

Operating a Natural RPC Environment

This section mainly describes the tasks required to operate a Natural RPC environment. Some of these tasks are performed with the SYSRPC utility. For instructions on the functions the SYSRPC utility provides, refer to the Natural SYSRPC Utility documentation.

This section covers the following topics:

- Specifying RPC Server Addresses
 - Stubs and Automatic RPC Execution
 - Modifying RPC Profile Parameters Dynamically
 - Executing Server Commands
 - Logon to a Server Library
 - Using the LOGON Option
 - Using Natural RPC with Natural Security
 - Using Natural RPC with EntireX Security
 - Using Compression
 - Monitoring the Status of an RPC Session
 - Handling Errors
-

Specifying RPC Server Addresses

To each remote CALLNAT request, a server must be assigned (identified by *servername* and *nodename*) on which the CALLNAT is to be executed. Therefore, all subprograms to be accessed remotely must be defined:

- in a local service directory on the client side,
- or in a remote directory accessed via a remote directory server,
- or by way of default server addressing with the RPC profile parameter DFS,
- or within the client application itself by way of default server addressing.

In addition to the methods mentioned above, you can specify alternative servers.

Below is information on:

- Using Local Directory Entries
- Using Remote Directory Entries
- Specifying a Default Server Address at Natural Startup
- Specifying a Default Server Address within a Natural Session
- Using an Alternative Server

Using Local Directory Entries

All data of a client's local service directory is stored in the subprogram NATCLTGS. At execution time, this subprogram is used to retrieve the target server. As a consequence, NATCLTGS must be available in the client application or in one of the Natural steplib defined for the application.

If NATCLTGS has not been generated into a steplib or resides on another machine, use the appropriate Natural utility (SYSMAIN, SYSTRANS or SYSOBJH) to move NATCLTGS into one of the steplib defined for the application.

Note:

The NATCLTGS subprogram is always generated into the SYSRPC library on the FNAT system file. We strongly recommend that you move NATCLTGS into one of the steplib defined for the application.

If you are using a NATCLTGS for joint usage, you must make it available to all client environments, for example by copying it to the library SYSTEM, or, if an individual copy is used for a client, it must be maintained for this client using the Service Directory maintenance function of the SYSRPC utility.

To define and edit RPC service entries, see the Service Directory Maintenance function, as described in the SYSRPC Utility documentation.

Using Remote Directory Entries

A remote directory contains service entries that can be made available to several Natural clients. The Natural clients can retrieve these service entries from remote directory servers. For information on the purpose and on the installation of remote directory servers, see Using a Remote Directory Server.

For information on the SYSRPC Remote Directory Maintenance function, see the relevant section in the SYSRPC Utility documentation.

Specifying a Default Server Address at Natural Startup

Instead of addressing a server by using a local or remote service directory, you can preset a default server with the RPC profile parameter DFS, as described in your Natural Operations documentation. This server address is used if the subprogram can be found in neither the local nor the remote service directory.

The DFS setting determines the default server for the whole session or until it is overwritten dynamically.

If no DFS setting exists and the server address of a given remote procedure call could not be found in the service directory, a Natural error message is returned.

A default server address defined within a client application remains active even if you log on to another library or if a Natural error occurs.

Specifying a Default Server Address within a Natural Session

The client application itself may dynamically specify a default server address at runtime. For this purpose, Natural provides the user exit **USR2007N** in the library SYSEXT. The user exit enables you to determine a default server address that is to be used each time a remote program cannot be addressed via the service directory. It includes the following parameters:

Parameter	Format	Explanation
<i>function</i>	A1	<p>P Put: Determines that the server address (composed of the parameters <i>nodename</i> and <i>servername</i>, see below) is the default address for all subsequent remote procedure calls not defined in the service directory.</p> <p>To remove a default server address, specify a "blank" for <i>nodename</i> and <i>servername</i>.</p> <p>G Get: Retrieves the current default server address as set by the function P.</p>
<i>nodename</i>	A8	Specifies/returns the name of the server node to be addressed.
<i>servername</i>	A8	Specifies/returns the server name to be addressed.
<i>logon</i>	A1	Specifies/returns the logon option.
<i>protocol</i>	A1	Specifies/returns the transport method. Valid value: B (=EntireX Broker).

The Natural subprogram NATCLTPS in the library SYSRPC is only maintained for compatibility reasons. Except for logon and protocol, it provides the same parameters as the user exit USR2007N.

