

HP CIFS Server 2.2j 发行说明 A.01.11.02

HP-UX 11.0、11i v1 和 v2



i n v e n t

生产部件号: B8725-90072

E0704

© 版权所有 2004 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 © 1983-2004 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。

关于本文档

本文档介绍有关自本发行版以来最新 HP CIFS Server 产品的技术信息。本文档以及以前发行的文档均可从 <http://www.docs.hp.com> 上获得联机版本。

目标读者

本文档面向那些对 HP CIFS Server 产品已经比较熟悉的用户。有关 HP CIFS Server 的详细信息，请参考 <http://www.docs.hp.com> 上有关 HP CIFS Server 的联机文档。

本版本中的新增内容及修订内容

本版本记录了 HP CIFS Server 2.2i A.01.11.01 中发生的下列变化：

- 支持与 LDAP 目录服务器的安全套接字层 (SSL) 连接
- 支持 smb.conf 文件中的新配置参数 ldap ssl，以启用 SSL 功能
- 对于 /opt/samba/LDAP/smbldap-tools 目录中的所有 LDAP 管理工具，支持两个新选项 -z 和 -S

印刷字体约定

表 1

文档约定

信息类型	字体	示例
表示显示器上输出的内容、程序和（或）脚本代码以及命令名称或参数。	Monotype	> user logged in.
第一次定义的名词和强调的内容用 黑体 表示。	粗体	相关文档

版本说明

表 2

版本说明详细信息

文档的生产部件号	支持的操作系统	支持的产品版本	出版日期
B8725-90045	11.0、 11.11、 11.22	A.01.09.02	2003 年 6 月
B8725-90050	11.0、 11.11、 11.22	A.01.09.04	2003 年 6 月
B8725-90051	11.0、 11.11、 11.22	A.01.09.05	2003 年 5 月
B8725-90058	11.0、 11.11、 11.22、 11.23	A.01.10	2003 年 12 月
B8725-90062	11.0、 11.11、 11.23	A.01.11	2004 年 2 月
B8725-90072	11.0、 11.11、 11.23	A.01.11.01	2004 年 6 月

HP 欢迎您提出宝贵的意见和建议

HP 欢迎您就本文档提出宝贵的意见和建议。我们真正承诺能够提供可满足您的需要的文档。

请将您的意见和建议发送至：netinfo_feedback@cup.hp.com

请在您的电子邮件中注明文档标题、生产部件号、任何意见和建议、在文档中发现的错误或者为改进本文档质量而提出的建议。另请注明我们处理得体的地方，以便可以在其他文档中利用。

第 1 章 HP CIFS Server 发行说明

声明

本文档包含有关 HP CIFS Server A.01.11.02 发行版中提供的新功能和缺陷修复程序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.01.11.02

- 此版本的 HP CIFS Server 是基于 Samba 2.2.10 的一个修复版本。
- 为一个潜在的安全漏洞提供了修复方法，该漏洞可能会使 HP CIFS Server A.01.11.01 及以前的版本在使用 hash 散列函数时出现缓冲区溢出问题。此问题可能会被利用，从而可以远程获得超级用户访问权限。有关详细信息，请参考 CR JAGaf33614。
- 此版本的 CIFS Server 解决了自 A.01.11.01 版以来解决的问题。有关详细信息，请参考第 7 页上的“HP CIFS Server A.01.11.02 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

在以前的发行版中，已经支持将不同版本的 CIFS Server 中的二进制文件存放在 `/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，该方法会使此发行版附带的二进制文件以外的任何二进制文件在使用时失去安全性。必须使用 `swinstall` 实用程序正式安装 CIFS Server 的不同版本，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，它可能是功能版本，也可能是修复版本。

功能版本包括新功能和（或）新的 Samba 源版本。基本产品修订号 (A.xx.xx) 依次递增；不使用修复后缀编号。

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；只有修复后缀编号 (A.xx.xx.FF) 依次递增。

