.hp.com:88
admin_server = hpcif23.org.hp.com
}
[domain_realm]
.org.hp.com = HPCIF23DOM.ORG.HP.COM

[logging]
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmin.log
default = FILE:/var/log/krb5lib.log
```

참고

서버 필드에 :88이 필요합니다.

샘플 /etc/nsswitch.conf 파일

ADS 도메인 모델에서 winbind 이름 서비스 및 사용하려는 기타 이름 서비스를 지정하도록 /etc/nsswitch.conf 파일을 구성해야 합니다.

다음은 그림 9-7에 표시된 샘플 ADS 도메인 모델에 사용되는 샘플인 /etc/nsswitch.conf입니다.

```
# /etc/nsswitch.conf                                          #
#                                                             #
# This sample file uses Lightweigh Directory Access           #
# Protocol(LDAP) in conjunction with dns and files.           #
passwd:     files winbind [NOTFOUND=return] ldap
group:      files winbind [NOTFOUND=return] ldap
hosts:      files dns [NOTFOUND=return] wins
networks:   files
protocols:  files
rpc:        files
publickey:  files
netgroup:   files
automount:  files
aliases:    files
services:   files
```

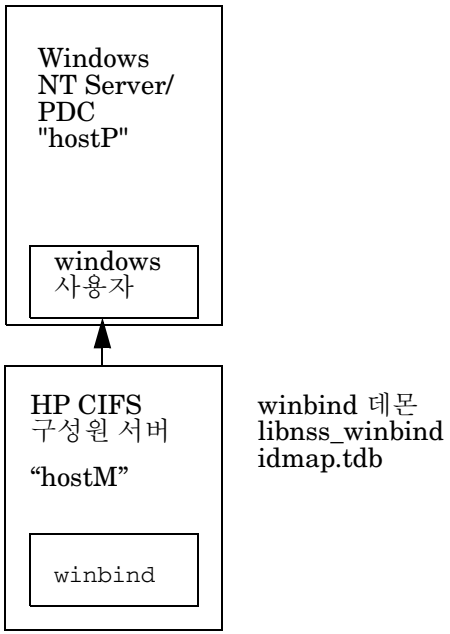
참고

HP CIFS Server에서는 POSIX 사용자 및 그룹을 할당하고 매핑하는 다양한 방법을 지원합니다. winbind가 사용되는 경우에는 /etc/nsswitch.conf에 winbind 이름 서비스가 필요합니다. winbind가 사용되지 않는 경우에는 각 Windows 사용자 및 그룹에 연결된 로컬 POSIX 계정을 만들어야 합니다. 이러한 계정을 자동으로 만드는 하나의 방법은 smb.conf에 "add user script" 및 "add group script" 옵션을 정의하는 것입니다. 자세한 내용은 SWAT 도움말 텍스트를 참조하십시오.

Windows NT 도메인 모델의 예제

그림 9-8에서는 PDC 역할을 하는 Windows NT 서버 `hostP`, 도메인 구성원 서버 역할을 하는 HP CIFS Server 시스템 `hostM`이 있는 Windows NT 도메인 모델의 예제를 보여 줍니다. ID 맵은 로컬 파일 `idmap.tdb`에 저장됩니다.

그림 9-8 Windows NT 도메인 모델의 예제



HP CIFS 구성원 서버에 대한 샘플 smb.conf 파일

다음은 그림 9-8에 표시된 샘플 Windows NT 도메인 모델의 구성원 서버 역할을 하는 HP CIFS Server 시스템 `hostM`에 사용되는 샘플 Samba 구성 파일인 `/etc/smb.conf`입니다.

```
########################################################
#
# An sample smb.conf file for an HP CIFS ADS member server
#
# Global Parameters
```

```
[global]
workgroup = hpcif23_dom    # Domain Name
server string = CIFS Server as a member of NT domain
netbios name = hostM
# For NT specific option
workgroup = hostP_dom
security = domain
encrypt passwords = yes
passdb backend = smbpasswd
password server = hostP.org.hp.com
log level = 0
log fie = /var/opt/samba/log.%m
max log size = 1000

#
# For non winbind solution
# add user script = /usr/sbin/useradd -g users -c \
add_user_script -d /tmp -s /bin/false %u
#
# For winbind specific options
winbind use default domain =yes
winbind uid = 10000-20000
winbind gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
winbind cache time = 10
template homedir = /home/%U
template shell = /bin/false
#
[homes]
comment = Home Directory
create mode = 0664
directory mode = 0775
valid users = %S
browseable = No
read only = No
writable = yes

[print$]
comment = For Printer share
browseable = yes

[printers]
comment = All Printers
path = /tmp
printable = yes
browseable = yes
```

```
printer admin = root, admuser
create mask = 0600
guest ok = Yes
use client driver = Yes

[lj810002]
path = /tmp
printable = yes
print command = /usr/bin/lp -d%p %s; /usr/bin/rm %s

[locshare1]
comment = Local file system service1 for read only
path = /tmp
admin users = admuser
read only = Yes

[locshare2]
comment = Local file system service2 for writable
path = /tmp
admin users = admuser
read only = No

[nfsshare]
comment = Remote NFS service
path = /mount/public
read only = No

[%U]
comment = Domain Valid user personal share
path = /home/%U

[tmp]
path = /tmp
read only = no
browseable = yes
writable = yes
```

통합 도메인 모델

다음과 같은 특성을 가진 환경에서 통합 도메인 배포 모델을 사용할 수 있습니다.

- 도메인이 Windows 200x 서버로 구성됩니다.
- Windows 2000 또는 2003 도메인 컨트롤러가 UNIX(SFU)용 Windows 서비스를 사용하여 UNIX UID 및 GID 데이터를 유지 관리합니다.

참고

SFU 버전 3.5에서는 Windows NT4 도메인을 지원하지 않습니다.

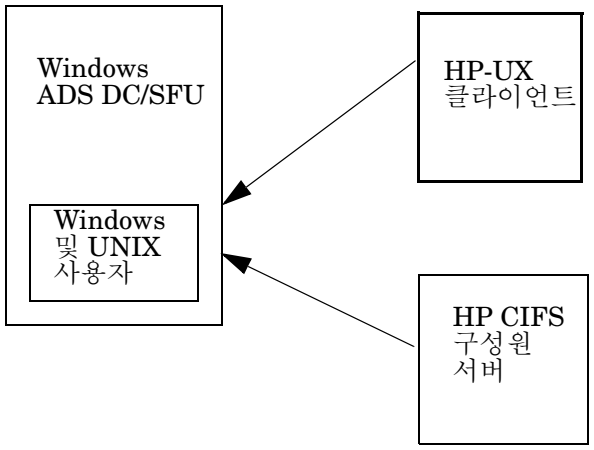
- 서버 수만큼의 사용자에게 파일 및 인쇄 서비스를 제공하는 HP CIFS Server를 지원합니다. 이렇게 하려면 HP CIFS 구성원 서버에 LDAP-UX Integration 소프트웨어가 필요합니다.

통합 도메인 모델에서는 다음과 같은 이점을 제공합니다.

- Windows 도메인 구성원의 단일 사인온, 네트워크 로그온 및 Windows와 UNIX 계정 관리 시스템을 지원합니다.
- 쉬운 확장 기능을 제공합니다.

그림 9-9에서는 다음과 같이 통합 도메인 배포 모델을 보여 줍니다.

그림 9-9 통합 도메인



통합 도메인 모델은 DC(도메인 컨트롤러)로 구성된 ADS(Active Directory Services)를 사용하는 Windows 200x 서버 및 하나 이상의 HP CIFS 구성원 서버로 구성됩니다. Windows 200x ADS 서버를 Windows 및 UNIX 사용자 계정을 통합하는 데이터 저장소로 사용하려면 RFC 2307을 기반으로 Active Directory 스키마를 확장하는 UNIX(SFU)용 서비스 추가 패키지를 설치하여 POSIX 속성 통합을 허용해야 합니다. 모든 사용자 관리는 Windows 2000/2003 ADS 서버에 통합되며 `winbind`가 필요하지 않습니다. HP CIFS 구성원 서버에 LDAP-UX Integration 소프트웨어를 설치하고 구성해야 합니다. LDAP-UX Integration 소프트웨어를 사용하면 HP CIFS Server 시스템이 ADS 서버에서 UNIX 사용자 계정에 액세스할 수 있습니다.

*http://docs.hp.com*에서 사용할 수 있는 "*LDAP-UX Client Service with Micrsoft Windows 2000 Active Directory Administrator's Guide*"에서는 HP-UX ADS 클라이언트 구성에 대한 도움말을 제공합니다.

통합 도메인 구성 요소

Windows 200x ADS 구성원 서버 역할을 하는 HP CIFS

통합 도메인에서 작동하는 HP CIFS 구성원 서버는 UNIX용 서비스(SFU)에서 지원되는 ADS에 따라 다릅니다. SFU는 Windows SID 매핑에 필요한 UNIX UID 및 GID 관리를 제공합니다. SFU 및 해당 설명서는 *http://www.microsoft.com/windows/sfu*에서 다운로드할 수 있습니다. 모든 사용자 관리가 Windows 2000/2003 ADS 서버에 통합되므로 `winbind`가 필요하지 않으며 HP CIFS 구성원 서버 수에 관계없이 ID 일관성 문제가 발생하지 않습니다.

HP CIFS Server에서는 Windows 통합 도메인 설정에 Kerberos 보안을 사용합니다. Kerberos 보안을 사용하여 HP CIFS Server를 Windows 200x 도메인에 참여시키는 방법에 대한 자세한 내용은 5장, 123페이지의 “Windows 2000/2003 도메인”을 참조하십시오.

통합 도메인 모델 설정

UNIX용 Windows 서비스(SFU)를 사용하여 통합 도메인 모델을 배포하도록 다음 구성 요소를 설정 및 구성해야 합니다.

- ADS(Active Directory Service)를 사용하는 Windows 2000 또는 2003 도메인 컨트롤러
- HP CIFS 구성원 서버에 LDAP-UX Integration 소프트웨어 B.03.20 이상
- Windows 2000 또는 2003 도메인 컨트롤러에 SFU 3.5
- HP CIFS Server를 SFU 활성 Windows 200x 도메인에 설치, 구성 및 참여시킵니다. HP CIFS Server를 Windows 도메인에 구성 및 참여시키는 방법에 대한 자세한 내용은 5장, 123페이지의 “Windows 2000/2003 도메인”을 참조하십시오.

HP CIFS Server에 LDAP-UX 클라이언트 서비스 설정

통합 도메인 모델에서 HP CIFS 도메인 구성원 서버를 Windows 200x ADS와 통합하여 사용자 계정 데이터베이스 관리를 중앙 집중화합니다. HP LDAP-UX 통합 소프트웨어 B.03.20 이상을 설치하고 LDAP-UX 클라이언트를 구성해야 합니다. 이렇게 하면 ADS 디렉토리에 Posix 및 Windows 사용자 계정을 통합할 수 있습니다.

또한 Kerberos를 사용하여 사용자를 인증하도록 `/etc/krb5.conf` 파일을 구성해야 합니다.

HP CIFS Server에 LDAP-UX 클라이언트 서비스 설치 및 구성

다음에서는 LDAP-UX 클라이언트 서비스를 설치하고 구성하기 위해 수행해야 할 주요 단계에 대해 간략하게 설명합니다. Windows 2000 ADS와 함께 작동하도록 LDAP-UX 클라이언트 서비스를 설치 및 구성하는 방법에 대한 자세한 지침은 *http://docs.hp.com*에서 사용할 수 있는 *LDAP-UX Client Services with Microsoft Windows 2000 Active Directory Server Administrator's Guide*의 2장 "Installing LDAP-UX Client Services"를 참조하십시오.

단계 **1.** 각 HP CIFS 구성원 서버에 LDAP-UX 클라이언트 서비스를 설치합니다.

단계 **2.** 지원되는 이름 서비스 데이터를 디렉토리로 마이그레이션합니다. *http://docs.hp.com*에서 사용할 수 있는 *LDAP-UX Client Services with Microsoft Windows 2000 Active Directory Server Administrator's Guide*의 "Importing Name Serice Data into Your Directory" 절을 참조하십시오.

단계 **3.** Setup 프로그램을 실행하여 클라이언트 시스템에 LDAP-UX 클라이언트 서비스를 구성합니다. Setup 프로그램은 다음 작업을 수행합니다.

- 확장되어 있지 않은 경우 구성 프로파일 스키마를 사용하여 Active Directory 스키마를 확장합니다.
- 클라이언트에 시작 파일을 만듭니다. 이를 통해 각 클라이언트에서는 구성 프로파일을 다운로드할 수 있습니다.
- 한 클라이언트 그룹 또는 모든 클라이언트에서 공유하는 디렉토리 액세스 정보의 구성 프로파일을 디렉토리에 만듭니다.
- 디렉토리에서 클라이언트로 구성 프로파일을 다운로드합니다.
- 제품 데몬 `ldapclientd`를 시작합니다.

단계 **4.** 클라이언트의 `/etc/pam.conf` 및 `/etc/nsswitch.conf` 파일을 수정하여 각각 Kerberos 인증 및 LDAP 이름 서비스를 지정합니다.

Kerberos를 사용하여 인증하도록 /etc/krb5.conf 구성

HP CIFS Server에서 Kerberos 구성 파일 /etc/krb5.conf를 만들어 이 파일에서 기본 영역, KDC(Key Distribution Center) 서버 및 로깅 파일 이름을 지정합니다. Kerberos 클라이언트는 영역의 KDC를 저장하는 구성에 따라 다릅니다. 다음은 CIFSW2KSFU.ORG.HP.COM이라는 영역과 KDC 역할을 하는 hostA.org.hp.com 시스템이 있는 /etc/krb5.conf의 예제입니다.

