

# HP CIFS Server 2.2I 发行说明 A.01.11.04

HP-UX 11.0、 11i v1 和 v2



i n v e n t

生产部件号: B8725-90084

E0505

© 版权所有 2005 Hewlett-Packard Development Company, L.P.

---

## 法律声明

本文档中的信息如有更改，恕不另行通知。

Hewlett-Packard 对本手册不作任何担保，包括但不限于适销性及特定用途适用性的隐含担保。Hewlett-Packard 对本手册中包含的错误以及与其结构、性能或使用有关的直接、间接、特殊、偶发或继发性损失不负任何责任。

### 保修

可以从当地销售与服务机构索取适用于您所购买的 Hewlett-Packard 产品及更换部件的特定保修条款。

### 有限权利注释

美国政府使用、复制或披露本文，国防部应遵守 DFARS 252.227-7013 中“技术数据和计算机软件权利”条款的 (c) (1) (ii) 小节的规定；其他部门则应遵守 FAR 52.227-19 中“商业计算机软件有限权利”条款的 (c) (1) 和 (c) (2) 小节的规定。

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

本手册及软件包中提供的软盘或磁带仅限于本产品使用。

### 版权声明

版权所有 © 1983-2005 Hewlett-Packard Development Company, L.P.。除非版权法允许，否则未经书面许可，不得对本文档进行复制、改编或翻译。

### 商标声明

UNIX® 是 The Open Group 的注册商标。

# 第 1 章 HP CIFS Server 发行说明

---

## 声明

本文档包含有关 HP CIFS Server A.01.11.04 发行版中提供的缺陷修复程序的信息以及其他有用信息。下面重点列出主要更改内容。

### 通用互联网文件系统 (CIFS) Server A.01.11.04

- 该版本的 HP CIFS Server 是基于 Samba 2.2.12 的一个修复版本。
- 对可能出现的整数溢出漏洞提供了修复方法。在 HP CIFS Server 的 MS RPC 未封送处理代码中发现了安全漏洞 CAN-2004-1154，该漏洞可能会使合法用户通过远程操作获取超级用户的权限。有关详细信息，请参考 CR JAGaf50678。
- 此版本的 CIFS Server 列举了自 A.01.11.03 版以来解决的问题。有关详细信息，请参考第 5 页上的“HP CIFS Server A.01.11.04 中的修复方法”一节。

---

## 注释

HP 不支持使用 `inetd` 配置来启动 HP CIFS Server。

---

## 警告

在以前的发行版本中，可以将不同版本的 CIFS Server 中的二进制文件放在 `/opt/samba/bin` 子目录中，而不会出现明显的负面影响。而在 A.01.11.01 或更高版本中，HP 实现了一种锁定 TDB 文件的新方法，在此情况下，除了此发行版附带的二进制文件外，使用任何其他二进制文件都极不安全。必须使用 `swinstall` 实用程序正规安装 CIFS Server 的各个版本，而不要在系统间复制不同修订版的 CIFS Server 二进制文件。

## 产品修订号

新的 HP CIFS Server 版本采用产品修订号 (A.xx.xx.FF) 来标识，它可能是代表功能特性修改的版本，也可能是代表缺陷修复的版本。

功能特性版本包括新功能和（或）新的 Samba 源代码版本。基本产品修订号 (A.xx.xx) 依次递增；不使用代表缺陷修复的后缀编号。

缺陷的修复版本仅包括解决特定缺陷所需的产品变更。基本产品修订号 (A.xx.xx) 不变；只对代表缺陷修复的后缀编号 (A.xx.xx.FF) 依次递增。

## HP CIFS Server A.01.11.04 中的修复方法

HP CIFS Server A.01.11.04 提供了下列修复方法：

- 潜在的整数溢出漏洞 SSRT4885 (CR JAGaf50678)

在 HP CIFS Server 的 MS RPC 未封送处理代码中发现了安全漏洞 CAN-2004-1154。利用此问题可能通过远程操作获取超级用户访问权限。HP 在 Samba 3.0 的基础上研制了修复方法，并推荐使用该修复方法。

- 错误的软件仓库大小 (CR JAGaf02001)

现在，HP CIFS Server 将只在一个压缩的 gz 文件 `/opt/samba_src/samba/source.tar.gz` 中提供 Samba 源代码文件，而不像以前的发行版提供多个未压缩的文件。只有超级用户可以使用 `gunzip/untar` 对该文件进行解压缩。只有超级用户可以访问这些源代码文件。

