

HP CIFS Client A.02.01 관리자 설명서

HP-UX 11i v1 및 v2



i n v e n t

제품 제조 번호: B8724-90074

2005년 4월

© Copyright 2005 Hewlett-Packard Company. .

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 이 설명서의 오류나 공급, 수행 또는 사용에 따른 직접적, 간접적, 부수적, 파생적인 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 252.227-7013의 Rights in Technical Data and Computer Software 조항의 (c) (1) (ii) 부속 조항에 기술된 제한이 적용됩니다. 그리고 기타 기관의 경우 FAR 52.227-19의 Commercial Computer Software Restricted Rights 조항의 (c) (1) 및 (c) (2) 부속 조항에 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. 프로그램의 추가 사본은 보안 및 백업 목적으로만 만들 수 있습니다. 프로그램의 원본 또는 수정본을 전매하는 행위는 명시적으로 금지되어 있습니다.

PAM NTLM은 Open Source Samba 제품에서 파생된 라이브러리를 포함합니다. 이 라이브러리는 GPL 라이선스가 적용됩니다. 자세한 내용은 CIFS/9000 Server 설명서의 5장에서 GPL 라이선스를 참조하십시오.

저작권

©copyright 1983-2005 Hewlett-Packard Company, all rights reserved.

저작권 법에 의해 허용되지 않는 한, 이 자료의 어떠한 부분도 HP의 사전 서면 동의 없이 재생산, 각색 또는 다른 언어로 번역될 수 없습니다.

©copyright 1998 Christian Starkjohann, All Rights Reserved.

상표권

UNIX는 Open Group의 등록 상표입니다.

1. HP CIFS Client 소개

HP CIFS 소개 15

 CIFS 프로토콜의 개념 15

HP CIFS Client 설명 17

HP CIFS Client 기능 18

 CIFS UNIX Extensions 18

 NTLM PAM 통합 18

 Kerberos 인증: 시스템 Kerberos 캐시와의 통합 19

 HP CIFS Client에 대한 AutoFS 2.3 지원 19

 국제화된 클라이언트 지원 20

 NTLM, NTLMv2 암호의 암호화 20

 패킷 서명 20

 NetBIOS 이름 서비스, WINS 및 DNS 지원 21

2. HP CIFS Client의 설치, 구성 및 사용

HP CIFS Client 설치 및 구성 개요 25

1단계: HP CIFS Client 설치 전제 조건 확인 26

2단계: HP CIFS Client 및 PAM 소프트웨어 설치 27

 CD에서 설치 27

 소프트웨어 저장소 파일에서 설치 27

3단계: HP CIFS Client 구성 28

 cifsclient.cfg 편집 28

4단계: HP CIFS Client 데몬 시작 및 중지 30

HP CIFS Client 사용 31

 마운트 및 로그인을 한 단계로 처리 35

 CIFS Client 로깅 35

CIFS 파일 시스템 자동 마운트 36

 /etc/fstab 사용 36

 CIFS Client 마운트 데이터베이스에 마운트 저장 36

이름 확인: NetBIOS 이름 서비스, WINS, DNS, IP 구성 37

HP CIFS Client 파일 및 디렉토리 39

3. CIFS 보안 및 인증

소개 43

 인증 방법 43

 인증 구성 설정 43

사용자 로그인 절차 45

Kerberos 소개 47

목차

Kerberos 사용에 대한 요구 사항 및 제한 사항	47
HP CIFS Client에서 Kerberos 사용	48
1단계. 기본적인 Kerberos 작동 원칙 검토	48
2단계. Kerberos 하부 구조 설치 및 검증	49
3단계. HP CIFS Client에 Kerberos 구성	51
CIFS Client Kerberos 인증 정책	52
명시적 로그인: cifslogin	52
자동 로그인: 시스템 Kerberos 캐시와 통합(kinit(1) 및 PAM Kerberos)	52
티켓 수명	52
패킷 서명	53
HP CIFS Client에서의 패킷 서명 구성	53

4. HP CIFS Client A.01에서 A.02로 마이그레이션

HP CIFS Client A.01.* 버전에서 A.02.* 버전으로 마이그레이션	57
HP CIFS Client 버전 A.01.* 사용자를 위한 지침	57
A.01 설치에서 데이터 보존	57
A.01 버전으로 되돌리기	58
HP CIFS Client A.01.* 및 A.02.*의 기능적 차이	60
HP CIFS Client A.01.* 및 A.02.*의 구성적 차이	61
구성 파일의 주석	61
구성 매개 변수의 차이점	61
HP CIFS Client A.01.* 및 A.02.*의 명령 옵션 차이	65

5. 명령줄 유틸리티

cifsclient	71
구문	71
설명	71
명령	71
파일	72
관련 항목	73
cifsmount	74
구문	74
설명	74
옵션	74
예제	76
파일	76
관련 항목	76
cifslogin	77

구문	77
설명	77
옵션	77
예제	79
파일	79
관련 항목	79
cifs mount	80
구문	80
설명	80
옵션	80
관련 항목	80
cifs logout	81
구문	81
설명	81
관련 항목	81
cifs list	82
구문	82
설명	82
옵션	82
cifs list 출력 예제	82
cifs smb	85
구문	85
설명	85
옵션	86
파일	86
관련 항목	86
mount_cifs, umount_cifs	87
구문	87
설명	87
옵션	87
파일	89
관련 항목	89

6. 문제 해결 및 오류 메시지

질문과 대답을 통한 문제 해결	93
cifsclient stop 명령으로 데몬을 종료하는 방법	93
데몬이 종료된 경우 처리 방법	93

목차

HP CIFS Client에서 Kerberos 문제 해결	94
CIFS Client 로그 파일 및 로그 수준	96
7. 구성 파일	
일반 구조	99
구성 매개 변수	101
8. PAM NTLM	
소개	126
PAM NTLM	128
PAM NTLM 기능	128
사용자 맵 파일	128
PAM NTLM 구성	129
PAM-NTLM 모듈 구성	129
사용자 맵 파일 구성	133
사용자 맵 파일의 NIS 배포 사용	133
색인	135

머리말: 설명서 정보

이 설명서의 최신 버전은 다음 웹 사이트에서 온라인으로 구할 수 있습니다.

<http://www.docs.hp.com>(영문 설명서)

<http://www.docs.hp.com/ko>(한글 설명서)

이 문서는 HP-UX 플랫폼에서 HP CIFS Client를 설치 및 구성하고 문제를 해결하는 방법에 대해 설명합니다.

문서의 발행 날짜와 제품 번호로 설명서의 버전을 확인할 수 있습니다. 새로운 버전의 설명서가 발행되면 발행 날짜가 변경됩니다. 설명서의 내용이 약간 변경되면 판본을 다시 찍을 때 발행 날짜가 변경되지 않습니다. 설명서의 내용이 크게 변경되면 제품 번호가 변경됩니다.

다음 버전이 출판되기 전이라도 오류 수정이나 제품 변경에 따른 문서화를 위해 설명서가 업데이트될 수 있습니다. 업데이트 또는 새 버전의 설명서를 받으려면 해당 제품 지원 서비스에 가입해야 합니다. 자세한 사항은 HP 영업 담당자에게 문의하십시오.

대상 독자

이 설명서는 HP CIFS Client를 설치, 구성 및 관리하는 시스템 및 네트워크 관리자를 대상으로 합니다. 관리자는 HP CIFS Client 제품에 대한 지식을 가지고 있어야 합니다.

새로운 내용 및 변경된 내용

NetBIOS 이름 서비스, WINS 및 DNS 지원에 대한 정보가 추가되었습니다.

NTLM, NTLMv2 및 Kerberos를 사용하는 CIFS 보안 및 인증 방법이 추가되었습니다.

패킷 서명을 사용하는 CIFS 세션 보안이 추가되었습니다.

HP CIFS Client A.01.* 및 A.02.* 간 구성 매개

변수 및 명령 옵션의 차이점에 대한 정보가 추가되었습니다.

CIFS Client 구성 파일 및 명령 유틸리티에 대한 정보가 업데이트되었습니다.

발행 정보

표 1

자세한 발행 정보

설명서 제품 번호	지원되는 운영 체제	지원되는 제품 버전	발행 날짜
B8724-90074	11i v1 및 v2	A.02.01	2005년 4월
B8724-90054	11.0, 11i v1 및 v2	A.01.09	2003년 8월
B8724-90035	IA 11.22	A.01.08	2002년 6월
B8724-90019	11.0, 11i v1 및 v2	A.01.06	2001년 6월

설명서 내용

이 설명서에서는 HP CIFS Client 소프트웨어 제품을 설치 및 구성하고 문제를 해결하는 방법에 대해 설명합니다.

이 설명서는 다음과 같이 구성되어 있습니다.

- 1장 **HP CIFS Client 소개** — HP CIFS Client 제품의 기능, 요구 사항 및 제한 사항에 대해 설명합니다.
- 2장 **HP CIFS Client의 설치, 구성 및 사용** — HP CIFS Client 소프트웨어를 설치, 구성 및 사용하는 방법에 대해 설명합니다.
- 3장 **CIFS 보안 및 인증** — CIFS 보안 및 인증 방법에 대해 설명합니다.
- 4장 **HP CIFS Client A.01.*에서 A.02.*으로 업데이트** — HP CIFS Client A.01.* 및 A.02.* 간 구성 매개 변수 및 명령 옵션의 차이점에 대해 설명합니다. 또한 CIFS Client 업그레이드를 계획하고 수행할 때 필요한 업데이트 절차를 제공합니다.

- 5장 **명령줄 유틸리티** — 모든 HP CIFS Client 유틸리티에 대한 UNIX 맨페이지에 대해 설명합니다.
- 6장 **HP CIFS Client 문제 해결** — HP CIFS Client의 문제점을 진단하기 위한 자세한 절차에 대해 설명합니다.
- 7장 **구성 파일** — HP CIFS Client 소프트웨어를 사용자 정의하려는 경우 알아야 할 모든 구성 변수 목록에 대해 설명합니다.
- 8장 **PAM NTLM** — PAM NTLM 인증 서비스에 대해 자세히 설명합니다.

표기법

이 설명서에서는 다음과 같은 표기법을 사용합니다.

- 이탤릭체* 설명서 제목, 파일 이름 및 경로를 나타냅니다.
- 고딕체** 강한 강조 텍스트입니다.
- 모노 타입** 프로그램/스크립트, 명령 이름, 매개 변수 또는 화면 표시를 나타냅니다.

사용자 의견 접수

HP는 이 설명서에 대한 사용자 여러분의 의견을 기다리고 있습니다. HP는 사용자 요구를 충족하는 설명서를 만들기 위해 최선을 다할 것입니다.

여러분의 의견을 netinfo_feedback@cup.hp.com으로 보내주십시오.

의견을 보내실 때는 문서 제목, 제품 번호, 귀하의 의견, 발견한 오류 그리고 이 설명서를 개선하기 위해 도움이 될 만한 제안 사항 등을 함께 보내주십시오. 또한 잘 된 부분에 대해서도 의견을 주시면 다른 설명서를 만들 때 반영하도록 하겠습니다.

1 HP CIFS Client 소개

이 장에서는 HP CIFS Client에 대해 설명합니다.

이 장의 구성은 다음과 같습니다.

- HP CIFS 소개
- HP CIFS Client 설명
- HP CIFS Client 기능

HP CIFS 소개

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

HP CIFS Server는 검증된 개방형 소스 소프트웨어인 Samba에 기반하며 Windows, 기타 CIFS Client 및 HP-UX 컴퓨터를 포함한 HP CIFS Client 소프트웨어를 실행 중인 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 또한 Windows NTLM(NT Lan Manager) 인증 프로토콜을 구현하는 선택적인 PAM(Pluggable Authentication Module)을 제공합니다. HP-UX PAM 설비 내에서 설치하고 구성할 경우, PAM NTLM은 HP-UX 사용자가 Windows 인증 서버에 대해 인증되도록 합니다.

CIFS 프로토콜의 개념

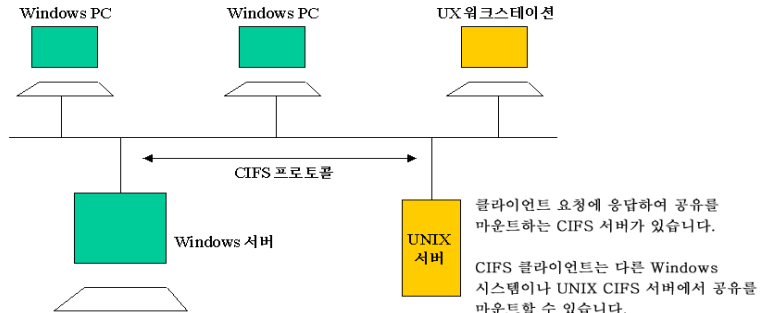
CIFS는 1980년대 후반 IBM이 개발한 서버 메시지 블록(SMB) 프로토콜이라고도 하는 네트워킹 프로토콜에서 시작되었습니다. SMB는 Microsoft Windows에서 사용되는 기본 파일 공유 프로토콜입니다.

CIFS는 단지 SMB의 다른 이름일 뿐이며 CIFS와 SMB는 같은 것입니다. 현재 Microsoft는 CIFS를 사용하도록 권장하지만 SMB도 여전히 사용되고 있습니다. CIFS는 또한 UNIX, Linux, Macintosh 및 다른 플랫폼에서도 폭넓게 사용됩니다.

CIFS는 원격 파일 액세스 프로토콜이며 원격 시스템의 파일에 대한 액세스를 제공합니다. 또한 서버와 클라이언트 모두를 정의합니다. CIFS Client는 CIFS Server에 있는 파일에 액세스하는 데 사용됩니다.

HP CIFS는 HP-UX 컴퓨터에서 CIFS 프로토콜을 사용하여 HP-UX 서버의 디렉터리가 Windows 컴퓨터에 마운트되도록 하며 반대의 경우도 가능하도록 합니다.

CIFS 패러다임



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

PAM NTLM

시스템 관리자는 HP-UX PAM 부속 시스템을 통해 인증을 수행하는 시스템에서 사용할 수 있는 다양한 인증 서비스를 융통성 있게 선택할 수 있습니다. 또한 프레임워크를 사용하면 기존 응용 프로그램을 수정할 필요 없이 새로운 인증 서비스 모듈을 추가하여 사용할 수 있습니다.

PAM 프레임워크인 *libpam*은 인터페이스 라이브러리와 다중 인증 서비스 모듈로 구성됩니다. 인증 서비스 모듈은 동적으로 로드할 수 있는 일련의 객체이며 특정 사용자 인증 유형을 제공하는 PAM API로 호출됩니다.

NTLM(NT LAN Manager)은 CIFS Server가 CIFS Client를 인증하는 프로토콜입니다. PAM NTLM은 NTLM 프로토콜을 구현하는 PAM 모듈입니다. 이 모듈을 사용하면 `cifslogin` 명령을 사용하지 않고도 HP-UX 시스템에 로그인하여 CIFS로 마운트된 파일 시스템을 액세스할 수 있습니다.

HP CIFS Client 설명

HP CIFS Client는 HP-UX 사용자가 CIFS Server의 공유를 UNIX 파일 시스템으로 마운트할 수 있도록 HP-UX에서 CIFS 프로토콜을 구현합니다.

HP CIFS Client 기능

다음은 HP CIFS Client의 주요 기능입니다.

- CIFS UNIX Extensions
- NTLM PAM 통합
- Kerberos 인증, 시스템 Kerberos 캐시와의 통합
- ONC AutoFS 2.3 지원
- 국제화된 클라이언트 지원
- NTLM, NTLMv2 암호의 암호화
- 패킷 서명
- NetBIOS 이름 서비스, WINS 및 DNS 지원

CIFS UNIX Extensions

CIFS UNIX Extensions를 사용하면 CIFS Client와 Samba 서버로 표준 UNIX 파일 시스템 기능을 구현할 수 있습니다. 여기에는 다음과 같은 항목이 포함됩니다.

- UNIX 사용 권한 모드
- UNIX UID 및 GID에 기반한 파일 소유권
- 심볼릭 링크 및 하드 링크
- 파일 액세스, 변경 및 수정에 대한 표준 UNIX 시간 스탬프
- UNIX stat(2) 데이터 구조에 포함된 기타 데이터 포함 기능

주

이 기능은 CIFS UNIX Extentions를 지원하는 CIFS Server에서만 작동합니다.

NTLM PAM 통합

NTLM(NT LAN Manager)은 CIFS Server가 CIFS Client를 인증하는 기본 프로토콜입니다. HP의 NTLM PAM(Pluggable Authentication Module) 및 HP CIFS Client와 함께 사용하면 HP-UX 시스템에 로그인한 사용자가 자동으로 CIFS로 마운

트된 파일 시스템을 액세스할 수 있습니다. 단, PAM NTLM 및 CIFS Server가 동일한 데이터베이스를 사용해야 합니다.

Kerberos 인증: 시스템 Kerberos 캐시와의 통합

CIFS Client는 Kerberos 인증 메커니즘을 지원합니다. Kerberos는 안전한 업계 표준의 인증 프로토콜입니다. 지금까지 CIFS Client와 서버가 사용해 온 이전의 NTLM 프로토콜에 비해 크게 향상된 기능을 제공합니다. HP CIFS Client에서 Kerberos 지원을 활용하려면 네트워크상의 CIFS Server가 Kerberos를 지원해야 합니다. Kerberos는 클라이언트가 실행되는 HP-UX 호스트 및 사용자 네트워크 모두에 올바르게 구성되어야 합니다.

추가 기능으로 HP CIFS Client가 시스템 Kerberos 캐시에 통합되었습니다. HP-UX 호스트가 **kinit (1)** 과 같은 시스템 Kerberos 캐시를 활용하는 PAM Kerberos나 다른 Kerberos 인식 프로그램을 사용하는 경우, CIFS Client는 캐시된 이 자격 증명을 사용하여 각 서버에 대해 사용자가 명시적으로 인증을 받지 않고도 마운트된 CIFS Server에 자동 액세스할 수 있습니다.

HP CIFS Client에 대한 AutoFS 2.3 지원

AutoFS는 HP ONC 제품 세트에 포함된 서비스로서 일반 사용자에게 투명성이 보장되도록 자동으로 파일 시스템을 마운트하거나 마운트를 해제합니다. AutoFS 2.3 최신 버전은 HP CIFS Client가 마운트한 파일 시스템의 마운트 또는 마운트 해제를 지원합니다. AutoFS 2.3은 HP CIFS 파일 시스템의 직접 및 간접 마운트를 자동으로 수행할 수 있습니다. AutoFS 2.3은 직접 및 간접 맵 파일을 가지고 있는 HP CIFS Client만을 지원하며 특수하거나 실행 가능한 맵 파일을 가지고 있는 CIFS Client 또는 복수(복제된) 서버를 가지고 있는 CIFS Client는 지원하지 않습니다.

HP CIFS Client AutoFS 지원을 제공하려면 AutoFS 2.3을 시스템에 설치 및 구성해야 합니다. AutoFS의 설치 및 구성에 대한 자세한 내용은 HP-UX 사이트 (<http://www.docs.hp.com>)의 *NFS Services Administrator's Guide*에서 "Configuring and Administering AutoFS" 부분을 참조하십시오.

주

HP ONC+ AutoFS 서비스를 사용한 CIFS 파일 시스템의 자동 마운트는 HP-UX 릴리즈 11i v1 및 v2에서만 지원됩니다. HP-UX 11i v1 시스템을 사용하는 경우에는 <http://software.hp.com>에서 구할 수 있는 ONC 소프트웨어 패키지 Enhanced AutoFS를 설치하여 AutoFS 2.3 지원을 사용 가능하게 해야 합니다. HP-UX 릴리즈 11.0에서는 AutoFS에서 HP CIFS Client를 지원하지 않습니다.

국제화된 클라이언트 지원

CIFS Client는 국제화된 다양한 클라이언트 및 서버와 작동하도록 설계되었습니다. 또한 Unicode를 사용하여 네트워크상에서 멀티바이트 문자를 전송하거나, `/etc/opt/cifsclient/unitables`에 있는 임의의 문자 인코딩 테이블을 사용할 수 있습니다. 테이블의 색인에 대해서는 해당 디렉토리에 있는 **README** 파일을 참조하십시오.

NTLM, NTLMv2 암호의 암호화

NTLM은 챌린지 응답 프로토콜입니다. 서버는 챌린지 키를 클라이언트로 보내고 클라이언트는 이를 사용자 암호로 암호화하여 서버로 다시 보냅니다. 서버는 동일한 암호화를 수행하고 클라이언트 요청이 일치하는지 확인합니다. 사용자 암호와 유사한 것이 네트워크를 통해 전송될 수 없습니다. CIFS Client에서는 NTLM 및 NTLMv2를 지원합니다. NTLM 버전 2(NTLMv2)는 NTLM과 동일한 챌린지 응답 프로토콜을 사용하지만 보다 복잡한 암호화 알고리즘을 제공하므로 암호를 더 잘 보호할 수 있습니다.

패킷 서명

CIFS 패킷 서명의 목적은 끼어들기(man-in-the-middle) 공격을 예방하는 것입니다. 클라이언트와 서버가 각 SMB 패킷에 대한 고유한 서명을 요청하여 상호 간에 상대의 ID를 확인합니다.

CIFS 프로토콜에서는 클라이언트가 서버에 처음으로 연결할 때 패킷 서명이 협상됩니다. 첫 사용자가 서버에 로그인한 이후에는 클라이언트와 서버 간의 모든 SMB 패킷이 서명되어야 합니다.

`smbPacketSigning` 구성 매개 변수에 대한 설명은 53페이지의 “패킷 서명”을 참조하십시오.

NetBIOS 이름 서비스, WINS 및 DNS 지원

HP CIFS Client A.02.01에서는 WINS(DNS와 유사한 Windows 이름 확인 서비스)를 포함하여 DNS 및 NetBIOS 이름 서비스를 지원합니다. lookupTryNetbios, lookupTryDns 및 nbnsWinsIP 구성 매개 변수는 사용할 조회 메커니즘을 구성하는데 사용됩니다. 자세한 내용은 37페이지의 “이름 확인: NetBIOS 이름 서비스, WINS, DNS, IP 구성”을 참조하십시오.

HP CIFS Client 소개
HP CIFS Client 기능

2 HP CIFS Client의 설치, 구성 및 사용

이 장에서는 시스템에 HP CIFS Client 소프트웨어를 설치하는 절차를 설명합니다.

이 장의 구성은 다음과 같습니다.

- 25페이지의 “HP CIFS Client 설치 및 구성 개요”
- 26페이지의 “1단계: HP CIFS Client 설치 전제 조건 확인”
- 27페이지의 “2단계: HP CIFS Client 및 PAM 소프트웨어 설치”
- 28페이지의 “3단계: HP CIFS Client 구성”
- 30페이지의 “4단계: HP CIFS Client 데몬 시작 및 중지”
- 31페이지의 “HP CIFS Client 사용”
- 36페이지의 “CIFS 파일 시스템 자동 마운트”
- 37페이지의 “이름 확인: NetBIOS 이름 서비스, WINS, DNS, IP 구성”
- 39페이지의 “HP CIFS Client 파일 및 디렉토리”

HP CIFS Client 설치 및 구성 개요

HP CIFS Client 설치에 설치 전제 조건 확인, *swinstall(1M)* 유틸리티를 사용한 HP CIFS Client 파일 세트 로드 및 HP CIFS 구성 절차 완료로 구성됩니다.

