

HP CIFS Server Release Notes Version A.03.01

HP-UX 11i v2 and HP-UX 11i v3



© Copyright 2011 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

HP CIFS Server is derived from the Open Source Samba product and is subject to the GPL license.

Trademark Acknowledgments

Microsoft®, Windows®, Windows NT®, Windows Server®, Windows XP®, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Contents

Announcement.....	4
Changes in HP CIFS server A.03.01	4
Product revision number	4
What's new in HP CIFS server A.03.01	4
Fixes in HP CIFS server A.03.01	4
Installation and patch requirements for HP CIFS server A.03.01	5
Operating system requirements.....	5
HP CIFS server installation requirements.....	5
HP-UX memory and disk requirements.....	5
Kerberos product requirements.....	5
The smb.conf parameters.....	6
Known issues and workarounds.....	7

Announcement

This document describes HP CIFS Server A.03.01 changes, defect fixes, and other information. HP CIFS Server A.03.01 is supported on HP-UX 11i v2 and HP-UX 11i v3.

Changes in HP CIFS server A.03.01

- HP CIFS Server A.03.01 is a feature release based on Samba 3.4.3, with many defect fixes and applicable security fixes. HP CIFS Server now supports Windows Server 2008 and 2008R2, Windows Vista, and Windows 7 operating systems. For more information, see [“Fixes in HP CIFS server A.03.01” \(page 4\)](#)
- The Dynamic DNS update option is available in HP CIFS Server A.02.04.01 and later. For details, see [“What's new in HP CIFS server A.03.01 ” \(page 4\)](#).

△ CAUTION: HP only supports HP CIFS Server binaries as delivered by HP. You must use the `swinstall` utility to formally install versions of HP CIFS Server. Do not copy HP CIFS Server binaries of different revisions between systems into the `/opt/samba/bin` subdirectory.

NOTE: HP CIFS Server A.03.01 no longer provides support for CFSM.

Product revision number

New versions of the HP CIFS Server are identified by the product revision number (A.xx.xx.FF), and are either a feature or fix release.

Feature releases include new functionality and a new Samba source version. The base product revision number (A.xx.xx) is incremented. A fix suffix number is not used.

Fix releases include only those changes required to correct specific defects. The base product revision number (A.xx.xx) is unchanged. Only the fix suffix number (A.xx.xx.FF) is incremented.

What's new in HP CIFS server A.03.01

HP CIFS Server A.03.01 supports:

- Windows Server 2008R2 and Windows 7 operating systems
- Inter-domain trust relationships with Windows 2008 and 2008R2 domains
- Windows Vista clients authenticating through Kerberos

Fixes in HP CIFS server A.03.01

- CIFS Server `rpc.quotad` is not enabled by default. This setting prevents CIFS from accessing quotas.
QXCR1000994951
This issue is fixed.
- The SWAT Status page displays incorrect information for Open Files.
QXCR1000996025
This issue is fixed.
- The old Kerberos fileset is still used. You cannot use the `>=` operator.
QXCR1001014701, QXCR1001029109
This issue is resolved with warning messages.

- Investigation of security bulletin CVE-2010-2063 is completed.
QXCR1001051340
This issue is fixed.
- A.02.04.01 ships on 11.11 with libuuid.sl, a PA-RISC 2.0 lib.
QXCR1001040672
This issue is fixed.
- An error occurs when installing version A.02.04.01 on top of existing version A.02.04a
QXCR1001011947
Use `allow_downdate=true` as a workaround.
- The `WTEC_Support_Tools` directory is missing in versions A.02.04 and later.
QXCR1001011182
This issue is fixed.
- The `samba_setup` incorrectly adds * to password server line automatically.
QXCR1000988896
This issue is fixed.
- Multiple `smbds` are spawned for the same client connection, which causes resource issues
QXCR1000963520
This issue is fixed.

Installation and patch requirements for HP CIFS server A.03.01

Operating system requirements

HP CIFS Server A.03.01 can be installed on HP 9000 or HP Integrity systems running HP-UX 11i v2 and HP-UX 11i v3.

HP CIFS server installation requirements

The HP CIFS Server requires approximately 210 MB of disk space for installation on an HP-UX 11i v2 system and 215 MB of disk space for installation on an HP-UX 11i v3 system. The HP CIFS Server source code files requires approximately 36 MB of disk space.

