SAMBA Developers Guide

Abstract

Last Update : Fri Oct 10 00:59:58 CEST 2003

This book is a collection of documents that might be useful for people developing samba or those interested in doing so. It's nothing more than a collection of documents written by samba developers about the internals of various parts of samba and the SMB protocol. It's still (and will always

2.2.3.12 OBJ_ATTR (object attributes) xxiii

2.3.6 LSA Open Policy xliii
2.3.6.1 Request xliii
2.3.6.2 Response xliv
2.3.7 LSA Query Info Policy xliv
2.3.7.1

4.5.1 dbgtext() lxxii
4.5.2 dbghdr() lxxiii
4.5.3 format_debug_text() lxxiii

Chapter 5 SAMBA INTERNALS lxxiv

Part I

This is enforced in Unix as non-root users can't open a socket for listening on port numbers less than 1000.

Most PC based SMB clients (such as WfWg and WinNT) don't follow this convention completely. The main culprit is the netbios nameserving on udp port 137. Name query requests come from a source port of 137. This is a problem when you combine it with the common firewalling technique of

level" functions. It supports only 8 (so far) of the SMBtrans sub-functions. Even NT doesn't support them all.

Samba currently supports up to the "NT LM 0.12" protocol, which is the one preferred by Win95 and WinNT3.5. Luckily this protocol level has a "capabilities" field which specifies which super-duper new-fangled options4(th)1(e)]TJ0-13.5ihe

issa prbpihihes2383Shp(c)-1icaptions- ispenp(c)-1,l4(th)1(e)]TJ0-13.b(u)1rt thepenpknromn, ar
protocol SMB Command(e)-1rrese
neo specicaptions-ups-eihes2672oldrpenocnses2672bpthe

UINT8[6] 6 bytes for domain SID - Identifier Authority.

UINT16[n_subauths] domain SID sub-authorities

Note: the domain SID is documented elsewhere.

2.2.3.6 STR (string)

STR (string) is a char[] : a null-terminated string of ascii characters.

2.2.3.7 UNIHDR (unicode string header)

UINT16 length of unicode string

UINT16 max length of unicode string

UINT32 4 - undoc0e1mented.

Section

2.2.3.13 POL_HND (LSA policy handle)

char[20] policy handle

2.2.3.14 DOM_

Section 2.2. Notes and Structures

2.2.3.19 CLNT_INFO2 (server, client structure, client credentials)

Section

```
switch (switch_value)
case 1:
{
    ID_INFO_1     id_info_1;
}
```

2.2.3.23 GID (group id info)

UINT32 group id

UINT32 user attributes (only used by NT 3.1 and 3.51)

2.2.3.24 DOM

Section 2.2. Notes and Structures

Section

UINT8 flags reply same as request (0x00 for Bind, 0x03 for Request)

UINT32 representation

UINT16 maxrsize

2.3.2.8 RPC_ResNorm RW

UINT32 allochint # size of the stub data in bytes

UINT16 prescontext # presentation context identifier (same as request)

UINT8 cancelcount # cancel count? (0x0)

UINT8 reserved # 0 - one byte padding

* stub USE TvPacket # the remainder of the reply

2.3.3 Tail

The end of eub 3(NT)-33LSTThaad3(NETLOGd)1ONTd[(3(n50s)-)1dTd[(3(1(e))-3527

Note: The RPC_ResBind response member secondaddr contains the name of what is presumed to be the service behind the RPC pipe. The mapping identified so far is:

initial SMBopenX request:

Establish a connection to the IPC$ share (SMBtconX). use encrypted passwords.
Open an RPC Pipe with the name "\\PIPE\\lsarpc". Store the file handle.
Using the file handle, send a Set Named Pipe Handle state to 0x4300.
Send an LSA Open Policy request. Store the Policy Handle.
Using the Policy Handle, send LSA Query Info Policy requests, etc.

OBJ_ATTR object attributes

UINT32 1 - desired access

```
}

return    0 - indicates success
```

2.3.8 LSA Enumerate Trusted Domains

2.3.8.1 Request

no extra data

2.3.8.2 Response

UINT32 0 - enumeration context

UINT32 0 - entries read

UINT32 0 - trust information

return 0x8000 001a - ”no trusted domains” success code

VOID* undocumented domain SID buffer pointer

VOID* undocumented domain name buffer pointer

NAME[num_entries] names to be looked up.

char[] undocumented bytes - falsely translated SID structure?

2.3.12.2 Response

DOM_REF domain reference response

UINT32 num_entries (listed above)

VOID* undocumented buffer pointer

UINT32 num_entries (listed above)

```
}
```

2.6.1 Net Share Enum

Note: share level and switch value in the response are presumably the same as those in the request.

Note: cifsrap2.txt (section 5) may be of limited assistance here.

2.6.1.1 Request

VOID* pointer (to server name?)

UNISTR2 server name

UINT8[] padding to get unicode string 4-byte aligned with the start of the SMB header.

UINT32

SHARE_INFO_1_CTR share info (only added if share info ptr is non-zero)

return 0 - indicates success

2.6.2 Net Server Get Info

Note: level is the same value as in the request.