```
[libdefaults]
  default_realm = CIFSW2KSFU.ORG.HP.COM  #Samba Domain
  default_tkt_enctypes = DES-CBC-CRC
  default_tgs_enctypes = DES-CBC-CRC
  ccache_type = 2
[realms]
  CIFSW2KSFU.ORG.HP.COM = {
         kdc = hostA.org.hp.com:88
        admin_server = hostA.org.hp.com
}

[domain_realm]
  .org.hp.com = CIFSW2KSFU.ORG.HP.COM
```

[logging]

```
   kdc = FILE: /var/log/krb5kdc.log
  admin_server = FILE:/var/log/kadmin.log
  default = FILE:/var/opt/KRB5lib.log
```

Window 2000 또는 2003 도메인 컨트롤러에 SFU 3.5 설치

POSIX 계정에는 사용자 ID, 로그인 셸 및 홈 디렉토리 같이 Windows 2000 또는 2003에서 사용되지 않는 속성이 있습니다. Active Directory를 HP-UX 사용자의 데이터 저장소로 사용하려면 Windows 2000 또는 2003 도메인 컨트롤러에 SFU 버전 3.5를 설치해야 합니다. SFU는 Active Directory 스키마를 확장하여 POSIX 스키마를 포함하는 데 사용됩니다. SFU 3.5에 대한 자세한 설치 지침은 *http://docs.hp.com*에서 사용할 수 있는 *LDAP-UX Client Services with Windows 2000 Active Directory Server Administrator's Guide*의 2장 "Installing LDAP-UX Client Services"를 참조하십시오.

SFU에 대한 자세한 내용은 Microsoft 웹 사이트(*http://www.microsoft.com/windows2000/sfu/*)를 참조하십시오.

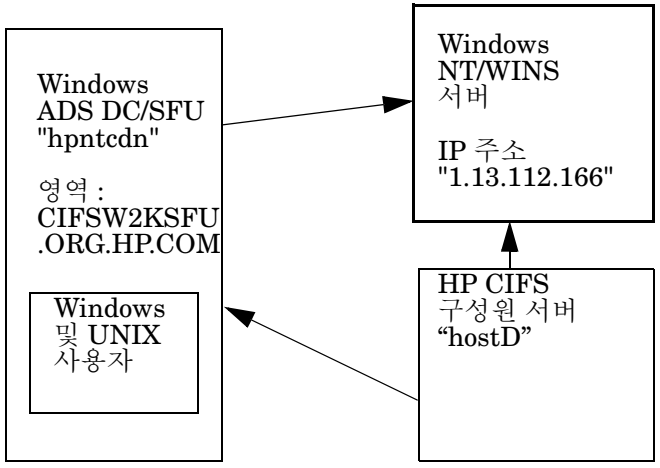
참고

Windows 2000 또는 2003 도메인 컨트롤러에 SFU를 설치하기 전에 HP CIFS 구성원 서버에 LDAP-UX 클라이언트 서비스 소프트웨어를 설치해야 합니다.

통합 도메인 모델의 예제

그림 9-10에서는 `HPCIFSW2KSFU.ORG.HP.COM`이라는 영역, ADS 도메인 컨트롤러 시스템 `hpntcdn`, 구성원 서버 역할을 하는 HP CIFS Server 시스템 `hostD` 및 WINs 서버 역할을 하는 Windows NT 시스템(IP 주소: `1.13.112.166`)이 있는 통합 도메인 모델의 예제를 보여 줍니다.

그림 9-10 통합 도메인의 예제



HP CIFS 구성원 서버에 대한 샘플 smb.conf 파일

다음은 그림 9-10에 표시된 샘플 통합 도메인 모델의 ADS 구성원 서버 역할을 하는 HP CIFS Server 시스템 hostD에 사용되는 샘플 Samba 구성 파일인 /etc/smb.conf입니다.

```
########################################################
#
# An sample smb.conf file for an HP CIFS ADS member server
#
# Global Parameters
[global]
workgroup = CIFSW2KSFU    # Domain Name
server string = CIFS Server as a domain member
realm = CIFSW2KSFU.ORG.HP.COM
security = ADS
netbios name = hostD
security = ads
local master = no
wins server = 1.12.112.166
log fie = /var/opt/samba/log.%m
short preserve case = no
dos filetime resolution = yes
read only = no
#
[homes]
comment = Home Directory
browseable = No
#
[tmp]
comment = temporary file space
path = /tmp
```

샘플 /etc/krb5.conf 파일

ADS 구성원 서버 역할을 하는 HP CIFS Server에서 Kerberos 구성 파일 /etc/krb5.conf를 만듭니다. 이 파일에서 영역 이름, KDC(Key Distribution Center) 서버의 위치 및 로깅 파일 이름을 지정합니다.

다음은 CIFSW2KSFU.ORG.HP.COM 영역 및 KDC 역할을 하는 hpntcdn.org.hp.com 시스템이 있는 샘플 /etc/krb5.conf입니다.

```
# Kerberos Configuration                                        #
#                                                               #
# This krb5.conf file is intended as an example only.           #
# See krb5.conf(4) for more details.                            #
```

```
#
# Please verify that you have created the directory /var/log.#
#                                                           #
# Replace HPCIFSW2KSFU.ORG.HP.COM with your kerberos Realm.  #
# Replace hpntcdn.org.hp.com with your Windows ADS DC full   #
# domain name.                                              #
#                                                           #
[libdefaults]
default_realm = HPCIFSW2KSFU.ORG.HP.COM
default_tkt_enctypes = DES-CBC-CRC
default_tgs_enctypes = DES-CBC-CRC
ccache_type = 2

[realms]
CIFSW2KSFU.ORG.HP.COM = {
kdc = hpntcdn.org.hp.com:88
admin_server = hpntcdn.org.hp.com
}
[domain_realm]
.org.hp.com = CIFSW2KSFU.ORG.HP.COM

[logging]
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmin.log
default = FILE:/var/log/krb5lib.log
```

참고

서버 필드에 :88이 필요합니다.

샘플 /etc/nsswitch.conf 파일

통합 도메인 모델에서 LDAP 이름 서비스 및 사용하려는 기타 이름 서비스를 지정하도록 /etc/nsswitch.conf 파일을 구성해야 합니다.

다음은 그림 9-10에 표시된 샘플 통합 도메인 모델에 사용되는 샘플인 /etc/nsswitch.conf입니다.

```
# /etc/nsswitch.conf                                    #
#                                                       #
# This sample file uses Lightweigh Directory Access     #
# Protocol(LDAP) in conjunction with dns and files.     #
passwd:    files ldap
```

```
group:      files ldap
hosts:      dns [NOTFOUND=return] files ldap
networks:   files ldap
protocols:  files ldap
rpc:        files ldap
publickey:  files
netgroup:   files ldap
automount:  files
aliases:    files
services:   files ldap
```

10 HP CIFS Server 보안

이 장에서는 HP CIFS Server를 보호하는 데 사용할 수 있는 네트워크 보안 방법을 설명합니다. 이 장에는 다음 절이 포함됩니다.

- 259페이지의 “HP 보안 정보 자동 수신”

보안 보호 방법

HP CIFS Server에서는 유연한 네트워크 보안 방법을 제공하고 Microsoft Windows 파일 및 인쇄 서비스를 보다 안전하게 지원하기 위한 프로토콜을 구현합니다.

host-based protection을 사용하여 로컬 네트워크 외부에서 시작되는 연결로부터 HP CIFS Server를 보호할 수 있습니다. 또한 interface-based exclusion을 사용하여 SMBD가 특정 허용 인터페이스에만 바인딩되도록 할 수도 있습니다. 특정 공유 또는 리소스 기반 제외를 설정할 수도 있습니다. 예를 들면, IPC$ 공유에 특정 거부를 설정할 수 있습니다.

HP CIFS Server를 보호하기 위해 공유에 대한 액세스 제어 목록(ACL)에서 액세스 제어 항목(ACE)을 설정할 수도 있습니다.

네트워크 액세스 제한

호스트 기반 제한, 인터페이스 기반 보호, 방화벽 또는 IPC$ 공유 기반 거부를 사용하면 네트워크 액세스를 제한하고 HP CIFS Server를 보호할 수 있습니다. 이 절에서는 이러한 보호 방법을 구성하고 사용하는 방법에 대해 설명합니다.

호스트 제한 사용

대부분의 설치에서 서버 보안에 대한 위협은 인접한 네트워크 외부에서 들어옵니다. 기본적으로 HP CIFS Server는 모든 호스트의 연결을 받아들이므로 smb.conf 구성 파일의 hosts allow 및 hosts deny 옵션을 설정하여 특정 범위의 호스트에 대해서만 서버 액세스를 허용하도록 설정할 수 있습니다.

예제

다음 구성 예제에서는 "localhost"(사용자의 고유 컴퓨터)와 두 개의 개인 네트워크(192.168.2 및 192.168.3)로부터만 SMB 연결을 허용합니다. 다른 모든 연결은 클라이언트가 첫 번째 패킷을 보내자 마자 거부됩니다. 거부 메시지는 not listening on called name 오류로 표시됩니다.

