CIFS/9000 Client 설치 및 관리

버전 A.01.08

제조 제품 번호: B8724-90035

IA1122

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.

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 라이센스가 적용됩니다. 자세한 내용은 CIFS/9000 Server 설명서의 5장에서 GPL 라이센스를 참조하십시오.

상표권. UNIX는 The Open Group의 등록 상표입니다.

목차

1. CIFS/9000 Client 소개

2. CIFS/9000 Client 설치 및 구성

3. 명령줄 유틸리티

4. CIFS/9000 Client 문제 해결

5. 구성 파일

6. PAM NTLM

머리말

본 설명서의 정보는 CIFS/9000 Client를 설치하고 관리하는 네트워크 관리자 또는 네트워크 보안 관리자를 대상으로 합니다.

본 설명서에서는 HP CIFS/9000 Client 소프트웨어 제품을 HP 9000 시스템에 설치하고, 구성하고, 문제를 해결하는 방법을 설명합니다.

이 설명서는 다음과 같이 구성되어 있습니다.

1장	“CIFS/9000 Client 소개”에서는 CIFS/9000 Client 제품 기록, 기능, 요구 사항 및 제한에 대해 설명합니다.
2장	“CIFS/9000 Client 설치 및 구성”에서는 CIFS/9000 클라이언트 소프트웨어 설치, 구성 및 확인 방법에 대해 설명합니다.
3장	“명령줄 유틸리티”에서는 모든 CIFS/9000 Client 유틸리티에 대한 Unix man 페이지를 설명합니다.
4장	“CIFS/9000 Client 문제 해결”에서는 CIFS/9000 Client 문제를 해결하는 데 도움이 되는 자세한 절차를 설명합니다.
5장	“CIFS/9000 구성 파일”에서는 CIFS/9000 소프트웨어를 사용자 정의하는 경우 필요한 모든 구성 변수에 대해 설명합니다.
6장	“CIFS 인증(PAM 모듈)”에서는 NTLM PAM 인증 서비스에 대해 자세히 설명합니다.

1 CIFS/9000 Client 소개

이 장에서는 CIFS/9000 Client에 대해 설명합니다.

이 장의 구성은 다음과 같습니다.

- CIFS/9000 소개
- CIFS/9000 Client 설명
- CIFS/9000 Client 기능

CIFS/9000 소개

CIFS/9000은 HP-UX에 Microsoft 공통 인터넷 파일 시스템(CIFS) 프로토콜에 기반한 분산 파일 시스템을 제공합니다. CIFS/9000은 HP-UX에 CIFS 프로토콜의 서버 및 클라이언트 구성 요소를 모두 구현합니다.

CIFS/9000 Server는 검증된 오픈 소스 소프트웨어인 Samba 2.0.6 버전에 기반하며 Windows 95, 98, NT, 2000 및 HP-UX 컴퓨터를 포함한 CIFS/9000 Client 소프트웨어를 실행 중인 CIFS 클라이언트에 파일 및 인쇄 서비스를 제공합니다.

CIFS/9000 Client를 사용하면 HP-UX 사용자가 CIFS/9000 Server를 실행 중인 Windows 서버 및 HP-UX 컴퓨터를 포함한 CIFS 파일 서버를 UNIX 파일 시스템 공유로 마운트할 수 있습니다. 또한 CIFS/9000 Client는 Windows NTLM 인증 프로토콜을 구현하는 선택적인 Pluggable Authentication Module(PAM)을 제공합니다. HP-UX PAM 설비 내에서 설치하고 구성할 경우, PAM NTLM은 HP-UX 사용자가 Windows 인증 서버에 대해 인증되도록 합니다.

CIFS 프로토콜의 개념

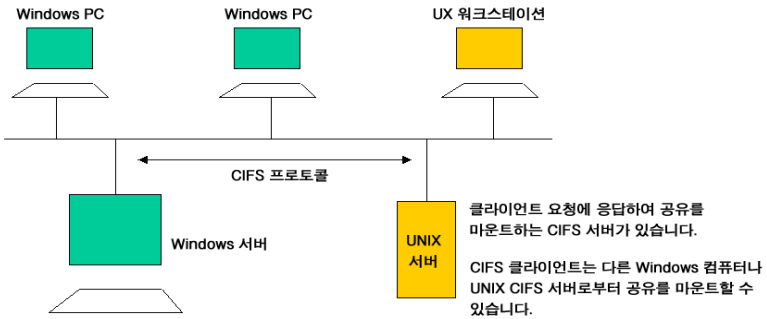
CIFS는 1980년대 후반에 막 태동하던 LAN 기술(예: 이더넷)을 통해 PC 간에 파일을 공유하기 위해 개발된 서버 메시지 블록(SMB) 프로토콜이라고도 하는 네트워킹 프로토콜에서 시작되었습니다. SMB는 Microsoft Windows 95, Windows NT 및 OS/2 운영 체제의 기본 파일 공유 프로토콜이며 수백만의 PC 사용자가 회사 인트라넷을 통해 파일을 공유하는 데 사용하는 표준 방식입니다.

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

이름은 파일 시스템이지만 CIFS는 실제로 자체 파일 시스템은 아닙니다. 엄밀하게 말하자면 CIFS는 원격 파일 액세스 프로토콜이며 원격 시스템의 파일에 대한 액세스를 제공합니다. CIFS는 호스트 시스템의 파일 시스템 상단에 위치하여 호스트 시스템의 파일 시스템과 동작합니다. CIFS는 서버와 클라이언트 모두를 정의합니다. CIFS 클라이언트는 CIFS 서버의 파일에 액세스하는 데 사용됩니다.

CIFS/9000은 HP-UX 컴퓨터에서 CIFS 프로토콜을 사용하여 HP-UX 서버의 디렉토리가 Windows 컴퓨터에 마운트되도록 하며 반대의 경우도 가능하도록 합니다.

CIFS 패러다임



CIFS 서버가 설치되어 있으면, UNIX 컴퓨터가 네트워크 상의 Windows 서버의 역할만 하도록 할 수 있습니다. 네트워크 상의 Unix 워크스테이션은 UNIX 서버로부터 CIFS 공유를 사용할 수 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 인증 유형을 제공하는 PAM API로 호출됩니다.

NTLM(NT LAN Manager)은 CIFS 서버가 CIFS 클라이언트를 인증하는 프로토콜이며, PAM NTLM은 NTLM 프로토콜을 구현한 PAM 모듈입니다. 이 모듈을 사용하면 사용자가 cifslogin 명령을 사용할 필요 없이 HP-UX 시스템으로 로그인하여 CIFS로 마운트된 파일 시스템을 액세스할 수 있습니다.

CIFS/9000 Client 설명

CIFS/9000 Client는 HP-UX 사용자가 CIFS 서버의 공유를 UNIX 파일 시스템으로 마운트할 수 있도록 HP-UX에서 CIFS 프로토콜을 구현합니다.

CIFS/9000 Client 기능

다음은 CIFS/9000 Client의 주요 기능입니다.

- CIFS UNIX Extensions
- NTLM PAM 통합
- 클라이언트측 캐싱
- 국제화된 클라이언트 지원

CIFS UNIX Extensions

CIFS UNIX Extensions을 사용하면 CIFS 클라이언트와 Samba 서버로 표준 UNIX 파일 시스템 기능을 구현할 수 있습니다. 여기에는 다음과 같은 기능이 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 확장을 지원하는 CIFS 서버에서만 작동합니다. 현재로는 HP Samba가 CIFS 확장을 지원하는 유일한 CIFS 서버입니다.

NTLM PAM 통합

NTLM(NT LAN Manager)은 CIFS 서버가 CIFS 클라이언트를 인증하는 프로토콜입니다. HP의 NTLM PAM(Pluggable Authentication Module) 및 CIFS/9000 Client와 함께 사용하면 HP-UX 시스템에 로그인한 사용자는 자동으로 CIFS로 마운트된 파일 시스템을 액세스할 수 있습니다. 단, PAM NTLM 및 CIFS 서버가 동일한 데이터베이스를 사용해야 합니다.

클라이언트측 캐싱

CIFS/9000 클라이언트는 CIFS 사양에 따라 클라이언트측 데이터 캐시와 선행 읽기(read ahead)를 제공하는 기회 잠금(Opportunistic Locks)을 지원합니다. 따라서 네트워크 성능이 몇 배 향상될 수 있습니다.

국제화된 클라이언트 지원

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

2 CIFS/9000 Client 설치 및 구성

이 장에서는 시스템에 HP CIFS/9000 Client 소프트웨어를 설치하는 절차를 설명합니다.

이 장의 구성은 다음과 같습니다.

- CIFS/9000 Client 요구 사항 및 제한 사항
- HP CIFS/9000 Client 설치 및 구성 개요
- 1단계: HP CIFS/9000 Client 설치 전제 조건 확인
- 2단계: HP CIFS/9000 Client 및 PAM 소프트웨어 설치
- 3단계: CIFS/9000 Client 구성
- 4단계: CIFS/9000 Client 데몬 시작 및 중지

CIFS/9000 Client 요구 사항 및 제한 사항

시스템 요구 사항

CIFS/9000 Client는 HP-UX 버전 11.0 이상을 32비트나 64비트 모드로 실행할 수 있는 모든 HP 워크스테이션과 서버에서 실행됩니다. CIFS/9000 Client에 필요한 특정 시스템 패치는 없습니다.

HP CIFS/9000 Client 설치 및 구성 개요

HP CIFS/9000 클라이언트 설치는 설치 전제 조건 확인, *swinstall(1M)* 유틸리티를 사용한 HP CIFS/9000 Client 파일 세트 로드 및 CIFS/9000 구성 절차 완료로 구성됩니다.

CIFS Client 소프트웨어 및 PAM NTLM 소프트웨어에는 HP Software Distributor(SD)를 사용하여 설치 패키지로 만든 두 개의 개별 제품으로 제공됩니다. 두 제품을 동시에 설치하는 것이 좋습니다. 하지만 각 제품을 독립형 제품으로 설치하고 실행할 수도 있습니다. 소프트웨어를 설치하고 제거하려면 swinstall(1M) 및 swremove(1M) HP-UX 명령을 사용하십시오. 이들 명령에 대한 자세한 내용은 HP-UX man 페이지를 참고하십시오.

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

CIFS/9000 Client 소프트웨어 묶음을 설치할 경우 CIFS/9000 클라이언트 소프트웨어와 NTLM PAM 모듈(선택 사항)의 두 제품을 설치할 수 있습니다.

주

www.software.hp.com에서 CIFS/9000 Client 소프트웨어를 다운로드할 수 있습니다.