- %U 问题 (CR JAGaf50442)

此前，在 CIFS Server 上，无法将 %U 变量视为会话名称，%U 变量被错误地扩展为 HPUX 用户名而不是 Windows 用户名，此修复方法解决了这一问题。

## 最近几个发行版中的特性和修复内容

### HP CIFS Server A.01.11.03 中的修复方法

HP CIFS Server A.01.11.03 提供了下列修复方法：

潜在的安全漏洞  
(CR JAGaf42460)

修复了一个潜在的安全漏洞，该漏洞可能使用户通过设置 `wide links= yes` `smb.conf` 选项获取对某一共享目录中任意文件的访问权限。

### HP CIFS Server A.01.11.02 新增修复方法

潜在的安全漏洞  
(CR JAGaf33614)

此修复方法会在使用 `name mangling` 函数时检查潜在的缓冲区溢出问题。

### HP CIFS Server A.01.11.01 中的修复方法

HP CIFS Server A.01.11.01 提供了下列修复方法：

多个 %U 扩展共享  
(CR JAGaf14310)

此前，当新用户从一台计算机（使用“runas”，或通过终端服务器或 Citrix Metaframe 在单个连接上实现多路复用）连接到 %U 形式的共享名上时，同一台计算机上使用“runas”工具或终端服务器或 `citrix metaframe` 的客户将无法访问到由某些用户使用类似 %U 的形式定义的共享名，此处的更改解决了这一问题。

安装错误  
(CR JAGae74686)

此处的更改可防止在 NIS 环境中安装 CIFS 软件仓库时 `swinstall` 操作失败，此操作无法将 `smbnull` 组添加到本地帐户 `/etc/group` 中。

### HP CIFS Server A.01.11.01 最新变化

HP CIFS Server A.01.11.01 提供了下列增强功能：

- HP CIFS Server 提供 SSL 支持实现与 LDAP 通信

HP CIFS Server 提供了安全套接字层 (SSL) 支持，以保护 CIFS 服务器与启用了 SSL 的 LDAP 目录服务器之间的通信。

现在，可以配置 `smb.conf` 文件中指定的 `ldap ssl` 参数，来启用安全套接字层 (SSL) 支持。启用 SSL 支持后，HP CIFS Server 即可使用户访问启用了 SSL 的 LDAP 目录来保护网络口令，并确保 CIFS Server 与启用了 SSL 的 LDAP 目录服务器之间通信的机密性和数据完整性。

有关如何安装和配置 Netscape Directory Server、LDAP-UX Client Services 和 HP CIFS Server 来启用 SSL 协议实现与 LDAP 的通信的详细信息，请参阅《HP CIFS Server 2.2i Administrator's Guide》中的“LDAP Integration Support”一章，该手册位于 <http://www.docs.hp.com> 网站上。

---

注释

尽管其他 LDAP 产品可与 HP CIFS Server 协调工作，但 HP 仅为带有 HP LDAP-UX Integration (J4269AA) 和 HP Netscape Directory Server (J4258CA) 产品配置的 HP CIFS Server 提供 LDAP 支持。

---

注释

HP CIFS Server 仅支持在 Windows 200x 域中使用早于 Windows 2000 版本的计算机成员。

- 用于 SSL 支持功能的新增配置参数

HP CIFS Server 提供了一个新的全局参数 `ldap ssl`，用于将 HP CIFS Server 配置为允许与 LDAP 目录建立 SSL 连接。此参数在 `/etc/opt/samba/smb.conf` 文件中进行定义。

可以使用 `ldap ssl` 选项来指定安全套接字层 (SSL) 支持。HP CIFS Server 不支持 `ldap ssl = start tls` 选项。如果目录服务器在 LDAP 中使用 SSL，则将此参数指定为 **Yes** 可以启用 SSL 功能，反之，如果指定为 **No**，则会禁用 SSL。缺省情况下，此参数设置为 **No**。

- 用于 Samba LDAP 工具的新选项

HP CIFS Server 为 `/opt/samba/LDAP/smbldap-tools` 目录中的所有 Samba LDAP 工具提供了两个新的脚本选项 `-Z` 和 `-S`。下面将介绍这些新选项：

<code>-Z</code>	使用与 LDAP 目录的安全 SSL 连接
<code>-S</code>	从 <code>/etc/opt/samba/smb.conf</code> 文件（而不是 <code>/opt/samba/LDAP/smbldap-tools/smbldap_conf.pm</code> 文件）中获取 LDAP 配置参数。