HP-UX memory and disk requirements

The minimum requirements of 64-bit HP-UX 11i v2 and HP-UX 11i v3 systems are 1 GB RAM and 2 GB disk space. HP recommends the following minimum memory and disk requirements to enable upgrade and maintenance:

- HP-UX 11i v2, HP-UX 11i v3 64-bit – 1 GB RAM for each CPU – 2-8.5 GB disk

Kerberos product requirements

Kerberos v5 Client version D 1.6.2 or later is required to support HP CIFS Server integration with Windows 2003 or later ADS Domain Controller (DC) on HP-UX 11i v2 systems.

Kerberos v5 Client version E 1.6.2 or later is required to support HP CIFS Server integration with Windows 2003 or later ADS Domain Controller (DC) on HP-UX 11i v3 systems.

You can download the Kerberos v5 Client (`KRB5CLIENT`) product from the Software Depot website:

<http://www.hp.com/go/softwaredepot>

In the search field, enter KRB5CLIENT.

The smb.conf parameters

Parameter Name	Description	Default
kerberos method	New	secrets only
map untrusted to domain	New	No
debug class	New	No
client ldap sasl wrapping	New	plain
cups connection timeout	New	30
ldap ssl ads	New	No
ldap connection timeout	New	2
state directory	New	/var/opt/samba/locks
cache directory	New	/var/opt/samba/locks
registry shares	New	No
winbind reconnect delay	New	30
winbind expand groups	New	1
winbind rpc only	New	No
access based share enum	New	No
passdb backend	Changed default	tddb
lanman auth	Changed default	No
client lanman auth	Changed default	No
client plaintext auth	Changed default	No
max open files	Changed default	2048
max stat cache size	Changed default	256
preferred master	Changed default	No
ldap ssl	Modified	start tls
idmap backend	Changed default	tdb
idmap cache time	Changed default	604800
allocation roundup size	Modified	1048576
kernel oplocks	Modified	Yes
use kerberos keytab	Removed	
read bmpx	Removed	
mangled map	Removed	
kernel share modes	Removed	

Known issues and workarounds

Issue

The `wbinfo` command fails sometimes when a large number of users or groups (~32k users or groups) are in a trusted domain.

Workaround

No known workaround exists.

Issue

The `wbinfo` command hangs when the trusted domain is unavailable.

Workaround

No known workaround exists.

Issue

If the `libnss_wins` NSS library is used, then the `sh_load()` error message is returned.

Workaround

The `libnss_wins` NSS library is not tested. Therefore, it must not be used. The library will be removed in the future versions of the product.

Issue

After the `wins server` option is set in the `smb.conf` file, it cannot be cleared using SWAT utility

Workaround

Manually edit the `smb.conf` file to remove the `wins server` entry.

Issue

A non-root user running `smbstatus` might receive the following errors when HP CIFS Server is not started and `tdb` files have not been initialized:

```
could not open file /var/opt/samba/locks/sessionid.tdb: No such files  
or directory
```

```
Error: Failed to initialize locking database
```

Workaround

The current version of `smbstatus` does not allow a normal user to initialize `tdb` files. A normal user must perform `smbstatus` after HP CIFS Server is started by root, or `tdb` files have been initialized.

Issue

Changing the password stored in the `smbpasswd` file from a Windows XP machine without the sign-and-seal patch fails and corrupts the user's password.

Workaround

The administrator must reset the password.

Issue

When you use terminal server clients to access shares on a CIFS server, all of the clients from that terminal server connect over a single virtual connection and are serviced by a single SMBD process on the CIFS Server. These actions might lead to a number of issues, including too many files open by a process, too many locks, and performance degradation for the clients, since the clients share a single SMBD process.

Workaround

For the Windows NT, you can set a registry parameter, `MultipleUsersOnConnection`, to 1, which forces each terminal server client to negotiate its own connection, so that each client receives a separate SMBD process. For the Windows 2000 terminal services, Microsoft provides a hotfix, Q818528. You can apply this hotfix, and then set the following values:

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

NOTE: Do not install the Q818528 hotfix on a system running Windows 2003. This hotfix only applies to Windows 2000.

For more information, see the Microsoft Q818528 article:
<http://support.microsoft.com/default.aspx?kbid=818528>

Issue

The The file may have been changed error message appears when you save an Excel file to Samba. The error message also provides choices to either save a copy or overwrite changes.

Workaround

When prompted, select `overwrite changes` otherwise the file must be saved under a different name.

To avoid this error, change the registry as described in the Microsoft knowledge base article at <http://support.microsoft.com/default.aspx?kbid=324491>

The Samba community also addressed the issue and has further characterized it on the Bugzilla webpage at https://bugzilla.samba.org/show_bug.cgi?id=1094

Issue

Because of increased Windows security requirements, profile storing might fail if adequate authority has not been configured for roaming profiles.