Using an Alternative Server

To avoid connection failures, you may want to define several alternative servers for a remote CALLNAT. If you specify such alternative servers, Natural proceeds as follows:

- The client makes a first attempt to establish the connection.
- If this attempt fails, instead of providing an error message, a second attempt is made, however, this time not on the same server. Instead, the service directory is searched again starting at the current entry to find out whether or not another server is available which offers the desired service.
- If a second entry is found, Natural tries to establish the connection to this server. If the remote procedure call is performed successfully, the client application keeps on running. The user does not notice whether the connection to the first server or to the alternative server produced the result.
- If no further entry is found or if the connection to alternative servers fail, Natural issues a corresponding error message.

To enable the use of an alternative server

1. Define more than one server in the service directory for the same service.
2. Set the Natural RPC profile parameter TRYALT to ON to give permission to use an alternative server.

This parameter can also be set dynamically for the current session. See the SYSRPC Parameter Maintenance function as described in the SYSRPC Utility documentation.

Stubs and Automatic RPC Execution

Stubs are no longer required if automatic Natural RPC execution is used, as described in Working with Automatic Natural RPC Execution below.

However, generating stubs provides the advantage of controlling the CALLNAT(s) executed remotely and facilitates error diagnoses. Should a remote call fail due to an incorrect CALLNAT name, the Natural error message issued then helps to immediately identify the problem cause. Without a stub, for an incorrect CALLNAT you may receive follow-up errors returned from the transport layer or the Natural server.

Below is information on:

- Creating Stub Subprograms
- Working with Automatic Natural RPC Execution

Creating Stub Subprograms

With the Stub Generation function of the SYSRPC utility, you can generate the Natural stub subprograms used to connect the client's calling program to a subprogram on a server. The stub consists of a parameter data area (PDA) and of the server call logic.

The PDA contains the same parameters as used in the CALLNAT statement of the calling program and must be defined in the Stub Generation screen of the Stub Generation function. If a compiled Natural subprogram with the same name already exists, the PDA used by this subprogram is used to preset the screen. The server call logic is generated automatically by the Stub Generation function after the PDA has been defined.

At execution time, the Natural application program containing the CALLNAT statement and the stub subprogram must exist on the client side. The Natural application subprogram must exist on the server side. Both the stub and server subprograms must have the same name.

For information on the SYSRPC Stub Generation function, see the relevant section in the SYSRPC Utility documentation.

Working with Automatic Natural RPC Execution

You are not required to generate Natural RPC stubs, but you can work with automatic Natural RPC execution (i.e. without using Natural stubs). To work with automatic Natural RPC execution set the RPC parameter AUTORPC as follows:

```
AUTORPC=ON
```

In that case, you can omit the generation of the client stub during your preparations for RPC usage. When the automatic Natural RPC execution is ON, Natural behaves as follows:

- if a subprogram cannot be found locally, Natural tries to execute it remotely (a stub subprogram is not needed),
- the parameter data area will then be generated dynamically during runtime.

As stubs only exist for client programs, this feature has no effect on the CALLNAT program on the server.

If AUTORPC is set to ON, and a Natural stub exists, it will still be used.

Modifying RPC Profile Parameters Dynamically

With the Parameter Maintenance function, for the current session, you can dynamically modify some of the RPC profile parameters set in the Natural profile parameter module.

Attention:

These modifications are retained as long as the user session is active; they are lost when the session is terminated. Static settings are only made using Natural profile parameters.

For information on the SYSRPC Parameter Maintenance function, see the relevant section in the SYSRPC Utility documentation.

Executing Server Commands

Active servers that have been defined in the service directory (see Specifying RPC Server Addresses) can be controlled with the SYSRPC Server Command Execution function, as described in the relevant section in the SYSRPC Utility documentation.

Logon to a Server Library

The server library on which the callnat is executed depends on the RPC LOGON option on the client side and a couple of parameters on the server side.