CIFS Client와 PAM NTLM 제품은 HP Software Distributor(SD)를 사용하여 설치 패키지로 만들어진 동일한 번들로 제공됩니다. 두 제품을 동시에 설치하는 것이 좋습니다. 하지만 각 제품을 독립형 제품으로 설치하고 실행할 수도 있습니다. 소프트웨어를 설치하거나 제거하려면 *swinstall(1M)* 및 *swremove(1M)* HP-UX 명령을 사용하십시오. 이들 명령에 대한 자세한 내용은 HP-UX 맨페이지를 참조하십시오.

CIFS Client 설치 및 제거 중에 자동으로 시스템이 다시 부팅됩니다. CIFS Client는 CIFS를 마운트 가능한 파일 시스템으로 인식하도록 커널을 수정합니다.

HP CIFS Client 번들을 설치할 때 HP CIFS Client 소프트웨어와 NTLM PAM 모듈(선택 사항)의 두 제품을 설치할 수 있습니다.

주

HP CIFS Client 소프트웨어는 <http://software.hp.com>에서 다운로드할 수 있습니다.

1단계: HP CIFS Client 설치 전제 조건 확인

HP CIFS Client 소프트웨어를 시스템으로 로드하기 전에 다음 하드웨어 및 소프트웨어 전제 조건을 충족하는지 확인하십시오.

1. HP CIFS Client는 HP-UX 버전 11.11 이상을 32비트나 64비트 모드로 실행할 수 있는 모든 HP 워크스테이션과 서버에서 실행됩니다. HP CIFS Client에 필요한 특정 시스템 패치는 없습니다. 아래 항목 3을 참조하십시오.
2. Kerberos 라이브러리인 *libkrb5.sl* 및 *libcom_err.lib*가 시스템에 있어야 합니다. HP-UX 버전 11i(B.11.11) 및 앞으로 발표되는 릴리즈에서는 기본 HP-UX 운영 체제 설치 중에 기본적으로 이러한 라이브러리를 시스템으로 가져옵니다. 그러나 HP-UX 버전 11.0(B.11.00)에는 이러한 라이브러리가 없을 수도 있습니다 (*/usr/lib* 확인). 이러한 라이브러리를 구하려면 <http://software.hp.com>에서 다운로드할 수 있는 PAM Kerberos 제품을 설치하십시오.
3. 최신 PAM 라이브러리 패치가 있는지 확인합니다. 패치는 HP의 온라인 패치 카탈로그에서 "libpam"을 검색하여 구할 수 있습니다. `swlist` 명령을 사용하여 시스템에 설치된 소프트웨어를 나열할 수 있습니다. 일반 릴리즈(General Release) 패치 목록이 있으면 다음 명령으로 이 내용에서 PAM 패치를 확인할 수 있습니다.

```
swlist -l fileset _patch-name_ | grep -i pam
```

패치 종속성에 대한 정보는 HP CIFS Client 릴리즈 노트를 참고하십시오.
4. 설치를 수행하려면 root 권한이 있는 사용자로 로그인해야 합니다.

주

현재 HP CIFS Client의 A.01.* 버전을 사용하고 있는 경우 A.02.* 버전을 설치하기 전에 57페이지의 "HP CIFS Client A.01.* 버전에서 A.02.* 버전으로 마이그레이션" 부분을 읽으십시오.

2단계: HP CIFS Client 및 PAM 소프트웨어 설치

HP-UX 시스템에서 소프트웨어를 설치하려면 root 권한이 있어야 합니다. CIFS Client에는 커널 모듈이 포함되어 있으므로 설치가 완료되면 시스템이 재부팅합니다.

CD에서 설치

CD에서 HP CIFS Client 및 PAM 소프트웨어를 설치하는 경우에는 `swinstall`을 실행하고 CD ROM 저장소 경로에서 HP CIFS Client, PAM NTLM 또는 둘 다를 선택합니다.

소프트웨어 저장소 파일에서 설치

<http://software.hp.com>에서 다운로드할 수 있는 것과 같은 저장소 파일에서 설치하는 경우에는 명령줄에 다음을 입력합니다.

```
swinstall options -s /path/filename B8724AA
```

여기서 각 항목에 대한 설명은 다음과 같습니다.

`options`는 `-x autoreboot=true -x mount_all_filesystems=false`입니다.

`path`는 절대 경로여야 하며 `/tmp`와 같이 `/`로 시작해야 합니다.

`filename`은 다운로드한 저장소 파일의 이름이며 일반적으로 다음과 같은 형식의 긴 이름입니다.

```
B8724AA_A.02...HP-UX_B.11...32+64.depot
```

예제

예를 들어, 다운로드한 저장소 파일을 사용하여 HP-UX 11i v2 시스템에 HP CIFS Client 번들 버전 A.02.01을 설치하려는 경우 명령줄에 아래와 같이 입력합니다.

```
swinstall -x autoreboot=true -x mount_all_filesystems=false\  
-s /tmp/B8724AA_A.02.01_HP-UX_11.23_IA+PA.depot B8724AA
```

3단계: HP CIFS Client 구성

HP CIFS Client 구성 파일인 `/etc/opt/cifsclient/cifsclient.cfg`는 기본값을 수정하지 않고 제공된 상태 그대로 사용할 수 있습니다.

cifsclient.cfg 편집

`/etc/opt/cifsclient/cifsclient.cfg.default` 파일에는 제품 출하 시의 기본 설정이 들어 있습니다. 이 파일을 수정하지 않고 참조용으로 저장하는 것이 좋습니다.

그러나 필요한 경우 아래 설명에 따라 파일을 편집할 수 있습니다.

1. WINS 조회를 사용하려면 `nbnsWinsIp` 매개 변수를 WINS 서버의 IP 주소로 설정합니다. 자세한 내용은 37페이지의 “이름 확인: NetBIOS 이름 서비스, WINS, DNS, IP 구성”을 참조하십시오.
2. 국제화된 클라이언트를 구성합니다.

CIFS Client는 국제화된 다양한 클라이언트 및 서버와 작동하도록 설계되었습니다. 또한 Unicode를 사용하여 네트워크상에서 멀티바이트 문자를 전송하거나, `/etc/opt/cifsclient/unitables`에 있는 임의의 문자 인코딩 테이블을 사용할 수 있습니다. 테이블의 색인에 대해서는 해당 디렉토리에 있는 **README** 파일을 참조하십시오.

각 테이블은 클라이언트 또는 서버에서 파일 및 디렉토리 이름 인코딩을 위해 구성할 수 있는 문자표 파일입니다(파일 내용은 변경되지 않음). CIFS Client 콘솔에 표시되는 문자 집합은 제품과 함께 제공된 많은 문자표 파일 중 원하는 것을 선택하는 `clientCharMapFile` 매개 변수를 통해 구성됩니다. CIFS Server와의 통신을 위한 문자 변환은 Unicode로 수행하거나 문자표 파일을 선택하는 데 사용되는 구성 매개 변수 `serverCharMapFile`을 통해 수행할 수 있습니다. Unicode 사용 여부는 `useUnicode` 매개 변수를 이용하여 설정하거나 해제합니다.

`cifsclient.cfg`의 기본 설정은 다음과 같습니다.

```
serverCharMapFile = "/etc/opt/cifsclient/unitables/unimapCP437.cfg";
clientCharMapFile = "/etc/opt/cifsclient/unitables/unimap8859-1.cfg";
```

예를 들어, CIFS Client가 *Shift-JIS* 로케일을 사용하는 일본어 시스템으로 구성 되어 있고, 마찬가지로 *Shift-JIS*를 사용하는 일본어 CIFS Server에 연결되어 있으면 다음과 같이 구성할 수 있습니다.

```
serverCharMapFile = "/etc/opt/cifsclient/unitables/unimapShiftJIS.cfg";
clientCharMapFile = "/etc/opt/cifsclient/unitables/unimapShiftJIS.cfg";
```

3. 인증 방법

authenticationMethod 매개 변수는 ntlm 또는 kerberos로 설정해야 합니다. 자세한 내용은 3장의 "HP CIFS Client에서 Kerberos 사용"을 참조하십시오.

4. NTLM 암호의 암호화

Kerberos를 사용하지 않는 서버의 경우, 구성 매개 변수 ntlmEncryptionVersion을 ntlm 또는 ntlmv2로 구성하여 사용할 NTLM 버전을 결정할 수 있습니다. 자세한 내용은 3장의 "인증 구성"을 참조하십시오.

5. 서버별 구성

CIFS Client에서는 서버별로 전역 설정을 재정의하는 방법을 제공합니다. 예를 들어, ntlmEncryptionVersion을 전역적으로 NTLM으로 설정했지만 *cifshostA* 서버에서 NTLMv2만 사용하도록 하려면, "servers" 섹션 내에 다음 섹션을 만들 수 있습니다(CIFS Client 구성 파일 맨 끝에 있는 예제 참조).

```
cifshostA = {
    ntlmEncryptionVersion = ntlmv2;
};
```

4단계: HP CIFS Client 데몬 시작 및 중지

`cifsclient` 명령을 사용하여 HP CIFS Client를 시작 및 중지할 수 있습니다.

구문은 다음과 같습니다.

`cifsclient {start | stop}`

`cifsclient`를 인수 없이 사용하면 `cifsclient start`와 같습니다. HP CIFS Client가 실행 중인 상태에서 명령을 실행한 경우 이미 실행 중이라는 메시지가 나타납니다.

`cifsclient` 명령의 `stop` 옵션을 사용하면 HP CIFS Client를 중지할 수 있습니다.

CIFS Client는 종료할 때 먼저 CIFS 공유의 마운트를 모두 해제하려고 시도합니다. 마운트를 해제할 수 없으면 종료가 완료되지 않습니다.

자세한 내용은 **명령줄 유틸리티** 장의 `cifsclient` 맨페이지를 참조하십시오.

HP CIFS Client 사용

이 절에서는 HP CIFS Client 사용 방법에 대해 간단히 설명합니다. 기본 절차는 (1)데몬 시작, (2)공유 디렉토리 마운트, (3)CIFS Server에 로그인입니다. 다음은 이러한 단계와 기타 유용한 추가 정보에 대한 예제입니다.

1. 데몬을 시작합니다.

일반적으로 **root**로 로그인한 시스템 관리자는 시스템 시작 시 다음 명령을 입력합니다.

```
$ cifsclient start
CIFS Client started; process id: 12783
```

상태 확인이 필요한 경우 다음을 입력합니다.

```
$ cifsclient status

path:      /opt/cifsclient/sbin/cifsclientd
version:   FILESET HP CIFS CLIENT: Version: A.02.01
           Compiled on HP-UX B.11.11, s785/C360, 03/05/30,
           13:34:15
           cifsclientd: ver_id=1291218999
cksum:    2781544263
status:    CIFS Client is up; process id 12783,
           started Apr 13
mntck:     ok
```

또한 실행 플래그가 1로 설정되도록 */etc/rc.config.d/cifsclient* 파일을 편집하여 (**RUN_CIFSCLIENT=1**) 부팅 시에 CIFS Client를 자동으로 시작하도록 HP-UX 시스템을 구성할 수 있습니다. 등호 양 옆에 공백이 있어서는 안 됩니다. 이 옵션을 사용하는 경우에도 시스템을 부팅한 후에도 HP CIFS Client를 중지 및 다시 시작할 수 있습니다.

2. CIFS Server에서 공유를 마운트하고 마운트 해제합니다.

이 작업은 **root**로 수행해야 합니다. HP CIFS Client가 마운트한 원격 디렉토리는 먼저 HP CIFS Server에서 공유로 구성해야 합니다.

다음 예제에서는 HP CIFS Server *buildsys*에서 공유로 구성된 공유 *source*를 CIFS Client에서 */home/devl/source* 디렉토리를 마운트 지점으로 사용하여 마운트합니다. 마운트 지점으로 사용되는 디렉토리는 기존 디렉토리여야 하며 절대 경로로 지정해야 합니다.

마운트하려면 다음 명령을 사용합니다.

```
$ mount -F cifs buildsys:/source /home/dev1/source
```

마운트를 해제하려면 마운트 지점만 지정하면 됩니다.

```
$ umount /home/dev1/source
```

3. 클라이언트에서 마운트 지점을 통해 공유 디렉토리를 액세스합니다.

CIFS 프로토콜을 사용하여 서버 또는 도메인 컨트롤러에 의해 인증된 사용자만 마운트된 디렉토리에 액세스하도록 허용할 수 있습니다. 이 작업은 `cifslogin` 명령을 사용하여 수행합니다.

다음 예제에서는 서버에 공유 *source*가 구성되었습니다. 클라이언트의 사용자 *joe*가 *buildsys*의 공유 디렉토리에 액세스하려고 합니다. 먼저 서버에 로그인하지 않은 상태로 디렉토리를 마운트 지점으로 변경하려 합니다(실패함).

그런 다음 사용자는 `cifslogin` 명령으로 *buildsys*에 로그인하여 *buildsys*의 인증을 받고 **CIFS Client**의 마운트 지점을 통해 공유된 *source* 디렉토리에 액세스할 수 있습니다. **CIFS Server**에 로그인하는 데 사용되는 사용자 이름은 **Client**의 현재 **HP-UX** 로그인 이름과 다를 수 있습니다. *cifslogin*에서 사용하는 계정과 암호 쌍은 인증을 수행하는 시스템에 있어야 합니다.

또한 서버가 **HP-UX** 시스템인 경우 서버를 액세스하는 클라이언트의 모든 사용자는 파일 소유권의 일관성이 유지되도록 양쪽 시스템에서 *uid*가 같아야 합니다.

```
$ whoami
joe
cd /home/dev1/source
sh: /home/dev1/source: not found
```

사용자가 아직 **CIFS Server** *buildsys*에 로그인하지 않았기 때문에 이 명령은 실패합니다.

```
$cifslogin buildsys joe
Remote user joe's password: *****
```


이 명령은 성공합니다. `cifslist` 명령을 사용하여 결과를 확인할 수 있습니다. `cifslist` 명령을 옵션 없이 사용하면 서버에 공유 및 마운트 지점 정보가 표시되며, 서버에서는 마운트된 객체를 `\\server\share` 형식으로 나타냅니다.

```
$ cifslist
```

Mounted Object	Mountpoint	State
\\buildsys\source	/home/devl/source	M

```
=====
```

Server	Local User	Remote User	Domain	State
buildsys	joe	joe		L

`cifslist -x` 명령을 사용하여 결과를 확인하는 경우 출력에서는 마운트된 객체를 UNIX 형식 `server:/share`로 표시하여 서버의 공유 및 마운트 지점 정보를 보여줍니다.

```
$ cifslist -x
```

Mounted Object	Mountpoint	State
buildsys:/source	/home/devl/source	M

```
=====
```

Server	Local User	Remote User	Domain	State
buildsys	joe	joe		L

```
$ cd /home/devl/source
```

이 명령은 위의 `cifslogin` 때문에 성공합니다.

`source`가 마운트되고 사용자 `joe`가 `buildsys`에서 인증된 위의 예제를 사용하는 경우 `lucy`라는 사용자는 다음과 같이 이 마운트를 액세스합니다.

```
$ cifslogin buildsys lucy
Remote user lucy's password: *****
```

`cifslist` 명령을 사용하여 결과를 확인할 수 있습니다.

HP CIFS Client 사용

```
$ cifslist
Mounted Object          Mountpoint              State
-----
\\BUILDSYS\source      /home/dev1/source      M
=====
Server      Local User  Remote User  Domain  State
-----
buildsys    joe        joe         buildsys L
buildsys    lucy       lucy        buildsys L
```

로컬 사용자(HP-UX 계정 이름)가 원격 사용자(CIFS Server 계정 이름)와 같을 필요는 없습니다. 앞의 예제에서 로컬(HP-UX) 사용자 *lucy*는 CIFS 계정 이름이 *lucille*인 경우 다음과 같이 로그인할 수 있습니다.

```
$ cifslogin buildsys lucille
Remote user lucille's password: *****
```

`cifslist` 명령을 사용하여 결과를 확인할 수 있습니다.

```
$ cifslist
Mounted Object          Mountpoint              State
-----
\\BUILDSYS\source      /home/dev1/source      M
=====
Server      Local User  Remote User  Domain  State
-----
buildsys    joe        joe         buildsys L
buildsys    lucy       lucille     buildsys L
```

`cifslist` 명령을 사용하여 HP CIFS Client의 내부 테이블을 보는 방법에 대한 자세한 내용은 5장, 69페이지의 “명령줄 유틸리티”를 참조하십시오.

마운트 및 로그인을 한 단계로 처리

root 사용자는 `cifslogin` 명령을 명시적으로 실행할 필요 없이 CIFS 파일 시스템 마운트와 CIFS Server 로그인을 한 단계로 처리할 수 있습니다. 위의 예에서 사용한 이름을 사용합니다.

```
$ mount -F cifs -o username=x,password=y buildsys:/source /home/dev1/source
```

여기서 *x* 및 *y*는 서버에서 인식하는 이름 및 암호 쌍입니다.

`cifsmount` 명령도 같은 기능을 수행합니다. 위의 예에서 사용한 이름을 사용합니다.

```
$ cifsmount -U <username> [-P<password>] //buildsys/source \
/home/dev1/source
```

명령줄에 `-P password`를 지정하지 않는 경우 `cifsmount`에서 암호를 입력하라는 메시지를 표시합니다.

CIFS Client 로깅

CIFS Client에서는 수행되는 작업에 대해 로그 파일을 생성합니다. 예를 들어, 소프트웨어 내의 서로 다른 모듈에 대한 작업에 대해 다양한 수준의 로깅을 설정하거나 해제할 수 있습니다. 자세한 내용은 96페이지의 “CIFS Client 로그 파일 및 로그 수준”을 참조하십시오.

CIFS 파일 시스템 자동 마운트

명시적으로 단일 마운트를 만드는 `mount` 명령(이전 절에서 설명) 외에 CIFS 파일 시스템의 마운트를 관리하는 다른 방법이 있습니다. 이 절에서 설명하지 않는 `mount_cifs` 및 `umount_cifs`의 자세한 구문 정보는 5장을 참조하십시오.

/etc/fstab 사용

`/etc/fstab`에 항목을 만들면 단일 명령을 수동으로 입력하여 하나 이상의 CIFS Server에서 부팅 시에 자동으로 CIFS 파일 시스템을 마운트하거나 다중 CIFS 파일 시스템을 마운트할 수 있습니다. 이 항목의 형식은 다음과 같습니다.

```
server:/share mount_point cifs defaults 0 0
```

이 파일 형식에 대한 자세한 내용은 `fstab(4)` 맨페이지를 참조하십시오.

그런 다음, 다음을 입력하여 `/etc/fstab`에 있는 모든 CIFS 항목을 수동으로 마운트합니다.

```
$ mount -aF cifs
```

현재 마운트된 모든 CIFS 파일 시스템을 마운트 해제하려면 다음을 입력합니다.

```
$ umount -aF cifs
```

31페이지의 “HP CIFS Client 사용”의 항목 1에서 설명한 것처럼 부팅 시에 CIFS Client를 시작하도록 시스템을 구성한 경우 이들 명령은 부팅 및 종료 시에 자동으로 수행됩니다.

CIFS Client 마운트 데이터베이스에 마운트 저장

CIFS 마운트 정보를 CIFS 마운트 데이터베이스에도 저장할 수 있습니다. 이렇게 하면 CIFS Client를 시작할 때마다 마운트가 다시 설정됩니다. `cifsdb` 또는 `cifsmount` 명령을 사용하여 마운트를 저장할 수 있습니다. 자세한 내용은 5장, 69페이지의 “명령 줄 유틸리티”를 참조하십시오.

CIFS Client 마운트 데이터베이스 파일은 `/var/opt/cifsclient/cfgdb.ppl`입니다. 이 파일의 경로는 구성할 수 없습니다. 이 파일은 자동으로 생성되며 수동으로 편집해서는 안 됩니다.

이름 확인: NetBIOS 이름 서비스, WINS, DNS, IP 구성

CIFS Client는 CIFS Server를 마운트하려고 시도할 때 먼저 서버에 대한 NetBIOS 연결을 설정해야 하므로 mount 또는 cifsmount 명령에 지정된 서버가 CIFS Server의 NetBIOS(Windows) 이름이어야 합니다. 이름을 IP 주소로 확인하기 위해 CIFS Client는 다음과 같은 순서의 조회 방법을 사용하며 일치하는 것을 찾으면 조회를 중단합니다.

- 구성된 서버별 IP 주소
- WINS 조회
- NetBIOS 브로드캐스트
- DNS 조회

NetBIOS 브로드캐스트 및 DNS만 기본적으로 사용되며 구성 매개 변수인 lookupTryNetbios 및 lookupTryDns를 yes로 설정하여 제어됩니다.

또한 CIFS Client는 WINS(DNS와 유사한 Windows 이름 확인 서비스) 또는 구성 파일의 서버 관련 설정을 사용하여 CIFS Server를 찾습니다. WINS에서는 대부분의 CIFS 환경에 맞는 효율적인 조회 메커니즘을 제공합니다. 이름 확인은 다음과 같이 구성할 수 있습니다.

- WINS를 사용하려면 nbnsWinsIp 매개 변수를 WINS 서버의 IP 주소로 설정합니다. 연결하려는 CIFS Server가 WINS 서버에 등록되어 있어야 합니다. 예를 들어, lookupTrynetbios 및 lookupTryDns 매개 변수를 yes로 설정하고 WINS 서버의 IP 주소를 110.112.114.115로 설정하면 CIFS Client는 WINS 조회, NetBIOS 브로드캐스트, DNS 조회를 차례로 시도합니다.

WINS는 NetBIOS 이름 서비스의 기능이므로 lookupTryNetbios를 사용하지 않도록 설정하면 WINS도 사용할 수 없습니다. 예를 들어, lookupTryNetbios를 no로 설정하면 HP CIFS Client는 nbnsWinsIp 설정을 무시하고 WINS 조회를 전혀 시도하지 않습니다.

- 서버의 NetBIOS 이름이 DNS 이름과 다르고(DNS에서 서버를 확인할 수 없음), 서버가 CIFS Client와 다른 서브넷에 있으며(NetBIOS 브로드캐스트에서 서버를 확인할 수 없음), 서버의 주소가 WINS에 의해 확인되지 않는 경우에는 CIFS Client 구성 파일에서 IP 주소의 서버 항목을 작성해야 합니다.

구성 파일에서 서버 관련 설정을 작성하려면, 먼저 파일 끝에 있는 예제에서 설명한 것처럼 서버 섹션을 만든 다음 ipAddress 매개 변수를 서버의 IP 주소로 설정합니다. 이 경우 구성된 IP 주소가 직접 사용되고 이 서버에 대해 다른 조회 방법을 건너뛸 것입니다.

예를 들면 다음과 같습니다.

```
buildsys = {  
    ipAddress = "110.112.114.115";  
};
```

IP 주소는 반드시 따옴표로 묶어야 합니다.

NetBIOS 브로드캐스트는 클라이언트와 같은 서브넷에 있는 서버에 대해서만 사용할 수 있으며, CIFS Client는 DNS를 사용하여 DNS와 Windows 이름이 동일한 서버에 대해서만 NetBIOS 연결을 설정할 수 있습니다.

HP CIFS Client 파일 및 디렉토리

이 절에서는 HP CIFS Client를 구성하는 주요 파일을 설명합니다.