```
hosts allow = 127.0.0.1 192.168.2.0/24 192.168.3.0/24
hosts deny = 0.0.0.0/0
```

인터페이스 보호 사용

기본적으로 HP CIFS Server에서는 시스템에서 검색되는 네트워크 인터페이스의 연결을 받습니다. 이는 ISDN 회선 또는 PPP 연결을 통해 인터넷에 연결된 경우 HP CIFS Server는 이러한 연결 상의 연결을 받을 수 있음을 의미합니다. `interface` 구성 옵션을 사용하면 인터페이스 동작을 변경할 수 있습니다.

인터페이스 보호 예제

예를 들면, 다음과 같이 옵션을 사용하여 인터페이스 동작을 변경할 수 있습니다.

```
interface = lan* lo0
bind interface only = yes
```

위의 예제에서 HP CIFS Server는 `lan0`, `lan1`과 같이 `lan`으로 시작하는 이름의 인터페이스와 `lo0`이라는 루프백 인터페이스 상의 연결만 수신합니다. 사용하는 데 필요한 인터페이스 이름은 사용하고 있는 OS에 따라 다릅니다. LAN 인터페이스를 사용하고 있을 때 누군가가 "`ppp0`"이라는 PPP 인터페이스 상에서 호스트와의 SMB 연결을 시도하는 경우 연결을 시도하던 사용자는 TCP 연결 거부 응답을 받게 됩니다.

방화벽 사용

방화벽을 사용하면 네트워크 외부 노출을 원하지 않는 서비스에 대해 액세스를 거부할 수 있습니다. 따라서 방화벽은 매우 효과적인 보호 방법이라 할 수 있습니다. 그러나 어떠한 이유로 방화벽이 활성화되지 않은 경우에는 위에서 언급한 방법을 사용할 수도 있습니다.

방화벽을 설정할 때는 허용할 TCP 및 UDP 포트를 알아야 합니다. HP CIFS Server에서는 다음 포트를 사용합니다.

```
UDP/137 - used by nmbd
UDP/138 - used by nmbd
TCP/139 - used by smbd
TCP/445  - used by smbd
```

포트 445는 중요한 포트로서, 이전의 여러 방화벽 설치에서는 이 포트를 인식할 수 없었으며 최근 몇 년 사이의 프로토콜에만 이 포트가 추가되었습니다.

IPC$ 공유 기반 거부 사용

또한 IPC$ 공유에 대해 보다 구체적인 거부를 사용할 수도 있습니다. 이렇게 하면 신뢰할 수 없는 호스트로부터의 IPC$ 공유 액세스를 거부하면서 다른 공유에 대한 액세스를 제공할 수 있습니다.

예를 들면, 다음과 같이 IPC$ 공유를 구성할 수 있습니다.

```
[ipc$]
hosts allow = 192.168.115.0/24 127.0.0.1
hosts deny = 0.0.0.0/0
```

이 구성은 HP CIFS Server에서 로컬 호스트와 로컬 서브넷을 제외한 다른 곳의 IPC$ 연결을 받지 못하도록 합니다. IPC$ 공유는 항상 익명으로 액세스할 수 있는 유일한 공유이므로, 이 구성은 호스트의 유효한 사용자 이름 및 암호를 모르는 공격자에 대해 일정 수준의 보호 기능을 제공합니다.

이 방법을 사용하는 클라이언트가 IPC$ 공유에 액세스하려 할 경우 `access denied` 응답을 받게 됩니다. 다시 말해서 이는 이러한 클라이언트에서 공유를 검색할 수 없으며 다른 리소스에 액세스할 수 없음을 나타냅니다.

중요 정보 보호

이 절에서는 중요 정보를 보호하는 데 사용할 수 있는 보안 방법에 대해 설명합니다.

인증 암호화

인증하는 동안 네트워크로 암호가 전송될 때 암호화를 사용하려면 `smb.conf` 파일의 `encrypt password` 매개 변수를 **yes**로 설정해야 합니다.

HP CIFS Server에서는 클라이언트 설정에 따라 `LM`, `NTLM` 및 `NTLMv2` 암호화 인증 방법을 사용합니다. `NTLMv2`가 가장 안전합니다. `NTLMv2` 인증을 사용하려면 다음 클라이언트 레지스트리 키를 구성해야 합니다.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
“lmcompatibilitylevel”=dword:00000003
```

`0x00000003` 값은 `NTLMv2` 응답만 전송함을 의미합니다.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\ /
MSV1_0]
"NtlmMinClientSec"=dword:00080000
```

`0x00080000` 값은 `NTLMv2` 세션 보안만 허용함을 의미합니다. `NtlmMinClientSec` 또는 `NtlmMinServerSec` 옵션이 **0x00080000**으로 설정된 경우에는 `NTLMv2` 세션 보안이 협상되지 않으면 연결이 실패합니다.

인증을 위해 LDAP(Lightweight Directory Access Protocol)도 사용할 수 있습니다. LDAP 디렉토리를 사용하여 일반 텍스트 암호 전송을 방지하려면 시스템에 SSL(Secure Socket Layer)을 구성하고 SSL을 지원하도록 HP CIFS Server를 활성화하면 됩니다. LDAP 상에서 SSL 통신을 활성화하는 방법에 대한 자세한 내용은 6장, 131페이지의 “LDAP 통합 지원”을 참조하십시오.

HP CIFS Server에서는 Windows 2000 Active Directory 구성을 위한 높은 보안 수준의 Kerberos 티켓을 사용합니다.

중요 구성 파일 보호

HP CIFS Server 구성 파일의 기본 권한은 적절한 액세스 가능성을 제공하면서 보안을 유지할 수 있도록 신중히 선택되었습니다. 그러나 무단 액세스로부터 이러한 구성 파일을 보호할 수 있어야 합니다. 특히 이러한 구성 파일을 다른 디렉토리에 저장하려는 경우에는 각별히 주의하십시오.

표 6-1은 일반적으로 사용되는 구성 파일 및 기본 위치의 목록을 제공합니다. 이러한 파일과 여러 매개 변수의 대체 위치를 허용하여 여기에 언급되지 않은 런타임 작업을 제어하는 추가 구성 파일이나 스크립트를 만드는 여러 개의 `smb.conf` 구성 매개 변수가 있습니다.

표 10-1 **구성 파일**

파일	설명
`/etc/opt/samba/smb.conf`	마스터 구성 파일
`/var/opt/samba/log.*`	로그 파일
`/var/opt/samba/locks/*.tdb`	중요한 내부 런타임 정보를 포함하는 데이터베이스 파일
`/var/opt/samba/locks/*.dat`	시스템 이름 및 주소를 포함하는 데이터 파일
`/var/opt/samba/locks/*.pid`	스크립트 시작, 중지 및 클러스터에 사용되는 마스터 데몬 프로세스 ID
`/var/opt/samba/private/*.tdb`	중요한 내부 런타임 정보를 포함하는 데이터베이스 파일

표 10-1 구성 파일(계속)

파일	설명
/var/opt/samba/private/smbpasswd	사용자 이름 및 암호 정보를 포함하는 데이터 파일
/var/opt/samba/private/passdb.tdb	사용자 이름 및 암호 정보를 포함하는 데이터 파일
/opt/samba/LDAP/smbldap-tools/smbldap_conf.pm	LDAP 관리자 사용자 및 암호를 일반 텍스트로 보관하는 데 사용되는 데이터 파일

smbpasswd -w 명령은 일반 텍스트로 /var/opt/samba/private/secrets.tdb 파일에 LDAP 관리자 사용자 및 암호를 저장합니다.

%m 이름 바꾸기 매크로 사용 시 주의

원격 클라이언트의 NetBIOS 이름은 smb.conf 구성 파일에 나타날 때마다 "%m" 매크로로 대체됩니다. 의도했던 Samba 디렉토리 외부의 파일 경로에서 고안된 NetBIOS 이름이 사용될 수 있습니다. 따라서 Samba에서 중요 시스템 파일에 데이터를 추가함으로써 서버의 보안을 손상시킬 수도 있습니다.

이 문제의 즉각적인 해결 방법은 smb.conf 구성 파일을 편집하여 매크로 "%m"의 모든 항목을 제거하는 것입니다. 각 사이트의 요구 사항에 따라 다른 smb.conf 매크로로 적절히 대체될 수 있습니다.

log file 옵션은 재정의 문제에 매우 취약합니다. 샘플 구성 파일에는 /var/opt/samba/log.%m 경로가 포함되어 있습니다. 이 기본 경로를 사용하면 접두사 "log"로 시작하는 /var/opt/samba 하위 디렉토리가 존재하지 않는 한 취약성이 만들어지지 않습니다.

log file 옵션에서 "%m" 매크로를 그대로 두려는 경우 기본값 /var/opt/samba/log.%m을 사용해야 합니다.

스택에 대한 실행 권한 제한

시스템 중단을 일으키는 일반적인 방법은 비정상적으로 긴 명령줄 인수를 권한이 필요한 프로그램(이와 같은 긴 명령줄 인수를 예상하지 못함)으로 전달하는 등 프로그램 스택에 대해 악의적으로 버퍼 오버플로를 일으키는 것입니다. 악의적이며 권한이 없는 사용자는 이 기술을 사용하여 권한이 부여된 프로그램을 슈퍼유저 셸로 시작하거나 이와 유사한 무단 작업을 수행할 수 있습니다.

이러한 유형의 공격으로부터의 위험을 줄이기 위한 효과적인 방법 중 하나는 프로그램의 스택 페이지에서 실행 권한을 제거하는 것입니다. 이렇게 하면 성능에 영향을 주지 않고 시스템 보안을 향상시킬 수 있으며 대부분의 합법적인 응용 프로그램에 악영향을 미치지 않습니다.

HP CIFS Server에서는 스택에 대한 실행이 필요하지 않습니다. HP CIFS Server에서 버퍼 오버플로 가능성을 방지하는 동안 HP-UX 커널 튜너블 매개 변수 `executable_stack`을 설정하여 스택 실행을 방지함으로써 악의적인 공격으로부터 보호할 수 있습니다. 자세한 내용은 `chatr`의 맨페이지를 참조하십시오.

사용자 액세스 제한

인증 서비스 외에도, HP CIFS Server는 `smb.conf` 파일에 구성 매개 변수인 `valid users` 및 `invalid users`를 제공합니다. 이 매개 변수를 사용하면 CIFS Server에 대한 액세스를 제한할 수 있습니다. 이 매개 변수와 함께 나열된 사용자에게만 관리 기능을 제공하도록 `admin users` 매개 변수를 구성하여 사용을 제한할 수 있습니다.

예를 들면, 다음과 같이 `smb.conf` 파일의 `valid users` 옵션을 구성할 수 있습니다.