1단계: HP CIFS/9000 Client 설치 전제 조건 확인

CIFS/9000 Client 소프트웨어를 시스템으로 로드하기 전에 다음 하드웨어 및 소프트웨어 전제 조건을 충족하는지 확인하십시오.

1. PAM 라이브러리 패치가 있는지 확인합니다.

   운영 체제에 대한 정보를 보려면 다음 명령을 실행합니다.

   ```
   uname -a
   ```

   패치에 대한 정보를 보려면 다음 명령을 실행합니다.

   ```
   swlist -i
   ```

   패치 종속성에 대한 정보는 CIFS/9000 Client 릴리즈 노트를 참고하십시오.

2. 설치를 수행하려면 “root”여야 합니다.

CIFS/9000 Client 사용

이 절에서는 CIFS/9000 Client 사용 방법의 "빠른 시작" 개요를 설명합니다. 기본 절차는 (1) 데몬 시작, (2) 공유 디렉토리 마운트, (3) CIFS 서버에 로그인입니다. 다음은 이들 단계에 대한 설명과 유용한 추가 정보입니다.

1. 데몬을 시작합니다.

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

   ```
   $ cifsclient start
   Starting CIFS Client daemon 'cifsclientd' ... done;
     process id = 1911
   ```

   상태 확인이 필요한 경우 다음을 입력합니다.

   ```
   $ cifsclient status

   path:     /opt/cifsclient/sbin/cifsclientd
   version:  FILESET HP CIFS CLIENT: Version: A.01.02
   cksum:    2843185805
   Status:   CIFS Client daemon is up; process id 1911,
             started Apr 13.
   ```

   또한 부팅 시에 자동으로 CIFS Client를 시작하도록 시스템을 구성할 수 있습니다. 그렇게 하려면 */etc/rc.config.d/cifsclient* 파일을 *RUN_CIFSCLIENT=1*로 설정하여 편집합니다. 등호 양 옆에 공백이 있어서는 안됩니다.

2. CIFS 서버에서 공유를 마운트하고 마운트 해제합니다.

   이러한 작업은 *root*로 수행해야 합니다. CIFS/9000 Client에 의해 마운트된 디렉토리를 먼저 CIFS/9000 Server에서 "공유"로 구성해야 합니다.

   이 예제에서는 CIFS/9000 Server에서 "share"로 구성된 공유 **원본**은 마운트 지점으로 */home/devl/source* 디렉토리를 사용하여 CIFS Client에 의해 마운트됩니다. 마운트 지점으로 사용되는 디렉토리가 이미 존재해야 합니다.

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

   마운트를 해제하려면 다음 명령을 사용합니다.

   ```
   $ umount /home/devl/source
   ```

10. 확인 창에서 **예** 단추를 활성화하여 소프트웨어 설치를 계속합니다. *swinstall*에서 설치 창을 표시합니다.

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

    *swinstall*에서 파일 세트를 로드하고 파일 세트에 대한 제어 스크립트를 실행하여 커널을 빌드합니다. 예상 처리 시간: 3분 ~ 5분

11. 참고 창에서 **확인** 단추를 활성화하여 시스템을 다시 부팅합니다.

    사용자 인터페이스가 사라지고 시스템이 다시 부팅됩니다.

12. 시스템이 다시 부팅된 후에 */var/adm/sw/swinstall.log* 및 */var/adm/sw/swagent.log*에서 설치가 성공했는지 로그 파일을 확인합니다.

3단계: CIFS/9000 Client 구성

CIFS/9000 Client 구성 파일인 */etc/opt/cifsclient/cifsclient.cfg*를 기본값을 수정하지 않고 제공된 상태 그대로 사용할 수 있습니다.

cifsclient.cfg 편집

필요한 경우 다음 설명에 따라 CIFS/9000 클라이언트 구성 파일 */etc/opt/cifsclient/cifsclient.cfg*를 편집합니다.

1. 클라이언트가 속할 NT 도메인 이름을 갖는 도메인 변수를 업데이트합니다. 이 단계를 권장하지만 필수 사항은 아닙니다.

   domain = hpnet_dom

2. 국제화된 클라이언트를 구성합니다.

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

   각 테이블은 클라이언트 또는 서버에서 파일 및 디렉토리 이름 인코딩을 위해 구성할 수 있는 "CharMap" 파일입니다(파일 내용은 변경되지 않음). CIFS 클라이언트 콘솔에 표시되는 문자 세트는 제품과 함께 제공된 많은 문자표 파일 중 원하는 것을 선택하는 매개 변수 *clientCharMapFile*을 통해 구성합니다. CIFS 서버와의 통신을 위한 문자 변환은 Unicode로, 또는 문자표 파일을 선택하는 데 사용되는 구성 매개 변수 *serverCharMapFile*을 통해 수행할 수 있습니다. Unicode의 사용은 *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, *Shift-JIS* 로케일을 사용하여 CIFS Client를 일본어 시스템으로 구성한 다음 *Shift-JIS*를 사용하는 일본어 CIFS Server에 연결하려는 경우 다음과 같이 구성할 수 있습니다.

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

3. 이 파일의 다른 구성은 수정하지 않는 것이 좋습니다.

Windows 파일 시스템의 제한 때문에 운영 환경의 두 구성 설정 *execMapping* 및 *caseSensitive*를 주의하여 다루어야 합니다. 이것에 대해서는 5장에서 자세히 설명합니다. 또한, CIFS/9000 Server 설명서의 “기타 Samba 문제”에 대해 다룬 절에서 대소문자 구분에 대한 설명을 참고하십시오.

주

현재 이 버전의 Samba는 Unicode를 지원하지 않습니다. Windows NT 및 Windows 2000은 기본적으로 Unicode를 사용합니다.

4단계: CIFS/9000 Client 데몬 시작 및 중지

CIFS/9000 클라이언트를 시작하고 중지하려면 *cifsclient* 명령을 사용합니다.

구문은 다음과 같습니다.

/opt/cifsclient/bin/cifsclient <start | stop>

인수가 없는 경우 기본적으로 데몬을 시작합니다. CIFS/9000 클라이언트가 실행 중인 상태에서 명령을 실행한 경우 이미 실행 중이라는 메시지가 나타납니다.

CIFS/9000 클라이언트를 중지하려면 *cifsclient* 명령의 *stop* 옵션을 사용합니다.

이 경우, 스크립트에서 데몬을 중지하기 전에 모든 공유를 마운트 해제합니다. 마운트 해제에 문제가 있는 경우 스크립트에서 CIFS/9000 Client를 중지하지 않습니다.

CIFS/9000 Client 사용

이 절에서는 CIFS/9000 Client 사용 방법의 "빠른 시작" 개요를 설명합니다. 기본 절차는 (1) 데몬 시작, (2) 공유 디렉토리 마운트, (3) CIFS 서버에 로그인입니다. 다음은 이들 단계에 대한 설명과 유용한 추가 정보입니다.

1. 데몬을 시작합니다.

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

   ```
   $ cifsclient start
   Starting CIFS Client daemon 'cifsclientd' ... done;
     process id = 1911
   ```

   상태 확인이 필요한 경우 다음을 입력합니다.

   ```
   $ cifsclient status

   path:     /opt/cifsclient/sbin/cifsclientd
   version:  FILESET HP CIFS CLIENT: Version: A.01.02
   cksum:    2843185805
   Status:   CIFS Client daemon is up; process id 1911,
             started Apr 13.
   ```

   또한 부팅 시에 자동으로 CIFS Client를 시작하도록 시스템을 구성할 수 있습니다. 그렇게 하려면 */etc/rc.config.d/cifsclient* 파일을 *RUN_CIFSCLIENT=1*로 설정하여 편집합니다. 등호 양 옆에 공백이 있어서는 안됩니다.

2. CIFS 서버에서 공유를 마운트하고 마운트 해제합니다.

   이러한 작업은 *root*로 수행해야 합니다. CIFS/9000 Client에 의해 마운트된 디렉토리를 먼저 CIFS/9000 Server에서 "공유"로 구성해야 합니다.

   이 예제에서는 CIFS/9000 Server에서 "share"로 구성된 공유 *원본*은 마운트 지점으로 */home/devl/source* 디렉토리를 사용하여 CIFS Client에 의해 마운트됩니다. 마운트 지점으로 사용되는 디렉토리가 이미 존재해야 합니다.

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

   마운트를 해제하려면 다음 명령을 사용합니다.

   ```
   $ umount /home/devl/source
   ```

3. 클라이언트에서 마운트 지점을 통해 공유 디렉토리를 액세스합니다.

   CIFS/9000 Client를 사용하면 개별 사용자 기반으로만 마운트된 디렉토리를 액세스할 수 있습니다. 따라서 각 사용자가 먼저 CIFS/9000 Server에 의해 인증되어야 합니다. 이 인증은 *cifslogin* 명령을 통해 수행됩니다.

   이 예제에서는 시스템 관리자가 *source* 공유를 마운트했습니다. 클라이언트에 있는 *root* 사용자가 *buildsys*에 있는 공유 디렉토리를 액세스하려는 경우 먼저 서버에 로그인하지 않은 상태로 디렉토리를 마운트 지점으로 변경하려 합니다(실패함). 그런 다음 *cifslogin* 명령을 사용하여 *buildsys*에 로그인함으로써 사용자가 *buildsys*에 의해 인증되고 공유된 *source* 디렉토리를 CIFS Client의 마운트 지점을 통해 액세스할 수 있습니다. CIFS Server에 로그인하는 데 사용되는 사용자 이름은 Client의 현재 로그인 이름과 다를 수 있습니다. *cifslogin*에 사용되는 계정 및 암호 쌍은 인증을 수행하는 시스템에 존재해야 합니다. 또한 CIFS Server가 HP-UX 시스템인 경우 Server를 액세스하는 Client의 모든 사용자는 파일 소유권의 일관성이 유지되도록 양쪽 시스템에서 *uid*가 같아야 합니다.

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

   사용자가 CIFS Server *buildsys*에 로그인하지 않았기 때문에 실패합니다.

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

   이 명령은 성공합니다. 다음 명령을 사용하여 결과를 확인합니다.

```
$ cifslist -A

============================================================
Server buildsys:
============================================================
Remote Username: root          Local Username: root

Share: \\BUILDSYS\source
       rw /home/dev1/source

$ cd /home/dev1/source
$ _
```

같은 방법으로 *root*가 아닌 일반 사용자가 CIFS 마운트를 액세스할 수 있습니다. *source*를 마운트하고 *buildsys*에서 root가 인증된 위의 예를 사용할 경우 사용자 이름이 *lucy*인 사용자는 다음과 같은 방법으로 마운트를 액세스합니다.