有关如何使用脚本选项的详细信息，请参阅《HP CIFS Server 2.2i Administrator's Guide》中的“LDAP management Tools”一节，该手册位于 <http://www.docs.hp.com> 网站上。

---

#### 注释

可以编辑脚本配置文件 `/opt/samba/LDAP/smbldap-tools/smbldap_conf.pm` 来设置 LDAP 参数。也可以在运行 LDAP 管理工具时指定 `-s` 选项以使用 `/etc/opt/samba/smb.conf` 文件中的 LDAP 配置参数。

如果为 LDAP 管理工具指定了 `-s` 选项，则会使用 `/etc/opt/samba/smb.conf` 文件中的 LDAP 配置值。如果不指定 `-s` 选项，则 LDAP 管理工具将使用 `/opt/samba/LDAP/smbldap-tools/smbldap_conf.pm` 文件中指定的 LDAP 配置值。

---

- **提高 CPU 使用率**

对锁定 TDB 文件的新方法进行了增强，从而在包含上百或上千个客户端连接的情况下提高了 CPU 的使用率。这一新的增强功能包括 为每个 TDB 分别创建一个锁文件，并使每个 `smbd` 在锁文件 (`*.tdb.lck`)（而不是 TDB (`*.tdb`) 文件）中拥有一个锁。这样，每个客户端连接都需要大约 10 个以上的文件描述符。

---

## 在 HP CIFS Server 中启用安全套接字层 (SSL)

如果打算使用 SSL，但尚未在 LDAP 中启用 SSL，则需要在 Netscape Directory Server 和 LDAP-UX 客户端上启用它。启用 LDAP 服务器和客户端后，可以对 HP CIFS Server 进行配置来使用 SSL。

在计划启用 LDAP 的 SSL 通信之前，必须正确配置 CA（Certification Authority，证书颁发机构）服务器。

以下内容总结了在配置和启用支持 SSL 的 HP CIFS Server 时所需的基本步骤。有关详细信息，请参阅《HP CIFS Server 2.2i Administrator's Guide》中的“LDAP Integration Support”一章。

- 第 1 步 .** 为 Netscape Directory Server 获取并安装一个证书，然后对 Netscape Directory Server 进行配置，使其信任 Certification Authority (CA) 证书。
- 有关详细说明，请参阅《Netscape Directory Server 6.1 Administrator's Guide》的“Managing SSL”一章中的“Obtaining and Installing Server Certificates”一节，该手册位于 <http://docs.hp.com> 网站上。
- 第 2 步 .** 在目录中启用 SSL。
- 有关如何在目录服务器中启用 SSL 的详细说明，请参阅《Netscape Directory Server 6.1 Administrator's Guide》的“Managing SSL”一章中的“Activating SSL”一节，该手册位于 <http://docs.hp.com> 网站上。
- 第 3 步 .** 配置 Administration Server，使其能够连接到启用了 SSL 的目录服务器。
- 有关配置 Administration Server 以连接到启用了 SSL 的目录服务器的详细说明，请参阅《Managing Servers with Netscape Console》，该手册位于 <http://docs.hp.com> 网站上。
- 第 4 步 .** 另外，还可确保目录服务器的每一位用户在通过 SSL 进行身份验证的所有 LDAP 客户端上都获取并安装一个私人证书。
- 在 LDAP-UX 客户端上安装证书数据库的一种方法是，通过 Netscape Communicator 下载该证书数据库。
- 根据所使用的 Netscape Communicator 的版本，此证书数据库文件 cert7.db 和 key3.db 将下载到客户端系统的 /.netscape 或 /.mozilla/default/\*.slt 目录中。如果使用 Netscape Communicator 7.0 下载 Certification Authority 证书，则证书数据库文件 cert7.db 和 key3.db 将下载到 /.mozilla/default/\*.slt 目录中。

## HP CIFS Server 发行说明

### 在 HP CIFS Server 中启用安全套接字层 (SSL)

如果使用 Netscape Communicator 4.75 下载 Certificate Authority 证书，则证书数据库 cert7.db 和 key3.db 将下载到 /.netscape 目录中。

将证书数据库文件 cert7.db 和 key3.db 下载到客户端后，需要创建指向 cert7.db 的符号链接 /etc/opt/ldapux/cert7.db 和指向 key3.db 的符号链接 /etc/opt/ldapux/key3.db。