```
[global]
valid users = @smbusers, jack
```

이렇게 하면 모든 서버 액세스가 `jack`이라는 사용자와 시스템 그룹 `smbusers`의 구성원으로 제한됩니다.

HP 보안 정보 자동 수신

서비스에 가입하여 전자 메일을 통해 HP IT 리소스 센터(ITRC)에서 HP 보안 정보 또는 기타 기술적인 자료를 자동으로 받아볼 수 있습니다.

다음 단계에 따라 HP Security Bulletins(보안 정보)에 등록하고 가입합니다.

단계 **1.** 브라우저를 사용하여 다음 HP IT 리소스 센터 웹 사이트(*http://itrc.hp.com*)로 이동합니다.

단계 **2.** 기존 로그인을 사용하거나 **Register** 단추를 사용하여 ITRC의 여러 영역에 액세스할 수 있는 로그인을 만듭니다. 사용자 ID와 암호를 반드시 저장하십시오.

단계 **3.** `Notification` 섹션(페이지 하단) 아래에 있는 **Support Information Digests** 옵션을 선택합니다.

단계 **4.** 향후 HP 보안 정보 및 기타 기술 자료를 받아 보려면 해당 자료의 확인란을 클릭한 후 **Update Subscriptions(가입 업데이트)** 단추를 누릅니다.

이미 발표된 정보를 보려면 해당 자료의 링크를 선택합니다.

다음 위치에서 ITRC 계정 보안 정보를 찾을 수 있습니다.
http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin

단계 **5.** 보안 패치 구조도에 액세스하려면 "Security Bulletins Archive(보안 정보 아카이브)" 링크를 선택합니다. 아카이브에서 세 번째 링크가 현재의 보안 패치 구조도의 링크입니다. 이 구조도는 플랫폼/OS 릴리즈 및 정보 항목별로 보안 패치를 분류합니다.
`Security Patch Check` 도구는 HP-UX 11i v1 및 v2 시스템에 대한 패치 구조도를 검토하는 프로세스를 완벽하게 자동화합니다.

`Security Patch Check` 도구는 수정 사항이 별도의 수동 작업이 필요하지 않은 패치 안에 완벽하게 구현되어 있을 때, 보안 정보가 HP-UX 11i v1 및 v2 시스템에 구현되었는지 확인할 수 있습니다. `Security Patch Check` 도구는 제품 업그레이드를 사용하여 구현된 수정 사항을 확인할 수 없습니다.

Security Patch Check 도구에 대한 자세한 내용은 다음 웹 사이트를 참조하십시오.
http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA

보안 패치 구조도는 다음 위치의 익명 ftp 사이트를 통해서도 사용할 수 있습니다.
ftp://ftp.itrc.hp.com/export/patches/hp-ux_patch_matrix/

새로운 보안 취약성 보고

전자 메일을 *security-alert@hp.com*으로 전송하여 새로운 보안 취약성을 보고할 수 있습니다.

보안 경고 PGP 키를 사용하여 정보를 암호화한 후 사용해야 합니다. 이 키는 로컬 키 서버에서 받거나 *security-alert@hp.com* 주소로 "get key"(따옴표 제외)라는 제목(본문 없이)으로 메시지를 보내서 받을 수 있습니다.

11 HA HP CIFS 구성

HA HP CIFS Server 개요

고가용성 HP CIFS Server를 사용하면 HP CIFS Server 제품을 MC/ServiceGuard 클러스터 노드에서 실행할 수 있습니다. MC/ServiceGuard를 사용하면 HP 9000 Server 컴퓨터의 고가용성 클러스터를 만들 수 있습니다.

HA HP CIFS Server를 설치하려면 먼저 MC/ServiceGuard 클러스터를 설치해야 합니다. MC/ServiceGuard 클러스터를 설치하는 방법은 **MC/ServiceGuard 관리** 설명서를 참조하십시오.

HA HP CIFS Server에서는 사용자 정의 가능한 구성, 제어 스크립트 및 모니터 스크립트를 제공합니다. 이러한 스크립트와 이 README 파일은 */opt/samba/HA* 디렉토리에 있습니다. 이 샘플 스크립트는 각 환경에 맞게 사용자 정의할 수 있습니다.

README 파일과 */opt/samba/HA*의 파일은 활성-대기 또는 활성-활성 HA 구성에 적용됩니다.

권장 클라이언트

HA HP CIFS Server용 권장 클라이언트는 Windows 2000, XP SP1, XP SP2, Windows 터미널 서버(NT4 및 2000) 및 HP CIFS Client입니다. DOS/Windows 3.1 LM 2.2C 및 Windows for Workgroups 등과 같은 기존 클라이언트는 HA HP CIFS Server 전환 시 발생하는 HP CIFS Server 중지 및 네트워크 연결 종료에 제대로 응답하지 못할 수 있습니다.

사용할 때 주의해야 할 점은 이 절 뒷부분의 "HA HP CIFS Server 특별 주의 사항" 절을 참조하십시오.

고가용성 HP CIFS Server 설치

구성에서는 HA HP CIFS Server를 모든 클러스터 노드에 설치 및 구성해야 합니다. 모든 클러스터 노드는 '기본' 노드의 역할을 하면서 동시에 다른 노드에 대한 '대체' 노드 역할을 할 수 있습니다(반드시 필요한 것은 아님). 장애 조치가 없는 경우 각 클러스터 노드는 패키지 중 하나를 실행합니다. 장애 조치가 발생하면 클러스터 노드는 원래 패키지 외에 실패한 패키지를 선택합니다.

고가용성 HP CIFS Server 패키지를 만들기 전에, 먼저 **MC/ServiceGuard 관리** 설명서의 지침에 따라 MC/ServiceGuard 클러스터를 설치해야 합니다.

설치 방법은 다음과 같습니다.

1. 지침에 따라 디스크 하드웨어를 고가용성 방식으로 구성합니다.
2. SAM 또는 LVM 명령이나 VxVM 명령을 사용하여, 장애 발생 시 기본 및 대체 클러스터 노드에서 사용할 데이터에 필요한 볼륨 그룹, 논리 볼륨 및 파일 시스템을 설정합니다.

HA HP CIFS Server 설치

1. SD를 사용하여 모든 클러스터 노드에 HP CIFS Server를 설치합니다. 두 노드에 HP CIFS Server를 이미 설치 및 구성한 경우에는 `/opt/samba/bin/stopsmb` 명령으로 HP CIFS Server를 중지하고 단계 4로 넘어갑니다.
2. 첫 번째 노드에서 다음을 수행합니다.

   /opt/samba/bin/samba_setup 스크립트를 실행하여 Samba 서버를 구성합니다. HA HP CIFS Server의 서버 이름과 도메인/작업 그룹 이름을 입력합니다.
3. 두 번째 노드에서 다음을 수행합니다.

   /opt/samba/bin/samba_setup 스크립트를 실행하여 두 번째 노드를 구성합니다. 첫 번째 노드에 지정한 것과 동일한 도메인/작업 그룹 이름을 지정해야 합니다. 서버 이름은 다르게 지정하십시오.
4. CIFS Client 인증에 사용되는 UNIX 사용자의 이름, 사용자 ID 번호, 주 그룹 및 암호는 두 노드 모두에서 동일해야 합니다.

   이는 활성-활성 구성의 두 Samba 서버에서 인증을 받아야 하는 모든 사용자에 대해 필수 사항입니다. 즉, 두 Samba 서버에 사용되는 모든 사용자 이름의 사용자 ID, 주 그룹 ID 및 암호는 두 클러스터 노드에서 서로 동일해야 합니다. 동일하지 않은 경우에는 Samba를 이 MC/ServiceGuard 클러스터의 활성-활성 서버로 사용할 수 없습니다.
5. */etc/rc.config.d/samba* 파일의 RUN_SAMBA 및 RUN_WINBIND 매개 변수가 두 노드에서 모두 0으로 설정되어 있는지 확인합니다.

고가용성 HP CIFS Server 구성

소개

MC/Serviceguard 패키지를 구성하려면 먼저 HP CIFS Server에서 활성-활성 구성이 지원되는 방식을 이해해야 합니다.

HP CIFS Server에서는 NetBIOS 및 SMB 마스터 데몬의 인스턴스가 여러 개 존재할 수 있습니다.

각 CIFS Server마다 해당 서버의 동작을 정의하는 고유한 smb.conf 파일이 있습니다. 클라이언트가 연결하는 NetBIOS 이름 및 IP 주소를 사용하여 연결에 사용할 smb.conf 파일을 결정합니다. HP CIFS는 이러한 다중 CIFS 마스터 데몬 구성을 통해 동시에 여러 MC/ServiceGuard 패키지를 실행할 수 있습니다.

장애 조치가 발생하면 MC/ServiceGuard는 장애가 있는 클러스터 노드의 IP 주소를 다른 노드로 전송합니다. MC/ServiceGuard는 패키지를 장애 클러스터 노드에서 다른 노드로 이동하면서 나머지 노드에서 적절한 CIFS Server를 활성화합니다. 이제 장애 노드로 전송되던 모든 트래픽은 전환된 IP 주소를 사용하여 다른 활성 노드로 향하게 됩니다. 여기서 중요한 점은 CIFS Server를 원래의 노드에서 실행되던 CIFS Server처럼 작동하도록 구성하는 것입니다.

특정 CIFS Server 이름(NetBIOS 이름)을 통해서만 CIFS 공유에 액세스할 수 있도록 설정하면 모든 시스템이 작동하는 동안 각 시스템 간 로드의 균형을 조정할 수 있습니다. 서버를 구성하는 동안 CIFS 공유 및 디렉토리를 논리 볼륨에 연결할 때 이 점을 염두에 두십시오.

각 클러스터 노드가 Samba 서버(패키지)에 연결하는 모든 UNIX 사용자를 알고 있어야 합니다. 즉, `/etc/passwd` 파일을 업데이트해야 할 수도 있습니다. NIS 설치에서는 새 passwd 또는 group 파일이 있는 경우 `ypmake`나 비슷한 도구를 사용하여 새 맵을 생성할 수 있습니다. LDAP 설치의 경우에는 LDAP-UX 통합 제품에서 제공되는 마이그레이션 도구를 사용하여 새 계정의 LDAP 데이터를 생성할 수 있습니다. 이 도구는 `/opt/ldapux/migrate`에 있으며 관련 설명은 http://docs.hp.com/hpux/internet의 *LDAP-UX Client Services Administrator's Guide*에 있습니다.

지침

다음은 MC/ServiceGuard 패키지 중 하나에 대한 지침입니다. 모든 CIFS Server 패키지(노드당 하나)마다 이 단계를 거쳐야 합니다. 그런 다음 모든 파일을 클러스터의 모든 노드로 복사해야 합니다.

작업이 완료되면 각 HP-UX 시스템에는 클러스터의 각 노드에 대해 고유한 이름을 사용하는 패키지가 만들어집니다. 장애 조치가 발생하기 전까지는 자체 패키지만 활성화됩니다.

예를 들면, 3개의 노드로 구성된 클러스터가 있다면 3개의 HPUX 시스템마다 각각 3개의 패키지가 있습니다.

클러스터 디렉토리는 다음 3개입니다.

1. /etc/cmcluster/samba/pkg1
2. /etc/cmcluster/samba/pkg2
3. /etc/cmcluster/samba/pkg3

구성 파일은 다음 3개입니다.

1. /etc/opt/samba/smb.conf.pkg1
2. /etc/opt/samba/smb.conf.pkg2
3. /etc/opt/samba/smb.conf.pkg3

디렉토리는 다음 3개입니다.

1. /var/opt/samba/pkg1
2. /var/opt/samba/pkg2
3. /var/opt/samba/pkg3

여기에는 잠금 및 로그 파일이 저장됩니다.

대부분의 구성에서는 동적 보안 및 데이터 파일을 공유 디스크에 설정하고 유지하는 것이 더 쉽습니다. 따라서 예제에 사용된 */var/opt/samba/<package name>* 경로를 공유 디스크에 만드는 것이 좋을 수도 있습니다.

MC/ServiceGuard 클러스터의 각 CIFS 패키지에 대해 다음 작업을 수행하십시오.

1. 다음과 같은 디렉토리를 만듭니다.

/var/opt/samba/<package name>
/var/opt/samba/<package name>/locks
/var/opt/samba/<package name>/logs
/var/opt/samba/<package name >/private

여기서 *<package name>*은 CIFS 서버의 클러스터 패키지 이름입니다. 예를 들면 다음과 같습니다.

