WINBIND TRACING

SAMBAXP 2023

Pavel Filipenský

Senior Software Engineer | Red Hat | Samba Team

ABOUT PAVEL

From NFS to Samba

Samba maintainer at Red Hat since 2021

Samba Core Team member since 2022

WHAT ARE WINBIND LOG FILES

```
$ ls -1 /var/log/samba/log.w*
log.winbindd
log.winbindd-idmap
log.wb-ADDOMAIN
log.wb-BUILTIN
log.wb-LOCALADMEMBER
```

```
[2023/05/04 16:20:51.998105,  3, pid=1153814, effective(0, 0), real(0, 0), class=winbind] ../../source3/winbindd/winbindd.c:502(process_request_send)
  process_request_send: [nss_winbind (1153856)] Handling async request: GETPWNAM
[2023/05/04 16:20:51.998111,  3, pid=1153814, effective(0, 0), real(0, 0), class=winbind] ../../source3/winbindd/winbindd_getpwnam.c:59(winbindd_getpwnam_send)
  [nss_winbind (1153856)] Winbind external command GETPWNAM start.
  Query username 'nt authority/'.
[2023/05/04 16:20:51.998118,  5, pid=1153814, effective(0, 0), real(0, 0), class=winbind] ../../source3/winbindd/wb_lookupname.c:52(wb_lookupname_send)
  WB command lookupname start.
  Search namespace 'nt authority' and domain 'NT AUTHORITY' for name ''.
[2023/05/04 16:20:51.998131,  1, pid=1153814, effective(0, 0), real(0, 0), class=rpc_parse] ../../librpc/ndr/ndr.c:490(ndr_print_function_debug)
       wbint_LookupName: struct wbint_LookupName
          in: struct wbint_LookupName
              domain                   : *
                  domain                   : 'NT AUTHORITY'
              name                     : *
                  name                     : ''
              flags                    : 0x00000008 (8)
[2023/05/04 16:20:51.998166,  1, pid=1153814, effective(0, 0), real(0, 0), class=rpc_parse] ../../librpc/ndr/ndr.c:490(ndr_print_function_debug)
       wbint_InitConnection: struct wbint_InitConnection
          in: struct wbint_InitConnection
              dcname                   : *
                  dcname                   : ''
```

5 STEPS

1. Improved function tracing [samba-4.17]
2. Debug header field traceid [samba-4.17]
3. Debug header field depth [samba-4.18]
4. Flow traces [samba-4.19]
5. Trace parser [samba-4.19]

#1: FUNCTION TRACING

Red Hat customers are asking for better logging of winbind asynchronous calls.

1. Some functions do not log at all
2. log level is not consistent
3. Function input/output should be traced

#1: FUNCTION TRACING

```
D_NOTICE("[%s (%u)] Winbind external command GETPWNAM start.\n"
         "Query username '%s'.\n",
         cli->client_name,
         (unsigned int)cli->pid,
         request->data.username);

D_NOTICE("Winbind external command GETDCNAME end.\n"
          "Got DCNAME '%s'.\n",
          response->data.dc_name);

D_INFO("WB command lookupsid start.\n");
```

```
46 per-file commits:
s3:winbind: Improve logging in wb_sids2xids.c
s3:winbind: Improve logging in wb_query_user_list.c
s3:winbind: Improve logging in wb_queryuser.c
s3:winbind: Improve logging in wb_query_group_list.c
s3:winbind: Improve logging in wb_next_pwent.c
s3:winbind: Improve logging in wb_next_grent.c
...
s3:winbind: Improve logging in winbindd_getpwsid.c
s3:winbind: Improve logging in winbindd_endgrent.c
s3:winbind: Improve logging in winbindd_dsgetdcname.c
s3:winbind: Improve logging in winbindd_getusersids.c
s3:winbind: Improve logging in winbindd_group.c
s3:winbind: Improve logging in wb_xids2sids.c
s3:winbind: Improve logging in winbindd.c
```