표 2-1

HP CIFS Client 파일 및 디렉토리

파일/디렉토리	설명
<i>/opt/cifsclient/</i>	모든 CIFS Client 코어 파일 및 관리 파일에 대한 기본 디렉토리입니다.
<i>/opt/cifsclient/bin/</i>	CIFS 이진 파일입니다.
<i>cifsmount</i>	CIFS Server의 CIFS 공유를 마운트합니다. root 사용자만 사용할 수 있습니다.
<i>cifsumount</i>	CIFS 공유를 마운트 해제합니다. root 사용자만 사용할 수 있습니다.
<i>cifsgetkt</i>	Kerberos를 설정할 수 있는 유틸리티입니다. 자세한 내용은 48페이지의 “HP CIFS Client에서 Kerberos 사용”을 참조하십시오.
<i>cifslogin</i>	일반 사용자가 이미 마운트된 CIFS 공유를 사용하려면 먼저 CIFS 구성에 따라 자신의 사용자 이름과 암호를 사용하여 CIFS 도메인/컴퓨터에 로그인해야 합니다.
<i>cifslogout</i>	CIFS 도메인에서 사용자가 로그아웃하는 명령입니다. CIFS 도메인에서 마운트된 공유를 사용할 수 없게 됩니다.
<i>cifslist</i>	Client에서 마운트된 공유를 나열합니다.
<i>cifsclient</i>	CIFS Client의 시작/중지 스크립트입니다. 이 스크립트에 대한 자세한 내용은 "4단계: CIFS Client 시작 및 중지"를 참조하십시오.

표 2-1 HP CIFS Client 파일 및 디렉토리 (계속)

파일/디렉토리	설명
<i>cifsdb</i>	CIFS Client 데이터베이스의 항목을 추가, 수정 및 삭제합니다. 이 항목을 사용하면 CIFS 마운트 및 로그인을 자동으로 수행할 수 있습니다.
<i>/opt/cifsclient/pam</i>	HP CIFS PAM 파일
<i>/opt/cifsclient/sbin</i>	관리자나 root 사용자가 사용하는 CIFS Client입니다. CIFS Client 데몬이 이 디렉토리에 있습니다.
<i>/etc/opt/cifsclient/</i>	CIFS Client 로그, 데이터베이스, 코어 파일 및 기타 임시 파일의 디렉토리입니다.
<i>cifsclient.cfg</i>	CIFS Client 데몬이 액세스하는 구성 파일입니다.
<i>cifsclient.cfg.default</i>	출하 시 기본 설정이 들어 있으며 참조용으로 사용됩니다. 이 파일을 수정하지 마십시오.
<i>/etc/opt/cifsclient/unitables</i>	국제화된 클라이언트를 위한 문자표입니다.
<i>pam/smb.conf</i>	PAM 구성 파일입니다. 필요에 따라 수정해야 합니다. 이 파일에 대한 자세한 내용은 "6장: PAM NTLM"을 참고하십시오.
<i>pam/smb.conf.default</i>	기본 PAM 파일입니다. <i>pam/smb.conf</i> 로 복사해서 사용해야 합니다. 이 파일을 수정하지 마십시오.
<i>/var/opt/cifsclient</i>	CIFS Client 로그 파일인 <i>pid</i> 파일 및 클라이언트에서 자체적으로 사용하기 위해 만든 임시 파일의 디렉토리입니다.

3 CIFS 보안 및 인증

이 장에서는 CIFS 보안과 Windows NT LanManager(NTLM), NTLMv2 및 Kerberos를 사용한 인증 방법에 대해 설명합니다. 이 장의 구성은 다음과 같습니다.

- 43페이지의 “소개”
- 45페이지의 “사용자 로그인 절차”
- 47페이지의 “Kerberos 소개”
- 48페이지의 “HP CIFS Client에서 Kerberos 사용”
- 52페이지의 “CIFS Client Kerberos 인증 정책”
- 53페이지의 “패킷 서명”

소개

CIFS 파일 공유 프로토콜의 중요한 특성 중 하나는 보안 모델입니다. CIFS Client의 사용자가 CIFS Server의 마운트 지점에 액세스하려면 서버의 인증을 받아야 합니다(사용자가 서버에 로그인해야 함). 네 가지 로그인 방법을 사용할 수 있으며 이에 대해서는 다음 페이지에서 설명합니다. 서버의 파일 시스템에서 파일 또는 디렉토리 수준의 제한 역시 서버에 의해 부여됩니다.

인증 방법

HP CIFS Client는 두 가지 인증 프로토콜을 지원합니다. 이러한 프로토콜은 시스템 관리자가 CIFS Client 구성 파일에서 전역적으로 또는 특정 서버를 기반으로 구성합니다.

- Windows NT LanManager(NTLM) 및 NTLMv2

NTLM은 챌린지 응답 프로토콜입니다. 서버는 챌린지 키를 클라이언트로 보내고 클라이언트는 이를 사용자 암호로 암호화하여 서버로 다시 보냅니다. 서버가 클라이언트와 동일한 암호화를 수행하고 클라이언트 요청과 일치하는지 확인합니다. 사용자 암호와 유사한 것은 네트워크를 통해 전송될 수 없습니다. HP CIFS Client는 NTLM 및 NTLMv2(NTLM 버전 2)를 지원합니다. NTLMv2는 동일한 챌린지 응답 프로토콜을 사용하지만 NTLM보다 복잡한 암호화 알고리즘을 제공하므로 암호를 더 잘 보호할 수 있습니다.

- Kerberos

Kerberos는 분산 인증 서비스로서 사용자 대신 실행 중인 클라이언트가 나중에 공격자가 사용자를 가장하여 침입할 위험이 있는 데이터를 네트워크를 통해 전송하지 않고도 응용 프로그램 서버에 자신을 입증할 수 있도록 해줍니다. Kerberos는 NTLM 프로토콜에 비해 훨씬 향상된 기능을 제공하는 안전한 업계 표준의 인증 프로토콜입니다.

인증 구성 설정

구성 매개 변수인 authenticationMethod 및 ntlmEncryptionVersion은 HP CIFS Client 구성 파일의 서버 섹션에서 전역적으로 지정됩니다. 또한 구성 파일의 사용자 정의 섹션 또는 서버별 섹션에서 설정할 수도 있습니다. 아래에 있는 서버별 구성

부분을 참조하십시오. 이러한 매개 변수는 CIFS Client가 CIFS Server에 대해 사용자를 인증하는 메커니즘을 선택하는 데 사용됩니다.

authenticationMethod 매개 변수에 대한 올바른 항목은 ntlm 또는 kerberos입니다. 이 매개 변수의 기본값은 ntlm입니다. Kerberos를 사용하려는 경우 구성 설정은 다음과 같습니다.

```
authenticationMethod = kerberos;
```

이 경우 CIFS Client는 CIFS Server와 초기 연결을 수행할 때 Kerberos를 사용하도록 요청합니다. 서버의 응답이 긍정적이면 이 서버에 사용자를 인증할 때 Kerberos만 사용되며, 그렇지 않은 경우 NTLM이 사용됩니다. NTLM 프로토콜을 사용하는 경우 CIFS Client는 ntlmEncryptionVersion 구성에 따라 사용할 NTLM 버전을 결정합니다.

종래의 Windows NT LAN Manager(NTLM) 프로토콜을 사용하려면 authenticationMethod 매개 변수를 ntlm으로 설정합니다. 이런 경우 CIFS Client는 ntlmEncryptionVersion 구성에 따라 사용할 NTLM 버전을 결정합니다.

ntlmEncryptionVersion 매개 변수에 대해 유효한 항목은 ntlm 또는 ntlmv2입니다. Kerberos를 사용하지 않는 CIFS Server의 경우 NTLMv2 암호의 암호화만 사용하려면 ntlmEncryptionVersion 매개 변수를 ntlmv2로 설정합니다. 그렇지 않고 NTLM 암호의 암호화만 사용하려면 이 매개 변수를 ntlm으로 설정합니다. 기본적으로 ntlmEncryptionVersion 매개 변수는 ntlm으로 설정되어 있습니다.

서버별 구성

CIFS Client는 서버별로 전역 설정값을 재정의할 수 있는 방법을 제공합니다. 예를 들어, ntlmEncryptionVersion을 NTLM으로 전역적으로 설정하였으나 서버 *buildsys*는 NTLMv2만 사용하도록 하려면 포함하는 "cifs" 섹션 내에 다음 섹션을 만들 수 있습니다(CIFS Client 구성 파일 맨 끝에 있는 예제 참조).

```
buildsys = {  
    ntlmEncryptionVersion = ntlmv2;  
};
```

사용자 로그인 절차

- 명시적 로그인(cifslogin)

CIFS Client의 사용자들은 `cifslogin` 명령을 사용하여 CIFS Server에 명시적으로 자신을 인증할 수 있습니다. **명령줄 유틸리티** 장의 `cifslogin` 맨페이지를 참조하십시오.

- 자동 로그인

CIFS Client에서는 마운트된 CIFS 파일 서버에 자동으로 액세스할 수 있는 방법이 있습니다. CIFS 마운트 지점에서의 초기 액세스 요청(`cd`, `ls` 등)을 통해 CIFS Client는 사용자를 백그라운드 로그인시킵니다. 백그라운드 로그인이 정상적으로 이루어지면 사용자의 액세스 요청은 올바르게 이루어진 것이며 `cifslogin` 명령은 필요하지 않습니다.

CIFS Client의 자동 로그인 정책은 다음과 같습니다.

1. Kerberos: kinit 및 PAM Kerberos와의 통합

Kerberos 인증이 구성되어 있고 사용자가 시스템 Kerberos 자격 증명 캐시에 TGT(Ticket-Granting Ticket)를 가지고 있는 경우(`kinit(1)` 명령으로 명시적으로 작성되거나 PAM Kerberos에 의해 자동 작성됨) 및 마운트된 CIFS Server와 협상하여 Kerberos를 사용하는 경우 CIFS Client는 TGT를 사용하여 자동 로그인을 수행합니다. CIFS Client에서 Kerberos 인증을 사용하는 방법에 대한 자세한 내용은 48페이지의 “HP CIFS Client에서 Kerberos 사용”을 참조하십시오.

2. PAM NTLM과의 통합

PAM NTLM이 `/etc/pam.conf`에서 시스템에 구성되어 있고 사용자가 PAM NTLM을 사용하여 CIFS Client HP-UX 호스트에 로그인한 경우 CIFS Client는 사용자의 캐시된 PAM NTLM 자격 증명을 다시 사용하여 CIFS Server로 사용자를 인증하려고 합니다. PAM NTLM에 대한 자세한 내용은 8장을 참조하십시오.

3. 사용자 데이터베이스

PAM NTLM 자격 증명을 찾을 수는 없지만 CIFS Client 사용자 데이터베이스에 항목이 있는 경우 CIFS Client는 사용자 데이터베이스의 암호화된 암호를 사용하여 CIFS Server로 사용자를 로그인하려고 시도합니다. 암호화된

암호를 저장하려면 먼저 수동 로그인에 성공해야 합니다. `cifslogin -s` 또는 `cifsd` 명령을 사용하여 사용자 데이터베이스에 항목을 저장하거나 `cifsd -d` 명령을 사용하여 사용자 데이터베이스에서 항목을 삭제할 수 있습니다. 자세한 내용은 5장, 69페이지의 “명령줄 유틸리티”의 `cifslogin` 및 `cifsd` 맨페이지를 참조하십시오.

주

Kerberos는 사용자 데이터베이스를 사용한 자동 로그인을 지원하지 않습니다.

4. 게스트 사용자

이 기능을 통해 마운트된 **CIFS Server**에 로그인하지 않은 **HP CIFS Client** 호스트상의 모든 사용자는 게스트 사용자의 권한으로 서버의 마운트 지점에 액세스할 수 있습니다. 7장의 `guestRemoteUser` 매개 변수에서 자세한 정보를 참조하십시오.

게스트 사용자 기능을 설정하려면 `guestRemoteUser` 및 `guestPassword` 구성 매개 변수를 서버상에서 유효한 계정의 구성 매개 변수로 설정합니다. 게스트 사용자의 액세스 권한을 제한할 수 있도록 서버의 일반적인 게스트 사용자 계정을 설정하는 것이 좋습니다. 이제 **CIFS Server**에 로그인하지 않은 **CIFS Client HP-UX** 호스트의 **Unix** 사용자가 마운트된 공유에 액세스하려고 시도하면 해당 사용자는 게스트 사용자로서 명시적인 `cifslogin`을 수행하지 않고 자동으로 해당 공유에 액세스하게 됩니다.

Kerberos 소개

Kerberos는 분산 인증 서비스로서 프린시펄(사용자) 대신 실행 중인 프로세스(클라이언트)가 나중에 공격자 또는 검증자가 프린시펄을 가장하여 침입할 위험이 있는 데이터를 네트워크를 통해 전송하지 않고도 검증자(응용 프로그램 서버 또는 단순한 서버)에 자신을 입증할 수 있도록 해줍니다. Kerberos는 클라이언트와 서버간에 보내지는 데이터에 대한 무결성과 기밀성을 선택적으로 제공합니다. [B. Clifford Neuman, Theodore Tso: *Kerberos: An Authentication Service for Computer Networks*]

Kerberos는 MIT(Massachusetts Institute of Technology)에서 개발되었습니다.

지금까지 CIFS Client와 Server에서 사용해 오던 NT LanManager(NTLM) 프로토콜에 비해 CIFS 환경에서 Kerberos를 사용함으로써 크게 향상된 보안 기능을 누릴 수 있게 되었습니다.

Kerberos 사용에 대한 요구 사항 및 제한 사항

Kerberos Key Distribution Center 및 CIFS Server

HP CIFS Client는 Windows 2000 및 Windows 2003 KDC(Key Distribution Center)만 지원합니다.

획득되지 않는 티켓

이 릴리즈에서 다음과 같은 티켓 유형은 HP CIFS Client가 획득할 수 없습니다.

- 갱신 가능
- 프록시 가능
- 전달 가능

주

영역간 인증은 이 릴리즈에서 지원되지 않습니다.

HP CIFS Client에서 Kerberos 사용

HP CIFS Client에서 Kerberos를 사용하려면 다음 절차를 수행해야 합니다.

1단계. 기본적인 Kerberos 작동 원칙을 검토합니다.

2단계. Kerberos 하부 구조를 설치 및 검증합니다.

3단계. HP CIFS Client에 Kerberos를 구성합니다.

1단계. 기본적인 Kerberos 작동 원칙 검토

Kerberos의 기본적인 기능이나 작동에 대해 잘 알지 못한다면 다음 자료들을 참조하십시오.

다음 HP-UX 리소스에서는 Kerberos의 핵심 내용을 설명합니다(각 설명서의 **개요** 장 참조). 이 내용을 참조하면 성공적으로 설치할 수 있습니다.

- *Configuration Guide for Kerberos Client Products on HP-UX:*
<http://docs.hp.com/hpux/onlinedocs/T1417-90005/T1417-90005.html>
- *Installing, Configuring and Administering the Kerberos Server on HP-UX 11i:*
<http://docs.hp.com/hpux/onlinedocs/T1417-90001/T1417-90001.html>
- *Installing, Configuring and Administering the Kerberos Server V 2.0 on HP-UX 11i:*
<http://docs.hp.com/hpux/onlinedocs/T1417-90003/T1417-90003.html>

<http://docs.hp.com>에서 kerberos를 검색하면 다른 HP-UX 리소스를 찾을 수 있습니다.

Kerberos 프로토콜에 대한 보다 자세한 내용은 다음 자료들을 참조하십시오.

- *Kerberos: An Authentication Service for Computer Networks*, B. Clifford Neuman and Theodore Ts'o:

<http://www.isi.edu/gost/publications/kerberos-neuman-tso.html>

- Kerberos 개발 주체인 MIT(Massachusetts Institute of Technology)의 문서 저장소:

<http://web.mit.edu/kerberos>

- Kerberos 사양, RFC 1510. 메시지 교환에 대한 소개(1절)와 설명(3절):

<http://ftp.rfc-editor.org/in-notes/rfc1510.txt>

- Microsoft 웹 사이트에서도 몇몇 정보용 문서를 찾을 수 있습니다. 이들 문서에는 대개 Windows 컴퓨터로 이루어진 네트워크에서 보안을 설정하는 방법에 대한 실제적인 정보도 들어 있습니다. 다음에서 kerberos 또는 관련 주제를 검색하십시오.

<http://www.microsoft.com>

2단계. Kerberos 하부 구조 설치 및 검증

HP CIFS Client에서 Kerberos를 사용하려면 먼저 HP-UX 호스트를 포함하는 사용자 네트워크에서 작동하는 Kerberos 하부 구조(CIFS Client와 별도로야 함)가 있어야 합니다. Kerberos 하부 구조는 다음과 같이 구성됩니다.

- KDC(Key Distribution Center)
- Kerberos를 지원하는 최소 하나의 CIFS Server. 이 서버는 KDC 도메인 (Kerberos 용어로는 "영역"이라 함)의 구성원이어야 합니다.
- KDC에서 최소 하나의 사용자 계정
- HP CIFS Client가 실행 중인 시스템에서 적절하게 설치 및 구성된 HP-UX Kerberos Client

주

네트워크상의 Windows 서버에서 도메인 이름 서버(DNS)가 활성화되어 있는 것이 좋습니다. 연결하려는 CIFS Server를 KDC가 인식하도록 하려면 해당 서버가 Windows DNS 테이블에 구성되어 있어야 합니다.

Windows 2000 또는 2003 Server에서 KDC(Key Distribution Center)를 설치하는 방법은 Microsoft 설명서를 참조하십시오.

CIFS Client와의 Kerberos를 통해 연결하려는 CIFS Server를 Windows 도메인에 포함시켜야 합니다. 자세한 내용은 Windows 온라인 도움말 또는 **HP CIFS Server 관리자 설명서**를 참조하십시오.

Windows KDC에서 사용자 계정을 설정하는 방법은 온라인 도움말에서 사용자 도메인 계정 관리 부분을 참조하십시오.

HP-UX Kerberos 클라이언트를 설치하려면 위 1단계에서 소개된 구성 설명서를 참조하십시오. *kerberos(9)*, *krb5.conf(4)*, *kpasswd(1)*, *kinit(1)*, *klist(1)*, *kdestroy(1)* 등의 HP-UX 맨페이지에서도 유용한 정보를 찾을 수 있습니다.

일단 Kerberos 하부 구조의 이들 요소를 설치하고 나면 다음과 같은 점검을 통해 모든 것이 제대로 작동하고 있는지 확인해야 합니다. 이러한 확인 단계를 수행하지 않고 3단계로 진행하지 마십시오.

- KDC에서 사용자 계정이 올바르게 설정되었는지, KDC에 Kerberos 인증 서비스가 올바르게 설치되었는지, HP-UX Kerberos 클라이언트가 올바르게 통신할 수 있는지 확인하려면 다음과 같이 입력합니다.

```
$ kinit name
```

여기서 *name*은 사용자 이름 중 하나입니다. 정상적으로 작동하면 *name*에 대해 TGT(Ticket-Granting Ticket)가 발행될 것입니다. 실제로 TGT가 발행되었는지 확인하려면 *klist* 명령을 실행하여 시스템 Kerberos 캐시에 저장되어 있는 티켓의 내용을 표시합니다.

- CIFS Server가 KDC에서 구성원 서버로 제대로 구성되었는지 확인하려면 */opt/cifsclient/bin*에 있는 테스트 프로그램 *cifsgetttkt*를 다음 명령을 통해 실행하십시오.

```
$ cifsgetttkt -s server
```

여기서 *server*는 CIFS Server 중 하나입니다. 이 명령은 *kinit*로 획득한 TGT를 사용하여 TGT(Ticket-Granting Ticket)로부터 서비스 티켓(ST)을 요청합니다. *cifsgetttkt*는 테스트용으로만 사용되므로 시스템 Kerberos 캐시를 수정하지 않지만 콘솔에 정보 메시지가 생성됩니다.

이러한 확인 단계를 정상적으로 수행하면 CIFS Client 및 서버에 대한 Kerberos 인증이 올바르게 이루어져야 합니다. 이제 3단계로 넘어갈 준비가 되었습니다.

3단계. HP CIFS Client에 Kerberos 구성

구성 매개 변수 authenticationMethod를 kerberos로 설정합니다. 구성 설정은 다음과 같습니다.

```
authenticationMethod = kerberos;
```

서버에 활성 CIFS 마운트 또는 로그인이 없는지 확인한 다음 45페이지의 “사용자 로그인 절차”에 설명된 대로 로그인합니다.

Kerberos가 사용되고 있는지 확인하려면 로그 수준 cifstrace와 인증을 사용합니다. 로그 수준 및 로그 파일에 대한 자세한 내용은 96페이지의 “CIFS Client 로그 파일 및 로그 수준”을 참조하십시오. Kerberos가 협상되어 사용자 인증에 사용되고 있는지 확인한 다음 cifstrace 및 인증 로깅을 사용하지 않도록 설정합니다.

CIFS Client Kerberos 인증 정책

이 절에서는 CIFS Server와 Client가 Kerberos를 사용한다고 가정합니다.

명시적 로그인: cifslogin

Kerberos 인증은 이 명령에 투명하게 구현됩니다. 필요한 Kerberos 자격 증명(TGT와 ST)은 사용자 대신 KDC로부터 획득되고 서비스 티켓(ST)은 SESSION_SETUP 요청 내에서 CIFS Server로 보내집니다. 사용자가 특별히 다른 조치를 취할 필요는 없습니다.

자동 로그인: 시스템 Kerberos 캐시와 통합(kinit(1) 및 PAM Kerberos)

이 기능을 통해 사용자는 cifslogin을 사용하지 않고 마운트된 CIFS Server에 액세스할 수 있습니다. 시스템 Kerberos 캐시에 *kinit(1)* 또는 PAM Kerberos를 사용하여 만들어진 미리 존재하던 TGT(Ticket-Granting Ticket)가 있는 경우 CIFS 마운트 지점에 직접 액세스를 시도할 수 있습니다(cd, ls 등). CIFS Client는 TGT를 사용하여 마운트된 CIFS Server에 대해 서비스 티켓(ST)을 획득하고 모두 백그라운드에서 CIFS 로그인을 수행합니다. 이 경우 명시적으로 cifslogin을 실행할 필요가 없습니다.

티켓 수명

최대 티켓 수명은 KDC 구성에 의해 제어됩니다. cifslogin의 경우 CIFS Client는 TGT에 대해 30일의 수명을 요청합니다. 따라서 CIFS Client로 발행되는 TGT의 실제 수명은 30일 미만이며 KDC에서 최대 값으로 구성됩니다. 자동 로그인의 경우 사용자 ST의 만료 시간은 시스템 캐시의 TGT 만료 시간과 같습니다.

패킷 서명

CIFS 패킷 서명의 목적은 끼어들기(man-in-the middle) 공격을 예방하는 것입니다. 각 SMB 패킷에 대한 고유한 서명을 요청하여 클라이언트와 서버가 수동으로 다른 사람의 ID를 확인합니다. 다음 용어는 동일한 의미를 가지며 서로 구분 없이 사용할 수 있습니다.

- 보안 서명
- 패킷 서명(packet signing)
- 패킷 서명(Packet signatures)
- 디지털 서명
- 메시지 무결성
- 메시지 인증 코드(MAC)

패킷 서명은 서버당 연결을 기준으로 수행됩니다. 일단 서버와 패킷 서명을 협상하고 나면 첫번째 사용자의 로그인 요청 및 그 이후의 모든 SMB 패킷은 서명되어야 합니다.