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

결과를 확인합니다.

```
$ cifslist -A

============================================================
server buildsys:
============================================================
Remote Username: root                Local Username: root
Remote Username: lucy                 Local Username: lucy

Share: \\BUILDSYS\source
        rw /home/devl/source
```

CIFS 파일 시스템 마운트 추가 정보

명시적으로 단일 마운트를 만드는 이전 절에서 설명한 mount 명령 외에 CIFS 파일 시스템의 마운트를 관리하는 다른 방법이 있습니다. 이 절에서 설명하지 않는 mount_cifs 및 umount_cifs의 자세한 구문 정보는 4장을 참고하십시오.

/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. 항목의 형식은 다음과 같습니다.

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

그런 후에 다음을 입력하여 */etc/fstab*의 모든 CIFS 항목을 마운트합니다.

```
$ mount -aF cifs
```

현재 마운트된 모든 CIFS 파일 시스템을 마운트 해제하려면 다음을 입력합니다.

```
$ umount -aF cifs
```

위에서 설명한 것처럼 부팅 시에 CIFS Client를 시작하도록 시스템을 구성한 경우 이들 명령이 부팅 및 종료 시에 각각 자동으로 수행됩니다.

주

HP ONC+ Autofs 서비스를 사용한 CIFS 파일 시스템의 자동 마운트는 현재 지원하지 않습니다. Autofs를 통해 CIFS 파일 시스템을 마운트할 경우 시스템 프로세스 테이블을 유지하는 프로세스가 멈출 수 있으며 마운트 지점 디렉토리를 액세스할 수 없게 될 수 있습니다.

마운트 및 로그인을 한 단계로 처리하는 방법

root 사용자에게는 명시적으로 *cifslogin* 명령을 실행할 필요 없이 한 단계로 CIFS 파일 시스템을 마운트하고 CIFS Server에 로그인하는 옵션이 있습니다. 위의 예에서 사용한 이름을 사용합니다.

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

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

마운트 및 마운트 해제 명령 참고 정보

cifsmount 및 *cifsumount* 명령은 *mount* 및 *umount* 명령과 동일한 기능을 제공하지만 되도록 사용하지 마십시오. 이들 명령은 구문이 다르며 CIFS/9000 Client의 이후 릴리즈에서는 지원하지 않을 수도 있습니다. 개발 순서에 따라 이들 명령에 대한 *man* 페이지는 3장에 제공됩니다.

CIFS/9000 Client 파일 및 디렉토리

이 절에서는 CIFS/9000 Client를 구성하는 주요 파일을 설명합니다.

표 2-1 **CIFS/9000 Client 파일 및 디렉토리**

파일/디렉토리	설명
/opt/cifsclient/	모든 CIFS Client 코어 파일 및 관리 파일에 대한 기본 디렉토리입니다.
/opt/cifsclient/bin/	CIFS 이진 파일입니다.
cifsmount	CIFS Server의 CIFS 공유를 마운트하는 명령입니다. root 사용자만 사용할 수 있습니다.
cifsumount	CIFS 공유를 마운트 해제하는 명령입니다. root 사용자만 사용할 수 있습니다.
cifslogin	일반 사용자가 이미 마운트된 CIFS 공유를 사용하려면 먼저 CIFS 구성에 따라 자신의 사용자 이름과 암호를 사용하여 CIFS 도메인/컴퓨터에 로그인해야 합니다.
cifslogout	CIFS 도메인에서 사용자가 로그아웃하는 명령입니다. CIFS 도메인에서 마운트된 공유를 사용할 수 없게 됩니다.
cifslist	Client에서 마운트된 공유를 나열합니다.
cifsclient	CIFS Client의 시작/중지 스크립트입니다. 이 스크립트에 대한 자세한 내용은 “4단계: CIFS Client 시작 및 중지”를 참고하십시오.
/opt/cifsclient/pam	CIFS/9000 PAM 파일입니다.

표 2-1 CIFS/9000 Client 파일 및 디렉토리 (계속)

파일/디렉토리	설명
/opt/cifsclient/sbin	관리자나 root 사용자가 사용하는 CIFS Client입니다. 예를 들어, CIFS Client 데몬이 이 디렉토리에 있습니다.
/etc/opt/cifsclient	CIFS Client 구성 및 지역화 파일을 위한 디렉토리입니다.
cifsclient.cfg	CIFS Client 데몬이 액세스하는 구성 파일입니다.
cifsclient.cfg.default	기본 구성 파일입니다. *cifsclient.cfg*로 복사하여 사용해야 합니다. 이 파일 자체는 수정하지 마십시오.
/etc/opt/cifsclient/unitables	국제화된 클라이언트를 위한 문자표입니다.
pam/smb.conf	PAM 구성 파일입니다. 필요에 따라 수정해야 합니다. 이 파일에 대한 자세한 내용은 “6장: PAM NTLM”을 참고하십시오.
pam/smb.conf.default	기본 PAM 파일입니다. 사용하려면 *pam/smb.conf*로 복사해서 사용해야 합니다. 이 파일 자체는 수정하지 마십시오.
/var/opt/cifsclient	CIFS Client 로그 파일, pid 파일 및 클라이언트 자체에서 사용하기 위해 만든 모든 임시 파일을 위한 디렉토리입니다.

3 명령줄 유틸리티

이 장에서는 CIFS Client의 명령줄 유틸리티에 대해 자세히 설명합니다.

CIFS/9000 Client 소프트웨어 패키지의 구성은 다음과 같습니다.

cifsclient	CIFS 클라이언트를 시작하고 중지하는 데 사용되는 명령입니다.
cifsmount	원격 서버의 디렉토리를 마운트하는 명령입니다.
cifslogin	원격 서버에 대한 사용자 인증을 수행하는 명령입니다. 인증된 후에는 다른 사용자가 마운트한 모든 공유를 사용할 수 있습니다.
cifsumount	*cifsmount*와 반대 동작을 하는 명령입니다. 로컬 마운트 지점을 제거하고 다른 지점에 마운트되어 있지 않은 경우 서버로부터 연결을 끊습니다.
cifslogout	*cifslogin*과 반대 동작을 하는 명령입니다. 로그아웃한 후에는 지정된 서버의 모든 공유를 사용할 수 없습니다.
cifslist	연결된 서버, 마운트 지점, 마운트된 공유 등을 나열합니다.
mount	CFIS 파일 시스템을 마운트합니다.
umount	CIFS 파일 시스템을 마운트 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.

주

CIFS Client 명령줄 유틸리티의 인수 순서는 중요하며 전통적인 Unix 명령과 반대입니다. 다음 예를 참고하십시오.

cifslogin server -U user

인수 쌍 *-U user*는 server 인수 다음에 와야 합니다.

cifsclient

구문

```
cifsclient start | stop | restart | status | ver [-v] [-x]

cifsclient force_umount moutpoint [ . . . ]
```

설명

*cifsclient*는 CIFS/9000 클라이언트의 전역 작업을 제어하는 데 사용되는 범용 셸 스크립트입니다. 첫 번째 형태로는 CIFS 클라이언트 데몬인 *cifsclientd*를 관리합니다. 두 번째 형태는 심각한 네트워크 오류 상태를 복구하는 데에만 사용됩니다. 옵션이 없는 "cifsclient"는 "cifsclient start"와 동일합니다.

부팅 시에 CIFS Client를 시작하도록 시스템을 구성하는 방법에 대해서는 이 설명서의 2장에서 "CIFS/9000 Client 사용"을 참고하십시오.

옵션

start	CIFS 클라이언트를 시작합니다. 즉, 시작하는 즉시 데몬이 시작되어 백그라운드로 이동합니다. 부팅 시에 CIFS 클라이언트를 시작하도록 시스템을 구성하는 방법에 대해서는 2장의 "CIFS/9000 Client 사용"을 참고하십시오.
stop	모든 CIFS 파일 시스템을 마운트 해제하고 클라이언트를 중지합니다. CIFS 클라이언트 호스트에 있는 모든 세션의 현재 작업 디렉토리가 마운트된 CIFS 파일 시스템에 있는 경우 "장치 사용" 오류와 함께 마운트 해제가 실패하고 클라이언트가 종료되지 않습니다. 오류 상태(아래의 force_umount 참고)를 제외하면 직접 CIFS 클라이언트 데몬을 강제 종료하기 보다는 stop 옵션을 사용하여 정상적으로 종료하는 것이 좋습니다.
restart	"cifsclient stop; sleep 1; cifsclient start"와 동일합니다.
status	데몬 상태에 대한 일반적인 정보를 표시합니다. 출력 예제에 대해서는 2장의 "CIFS/9000 Client 사용"을 참고하십시오.

`ver` 호스트 시스템의 Installed Product Database에 저장된 CIFS/9000 클라이언트 제품 버전을 표시합니다. `ver` 인수에는 다음 옵션이 있습니다.

`-v` Verbose; 제품 버전과 함께 모든 CIFS 클라이언트 이진 파일, 스크립트 및 구성 파일에 대한 `what(1)` 문자열을 표시합니다.

`-x` 추가 버전 정보, `-x` 옵션은 `-v` 옵션으로 표시되는 정보 외에 각 이진 파일 구성 요소 소스 파일의 CVS 버전을 표시합니다. 이 옵션은 CVS가 지원되는 경우에만 유용합니다.

`force_umount` 이것은 심각한 오류가 발생한 경우에만 사용하는 옵션으로 호스트 시스템에서 CIFS 클라이언트에 의해 마운트 해제할 수 없는 CIFS 파일 시스템을 강제로 마운트 해제하게 됩니다. 이러한 오류는 특정 유형의 네트워크 오류로 인해 발생할 수 있습니다. CIFS 클라이언트 데몬이 실행 중인 경우 `force_umount`를 사용하기 전에 *cifsclientd* 프로세스를 강제 종료해야 합니다.

파일

/etc/opt/cifsclient/cifsclient.cfg

이 파일은 CIFS/9000 Client에 대한 런타임 구성 옵션을 포함합니다. 자세한 내용은 5장, “구성 파일”을 참고하십시오.

관련 항목

cifsmount, cifslogin, cifsumount, cifslogout, cifslist

cifsmount

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

구문

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

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.

주

HP는 SSL 옵션을 지원하지 않습니다.

옵션

-c <clientname>

클라이언트의 NetBIOS 이름을 설정합니다. CIFS는 Netbios에 기반합니다. Netbios에는 클라이언트 및 서버 연결 설정 중에 유효한 Netbios 컴퓨터 이름이 제공되어야 합니다. 클라이언트 이름은 대개 컴퓨터의 호스트 이름을 가져옵니다. 이 기능이 작동하지 않거나 컴퓨터의 Netbios 이름이 다른 경우에는 이 매개 변수와 함께 사용할 값을 제공해야 합니다. 서버가 연결된 상태이면 이 매개 변수는 무시됩니다.