```
$mkdir /var/opt/samba/pkg1
$mkdir /var/opt/samba/pkg1/locks
$mkdir /var/opt/samba/pkg1/logs
$mkdir /var/opt/samba/pkg1/private
```

이 경로는 MCServiceGuard 클러스터 스크립트인 samba.cntl 및 samba.mon이 참조하므로 이 단계는 매우 중요합니다.

2. */etc/opt/samba/smb.conf.<package>* 파일
(예제: */etc/opt/samba/smb.conf.pkg1*)을 만들어 다음 행을 입력합니다.

```
[global]
  workgroup = ha_domain
  netbios name = ha_server1
  interfaces = XXX.XXX.XXX.XXX/xxx.xxx.xxx.xxx
  bind interfaces only = yes
   # g
   # with "log." if you plan to use "%m" this way
  log file = /var/opt/samba/pkg1/logs/log.%m
  lock directory = /var/opt/samba/pkg1/locks
   pid directory = /var/opt/samba/pkg1/locks
   smbpasswd file = /var/opt/samba/pkg1/private/smbpasswd
```

여기서 "XXX.XXX.XXX.XXX/xxx.xxx.xxx.xxx"는 MC ServiceGuard 패키지에의 변동 가능한 IP 주소 및 서브넷 마스크로 대체합니다.

설치 시 */opt/samba/bin/samba_setup*을 실행한 경우 다음을 수행합니다.

- */etc/opt/samba/smb.conf* 파일에서 작업 그룹 행을 가져옵니다. 원하는 나머지 구성 항목에 추가합니다.
- NetBIOS 이름 행 역시 같은 파일에서 가져오고, NetBIOS 이름 행이 없는 경우 NetBIOS 이름 행에 서버의 UNIX 호스트 이름을 입력합니다.
- 공유 경로를 만들 때는 로드 균형 조정의 사용을 고려하십시오.

- smbpasswd 및 개인 파일을 공유 볼륨에 두어야 하는지 여부 등을 고려하십시오. 이 절 끝부분에 있는 "HA HP CIFS Server 특별 주의 사항"을 참조하십시오. SWAT 또는 smbpasswd 유틸리티를 실행하는 경우에는 유틸리티가 smb.conf.<package name> 구성이 아닌 smb.conf에서 작동한다는 점을 기억해야 합니다. 따라서 smb.conf.<package name>을 smb.conf에 복사하는 것이 좋을 수도 있습니다. 도메인을 결합하려면 도메인 보안 구성에서 'net join'을 실행해야 합니다. 이 명령은 secrets.tdb 파일을 업데이트하기 때문에 개인 디렉토리(smb.conf에서 "smb passwd file"로 구성)의 정확한(공유 논리 볼륨 가능) 경로로 smb.conf를 업데이트한 후에 이 단계를 수행해야 합니다.

  파일 이름이 모두 소문자로 되어 있는지 확인합니다 (예제: */etc/opt/samba/smb.conf.PKG1*이 아닌 */etc/opt/samba/smb.conf.pkg1*). 파일 이름에 대문자를 사용하면 장애 조치가 올바르게 작동하지 않습니다.

3. 관련 데이터를 모두 HP CIFS Server 패키지 공유 볼륨으로 이동합니다.

   HP CIFS Server를 사용하여 액세스할 모든 디렉토리 및 파일로 구성된 관련 데이터는 공유 볼륨에 있어야 합니다. 이 데이터에는 사용자가 만든 공유도 포함됩니다. 예를 들면, HP CIFS Server 관리자가 TEST=c:/tmp/test 공유를 만들었다면 */tmp/test*의 모든 데이터는 공유된 논리 볼륨에 있어야 합니다.

   다음은 필수 HP CIFS Server 디렉토리의 데이터를 볼륨 그룹 *vg01*의 논리 볼륨으로 복사하는 경우의 예제입니다. 이 예제는 *pkg2*에도 적용됩니다.

   ```
   mkdir /tmp/share1 /tmp/share2
   mount /dev/vg01/lvol1 /tmp/share1
   mount /dev/vg01/lvol2 /tmp/share2
   cp -r /your/data1/* /tmp/share1
   cp -r /your/data2/* /tmp/share2
   umount /tmp/share1
   umount /tmp/share2
   rm -rf /tmp/share1 /tmp/share2
   ```

4. HP CIFS Server 클러스터 패키지를 위한 디렉토리를 만듭니다.

   ```
   mkdir /etc/cmcluster/samba/pkg1
   ```

5. 샘플 스크립트 *samba.conf, samba.cntl* 및 *samba.mon*을 */opt/samba/HA*에서 주 노드의 */etc/cmcluster/samba/pkg1*(또는 */etc/cmcluster/samba/pkg2*)로 복사합니다. 모든 스크립트를 쓰기 가능으로 설정합니다.

   ```
   cp /opt/samba/HA/samba.* /etc/cmcluster/samba/pkg1
   chmod 666 samba.conf samba.cntl samba.mon
   ```

6. 샘플 스크립트를 현재의 MC/ServiceGuard 구성에 맞게 사용자 정의합니다. 다음 샘플은 HA HP CIFS Server 패키지의 구성, 제어 및 모니터 스크립트를 사용자 정의한 것입니다.

7. 제어 스크립트(*samba.cntl*) 및 모니터 스크립트(*samba.mon*)는 실행 가능으로 설정해야 합니다.

   ```
   chmod 750 samba.cntl samba.mon
   ```

samba.conf 패키지 구성 파일을 편집

samba.conf 구성 파일을 구성하려면 다음 작업을 수행합니다.

1. PACKAGE_NAME 변수를 설정합니다.

   ```
   PACKAGE_NAME pkg1
   ```

   또는

   ```
   PACKAGE_NAME pkg2
   ```

   현재 작업 중인 패키지에 따라 위의 두 가지 중 하나를 사용합니다.

2. 이 패키지를 실행할 각 노드에 대해 NODE_NAME 변수를 만듭니다. 첫 번째 NODE_NAME 변수에는 주 노드를 지정해야 합니다. 다른 모든 NODE_NAME 변수에는 대체 노드들을 실행 순서에 따라 지정해야 합니다.

   ```
   NODE_NAME   ha_server1
   NODE_NAME   ha_server2
   ```

   ...(pkg1의 경우),

   ```
   NODE_NAME   ha_server2
   NODE_NAME   ha_server1
   ```

   ...(pkg2의 경우) 등.

3. RUN_SCRIPT 및 HALT_SCRIPT 변수를 제어 스크립트의 전체 경로 이름으로 설정합니다.

```
RUN_SCRIPT /etc/cmcluster/samba/pkg1/samba.cntl
RUN_SCRIPT_TIMEOUT  NO_TIMEOUT
HALT_SCRIPT  /etc/cmcluster/samba/pkg1/samba.cntl
HALT_SCRIPT_TIMEOUT NO_TIMEOUT
```

...(pkg1의 경우),

```
RUN_SCRIPT /etc/cmcluster/samba/pkg2/samba.cntl
RUN_SCRIPT_TIMEOUT  NO_TIMEOUT
HALT_SCRIPT  /etc/cmcluster/samba/pkg2/samba.cntl
HALT_SCRIPT_TIMEOUT NO_TIMEOUT
```

...(pkg2의 경우) 등.

4. SERVICE_NAME 변수를 samba_mon으로 설정합니다.

```
SERVICE_NAME  samba_mon1
SERVICE_FAIL_FAST_ENABLED  NO
SERVICE_HALT_TIMEOUT       300
```

...(pkg1의 경우),

```
SERVICE_NAME  samba_mon2
SERVICE_FAIL_FAST_ENABLED  NO
SERVICE_HALT_TIMEOUT       300
```

...(pkg2의 경우) 등.

5. 다음 예제처럼 SUBNET 변수를 패키지를 모니터링할 서브넷으로 설정합니다.

```
SUBNET 1.13.2.0
```

samba.cntl 제어 스크립트를 편집

samba.cntl 제어 스크립트 파일을 구성하려면 다음 작업을 완료해야 합니다.

1. HP CIFS Server 디렉토리에 대해 논리 볼륨 그룹 또는 VxVM 볼륨 그룹으로 볼륨 그룹을 만듭니다. 예를 들면 다음과 같습니다.