HP CIFS Server A.01.11.02 中的修复方法

HP CIFS Server A.01.11.02 提供了下列修复方法：

潜在安全漏洞
(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。

最新版本中的功能及修复方法

HP CIFS Server A.01.11.01 最新变化

SSL 功能支持

- 在 HP CIFS Server 中启用 LDAP 上的 SSL 支持

HP CIFS Server 提供了安全套接字层 (SSL) 支持，以使 CIFS 服务器与启用了 SSL 的 LDAP 目录服务器之间进行安全通信。

现在可以配置 `smb.conf` 文件中的 `ldap ssl` 参数来启用安全套接字层 (SSL) 支持。通过 SSL 支持功能，HP CIFS Server 允许您访问启用了 SSL 的 LDAP 目录，以保护网络口令，并确保机密性及 CIFS 服务器与启用了 SSL 的 LDAP 目录服务器之间的数据完整性。

有关如何安装和配置 Netscape Directory Server、LDAP-UX Client Services 和 HP CIFS Server 以启用 LDAP 上的 SSL 通信的详细信息，请参考 <http://www.docs.hp.com> 上的《HP CIFS Server 2.2i Administrator's Guide》中的“LDAP Integration Support”一章。

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 不支持 Microsoft Active Directory Services (ADS) 配置。

用于 SSL 支持功能 的新增配置参数

- LDAP SSL

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 LDAP 管理
工具的新选项

- Samba LDAP 工具

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

<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，请参考 <http://www.docs.hp.com> 上的《HP CIFS Server 2.2i Administrator's Guide》中的“LDAP management Tools”一节。

注释

您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` 选项来使用 `/etc/opt/samba/smb.conf` 文件中的 LDAP 配置参数。

如果在运行 LDAP 管理工具时指定 `-s` 选项，则会使用 `/etc/opt/samba/smb.conf` 文件中的配置值。如果不指定 `-s` 选项，LDAP 管理工具就会使用 `/opt/samba/LDAP/smbldap-tools/smbldap_conf.pm` 文件中指定的 LDAP 配置值。

提高性能

- 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；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。

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连接到 %U 共享（使用 runas 或通过终端服务器或 Citrix Metaframe 从单个连接上多路复用）时，同一台计算机上使用“runas”工具或终端服务器或 citrix metaframe 的客户将无法访问由某些用户的类似 %U 定义的共享，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。 |

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 进行配置以使用 SSL。

在启用 LDAP 的 SSL 通信之前，必须正确设置 CA（Certification Authority，证书颁发机构）服务器。

以下内容总结了在 HP CIFS Server 中配置和启用 SSL 支持功能时所需的基本步骤。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，使其信任此 Certification Authority (CA) 证书。

有关详细说明，请参阅《Netscape Directory Server 6.1 Administrator's Guide》中的“Managing SSL”一章内的“Obtaining and Installing Server Certificates”一节，该手册位于 <http://docs.hp.com> 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》中的“Managing SSL”一章内的“Activating SSL”一节，该手册位于 <http://docs.hp.com> 上。

- 第 3 步 .** 配置管理服务器，使其能够连接到启用了 SSL 的目录服务器。

有关配置管理服务器以连接到启用了 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> 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 客户端上设置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。

如果使用 Netscape Communicator 4.75 下载 Certificate Authority 证书，则证书数据库文件 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，需要创建符号链接 `/etc/opt/ldapux/cert7.db` 以指向 `cert7.db`，并创建符号链接 `/etc/opt/ldapux/key3.db` 以指向 `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》中的“Installing LDAP-UX Client Services”一章内的“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` 程序来在 LDAP-UX 客户端服务上启用 SSL 的详细说明，请参阅《LDAP-UX Client Services B.03.20 Administrator's Guide》中的“Installing LDAP-UX Client Services”一章内的“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，请按如下说明修改 `/etc/opt/ldapux/ldapux_profile` 中的 `authenticationMethod` 和 `preferredServerList` 属性：

- 修改 `authenticationMethod` 属性，以便在原身份验证方法 `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，以便将常规的 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**。该配置选项位于 `/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 Windows NT/XP/2000 打印机驱动程序新的支持功能，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 1 MB 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。 相关缺陷： 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">• 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。• 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。

- 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/startsmmb`。
 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 Q818528。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 不要在 Windows 2003 上安装此修补程序 Q818528。此修补程序仅适用于 Windows 2000。

有关此修补程序的详细信息，请参阅 Microsoft Q818528 文章，此文章位于：
<http://support.microsoft.com/default.aspx?kbid=818528>

HP CIFS Server A.01.11.02 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。