

Processor

Processing Status

new

Implementation Status

Cannot be implemented

Language

E

Short Text

ICM: Binding ports < 1024 on UNIX

Component

BC-CST-IC

Internet Communication Manager

---

## Description

### Symptom

To bind ports < 1024 (well known ports), the process on Unix must have superuser authorization rights.

### Reason and Prerequisites

Authorization concept on UNIX.

### Solution

Since only users with superuser authorization rights can bind ports < 1024 (well known ports) on a UNIX system and the ICM process or the SAP Web Dispatcher should not have these rights (and ICM cannot have them for technical reasons), the port must be bound by an external program and the listen socket then transferred to the calling process.

With the standard authorization rights of the <sid>adm user, the process can bind all ports >= 1024 (provided that they are not bound by another program).

To be able to bind ports < 1024, the external bind program icmbnd is started directly by the ICM, or the SAP Web Dispatcher, the port is bound by icmbnd and the listen socket is returned to the calling process. The bind program icmbnd then stops again.

To be able to bind ports < 1024, the icmbnd must have superuser authorization. User 'root' can assign these authorizations using the following UNIX commands:

```
### cp icmbnd.new icmbnd
# chown root:sapsys icmbnd
# chmod 4750 icmbnd
# ls -al
```

should then output the following authorizations for "icmbnd":

```
-rwsr-x--- 1 root sapsys 1048044 Mar 20 16:19 icmbnd
```

To prevent the ICM/SAP Web Dispatcher from attempting to bind the port itself, an additional option must be specified when the ports are configured with icm/server\_port\_: "EXTBIND=1".

The format for this parameter is as follows:

PROT=<protocolname>, PORT=<Port or servicename>  
[, TIMEOUT=<keep alive timeout>, EXTBIND=1]

where TIMEOUT and EXTBIND are optional specifications.

For example: "PROT=HTTP, PORT=8080, TIMEOUT=15, EXTBIND=1"

#### Note

icmbnd is generally called directly from the ICM or SAP Web Dispatcher. However, the program can also be called externally to notify t

he ICM of new ports (not recommended).

Naturally, you can also use "icmbnd" to bind ports >= 1024, but this lengthens the startup time of the call process.

"icmbnd" is avail

able for Windows because the user <sid>adm can bind any ports on this system, but its use does not make sense here.

The program icmbnd is delivered under icmbnd.new as of Release 7.10. This prevents an icmbnd program that belongs to the root user fro

m being overwritten regularly by an icmbnd program without root authorizations when you apply patches. When you install the 7.10 Kerne

l for the first time, you must copy icmbnd.new to icmbnd once and, as described above, it must have the required (root) authorizations

"icmbnd" with superuser authorization must be created in the local executable directory (DIR\_EXECUTABLE) on each application server. T

his is because the superuser authorization is lost when executables are copied from the central executable directory to the local dire

ctory.

#### Description of "icmbnd"

During normal operations, "icmbnd" is never called manually; the description below takes the form of documentation only.

#### NAME

icmbnd

#### SYNOPSIS

icmbnd -S <server port> -l <listen port> -p <protocol>  
[-k <keep alive> -t <trace level> -f <trace file>]  
-v[ersion]

#### Description

icmbnd is an external utility program for the Internet Communication Manager (ICM) for binding ports.

#### parameter

-S <server port>

This is the administration port of the ICM through which the listen socket is transferred from "icmbnd" to the ICM.

-l <listen port>

Port that should be bound by "icmbnd". This can be a port number or a port name (for example, http, smtp, nntp)

-p <protocol>

Specification of the log for the port to be bound (such as HTTP, HTTPS, SMTP).

#### Optional parameters:

-k <keep alive>

Specification of the keep-alive timeout (in seconds) for the port to be bound. If this parameter is not specified, the

standard value  
of the ICM is transferred.  
-t <trace level>

Specification of the trace level (1-3). The standard value is 1.  
-f <trace file>

Specification of the name of the trace file to be used. The standard value is "dev\_icmbnd".  
-v [version]

"icmbnd" issues the current version information and terminates.

#### Error messages

The following errors may occur and be logged by icmbnd:

"missing argument for option <option>"

The required argument was not specified in the command line.

"Illegal option <option>"

Invalid argument

"Missing values for service, listen port or protocol"

One of the -S -l -p options was not specified.

"IcmConnect to port %d failed (rc=%d)"

A connection to the ICM could not be established on the port number of the "-S <server port>" argument. Check the specification for the  
e "-S <server port>" parameter.

"NiBuf2Listen failed(rc=%d)"

The listen port could not be bound. Either the authorizations for binding are missing or the port is already bound by another program.

"IcmBndSendHdl failed (rc = %d)"

"NiSendHandle failed (rc = %d)"

The listen socket could not be transferred to the ICM (communication error).

Note for Release 6.x:

The following adjustments must be taken into account for Release 6.10:

The procedure only works if the latest version of icmbnd is used (this is available on sapserv). If an old icmbnd is used, the trace f

ile dev\_icm contains the following entries:

\*\*\* ERROR => IcmMsgProcess: got illegal Partner: 0 [icxxman\_mt.c 2123]

\*\*\* ERROR => IcmMsgProcess: login expected, got opcode=16 [icxxman\_mt.c

\*\*\* ERROR => IcmRecvListenHdl: illegal state: 1 for accepting

\*\*\* ERROR => IcmLoop: IcmRecvListenHdl failed [icxxman\_mt.c 1120]

In addition, Release 6.10 requires a kernel patch level > 37 (disp+work -V or icman -V).

When using the 6.20 kernel and a patch level < 270, the following parameter should be set in the profile:

UNIX: exe/icmbnd = \$(DIR\_EXECUTABLE)/icmbnd

NT: exe/icmbnd = \$(DIR\_EXECUTABLE)/icmbnd.exe

Other terms

ICM, SAP Web Dispatcher, NiBuf2Listen, bind, listen, permission denied

## Valid Releases

Software Component	Release
--------------------	---------

SAP Basis component	
---------------------	--

610
620
640
700
710
711
701
702
720
730

Unknown	
---------	--

Unknown
---------

Unknown	
---------	--

Unknown
---------

Unknown	
---------	--

Unknown
---------

Unknown	
---------	--

Unknown
---------

Unknown	
---------	--

Unknown
---------

Unknown	
---------	--

Unknown
---------