```
VG[0]=/dev/vg01      # LVM 볼륨 그룹의 경우
DG[0]=/dev/vx/dg01   # VxVM 볼륨 그룹의 경우
```

...(pkg1의 경우),

```
VG[0]=/dev/vg02       # LVM 볼륨 그룹의 경우
DG[0]=/dev/vx/dg02    # VxVM 볼륨 그룹의 경우
```

...(pkg2의 경우) 등.

2. 서버에 마운트할 각 볼륨 그룹 및 파일 시스템마다 별도의 `LV[n]` 및 `FS[n]` 변수를 만듭니다. 예를 들면 다음과 같습니다.

   pkg1의 경우:

   LVM 볼륨 그룹의 경우

   ```
   LV[0]=/dev/vg01/lvol1;FS[0]=/your/data1;
   FS_MOUNT_OPT[0]="-o rw" FS_UMOUNT_OPT[0]="";
   FS_FSCK_OPT[0]=""; FS_TYPE[0]="vxfs"

   LV[1]=/dev/vg01/lvol2;FS[1]=/your/data2;
   FS_MOUNT_OPT[0]="-o rw" FS_UMOUNT_OPT[0]="";
   FS_FSCK_OPT[0]=""; FS_TYPE[0]="vxfs"
   ```

   VxVM 볼륨 그룹의 경우

   ```
   LV[0]=/dev/vx/dg01/lvol1;FS[0]=/your/data1; FS_MOUNT_OPT[0]="-o rw"
   FS_UMOUNT_OPT[0]=""; FS_FSCK_OPT[0]=""; FS_TYPE[0]="vxfs"

   LV[1]=/dev/vx/dg01/lvol2;FS[1]=/your/data2;
   FS_MOUNT_OPT[0]="-o rw" FS_UMOUNT_OPT[0]="";
   FS_FSCK_OPT[0]=""; FS_TYPE[0]="vxfs"
   ```

   pkg2의 경우:

   LVM 볼륨 그룹의 경우

   ```
   LV[0]=/dev/vg02/lvol1;FS[0]=/halvm/2a;
   FS_MOUNT_OPT[0]="-o rw" FS_UMOUNT_OPT[0]="";
   FS_FSCK_OPT[0]=""; FS_TYPE[0]="vxfs"

   LV[1]=/dev/vg02/lvol2;FS[1]=/halvm/2b;FS_MOUNT_OPT[0]="-o rw"
   FS_UMOUNT_OPT[0]=""; FS_FSCK_OPT[0]=""; FS_TYPE[0]="vxfs"
   ```

   VxVM 볼륨 그룹의 경우

   ```
   LV[0]=/dev/vx/dg02/lvol1;FS[0]=/your/data3;
   FS_MOUNT_OPT[0]="-o rw" FS_UMOUNT_OPT[0]="";
   FS_FSCK_OPT[0]=""; FS_TYPE[0]="vxfs"

   LV[1]=/dev/vx/dg02/lvol2;FS[1]=/your/data4;
   FS_MOUNT_OPT[0]="-o rw" FS_UMOUNT_OPT[0]="";
   FS_FSCK_OPT[0]=""; FS_TYPE[0]="vxfs"
   ```

3. 변동 가능 IP 주소와 IP 주소가 속한 서브넷의 주소를 지정합니다.

```
IP[0]=1.13.17.20
SUBNET[0]=1.13.168.0
```

(pkg1의 경우),

```
IP[0]=1.13.17.21
SUBNET[0]=1.13.16.0
```

...(pkg2의 경우) 등.

4. HP CIFS Server 모니터 스크립트를 사용하려면 NFS_SERVICE_NAME 변수를 패키지 구성 파일 samba.conf의 SERVICE_NAME 변수 값으로 설정합니다.

   ```
   SERVICE_NAME[0]=samba_mon1
   SERVICE_CMD[0]=/etc/cmcluster/samba/pkg1/samba.mon
   ```

   (pkg1의 경우),

   ```
   SERVICE_NAME[0]=samba_mon2
   SERVICE_CMD[0]=/etc/cmcluster/samba/pkg2/samba.mon
   ```

   (pkg2의 경우).

5. winbind를 사용하는 smb.conf 파일이 있는 경우에는 이런 winbind 행의 주석을 해제하여 클러스터의 winbind를 지원해야 합니다.

samba.mon 모니터 스크립트 편집

samba.mon 모니터 스크립트 파일을 구성하려면 다음 작업을 완료해야 합니다.

1. *samba.mon*과 함께 제공된 다음 템플릿을 사용합니다.

   pkg1의 경우:

   ```
   CONF_FILE=/etc/opt/samba/smb.conf.pkg1
   LOG_FILE=/var/opt/samba/pkg1/logs
   SMBD_PID_FILE=/var/opt/samba/pkg1/locks/smbd.pid
   NMBD_PID_FILE=/var/opt/samba/pkg1/locks/nmbd.pid
   #WINBIND_PID_FILE=/var/opt/samba/pkg1/locks/winbindd.pid
   ```

pkg2의 경우:

```
CONF_FILE=/etc/opt/samba/smb.conf.pkg2
LOG_FILE=/var/opt/samba/pkg2/logs
SMBD_PID_FILE=/var/opt/samba/pkg2/locks/smbd.pid
NMBD_PID_FILE=/var/opt/samba/pkg2/locks/nmbd.pid
#WINBIND_PID_FILE=/var/opt/samba/pkg2/locks/winbindd.pid
```

참고

winbind를 사용하는 smb.conf 파일이 있는 경우 이런 winbind 행의 주석을 해제하여 winbind를 지원해야 합니다.

MC/ServiceGuard 바이너리 구성 파일 작성

참고

다음 예제에서는 클러스터 구성 파일에 */etc/cmcluster/cluster.conf*라는 이름을 지정하고, HA HP CIFS Server 패키지 구성 파일에는 */etc/cmcluster/samba/pkg1/samba.conf*라는 이름을 지정합니다. 실제 클러스터 및 HA HP CIFS Server 패키지 구성 파일 이름은 시스템에 따라 다를 수도 있습니다.

1. 대체 노드에 클러스터 패키지 디렉토리를 만듭니다.

   ```
   mkdir /etc/cmcluster/samba/pkg1 or pkg2, pkg3..n
   ```

   주 노드의 패키지 스크립트를 복사합니다.

   ```
   rcp primary_node:/etc/cmcluster/samba/* \
   alternate_node:/etc/cmcluster/samba
   ```

2. cmquerycl 명령을 사용하여 CIFS 서버의 클러스터 구성 파일을 만듭니다.

   ```
   cmquerycl -v -C clucifs.conf -n primary_node -n \
   alternate_node
   ```

3. cmcheckconf 명령을 사용하여 클러스터 및 패키지 구성의 내용을 확인합니다. 이 단계에서는 MCServiceGuard 절차를 통해 MCServiceGuard 클러스터 구성 파일(clucifs.conf)을 만든 것으로 가정합니다.

```
cmcheckconf -C /etc/cmcluster/clucifs.conf \
            -P /etc/cmcluster/samba/pkg1/samba.conf \
            -P /etc/cmcluster/samba/pkg2/samba.conf
```

4. cmapplyconf 명령을 사용하여 바이너리 구성 파일을 클러스터의 모든 노드로 복사합니다.