2.6.2.1 Request

UNISTR2 server name

UINT32 switch level

2.6.2.2 Response

UINT32 switch level

VOID* pointer to SERVER_INFO_101

SERVER_INFO_101 server info (only added if server info ptr is non-zero)

return 0 - indicates success

E(K,D) DES ECB encryption of 8 byte data D using 7 byte key K

lmowf() Lan man hash

ntowf()

(Logon IDs) S-1-5-5-X-Y

lxiii

(NT non-unique IDs)

Chapter 3

SAMBA ARCHITECTURE

3.1 Introduction

we would have to code nmbd both with and without threads, and as the real aim of threads is to make the code clearer we would not have gained anything. (it is a myth that threads make things faster. threading is like recursion, it can make things clear but the same thing can always be done faster by some other method)

Chris tried to spec out a general design that would abstract threading vs separate processes (vs other methods?) and make them accessible through

Chapter 4

THE SAMBA DEBUG SYSTEM

4.1 New Output Syntax4.=etsyntMofxaxdMd1gxNewe52S1(A4lt)-34(sis)-343(repres)-1be

```
>debugfile< :== { >debugmsg< }

>debugmsg<  :== >debughdr< '\n' >debugtext<

>debughdr<  :== '[' TIME ',' LEVEL ']' FILE ':' [FUNCTION] '(' LINE ')'

>debugtext< :== { >debugline< }

>debugline< :== TEXT '\n'
```

Section

6. all lp_

5.3.7 IVALS(buf,pos)

returns the value of the signed 32 bit little-endian integer at offset pos within buffer buf.

5.3.8 SSVAL(buf,pos,val)

sets the unsigned short (16 bit) little-endian integer at offset pos within buffer buf to value val.

5.3.9 SIVAL(buf,pos,val)

sets the unsigned 32 bit little-endian integer at offset pos within buffer buf to the value val.

Section

Chapter 6

CODING SUGGESTIONS

So you want to add code to Samba ...

14. Try to avoid using in/out parameters (functions that return data which

Chapter 8

MODULES

8.1 Advantages

The new modules system has the following advantages:

Transparent loading of static and shared modules (no need for a subsystem to know about mod

Note

There currently also is a configure.in command called SMB_MODULE_

This struct contains the function and handle pointers for all operations.

Section

10.1.2 Possible VFS operation layers

These values are used by the VFS subsystem when building the conn->

layer the vfs_op_

```
NULL,           /* fsync */
example_stat,       /* stat  */
example_fstat,      /* fstat */
example_lstat,      /* lstat */
NULL,           /* unlink */
NULL,           /* chmod */
NULL,           /* fchmod */
NULL,           /* chown */
NULL,           /* fchown */
NULL,           /* chdir */
NULL,           /* getwd */
NULL,           /* utime */
NULL,           /* ftruncate */
NULL,           /* lock */
NULL,           /* symlink */
NULL,           /* readlink */
NULL,           /* link */
NULL,           /* mknod */
NULL,           /* realpath */
NULL,           /* fget_nt_acl */
NULL,           /* get_nt_acl */
NULL,           /* fset_nt_acl */
NULL,           /* set_nt_acl */

NULL,           /* chmod_acl */
NULL,           /* fchmod_acl */
```

9.

```
         * we don't need to specify a free_function here because
         * we use the connection TALLOC context.
         * (return -1 if something failed.)
         */
        VFS_HANDLE_SET_DATA(handle, data, NULL, strudAs2.



*/
```

```
    DEBUG(0,("some_string: %s\n",data->some_string));

    return SMB_VFS_NEXT_CLOSE(handle, fsp, fd);
}
```

11. To make it easy to build 3rd party modules it would be usefull to provide configure.in, (configure), install.sh and Makefile.in with the module. (Take a look at the example in examples/VFS.)

    The configure script accepts `--with-samba-source` to specify the path to the samba source tree. It also accept `--enable-developer` which lets the compiler give you more warnings.

    The idea is that you can extend this `configure.in` and `Makefile.in` scripts for your module.

	`./configure --enable-developer ...` `make`
12. Compiling & Testing...	Try to fix all compiler warnings `make` Testing, Testing, Testing ...

10.4 Some Notes

10.4.1 Implement TRANSPARENT functions

Avoid writing functions like this:

```
static int example_close(vfs_handle_struct *handle, files_struct *fsp, int fd)
{
```

Section

Chapter 12

a technical requirement.

```
[global]
   wins server = 192.168.1.2:eth0 192.168.1.3:eth0 192.168.2.2:eth1
```

Using this configuration, nmbd would attempt to register the server's Net-

When a client (LanManager, Windows for WorkGroups, Windows 95 or

Section

Part IV

Debugging and tracing

Chapter 14

TRACING SAMBA SYSTEM CALLS

```
[pid 28268] open("/dev/null", O_WRONLY) = -1 EACCES (Permission denied)
```

The process is trying to first open `/dev/null` read-write then read-only. Both fail. This means `/dev/null` has incorrect permissions.

- a set of CUPS specific functions (this is only enabled if the CUPS

```
   fstring queuename; /* service number of printer for this job */
   NT_DEVICEMODE *nt_devmode;
};
```

The current manifestation of the printjob structure contains a field for the UNIX job id returned from the "lpq command" and a Windows job ID (32-bit bounded by PRINT_MAX_JOBID). When a print job is returned by the "lpq command" that does not match an existing job in the queue's TDB, a 32-bit job ID above the <*vance doesn't know what word is missing here*> is generating by adding UNIX_JOB_START to the id reported by lpq.

Section

cxxx

request back to the client first. However a request of this nature from the client is often an indication that the previous notification event was not marshalled correctly by the server or a piece of data was wrong.

S: The server closes the internal change notification handle

Chapter 16

NOTES TO PACKAGERS

16.1 Versioning

Please, please update the version number in