有关如何在 LDAP-UX 客户端系统上安装 Certification Authority 证书的详细说明，请参阅《LDAP-UX Client Services B.03.20 Administrator's Guide》的“Installing LDAP-UX Client Services”一章中的“Configuring LDAP Clients to Use SSL”一节，该手册位于 <http://docs.hp.com> 网站上。

- 第 5 步 . 通过运行 setup 程序来配置 LDAP-UX 客户端服务以使用 SSL。有关如何运行 setup 程序在 LDAP-UX 客户端服务中启用 SSL 的详细说明，请参阅《LDAP-UX Client Services B.03.20 Administrator's Guide》的“Installing LDAP-UX Client Services”一章中的“Custom Configuration”一节，该手册位于 <http://docs.hp.com> 网站上。

如果已经设置了 LDAP-UX 客户端服务，则按如下说明修改 /etc/opt/ldapux/ldapux\_profile 中的 authenticationMethod 和 preferredServerList 属性：

- 修改 authenticationMethod 属性，在原身份验证方法 simple 前面添加传输层安全身份验证方法 tls:。

例如，在未启用 SSL 的情况下，原条目 authenticationMethod 为 authenticationMethod: simple。启用 SSL 后，authenticationMethod 条目将为 authenticationMethod: tls:simple。

- 修改 preferredServerList 属性，将常规的 LDAP 端口号 389 更改为 SSL 端口号 636。

例如，在未启用 SSL 的情况下，原条目 preferredServerList 为 preferredServerList: 15.13.111.200:389。启用 SSL 后，preferredServerList 条目将为 preferredServerList: 15.13.111.200:636。

- 第 6 步 . 将 HP CIFS 配置选项 ldap ssl 设置为 Yes。ldap ssl 配置选项位于 /etc/opt/samba/smb.conf 文件中。

---

## 从 A.01.07 或更早版本进行更新

更新时，请考虑下列问题：

### 打印机驱动程序

- 如果不希望使用新的 Windows NT/XP/2000 打印机驱动程序支持功能，请不要进行任何操作。现有的所有打印机服务配置参数都将与以前一样继续保持有效
- 如果希望使用新的 NT/XP/2000 打印机驱动程序支持功能，但又不希望将 Windows 9x 驱动程序更新为新的设置，请使用现有的 printers.def 文件
- 如果要为 HP CIFS Server 上的打印机安装 Windows 9x 驱动程序，将会优先使用新的设置信息，并会忽略三个旧参数（printer driver、printer driver file 和 printer driver location）
- 如果在 HP CIFS Server A.01.07 或更低版本上安装了一台打印机，并且要更新到 Server A.01.08 或更高版本，则必须重新引导 Windows 客户端以使该打印机能够在 A.01.08 或更高版本上工作

### 配置

- 在 POSIX ACL 管理中必须使用 smbpasswd 文件

为了在操作 POSIX ACL 时可以正确列举用户名，必须将 HP-UX 用户输入到 smbpasswd 文件中。与以前版本直接查询 UNIX 用户数据库不同，在本地计算机上显示用户名时，A.01.08 及更高版本将始终访问 smbpasswd 文件。可以使用所提供的命令行工具 syncsmbpasswd 填写 smbpasswd 文件。

### HP-UX 资源

- 内核参数

HP CIFS Server A.01.08 及更高版本与以前的版本在系统资源的使用方面具有一些差异。必须相应调整下列 HP-UX 内核参数：

#### — NFILES — 每个系统打开的文件总数

每个 smbd 进程最初将打开 23 个文件供内部使用。而客户端将在会话期间打开更多的文件。因此，nfiles 的最小值应是：

$$\text{nfiles} = (23 + \text{max\_client\_files}) * \text{max\_connected\_clients}$$

注意：以前版本的 CIFS Server 会打开 8 个文件供内部使用。

— NFLOCKS — 每个系统的文件锁总数

每个 `smbd` 进程至少分配有十 (10) 个文件锁供内部使用。根据所使用的应用程序的不同，客户端可能需要更多的文件锁。因此，`nflocks` 的最小值应是：

`nflocks = 10 * max_connected_clients`

注意：以前版本的 CIFS Server 不要求对此参数进行显式配置。

这些最小参数值准则仅说明 HP CIFS Server 的系统资源使用情况。其他应用程序和系统进程可能要求进一步提高这些参数的值。

• 内存要求

连接的每个客户端至少使用 1MB 的内存，这种内存需求大约是 A.01.07 的两倍。例如，如果某系统要连接 1024 个客户端，则该系统的物理内存量应至少为 1 GB。该内存数大于与 CIFS Server 并发运行的其他应用程序的要求。