```
cmapplyconf -v -C /etc/cmcluster/clucifs.conf \
            -P /etc/cmcluster/samba/pkg1/samba.conf \
            -P /etc/cmcluster/samba/pkg2/samba.conf
```

이 명령을 사용하면 업데이트된 클러스터 바이너리 구성 파일이 클러스터의 모든 노드에 배포됩니다.

이제 HA HP CIFS Server 패키지를 시작할 준비가 되었습니다.

HA HP CIFS Server의 구성이 완료되었습니다.

HA HP CIFS Server 특별 주의 사항

MC/ServiceGuard HA 프레임워크에서 Samba를 구현할 때는 다음과 같은 사항을 주의해야 합니다. 이 주의 사항에 대해 설명하겠습니다.

- 클라이언트 응용 프로그램

  HA HP CIFS Server에서는 HP CIFS Server 공유에 파일을 열어 놓은 클라이언트 응용 프로그램 또는 HP CIFS Server 공유에서 실행된 응용 프로그램이 전환 시 항상 투명하게 복구되는 것은 아닙니다. 이 경우, 전환 과정은 HP CIFS Server의 논리적인 종료 및 재시작 과정이기 때문에 응용 프로그램을 다시 시작하고 파일을 다시 열어야 할 수도 있습니다.

- 파일 잠금

  장애 조치 시간 동안 파일 잠금이 유지되지 않습니다. 파일 잠금은 손실되며 응용 프로그램에 이러한 사실이 통보되지 않습니다.

- 인쇄 작업

  인쇄 작업이 진행 중일 때 장애 조치가 발생하면 장애 조치 발생 시의 작업 상태에 따라 작업이 두 번 인쇄되거나 전혀 인쇄되지 않을 수도 있습니다.

- 심볼릭 링크

  follow symlinks 매개 변수를 기본값인 *yes*로 설정하고 *wide links* 매개 변수를 역시 기본값인 *yes*로 설정하여 Samba 서버를 구성한 경우에는 매우 주의해야 합니다.

  공유된 디렉토리 트리의 심볼릭 링크가 공유 디렉토리 외부에 있는 파일을 가리킬 수도 있습니다. 심볼릭 링크가 논리적 공유 볼륨 외부의 파일을 가리키고 있는 경우 장애 조치가 발생하면 심볼릭 링크가 잘못된 파일을 가리키거나 가리키는 파일이 없을 수도 있습니다. 이런 상황에서 모든 공유된 심볼릭 링크의 대상을 모든 MC/ServiceGuard 노드와 항상 동기화하는 것은 어려울 수도 있습니다.

  이 문제는 *wide links*를 *no*로 설정하거나 논리적 공유 볼륨에 있는 파일 또는 디렉토리만 가리키도록 설정하면 손쉽게 해결할 수 있습니다.

- 보안 파일

  *secrets.tdb*는 중요한 보안 파일입니다. 시스템 계정 정보는 이 파일의 중요한 내용입니다. 이 파일은 주기적으로(*smb.conf*에서 `machine password timeout`

으로 정의되며 기본값은 604800초) 업데이트되므로 *secrets.tdb*는 공유 논리 볼륨에 저장하는 것이 좋습니다. secrets.tdb 파일의 위치는 *smb.conf* 매개 변수인 `private dir`로 정의됩니다. 예를 들면, `private dir = /var/opt/samba/shared_vol_1/private`는 */var/opt/samba/shared_vol_1/private/secrets.tdb* 파일을 생성합니다.

사용자 인증도 여러 보안 파일의 여러 항목에 의존합니다. 기타 중요한 보안 파일로는 사용자 암호 파일인 *smbpasswd* 및 *passdb.tdb*가 있습니다. 예를 들면, 'passdb backend = smbpasswd'를 사용하여 Samba 서버를 구성한 경우에는 smbpasswd 파일이 있습니다. 기본적으로 이 파일은 */var/opt/samba/private* 경로에 있지만 `passdb backend` 매개 변수는 특정 백엔드에만 적용되는 위치 문자열과 백엔드 이름의 두 부분으로 구성될 수 있습니다. 예를 들면, `passdb backend = tdbsam:/var/opt/samba/private/path1/passdb.tdb, smbpasswd:/var/opt/samba/private/path2/smbpasswd`는 */var/opt/samba/private/path1/passdb.tdb* 및 */var/opt/samba/private/path2/smbpasswd* 파일을 생성합니다.

시스템 계정 파일과 사용자 암호 파일은 모두 공유 논리 볼륨의 공통적이고 안전한 디렉토리에 저장하는 것이 좋습니다.

- 사용자 이름 매핑 파일

  Samba 서버에서 사용자 이름 매핑 파일을 사용하도록 구성한 경우에는, 이 파일을 공유된 논리 볼륨에 저장하도록 구성하는 것이 좋습니다. 이렇게 하면 변경 사항이 있더라도 모든 노드가 항상 최신 상태를 유지합니다. 사용자 이름 매핑 파일의 위치는 *smb.conf*에 `username map` 매개 변수로 정의됩니다(예제: `username map = /var/opt/samba/shared_vol_1/username.map`). 기본적으로 사용자 이름 매핑 파일은 없습니다.

- Winbind 구성

  앞에서 설명한 대로 samba.mon 및 samba.cntl에 주석으로 처리된 winbind 줄을 추가합니다.

  Winbind는 /var/opt/samba/locks 디렉토리에서 winbindd.pid, winbindd_cache.tdb, winbindd_idmap.tdb 등의 여러 파일 및 winbindd_privileged 디렉토리를 사용합니다.

전체 /var/opt/samba/locks 디렉토리는 논리적 공유 볼륨에 둘 수 있지만 장애 조치 후 잠금 데이터가 제대로 해석되지 않을 수 있습니다. 시작 스크립트에 줄을 추가하여 잠금 데이터 파일 .../locks/locking.tdb를 제거할 수 있습니다.

- WINS 서버로서의 Samba

  `wins support` 매개 변수를 `yes`로 설정하여 Samba 서버를 WINS 서버로 구성한 경우, WINS 데이터베이스는 */var/opt/samba/locks/WINS.DAT* 파일로 저장됩니다.

  이 파일이 논리적 공유 볼륨에 있지 않으면, 장애 조치 발생 시 모든 WINS 클라이언트가 Samba WINS 서버에 자신의 주소를 업데이트하므로 약간의 시간이 소요됩니다. 그러나 WINS 데이터베이스 복원에 필요한 이 짧은 시간조차 허용되지 않는다면 전체 WINS 서비스를 복원하는 시간을 줄이면 됩니다.

  이렇게 하려면 */var/opt/samba/locks/WINS.DAT*를 논리적 공유 볼륨의 WINS.DAT 파일을 가리키는 심볼릭 링크로 구성하십시오. 장애 조치 후 잠금 데이터가 제대로 해석되지 않을 수 있으므로 전체 */var/opt/samba/locks* 디렉토리는 논리적 공유 볼륨에 두지 않는 것이 좋습니다.

- 마스터 브라우저로서의 Samba

  *domain master*를 `yes`로 설정하여 Samba 서버를 도메인 마스터 브라우저로 구성하면 검색 데이터베이스는 */var/opt/samba/locks/BROWSE.DAT* 파일에 저장됩니다. HA 구성에서 이 작업은 피하는 것이 좋습니다.

  이 작업이 필요하면 */var/opt/samba/locks/BROWSE.DAT*를 논리적 공유 볼륨에 있는 *BROWSE.DAT* 파일을 가리키는 심볼릭 링크로 구성하십시오. 장애 조치 후 잠금 데이터가 제대로 해석되지 않을 수 있으므로 전체 */var/opt/samba/locks* 디렉토리는 논리적 공유 볼륨에 두지 않는 것이 좋습니다.

- 자동 프린터 공유

  Samba 서버에서 `[printers]` 공유가 HP-UX 시스템의 모든 프린터를 자동으로 공유하도록 구성한 경우, 모든 MC/ServiceGuard 노드에 동일한 HP-UX 프린터를 정의해야 합니다. 그렇지 않으면, 장애 조치 발생 시 Samba 서버에 공유된 프린터 목록이 변경되어 해당 프린터를 사용하는 클라이언트에 문제가 발생합니다.

- Samba의 **LMHOSTS 파일**

LMHOSTS 파일을 사용하여 특정 *NetBIOS* 이름에 대한 정적 주소를 저장할 경우, *LMHOSTS* 파일은 논리적 공유 볼륨에 저장하는 것이 좋습니다. 이렇게 하려면 *nmbd*를 호출할 때 -H 옵션을 사용하여 *LMHOSTS* 파일에 다른 경로를 지정해야 합니다. *LMHOSTS* 파일은 모든 노드에서 공유할 수 있도록 논리적 공유 볼륨에 두는 것이 좋습니다.

MC/ServiceGuard 스크립트를 편집하여 -H 옵션을 *nmbd*가 직접 호출되는 위치에 추가해야 합니다. 또한 */opt/samba/bin/startsmb* 스크립트를 편집하여 -H 옵션을 *nmbd*가 시작되는 위치에 추가해야 합니다.

- 유틸리티

  MC/SG 클러스터 환경에서는 일부 유틸리티에 패키지의 smb.conf 파일 위치를 지정해야 합니다. 예를 들면 다음과 같습니다.