`-I <IP number>`

서버의 IP 주소입니다. 기본적으로 서버의 호스트 이름은 공유의 서버 사양에서 가져옵니다. 서버에서 올바른 Netbios 이름을 요구하는 경우 이 이름이 서버의 Netbios 호스트 이름이기도 해야 합니다. CIFS/9000 Client는 Netbios 대신 DNS를 사용하여 서버 이름을 IP 주소로 변환합니다. 서버의 DNS 이름이 Netbios 이름과 다른 경우 이 매개 변수로 DNS 이름이나 서버의 IP 주소를 제공할 수 있습니다. 서버가 연결된 상태이면 이 매개 변수는 무시됩니다.

`-p <portnumber>`

연결 포트를 설정합니다. Netbios 연결은 대개 139 포트에서 이루어지지만 다른 포트에 연결하려는 경우 이 매개 변수와 함께 십진수 포트 번호를 제공할 수 있습니다. 서버가 연결된 상태이면 이 매개 변수는 무시됩니다.

`-r` 읽기 전용 파일 시스템으로 마운트합니다.

`-U <username>`

서버에 전송할 사용자 이름입니다. 기본적으로 CIFS/9000 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.

`-P <password>`

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

`-N` 암호를 프롬프트하지 않습니다. 사용자에게 암호가 없는 경우 암호를 프롬프트하지 않도록 하는 데 이 옵션을 사용할 수 있습니다.

`-u` 일반 텍스트 암호를 사용할 수 있도록 설정합니다. 보안 상의 위험이 있기 때문에, 기본적으로 CIFS/9000 Client는 암호를 일반 텍스트로 서버에 전송하지 않습니다. 네트워크에서 일반 텍스트 암호를 해킹(스니핑)하는 도구가 있습니다. 암호를 일반 텍스트로 전송해야 하는 경우(서버가 암호의 암호화를 지원하지 않는 경우) 이 옵션을 기능을 사용하도록 설정하십시오. 사용자가 서버에 로그인된 상태이면 이 옵션은 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.

`-s` 마운트 및 암호를 데이터베이스에 저장합니다. 보안 관련 사항을 이해하는 경우에만 사용하십시오. CIFS/9000 Client는 마운트, 사용자 이름 및 암호를 데이터베이스로 유지 관리할 수 있습니다. 이 데이터베이스는 시작 시에 저장된 마운트를 다시 연결하고 사용자가 클라이언트에 로그인하지 않은 경우에도 데몬에 사용자를 로그인하는 데 사용됩니다. 이 옵션은 자동 마운트와 사용자에게 암호를 요구하는 기능이 없는 cron 유틸리티로 프로그램을 실행하는 경우에 유용합니다. 암호는 CIFS/9000 Client의 사용자 데이터베이스 파일에 저장됩니다. 이 파일을 통해서 암호의 CIFS/9000 해시 값(암호 자체에 해당)을 해독할 수 있는 가능성이 있기 때문에 이 파일 자체로 보안이 충족되는 것은 아닙니다. 따라서, 컴퓨터를 실제로 혼자 사용하거나 루트로 액세스하는 경우 또는 파일을 액세스하는 모든 사용자를 신뢰할 수 있는 경우에만 이 옵션을 사용하는 것이 안전합니다. CIFS/9000 Client는 암호화되지 않은 암호를 사용자 데이터베이스에 저장하지 않습니다. 서버가 암호화된 암호를 지원하지 않는 경우 이 옵션을 사용할 수 없습니다.

예

다음은 로컬 마운트 지점 */mounts/bigserver*에서 bigserver 서버의 entiredisk 공유를 마운트하고 마운트 및 사용자 이름/암호 조합을 사용자 데이터베이스에 저장하는 명령입니다.

`cifsmount` *//bigserver/entiredisk /mounts/bigserver -s*

파일

마운트, 사용자 이름 및 암호가 CIFS/9000 Client의 사용자 데이터베이스 파일에 암호화되어 저장됩니다. 사용자 데이터베이스 파일에 대한 경로는 CIFS/9000 Client 구성 파일에서 구성할 수 있습니다. 기본 경로는 다음과 같습니다.

/var/opt/cifsclient/cifsclient.udb

관련 항목

cifslogin, cifsumount, cifslogout, cifslist

cifslogin

구문

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

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 *cifslogin*은 서버에 사용자의 로그인 이름을 보냅니다. 이 기능을 사용하지 않는 경우 명령줄에 사용자 이름을 지정할 수 있습니다.

옵션

`-c <clientname>`

클라이언트의 Netbios 이름을 설정합니다. CIFS/9000은 Netbios에 기반합니다. Netbios에는 클라이언트 및 서버 연결 설정 중에 유효한 Netbios 컴퓨터 이름이 제공되어야 합니다. 클라이언트 이름은 대개 컴퓨터의 호스트 이름을 가져옵니다. 이 기능이 작동하지 않거나 컴퓨터의 Netbios 이름이 다른 경우에는 이 매개 변수와 함께 사용할 값을 제공해야 합니다. 서버가 연결된 상태이면 이 매개 변수는 무시됩니다.

`-I <IP number>`

서버의 IP 주소입니다. 기본적으로 서버의 호스트 이름은 공유의 서버 사양에서 가져옵니다. 서버에서 올바른 Netbios 이름을 요구하는 경우 이 이름이 서버의 Netbios 호스트 이름이기도 해야 합니다. CIFS/9000 Client는 Netbios 대신 DNS를 사용하여 서버 이름을 IP 주소로 변환합니다. 서버의 DNS 이름이 Netbios 이름과 다른 경우 이 매개 변수로 DNS 이름이나 서버의 IP 주소를 제공할 수 있습니다. 서버가 연결된 상태이면 이 매개 변수는 무시됩니다.

`-p <portnumber>`

연결 포트를 설정합니다. Netbios 연결은 대개 139 포트에서 이루어지지만 다른 포트에 연결하려는 경우 이 매개 변수와 함께 십진수 포트 번호를 제공할 수 있습니다. 서버가 연결된 상태이면 이 매개 변수는 무시됩니다.

`-P <password>`

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

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

`-N` 암호를 프롬프트하지 않습니다. 서버에 사용자가 로그인한 경우 또는 사용자에게 암호가 없는 경우 암호를 프롬프트하지 않도록 이 옵션을 사용할 수 있습니다.

`-u` 일반 텍스트 암호를 사용할 수 있도록 설정합니다. 보안 상의 위험이 있기 때문에, 기본적으로 CIFS/9000 Client는 암호를 일반 텍스트로 서버에 전송하지 않습니다. 네트워크에서 일반 텍스트 암호를 해킹(스니핑)하는 도구가 있습니다. 암호를 일반 텍스트로 전송해야 하는 경우(서버가 암호의 암호화를 지원하지 않는 경우) 이 옵션을 기능을 사용하도록 설정하십시오. 사용자가 서버에 로그인된 상태이면 이 옵션은 무시됩니다.

`-f` 강제로 로그인합니다. 이 옵션을 사용하면 서버가 응답하지 않는 경우에도 로그인이 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 CIFS/9000 Client는 마운트, 사용자 이름 및 암호를 데이터베이스로 유지 관리할 수 있습니다. 이 데이터베이스는 시작 시에 저장된 마운트를 다시 연결하고 사용자가 클라이언트에 로그인하지 않은 경우에도 데몬에 사용자를 로그인하는 데 사용됩니다. 이 옵션은 자동 마운트와 사용자에게 암호를 요구하는 기능이 없는 cron 유틸리티로 프로그램을 실행하는 경우에 유용합니다. 암호는 CIFS/9000 Client의 사용자 데이터베이스 파일에 저장됩니다. 이 파일을 통해서 암호의 CIFS 해시 값(암호 자체에 해당)을 해독할 수 있는 가능성이 있기 때문에 이 파일 자체로 보안이 충족되는 것은 아닙니다. 따라서, 컴퓨터를 실제로 혼자 사용하거나 루트로 액세스하는 경우 또는 파일을 액세스하는 모든 사용자를 신뢰할 수 있는 경우에만 이 옵션을 사용하는 것이 안전합니다. CIFS/9000 Client는 암호화되지 않은 암호를 사용자 데이터베이스에 저장하지 않습니다. 서버가 암호화된 암호를 지원하지 않는 경우 이 옵션을 사용할 수 없습니다.

예

로컬 사용자 steve가 *bigserver* 서버의 공유를 마운트했다고 가정합니다. 로컬 사용자 bill은 서버에 로그인하지 않았기 때문에 마운트된 파일을 액세스할 수 없습니다. *bigserver*에서 실제 이름인 miller로 계정이 있는 bill은 다음 작업을 수행하여 액세스 권한을 얻을 수 있습니다.

```
cifslogin bigserver miller
```

bill에게 암호가 프롬프트되고 입력한 암호가 올바른 경우 *bigserver*의 사용자 miller와 동일한 권한으로 공유에 대한 액세스 권한이 부여됩니다.

파일

사용자 이름 및 암호가 CIFS/9000 Client의 사용자 데이터베이스 파일에 암호화되어 저장됩니다. 사용자 데이터베이스 파일에 대한 경로는 CIFS/9000 Client 구성 파일에서 구성할 수 있습니다. 기본 경로는 다음과 같습니다.

/var/opt/cifsclient/cifsclient.udb

관련 항목

cifsmount, cifsumount, cifslogout, cifslist

cifsumount

umount 명령을 사용하여 *cifsumount* 명령을 실행할 수 있습니다. 두 명령은 다음과 같습니다.

구문

`cifsumount <mountpoint> [<options>]`

`cifsumount -a [<options>]`

설명

cifsumount 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.

옵션

`-d`	데이터베이스에서 마운트를 삭제합니다. <*mountpoint*>와 연결된 마운트가 사용자 데이터베이스에 저장되어 있는 경우 해당 데이터베이스에서 마운트를 삭제합니다.
`-l`	마운트 삭제와 동시에 서버에 마운트된 공유가 없는 경우 서버에서 모든 사용자를 로그아웃합니다(기본 동작).
`-k`	마운트된 공유가 없는 경우에도 서버에 사용자를 로그인한 상태로 유지합니다.
`-f`	강제로 마운트 해제합니다. 서버에 요청을 보내지 않습니다(서버 중단 시 유용).