#2: DEBUG HEADER FIELD TRACEID

```
[2023/05/04 19:26:58.302837,  1, pid=1072074, effective(0, 0), real(0, 0), class=rpc_parse, traceid=92] ../../source3/
  wbint_LookupName: struct wbint_LookupName
     in: struct wbint_LookupName
            domain                   : 'ADDOMAIN'
            name                     : 'JOE'
         flags                    : 0x00000008 (8)
[2023/05/04 19:26:58.302925,  1, pid=1072074, effective(0, 0), real(0, 0), class=rpc_parse, traceid=90] ../../source3/
  wbint_LookupName: struct wbint_LookupName
     out: struct wbint_LookupName
            type                     : SID_NAME_USER (1)
            sid                      : S-1-5-21-118052468-2300894008-1344842092-1107
         result                   : NT_STATUS_OK
```

```
$ bin/wbinfo --name-to-sid ADDOMAIN/alice
S-1-5-21-118052468-2300894008-1344842092-1107 SID_USER (1)
$ bin/wbinfo --name-to-sid ADDOMAIN/joe
S-1-5-21-118052468-2300894008-1344842092-1110 SID_USER (1)
```

#3: DEBUG HEADER FIELD DEPTH

```
[2023/05/04 11:18:46.353302,  3, pid=1072074, effective(0, 0), real(0, 0), class=winbind, traceid=36, depth=1] ../../source3/winbindd/winbindd_getpw
  [nss_winbind (1072408)] Winbind external command GETPWNAM start.
  Query username 'ADDOMAIN/alice'.
[2023/05/04 11:18:46.353325,  5, pid=1072074, effective(0, 0), real(0, 0), class=winbind, traceid=36, depth=2] ../../source3/winbindd/wb_lookupname.
  WB command lookupname start.
  Search namespace 'ADDOMAIN' and domain 'ADDOMAIN' for name 'alice'.
...
[2023/05/04 11:18:46.354214,  5, pid=1072074, effective(0, 0), real(0, 0), class=winbind, traceid=36, depth=2] ../../source3/winbindd/wb_getpwsid.c:4
  WB command getpwsid start.
  Query user SID S-1-5-21-118052468-2300894008-1344842092-1107.
...
[2023/05/04 11:18:46.354235,  5, pid=1072074, effective(0, 0), real(0, 0), class=winbind, traceid=36, depth=3] ../../source3/winbindd/wb_queryuser.c
  WB command queryuser start.
  Query user sid S-1-5-21-118052468-2300894008-1344842092-1107
...
[2023/05/04 11:18:46.354546,  5, pid=1072074, effective(0, 0), real(0, 0), class=winbind, traceid=36, depth=4] ../../source3/winbindd/wb_lookupsid.c
  WB command lookupsid start.
```

#3: DEBUG HEADER FIELD DEPTH

```
[2023/05/04 11:18:46.353302,  3, pid=1072074, effective(0, 0), real(0, 0), class=winbind, traceid=36, depth=1] ../../source3/winbindd/winbindd_getpw
      [nss_winbind (1072408)] Winbind external command GETPWNAM start.
      Query username 'ADDOMAIN/alice'.
[2023/05/04 11:18:46.353325,  5, pid=1072074, effective(0, 0), real(0, 0), class=winbind, traceid=36, depth=2] ../../source3/winbindd/wb_lookupname.
          WB command lookupname start.
          Search namespace 'ADDOMAIN' and domain 'ADDOMAIN' for name 'alice'.
...
[2023/05/04 11:18:46.354214,  5, pid=1072074, effective(0, 0), real(0, 0), class=winbind, traceid=36, depth=2] ../../source3/winbindd/wb_getpwsid.c:4
          WB command getpwsid start.
          Query user SID S-1-5-21-118052468-2300894008-1344842092-1107.
...
[2023/05/04 11:18:46.354235,  5, pid=1072074, effective(0, 0), real(0, 0), class=winbind, traceid=36, depth=3] ../../source3/winbindd/wb_queryuser.c
              WB command queryuser start.
              Query user sid S-1-5-21-118052468-2300894008-1344842092-1107
...
[2023/05/04 11:18:46.354546,  5, pid=1072074, effective(0, 0), real(0, 0), class=winbind, traceid=36, depth=4] ../../source3/winbindd/wb_lookupsid.c
                  WB command lookupsid start.
```