HP CIFS Client에서의 패킷 서명 구성

HP CIFS Client 구성 파일에서 지정한 구성 매개 변수 smbPacketSigning이 CIFS Client에서의 패킷 서명 방식을 지정합니다. 이 매개 변수에 대해 유효한 항목은 enabled, required 및 disabled입니다. 기본적으로 이 매개 변수는 enabled로 설정되어 있습니다.

패킷 서명은 클라이언트와 서버 간에 초기 연결을 설정할 때 협상됩니다. 또한 서버의 구성을 사용하도록, 사용하지 않도록 또는 반드시 사용하도록 할 수 있습니다. 연결하려면 표 3-1에서처럼 클라이언트와 서버 간의 설정을 동기화해야 합니다.

표 3-1 smbPacketSigning에 대한 구성 옵션

유효한 옵션	설명
enabled	HP CIFS Client가 CIFS Server와 연결되며 서버에서 서명을 지원하는 경우 패킷을 서명합니다. HP CIFS Client가 CIFS Server와 연결되어 있지만 CIFS Server에서 서명을 지원하지 않는 경우 CIFS Server는 패킷을 서명하지 않습니다.
required	CIFS Server에서 반드시 서명을 지원해야 합니다. 서버에서 패킷 서명을 지원하지 않으면 CIFS Client에서 CIFS Server와 연결을 설정하지 않습니다.
disabled	HP CIFS Client가 패킷 서명을 사용하지 않습니다. CIFS Server가 서명을 요청하면 클라이언트가 서버에 연결할 수 없습니다.

4

HP CIFS Client A.01에서 A.02로 마이그레이션

HP CIFS Client A.02.*는 대부분의 경우 구성을 최소한으로 변경하면서 새로운 기능을 제공합니다.

그러나 HP CIFS Client A.01.* 버전과 HP CIFS Client A.02.* 버전 사이에는 구성 매개 변수와 명령 옵션에 약간의 차이가 있습니다. 이 장에서는 그러한 차이와 CIFS Client 업그레이드를 계획하고 수행할 수 있도록 업데이트 절차를 설명합니다. 이 장의 구성은 다음과 같습니다.

- 57페이지의 “HP CIFS Client A.01.* 버전에서 A.02.* 버전으로 마이그레이션”
- 60페이지의 “HP CIFS Client A.01.* 및 A.02.*의 기능적 차이”
- 61페이지의 “HP CIFS Client A.01.* 및 A.02.*의 구성적 차이”
- 65페이지의 “HP CIFS Client A.01.* 및 A.02.*의 명령 옵션 차이”

HP CIFS Client A.01.* 버전에서 A.02.* 버전으로 마이그레이션

HP CIFS Client 버전 A.01.* 사용자를 위한 지침

주

이러한 마이그레이션 절차는 다음과 같은 사용자를 위한 것입니다.

- CIFS Client A.01.* 버전으로 되돌리려는 사용자
- CIFS Client 구성 파일의 수정 버전을 사용하는 사용자
- CIFS Client 데이터베이스에서 마운트 또는 사용자 항목을 사용하는 사용자

CIFS Client A.01.* 버전에서 사용하는 구성 파일 및 사용자 데이터베이스 파일은 A.02.* 버전에서는 인식되지 않습니다. HP CIFS Client의 A.01.* 버전을 사용하고 `cifsclient.cfg`를 수정하였거나 CIFS Client 데이터베이스에 사용자 또는 마운트 항목이 있는 경우에는 CIFS Client A.01.* 버전을 A.02.* 버전으로 업데이트하기 전에 다음 지침을 따르십시오.

A.01 설치에서 데이터 보존

다음 절차에서는 구성 파일 및 데이터베이스 파일을 저장합니다. 데이터베이스에 저장된 사용자 및 마운트의 ASCII 목록도 A.02에서 해당 항목을 다시 작성할 수 있도록 저장됩니다. A.02 버전에서 데이터베이스 항목을 관리하는 방법에 대한 자세한 내용은 5장, 69페이지의 “명령줄 유틸리티”의 `cifsdb`, `cifsmount` 및 `cifslogin`을 참조하십시오.

이러한 데이터를 보존하면 A.01 버전으로 되돌릴 때 다시 사용할 수 있습니다.

다음 절차에 따라 구성 파일 및 데이터베이스 파일을 저장합니다.

단계 1. 백업 디렉토리를 만듭니다.

```
$ cd /var/opt/cifsclient
$ mkdir A.01_migration_files
```

- 단계 2. 백업 디렉토리에 구성 파일을 저장합니다. 구성 파일의 수정 버전을 사용하지 않는 경우에는 이 단계를 생략합니다.
- ```
$ cp /etc/opt/cifsclient/cifsclient.cfg A.01_migration_files/A.01.cfg
```
- 단계 3. `cifslist -U` 명령을 사용하여 데이터베이스에 저장된 사용자 기록의 ASCII 목록을 생성하여 백업 디렉토리에 저장합니다. 데이터베이스에 사용자 기록이 없으면 이 단계를 생략합니다(기록이 있는지 확인하려면 `cifslist -U` 사용). A.02 버전에서 사용자 데이터베이스 항목을 다시 생성할 때 이 목록을 참조할 수 있습니다.
- ```
$ cifslist -U > A.01_migration_files/A.01.udb.users.list
```
- 단계 4. `cifslist -M` 명령을 사용하여 데이터베이스에 저장된 마운트 기록의 ASCII 목록을 생성하여 백업 디렉토리에 저장합니다. 데이터베이스에 마운트 기록이 없으면 이 단계를 생략합니다(기록이 있는지 확인하려면 `cifslist -M` 사용). A.02 버전에서 마운트 데이터베이스 항목을 다시 생성할 때 이 목록을 참조할 수 있습니다.
- ```
$ cifslist -M > A.01_migration_files/A.01.udb.mounts.list
```
- 단계 5. CIFS Client 데이터베이스를 백업 디렉토리에 보존합니다. 위의 3, 4 단계를 생략한 경우에는 이 단계도 생략합니다.
- ```
$ mv cifsclient.udb A.01_migration_files/A.01.udb
```

주

CIFS Client 데이터베이스는 다른 요소 중에서 HP-UX 파일 시스템에 있는 데이터베이스의 `inode`를 사용하여 암호화됩니다. 이 방법은 데이터베이스가 다른 컴퓨터로 이동되는 것을 방지하는 보안 수단입니다. 따라서 CIFS Client A.01 버전으로 되돌리려면 데이터베이스의 `inode` 번호를 보존해야 합니다. 그렇지 않으면 CIFS Client가 데이터베이스를 해독할 수 없습니다. `inode` 번호를 보관하려면 `mv` 명령을 사용하여 동일한 논리 볼륨으로 데이터베이스를 백업해야 합니다. 파일의 `inode`를 변경하는 `cp` 또는 기타 다른 Unix 명령을 사용하지 마십시오. `mv` 명령을 사용하여 CIFS Client 데이터베이스를 백업합니다.

A.01 버전으로 되돌리기

HP CIFS Client의 A.02 버전보다 A.01 버전이 더 적절하다고 판단한 경우 다음 단계에 따라 최신 A.01 릴리즈 버전으로 되돌릴 수 있습니다.

- 단계 1. A.02 버전을 제거합니다. 제거가 완료되면 시스템이 재부팅됩니다.

```
$ swremove -x autoreboot=true -x mount_all_filesystems=false B8724AA
```

- 단계 2. <http://software.hp.com>에서 CIFS Client A.01 버전의 최신 릴리즈를 다운로드합니다.
- 단계 3. 다운로드한 CIFS Client 저장소를 설치합니다. 설치에 관한 자세한 내용은 27페이지의 “2단계: HP CIFS Client 및 PAM 소프트웨어 설치”를 참조하십시오.
- 단계 4. 위에 있는 "A.01 설치에서 데이터 보존" 절의 2단계에서 이전 구성 파일을 보존한 경우에는 `/etc/opt/cifsclient`로 해당 구성 파일을 복원합니다.
- 단계 5. "A.01 설치에서 데이터 보존" 절의 5단계에서 이전 데이터베이스 파일을 보존한 경우에는 `/var/opt/cifsclient`로 해당 구성 파일을 복원합니다. "A.01 설치에서 데이터 보존" 절의 5단계에서 설명한 대로 `mv` 명령을 사용하여 데이터베이스 파일을 보존해야 합니다.

HP CIFS Client A.01.* 및 A.02.*의 기능적 차이

다음은 HP CIFS Client A.01.* 및 A.02.*의 기능적 차이에 대해 설명합니다.

- HP CIFS Sever A.02.01에서는 서버에 대한 마지막 마운트를 해제하여도 서버에 로그인한 사용자를 로그아웃하지 않습니다. HP CIFS Client A.01.x 이전 버전은 마지막 공유가 마운트 해제될 때 사용자를 로그아웃합니다. A.02.01 버전의 이러한 새로운 동작은 시스템 관리자가 공유를 마운트 해제했다가 다시 마운트할 때 사용자가 자동으로 다시 연결되도록 해줍니다.
- HP CIFS Server A.02.01에서 `cifslist` 명령은 공유 및 마운트 지점 정보 외에도 `state` 정보를 표시합니다.

다음은 `cifslist` 출력에 나오는 `State` 기호에 대한 설명입니다.

마운트의 경우:

M = 마운트됨

S = 마운트 데이터베이스에 저장됨

R = 읽기 전용

사용자의 경우:

L = 로그인됨

S = 사용자 데이터베이스에 저장됨

HP CIFS Client A.01.* 및 A.02.*의 구성적 차이

구성 파일의 주석

HP CIFS Client A.01.*에서는 여러 개의 주석 태그가 사용되었습니다.

HP CIFS Client A.02.*에서는 # 문자로 주석을 시작하며 # 문자와 줄 끝까지의 텍스트가 주석입니다.

구성 매개 변수의 차이점

이 절에서는 다음과 같이 HP CIFS Client A.01.* 및 A.02.* 간의 구성 매개 변수 차이점에 대해 설명합니다. A.01.* 버전과 A.02.* 버전 간에 변경되지 않은 매개 변수에 대해서는 설명하지 않습니다. 이 절에서는 제거된 매개 변수 목록, 새 매개 변수 목록 및 HP CIFS Client A.02.*에서 변경된 매개 변수 이름 목록을 제공합니다. CIFS 구성 매개 변수에 대한 자세한 내용은 101페이지의 “구성 매개 변수”를 참조하십시오.

제거된 구성 매개 변수

다음은 HP CIFS Client A.02.*에서는 더 이상 사용되지 않는 A.01.* 구성 매개 변수 목록입니다.

- runAsUser
- databaseFile
- mtabName
- maxOpenFiles

매개 변수 이름 변경 사항

표 4-1은 HP CIFS Client A.02.*에서 이름이 변경된 A.01.* 구성 매개 변수 목록입니다.

표 4-1

매개 변수 이름 변경 사항

A.01.*	A.02.*
allowSaving	usersMayStoreSessionData
netbiosName	localNetbiosName
nfsAttributeCaching	nfsKernelCacheTime
authenticationLevel	authenticationMethod
dirDefaultLinks	fakedDirLinks
dirSize	fakedDirSize
guestUser	guestRemoteUser

새 구성 매개 변수

다음은 HP CIFS Client A.02.*의 logLevels 섹션에 대한 새로운 구성 매개 변수 목록입니다.

- smbConnect
- uiTrace
- nbnsTrace
- diskarb
- authentication

다음은 HP CIFS Client A.02.*의 Global 섹션에 대한 새로운 구성 매개 변수 목록입니다.

- corefileLimit
- networkInterfaces
- bindUdpExplicitly
- pagePoolInitialSize

다음은 HP CIFS Client A.02.*에서 nfs3 고유의 새로운 구성 매개 변수 목록입니다.

- cacheFiles
- cacheOpenFiles
- changeMicrosecondFileTimes
- nfsKernelCacheTime
- preferredPort

다음은 HP CIFS Client A.02.*에서 cifs 고유의 새로운 매개 변수 목록입니다.

- databaseParseInterval
- initialDataCaches
- initialDirCaches
- bindNbnsPort
- bindNbdgsPort
- lookupTryNetbios
- lookupTryDns
- nbnsWinsIp
- nbnsInitialTimeout
- nbnsTotalTimeout
- nbnsCacheTime

다음은 HP CIFS Client A.02.*에서 server 고유의 새로운 매개 변수 목록입니다.

- ntlmEncryptionVersion

HP CIFS Client A.01에서 A.02로 마이그레이션

HP CIFS Client A.01.* 및 A.02.*의 구성적 차이

- guestPassword
- allowHardLinks
- hardlinkUseRemoteCopy
- fileModeMask
- dirModeMask
- ctimeIsCreate
- smbPacketSigning

HP CIFS Client A.01.* 및 A.02.*의 명령 옵션 차이

이 절에서는 HP CIFS Client A.01.*과 A.02.* 간의 명령 옵션 차이에 대해 다음 표에서 설명합니다. 이 표에는 A.01.* 버전과 A.02.* 버전 간에 변경되지 않은 명령 옵션은 표시되어 있지 않습니다. 자세한 내용은 5장, 69페이지의 “명령줄 유틸리티”를 참조하십시오.

표 4-2는 A.01.* 버전과 A.02.* 버전 간의 cifsmount 명령 옵션 차이 목록을 보여 줍니다.

표 4-2

cifsmount

A.01.*	A.02.*	비고
-c <클라이언트 netbios 이름>	구성 매개 변수 전용: localNetbiosName	구성 파일로 이동됨
-p <tcp 포트>	구성 매개 변수 전용: bindNbnsPort	구성 파일로 이동됨
-I <ip 주소 또는 호스트 이름>	구성 매개 변수 ipAddress	구성 파일로 이동됨
구성 매개 변수 domain 전용	-D <도메인>	-D 옵션으로 구현되었으며 A.02.*에서 구성 매개 변수임

표 4-3은 A.01.* 버전과 A.02.* 버전 간의 mount -F cifs 명령 옵션 차이 목록을 보여 줍니다.

표 4-3 **mount_cifs**

A.01.*	A.02.*	비고
-o nbname=		A.02.*에서 구성 파일로 이동됨
-o port=		A.02.*에서 구성 파일로 이동됨
	-o domain=	A.02.*의 새 옵션
-o forcemnt		HP CIFS Client A.02.*에서 제거됨. 항상 true

표 4-4는 A.01.* 버전과 A.02.* 버전 간의 cifslist 명령 옵션 차이 목록을 보여 줍니다.

표 4-4 **cifslist**

A.01.*	A.02.*	비고
	-r	A.02.*의 새 옵션
	-s	A.02.*의 새 옵션
-s server, -m share	-m (추가 인수 없음)	
-u server	-u (추가 인수 없음)	
-A, -S		A.02.*에서 제거됨
	-x	A.02.*의 새 옵션
-U, -M		A.02.*에서 제거됨. 항상 true

표 4-5는 A.01.* 버전과 A.02.* 버전 간의 cifslogin 명령 옵션 차이 목록을 보여 줍니다.

표 4-5

cifslogin

A.01.*	A.02.*	비고
명령줄에서 지정한 사용자 이름	-U 사용자 이름	A.02.*에서는 -U 옵션을 사용하거나 사용하지 않고 사용자 이름을 지정할 수 있음
	-D 도메인	A.02.*의 새 매개 변수로서 구성된 값을 재정의

표 4-6은 A.02.*에서 새롭게 구현된 cifsdب 명령에 대한 설명입니다.

표 4-6

cifsdб

A.01.*	A.02.*	비고
	cifsdб <server>	
	cifsdб -d <server>	
	cifsdб <mount_point>	
	cifsdб -d <mount_point>	

HP CIFS Client A.01에서 A.02로 마이그레이션
HP CIFS Client A.01.* 및 A.02.*의 명령 옵션 차이

5 명령줄 유틸리티

이 장에서는 CIFS Client의 명령줄 유틸리티에 대해 자세히 설명합니다.

HP CIFS Client 소프트웨어 패키지는 다음과 같은 프로그램으로 구성되어 있습니다.

<code>cifsclient</code>	CIFS Client 를 시작하고 중지합니다.
<code>cifsmount</code>	원격 서버에서 디렉토리를 마운트합니다.
<code>cifslogin</code>	사용자를 원격 서버에 인증합니다.
<code>cifsumount</code>	로컬 마운트 지점이 아무 곳에도 마운트되어 있지 않은 경우 서버에서 해당 마운트 지점의 연결을 끊습니다.
<code>cifslogout</code>	사용자 로그인 세션의 연결을 끊고 지정된 서버에서 서버 공유 연결을 끊습니다. 로그아웃한 다음에는 해당 서버의 파일에 액세스할 수 없습니다.
<code>cifslist</code>	연결된 서버, 마운트 지점, 마운트된 공유 등을 나열합니다.
<code>cifsdb</code>	CIFS Client 데이터베이스에 항목을 추가, 수정 및 삭제합니다. 이 항목을 사용하면 CIFS 마운트 및 로그인을 자동으로 수행할 수 있습니다.
<code>mount_cifs</code>	<code>mount (1M)</code> 를 사용하여 CIFS 파일 시스템을 마운트합니다.
<code>umount_cifs</code>	<code>umount (1M)</code> 를 사용하여 CIFS 파일 시스템의 마운트를 해제합니다.

또한 위에서 설명한 각 유틸리티의 유일한 매개 변수로 지정하여 `-h` 및 `-v` 옵션을 사용할 수 있습니다. `-h` 옵션은 표준 오류에 대한 간략한 도움말을 표시하며 `-v` 옵션은 현재 버전 번호를 표준 출력에 표시합니다.

cifsclient

구문

```
cifsclient { command }
cifsclient fuser [-v] mountpoint [...]
cifsclient force_umount {mountpoint [...] | -a}
```

설명

이 셸 스크립트는 **HP CIFS Client**를 시작 및 중지하고 다른 유용한 작업을 수행하는데 사용됩니다. root 자격을 갖는 사용자만이 start, stop, restart, fuser 및 force_umount를 호출할 수 있습니다(klist 및 kdestroy에 -a 옵션을 지정하는 것도 참조하십시오). status, klist, kdestroy 및 ver는 어떤 사용자든 실행할 수 있으며 cifsclient에 아무런 명령도 추가하지 않으면 cifsclient start와 같습니다.

명령

start	데몬을 시작합니다.
stop	데몬을 종료합니다.
restart	중지했다가 1초간 휴면 상태를 유지한 다음 다시 시작합니다.
status	데몬에 대한 정보를 표시합니다.
klist [-a]	모든 호출 사용자의 CIFS Client Kerberos 자격 증명 파일의 내용을 표시합니다. 이 명령은 모든 사용자의 자격 증명 파일에서 klist(1)을 호출하며 각 파일에 대해 자동으로 -c {filename} 옵션을 추가합니다. -a(root만 사용할 수 있음)는 모든 사용자에 대한 항목을 나열합니다. CIFS Client Kerberos 자격 증명 파일은 rmTmpKerbCredFiles 구성 매개 변수가 no로 설정된 경우에 만 시스템에 존재하게 됩니다. 이 파일은 <i>/var/opt/cifsclient/krb5_tmp</i> 에 있습니다.
kdestroy [-a]	kdestroy(1)를 사용하여 호출한 사용자의 CIFS Client Kerberos 자격 증명 파일을 모두 삭제합니다. 하나의 CIFS Kerberos 자격 증명 파일을 삭제하려면 -c {filename} 옵션을

지정하여 직접 `kdestroy(1)`을 사용하십시오. **CIFS Client Kerberos** 자격 증명 파일은 `/var/opt/cifsclient/krb5_tmp`에 있습니다. 이 파일들은 `rmTmpKerbCredFiles` 구성 매개 변수가 `no`로 설정된 경우에만 시스템에 존재합니다. `-a` (root만 사용할 수 있음)는 모든 사용자의 모든 파일을 삭제합니다.

`ver [-v]` 버전 정보를 보고합니다. 다음 변경자도 인식됩니다.
`-v` 상세 정보 표시: 이진, 스크립트 및 구성 파일에 대해 `what(1)` 문자열을 표시합니다.

`fuser [-v] mountpoint [...]`

주어진 **CIFS** 파일 시스템 마운트 지점과 하위 디렉토리 각각에 대해 `fuser -fu`를 실행합니다(`fuser(1M)` 참조). 이것은 마운트 해제가 실패하고 "**Device busy**" 메시지가 표시되는 경우 어떤 사용자가 마운트에 액세스하고 있는지 판별하는 데 유용합니다. 이 명령을 유효하게 사용하려면 마운트된 **CIFS** 파일 서버에 로그인해야 합니다. `-v` 명령을 사용하면 자세한 정보가 출력됩니다(모든 하위 디렉토리가 표시됨). 그렇지 않은 경우 활성화된 사용자 프로세스가 있는 디렉토리만 표시됩니다.

참고: 이 명령의 실행 시간은 마운트된 파일 시스템의 항목 수에 비례합니다.

`force_umount {mountpoint [...] |-a}`

지정된 마운트 지점에서 강제로 마운트를 해제하며 이는 표준 `umount` 명령이 작동하지 않을 때에만 사용하는 비상 절차입니다.

`umount mountpoint`

또는

`cifsumount mountpoint`

`-a` 잘못된 **CIFS** 마운트를 모두 강제로 마운트 해제합니다.

CIFS Client가 중지되어야 사용할 수 있습니다.

파일

`/etc/opt/cifsclient/cifsclient.cfg`

이 파일은 HP CIFS Client에 대한 런타임 구성 옵션을 포함합니다. 자세한 내용은 7장을 참조하십시오.

```
/var/opt/cifsclient/krb5_tmp/krb5cc_<server>_<uid>
```

임시 CIFS Client Kerberos 자격 증명 파일입니다. <server>는 사용자가 인증된 CIFS Server의 이름이고 <uid>는 사용자의 10진수 UID입니다.

관련 항목

cifsmount, fuser(1M), kdestroy(1), klist(1), mount_cifs, umount_cifs

cifsmount

`mount` 명령을 사용하여 `cifsmount` 명령을 실행할 수 있습니다. 두 명령은 다음과 같습니다.

구문

```
cifsmount [<options>] //<server>/<share> <mountpoint>
```

설명

`cifsmount` 명령은 로컬 파일 시스템에서 원격 공유를 마운트하는 데 사용됩니다. 이 명령은 `<mountpoint>`에 있는 로컬 파일 시스템에서 `<server>` 서버의 `<share>` 공유를 마운트합니다. 마운트 지점이 존재해야 합니다. 사용자가 암호를 입력하면 프로그램에서 사용자 이름/암호 조합을 사용하여 서버에 로그인합니다. 현재 사용자가 지정된 서버에 로그인한 상태인 경우 암호를 입력하는 과정이 생략됩니다. 암호를 묻지 않도록 `-N` 옵션을 사용할 수 있습니다.

root 권한이 있는 사용자만이 `cifsmount` 명령을 사용하여 파일 시스템을 마운트할 수 있습니다.

옵션

`-r` 읽기 전용 파일 시스템으로 마운트합니다.