파일

마운트, 사용자 이름 및 암호가 CIFS/9000 Client의 사용자 데이터베이스 파일에 암호화되어 저장됩니다. 사용자 데이터베이스 파일에 대한 경로는 CIFS/9000 Client 구성 파일에서 구성할 수 있습니다. 기본 경로는 다음과 같습니다.

/var/opt/cifsclient/cifsclient.udb

관련 항목

cifsmount, cifslogin, cifslogout, cifslist

cifslogout

구문

```
cifslogout <servername> [<options>]
```

설명

cifslogout 명령은 명령을 사용한 사용자를 지정된 서버에서 로그아웃하는 데 사용됩니다. *cifslogout*을 실행한 후에는 사용자 데이터베이스에 사용자가 저장되어 있지 않는 한 해당 사용자가 해당 서버의 모든 파일을 액세스할 수 없게 됩니다.

옵션

`-d` 데이터베이스에서 암호를 삭제합니다. 사용자의 암호가 사용자 데이터베이스에 저장되어 있는 경우 데이터베이스에서 암호를 삭제합니다.

파일

마운트, 사용자 이름 및 암호가 CIFS/9000 Client의 사용자 데이터베이스 파일에 암호화되어 저장됩니다. 사용자 데이터베이스 파일에 대한 경로는 CIFS/9000 Client 구성 파일에서 구성할 수 있습니다. 기본 경로는 다음과 같습니다.

/var/opt/cifsclient/cifsclient.udb

관련 항목

cifsmount, cifslogin, cifsumount, cifslist

cifslist

구문

`cifslist -A` 공유 및 마운트 지점과 함께 서버를 나열합니다.

`cifslist -U` 데이터베이스의 사용자를 나열합니다.

`cifslist -M` 데이터베이스의 마운트를 나열합니다.

`cifslist -S` 연결된 서버를 나열합니다.

`cifslist -s <server>` 서버에서 열린 공유를 나열합니다.

`cifslist -u <server>` 서버에 로그인한 사용자를 나열합니다.

`cifslist -m <share>` 공유의 마운트 지점을 나열합니다.

설명

cifslist 명령은 CIFS/9000 Client의 내부 테이블을 표시하는 데 사용됩니다.

mount_cifs, umount_cifs

CIFS 파일 시스템을 마운트하고 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 *mount*를 사용하여 마운트된 파일 시스템을 나열할 수 있습니다. CIFS별 마운트 및 사용자 연결을 표시하려면 *cifslist -A*를 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 루트 이름이 됩니다.

*mount*를 인수 없이 호출하는 경우 파일 시스템 마운트 테이블 */etc/mnttab*의 마운트된 모든 파일 시스템이 나열됩니다.

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

옵션

`-F cifs` 파일 시스템별 ID입니다. 이것은 *umount moint_point* 형태의 명령을 제외한 CIFS 파일 시스템을 마운트하고 마운트 해제하는 데 항상 필요합니다.

`-a` *mount*와 함께 사용할 경우 */etc/fstab*에 항목이 있는 모든 CIFS 파일 시스템을 마운트합니다. *umount*와 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 keywrd[,keywrd...],keywrd=value[,keywrd=value...]

즉, 일부 키워드는 키워드/값 쌍으로 지정하고 -o 옵션이 아닌 일부 키워드는 쉼표로 구분해야 합니다. 중간에 공백이 있어서는 안됩니다. 예를 들면 다음과 같습니다.

-o ro,username=fulton,password=pokey

다음은 CIFS Client가 지원하는 *mount*에 대한 *-o* 옵션입니다. 값이 필요한 키워드는 "keyword=*value*"로 표시합니다.

nbname=*nbname* 클라이언트의 Netbios 이름을 설정합니다. CIFS/9000은 Netbios에 기반합니다. Netbios에는 클라이언트 및 서버 연결 설정 중에 유효한 Netbios 컴퓨터 이름이 제공되어야 합니다. 클라이언트 이름은 대개 컴퓨터의 호스트 이름을 가져옵니다. 이 기능이 작동하지 않거나 컴퓨터의 Netbios 이름이 다른 경우에는 이 매개 변수와 함께 사용할 값을 제공해야 합니다. 서버가 연결된 상태이면 이 매개 변수는 무시됩니다.

ipaddr=*addr* 서버의 IP 주소입니다. 기본적으로 서버의 호스트 이름은 공유의 서버 사양에서 가져옵니다. 서버에서 올바른 Netbios 이름을 요구하는 경우 이 이름이 서버의 Netbios 호스트 이름이기도 해야 합니다. CIFS/9000 Client는 Netbios 대신 DNS를 사용하여 서버 이름을 IP 주소로 변환합니다. 서버의 DNS 이름이 Netbios 이름과 다른 경우 이 매개 변수로 DNS 이름이나 서버의 IP 주소를 제공할 수 있습니다. 서버가 연결된 상태이면 이 매개 변수는 무시됩니다.

port=*port* 연결 포트를 설정합니다. Netbios 연결은 대개 139 포트에서 이루어지지만 다른 포트에 연결하려는 경우 이 매개 변수와 함께 십진수 포트 번호를 제공할 수 있습니다. 서버가 연결된 상태이면 이 매개 변수는 무시됩니다.

`ro` 읽기 전용 파일 시스템으로 마운트합니다.

username=*name* 서버에 전송할 사용자 이름입니다. 기본적으로 CIFS/9000 Client는 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=*passwd* 명령줄에 지정한 암호입니다. *ps* 명령의 출력에 모든 명령줄 매개변수가 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 CIFS/9000 Client는 암호를 일반 텍스트로 서버에 전송하지 않습니다. 네트워크에서 일반 텍스트 암호를 해킹(스니핑)하는 도구가 있습니다. 암호를 일반 텍스트로 전송해야 하는 경우(서버가 암호의 암호화를 지원하지 않는 경우) 이 옵션을 기능을 사용하도록 설정하십시오. 사용자가 서버에 로그인된 상태이면 이 옵션은 무시됩니다.

forcemnt 이 옵션을 사용하면 서버가 응답하지 않는 경우에도 마운트가 수행됩니다. 서버에 요청을 보내지 않습니다. 따라서 유효성을 확인할 수 있는 매개 변수가 없습니다.

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*

4 CIFS/9000 Client 문제 해결

이 장에서는 CIFS/9000 클라이언트를 사용할 경우 발생할 수 있는 문제에 대한 정보와 CIFS/9000 명령에서 나타날 수 있는 오류 메시지에 대해 설명합니다.

- 질문과 대답을 통한 문제 해결
- CIFS/9000 Client 오류 메시지

질문과 대답을 통한 문제 해결

이 절에서는 CIFS/9000의 일반적인 문제에 대해 설명합니다.

cifsclient stop 명령으로 데몬을 강제 종료하는 방법

데몬 프로세스를 직접 강제 종료해서는 안됩니다. CIFS/9000에서 모든 마운트된 공유를 마운트 해제하려고 시도하지만 성공하지 못할 수 있으며 멈춘 마운트를 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, 클러스터 시작 및 중지”를 참조하십시오.

데몬이 종료된 경우 처리 방법

데몬이 종료되는 즉시 CIFS/9000이 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.

CIFS/9000 Client 오류 메시지

이 절에서는 다음 명령에 대한 CIFS/9000 Client 오류 메시지를 설명합니다.

- cifsclient
- cifsmount
- cifslogin
- cifsumount
- cifslogout
- cifslist

`userdb: cannot open file`

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

cifsclient에서 메시지에 지정된 이유로 인해 사용자 데이터베이스 파일을 열 수 없습니다. CIFS/9000을 처음 시작한 경우 또는 사용자 데이터베이스에 저장한 데이터가 없는 경우 이 오류가 발생하는 것이 정상입니다.

`userdb: database file is incompatible`

cifsclient에서 사용자 데이터베이스 파일을 찾았지만 해당 파일이 다른 버전의 CIFS/9000 Client로 작성되었습니다. 보안 상의 이유로 모든 버전(다른 컴파일러로 실행한 경우 포함)의 CIFS/9000 Client가 서로 호환되지 않습니다.

`ipcclient: error connecting to daemon: ...`

명령줄 유틸리티에서 CIFS/9000 Client 데몬에 연결할 수 없습니다. 자세한 Unix 오류 메시지가 제공됩니다. 대개 데몬이 실행 중이지 않은 것입니다.

`LOC: Server can't encrypt passwords, use option to override`

서버가 암호화된 암호를 지원하지 않습니다. 기본적으로 CIFS/9000 Client는 암호를 일반 텍스트로 보내지 않습니다. 이 동작을 *-u* 옵션으로 재정의할 수 있습니다. 하지만 네트워크를 스니핑하는 해커가 네트워크 상의 암호화되지 않은 암호를 알 수 있기 때문에 주의하여 사용해야 합니다. 거의 모든 Unix 컴퓨터가 네트워크 스니핑의 대상이 될 수 있습니다. 또한 CIFS/9000 Client는 사용자 데이터베이스에 암호화되지 않은 암호를 저장하지 않습니다.

```
error: DOS: Access denied
```

제공한 사용자 이름/암호 쌍이 서버에 적용되지 않습니다. *-U* 옵션으로 사용자 이름을 명시적으로 제공해 볼 수 있습니다.

5 구성 파일

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

구성 파일은 시작 및 편집 시에 CIFS/9000 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 구성 변경 사항을 적용하려면 먼저 해당 서버에서 모든 공유를 마운트 해제하고 모든 사용자를 로그아웃해야 합니다.

주 CIFS/9000은 SSL 옵션을 지원하지 않습니다.

일반 구조

구성 파일은 다음과 같은 간단한 구문 구조로 구성됩니다.

- 참고 사항
- 문자열
- 배열
- 딕셔너리

문자열, 배열 및 딕셔너리는 “속성”이라는 일반 용어로 분류됩니다.

참고 사항은 다음과 같은 세 가지 형태로 작성할 수 있습니다.

```
/* remark */
```

C 형태

```
// remark to end of line
```

C++ 또는 Objective-C 형태

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

셸 스크립트 형태

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 변경됩니다.