#4: FLOW TRACES

```
[2023/05/04 11:18:46.353317, 20, pid=1072074, effective(0, 0), real(0, 0), class=winbind, traceid=36, depth=2] ../../source3/winbindd/winbindd_mi
          flow: -> wb_lookupname_send>
```

```
 -> process_request_send
     -> winbindd_getpwnam_send
         -> wb_lookupname_send
             -> dcerpc_wbint_LookupName_send
             <- dcerpc_wbint_LookupName_done
         <- wb_lookupname_done
     <- winbindd_getpwnam_lookupname_done
         -> wb_getpwsid_send
             -> wb_queryuser_send
                 -> wb_parent_idmap_setup_send
             <- wb_queryuser_idmap_setup_done
                 -> wb_sids2xids_send
             <- wb_queryuser_got_uid
                 -> wb_lookupsid_send
                     -> dcerpc_wbint_LookupSid_send
                     <- dcerpc_wbint_LookupSid_done
                 <- wb_lookupsid_done
             <- wb_queryuser_got_domain
                 -> dcerpc_wbint_GetNssInfo_send
                 <- dcerpc_wbint_GetNssInfo_done
             <- wb_queryuser_done
                 -> wb_sids2xids_send
             <- wb_queryuser_got_gid
                 -> wb_lookupsid_send
                     -> dcerpc_wbint_LookupSid_send
                     <- dcerpc_wbint_LookupSid_done
                 <- wb_lookupsid_done
             <- wb_queryuser_got_group_name
         <- wb_getpwsid_queryuser_done
     <- winbindd_getpwnam_done
 <- process_request_done
```