---

注释

使用非常大的 `smb.conf` 文件可能会显著增加内存使用率。因此，最好将 `smb.conf` 文件中不必要的行数减至最少。要实现此目的，方法之一就是使用 SWAT 实用程序进行配置。

---

---

## 已知问题和解决办法

### 用于 HP CIFS Server

下面列出了 HP CIFS Server A.01.11 中的已知问题以及相应的解决办法（如果有）\*：

问题	共享模式安全性对于 POSIX ACL 无效。
解决办法	Microsoft 服务器不支持共享模式安全性和 Windows NT ACL。目前尚无解决办法。
问题	CIFS 客户端无法删除打开的文件。 <b>相关缺陷：</b> 文件保持打开状态时，CIFS 客户端无法删除与打开的文件的硬链接。
解决办法	请先关闭文件，然后再删除文件和硬链接。
问题	在客户端连接到 CIFS Server 之前，smbstatus 实用程序和 SWAT 状态屏幕不显示任何信息。
解决办法	请先连接 CIFS Server，再使用 smbstatus 实用程序和 SWAT 状态屏幕。
问题	在共享 CIFS Server 驱动器的 DOS 提示符下，使用通配符和多字节字符集匹配文件名中的单个字符时，有时工作不正常（例如：使用日语 Shift-JIS 和 ???? 匹配的是两个多字节字符，而不是四个多字节字符）。
解决办法	使用 ?? 与每个单字符匹配。例如，如果要与四个字符匹配，必须使用八个通配符 ????????。
问题	当 Windows XP 客户端尝试加入和登录到 CIFS Server PDC 域时，需要正确设置本地安全策略和注册表条目。
解决办法	使用 Windows XP 界面 (Start → Control Panel → Administrative Tools → Local Security Policy → Security Options) 设置本地安全策略，如下所示： <ul style="list-style-type: none"><li>• 找到条目 Domain Member:Digitally encrypt or sign secure channel data (always)，然后将其禁用。缺省情况下，此选项是启用的。</li><li>• 找到条目 Domain member:Disable machine account password changes，然后将其禁用。缺省情况下，此选项是启用的。</li></ul>

- 找到条目 `Domain member:Require strong (Windows 2000 or later) session key`，然后将其禁用。缺省情况下，此选项是启用的。

运行 `regedit` 命令来编辑或验证下列注册表条目：

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netlogon\parameters\RequireSignOrSeal`="dword:00000000"（缺省值 = 0）
- `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\LMcompatibilitylevel` = 0（缺省值 = 0）
- `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\RestrictAnonymous` = 0（缺省值 = 0）
- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System\CompatibleRUPSecurity`（将 `DWORD` 值设置为 1）。

**问题** 更改 HP CIFS Server 的域后，用户需要很长时间才能登录。

**解决办法** 删除 `/var/opt/samba/locks` 目录中的 `.tdb` 文件。

**问题** 从 Windows 终端服务和 UNIX 上同时访问同一个文件可能导致该文件损坏，即使已经启用了共享模式锁定。

**解决办法** 请直接从 Windows 客户端访问该文件，而不通过 Windows 终端服务。

**问题** 如果使用完整路径指定符号链接，则在使用 UNIX 扩展创建该符号链接时会失败。

**解决办法** 请转到要放置符号链接的目录，然后使用相对路径创建该链接。

**问题** 一旦在 `smb.conf` 文件中设置了 `wins server` 选项，便不能使用 SWAT 实用程序将其清除。

**解决办法** 手动编辑 `smb.conf` 文件以删除 `wins server` 条目。

**问题** 与 Samba 建立连接后，运行 `smbstatus` 的非超级用户可能收到下列错误：

```
"/var/opt/samba/locks/connections.tdb not initialized.  
This is normal if an SMB client has never connected to your  
server."
```