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")
```

딕셔너리는 명명된 속성의 순서가 지정되지 않은 목록입니다. 이러한 목록은 중괄호로 묶습니다. 각 딕셔너리 항목은 문자열인 좌항(키), 등호, 임의 값이 될 수 있는 우항(값)으로 구성됩니다. 각 항목은 세미콜론으로 구분합니다. 다음은 *property1*부터 *property3*까지 세 개의 항목으로 구성된 딕셔너리의 예입니다. 여기서 첫 번째 항목은 문자열 값, 두 번째 항목은 배열 값, 세 번째 항목은 딕셔너리 값을 가집니다.

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

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

문자열로 구문 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. 마지막으로 부울 값은 *yes* 및 *no* 문자열로 구성된 열거의 특수한 경우입니다.

구성 변수

다음은 최상위 수준에서 구성할 수 있는 모든 변수 목록입니다.

logLevels 이 변수 값은 활성화된 모든 로깅 모드를 열거하는 배열입니다. 로깅 모드는 다음 집합을 구성하는 문자열입니다.

`info`

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

`error`

[1] 오류 메시지를 로그에 기록합니다. 반드시 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 경우 사용하도록 설정해야 합니다. CIFS/9000 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] 이 옵션은 모든 Netbios 송신 및 수신 트래픽의 16진수 덤프를 생성합니다. 디버그에는 매우 유용하지만 일반적인 작동에는 사용하지 말아야 합니다.

`nfsTrace`

[7] 이 유형의 로그 메시지는 커널에 의해 수행된 모든 NFS 요청과 관련 반환 값에 대한 자세한 정보를 제공합니다. NFS 부분의 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) 메카니즘을 디버그합니다. 디버그 중에만 유용합니다.

`warn`

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

`smbSequence`

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

`debugAttributes`

[13] 파일 속성 루틴의 디버그입니다. 디버그 중에만 유용합니다.

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

cfgParseInterval CIFS/9000 Client는 실행 중에 구성의 구문을 다시 분석할 수 있습니다. 이 기능이 작동하려면 CIFS/9000 Client가 정기적으로 파일을 폴링해야 합니다. *cfgParseInterval* 변수는 이 폴링 주기를 초 단위로 정의합니다. 0으로 설정할 경우 시작 시에 한 번만 파일을 구문 분석합니다. 기본값은 0입니다.

sockMode
sockOwner
sockGroup CIFS/9000 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 지정할 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 않은 경우 올바른 기본값으로 설정됩니다.

runAsUser CIFS/9000 Client 도메인은 루트로 시작해야 합니다. 보안을 향상시키기 위해서 루트 권한이 필요하지 않은 경우 다른 사용자 ID로 전환됩니다. 이러한 용도로 사용될 사용자 ID를 이 값으로 구성할 수 있습니다. 이것은 사용자 이름이거나 숫자 ID일 수 있습니다.

pidFile 필요에 따라 CIFS/9000 Client가 데몬의 프로세스 ID로 파일을 유지 관리할 수 있습니다. 이 값을 정의한 경우 pid를 저장해야 하는 파일의 경로로 해석됩니다. 정의하지 않은 경우 파일이 만들어지지 않습니다.

databaseFile 이 변수는 사용자 데이터베이스 파일 경로를 구성합니다. 여기에는 암호, 마운트 및 등록 키가 저장됩니다. 기본값은 */var/opt/cifsclient/cifsclient.udb*입니다.

allowSaving 이 부울 값은 사용자 데이터베이스에 사용자 암호 및 마운트를 저장할지 여부를 정의합니다. 저장하지 않으려면 *no*로 설정하십시오. 기본값은 *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 CIFS/9000 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 Unicode를 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 CIFS/9000 Client와 함께 배포됩니다. 이러한 파일은 *unitables* 디렉토리에 있습니다.

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.

nfsSockRxBuf 이 정수 변수는 커널과 통신하는 데 사용되는 소켓의 수신 버퍼 크기를 설정합니다. 지정된 값이 컴퓨터의 적용 가능한 범위를 벗어나는 경우 자동으로 CIFS/9000 Client가 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 CIFS/9000 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.x에서 그러한 경우가 많습니다. 블록 크기로 2의 승수만 사용하는 것이 좋습니다. 기본값은 8192입니다.

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.

defaultServer CIFS 구조에는 CIFS 연결에 대한 많은 구성 옵션이 있습니다. 이 변수는 각 서버별 구성으로 재정의할 수 있는 기본 동작을 정의합니다. 값은 다음 키를 사용하는 딕셔너리입니다.

localNetbiosName

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

mtabName 이 문자열 변수는 마운트 테이블 항목에 사용되는 호스트 이름을 정의합니다. Solaris의 경우 이 이름에 영향을 많이 받습니다. 지정된 호스트가 존재하지만 NFS(또는 RPC) 서비스를 제공하지 않는 경우 로그인에 오랜 시간이 걸릴 수 있습니다. 이 변수를 정의하지 않은 경우 기본값은 서버의 *hostname*(지정된 경우 *IP address*)입니다.

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 60000ms(60초)입니다.

nfsTimeout

이 정수 변수는 커널에서 CIFS/9000 Client에 데이터를 요청할 때 사용되는 초기 제한 시간(1/10초)을 정의합니다. 재시도를 할 때마다 이 값이 두 배가 됩니다. *nfsRetransmit*와 함께 사용하면 이 변수로 NFS 요청의 절대 제한 시간을 정의할 수 있습니다. 50(5초)의 값이면 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 CIFS/9000 Client가 정해진 시간 내에 응답하지 않을 경우 커널의 재시도 횟수를 정의합니다. 시간 제한은 *nfsTimeout*부터 시작하여 각 재시도마다 두 배가 됩니다. CIFS/9000 Client에서 손실되는 요청이 없기 때문에 다시 전송할 필요는 없습니다. 하지만 시스템의 NFS 클라이언트로 인해 NFS 서버의 로드가 많아지고 최대 소켓 버퍼 크기가 작은 경우 버퍼 오버플로로 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.

nfsAttributeCaching

NFS에 의한 파일 속성 캐싱을 사용하도록 설정하는 부울 변수로 CIFS 클라이언트의 속성 캐시를 효율적으로 재정의합니다. 이러한 캐시는 네트워크를 통해 전송되는 “속성 가져오기” 호출의 횟수를 줄여 마운트된 CIFS 파일 시스템에 있는 많은 파일의 *tar*(1) 압축 파일 만들기와 같은 특정 유형의 작업 성능을 개선합니다. 기본 설정은 “no”입니다.

sslRequireEncryption	이 부울 변수를 *yes*로 설정한 경우 비SSL 서버에 대한 연결이 거부됩니다. 그렇지 않은 경우 서버가 SSL(Secure Socket Layer) 사용 여부를 결정합니다.
sslVersion	SSL은 계속 발전하는 표준으로 여러 버전이 있습니다. 이 열거 변수는 사용되는 버전을 정의합니다. *ssl2, ssl3,ssl2or3* 또는 tls1로 설정할 수 있습니다. 기본값은 버전 2 또는 3을 자동 협상하는 *ssl2or3*입니다.
sslCompatibility	다른 SSL 구현의 버그에 대해서도 이상 없이 동작하도록 SSLeay를 구성할 수 있습니다. 비록 표준을 준수하지는 않지만 상호 운용성이 중요한 경우 유용합니다. 현재 모든 SSL CIFS 서버가 SSLeay를 사용하며 다른 호환성 고려 사항은 없습니다. 이 부울 변수를 *yes*로 설정한 경우 호환 모드로 전환됩니다.
sslCertFile	SSL 서버를 클라이언트로부터 인증서를 요구하도록 구성할 수 있으며 실제로 그렇게 구성해야 합니다. 클라이언트에 인증서가 필요한 경우 이 문자열 변수는 PEM 형식의 인증서를 포함하는 파일을 가리킵니다.
sslKeyFile	인증서는 키에 특정합니다. 인증서를 사용할 경우 키도 지정해야 합니다. 인증서 파일에 키가 포함되지 않은 경우 이 변수는 PEM으로 인코드된 형식으로 키가 있는 파일의 경로를 포함해야 합니다.

sslServerCert	이 변수는 협상 중에 서버에 유효한 인증서가 존재해야 하는지 여부를 정의합니다. 이것을 *required* 및 *allowOverride* 키를 포함하는 딕셔너리로 설정해야 합니다. *required* 항목은 서버 인증서가 필요한지 여부를 결정하는 부울 값을 가지며, *allowOverride* 항목은 *required*에 설정된 값을 *cifsmount* 명령줄에서 재정의할 수 있는지 여부를 결정하는 부울 값으로 설정해야 합니다.
sslCACertDir	서버 인증서가 필요한 경우 확인 방법이 있어야 합니다. 이 문자열 변수는 신뢰할 수 있는 모든 인증 기관(CA)의 인증서를 해시 처리(파일 이름이 CA 이름의 해시 값)된 형식으로 포함하는 디렉토리를 가리킵니다.
sslCACertFile	CA 인증서가 있는 디렉토리를 정의하는 대신 또는 추가로, PEM 형식으로 CA 인증서를 포함하는 단일 파일을 지정할 수 있습니다. 이 문자열 변수는 해당 파일의 경로를 포함합니다.
sslCiphers	이 문자열 변수를 사용하여 선호하는 암호 처리기를 설정할 수 있습니다. 하지만 연결 설정 중에 암호 처리기를 협상하므로 필수 사항은 아닙니다.
lookupStrategy	이 구성 변수에는 약간의 설명이 필요합니다. 알고 있는 것처럼 CIFS/9000 Client는 NFS 요청과 SMB/CIFS 요청을 매핑합니다. NFS 측에서는 NFS 파일 핸들이라고 하는 고유 ID로 파일을 참조합니다. 하지만 CIFS측에서는 단순히 파일 경로로 파일을 참조합니다. 따라서 CIFS/9000 Client가 NFS 파일 핸들로 지정된 경로를 확인할 수 있어야 합니다. 이러한 확인에 사용할 수 있는 다음과 같은 두 가지 방법이 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 CIFS/9000 Client에 공유 당 500KB 이상의 실제 메모리와 약 10MB 이상의 가상 메모리가 필요합니다.

database 방법이 기본값입니다.

caseSensitive	이것은 가능한 값이 *yes* 또는 *no*인 부울 변수로 서버에 있는 파일 이름의 대소문자를 구분할 것인지 여부를 지정합니다. 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 95는 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 CIFS/9000 Client에서 서버가 지원하는 경우 Unicode를 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.
alwaysEncryptData	이 부울 변수를 *yes*로 설정한 경우 서버와의 SSL(Secure Socket Layer) 연결만 허용됩니다. *no*로 설정한 경우 서버와 SSL을 협상합니다.

guestUser

guestUser 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. *guestUser*를 정의한 경우 로그인하지 않은 모든 Unix 사용자를 지정된 Unix 사용자인 것으로 취급할 수 있습니다. 물론 *guestUser*로 지정된 Unix 사용자는 *cifsmount* 또는 *cifslogin*의 *-s* 옵션을 사용하여 로그인해야 합니다.

fakeMountpointDate

이 부울 변수가 *yes*인 경우 마운트 지점의 수정 및 액세스 시간이 항상 현재 시간으로 표시됩니다. 이것은 Windows NT 또는 Windows 95처럼 루트 디렉토리의 수정 날짜에 대해 의미 없는 값을 반환하는 서버에 유용합니다. 기본값은 *no*입니다.

execMapping

이 열거 변수는 Windows 서버에 저장되는 파일에 유용합니다. 이것은 Unix *execute* 권한으로 매핑될 DOS 속성을 정의합니다. 사용할 수 있는 키워드는 *archive, system, hidden, on* 또는 *off*입니다. 기본값은 *on*입니다. *execMapping*의 부작용은 구성된 속성이 NT 서버에서 설정된 속성인 경우 Unix 클라이언트에서 파일이 실행 비트가 모든 사용자(*owner, group* 및 *other*)로 설정되어 나타나는 것입니다.

경고

Unix 실행 파일을 NT 서버에 저장하고 Unix 클라이언트에서 호출할 계획인 경우 기본 설정인 *execMapping* = *on*을 사용해야 합니다. 이 경우 Unix 클라이언트측에서 보면 Windows 서버에서 나열하는 모든 파일에 실행 비트가 설정됩니다 *execMapping* = *on*을 사용하면 CIFS/9000 서버에 있는 파일 속성에 영향을 미치지 않으므로 정상적인 Unix 파일처럼 작동합니다.

execInvert	이 부울 변수가 *yes*인 경우 *execMapping* 설정에서 파생된 실행 비트가 반전됩니다.
dirDefaultLinks	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 find에서 이러한 최적화를 사용하는 경우 링크 수가 큰 디렉토리를 링크 수가 적은 것처럼 가장할 수 있습니다. 대신 find의 명령줄 스위치를 사용하여 이 최적화를 끌 수 있습니다.
enableFakeLinks	이 부울 변수를 *yes*로 설정한 경우 CIFS/9000 Client가 Windows 서버에서 소프트 링크를 처리할 수 있습니다. 물론 해당 소프트 링크는 CIFS/9000 Client에서만 사용됩니다. Windows 서버에서는 해당 링크가 특수한 속성(구성을 수정하지 않은 경우 시스템 및 숨김 속성)이 설정된 일반적인 파일로 표시됩니다.

linkModeMask, linkMode

이 두 정수 변수는 일반 파일의 가장된 소프트 링크를 구분하는 데 사용되는 파일 속성을 정의합니다. *linkModeMask*의 기본값은 *read-only*, *hidden* 및 *system* 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 5-1

1	read-only	2	hidden	4	system	32	archive

linksAreUnicode 이 부울 변수를 *yes*로 설정한 경우 CIFS/9000 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 Windows에서 CygWin32와 호환되지만 서버 문자 집합으로 변환하는 과정이 수행됩니다. 이 변수에 관계 없이 CIFS/9000 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.

maxOpenFiles

서버에서 열린 상태를 유지하는 최대 파일 수입니다.

dataCacheSize

열린 파일에 할당되는 데이터 캐시의 크기(바이트)입니다. 값은 최대 전송 허용 크기에서 계산된 캐시 페이지 크기의 배수가 되도록 반올림됩니다. 페이지 크기는 항상 2의 거듭제곱입니다.

closeDelay

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

exclusiveLock

배타적 *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 oplock을 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 딕셔너리입니다.

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. NFS2와 함께 사용할 경우 다시 쓰기는 오류 복구의 측면에서 안전하지 않지만 성능이 상당히 향상됩니다. 값은 다음 키를 사용하는 딕셔너리입니다.

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 oplock을 요청할지 여부를 정의합니다. Windows95 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. 기본값은 *no*입니다.

disableSmbs

모든 서버가 모든 SMB 명령을 동일하게 지원하는 것은 아닙니다. 실제로 특정 유형의 서버에서는 많은 명령을 사용할 수 없습니다. 이 변수 값은 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 95에서 문제가 있는 것으로 보입니다.

`attrUnix`

파일 속성의 Unix 확장을 사용하지 않도록 설정합니다.

`setattrTrans2SetFile`

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

`setattrTrans2SetPath`

파일 속성 설정에 사용되는 *trans2/setpathinfo* 명령을 억제합니다. 이 SMB 명령은 NT에서 올바로 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_CONNNECT_ANDX 명령을 억제합니다(*TREE_CONNECT*를 대신 사용함).

`setDirDates`

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

servers

이 변수는 특정 서버의 *defaultServer*로 구성된 값을 수정할 수 있습니다. 이것은 키가 서버의 Netbios 이름인 딕셔너리로 구성됩니다. 각 서버 키의 값 또한 딕셔너리입니다. 이 딕셔너리는 *defaultServer* 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 *cifsmount* 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 139입니다.

serverClasses

세션 설정에서 파생된 정보에 기반하여 연결이 설정된 후에 *defaultServer* 및 *servers*로 구성된 값을 이 변수로 수정할 수 있습니다. 결정은 서버 운영 체제와 LAN 관리자 유형에 따라 달라집니다. 이 변수의 형식은 딕셔너리 배열입니다. 각 딕셔너리에는 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(딕셔너리)이 서버 구성으로 사용됩니다. 옵션이 지정된 경우 이전 구성의 해당 옵션을 재정의합니다. 하지만 *disableSmbs* 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.

6 PAM NTLM

이 장에서는 PAM NTLM을 설명합니다.

소개

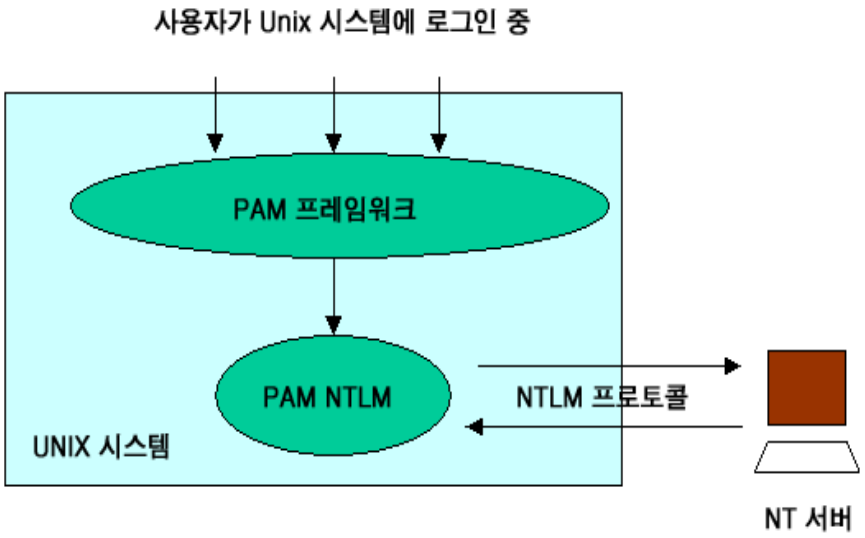
PAM NTLM은 HP-UX 사용자가 시스템 로그인 중에 Windows 서버에 인증할 수 있게 하는 플러그인 인증 모듈(Pluggable Authentication Module)입니다.

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 NT 서버를 사용하여 HP-UX 시스템에 로그인하는 사용자를 인증합니다. 즉, PAM NTLM은 NT LanManager 프로토콜을 사용하여 UNIX 사용자를 인증합니다. 따라서 UNIX 사용자 이름과 암호를 확인을 위해 NT 서버로 전송하고 결과가 PAM 프레임워크로 반환됩니다. CIFS/9000 클라이언트는 PAM NTLM 인증 정보를 사용하여 CIFS/9000 서버에 있는 공유를 액세스합니다. 따라서 *cifslogin* 명령을 사용할 필요 없이 HP-UX 시스템에 로그인한 사용자가 CIFS로 마운트된 파일 시스템을 액세스할 수 있습니다.

PAM NTLM을 구성하려면 PAM 프레임워크의 일반적인 사항을 이해해야 합니다. PAM에 대한 자세한 내용은 *pam(3)*, *pam.conf(4)* 및 http://docs.hp.com/hpux/os의 *Managing Systems and Workgroups*를 참조하십시오.

그림 6-1 PAM 소개



PAM NTLM은 동적으로 로드할 수 있는 모듈입니다. PAM 프레임워크는 사용자 이름과 암호를 PAM NTLM 모듈에 전송하고, PAM NTLM은 NTLM 프로토콜을 사용하여 Windows 서버에 대한 인증을 수행합니다.

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 NT 도메인 사용자 이름으로 매핑하는 **사용자 이름 매핑**을 지원합니다. 자세한 내용은 PAM NTLM 구성 절을 참조하십시오.
- 사용자/암호 인증에 성공하면 CIFS 클라이언트에서 사용할 수 있도록 캐시에 저장됩니다.
- CIFS 서버에 대한 로그인 인증은 NTLM의 암호화된 암호를 사용합니다.
- HP-UX *passwd(1)* 명령을 사용하여 NT 4.0 PDC(Primary Domain Controller)의 CIFS 사용자 암호를 업데이트합니다.

설치 단계에 대해서는 2장을 참조하십시오.

사용자 맵 파일

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

PAM NTLM을 사용하도록 *password(1M)*를 구성한 경우 매핑된 NT 도메인 사용자의 암호가 NT 서버에서 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 참고해야 하기 때문에 기본 구성 파일을 변경해서는 안됩니다.

표 6-1