`-U <username>`

이 사용자로 서버에 로그인합니다. 기본적으로 HP CIFS Client는 `cifsmount` 명령을 실행한 사용자의 로그인 이름과 같은 사용자 이름으로 서버를 액세스합니다. 서버에서 다른 사용자 이름을 사용하는 경우 이 옵션을 사용하여 해당 이름을 설정할 수 있습니다. 서버에 로그인된 상태이면 이 매개 변수는 무시됩니다.

`-D <domain>` 이 도메인 이름을 CIFS Server로 보냅니다.

`-P <password>`

명령줄에 지정한 암호입니다. `ps` 명령의 출력에 모든 명령줄 매개 변수가 표시되므로 필요한 경우에만 이 옵션을 사용하십시오. 이 매개 변수를 사용하면 동적으로 생성한 암호를 서버에 전달할

수 있습니다. 사용자가 서버에 로그인된 상태이면 암호가 무시됩니다.

- S **stdin**에서 암호를 읽습니다. 셸 스크립트나 기타 프로그램에서 **cifs mount**를 사용하려는 경우 이 옵션이 유용합니다. **Unix**의 **ps** 명령으로 실행 중인 프로세스의 명령줄 매개 변수를 표시할 수 있기 때문에 이러한 용도로 **-P** 옵션을 사용하는 것은 보안 상의 문제가 있습니다.
- N 암호를 묻지 않습니다. 사용자에게 암호가 없는 경우 암호를 묻지 않도록 하는 데 이 옵션을 사용할 수 있습니다.
- u 일반 텍스트 암호를 사용할 수 있도록 설정합니다. 보안 상의 위험이 있기 때문에, 기본적으로 **HP CIFS Client**는 암호를 일반 텍스트로 서버에 전송하지 않습니다. 네트워크에서 일반 텍스트 암호를 스니핑할 수 있는 도구가 있습니다. 서버가 암호의 암호화를 지원하지 않아서 불가피하게 암호를 일반 텍스트로 전송해야 하는 경우 이 옵션을 사용하여 일반 텍스트로 전송할 수 있습니다. 서버에 로그인된 상태이면 이 매개 변수는 무시됩니다.
- f 강제로 마운트합니다. 이 옵션을 사용하면 서버가 응답하지 않는 경우에도 마운트가 수행됩니다. 서버에 요청을 보내지 않습니다. 따라서 유효성을 확인할 수 있는 매개 변수가 없습니다.
- v 버전 정보를 인쇄합니다.
- s 마운트 및 암호를 데이터베이스에 저장합니다. 보안 관련 사항을 이해하는 경우에만 사용하십시오. **HP CIFS Client**는 마운트, 사용자 이름 및 암호를 데이터베이스로 유지 관리할 수 있습니다. 이 데이터베이스는 시작 시에 저장된 마운트를 다시 연결하고 사용자가 클라이언트에 로그인하지 않은 경우에도 필요한 경우 사용자를 로그인시키는 데 사용됩니다.

이 옵션은 자동 마운트와 사용자에게 암호를 요구하는 기능이 없는 **cron** 유틸리티로 프로그램을 실행하는 경우에 유용합니다. 암호는 **HP CIFS Client**의 사용자 데이터베이스 파일에 저장됩니다. 이 파일 자체로 충분하지는 않지만 이 파일을 통해서 암호의 **CIFS** 해시 값(기능적으로 암호 자체에 해당)을 얻을 수 있는 가능성이 있습니다.

따라서, 컴퓨터에 대한 물리적 액세스 권한 및 **root** 액세스 권한을 가진 유일한 사용자인 경우 또는 파일을 액세스하는 모든 사용자를 신뢰할 수 있는 경우에만 이 옵션을 사용하는 것이 안전합니다. **HP CIFS Client**는 암호화되지 않은 암호를 사용자 데이터베이스에 저장하지 않습니다. 서버가 암호화된 암호를 지원하지 않는 경우 이 옵션을 사용할 수 없습니다.

예제

다음 명령은 로컬 마운트 지점 */mounts/bigserver*에서 bigserver 서버로부터 entiredisk 공유를 읽기 전용 파일 시스템으로 마운트합니다.

```
cifsmount -r //bigserver/entiredisk /mounts/bigserver
```

파일

cifsmount -s 명령을 사용하는 마운트 정보는 **HP CIFS Client**의 데이터베이스 파일인 */var/opt/cifsclient/cfgdb.ppl*에 저장됩니다. 이 파일의 경로는 구성할 수 없습니다.

관련 항목

cifslogin, cifsumount, cifslogout, cifslist

cifslogin

구문

```
cifslogin [<options>] <servername> [<username>]
```

```
cifslogin [<options>] //<servername>/<share>
```

설명

cifslogin 명령은 서버에서 추가 사용자를 인증하는 데 사용됩니다. 인증된 사용자만 마운트된 파일을 액세스할 수 있습니다. 각 사용자는 서버에서 자신의 권한 상태에 따라 해당 서버에 있는 파일을 액세스합니다. 로컬 사용자는 원격 사용자와 일대일(다대일) 매핑 관계여야 하므로 각 사용자는 지정된 서버에 한 번만 로그인할 수 있습니다. 기본적으로 cifslogin은 서버에 사용자의 로그인 이름을 보냅니다. -U 옵션을 사용하여 사용자 이름을 지정할 수 있습니다.

옵션

-P <password>

명령줄에 지정한 암호입니다. *ps* 명령의 출력에 모든 명령줄 매개 변수가 표시되므로 필요한 경우에만 이 옵션을 사용하십시오. 이 매개 변수를 사용하면 동적으로 생성한 암호를 서버에 전달할 수 있습니다. 사용자가 서버에 로그인된 상태이면 암호가 무시됩니다.

-U <username>

이 사용자로 서버에 로그인합니다.

-D <domain name>

서버로 전송되는 도메인 이름을 지정합니다.

-S

stdin에서 암호를 읽습니다. 셸 스크립트나 기타 프로그램에서 cifslogin을 사용하려는 경우 이 옵션이 유용합니다. **Unix**의 *ps* 명령으로 실행 중인 프로세스의 명령줄 매개 변수를 표시할 수 있기 때문에 이러한 용도로 -P 옵션을 사용하는 것은 보안 상의 문제가 있습니다.

- N 암호를 묻지 않습니다. 서버에 사용자가 로그인한 경우 또는 사용자에게 암호가 없는 경우 암호를 묻지 않도록 이 옵션을 사용할 수 있습니다.
- u 일반 텍스트 암호를 사용할 수 있도록 설정합니다. 보안 상의 위험이 있기 때문에, 기본적으로 **HP CIFS Client**는 암호를 일반 텍스트로 서버에 전송하지 않습니다. 네트워크에서 일반 텍스트 암호를 스니핑할 수 있는 도구가 있습니다. 서버가 암호의 암호화를 지원하지 않아서 불가피하게 암호를 일반 텍스트로 전송해야 하는 경우 이 옵션을 사용하여 일반 텍스트로 전송할 수 있습니다. 서버에 로그인된 상태이면 이 매개 변수는 무시됩니다.
- f 강제로 로그인합니다. 이 옵션을 사용하면 서버가 응답하지 않는 경우에도 로그인 수행됩니다. 서버에 요청을 보내지 않습니다. 따라서 유효성을 확인할 수 있는 매개 변수가 없습니다.
- s 데이터베이스에 암호를 저장합니다. 보안 관련 사항을 이해하는 경우에만 사용하십시오. 이 옵션으로 마운트, 사용자 이름 및 암호 데이터베이스를 유지 관리할 수 있습니다. 이 데이터베이스는 시작 시에 저장된 마운트를 다시 연결하고 사용자가 클라이언트에 로그인하지 않은 경우에도 필요할 경우 사용자를 로그인시키는 데 사용됩니다.

이 옵션은 자동 마운트와 사용자에게 암호를 요구하는 기능이 없는 **cron** 유틸리티로 프로그램을 실행하는 경우에 유용합니다. 암호는 **HP CIFS Client**의 사용자 데이터베이스 파일에 저장됩니다. 이 파일 자체로 충분하지는 않지만 이 파일을 통해서 암호의 **CIFS** 해시 값(기능적으로 암호 자체에 해당)을 얻을 수 있는 가능성이 있습니다.

따라서, 컴퓨터에 대한 물리적 액세스 권한 및 **root** 액세스 권한을 가진 유일한 사용자인 경우 또는 파일을 액세스하는 모든 사용자를 신뢰할 수 있는 경우에만 이 옵션을 사용하는 것이 안전합니다. **HP CIFS Client**는 암호화되지 않은 암호를 사용자 데이터베이스에 저장하지 않습니다. 서버가 암호화된 암호를 지원하지 않는 경우 이 옵션을 사용할 수 없습니다.

예제

로컬 사용자인 **steve**가 *bigserver* 서버로부터 공유를 마운트한 경우 로컬 사용자 **bill**은 이 서버에 로그인하지 않았으므로 마운트된 파일에 액세스할 수 없습니다. *bigserver*에서 실제 이름인 **miller**로 계정이 있는 **bill**은 다음 작업을 수행하여 액세스 권한을 얻을 수 있습니다.

```
cifslogin bigserver -U miller
```

bill에게 암호를 입력하라는 메시지가 표시되고 입력한 암호가 올바른 경우 **bill**은 *bigserver*의 사용자 **miller**와 동일한 권한으로 공유에 대한 액세스 권한이 부여됩니다.

파일

사용자 이름 및 암호가 HP CIFS Client의 사용자 데이터베이스 파일에 암호화되어 저장됩니다. 사용자 데이터베이스 파일에 대한 경로는 HP CIFS Client 구성 파일에서 구성할 수 있습니다. 기본 경로는 다음과 같습니다.

```
/var/opt/cifsclient/cifsclient.udb
```

관련 항목

cifsmount, cifsd, cifslogout, cifslist

cifsmount

umount 명령을 사용하여 cifsmount 명령을 실행할 수 있습니다. 두 명령은 다음과 같습니다.

구문

```
cifsmount [<options>] <mountpoint>
```

```
cifsmount -a
```

설명

cifsmount 명령은 *cifsmount*로 마운트된 모든 공유를 마운트 해제하는 데 사용됩니다. 공유를 지정된 마운트 지점에 마운트한 사용자나 슈퍼유저만 해당 공유를 마운트 해제할 수 있습니다. 명령의 두 번째 형태(-a 옵션 사용)는 현재 사용되고 있는 모든 마운트를 마운트 해제합니다.

HP CIFS Sever A.02.01에서는 서버에 대한 마지막 마운트를 해제하여도 서버에 로그인한 사용자를 로그아웃하지 않습니다. HP CIFS Client A.01.x 이전 버전은 마지막 공유 마운트를 해제할 때 사용자를 로그아웃합니다. A.02.01 버전의 이러한 새로운 동작은 시스템 관리자가 공유를 마운트 해제했다가 다시 마운트할 때 사용자가 자동으로 다시 연결되도록 해줍니다.

옵션

- a CIFS 파일 시스템을 모두 마운트 해제합니다.
- f 강제로 마운트 해제합니다. 서버에 요청을 보내지 않습니다(서버 중단 시 유용).

관련 항목

cifsmount, *cifslist*, *mount_cifs*, *umount_cifs*

cifslogout

구문

```
cifslogout <servername>
```

설명

cifslogout 명령은 명령을 사용한 사용자를 지정한 서버에서 로그아웃하는 데 사용됩니다. cifslogout을 실행한 후에는 사용자 데이터베이스에 사용자가 저장되어 있지 않는 한 해당 사용자가 해당 서버의 모든 파일에 액세스할 수 없게 됩니다.

관련 항목

cifslogin, cifslist

cifslist

구문

```
cifslist [<options>]
```

설명

cifslist 명령은 HP CIFS Client의 내부 테이블을 표시하는 데 사용됩니다. HP CIFS Client A.02.*에서 옵션 없이 cifslist 명령을 실행하면 연결된 모든 서버를 공유 및 마운트 지점 정보와 함께 나열합니다.

옵션

- h 간단한 도움말을 인쇄하고 종료합니다.
- u 사용자만 나열합니다.
- m 마운트만 나열합니다.
- x Unix 형식인 `server:/share` 형식을 사용하여 마운트된 객체를 표시합니다.
- r 원시 출력 형식을 인쇄합니다.
- s <separator> 테이블 항목을 구분하는 데 사용되는 문자열을 설정합니다(-r과 함께 사용되는 경우에만 인식됨).

cifslist 출력 예제

이 절에서는 -x, -u 및 -m 옵션이 포함된 cifslist 출력을 예를 들어 설명합니다.

cifslist 명령의 출력 예제는 다음과 같습니다.

```
$ cifslist
```

Mounted Object	Mountpoint	State
\\er721142\pub	/mnt/cifs_linux/00	M
\\er721141\pub	/mnt/cifs_nt/00	M
\\hpntc43\pub	/mnt/cifs_nt/01	MS

Server	Local User	Remote User	Domain	State
er721141	root	cifsuser		L
er721142	root	john		L
hpntc43	root	cifsuser	WORKGROUP	LS

위 예제에서 옵션이 사용되지 않은 cifslist 명령은 공유 및 마운트 지점 정보와 함께 서버를 표시하며 마운트된 객체에 대해 \\server\share 형식을 사용합니다.

다음은 cifslist 출력에 나오는 State 기호에 대한 설명입니다.

마운트의 경우

M = 마운트됨

S = 마운트 데이터베이스에 저장됨

R = 읽기 전용

사용자의 경우

L = 로그인됨

S = 사용자 데이터베이스에 저장됨

다음은 cifslist -x 명령의 출력 예제입니다.

```
$ cifslist -x
```

Mounted Object	Mountpoint	State
er721142:/pub	/mnt/cifs_linux/00	M
er721141:/pub	/mnt/cifs_nt/00	M
hpntc43:/pub	/mnt/cifs_nt/01	MS

Server	Local User	Remote User	Domain	State
er721141	root	cifsuser		L
er721142	root	john		L

```
hpntc43      root          cifsuser     WORKGROUP    LS
```

위 예제에서 **HP CIFS Client**는 공유 및 마운트 지점 정보와 함께 서버를 표시하며 마운트된 객체에 대해 **Unix** 형식인 `server:/share` 형식을 사용합니다.

다음은 `cifslist -u` 명령의 출력 예제입니다.

```
$ cifslist -u
```

Server	Local User	Remote User	Domain	State
er721141	root	cifsuser		L
er721142	root	john		L
hpntc43	root	cifsuser	WORKGROUP	LS

다음은 `cifslist -m` 명령의 출력 예제입니다.

```
$ cifslist -m
```

Mounted Object	Mountpoint	State
\\er721142\pub	/mnt/cifs_linux/00	M
\\er721141\pub	/mnt/cifs_nt/00	M
\\hpntc43\pub	/mnt/cifs_nt/01	MS

위 예제에서 **HP CIFS Client**는 마운트된 객체에 대해 `\\server\share` 형식을 사용합니다.

cifsdb

구문

```
cifsdb [-d] {<mount_point|server>}
```

설명

cifsdb 명령은 CIFS Client 데이터베이스에서 항목을 추가, 수정 및 삭제하는 데 사용됩니다. 아래에 설명된 대로 이 항목을 사용하면 CIFS 마운트 및 로그인을 자동으로 수행할 수 있습니다.

CIFS 마운트

CIFS Server의 공유 디렉토리가 mount_point에서 마운트되면 cifsdb mount_point는 마운트 지점, 서버, 공유 디렉토리 이름 및 CIFS Client 마운트 데이터베이스 파일 /var/opt/cifsclient/cfgdb.ppl 내의 기타 관련 정보, 즉 CIFS Client를 시작할 때마다 자동으로 마운트가 다시 설정되는지 여부 등을 저장합니다. 데이터베이스 내의 해당 마운트 지점에 대한 항목이 이미 존재하면 해당 항목이 대체됩니다. mount_point는 절대 경로여야 합니다. root 권한을 가진 사용자만이 CIFS 마운트 데이터베이스 항목을 관리할 수 있습니다.

HP CIFS Client는 표준 Unix /etc/fstab 메커니즘을 통해 유사한 기능을 지원합니다. 자세한 내용은 36페이지의 “/etc/fstab 사용” 또는 fstab(4)를 참조하십시오.

CIFS 로그인

사용자가 NTLM 인증 프로토콜을 사용하여 server에 CIFS 로그인 세션을 설정한 경우, 해당 사용자가 cifsdb server를 호출하면 사용자 암호의 NTLM 해시 및 사용자가 이후에 자동으로 server에 로그인할 수 있는지 여부 등의 로그인 세션에 관련된 기타 정보가 암호화되어 cifsclient.udb CIFS Client 사용자 데이터베이스에 저장됩니다. 데이터베이스에 이 사용자 서버 쌍에 대한 항목이 이미 존재하면 해당 항목이 대체됩니다.

Kerberos로 인증된 CIFS 로그인인 경우, 사용자의 NTLM 암호 해시가 CIFS Client 사용자 데이터베이스에 저장되지 않습니다. 3장, 41페이지의 “CIFS 보안 및 인증”에서 설명한 것과 같이 kinit(1) 또는 PAM-KERBEROS를 통해 Kerberos를 사용하는 자동 CIFS 로그인을 설정할 수 있습니다.

옵션

-d {<mount_point|server>}

데이터베이스에서 mount_point 또는 server에 대한 항목을 삭제합니다. 마운트 또는 로그인 둘 다 활성 상태가 아니라도 항목을 삭제할 수 있습니다.

파일

/var/opt/cifsclient/cifsclient.ldb

CIFS 사용자 데이터베이스 파일입니다.

/var/opt/cifsclient/cfgdb.ppl

CIFS 마운트 데이터베이스 파일입니다.

관련 항목

cifsmount, cifslogin, cifslist

mount_cifs, umount_cifs

CIFS 파일 시스템을 마운트 및 마운트 해제합니다.

구문

```
mount -F cifs [-ar] [-o option[,option...]] [server:/share mount_point]
umount -aF cifs | mount_point
```

설명

mount 명령은 파일 시스템을 마운트합니다. 슈퍼유저만 파일 시스템을 마운트할 수 있습니다. 다른 사용자는 mount를 사용하여 마운트된 파일 시스템을 나열할 수 있습니다. CIFS별 마운트 및 사용자 연결을 표시하려면 cifslist를 사용합니다.

mount 명령은 *server:/share*를 *mount_point*에 연결합니다. *server*는 원격 시스템입니다. *share*는 이 원격 시스템에 있는 디렉토리이며 *mount_point*는 로컬 파일 트리에 있는 디렉토리입니다. *mount_point*는 이미 존재해야 하며 절대 경로 이름으로 지정해야 합니다. 이 이름이 새로 마운트된 파일 시스템의 **root** 이름이 됩니다.

mount를 인수 없이 호출하는 경우 파일 시스템 마운트 테이블 */etc/mnttab*의 마운트된 파일 시스템이 모두 나열됩니다.

umount 명령은 현재 마운트된 파일 시스템을 마운트 해제합니다. 슈퍼유저만 파일 시스템을 마운트 해제할 수 있습니다.

HP CIFS Sever A.02.01에서는 서버에 대한 마지막 마운트를 해제하여도 서버에 로그인한 사용자를 로그아웃하지 않습니다. 이러한 새로운 동작은 사용자가 공유를 마운트 해제했다가 다시 마운트할 때 자동으로 다시 연결될 수 있도록 해줍니다.

옵션

- F cifs 파일 시스템별 ID입니다. 이것은 *umount mount_point* 형태의 명령을 제외한 CIFS 파일 시스템을 마운트하고 마운트 해제하는데 항상 필요합니다.
- a mount와 함께 사용할 경우 */etc/fstab*에 항목이 있는 모든 CIFS 파일 시스템을 마운트합니다. umount와 함께 사용할 경우 현재 마운트된 모든 CIFS 파일 시스템을 마운트 해제합니다.

- r** 읽기 전용으로 마운트합니다.
- o** 이 유형의 옵션은 다음 형식의 구문을 사용하여 지정합니다.
`-o keywrđ[,keywrđ...],keywrđ=value[,keywrđ=value...]`
즉, 일부 키워드는 키워드/값 쌍으로 지정하고 일부 키워드는 그렇지 않습니다. **-o** 옵션은 쉼표로 구분하며 공백은 사용할 수 없습니다. 예를 들면, 다음과 같습니다.
`-o ro,username=fulton,password=pokey`
다음은 **CIFS Client**가 지원하는 *mount*에 대한 **-o** 옵션입니다. 값이 필요한 키워드는 "**keyword=value**"로 표시합니다.
- ro** 읽기 전용 파일 시스템으로 마운트합니다.
- domain=domain** 이 도메인 이름을 서버로 전송합니다.
- username=name** 서버에 전송할 사용자 이름입니다. 기본적으로 **HP CIFS Client**는 사용자의 로그인 이름과 같은 사용자 이름으로 서버를 액세스합니다. 서버에서 다른 사용자 이름을 사용하는 경우 이 옵션을 사용하여 해당 이름을 설정할 수 있습니다. 서버에 로그인된 상태이면 이 매개 변수는 무시됩니다.
- password=password** 명령줄에 지정한 암호입니다. *ps* 명령의 출력에 모든 명령줄 매개 변수가 표시되므로 필요한 경우에만 이 옵션을 사용하십시오. 이것을 사용하면 동적으로 생성한 암호를 서버에 전달할 수 있습니다. 사용자가 서버에 로그인된 상태이면 암호가 무시됩니다.
- plaintxt** 일반 텍스트 암호를 사용할 수 있도록 설정합니다. 보안 상의 위험이 있기 때문에, 기본적으로 **HP CIFS Client**는 암호를 일반 텍스트로 서버에 전송하지 않습니다. 네트워크에서 일반 텍스트 암호를 스니핑할 수 있는 도구가 있습니다. 서버가 암호의 암호화를 지원하지 않아서 불가피하게 암호를 일반 텍스트로 전송해야 하는 경우 이 옵션을 사용하여 일반 텍스트로 전송할 수 있습니다. 사용자가 서버에 로그인된 상태이면 이 옵션은 무시됩니다.

파일

/etc/mnttab 마운트된 파일 시스템의 테이블입니다.
/etc/fstab 각 CIFS 파일 시스템의 기본 매개 변수를 나열합니다.

관련 항목

mount (1M), *umount*(1M), *cifslogin*, *cifsumount*, *cifslogout*, *cifslist*

명령줄 유틸리티
`mount_cifs, umount_cifs`

6 문제 해결 및 오류 메시지

이 장에서는 HP CIFS Client를 사용할 경우 발생할 수 있는 문제에 대한 정보와 HP CIFS 명령에서 나타날 수 있는 오류 메시지에 대해 설명합니다.

- 93페이지의 “질문과 대답을 통한 문제 해결”
- 94페이지의 “HP CIFS Client에서 Kerberos 문제 해결”
- 96페이지의 “CIFS Client 로그 파일 및 로그 수준”

질문과 대답을 통한 문제 해결

이 절에서는 HP CIFS의 일반적인 문제에 대해 설명합니다.

cifsclient stop 명령으로 데몬을 종료하는 방법

데몬 프로세스를 직접 강제 종료해서는 안됩니다. HP CIFS에서 모든 마운트된 공유를 마운트 해제하려고 시도하지만 성공하지 못할 수 있으며 잘못된 마운트는 사용할 수 없게 되고 문제가 발생합니다. 데몬 프로세스를 종료하는 올바른 방법은 *cifsclient stop*을 사용하는 것입니다.

*cifsclient stop*에 대한 자세한 내용은 이 설명서의 2장에서 "4단계. 클라이언트 시작 및 중지" 부분을 참조하십시오.