- 解决办法**                    当前版本的 smbstatus 需要对  
/var/opt/samba/locks/connections.tdb、  
/var/opt/samba/locks/locking.tdb 和  
/var/opt/samba/locks/brlock.tdb 文件具有写权限。  
要解决此问题，请确保尝试运行 smbstatus 的所有用户都获得了对这些文件的写权限。
- 问题**                        通过设置 log file (smb.conf 变量) 更改调试日志文件的目标之后，nmbd 日志文件未保存在日志文件目录中。
- 解决办法**                    一种解决办法是，启动 CIFS Server 时，在命令行上输入以下命令来指定 nmbd 日志文件的存放位置：  
  
nmbd -l "/new/log/file/path/logfilename" -D  
  
如果希望一劳永逸地解决此问题，则请编辑 /opt/samba/bin/start smb。  
  
1. 将 \${samba\_path}/nmbd -D  
   更改为  
   \$ {samba\_path}/nmbd-l/new/log/file/path/logfile -D
- 问题**                        HP CIFS Server 会创建一个 smbnull 用户，并将其设置为 guest 身份，但该用户没有 home 目录，也不需要该目录。而 HP-UX 上的口令或组文件检查工具 pwck 始终假定 /etc/passwd 文件中的每个条目都有其自己的登录目录。如果没有相应的条目，pwck 命令就会报错，并显示下列检查结果：  
  
smbnull:\*:101:101:DO NOT USE OR DELETE - needed by  
Samba:/home/smbnull:/sbin/sh Login directory not found  
  
出于同样的原因，pwck 命令还会报告 HP CIFS Server 中的计算机信任帐户出现问题。
- 问题**                        在未安装签名和封印修补软件的 Windows XP 计算机上更改 smbpasswd 文件中存储的口令将使相关用户的口令遭到损坏。此时，该口令必须由管理员重新设置。
- 问题**                        当使用终端服务器客户端访问 CIFS Server 上的共享时，该终端服务器上的所有客户端将通过一个虚拟连接进行连接，并由 CIFS Server 上的一个 SMBD 进程提供服务。这样就会导致诸多问题，包括某个进程打开的文件太多、锁定太多以及客户端性能下降，原因是所有客户端都共享一个 SMBD 进程。

## 解决办法

对于 Windows NT，可以将一个注册表参数 `MultipleUsersOnConnection` 设置为 1，这样就会强制每个终端服务器客户端自行处理各自的连接，从而使每个客户端获得一个单独的 `SMBD` 进程。

对于 Windows 2000 终端服务，Microsoft 提供了一个修补程序 818528。您可以应用此修补程序，并设置下列值：

```
Subkey:  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxSmb\ /  
Parameters  
Type:REG_DWORD  
Entry: MultiUserEnabled  
Value: 1
```

---

## 注释

在 MS 文章 818528 中引用的修补程序仅适用于 Windows 2000，请不要在 Windows 2003 上安装它。

---

有关此修补程序的详细信息，请参阅 Microsoft 文章 818528，此文章位于：  
<http://support.microsoft.com/default.aspx?kbid=818528>

## HP CIFS Server A.01.11.04 安装要求

### HP CIFS Server 安装要求

HP CIFS Server 大约需要 43 MB 的磁盘空间才能安装在 HP-UX 11.0 或 11.11 PA 计算机上，大约需要 61 MB 的磁盘空间才能安装在 HP-UX 11.23 IA 计算机上。HP CIFS Server 由下列组件组成：

- CIFS Server 源代码文件（HP-UX 11.00 或 11.11）— 14 MB
- CIFS Server 文件和打印服务（HP-UX 11.00 或 11.11）— 29 MB
- CIFS Server 源代码文件 (HP-UX 11.23) — 16 MB
- CIFS Server 文件和打印服务 (HP-UX 11.23) — 45 MB

### HP-UX 内存和磁盘要求

32 位和 64 位 HP-UX 11.00/11.11 系统只需 64 MB RAM 和 1 GB 的磁盘空间就可以进行引导。64 位 HP-UX 11.23 系统只需 1 GB RAM 和 2 GB 的磁盘空间就可以进行引导。为便于日后进行系统扩展和维护，HP 建议的最低内存和磁盘空间要求如下：

- HP-UX 11.00 (11.11) 32 位 — 128 MB RAM — 1-2 GB 磁盘空间
- HP-UX 11.00 (11.11) 64 位 — 512 MB RAM — 2-3 GB 磁盘空间
- HP-UX 11.23 64 位 — 1 GB RAM（对于每个 CPU）— 2-8.5 GB 磁盘空间

## 软件支持的语言

目前，HP CIFS Server 为以下内容提供了德语 (ISO 8859-1) 和日语 Shift-JIS 语言环境支持：

- 文件名和内容
- 目录名和内容
- 打印作业

类似 `smbstatus` 和 `SWAT` 的管理实用程序未经过国际化。国际化的重点是用户级，而非管理级。

虽然目前完全可以支持其他语言环境，但 HP 只用德语 (ISO 8859-1) 和日语 Shift-JIS 语言环境对此发行版的 HP CIFS Server 进行了测试。