```
     ##
## 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: NT-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.conf를 편집하는 과정입니다.

중요

PAM을 올바르게 구성하지 않은 경우 시스템에 로그인할 수 없습니다. pam.conf를 수정하려면 PAM 프레임워크를 이해해야 합니다. PAM에 대한 자세한 내용은 HP-UX 온라인 설명서에서 pam.conf(4), pam_unix(5)를 참고하십시오.

보안 상의 이유로 PAM-NTLM에 의해 구성된 암호 서버 대신 호스트 시스템(PAM-UNIX)이 루트 및 기타 권한이 있는 사용자를 인증하도록 직접 구성하는 것이 좋습니다. 또한 PAM-UNIX의 대체 대상이 아닌 추가 대상으로 PAM-NTLM을 사용하는 것이 좋습니다. 이 구성에 대해 아래의 pam.conf에서 설명합니다.

배경 정보 PAM NTLM은 HP-UX와 Microsoft Windows NT 서버 또는 HP CIFS/9000 Server가 실행되고 있는 다른 UNIX 서버에 중앙 집중식 인증 서비스를 제공합니다. HP CIFS/9000 Client 제품에는 HP-UX 로그인을 아무 CIFS/9000 Server나 Windows NT 도메인 컨트롤러와 통합하는 PAM NTLM이 있습니다.