#4: FLOW TRACES

```
-> process_request_send
    -> winbindd_getpwnam_send
        -> wb_lookupname_send
            -> dcerpc_wbint_LookupName_send
                -> dcerpc_wbint_LookupName_r_send
                    -> dcerpc_binding_handle_call_send
                        -> dcerpc_binding_handle_raw_call_send
                            -> wbint_bh_raw_call_send
                                -> wb_domain_request_send
                                    -> wb_child_request_send
                                        -> tevent_queue_wait_send
                                    <- wb_child_request_waited
                                        -> wb_simple_trans_send
                                            -> wb_req_write_send
                                                -> writev_send
                                            <- wb_req_write_done
                                        <- wb_simple_trans_write_done
                                            -> wb_resp_read_send
                                                -> read_packet_send
                                            <- wb_resp_read_done
                                        <- wb_simple_trans_read_done
                                    <- wb_child_request_done
                                <- wb_domain_request_done
                            <- wbint_bh_raw_call_domain_done
                        <- dcerpc_binding_handle_raw_call_done
                    <- dcerpc_binding_handle_call_done
                <- dcerpc_wbint_LookupName_r_done
            <- dcerpc_wbint_LookupName_done
        <- wb_lookupname_done
    <- winbindd_getpwnam_lookupname_done
        -> wb_getpwsid_send
            -> wb_queryuser_send
                -> wb_parent_idmap_setup_send
            <- wb_queryuser_idmap_setup_done
                -> wb_sids2xids_send
            <- wb_queryuser_got_uid
                -> wb_lookupsid_send
                    -> dcerpc_wbint_LookupSid_send
                        -> dcerpc_wbint_LookupSid_r_send
                            -> dcerpc_binding_handle_call_send
                                -> dcerpc_binding_handle_raw_call_send
                                    -> wbint_bh_raw_call_send
                                        -> wb_domain_request_send
                                            -> wb_child_request_send
                                                -> tevent_queue_wait_send
                                            <- wb_child_request_waited
                                                -> wb_simple_trans_send
                                                    -> wb_req_write_send
                                                        -> writev_send
                                                    <- wb_req_write_done
                                                <- wb_simple_trans_write_done
                                                    -> wb_resp_read_send
                                                        -> read_packet_send
                                                    <- wb_resp_read_done
                                                <- wb_simple_trans_read_done
                                            <- wb_child_request_done
                                        <- wb_domain_request_done
                                    <- wbint_bh_raw_call_domain_done
                                <- dcerpc_binding_handle_raw_call_done
                            <- dcerpc_binding_handle_call_done
                        <- dcerpc_wbint_LookupSid_r_done
                    <- dcerpc_wbint_LookupSid_done
                <- wb_lookupsid_done
            <- wb_queryuser_got_domain
```

```
-> dcerpc_wbint_GetNssInfo_send
                        -> dcerpc_wbint_GetNssInfo_r_send
                            -> dcerpc_binding_handle_call_send
                                -> dcerpc_binding_handle_raw_call_send
                                    -> wbint_bh_raw_call_send
                                        -> wb_child_request_send
                                            -> tevent_queue_wait_send
                                        <- wb_child_request_waited
                                            -> wb_simple_trans_send
                                                -> wb_req_write_send
                                                    -> writev_send
                                                <- wb_req_write_done
                                            <- wb_simple_trans_write_done
                                                -> wb_resp_read_send
                                                    -> read_packet_send
                                                <- wb_resp_read_done
                                            <- wb_simple_trans_read_done
                                        <- wb_child_request_done
                                    <- wbint_bh_raw_call_child_done
                                <- dcerpc_binding_handle_raw_call_done
                            <- dcerpc_binding_handle_call_done
                        <- dcerpc_wbint_GetNssInfo_r_done
                    <- dcerpc_wbint_GetNssInfo_done
                <- wb_queryuser_done
                    -> wb_sids2xids_send
                <- wb_queryuser_got_gid
                    -> wb_lookupsid_send
                        -> dcerpc_wbint_LookupSid_send
                            -> dcerpc_wbint_LookupSid_r_send
                                -> dcerpc_binding_handle_call_send
                                    -> dcerpc_binding_handle_raw_call_send
                                        -> wbint_bh_raw_call_send
                                            -> wb_domain_request_send
                                                -> wb_child_request_send
                                                    -> tevent_queue_wait_send
                                                <- wb_child_request_waited
                                                    -> wb_simple_trans_send
                                                        -> wb_req_write_send
                                                            -> writev_send
                                                        <- wb_req_write_done
                                                    <- wb_simple_trans_write_done
                                                        -> wb_resp_read_send
                                                            -> read_packet_send
                                                        <- wb_resp_read_done
                                                    <- wb_simple_trans_read_done
                                                <- wb_child_request_done
                                            <- wb_domain_request_done
                                        <- wbint_bh_raw_call_domain_done
                                    <- dcerpc_binding_handle_raw_call_done
                                <- dcerpc_binding_handle_call_done
                            <- dcerpc_wbint_LookupSid_r_done
                        <- dcerpc_wbint_LookupSid_done
                    <- wb_lookupsid_done
                <- wb_queryuser_got_group_name
            <- wb_getpwsid_queryuser_done
        <- winbindd_getpwnam_done
<- process_request_done
    -> wb_resp_write_send
        -> writev_send
    <- wb_resp_write_done
<- process_request_written
<- winbind_client_processed
    -> read_packet_send
```

#5: TRACE PARSER

```
$ source3/script/samba-traceparser -h
usage: samba-traceparser [-h] [-t ID] [-p PID] [-b] [-m] [-f] [-c] path


positional arguments:
  path                  logfile or directory



options:
  -h, --help            show this help message and exit
  -t ID, --traceid ID   specify the traceid
  -p PID, --pid PID     specify the winbind client pid
  -b, --breakdown       breakdown the traces into per traceid files
  -m, --merge           merge logs by timestamp
  -f, --flow            show the request/sub-request flow traces
  -c, --flow-compact    show the request/sub-request flow traces
                        without dcerpc details
```

#5: TRACE PARSER

TRACE PARSER DEMO SESSION

MAN PAGES

```
SMB.CONF(5)

   winbind debug traceid (G)


   With this boolean parameter enabled, the per request
   unique traceid will be displayed in the debug header
   for winbind processes.


   Default: winbind debug traceid = no
```

```
SAMBA-TRACEPARSER(1)     User Commands      SAMBA-TRACEPARSER(1)

NAME
       samba-traceparser - Samba (winbind) trace parser.
```

MERGE REQUESTS

Tevent flow support

```
https://gitlab.com/samba-team/samba/-/merge_requests/3060
```

Trace parser

```
https://gitlab.com/samba-team/samba/-/merge_requests/3076
```