The following table shows which the relevant parameters are and how they influence the library setting:

	Client		Server				
	1	2	3	4	5	6	7
	*library-id	RPC LOGON flag for server entry set?	LOGONRQ set?	Server started with STACK=	NSC or native Natural?	NSC: RPC LOGON option in library profile	Server *library-id
1	Lib1	no	no	logon lib1	No influence	N/--	Lib1
2	Lib1	no	no	logon lib2	No influence	N/--	Lib2
3	Lib1	no	yes	(Client LOGON flag = no) and (LOGONRQ = yes) is not possible.			
4	Lib1	yes	No influence	No influence	NSC	AUTO	Lib1
5	Lib1	yes	No influence	No influence	NSC	N	Lib1
6	Lib1	yes	No influence	No influence	Native Natural	--	Lib1

Explanation of the table columns:

1. The library ID of the client application where the callnat is initiated.
2. The value of the RPC LOGON flag. Can be set for a whole node or a server. The flag can be set in the Service Directory of SYSRPC or using the DFS parameter or using the user exit program USR2009P.
3. LOGONRQ can be set as a Natural profile parameter at server startup.
4. The library ID to which the server is positioned at its startup.
5. Does the server run under Natural Security (NSC) or not?
6. The setting of the LOGON option in the NSC library profile (Session options > RPC restrictions) of the NSC server application. If the NSC LOGON option is set to AUTO, only library and user ID are taken. If set to N (default), the library, user ID and password parameters are evaluated.
7. The library on the server where the CALLNAT program is finally executed.

Using the LOGON Option

The LOGON option defines on which library the remote subprogram is to be executed. See also Logon to a Server Library.

When you do not use the LOGON option, the CALLNAT is executed on the library to which the server is currently logged on. This server logon is defined with the Natural profile parameter STACK = (LOGON *library*). The server will search for the CALLNATs to be executed in *library* (and all associated steplib defined for *library*).

A client application can be enabled to execute a subprogram on a different library by setting the LOGON option for this subprogram. This causes the client to pass the name of its current library to the server, together with this LOGON option. The server will then logon to this library, searching it for the desired subprogram and, if the latter is found, it will execute it. After that, it will make a logoff to the previous library.

Settings Required on the Client Side

To set the LOGON option, you can use either the Service Directory Maintenance function (see the SYSRPC Utility documentation) or - when using a default server - the DFS profile parameter or the User Exit USR2007N.

Settings Required on the Server Side

No setting is required on the server side.

Using Natural RPC with Natural Security

Natural RPC also supports Natural Security in client/server environments, where security may be active on either (or both) sides. If security data is to be passed to the server, the LOGON option (see also Using the LOGON Option) must be used.

The user ID and password are established as follows:

- If the client runs under Natural Security, the user ID and password from the Natural Security logon on the client are used and passed to the server.
- For non-Natural Security clients, the user exit **USR1071** is provided which the user has to execute and which prompts the user to specify his logon data - which are then passed to the server. The user exit USR1071 is contained in the library SYSEXT. The logon data contains the user ID and password from which the so-called security token is generated, and additionally some administrative information. For a more detailed description, see the USR1071T member in library SYSEXT. A typical user exit call would read:

```
USR1071P userid password '0' '0' '0' '0' 'Y' 'Y'.
```

If the server runs under Natural Security, the user ID and password from the client are verified against the corresponding user security profile on the server, and the logon to the requested library and the execution of the subprogram are performed according to the corresponding Natural Security library and user profile definitions on the server.

After the execution of the subprogram, the library used before the CALLNAT request is made current again on the server. In the case of a conversational RPC, the first CALLNAT request within the conversation sets the library ID on the server; and the CLOSE CONVERSATION statement resets the library ID on the server to the one before the conversation was opened.

To enforce the LOGON option - that is, if you want a server to accept only requests from clients where the LOGON option is set - set the profile parameter/subparameter LOGONRQ to ON for the server.

As part of the Natural RPC Restrictions in library profiles of Natural Security, a session option "Close all databases" is provided. It causes all databases which have been opened by remote subprograms contained in the library to be closed when a Natural logon/logoff to/from the libraries is performed. This means that each client uses its own database session. See Natural RPC Restrictions in the Natural Security documentation.

Using Natural RPC with EntireX Security

Natural RPC fully supports EntireX Security on the client side and the server side.

Client Side

To logon to and logoff from the EntireX Broker, the user exit USR2071N is provided in library SYSEXT. To logon to EntireX Broker, you use the logon function of USR2071N and pass your user ID and password to the selected EntireX Broker. After a successful logon, the security token returned is saved by Natural and passed to the EntireX Broker on each subsequent call. The logon feature is fully transparent to the Natural application.

If EntireX Security has been installed or if AUTOLOGON=NO has been specified in the EntireX Broker attribute file, you must invoke USR2071N with the logon function before the very first remote CALLNAT execution.

- An internal reLOGON is done after an EntireX Broker timeout has occurred, if the original LOGON was done without a password (the password used in the LOGON is not saved). If no internal reLOGON is possible after a timeout has occurred, the client has to explicitly reissue the LOGON.