PAM NTLM은 암호화된 암호를 사용하여 사용자를 인증합니다. 또한 NTLM은 암호 변경과 암호 만료를 지원하므로, 사용자가 HP-UX 워크스테이션에서 자신의 NT 암호를 변경할 수 있습니다.

PAM NTLM은 공유 PAM NTLM 라이브러리 두 개로 구성되는데, 그 중 한 개는 PAM 모듈 인증, 계정 관리, 세션 관리, 암호 관리 네 개 모두를 위한 기능을 제공하며, 다른 한 개는 NT LanManager 프로토콜을 이용한 NT 서버와의 통신을 지원합니다.

인증 모듈 인증 모듈에서는 사용자의 ID를 확인하고 사용자별 자격 증명을 설정한 다음, 사용자를 NT 서버에 인증합니다(*/etc/opt/cifsclient/pam/smb.conf*에 구성됨). 암호가 일치하고 사용자가 로그인 권한을 가지고 있으면(계정이 비활성화되어 있지 않으면) 해당 사용자가 시스템에 로그인할 수 있습니다.

CIFS/9000 클라이언트는 사용자가 CIFS 마운트 공유 볼륨에 액세스할 때 이 로그인 정보를 사용할 수 있습니다. 그러므로 사용자는 CIFS 공유 볼륨에 액세스하기 전에 cifslogin 명령을 사용할 필요가 없습니다.

인증 모듈은 use_first_pass, try_first_pass및 debug 옵션을 지원합니다. debug 옵션을 지정하면 PAM NTLM이 syslog에 디버그 메시지를 기록합니다. 다른 옵션에 대한 자세한 내용은 PAM 설명서를 참조하십시오.

계정 관리 계정 관리 모듈은 사용자의 암호 만료 정보를 검색하고 암호가 만료되지 않았는지 확인합니다.

위에 지적한 용도를 제외하고는 이 기능은 NT/UX 서버에서 실질적인 계정 관리를 수행하지 않으며, PAM 사양과의 호환성을 위해 제공됩니다.

세션 관리 세션 관리 모듈은 세션을 시작하고 종료하는 기능을 제공합니다. PAM NTLM은 세션 관리를 지원하지 않으며 언제나 결과가 성공으로 나타납니다. 이 모듈은 PAM 사양과의 호환성을 위해 제공됩니다.

암호 관리 암호 관리 모듈은 NT 서버 데이터베이스의 암호를 변경하는 기능을 제공합니다. 이 PAM 모듈에 대해 `use_first_pass`, `try_first_pass` 및 `debug` 옵션을 지정할 수 있습니다. `debug` 옵션을 지정하면 PAM NTLM이 `syslog`에 디버그 메시지를 기록합니다. 다른 옵션에 대한 자세한 내용은 PAM 설명서를 참조하십시오.

PAM-NTLM은 다음 서비스를 제공합니다.

- 암호 인증
- 암호 변경
- 만료 통지 시 암호 변경

각 서비스는 pam.conf의 특정 섹션에 해당합니다. 사용하려는 서비스에 대한 항목을 추가합니다.

- 암호 인증의 경우 pam.conf의 “Authentication management” 섹션을 수정합니다.
- 암호 변경의 경우 “Password management” 섹션을 수정합니다.
- 만료 통지 시 암호 변경의 경우 “Authentication management”, “Password management” 및 “Account management”를 수정합니다(만료 통지 시 암호 변경을 이용하려면 암호 인증과 암호 변경도 사용하도록 설정해야 함).

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

경고

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

다음 pam.conf 예제 파일은 HP-UX B.11.22 버전용입니다.

예제 6-1 HP-UX 버전 B.11.22용 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 6-2 **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

*UNIXusername*은 HP-UX 시스템의 기존 계정이며, *DomainUserName*은 NT 도메인에서 매핑된 사용자 이름입니다. *DOMAIN_NAME*은 선택 사항입니다.

사용자 맵 파일은 줄 단위로 구문 분석됩니다. # 또는 ;으로 시작하는 모든 줄은 무시됩니다. 각 줄은 왼쪽에 단일 Unix 사용자 이름이 있고 탭이나 '='으로 구분된 오른쪽에 단일 NT 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.byname으로 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.

용어집

A

ACL Access Control List(액세스 제어 목록)의 약자이며, 파일 데이터에 어떤 사용자가 액세스할 수 있으며 그 데이터에 어떤 유형의 액세스가 허용되어 있는지 기술하는 메타 데이터입니다. ACL은 "액세스 권한"을 정의합니다. 이 구조에서 사용자는 일반적으로 "그룹"에 속하며 그 그룹 전체에 액세스 권한이 부여됩니다. 액세스 권한의 일반적 유형으로 읽기(list), 쓰기(modify) 또는 작성(insert)이 있습니다. 파일 시스템에 따라 다양한 ACL 지원 레벨이 있으며 각 파일 시스템마다 액세스 권한을 다르게 정의합니다. 예를 들어, DOS에는 파일에 대해 한 세트의 권한만 존재합니다(DOS 시스템은 한 명의 사용자만 사용하는 것으로 간주하므로). POSIX 6 호환 파일 시스템에서는 여러 사용자와 여러 사용자 그룹에 대해 여러 파일 및 디렉토리에 여러 권한을 할당할 수 있습니다.

ASP 응용 프로그램 서비스 제공자(Application Service Provider)를 의미하며, 사용자에게 응용 프로그램을 "임대"하는 e-business입니다.

인증 파일 데이터에 액세스하는 사용자의 신원을 확인하기 위한 구조입니다. 보안 네트워크 파일 시스템에서는 인증을 사용하여 사용자가 다른 사용자를 가장하여 액세스하는 것을 방지합니다.

권한 사용자가 액세스 권한을 가진 파일 시스템에만 액세스할 수 있게 합니다. 인증된 사용자라 하더라도 모든 파일을 읽고 쓸 수 있다는 것을 의미하는 것은 아니기 때문입니다. 가장 간단한 형태의 권한을 예로 들면, 사용자는 액세스 제어 정보(액세스 제어 목록, ACL)의 사용을 통해 파일 시스템의 개별적 파일 및 디렉토리에 대한 읽기 또는 쓰기 권한을 부여 받습니다.

C

CIFS Common Internet File System(공통 인터넷 파일 시스템)의 약자로 인터넷을 위해 설계된 파일 액세스 프로토콜 사양입니다.

CIFS/9000 Hewlett-Packard의 UXNI용 CIFS의 구현입니다. CIFS/9000은 HP 9000 서버 및 워크스테이션을 위한 서버 및 클라이언트 모듈을 모두 제공합니다.

자격 증명(Credential) 사용자를 식별하는 정보입니다. 자격 증명은 사용자에게 고유하게 연결된 번호(예를 들어, 주민등록번호)처럼 간단한 것일 수 있고, 추가적인 식별 정보가 포함된 복잡한 것일 수도 있습니다. 강력한 자격 증명에는, 자격 증명의 사용자가 해당 자격 증명이 식별하는 실제 사용자라는 증거(증명자라고도 함)가 들어있습니다.

D

Diffie-Hellman 비밀 키를 두 사용자 간에 안전하게 공유하기 위한 프로토콜입니다. Diffie-Hellman 프로토콜은 공개 키 교환 형태를 사용해 비밀 키를 공유합니다. Diffie-Hellman은 중간에 가로채기하는 공격의 가능성이 있는 것으로 알려졌지만, 이후 향상된 인증된 Diffie-Hellman Key Agreement에서는 그런 중간 공격이 방지되었습니다.

E

암호화 암호화를 사용하면 비밀(또는 개인) 키를 소유한 사용자만 데이터를 볼 수 있습니다. 암호화된 데이터는 비밀 키를 사용해 해독하기 전까지는 무의미한 데이터입니다. 데이터의 암호화 및 암호 해독을 암호(ciphering)라고 합니다.

I

무결성 무결성은 파일 시스템 데이터가 침입자에 의해 수정되지 않았다는 것을 보증하는 것입니다. 침입자는 네트워크 파일 시스템 발견 및 간섭 거부 없이는 파일 시스템 데이터 패킷을 가로채어 수정할 수 없습니다.

K

Kerberos MIT 및 IETF 워킹 그룹이 개발한 인증 및 권한 부여 보안 시스템입니다. 비밀 키 기술을 기반으로 하며 중앙 집중식 설계 때문에 일반적으로 공개 키 인프라에 비해 관리가 쉽습니다. 하지만 Kerberos는 공개 키 인프라만큼 확장성이 좋지 않습니다.

P

공개 키 두 사용자가 데이터를 안전하게 교환할 수 있지만 한 방향으로만 가능한 암호화 방식입니다. 개인 키를 가진 사용자가 그에 해당하는 공개 키를 만듭니다. 이 공개 키는 다른 사람에게 줄 수 있습니다. 이 사용자에게 암호화된 데이터를 전송하고자 하는 사람은 공개 키를 사용해 데이터를 암호화할 수 있습니다. 개인 키를 소유한 사용자만 이 데이터의 암호화를 해독할 수 있습니다.

공개 키 인프라 공개 키 암호화를 관리하는 방식입니다. 공개 키 기술은 암호 해독 키를 교환하지 않는다는 장점이 있지만 관리가 어렵다는 단점이 있습니다. 공개 키 배포에 따르는 문제점 중에는 키의 소유자를 증명하는 것과 만료 또는 종료된 키의 폐지에 관한 문제가 있습니다.

S

Samba 1990년대 중반에 처음 선보인 오픈 소스 제품입니다. Samba는 기본 도메인 컨트롤러(PDC) 및 백업 도메인 컨트롤러(BDC) 동기화 프로토콜을 제외한 Advanced Server for UNIX의 기능 대부분과, UNIX 시스템에 NT 파일 및 인쇄 서버 기능을 제공합니다. Samba는 널리 사용되고는 있지만 업체 지원은 그리 많지 않습니다.

비밀 키 대칭형 키 또는 공유 키라고도 하는 비밀 키 암호화는, 두 사용자가 공유된 비밀 키로 데이터를 암호화 및 암호 해독하는 암호 기법입니다. 같은 키를 사용해 데이터를 암호화 및 암호 해독합니다. 비밀 키를 알면 누구나 데이터를 암호 해독할 수 있으므로 비밀 키는 안전한 방식으로 교환해야 합니다.

SMB Server Message Block(서버 메시지 블록)의 약자로, Windows 네트워킹의 핵심을 이루는 파일 공유 프로토콜입니다. SMB는 Windows NT, Windows 95, Windows for Workgroups 및 OS/2 LAN Manager가 공유합니다. 근본적으로 보면 CIFS는 이 프로토콜의 이름을 바꾼 것입니다.

자

카

파