Workaround

Set `profile acls = yes` for the profile share used for the user profile files. Do not set `profile acls = yes` on normal shares because this causes the incorrect ownership of the files created on those shares.

Issue

No 64 bit Windows XP clients can connect to the CIFS Server when configured with `smb.conf` parameter `security=server`. Other Windows clients, including the 64-bit version of Windows XP clients by default, might also fail to connect if they have the local policy for LAN Manager set to `Send NTLM response only`.

Workaround

Using the Administrative Tool on each failing client:

1. Select Local Security Policy.
2. Select Local Policies.
3. Select Security Options.
4. Select Network security: LAN Manager authentication level.
5. Set the authentication level to Send LM & NTLM response or Send LM & NTLM - use NTLMv2 session security if negotiated.

Issue

When using the `smbpasswd` command during the first time you add a Samba user to a new CIFS Server installation, the command might respond with a misleading message as in the following example:

```
./smbpasswd -a user1
```

New SMB password:

Retype new SMB password:

The misleading messages appear as follows:

```
startsmbfilepent_internal: file /var/opt/samba/private/smbpasswd did not exist.  
File successfully created.  
account_policy_get: tdb_fetch_uint32 failed for field 1  
(min password length), returning 0  
account_policy_get: tdb_fetch_uint32 failed for field 2  
(password history), returning 0  
account_policy_get: tdb_fetch_uint32 failed for field 3  
(user must logon to change password), returning 0  
account_policy_get: tdb_fetch_uint32 failed for field 4  
(maximum password age), returning 0  
account_policy_get: tdb_fetch_uint32 failed for field 5  
(minimum password age), returning 0  
account_policy_get: tdb_fetch_uint32 failed for field 6  
(lockout duration), returning 0  
account_policy_get: tdb_fetch_uint32 failed for field 7  
(reset count minutes), returning 0  
account_policy_get: tdb_fetch_uint32 failed for field 8  
(bad lockout attempt), returning 0  
account_policy_get: tdb_fetch_uint32 failed for field 9  
(disconnect time), returning 0  
account_policy_get: tdb_fetch_uint32 failed for field 10  
(refuse machine password change), returning 0  
Added user user1
```

The user is added correctly, and the misleading messages only appear with the first occurrence of adding a new Samba user.

Workaround

Verify that the user has been added correctly, and ignore the misleading messages.

Issue

The 64-bit Windows XP clients are unable to add a new ACE. Adding an ACE through Windows Explorer File->Properties->Security interface to a file or directory from a Windows XP Professional 64-bit edition results in the following error message:

```
This program cannot open the required dialog box because the specified  
computer <samba servername> cannot be determined to belong to a domain.  
Try again.
```

Workaround

No workaround exists.

Issue

Some Windows 2000/2003 Domain trusts might not be recognized by HP CIFS Server, including some intra/inter-forest trusts.

Workaround

When required to accommodate the intra/inter-forest trusts that HP CIFS Member Servers might be exposed to in a forest, shortcut trusts can be explicitly created. HP CIFS PDCs support external trusts, which can be sufficient for Samba and Windows inter-domain trust relationships. For more information about Windows 2000/2003 trusts, see the MS TechNet documentation at <http://technet.microsoft.com>.

Issue

An existing POSIX machine account must already exist before you add the corresponding Samba machine account and `thesambaSamAccount` information required for HP CIFS Server machine account authentication. You can use the `useradd` command to add the POSIX machine account with `$` at the end to the `/etc/passwd` file for HP CIFS Server to recognize it as a machine account. If the POSIX machine account does not exist, running the `pwck` command displays the following error message:

```
1 Bad character(s) in logname
```

Workaround

No workaround exists.

Issue

Use the `useradd` command to add the POSIX machine account with a `$` at the end to the `/etc/passwd` file for HP CIFS Server to recognize it as a machine account. The `pwck` command might display the following error message:

```
Login directory not found
```

The above error indicates that the home directory does not exist.

Workaround

Use the `-m` option with `useradd` when adding a POSIX machine account. If the home directory does not exist for the new account, it is created.

Issue

The delete operation on a large number of files from a directory takes a long time to complete.

Workaround

Close Windows Explorer after the delete process is started. Beginning with A.02.03.01, another workaround is to set the `change_notify_timeout smb.conf` parameter to 0. When set to 0, change notification messages are not sent and long delays do not occur. Clients must initiate updates to view changes (by pressing F5) that might have occurred on the file share. Beginning with A.02.03.01, the `change_notify_timeout` parameter moves from a global to share level parameter. The `change_notify_timeout` parameter is not available starting from A.02.04.