데몬이 종료된 경우 처리 방법

데몬이 종료되는 즉시 HP CIFS가 제공하는 모든 공유를 사용할 수 없게 됩니다. NFS 만료 시간(구성 파일에서 구성)이 경과될 때까지 모든 액세스가 정지됩니다. 대부분의 경우 마운트를 사용 중인 모든 프로세스를 즉시 종료하고, 마운트의 모든 현재 디렉토리를 변경한 다음 *cifsclient force_umount <mountpoint>* 명령을 사용하여 멈춘 마운트를 마운트 해제하면 다시 부팅할 필요 없이 문제가 해결됩니다. 이러한 문제가 발생하면 문제 재현 방법과 함께 HP 기술 지원 부서로 알려주십시오.

HP CIFS Client에서 Kerberos 문제 해결

- `cifsTrace`, `authentication log levels`

`cifsTrace` 및 `authentication log levels`를 사용하도록 설정하면 **Kerberos** 처리에 의해 **HP CIFS Client** 로그 파일에 정보용 로그 메시지가 만들어집니다.

- 임시 자격 증명 파일

Kerberos 인증을 사용하는 경우 **HP CIFS Client**는 임시 파일을 사용하여 로그인 처리 중에 사용자의 자격 증명을 저장합니다. 서버 하나, 사용자 하나 당 하나의 임시 자격 증명 파일이 존재합니다. **HP CIFS Client**는 **Kerberos** 티켓을 다시 사용하지 않습니다. 따라서 사용자 로그인 처리가 완료되면 임시 파일은 제거됩니다.

임시 자격 증명 파일이 문제 해결에 필요한 경우 구성 변수

`rmTempKerbCredFiles`를 `no`로 설정하면 파일을 보관할 수 있습니다. 그런 다음 표준 **Kerberos Client** 유틸리티인 `klist(1)` 및 `kdestroy(1)`를 사용하여 파일을 조사하고 제거합니다. 이 명령에 `-c cache_filename` 옵션을 함께 사용할 수 있는데 파일 이름은 다음과 같은 형식으로 지정합니다.

```
/var/opt/cifsclient/krb5_tmp/krb5cc_servername_uid
```

여기서 `servername`은 **CIFS Server**이며 `uid`는 **CIFS Client**가 실행 중인 로컬 **HP-UX** 호스트상에서의 사용자의 **Unix uid**입니다.

`cifsclient` 제어 스크립트는 편의상 파일이나 경로 이름을 참조하지 않고 자격 증명 파일에 대해 작동되도록 할 때 사용할 수 있습니다. 구문 요약은 `cifsclient -h`를 입력합니다.

- 기본적인 **Kerberos** 기능

Kerberos 하부 구조의 기본 기능이 올바르게 작동하지 않는다고 생각될 때는 2단계의 점검 확인을 반복하십시오.

- 특정 서버에 대한 `authenticationMethod` 값을 구성 파일의 `default Server` 섹션의 전역 설정값이 아닌 다른 값으로 설정하려면 `servers` 섹션에서 서버별

옵션을 작성할 수 있습니다. 구성 파일의 `servers` 섹션에 대한 내용은 7장 끝에서 설명되며 구성 파일 자체에는 샘플 `servers` 항목이 포함되어 있습니다.

CIFS Client 로그 파일 및 로그 수준

CIFS Client는 `/var/opt/cifsclient/debug` 디렉토리에 활동에 대해 로그 파일을 생성합니다. 클라이언트가 시작될 때마다 `client-log.pid`라는 새 로그 파일을 생성합니다. 여기서 `pid`는 CIFS Client 데몬인 `cifsclientd`의 HP-UX 프로세스 ID입니다.

일반적으로 로그 파일은 오류 또는 경고만 기록합니다. 그러나 CIFS Client에서는 다양한 모듈 활동을 점검하는 데 여러 가지 로그 수준을 사용할 수 있습니다.

HP에 문제를 보고하면 지원 담당자가 하나 이상의 로그 수준을 사용하도록 요청할 수 있습니다. CIFS Client 구성 파일 `/etc/opt/cifsclient/cifsclient.cfg`를 편집하고 앞에 있는 `#` 문자를 제거하고 파일을 저장하여 특정 로그 수준을 주석처리 하지 않으면 여러 수준의 로그를 사용할 수 있습니다.

CIFS Client를 다시 시작하지 않아도 CIFS Client는 새로 사용할 수 있게 되거나 사용할 수 없게 된 로그 수준을 인식할 수 있습니다.

로깅이 증가하면 디스크 공간을 많이 차지하게 되며 CIFS Client의 성능이 저하됩니다. 따라서 로깅이 필요하지 않을 때는 사용하지 않는 것이 좋습니다. 권장되는 기본 운영 로그 수준을 보려면 `cifsclient.cfg.default` 파일을 참조하십시오.

로그 크기가 50MB에 이르면 파일 이름에 `.prev`가 붙어 복사되고 새 로그 파일이 시작됩니다. 새 로그가 50MB에 이르면 이전 파일을 덮어쓰고 파일 이름에 `.prev`가 붙어 복사됩니다.

7 구성 파일

기본 구성 파일을 수정 없이 사용해도 문제가 없습니다. 작업 내용을 이해하지 못하는 경우에는 구성을 수정하지 마십시오.

구성 파일은 시작 및 편집 시에 **HP CIFS Client** 데몬에 의해 구문 분석됩니다. 실행 중인 데몬이 구성 파일을 다시 읽지만 모든 구성 변경 사항이 즉시 적용되는 것은 아닙니다. 대부분의 옵션은 사용할 때 내부 변수에 할당됩니다. 예를 들어, 서버 구성은 서버 연결이 열릴 때 내부 구조로 전달됩니다. 따라서 서버 구성을 변경하려면 먼저 해당 서버에서 모든 공유를 마운트 해제하고 모든 사용자를 로그아웃해야 합니다.

주

HP CIFS Client A.01.*에 사용된 CIFS Client 구성 파일 `cifsclient.cfg`는 HP CIFS Client A.02.*에 유효하지 않습니다.

일반 구조

구성 파일은 다음과 같은 간단한 구문 구조로 구성됩니다.

- 참고 사항
- 문자열
- 배열
- 디셔너리

문자열, 배열 및 디셔너리는 "속성"이라는 일반 용어로 분류됩니다.

문자는 주석을 나타내며 # 문자와 줄 끝까지의 텍스트가 주석이 됩니다.

```
# remark to end of line
```

문자열은 밑줄을 포함한 일련의 영숫자 문자입니다. 문자열이 공백과 같은 기타 문자를 포함하는 경우 문자열을 큰따옴표로 묶어야 합니다. 큰따옴표 내에서는 C 문자열과 동일한 이스케이프 시퀀스를 사용할 수 있습니다. 숫자 인수에 대한 별도의 구문은 없습니다. 숫자 인수는 문자열로 간주되며 사용할 때 변환됩니다.

배열은 여러 속성의 순서가 지정된 목록입니다. 배열은 괄호로 묶고 배열을 구성하는 속성은 쉼표로 구분합니다. 다음은 여러 문자열 요소로 구성된 배열의 예입니다.

```
(1, 2, 3, hello, "how are you")
```

디셔너리는 명명된 속성의 순서가 지정되지 않은 목록입니다. 이러한 목록은 중괄호로 묶습니다. 각 디셔너리 항목은 문자열인 좌항(키), 등호, 임의 값이 될 수 있는 우항(값)으로 구성됩니다. 각 항목은 세미콜론으로 구분합니다. 다음은 property1부터 property3까지 세 개의 항목으로 구성된 디셔너리의 예입니다. 여기서 첫 번째 항목은 문자열 값, 두 번째 항목은 배열 값, 세 번째 항목은 디셔너리 값을 가집니다.

```
{
    property1 = "value of property1";
    property2 = (value, of, property2);
    property3 = {
        firstWord = value;
        secondWord = of;
        thirdWord = property3;
    }
}
```

```
};  
}
```

구성 파일 자체가 디렉터리입니다. 이 경우 다른 속성을 사용할 수 없기 때문에 중괄호를 생략할 수 있습니다. 최상위 수준의 키는 구성 변수 이름입니다.

문자열로 구분 분석된 속성은 다음 방법 중 하나로 해석할 수 있습니다.

- 문자열
- 숫자
- 열거
- 부울

문자열에 대해서는 따로 설명하지 않습니다. 숫자는 0(8진수) 또는 0x(16진수) 접두사가 없는 경우 10진수로 해석됩니다. 열거는 미리 정의된 문자열 집합의 문자열입니다. 부울 변수는 yes 및 no로 구성된 특수한 열거 집합입니다.

구성 매개 변수

다음은 loglevels, global, nfs, cifs 및 server라는 최상위 5개 수준에서 구성할 수 있는 모든 변수 목록입니다.

logLevels

이 변수 값은 활성화된 모든 로깅 모드를 열거하는 배열입니다. 대괄호 속의 숫자는 로그 파일의 로깅 메시지 유형을 나타냅니다. 로깅 모드는 다음 집합을 구성하는 문자열입니다.

info

[0] 정보 메시지를 로그에 기록합니다. 사용하도록 설정해야 합니다.

error

[1] 오류 메시지를 로그에 기록합니다. 사용하도록 설정해야 합니다.

debug

[2] 일반 디버그 메시지입니다. 디버그 중에만 유용합니다.

resource

[3] 객체 할당 및 할당 취소에 대한 메시지입니다. 디버그 중에만 유용합니다.

netbiosError

[4] Netbios 계층의 오류 메시지를 로그에 기록합니다. 오류가 지나치게 많이 발생하지 않는 한 사용하도록 설정해야 합니다. HP CIFS Client가 Netbios의 기능을 모두 구현하는 것은 아니며 구현되지 않은 기능으로 인해 Netbios 오류 메시지가 발생하므로 이것은 일반 오류 로그와 구분됩니다.

netbiosDebug

[5] Netbios 계층의 디버그 메시지입니다. 디버그 중에만 유용합니다.

netbiosTrace

[6] 모든 Netbios 송신 및 수신 트래픽의 16진수 덤프를 생성합니다. 디버그에는 매우 유용하지만 일반적인 작동에는 사용하지 말아야 합니다.

nfsTrace

[7] 커널에 의해 수행된 모든 NFS 요청과 관련 반환 값에 대한 자세한 정보를 제공합니다. NFS 디버그에는 매우 유용하지만 일반적인 작동에는 사용하지 말아야 합니다.

rare

[8] 거의 발생하지 않는 조건의 로그를 기록합니다. 디버그 중에만 유용합니다.

cacheDebug

[9] 캐시 작동을 디버그합니다. 디버그 중에만 유용합니다.

cifsTrace

[10] 실행된 모든 CIFS 명령과 관련 반환 값의 로그를 기록합니다. 디버그용으로 netbiosTrace와 함께 사용할 경우 매우 유용하지만 일반적인 작동에는 사용하지 말아야 합니다.

oplock

[11] 기회 잠금(opportunistic lock) 메커니즘을 디버그합니다. 디버그 중에만 유용합니다.

warn

[12] 대개 구성 파일 분석기에 의해 사용되는 모든 종류의 경고입니다. 사용하도록 설정해야 합니다.

smbSequence

[13] HP CIFS 요청의 순서와 관련 메시지에 대한 디버그 메시지입니다. 디버그 중에만 유용합니다.

debugAttributes

[14] 파일 속성 루틴의 디버그입니다. 디버그 중에만 유용합니다.

설명 앞에 나오는 대괄호로 둘러싸인 숫자는 로그 출력에서 해당 로깅 모드의 메시지를 나타내는 데 사용됩니다.

smbConnect

[16] NetBIOS의 서버 연결 및 연결 끊기 메시지를 디버그합니다. 디버그 중에만 유용합니다.

uiTrace

[17] 사용자 인터페이스가 사용되는 통신의 16진수 덤프를 생성합니다. 디버그에는 유용하지만 일반적인 작동에는 사용하지 마십시오.

nbnsTrace

[18] 모든 NetBIOS 이름 서비스 트래픽의 16진수 덤프를 생성합니다. 디버그에는 유용하지만 일반적인 작동에는 사용하지 마십시오.

diskarb

[19] 디스크 중재를 디버그합니다. 디버그 중에만 유용합니다.

authentication

[20] CIFS 인증 세부 사항을 디버그합니다. 디버그 중에만 유용합니다.

cfgParseInterval

HP CIFS Client는 실행 중에 구성 파일을 다시 분석할 수 있습니다. 이 기능이 작동하려면 HP CIFS Client가 정기적으로 파일을 폴링해야 합니다. *cfgParseInterval* 변수는 이 폴링 주기를 밀리초 단위로 정의합니다. 0으로 설정할 경우 시작 시에 한 번만 파일을 구문 분석합니다. 기본값은 0입니다.

sockMode **sockOwner** **sockGroup**

HP CIFS Client 데몬과 명령줄 유틸리티 사이의 통신에 사용되는 Unix 도메인 소켓의 파일 액세스 모드와 소유권입니다. 접두사 0을 붙이면 8진수 표현법, 접두사 0x를 붙이면 16진수 표현법, 접두사를 붙이지 않으면 10진수 표현법으로 액세스 모드를 지정

할 수 있습니다. 이름이나 숫자 ID로 소유자 및 그룹을 지정할 수 있습니다. 내용을 이해하지 못하는 경우에는 이 값을 *mode=0600* 및 *owner=root* 이외의 값으로 설정하지 마십시오. 이 **Unix** 도메인 소켓의 파일 액세스 모드는 데몬에 서비스를 요청하는 사용자의 보안 인증을 제공하는 데 사용됩니다. 파일에서 이들 변수를 구성하지 않으면 올바른 기본값으로 설정됩니다.

pidFile

필요에 따라 **HP CIFS Client**가 데몬의 프로세스 ID로 파일을 유지 관리할 수 있습니다. 이 값을 정의한 경우 **pid**를 저장해야 하는 파일의 경로로 해석됩니다. 이 변수를 정의하지 않은 경우 해당 파일이 만들어지지 않습니다.

usersMayStoreSessionData

시스템 관리자는 **usersMayStoreSessionData** 매개 변수를 사용하여 사용자가 사용자 데이터베이스 **cifsclient.udb**에 암호를 저장할 수 있는지 여부를 제어할 수 있습니다. 이 데이터베이스는 **CIFS Server**에 자동 사용자 로그인을 설정하는 데 사용할 수 있습니다. **root** 권한이 있는 사용자는 이 매개 변수의 설정 방법에 관계없이 마운트 또는 암호를 저장할 수 있습니다. 이 매개 변수를 **no**로 설정하면 저장할 수 없습니다. 기본 설정은 **yes**입니다.

caseConvertFile

이 변수는 대소문자 변환 테이블 경로를 구성합니다. 이 파일은 모든 **Unicode** 문자에 대한 대소문자 매핑을 정의합니다. 기본값은 테이블 파일을 사용하지 않는 것이며 기본 **ISO 8859-1** 매핑을 유지합니다. **Unicode** 표준에서 파생된 매핑 파일이 **HP CIFS Client** 배포의 일부로 제공됩니다. 이 파일은 *unitables/unicase.cfg*에서 찾을 수 있습니다.

serverCharMapFile

이 변수는 서버에 대한 문자 매핑 파일 경로를 구성합니다. 클라이언트 및 서버에서 **Unicode**를 사용하지 않을 경우에 사용되는 이 파일은 서버에 보낼 내부 **Unicode** 표현의 **ASCII** 문자열 매핑을 정의합니다(반대의 경우도 정의). 기본값은 미국 영어 **DOS** 문자

집합인 `codepage 437` 매핑입니다. 다양한 문자 집합에 대한 매핑 파일이 HP CIFS Client와 함께 `unitables` 디렉토리에 배포됩니다.

clientCharMapFile

이 변수는 클라이언트에 대한 문자 매핑 파일 경로를 구성합니다. 이 파일은 클라이언트에 표시될 내부 Unicode 표현의 ASCII 문자열을 정의합니다. `serverCharMapFile`과 함께 사용하면 서버와 클라이언트 문자 코드 사이의 모든 변환을 수행할 수 있습니다. 공급업체 특정 문자 집합의 문제를 해결하고 일본어의 JIS 및 ShiftJIS처럼 다양한 국가 문자 집합을 처리하기 위해 이들 테이블을 사용할 수 있습니다. 기본값은 ISO 8859-1 매핑입니다.

uniTableCompressBlocks

이 정수 변수는 Unicode 테이블 압축을 사용자 정의합니다. 값이 클수록 변환 속도가 느려지지만 메모리 효율이 개선됩니다. 사용되지 않은 연속된 코드 블록 수보다 큰 값은 적용되지 않습니다. 기본값은 3입니다.

corefileLimit

이 정수 변수는 데몬이 만드는 최대 코어 덤프 크기를 메가바이트 단위(1024 * 1024바이트)로 정의합니다. 코어 덤프를 사용하지 않으려면 이 값을 0으로 설정하십시오. 기본값은 500(메가바이트 단위)입니다.

networkInterfaces

이 변수는 네트워크 인터페이스를 정의합니다. 구문은 문자열 배열입니다. 각 문자열은 인터페이스의 IP 주소, 슬래시 및 네트워크 주소에 사용되는 비트 수로 구성됩니다(넷마스크 지정의 변형). 이 변수를 구성하려면 `bindUdpExplicitly` 변수 또한 사용하는 것도 좋습니다. 예를 들어 `networkInterfaces = ("192.168.1.21/24", "192.168.2.23/24")`입니다.

bindUdpExplicitly

이 변수가 `yes`로 설정되어 있으면 **HP CIFS Client**가 UDP 포트를 모든 네트워크에 명시적으로 바인딩합니다. 그렇지 않으면 설치된 모든 네트워크 인터페이스에 대한 와일드 카드인 주소 **0.0.0.0**에 바인딩합니다. 브로드캐스트의 소스 IP 주소를 올바르게 처리하지 않는 운영 체제에서 네트워크 인터페이스가 여러 개 있는 경우 명시적으로 바인딩해야 합니다. **HP CIFS Client**는 소켓 옵션 `SO_REUSEADDR`을 사용해야 하며 **Samba**와 동일한 소켓에 바인딩된 경우에 오류가 발생하지 않습니다. 이 옵션을 사용하는 경우에는 `bindNbnsPort` 및 `bindNbdgsPort`에 대해 기본 바인딩 포트를 변경해야 합니다. 기본적으로 이 매개 변수는 `no`로 설정되어 있습니다.

pagePoolInitialSize

이 정수 변수는 모든 공유에 대해 미리 할당된 가상 메모리의 **8k** 페이지의 수를 정의합니다. 기본값은 **128**입니다.

- nfs3** 이 섹션은 특정 구성으로 재정의할 수 있는 기본 동작을 정의합니다. **NFS3** 섹션에는 다음과 같은 매개 변수가 포함됩니다.
- cacheFiles** 이 변수는 **NFS** 핸들이 캐시하는 파일 수를 정의합니다. 기본값은 **500**입니다.
- cacheOpenFiles** 이 변수는 액세스하지 않은 상태에서도 열린 상태로 유지할 수 있는 파일 수를 정의합니다. 기본값은 **20**입니다.
- changeMicrosecondFileTimes**
이 부울 변수는 파일이 액세스될 때마다 파일 수정 날짜의 밀리초 부분을 변경할 것인지 여부를 결정합니다. 수정 날짜를 효과적으로 변경하면 커널의 **NFS** 캐시를 사용하지 않을 수 있습니다. 기본 설정은 **no**입니다.
- fakeDirLinks**
이 변수는 백엔드에서 유효한 값을 제공하지 못할 때 디렉토리에 대해 표시되는 하드 링크 수를 정의합니다. 기본값은 **2**입니다.
- fakeDirSize**
이 변수는 백엔드에서 유효한 값을 제공하지 못할 때 디렉토리에 대해 표시되는 크기를 정의합니다. 블록 크기의 배수로 설정해야 합니다.
- nfsKernelCacheTime**
NFS 커널이 이 시간 동안 캐시됩니다(초 단위). **NFS**로 커널을 캐시할 수 있도록 하는 변수입니다. 이 변수를 사용하면 네트워크로 전송되는 호출 수가 줄어들어 특정 유형의 작업 성능이 향상됩니다. 기본 설정은 **0**초입니다.
- lookupStrategy** 알고 있는 것처럼 **HP CIFS Client**는 **NFS** 요청과 **SMB/CIFS** 요청을 매핑합니다. **NFS**측에서는 **NFS** 파일 핸들이라고 하는 고유 **ID**로 파일을 참조합니다. 하지만 **HP CIFS**측에서는 단순히 파일 경로로 파일을 참조합니다. 따라서 **HP CIFS Client**가 **NFS** 파일 핸들로 지정된 경로를 확인할 수 있어야 합니다. 다음과 같은 두 가지 방법을 사용하여 확인할 수 있습니다.
- **pseudoInode**

이 방법은 경로의 해시 값으로 **NFS** 파일 핸들을 만듭니다. 디렉토리에서 파일 계층 깊이가 27 이하인 경우 효율적인 조회가 가능한 방식으로 해시를 선택합니다. 이 방법의 이점은 메모리 소모가 적다는 것입니다. 필요한 경우 파일을 조회할 수 있으며 메모리에 저장할 사항이 없습니다. 가장 큰 단점은 파일 이름이 변경되면 **NFS** 파일 핸들도 변경된다는 것입니다. 따라서 파일이 열린 상태로 이름이 변경되면 **Unix** 의미론과 충돌하게 됩니다. 즉, 이름을 변경한 후에는 열린 파일의 핸들이 의미가 없어지고 파일을 다시 열지 않으면 액세스할 수 없게 됩니다. 또한 파일을 닫는 동안이 아닌 파일을 닫은 후에 다시 쓰기가 발생하는 **Solaris NFS** 클라이언트의 코드 캐시 버그와 충돌하게 됩니다.