```
smbpasswd -c /etc/opt/samba/pkg1/smb.conf.pkg1 -a \
username
smbclient -s /etc/opt/samba/pkg1/smb.conf.pkg1 \
//ha_server1/lvm1a -c ls
testparm -s /etc/opt/samba/pkg1/smb.conf.pkg1
smbstatus -s /etc/opt/samba/pkg1/smb.conf.pkg1
```

- Veritas CFS(Cluster File System)

  Veritas CFS에서는 여러 노드가 동시에 파일에 액세스할 수 있습니다. HP CIFS Server는 클러스터를 인식하지 못하기 때문에 클러스터 환경에서 CIFS Server를 구성하는 경우에는 특히 주의해야 합니다. 2장, "CFS에서 HP CIFS를 사용하는 경우의 특수 고려 사항" 절을 참조하십시오.

12 HP CIFS용 HP-UX 구성

이 장에서는 HP CIFS Server의 사용을 위해 HP-UX를 조정하는 절차를 설명합니다. 이 장의 구성은 다음과 같습니다.

- HP CIFS Server 메모리 및 디스크 요구 사항
- HP CIFS 프로세스 모델
- 커널 구성 매개 변수의 개요
- HP CIFS 사용을 위한 커널 매개 변수 구성

다음 정보는 일반적인 지침일 뿐이며 HP-UX 11i v1 및 v2에서 실행되는 HP CIFS Server에 필요한 리소스 요구 사항을 판단하기 위한 절대적인 규칙은 아닙니다. 시스템 구성 방식은 다양하며, 각 시스템의 요구 사항을 확인하려면 일반적인 로드 하에 실행되는 시스템을 대상으로 온라인 도구를 사용하여 검사해야 합니다.

HP CIFS 프로세스 모델

SMB 데몬 프로세스 *smbd*는 클라이언트의 모든 SMB 요청을 처리합니다. 이 프로세스는 연결된 각 클라이언트당 하나씩 시작됩니다. 각 SMBD 프로세스는 하나의 클라이언트만 처리합니다. 따라서 2048개의 클라이언트가 연결되어 있다면 2048개의 SMBD 프로세스가 존재하게 됩니다. 이렇게 프로세스가 많으면 시스템 리소스도 많이 사용하게 되므로 특정 커널 구성 매개 변수를 조정해야 합니다. 이런 상황에서는 메모리, 디스크 및 스왑 공간도 많이 소모하게 됩니다.

커널 구성 매개 변수의 개요

커널 구성 매개 변수 *maxuser, nproc, ninode, nflocks* 및 *nfile*은 아래에서 설명합니다. HP CIFS에서 여러 클라이언트를 지원하려면 이 커널 매개 변수를 조정해야 합니다.

- *maxusers:* 이 커널 매개 변수는 HP-UX에 로그온할 수 있는 UNIX 사용자의 수를 직접 제어하지 않기 때문에 정확한 이름이라고 할 수는 없습니다. 그러나 이 커널 매개 변수는 커널 전체에 걸쳐 다양한 수식에서 사용됩니다. 실제로, *nproc, nfiles* 및 *ninodes*의 기본값은 *maxusers*의 식으로 나타냅니다.
- *nproc*: 이 커널 매개 변수는 프로세스 테이블의 크기를 제어합니다. 기본 수식은 (*20+8*maxusers*)입니다. 대부분의 시스템에서 이 매개 변수의 기본값은 21이며, 이 값은 20+8*32, 즉 276개의 최대 프로세스를 지원한다는 의미입니다. 프로세스를 시작하기 전에 이 테이블이 가득 차면 "proc: table is full" 오류 메시지가 콘솔에 나타납니다. 이 메시지는 *dmesg* 명령을 실행하면 볼 수 있습니다.
- *nfile*: 이 커널 매개 변수는 시스템 파일 테이블의 크기를 제어하고 시스템에서 열리는 파일의 총 개수를 제한합니다. 하나의 파일을 두 번 열면 시스템 파일 테이블에서 2개의 항목을 차지하므로 이 매개 변수는 열려진 파일의 각 인스턴스에 적용됩니다. 기본 수식은 (16*(nproc+16+maxusers)/10+32+2*(npty+nstrpty+nstrtel)) 입니다. 이 테이블이 가득 차면 file: table is full이라는 콘솔 메시지가 나타납니다.
- *ninode*: 이 커널 매개 변수는 인코어 inode 테이블 또는 inode 캐시의 크기를 제어합니다. 가장 최근에 액세스된 inode를 메모리에 보관하므로 성능이 향상됩니다. 이 매개 변수의 기본 수식은 ((nproc+16+maxusers)+32+(2*npty))입니다. 이 테이블의 용량을 초과하여 파일을 열면 inode 테이블이 가득 찼다는 메시지가 콘솔에 표시됩니다.
- *nflocks:* 시스템 전체의 모든 프로세스에서 언제든지 사용할 수 있는 파일 잠금의 총 개수에 대한 최대값을 정의합니다. 기본값은 200이지만 HP CIFS Server에서 사용하려면 값을 늘려야 합니다.

HP CIFS 사용을 위한 커널 매개 변수 구성

HP CIFS Server에서 여러 클라이언트를 지원하도록 HPUX를 구성하려면 먼저 *maxuser*의 커널 매개 변수를 조정해야 합니다.

두 번째 단계는 *nproc, nfile, nflocks* 및 *ninode*를 개별적으로 조정하여 동시에 여러 사용자가 접속할 수 있도록 설정하는 것입니다.

1. *maxusers* 구성

   동시에 연결 가능한 클라이언트의 최대 수를 결정한 다음 그 수를 *maxusers*의 현재 값에 더하십시오. 예를 들어, 2048개의 클라이언트를 지원할 예정이라면 *maxusers*의 현재 값에 2048을 더합니다. 매개 변수가 수동으로 변경되지 않은 경우, *maxusers*를 조정하면 *nproc, nfile* 및 *ninodes*의 해당 값도 자동으로 조정됩니다.

   예를 들어 2048개의 최대 클라이언트 수를 지원하기 위해 *maxusers* 값을 기본값인 32에서 32+2048(2080)로 조정하면, 일반적인 시스템에서 다른 매개 변수의 값은 다음과 같이 조정됩니다.

   *nproc*은 8,468로 증가합니다.

   *nfile*은 15,656으로 증가합니다.

   *ninode*는 9,692로 증가합니다.

   이 값이 너무 크거나 작다면 다음 설명에 따라 각 커널 매개 변수를 조정하면 됩니다.

2. *nproc, nfile* 및 *ninode* 구성

   - *nproc:* 각 클라이언트는 하나의 고유한 *smbd* 프로세스가 처리하며 각 프로세스는 프로세스 테이블에서 하나의 항목을 차지하므로, 이 매개 변수는 적어도 최대 동시 접속 클라이언트 수와 같아야 합니다. 이것은 필수적인 조건이지만, 사용자가 제어할 수 없는 시스템 프로세스를 비롯하여 다른 프로세스도 존재하며 이러한 프로세스 역시 *proc* 테이블 항목을 차지하므로 이 값으로는 충분하지 않습니다. 따라서 이 매개 변수는 예상 클라이언트 최대 수에 HP CIFS와 동시에 실행될 다른 프로세스의 수를 더한 값으로 설정해야 합니다.

- *nfile:* SMBD 프로세스는 시작되는 즉시 시스템 파일 테이블에서 28개의 항목을 차지합니다.

  여기에는 클라이언트에서 열고 작업할 다른 파일은 포함되지 않았습니다. 따라서 *nfile*의 값은 적어도 예상 동시 클라이언트 수에 (각 클라이언트가 동시에 여는 예상 파일 수+28)을 곱한 값이어야 합니다. 이 역시 필수 조건이긴 하지만, HP CIFS 이외의 프로세스가 HP CIFS와 동시에 파일을 열 수 있으므로 충분한 값은 아닙니다.

- *ninode*: *nfile*과는 달리, inode 항목의 수는 열려 있는 각 인스턴스에 따라 증가하지 않습니다. 즉 열려 있는 파일 하나는 열린 수에 관계 없이 하나의 항목만 차지합니다. 따라서 이 매개 변수는 HP CIFS에서 여는 각 파일의 예상 수에 시스템의 다른 프로세스가 여는 파일 수를 더한 값으로 설정해야 합니다.

- *nflocks:* 각 smbd 프로세스는 10개 이상의 파일 잠금을 활용합니다. 결국, *nflocks*의 값은 적어도 예상되는 동시 클라이언트 수에 10을 곱한 값과 같아야 합니다. 다른 응용 프로그램에서 *nflocks*를 사용할 가능성도 고려해야 합니다.

스왑 공간 요구 사항

HP CIFS에서는 클라이언트당 하나의 프로세스를 사용하기 때문에 시스템에서 가장 중요한 요구 사항은 스왑 공간에 대한 조건입니다. HPUX에서는 시작되는 각 프로세스마다 일정한 크기의 스왑 공간을 확보합니다. 따라서 메모리가 부족하여 일부 페이지를 스왑할 때 공간 부족으로 프로세스가 취소되는 것을 방지합니다. 다른 운영 체제는 필요할 때만 스왑 공간을 확보합니다. 따라서 필요한 스왑 공간을 찾지 못하는 프로세스가 발생하며 이 프로세스는 OS에 의해 실행이 종료됩니다.

각 *smbd* 프로세스에는 약 2MB의 스왑 공간이 할당되고 클라이언트 활동 종류에 따라 프로세스 크기가 4MB의 스왑 공간으로 증가할 수 있습니다. 최대 2048개의 클라이언트를 위해서는 4*2048(약 8GB)의 스왑 공간이 필요합니다. 따라서 HP CIFS Server에 동시에 연결되는 클라이언트의 최대 수를 수용할 수 있는 충분한 스왑 공간을 구성하는 것이 좋습니다.

메모리 요구 사항

각 *smbd* 프로세스에는 약 1MB의 메모리가 필요합니다. 따라서 2048개의 클라이언트를 지원하려면 시스템에 최소한 2GB의 물리적 메모리가 있어야 합니다. 이는 HP CIFS와 동시에 실행될 다른 응용 프로그램에 필요한 메모리보다 더 많은 양입니다.

용어집

ㄱ

공개 키 두 사용자가 데이터를 안전하게 교환할 수 있지만 한 방향으로만 가능한 암호화 방식입니다. 개인 키를 가진 사용자가 그에 해당하는 공개 키를 만듭니다. 이 공개 키는 다른 사람에게 줄 수 있습니다. 이 사용자에게 암호화된 데이터를 전송하려는 사용자는 공개 키를 사용해 데이터를 암호화할 수 있습니다. 개인 키를 소유한 사용자만 이 데이터를 해독할 수 있습니다.

공개 키 인프라 공개 키 암호화를 관리하는 방식입니다. 공개 키 기술은 암호 해독 키를 교환하지 않는다는 장점이 있지만 관리가 어렵다는 단점이 있습니다. 이와 관련된 문제로는, 공개 키의 소유자를 증명하여 배포하는 것과 만료 또는 종료된 키의 해지에 관한 문제가 있습니다.

권한 부여 사용자가 액세스 권한을 가진 파일 시스템 데이터에만 액세스할 수 있도록 제한합니다. 인증된 사용자라 하더라도 모든 파일을 읽고 수정할 수 있는 것은 아니기 때문입니다. 가장 간단한 경우를 예를 들어, 사용자는 액세스 제어 정보(액세스 제어 목록, ACL)를 통해 파일 시스템의 개별 파일 및 디렉토리에 대한 읽기 또는 수정 권한을 부여받습니다.

ㅁ

무결성 무결성은 파일 시스템 데이터가 침입자에 의해 변경되지 않았다는 것을 보증합니다. 침입자는 네트워크 파일 시스템 검색 및 변경 거부 과정을 거치지 않고는 파일 시스템 데이터 패킷을 해킹하여 수정할 수 없습니다.

ㅂ

비밀 키 비밀 키(대칭형 키 또는 공유 키라고도 함) 암호화는 두 사용자가 공유된 비밀 키로 데이터를 암호화하고 해독하여 교환하는 암호 기술입니다. 하나의 키를 사용해 데이터를 암호화 및 해독합니다. 비밀 키를 알면 누구나 데이터를 해독할 수 있으므로 비밀 키는 보안을 유지하여(예제: "cones of silence" 방식 사용) 교환해야 합니다.

ㅇ

암호화 암호화를 사용하면 비밀(개인) 키를 소유한 사용자만 데이터를 볼 수 있습니다. 암호화된 데이터는 비밀 키로 해독하기 전까지는 무의미한 데이터입니다. 데이터의 암호화 및 암호 해독을 암호 방식(ciphering)이라고 합니다.

인증 파일 데이터에 액세스하는 사용자의 신원을 확인하기 위한 스키마입니다. 보안 네트워크 파일 시스템에서는 인증을 통해, 원래의 사용자를 가장하여 액세스하는 것을 방지합니다.

ㅈ

자격 증명 사용자를 식별하는 정보입니다. 자격 증명은 사용자와 고유하게 연관된 번호(예를 들어 주민등록번호)처럼 간단한 것일 수도 있고, 추가적인 식별 정보가 포함된 복잡한 것일 수도 있습니다. 강력한 자격 증명에는 자격 증명의 현재 사용자가 해당 자격 증명이 나타내는 실제 사용자라는 증거(증명자라고도 함)가 들어있습니다.

A

ACL Access Control List(액세스 제어 목록)의 약자이며, 파일 데이터에 어떤 사용자가 액세스할 수 있으며 해당 데이터에 어떤 유형의 액세스가 허용되는지 기술된 메타 데이터입니다. ACL은 "액세스 권한"을 정의합니다. 이 체계에서 사용자는 일반적으로 "그룹"에 속하며 그 그룹 전체에 액세스 권한이 부여됩니다. 일반적인 액세스 권한의 유형으로는 읽기(나열), 쓰기(수정) 또는 만들기(추가) 등이 있습니다. 지원되는 ACL의 수준은 파일 시스템에 따라 다양하며 각 파일 시스템마다 액세스 권한은 서로 다르게 정의됩니다. 예를 들어, DOS에서 파일 시스템은 하나의 사용자만 사용하는 것으로 간주되므로 파일에 대한 권한 집합은 하나만 존재합니다. POSIX 6 호환 파일 시스템에서는 여러 사용자와 사용자 그룹에게 여러 파일 및 디렉토리에 대한 다양한 권한을 지정할 수 있습니다.

ASP Application Service Provider(응용 프로그램 서비스 제공자)를 의미하며, 기본적으로 사용자에게 응용 프로그램을 '임대'하는 e-business입니다.

C

CIFS Common Internet File System(일반 인터넷 파일 시스템)의 약자로, 인터넷을 위해 설계된 파일 액세스 프로토콜 사양입니다.

HP CIFS HP에서 구현한 UXNI용 CIFS입니다. HP CIFS는 HP 9000 서버 및 워크스테이션을 위한 서버 및 클라이언트 모듈을 모두 제공합니다.

D

Diffie-Hellman 비밀 키를 두 사용자 간에 안전하게 공유하기 위한 프로토콜입니다. Diffie-Hellman 프로토콜은 공개 키 교환 형태를 사용해 비밀 키를 공유합니다. Diffie-Hellman은 중간에 해커의 공격을 받을 가능성이 있는 것으로 알려졌지만, 이후 개선된 버전인 인증된 Diffie-Hellman Key Agreement에서는 그러한 중간 과정에서의 침입을 허용하지 않습니다.

K

Kerberos MIT 및 IETF 그룹이 개발한 인증 및 권한 부여 보안 시스템입니다. 비밀 키 기술을 기반으로 하며, 중앙 집중식으로 설계되었으므로 공개 키 인프라에 비해 관리하기가 더 쉽습니다. 하지만 Kerberos는 공개 키 인프라만큼 확장성이 좋지는 않습니다.

S

Samba 1990년대 중반에 처음 선보인 공개형 소스 제품입니다. Samba는 주 도메인 컨트롤러(PDC) 및 백업 도메인 컨트롤러(BDC) 동기화 프로토콜을 제외한 Advanced Server for UNIX의 기능 대부분과, UNIX 시스템용 NT 파일 및 인쇄 서버 기능을 제공합니다. Samba는 널리 사용되고는 있지만 공급업체의 지원은 받을 수 없습니다.

SMB Server Message Block(서버 메시지 블록)의 약자로, Windows 네트워킹의 핵심을 이루는 파일 공유 프로토콜입니다. SMB는 Windows NT, Windows 95, Windows for Workgroups 및 OS/2 LAN Manager가 공유합니다. CIFS는 이 프로토콜을 이름만 바꾼 것이라고 말할 수 있습니다.

색인