LOGOFF

An EntireX Broker LOGOFF function is executed to the *broker-id* named for the *user-id* passed.

Server Side

If the value of ACIVERS is 2 or higher, the server will log on to the EntireX Broker at the session start using the LOGON function. The user ID is the same as the user ID defined by SRVUSER.

If EntireX Security has been installed and if the EntireX trusted user ID feature is not available, there are two alternative ways to specify the required password:

- **SRVUSER=*NSC**

If Natural Security is installed on the server, you can specify SRVUSER=*NSC to determine that the current Natural Security userID which was used when the server was started is used for the LOGON in conjunction with the accompanying Natural Security password. In this case, the value set for ACIVERS must be at least 4.

- **USR2072N**

User exit USR2072N enables you to specify a password which is used for the LOGON in conjunction with SRVUSER.

Using the Subprogram USR2072N

USR2072N has the following parameter:

Parameter	I/O	Format	Description
<i>password</i>	I	A08	User ID's password.

The Subprogram USR2071N should be copied to the library SYSTEM or to the steplib library, or to any application.

The parameter listed above must be defined using the DEFINE DATA statement.

The calling program must contain the following statement:

```
CALLNAT 'USR2072N' PASSWORD
```

The calling program must be executed before the Natural RPC server has started its initialization. To accomplish this, put the name of the calling program on the Natural stack when starting the server:

```
STACK=(LOGON "server library";USR2072P "server password")
```

Using Compression

Compression types may be: 0, 1 or 2. Stubs generated with COMPR = 1 or 2 can help reduce the data transfer rate.

Compression Type	Description
COMPR=0	All CALLNAT parameter values are sent to and returned from the server, i.e. no compression is performed.
COMPR=1 (default)	M-type parameters are sent to and returned from the server, whereas O-type parameters are only transferred in the send buffer. A-type parameters are only included in the reply buffer. The reply buffer does not contain the Format description.
COMPR=2	Same as for COMPR = 1, except that the server reply message still contains the format description of the CALLNAT parameters. This might be useful if you want to use certain options for data conversion in the Software AG product EntireX Broker (for more information, see the description of Translation Services in the EntireX Broker documentation).

Monitoring the Status of an RPC Session

This part is organized in the following sections:

- Using the RPCERR Program
- Using the RPCINFO Subprogram
- Using the Server Trace Facility
- Defining the Trace File

Using the RPCERR Program

You can use the RPCERR program from the command line or invoke it via FETCH from within a Natural program.

RPCERR displays the last Natural error number and message if it was RPC related and it also displays the last BROKER reason code and associated message. Additionally, the node and server name from the last EntireX Broker call can be retrieved.

```

Example of an RPC Error Display: RPCERROR

NATURAL error number: NAT6972
  NATURAL error text :
  Directory error on Client, reason 3 :3:.

RPC error information:
  No additional information available.

Server Node: Library:      SYSRPC
  Server Name:      Program: NATCLT3
                                     Line No: 0480
    
```

Using the RPCINFO Subprogram

You can use the subprogram RPCINFO in your application program to retrieve information on the state of the current RPC session. This also enables you to handle errors more appropriately by reacting to a specific error class.

The subprogram RPCINFO is included in the library SYSRPC.

Example:

```
DEFINE DATA LOCAL USING RPCINFOL
  LOCAL
  1 PARM    (A1)
  1 TEXT    (A80)
  1 REDEFINE TEXT
    2 CLASS (A4)
    2 REASON (A4)
  END-DEFINE
  ...
  OPEN CONVERSATION USING SUBPROGRAM 'APPLSUB1'
    CALLNAT 'APPLSUB1' PARM
  CLOSE CONVERSATION *CONVID
  ...
  ON ERROR
    CALLNAT 'RPCINFO' SERVER-PARMS CLIENT-PARMS
    ASSIGN TEXT=C-ERROR-TEXT
    DISPLAY CLASS REASON
  END-ERROR
  ...
  END
```

RPCINFO has the following parameters which are provided in the PDA RPCINFOL:

Parameter	Format	Description
SERVER-PARMS		Contains information about the Natural session when acting as a server. The SERVER-PARMS only apply if you execute RPCINFO remotely on an RPC server.
S-BIKE	A1	Transport protocol used. Possible values: B (EntireX Broker) or C (CSCI, OpenVMS only).
S-NODE	A8	The node name of the server.
S-NAME	A8	The name of the server.
S-ERROR-TEXT	A80	Contains the message text returned from the transport layer.
S-CON-ID	I4	Current conversation ID. Note that this is the physical ID from EntireX Broker, not the logical Natural ID. This parameter always contains a value as EntireX Broker generates IDs for both conversational and non-conversational calls. If the physical conversation ID is either non-numeric or greater than I4, a -1 is returned.
S-CON-OPEN	L	Indicates whether there is an open conversation. This parameter contains value TRUE if a conversation is open, otherwise it contains FALSE.
CLIENT-PARMS		Contain information about the Natural session when acting as a client. The CLIENT-PARMS only apply if you execute RPCINFO remotely on an RPC client.
C-BIKE	A1	Transport protocol used. Possible values: B (EntireX Broker) or C (CSCI, OpenVMS only).
C-NODE	A8	The node name of the previously addressed server.
C-NAME	A8	The name of the previously addressed server.
C-ERROR-TEXT	A80	Contains the message text returned from the transport layer.
C-CON-ID	I4	Conversation ID of the last server call. Note that this is the physical ID from EntireX Broker, not the logical Natural ID. If no conversation is open, the value of this parameter is less than or equal to 0. If the physical conversation ID is either non-numeric or greater than I4, a -1 is returned.
C-CON-OPEN	L	Indicates whether there is an open conversation. This parameter contains value TRUE if a conversation is open, otherwise it contains FALSE.

Using the Server Trace Facility

Natural RPC includes a trace facility that enables you to monitor server activities and trace possible error situations.

Activating/Deactivating the Server Trace Facility

To activate/deactivate the server trace facility, start the server with the option

TRACE=*n*

The integer value "*n*" represents the desired trace level; that is, the level of detail in which you want your server to be traced. The following values are possible:

Value	Trace Level
0	No trace is performed (default).
1	All client requests and corresponding server responses are traced and documented.
2	All client requests and corresponding server responses are traced and documented; in addition, all RPC data are written to the trace file.

The RPC trace facility writes the trace data to the Natural Report Number 10.

Defining the Trace File

The trace file definition depends on the environment. Below is information on:

- Trace File Handling for OpenVMS and UNIX Environments

Trace File Handling for OpenVMS and UNIX Environments

It is recommended that you use a different file name (that is, a different NATPARM parameter file) for each server so that you can trace them individually. The trace file is defined in the NATPARM parameter file of the Natural server:

1. Report Assignments
Assign the logical device LPT10 to your Report Number 10.
2. Device Parameter Assignments
Instead of selecting a physical printer specification for LPT10, specify a file name that represents the name of your trace file.

Example:

```
For OpenVMS:      filename
For UNIX:         /bin/sh -c cat>>/filename
```

where *filename* represents the name of the trace file.

Handling Errors

- Remote Error Handling
- Avoiding Error Message NAT3009 from Server Program
- User Exit NATRPC01

Remote Error Handling

Any Natural error on the server side is returned to the client as follows:

- Natural RPC moves the appropriate error number to the *ERROR-NR system variable.
- Natural reacts as if the error had occurred locally.

Note:

If AUTORPC is set to ON and a subprogram cannot be found in the local environment, Natural will interpret this as a remote procedure call. It will then try to find this subprogram in the service directory.

If it is not found there, a NAT6972 error will be issued. As a consequence, no NAT0082 error will be issued if a subprogram cannot be found.

See also Using the RPCERR Program.

Avoiding Error Message NAT3009 from Server Program

If a server application program does not issue a database call during a longer period of time, the next database call might return a NAT3009 error message.

To avoid this problem, proceed as follows:

1. Add a FIND FIRST or HISTOGRAM statement in program NATRPC39, library SYSRPC.
2. Copy the updated program to library SYSTEM or to the appropriate user library.

User Exit NATRPC01

This exit is called when a Natural error has occurred, actually after the error has been handled by the Natural RPC runtime and immediately before the response is sent back to the client. This means, the exit is called at the same logical point as an error transaction, that is, at the end of the Natural error handling, after all ON ERROR blocks have been processed.

In contrast to an error transaction, this exit is called with a CALLNAT statement and must therefore be a subprogram which must return to its caller.

The interface to this exit is similar to the interface of an error transaction. In addition, the exit can pass back up to 10 lines of information which will be traced by the Natural RPC runtime. Only lines which begin with a non-blank character will be traced.

Important Notes:

1. NATRPC01 must be located in library SYSTEM on FUSER. The STEPLIB concatenation of the library to which the server currently is logged on is **not** evaluated.
2. The DEFINE DATA PARAMETER block must not be changed.