- **database**

이 방법에서는 파일 경로에 대한 모든 **NFS** 파일 핸들 관계가 내부 데이터베이스에 저장됩니다. 이것이 가장 안전하며 호환성이 높은 방법입니다. 단점은 모든 정보를 메모리에 유지한다는 것입니다. 이 방법을 사용하는 경우 **HP CIFS Client**에 공유 당 500kB 이상의 실제 메모리와 약 10MB 이상의 가상 메모리가 필요합니다.

database 방법이 기본값입니다.

nfsTimeout

이 정수 변수는 커널에서 **HP CIFS Client**에 데이터를 요청할 때 사용되는 초기 제한 시간(1/10초)을 정의합니다. 재시도를 할 때 마다 이 값이 두 배가 됩니다. *nfsRetransmit*와 함께 사용하면 이 변수로 **NFS** 요청의 절대 제한 시간을 정의할 수 있습니다. 값이 50(5초)이면 이미 실행 중인 느린 요청을 자주 재시도하지 않으며 총 제한 시간이 약 2분이 되게 할 수 있습니다. 이 값은 아주 느린 장치와 링크의 경우에도 적당합니다. **mp3** 플레이어를 사용하는 경우 *requestTimeout*을 늘릴 필요가 있습니다.

nfsRetransmit

이 정수 변수는 **HP CIFS Client**가 정해진 시간 내에 응답하지 않을 경우 커널의 재시도 횟수를 정의합니다. 시간 제한은 *nfsTimeout*부터 시작하여 각 재시도마다 두 배가 됩니다. **HP CIFS Client**에서 손실되는 요청이 없기 때문에 다시 전송할 필요는 없습니다. 하지만 시스템의 **NFS** 클라이언트로 인해 **NFS** 서버의 로드가 많아지고 최대 소켓 버퍼 크기가 작은 경우 버퍼 오버

플로로 인해 요청이 손실될 수 있습니다. 5(기본값)의 값이 적당합니다. 버퍼 오버플로가 자주 발생할 수 있지만 많은 시험을 통해 최적 성능의 *nfsTimeout* 값을 얻을 수 있습니다.

nfsSockRxBuf

이 정수 변수는 커널과 통신하는 데 사용되는 소켓의 수신 버퍼 크기를 설정합니다. 지정된 값이 컴퓨터의 적용 가능한 범위를 벗어나는 경우 자동으로 **HP CIFS Client**가 범위를 제한합니다. 쓰기가 느린 경우 버퍼 크기를 늘리십시오.

nfsSockTxBuf

이 정수 변수는 커널과 통신하는 데 사용되는 소켓의 전송 버퍼 크기를 설정합니다. 명시적으로 버퍼 크기를 설정할 필요는 없습니다.

nfsTransferSize

이 정수 변수는 커널과 **HP CIFS Client** 사이에서 데이터를 전송하는 데 사용되는 최대 블록 크기를 정의합니다. 최대 허용 값은 **8k(8192)**입니다. **NFS** 소켓에서 자주 오버플로가 발생하는 경우 이 값을 줄여야 합니다. 특히 **AIX 3.x**에서 그러한 경우가 많습니다. 블록 크기로 2의 제곱만 사용하는 것이 좋습니다. 기본값은 **8192**입니다.

preferredPort

이 정수 변수는 **HP CIFS Client**가 **NFS**용으로 사용하려고 시도하는 포트 번호를 정의합니다. 이 포트를 사용할 수 없으면 **HP CIFS Client**는 사용 가능한 포트를 선택합니다. **NFS**용 상수 포트를 가지면 다시 시작된 데몬이 이전 마운트 구현을 이어받을 수 있으므로 편리합니다. 트러스트되지 않은 로컬 사용자가 있는 경우 포트 번호는 **1024** 미만이어야 합니다.

cifs	CIFS 구조에는 CIFS 구성에 대한 많은 옵션이 있습니다. 이 절에서는 특정 구성에 의해 재정의될 수 있는 기본 동작을 정의합니다. CIFS 절에는 다음 매개 변수가 포함됩니다.
dataCacheSize	이 정수 변수는 데이터 캐시당 사용되는 바이트 수를 정의합니다. 이 변수의 값은 8k의 배수여야 합니다.
databaseFile	이 변수는 사용자 데이터베이스 파일 경로를 구성합니다. 또한 사용자 암호 및 등록 키를 저장합니다. 기본값은 <code>/var/opt/cifsclient/cifsclient.udb</code> 입니다.
databaseParseInterval	HP CIFS Client는 사용자 데이터베이스 파일이 변경되면 해당 파일을 다시 구문 분석할 수 있습니다. 이 기능이 작동하려면 HP CIFS Client가 정기적으로 파일을 폴링해야 합니다. <i>databaseParseInterval</i> 변수는 폴링 주기를 밀리초 단위로 정의합니다. 이 변수를 0으로 설정하면 사용자 데이터베이스 파일이 시작할 때 한 번만 구문 분석됩니다. 기본값은 10000입니다.
domain	이 문자열 변수는 클라이언트에서 서버로 전송하는 도메인 이름을 정의합니다. 정의하지 않은 경우 기본적으로 알려진 모든 서버에 사용할 수 있는 빈 문자열이 됩니다.
initialDataCaches, initialDirCaches	이러한 두 정수 변수는 시작할 때 디렉토리 및 데이터 파일에 할당되는 캐시 수를 정의합니다. 두 변수에 대한 기본값은 모두 8입니다.
bindNbnsPort	이 변수는 HP CIFS Client가 NetBIOS 이름 서비스 요청을 보내는 포트 번호를 정의합니다. 지정된 포트 번호를 사용할 수 없으면 HP CIFS Client가 사용 가능한 임의의 다른 포트로 되돌아갑니다. 기본값은 137입니다.
bindNbdgsPort	이 변수는 HP CIFS Client가 NetBIOS 데이터그램 요청을 보내는 포트 번호를 정의합니다. 지정된 포트 번호를 사용할 수 없으면 HP CIFS Client가 사용 가능한 임의의 다른 포트로 되돌아갑니다. 기본값은 138입니다.
lookupTryNetbios	

이 부울 변수는 NetBIOS 브로드캐스트 사용 여부를 구성합니다. WINS는 NetBIOS 이름 서버의 기능입니다. WINS 조회를 사용하려면 이 변수를 *yes*로 지정하고 *nbnsWinsIp* 변수를 WINS 서버의 IP 주소와 함께 지정해야 합니다. 연결하려는 CIFS Server가 WINS 서버에 등록되어 있어야 합니다. 기본적으로 이 매개 변수는 *yes*로 설정되어 있습니다.

lookupTryDns

이 변수는 DNS(Domain Name Server) 조회 사용 여부를 구성합니다. 기본 설정은 *yes*입니다.

nbnsWinsIp

이 문자열 변수는 WINS 서버의 IP 주소를 정의합니다. 네트워크에 WINS 서버가 없으면 이 변수를 빈 문자열로 설정하십시오.

nbnsInitialTimeout, nbnsTotalTimeout

nbnsInitialTimeout 변수는 NetBIOS 이름 서비스 작업을 할 때 사용되는 초기 시간 제한을 밀리초 단위로 정의합니다. 재시도를 할 때마다 이 값이 두 배가 됩니다. *nbnsTotalTimeout* 변수는 NetBIOS 이름 서비스 작업이 성공할 때까지 대기하는 최대 시간 제한을 밀리초 단위로 정의합니다. 최대 시간을 초과하면 시간 제한 오류로 작업이 실패합니다. 기본적으로 *nbnsInitialTimeout*은 100으로 설정되어 있으며 *nbnsTotalTimeout*은 1200으로 설정되어 있습니다.

nbnsCacheTime

NetBIOS 이름 조회를 이 시간(밀리초)만큼 캐시에 유지합니다.

scopeID

이 문자열 변수는 클라이언트의 Netbios 이름 범위를 정의합니다. 정의하지 않은 경우 범위 ID를 사용하지 않습니다. 범위 ID 개념에 대해 이해하지 못하는 경우 사용할 필요는 없습니다.

rmTmpKerbCredFiles

Kerberos 인증을 사용하는 경우 CIFS Client는 임시 파일을 사용하여 로그인 처리 중에 사용자의 자격 증명을 저장합니다. 서버 하나, 사용자 하나 당 하나의 임시 자격 증명 파일이 존재합니다. CIFS Client는 Kerberos 티켓을 다시 사용하지 않으므로 사용자의 로그인 처리가 완료되면 임시 파일이 제거됩니다. 문제 해결에

구성 파일
구성 매개 변수

임시 파일이 필요하면 이 변수를 no로 설정하여 이 파일을 보존할 수 있습니다. 이 파일은 `/var/opt/cifsclient/krb5_tmp`에 있습니다. 기본값은 yes입니다.

cifs.server.”.default”

CIFS 구조에는 CIFS 연결에 대한 많은 구성 옵션이 있습니다. 이 변수는 각 서버별 구성으로 재정의할 수 있는 기본 동작을 정의합니다. 값은 다음 매개 변수를 사용하는 디렉터리입니다.

localNetbiosName

이 항목을 사용하여 서버로 전송할 클라이언트 **Netbios** 이름을 설정할 수 있습니다.

ipAddress

이 항목은 연결할 **CIFS Server**의 IP 주소를 설정하는 데 사용할 수 있습니다.

connectTimeout

이 정수 변수는 연결 설정이 완료되기를 대기하는 최대 시간(밀리초)을 정의합니다. 네트워크가 느린 경우 이 시간을 늘려야 할 수도 있습니다. 기본값은 **2000ms(2초)**입니다.

requestTimeout

이 정수 변수는 연결이 설정된 경우 서버 응답의 최대 시간(밀리초)을 정의합니다. 기본값은 **6000ms(60초)**입니다.

authenticationMethod

이 항목은 **HP CIFS Client**가 **CIFS Server**에 사용자를 인증하기 위해 사용하는 방법을 지정합니다. 허용되는 값은 **ntlm** 또는 **kerberos**입니다. 기본 설정은 **ntlm**입니다. 값을 **ntlm**으로 설정하면 서버 로그인에 **NTLM** 프로토콜만 사용됩니다. 값을 **kerberos**로 설정하고 서버가 **Kerberos**를 지원하는 경우에는 로그인에 **Kerberos**만 사용됩니다. 그렇지 않은 경우 **NTLM**이 사용됩니다. **NTLM**을 사용하는 경우 **CIFS Client**가 **ntlmEncryptionVersion** 구성에 따라 사용할 **NTLM** 버전을 결정합니다.

ntlmEncryptionVersion

이 항목은 **HP CIFS Client**가 **CIFS Server**에 사용자를 인증하기 위해 사용하는 방법을 지정합니다. 허용되는 값은 **ntlm** 또는 **ntlmv2**입니다. 값을 **ntlm**으로 설정하면 서버 로그인에 **NTLM**의 암호화된 암호만이 사용됩니다. 값을 **ntlmv2**로 설정하면 **NTLMv2**가 사용됩니다. 기본 설정은 **ntlm**입니다.

smbPacketSigning

이 문자열 변수는 **HP CIFS Client**가 패킷 서명을 수행할 때 사용할 옵션을 지정합니다. 이 매개 변수에 대한 유효한 항목은 `enabled`, `required` 및 `disabled`입니다. 기본적으로 이 매개 변수는 `enabled`로 설정되어 있습니다.

caseSensitive

서버에서 파일 이름이 대소문자를 구분하는지 여부를 지정하는 부울 변수입니다. 사용할 수 있는 값은 `yes` 또는 `no`입니다. 기본적으로 **Unix** 파일 시스템과 호환되도록 대소문자를 구분합니다. `none`(다음 매개 변수 참조)이 아닌 대소문자 매핑을 사용하려는 경우 이 매개 변수를 `no`로 설정해야 합니다.

caseMapping

이 변수(열거 형식)는 파일 이름의 매핑을 정의합니다. `upper`는 모두 대문자로 `lower`는 모두 소문자로 매핑하며 `none`은 서버 상의 파일 이름을 유지합니다.

capitalizeShares

이 부울 변수는 연결을 시도하기 전에 공유 이름을 모두 대문자로 변경할지 여부를 정의합니다. 공유 이름은 대소문자를 구분하지 않지만 **Windows 95**는 소문자 이름을 인식하지 못합니다. `serverClasses` 섹션에 이 옵션을 사용할 경우 `no`를 `yes`로 재정의할 수 있지만 `yes`를 `no`로 재정의할 수는 없습니다. 기본값은 `yes`입니다.

useUnicode

이 부울 변수는 **HP CIFS Client**에서 서버가 지원하는 경우 **Unicode**를 사용할지 여부를 지정합니다.

domain

이 문자열 변수는 클라이언트에서 서버로 전송하는 도메인 이름을 정의합니다. 정의하지 않은 경우 기본적으로 모든 알려진 서버에 문제가 없는 빈 문자열이 됩니다. (`cifs.domain`으로 이동)

alwaysEncryptData

이 부울 변수를 `yes`로 설정한 경우 서버와의 **SSL(Secure Socket Layer)** 연결만 허용됩니다. `no`로 설정한 경우 서버와 **SSL**을 협상합니다.

<code>guestRemoteUser</code>	<code>guestRemoteUser</code> 구성은 다음 문제를 해결합니다. 공유가 공개인 경우에도 항목을 액세스하기 위해 각 Unix 사용자는 서버에 로그인해야 합니다. 즉, CIFS 사용자 이름/암호 쌍으로 매핑되어야 합니다. 액세스 권한이 중요하지 않은 공개 공유를 액세스하는 Unix 사용자가 많은 경우 각 사용자를 로그인하도록 하는 것은 실용적이지 않습니다. <code>guestRemotetUser</code> 를 정의한 경우 로그인하지 않은 모든 Unix 사용자를 지정된 Unix 사용자인 것으로 취급할 수 있습니다. 물론 <code>guestRemoteUser</code> 로 지정된 Unix 사용자는 <code>cifsmount</code> 또는 <code>cifslogin</code> 의 <code>-s</code> 옵션을 사용하여 로그인해야 합니다.
<code>guestPassword</code>	이 변수는 <code>guestRemoteUser</code> 매개 변수에서 지정된 사용자 암호를 설정합니다.
<code>fileModeMask</code>	이 변수는 CIFS 가 파일에 부여하는 Unix 권한을 제한하는 데 사용할 수 있습니다. 기본 설정은 0777 입니다. 내용을 이해하지 못하는 경우에는 이 값을 변경하지 마십시오. Unix 권한은 사용자가 파일에 액세스할 수 있는지 여부와는 관계가 없습니다. <code>cp</code> 명령이 속성을 보존하므로 CIFS 공유에서 로컬 디스크로 파일이 복사된 후에는 관계가 있습니다.
<code>dirModeMask</code>	이 변수는 CIFS 가 디렉토리에 부여하는 Unix 권한을 제한하는 데 사용할 수 있습니다. 기본 설정은 0777 입니다. 내용을 이해하지 못하는 경우에는 이 값을 변경하지 마십시오.
<code>ctimeIsCreate</code>	이 변수는 Unix <code>ctime</code> (변경 시간)이 DOS Creation Time으로 부터 정해지는지 또는 파일 수정 시간으로부터 복사되는지를 지정합니다. 이 매개 변수를 <code>yes</code> 로 설정하면 작성 시간이 사용됩니다. 기본 설정은 <code>no</code> 입니다.
<code>fakeMountpointDate</code>	이 부울 변수가 <code>yes</code> 이면 마운트 지점의 수정 및 액세스 시간이 항상 현재 시간을 읽습니다. 이것은 Windows NT 처럼 <code>root</code> 디렉토리의 수정 날짜에 대해 의미 없는 값을 반환하는 서버에 유용합니다. 기본 설정은 <code>no</code> 입니다.
<code>execMapping</code>	이 열거 변수는 Windows 서버에 저장되는 파일에 유용합니다. 이것은 Unix <code>execute</code> 권한으로 매핑될 DOS 속성을 정의합니다. 사용할 수 있는 키워드는 <code>archive</code> , <code>system</code> , <code>hidden</code> , <code>on</code> 또는 <code>off</code> 입니다. 기본값은 <code>on</code> 입니다. <code>execMapping</code> 의 부작용은 구성

된 속성이 서버에서 설정된 속성인 경우 **Unix** 클라이언트에서 파일이 실행 비트가 모든 사용자(owner, group 및 other)로 설정되어 나타나는 것입니다.

경고

Unix 실행 파일을 **CIFS Server**에 저장하고 **Unix** 클라이언트에서 호출할 계획인 경우 기본 설정인 *execMapping = on*을 사용해야 합니다. 이 경우 **Unix** 클라이언트측에서 보면 **CIFS Server**에서 나열하는 모든 파일에 실행 비트가 설정됩니다. *execMapping = on*을 사용하면 **HP CIFS Server**에 있는 파일 속성에 영향을 미치지 않으므로 정상적인 **Unix** 파일처럼 작동합니다.

<code>execInvert</code>	이 부울 변수가 <i>yes</i> 인 경우 <i>execMapping</i> 설정에서 파생된 실행 비트가 반전됩니다.
<code>fakeDirLinks</code>	서버가 디렉토리의 하드 링크 수를 제공하지 않는 경우 이 숫자를 사용합니다. 지정하지 않은 경우 기본값은 2입니다. 일부 Unix find 유틸리티 구현에서는 링크 수에서 재귀 호출이 필요한지 여부를 결정합니다. 사용 중인 find 에서 이러한 최적화를 사용하는 경우 링크 수가 큰 디렉토리를 링크 수가 적은 것처럼 가장할 수 있습니다. 대신 find 의 명령줄 스위치를 사용하여 이 최적화를 끌 수 있습니다.
<code>enableFakeLinks</code>	이 부울 변수를 <i>yes</i> 로 설정한 경우 HP CIFS Client 가 Windows 서버에서 소프트 링크를 처리할 수 있습니다. 이러한 소프트 링크는 HP CIFS Client 의 클라이언트만 사용할 수 있습니다. Windows 서버에서는 해당 링크가 특수한 속성(구성을 수정하지 않은 경우 시스템 및 숨김 속성)이 설정된 일반적인 파일로 표시됩니다.
<code>linkModeMask, linkMode</code>	이 두 정수 변수는 일반 파일의 가장된 소프트 링크를 구분하는데 사용되는 파일 속성을 정의합니다. <i>linkModeMask</i> 의 기본값은 <i>read-only, hidden</i> 및 <i>system</i> 속성에 해당하는 7입니다.

*linkMode*는 이러한 속성이 가져야 하는 실제 상태를 정의하며, 기본값은 `hidden` 및 `system`은 설정하지만 `read-only`는 설정하지 않는 6입니다. 구성 값은 다음 구성 요소의 합으로 계산합니다.

표 7-1

1	<code>read-only</code>	2	<code>hidden</code>	4	시스템	32	<code>archive</code>
---	------------------------	---	---------------------	---	-----	----	----------------------

linksAreUnicode 이 부울 변수를 `yes`로 설정한 경우 HP CIFS Client는 가장된 링크를 서버에 **Unicode** 형식으로 저장합니다. 이 형식은 심볼릭 링크의 **CygWin32** 형식과 호환되지 않지만 클라이언트 경로가 손실되지 않습니다. 반대로 `no`로 설정한 경우 심볼릭 링크가 **Windows**에서 **CygWin32**와 호환되지만 서버 문자 집합으로 변환하는 과정이 수행됩니다. 이 변수에 관계 없이 HP CIFS Client는 심볼릭 링크 파일을 두 형식 모두로 읽을 수 있습니다.

attributesCacheTime

파일 속성을 이 시간(밀리초)만큼 캐시에 유지합니다.

dirCacheTime

디렉토리 내용을 이 시간(밀리초)만큼 캐시에 유지합니다.

maxCachedFiles

NFS 파일 핸들의 캐시로 유지되는 파일 객체의 최대 수입니다. 캐시에 없는 **NFS** 파일 핸들이 요청된 경우 재귀적인 조회가 필요하므로 성능이 눈에 띄게 저하됩니다. 재귀적 조회는 거의 발생하지 않는 이벤트로 로그에 기록됩니다.

dataCacheSize

열린 파일에 할당되는 데이터 캐시의 크기(바이트)입니다. 값은 최대 전송 허용 크기에서 계산된 캐시 페이지 크기의 배수가 되도록 받아들여집니다. 페이지 크기는 항상 2의 거듭제곱입니다. (`cifs.dataCacheSize`로 이동)

closeDelay

이 변수는 파일을 사용하지 않을 경우 파일을 열린 상태로 유지하는 시간을 정의합니다. 값은 다음 키를 사용하는 디서너리입니다.

exclusiveLock

베타적 *oplock*이 적용된 경우의 열린 상태 유지 시간(밀리초)입니다.

batchLock

일괄 *oplock*이 적용된 경우의 열린 상태 유지 시간(밀리초)입니다.

noLock

잠금이 적용되지 않은 경우의 열린 상태 유지 시간(밀리초)입니다.

dataCacheTimeNoLock

*oplock*이 적용되지 않은 경우 캐싱이 수행되어서는 안됩니다. 그렇지 않으면 **oplock**을 지원하지 않는 서버에서는 성능에 나쁜 영향을 미칠 수 있습니다. 이 값은 *oplock*이 적용되지 않은 경우 사용되는 캐시 유효 시간(밀리초)을 설정합니다.

readAhead

이 변수는 선행 읽기할 캐시 페이지 수를 정의합니다. 값은 다음 키를 사용하는 디렉터리입니다.

lock

*oplock*이 적용된 경우 선행 읽기할 페이지 수입니다.

noLock

*oplock*이 적용되지 않은 경우 선행 읽기할 페이지 수입니다.

useWriteBack

이 변수는 캐시 다시 쓰기 기법의 사용 여부를 정의합니다. **NFS2**와 함께 사용할 경우 다시 쓰기는 오류 복구의 측면에서 안전하지 않지만 성능이 상당히 향상됩니다. 값은 다음 키를 사용하는 디렉터리입니다.

lock

*oplock*이 적용된 경우 다시 쓰기를 사용할지 여부를 구성하는 부울 값입니다.

noLock

*oplock*이 적용되지 않은 경우 다시 쓰기를 사용할지 여부를 구성하는 부울 값입니다.

안정성이 중요한 경우 이 옵션을 사용하지 마십시오. 이 구성 변수는 서버로도 전달됩니다. 바로 쓰기(write through) 모드에서 매우 느려지는 서버/운영 체제 조합이 있습니다(대표적으로 Samba/Linux). 이러한 경우 다시 쓰기를 구성할 수 있습니다.

- requestOplock** 이 부울 변수는 서버에서 **oplock**을 요청할지 여부를 정의합니다. **Windows 95** 컴퓨터의 경우 **oplock**을 지원하지 않음에도 적용이 가능하기 때문에 이 변수를 **no**로 설정해야 합니다.
- closeForSetattr** 이 부울 변수는 속성(쓰기 방지, 수정 날짜)을 변경하기 전에 파일을 닫아야 하는지 여부를 정의합니다. **Windows 95** 서버의 경우 열린 파일의 속성을 설정할 수 없기 때문에 이 변수가 매우 유용합니다. 하지만 이 기능을 사용하면 **Unix** 의미론 매핑이 완벽하게 작동하지 않습니다. 기본 설정은 **no**입니다.
- disableSmbs** 모든 서버가 모든 **SMB** 명령을 동일하게 지원하는 것은 아닙니다. 실제로 특정 유형의 서버에서는 많은 명령을 사용할 수 없습니다. 이 변수 값을 사용해서는 안되는 **SMB** 명령을 열거하는 배열입니다. 해당 명령은 자동으로 대체됩니다. 사용할 수 있는 열거 상수는 다음과 같습니다.

getattrFind

파일 속성을 읽는 **trans2/findfirst2** 명령의 사용을 억제합니다. 하지만 **trans2/findfirst2**가 속성을 조회하는 가장 좋은 방법이므로 필요한 경우에만 사용하지 않도록 설정하십시오.

getattrTrans2QueryPath

파일 속성을 읽는 **trans2/query_pathinfo** 명령의 사용을 억제합니다. **Trans2/query_pathinfo**는 **Windows 95**에서 문제가 있는 것으로 보입니다.

attrUnix

파일 속성의 **Unix** 확장을 사용하지 않도록 설정합니다.

setattrTrans2SetFile

파일 속성 설정에 사용되는 *trans2/setfileinfo* 명령을 억제합니다. 이 SMB 명령은 Windows에서 올바르게 작동하지 않습니다.

setattrTrans2SetPath

파일 속성 설정에 사용되는 *trans2/setpathinfo* 명령을 억제합니다. 이 SMB 명령은 Windows에서 올바르게 작동하지 않습니다.

setattrSetFile2

속성 설정을 위한 *SET_INFORMATION2*의 사용을 억제합니다.

setattrCoreWithTime

수정 날짜 설정을 위한 코어 *SET_INFORMATION* 명령의 사용을 억제합니다.

createOpenX

파일 작성을 위한 *SMB_COM_OPEN_ANDX*의 사용을 억제합니다.

openOpenX

파일 열기를 위한 *SMB_COM_OPEN_ANDX*의 사용을 억제합니다.

readReadX

파일 읽기를 위한 *SMB_COM_READ_ANDX*의 사용을 억제합니다.

readOpenRead

파일 읽기를 위한 *SMB_COM_READ_ANDX*로 배치 처리된 *SMB_COM_OPEN_ANDX*의 사용을 억제합니다.

writeWriteX

파일 쓰기를 위한 *SMB_COM_WRITE_ANDX*의 사용을 억제합니다.

writeOpenWrite

파일 쓰기를 위한 *SMB_COM_WRITE_ANDX*로 배치 처리된 *SMB_COM_OPEN_ANDX*의 사용을 억제합니다.

findUnix

디렉토리 읽기에 대한 CIFS Unix 확장을 사용하지 않도록 설정합니다.

findTrans2

디렉토리 읽기를 위한 *trans2/find*를 사용하지 않도록 설정합니다.

fsinfoTrans2

파일 시스템 정보를 읽는 *trans2/query_fs_info*의 사용을 억제합니다.

sessionSetup

코어 명령에서만 사용되는 세션 설정 명령을 억제합니다.

treeconAndX

TREE_CONNECT_ANDX 명령을 억제합니다
*TREE_CONNECT*를 대신 사용합니다.

setDirDates

디렉토리에서 파일을 만들거나 삭제할 때 디렉토리 수정 날짜가 설정되는 것을 억제합니다. 서버에서 디렉토리가 수정되면 자동으로 날짜를 설정하는 경우 유용합니다.

fileModeMask 이 정수 변수는 파일 권한을 정의합니다. **FileModeMask**의 기본값은 **0777**입니다. 작업 내용을 이해하지 못하는 경우에는 변경하지 마십시오. **Unix** 권한은 사용자가 파일에 액세스할 수 있는지와 여부와는 관계가 없습니다. **cp** 작업이 파일 속성을 보존하므로 **CIFS** 공유에서 로컬 디스크로 파일이 복사된 후에는 관계가 있습니다.

dirModeMask 이 정수 변수는 디렉토리 권한을 정의합니다. **dirModeMask**의 기본값은 **0777**입니다. 작업 내용을 이해하지 못하는 경우에는 변경하지 마십시오. **Unix** 권한은 사용자가 파일에 액세스할 수 있

구성 파일
구성 매개 변수

는지 여부와는 관계가 없습니다. 그러나 cp 작업이 파일 속성을 보존하므로 **CIFS** 공유에서 로컬 디스크로 파일이 복사된 후에는 관계가 있습니다.

cifs.servers	이 변수는 특정 서버의 <i>cifs.server.default</i> 로 구성된 값을 수정할 수 있습니다. 이것은 키가 서버의 Netbios 이름인 딕셔너리로 구성됩니다. 각 서버 키의 값 또한 딕셔너리입니다. 이 딕셔너리는 <i>defaultServer</i> 딕셔너리와 구조가 동일합니다. 또한 다음 키를 사용할 수 있습니다.
ipAddress	이 항목은 서버의 IP 주소나 DNS 이름을 포함할 수 있습니다. 기본적으로 DNS 조회에 Netbios 이름이 사용됩니다. 또한 <i>cifsmount</i> 명령줄에서 이 매개 변수를 재정의할 수 있습니다.
netbiosName	이 항목은 서버로 전송되는 Netbios 이름을 변경할 수 있는 마지막 기회입니다.
tcpPort	서버 연결에 사용되는 TCP 포트를 변경할 수 있습니다. 기본값은 Netbios 세션 서비스 포트인 139 입니다.

cifs.serverClasses

세션 설정에서 파생된 정보에 기반하여 연결이 설정된 후에 *cifs.server.default* 및 *servers*로 구성된 값을 이 변수로 수정할 수 있습니다. 결정은 서버 운영 체제와 LAN 관리자 유형에 따라 달라집니다. 이 변수의 형식은 디렉터리 배열입니다. 각 디렉터리에는 다음과 같은 세 개의 키가 모두 있어야 합니다.

- OS** 이 항목은 셸 형식 구문의 일치 패턴을 포함합니다. *은 모든 문자, ?는 한 문자, [*<characters>*]는 지정된 모든 문자, [^*<characters>*]는 지정된 문자를 제외한 모든 문자를 의미합니다. 이 항목은 세션 설정에서 파생된 운영 체제 이름과 비교됩니다.
- LanManager** 이 항목도 셸 형식 구문의 일치 패턴으로 구성되며 세션 설정에서 파생된 LAN 관리자 이름과 비교됩니다. *info* 로그 수준을 사용하는 경우 운영 체제 이름과 LAN 관리자 이름이 *syslog*에 기록됩니다.
- config** 위의 두 패턴이 일치하는 경우 *defaultServer*가 포함하는 모든 정의를 포함할 수 있는 이 변수의 내용(디렉터리)이 서버 구성으로 사용됩니다. 옵션이 지정된 경우 이전 구성의 해당 옵션을 재정의합니다. 하지만 *disableSmb*s 옵션은 예외입니다. 사용하지 않도록 설정된 모든 SMB는 사용하지 않도록 설정된 SMB 최종 목록을 제공할 수 있도록 목록에 추가됩니다.

배열의 첫 번째 항목에서 마지막 항목까지 검색합니다. 항목이 일치하는 경우 해당 구성이 사용되고 검색이 중단됩니다.

8 PAM NTLM

이 장에서는 PAM NTLM을 설명합니다.

소개

PAM NTLM(NT Lan Manager)은 HP-UX 사용자가 시스템 로그인 중에 Windows 서버에 인증할 수 있게 하는 플러그인 인증 모듈(Pluggable Authentication Module)입니다.

PAM은 UNIX 시스템에 로그인하는 사용자를 인증하는 데 사용되는 UNIX의 인증 프레임워크입니다. PAM은 실제 인증을 수행하는 동적으로 로드할 수 있는 모듈(공유 라이브러리)을 로드합니다. 또한 다중 공유 라이브러리 모듈을 사용하도록 PAM을 구성할 수 있습니다.

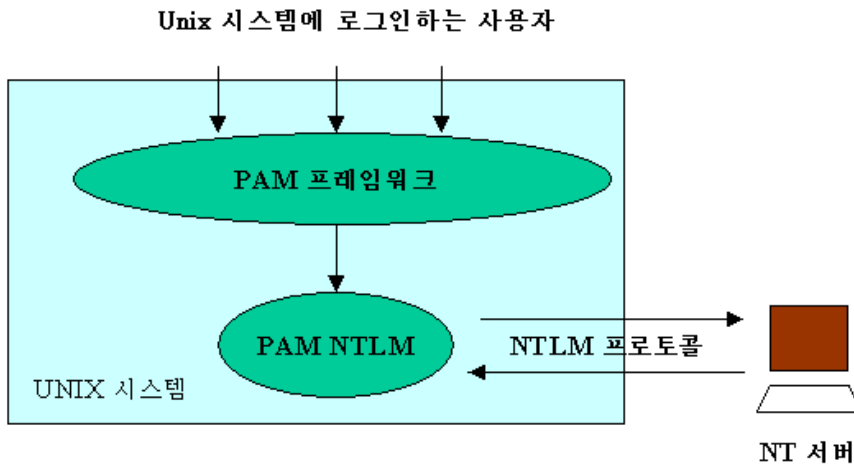
PAM NTLM은 CIFS Server를 사용하여 HP-UX 시스템에 로그인하는 사용자를 인증합니다. 즉, PAM NTLM은 NT LanManager 프로토콜을 사용하여 UNIX 사용자를 인증합니다. 따라서 UNIX 사용자 이름과 암호를 확인을 위해 CIFS Server로 전송하고 결과가 PAM 프레임워크로 반환됩니다. HP CIFS Client는 PAM NTLM 인증 정보를 사용하여 CIFS Server에 있는 공유를 액세스합니다. 따라서 HP-UX 시스템으로 로그인한 사용자가 *cifslogin* 명령을 사용할 필요 없이 CIFS로 마운트된 파일 시스템을 액세스할 수 있습니다.

주

PAM NTLM은 NTLMv2 암호의 암호화를 지원하지 않습니다.

PAM NTLM을 구성하려면 PAM 프레임워크의 일반적인 사항을 이해해야 합니다. PAM에 대한 자세한 내용은 *pam(3)*, *pam.conf(4)* 및 <http://docs.hp.com/hpux/os>의 시스템 및 작업 그룹 관리(localized documentatoin을 클릭하여 한글을 선택하면 한글 설명서를 찾을 수 있음)를 참조하십시오.

그림 8-1 PAM 소개



PAM NTLM은 동적으로 로드되는 모듈입니다. PAM 프레임워크는 NTLM 프로토콜을 사용하여 Windows 서버에 대해 인정하는 PAM NTLM 모듈에 사용자 이름과 암호를 전달합니다.

PAM NTLM

이 절에서는 PAM NTLM의 기능과 사용자 맵 파일에 대해 설명합니다.

PAM NTLM 기능

- PAM NTLM은 인증 및 암호 관리를 지원합니다.
- PAM NTLM은 Samba *smb.conf* 파일의 하위 집합을 구성 파일로 사용합니다. 자세한 내용은 아래의 PAM NTLM 설치 후 절차를 참조하십시오.
- PAM NTLM은 로컬 Unix 사용자 이름을 인증에 사용할 수 있도록 원격 CIFS 도메인 사용자 이름으로 매핑하는 **사용자 이름 매핑**을 지원합니다. 자세한 내용은 PAM NTLM 구성 절을 참조하십시오.
- 사용자/암호 인증에 성공하면 CIFS Client에서 사용할 수 있도록 캐시에 저장됩니다.
- CIFS Server에 대한 로그인 인증은 NTLM의 암호화된 암호를 사용합니다.
- HP-UX *passwd(1)* 명령을 사용하여 PDC(기본 도메인 컨트롤러)의 CIFS 사용자 암호를 업데이트합니다.

설치 단계에 대해서는 2장을 참조하십시오.

사용자 맵 파일

PAM NTLM은 CIFS Server 인증에 앞서 Unix 사용자 이름을 CIFS 도메인 사용자 이름으로 매핑하는 **사용자 맵 파일**을 지원합니다. PAM NTLM은 이 사용자 맵 파일에서 Unix 사용자 이름을 찾습니다. 찾은 경우 CIFS Server에서 사용자를 인증하는 데 매핑된 CIFS 도메인 사용자 이름을 사용합니다. 사용자가 인증되기 위해서는 매핑된 NT 사용자의 올바른 암호를 입력해야 합니다.

PAM NTLM을 사용하도록 *password(1M)*를 구성한 경우 매핑된 CIFS 도메인 사용자의 암호가 CIFS 도메인에서 변경됩니다.

PAM NTLM 구성

다음을 구성하여 PAM-NTLM을 설정합니다.

- PAM-NTLM 모듈
- PAM-NTLM 모듈을 사용하는 */etc/pam.conf* 시스템 파일
- 사용자 맵 파일(선택 사항)

PAM-NTLM 모듈 구성

PAM-NTLM 구성 파일은 */etc/opt/cifsclient/pam/smb.conf*입니다. 또한 기본 구성 파일(*smb.conf.default*)이 제공됩니다. 나중에 참조해야 할 수 있으므로 기본 구성 파일을 변경해서는 안됩니다.

표 8-1

```
##
## Name: smb.conf
##
## Set the values below to the actual names used in your environment ##
## Any line which starts with a semi-colon(;) or a hash(#)
## is a comment and is ignored.
##
##===== Global Settings =====
[global]

## workgroup: Domain-Name or Workgroup-Name
workgroup = workgroup

## password server: the netbios name of the system which will be ## used to
authenticate logins.
password server = pdc_name bdc1_name bdc2_name

## wins server: the system used to locate password servers, ## specified as a
fully-qualified DNS name or an IP address.
wins server = winserv.mycorp.com
```

PAM-NTLM 모듈을 사용하도록 시스템 구성

이 작업은 전역 HP-UX PAM 구성 파일 `/etc/pam.conf`를 편집하는 과정입니다.

중요

PAM을 올바르게 구성하지 않은 경우 시스템에 로그인할 수 없습니다. `pam.conf`를 수정하려면 PAM 프레임워크를 이해해야 합니다. PAM에 대한 자세한 내용은 HP-UX 매뉴얼에서 `pam.conf(4)`, `pam_unix(5)` 부분을 참조하십시오.

보안 상의 이유로 인증 및 암호 변경을 위해 PAM NTLM에 의해 구성된 암호 서버 대신 호스트 시스템(PAM-UNIX)이 root 및 기타 권한이 있는 사용자를 인증하도록 직접 구성하는 것이 좋습니다. 사용자별 액세스는 `pam.conf`에 `libpam_updb`를 사용하고 `pam_user.conf`의 `libpam_ntlm`에 `ignore` 옵션을 사용하여 제어할 수 있습니다. 사용 설명 및 예는 `pam.conf(4)`, `pam_user.conf(4)` 및 `pam_updb(5)`를 참조하십시오.

또한 PAM-UNIX의 대체 대상이 아닌 추가 대상으로 PAM-NTLM을 사용하는 것이 좋습니다. 이 구성에 대해 아래의 `pam.conf` 예제 파일에서 설명합니다.

PAM-NTLM은 다음 서비스를 제공합니다.

- 암호 인증
- 암호 변경
- 만료 통지 시 암호 변경

각 서비스는 `pam.conf`의 특정 섹션에 해당됩니다. 사용하려는 서비스 항목을 추가하십시오.

- 암호 인증의 경우 `pam.conf`의 "Authentication management" 섹션을 수정합니다.
- 암호 변경의 경우 Password management를 수정합니다.
- 만료 통지 시 암호 변경의 경우 Authentication management, Password management 및 Account management를 수정합니다(만료 통지 시 암호 변경을 이용하려면 암호 인증과 암호 변경도 사용하도록 설정해야 함).

다음은 세 개의 PAM NTLM 서비스 모듈을 구성하는 *pam.conf* 파일 예제입니다. 각 PAM NTLM 항목은 공유 라이브러리 *libpam_ntlm.1*을 참조하는 줄로 구성됩니다. authentication management 섹션에서 PAM UNIX와 함께 PAM NTLM을 사용하는 경우 다음에서 볼 수 있는 것처럼 PAM UNIX 항목과 함께 *try_first_pass* 옵션을 지정하는 것이 좋습니다.

경고

*pam.conf*에 잘못된 경로가 사용될 경우 시스템에 로그인하지 못할 수도 있습니다. 시스템에 설치된 HP-UX 버전과 일치하는 *pam.conf* 파일을 참조하는지 확인하십시오. **uname -r**을 사용하여 버전을 확인합니다. 특히 *pam.conf*에 줄을 추가할 때 경로를 수정하지 말고 아래와 똑같이 추가해야 합니다. **HP-UX B.11.22** 버전부터 PAM 라이브러리의 경로는 이전 버전과 다릅니다.

다음 *pam.conf* 예제 파일은 HP-UX B.110.23 버전용입니다.

예제 8-1

HP-UX 버전 B.110.23용 예제 파일

```
=====
#
# PAM configuration
#
# Authentication management
# Note: For PA applications, /usr/lib/security/libpam_unix.so.1 is a
# symbolic link that points to the corresponding PA PAM module.
#
#
login    auth sufficient  /usr/lib/security/$ISA/libpam_ntlm.so.1
login    auth required    /usr/lib/security/$ISA/libpam_unix.so.1
try_first_pass
su       auth required    /usr/lib/security/$ISA/libpam_unix.so.1
dtlogin  auth required    /usr/lib/security/$ISA/libpam_unix.so.1
dtaction auth required    /usr/lib/security/$ISA/libpam_unix.so.1
ftp      auth required    /usr/lib/security/$ISA/libpam_unix.so.1
OTHER    auth required    /usr/lib/security/$ISA/libpam_unix.so.1
#
# Account management
#
login    auth sufficient  /usr/lib/security/$ISA/libpam_ntlm.so.1
login    account required /usr/lib/security/$ISA/libpam_unix.so.1
su       account required /usr/lib/security/$ISA/libpam_unix.so.1
dtlogin  account required /usr/lib/security/$ISA/libpam_unix.so.1
dtaction account required /usr/lib/security/$ISA/libpam_unix.so.1
ftp      account required /usr/lib/security/$ISA/libpam_unix.so.1
#
OTHER    account required /usr/lib/security/$ISA/libpam_unix.so.1
#
# Session management
```

```

#
login    session required      /usr/lib/security/$ISA/libpam_unix.so.1
dtlogin  session required      /usr/lib/security/$ISA/libpam_unix.so.1
dtaction session required      /usr/lib/security/$ISA/libpam_unix.so.1
OTHER    session required      /usr/lib/security/$ISA/libpam_unix.so.1
#
# Password management
#
login    auth sufficient       /usr/lib/security/$ISA/libpam_ntlm.so.1
login    password required     /usr/lib/security/$ISA/libpam_unix.so.1
passwd   password required     /usr/lib/security/$ISA/libpam_unix.so.1
dtlogin  password required     /usr/lib/security/$ISA/libpam_unix.so.1
dtaction password required     /usr/lib/security/$ISA/libpam_unix.so.1
OTHER    password required     /usr/lib/security/$ISA/libpam_unix.so.1
=====

```

다음 *pam.conf* 예제 파일은 HP-UX B.11.00 및 B.11.11 버전용입니다.

예제 8-2

HP-UX 버전 B.11.00 및 B.11.11용 예제 파일

```

#
# PAM configuration
#
# Authentication management
#
login    auth sufficient       /usr/lib/security/libpam_ntlm.1
login    auth required         /usr/lib/security/libpam_unix.1
try_first_pass
su       auth required         /usr/lib/security/libpam_unix.1
dtlogin  auth required         /usr/lib/security/libpam_unix.1
dtaction auth required         /usr/lib/security/libpam_unix.1
ftp      auth required         /usr/lib/security/libpam_unix.1
OTHER    auth required         /usr/lib/security/libpam_unix.1
#
# Account management
#
login    account required     /usr/lib/security/libpam_ntlm.1
login    account required     /usr/lib/security/libpam_unix.1
su       account required     /usr/lib/security/libpam_unix.1
dtlogin  account required     /usr/lib/security/libpam_unix.1
dtaction account required     /usr/lib/security/libpam_unix.1
ftp      account required     /usr/lib/security/libpam_unix.1
OTHER    account required     /usr/lib/security/libpam_unix.1
#
# Session management
#
login    session required     /usr/lib/security/libpam_unix.1
dtlogin  session required     /usr/lib/security/libpam_unix.1
dtaction session required     /usr/lib/security/libpam_unix.1
OTHER    session required     /usr/lib/security/libpam_unix.1
#
# Password management

```

```
#
login      password sufficient /usr/lib/security/libpam_ntlm.1
login      password required /usr/lib/security/libpam_unix.1
passwd     password required /usr/lib/security/libpam_ntlm.1
dtlogin    password required /usr/lib/security/libpam_unix.1
dtaction   password required /usr/lib/security/libpam_unix.1
OTHER      password required /usr/lib/security/libpam_unix.1
```

사용자 맵 파일 구성

사용자 맵 파일을 사용하도록 PAM NTLM을 구성하려면 */etc/opt/cifsclient/pam/smb.conf* 파일의 [Global] 섹션에 다음 줄을 추가합니다.

```
Domain user map = /etc/opt/cifsclient/pam/domain_user.map
```

사용자 맵 파일의 이름과 위치를 구성할 수 있습니다. 이름과 위치에 대해 위와 같은 형식을 사용하는 것이 좋습니다.

도메인 사용자 파일 항목 형식은 다음과 같습니다.

```
UNIXusername = [\\DOMAIN_NAME\\] DomainUserName
```

UNIXusername은 HP-UX 시스템의 기존 계정이며 DomainUserName은 CIFS 도메인에서 매핑된 사용자 이름입니다. DOMAIN_NAME은 선택 사항입니다.

사용자 맵 파일은 줄 단위로 구문 분석됩니다. # 또는 a;로 시작하는 줄은 모두 무시됩니다. 각 줄은 왼쪽에 단일 Unix 사용자 이름이 있고 탭이나 ' '으로 구분된 오른쪽에 단일 CIFS 도메인 사용자 이름이 있어야 합니다. 이름이 공백을 포함하는 경우 따옴표로 묶어야 합니다.

사용자 맵 파일의 NIS 배포 사용

*/etc/passwd*를 NIS 클라이언트로 배포하는 것과 비슷한 방식으로 사용자 맵 파일을 NIS를 통해 배포할 수 있습니다.

기능을 사용하려면 다음 단계를 수행하십시오.

1. 마스터 사용자 맵 파일을 NIS 마스터 서버에서 *domainusermap.byname*으로 이름이 지정된 NIS 맵 파일로 변환합니다.

주

NIS 맵 파일 이름 *domainusermap.byname*은 PAM NTLM이 NIS 맵 파일에 대해 사용하는 기본 이름입니다. 각 NIS 클라이언트의 PAM NTLM 구성 파일 (*/etc/opt/cifsclient/pam/smb.conf*)에서 다른 NIS 사용자 맵 이름을 구성할 수 있습니다. 구성 옵션은 다음과 같습니다.

```
nis ntuser mapname = <new usr map filename>
```

-
2. 배포된 맵 파일을 받을 각 NIS 클라이언트의 사용자 맵 파일에서 줄의 첫 열에 더하기(+) 기호로 항목을 추가합니다. 더하기 기호는 해당 지점에서 파일 구문 분석을 중지한 다음 사용자 맵 파일의 나머지 검색은 NIS 서버에 대한 NIS 호출을 사용해야 한다는 것을 나타냅니다.

ㄱ

개요

구성, 25

설치, 25

구성

개요, 25

파일, 99

defaultServer, 107, 110, 113

logLevels, 101

국제화된 클라이언트, 20, 28

ㄴ

사용자 맵 파일, 128, 133

서버 메시지 블록, 15, 17

설치

개요, 25

전제 조건, 26

소프트웨어 로드, 27

ㅇ

유틸리티, 요약, 69

일반 인터넷 파일 시스템. CIFS 참고

ㅋ

클라이언트 사용, 31

ㅍ

파일 및 디렉토리, 39

C

CIFS

설명, 15

프로토콜, 15

cifsclient, 31, 71

cifsclient.cfg, 28

cifslis, 70, 82

cifslogin, 70, 77

cifslogout, 70, 81

cifsmount, 70, 74, 87

cifsumount, 70, 80

D

daemon

강제 종료, 93

장애가 발생한 경우, 93

H

HP 제품의 향상된 기능, 17

HP CIFS

소개, 15

시작, 30

중지, 30

파일 및 디렉토리, 39

HP CIFS 시작, 30

HP CIFS 중지, 30

HP CIFS Client

국제화, 20, 28

기능, 18

문제 해결, 93

UNIX Extensions, 18

HP CIFS Client 문제 해결, 93

M

mount 명령, 31

mount_cifs, 87

N

netbios, 87

NIS 및 사용자 맵 파일, 133

P

PAM NTLM

구성, 129

구성 파일, 129

기능, 52, 128

설명, 16, 126

안전한 저장소 통합, 18, 19

password(1M), 128

S

SMB. 서버 메시지 블록 참고

SSL 옵션, 98

swinstall(1M), 27

U

unmount 명령, 31

unmount_cifs, 87

