

FUJITSU Software BS2000 HIPLEX MSCF

Version V11.0A
February 2017

Release Notice

All rights reserved, including intellectual property rights.
Technical data subject to modifications and delivery subject to availability. Any liability that the data and illustrations are complete, actual or correct is excluded. Designations may be trademarks and/or copyrights of the respective manufacturer, the use of which by third parties for their own purposes may infringe the rights of such owner.

© 2017 Fujitsu Technology Solutions GmbH

Fujitsu and the Fujitsu logo are trademarks or registered trademarks of Fujitsu Limited in Japan and other countries. BS2000 is a trademark of Fujitsu Technology Solutions GmbH in Germany and other countries.

1 General	3
1.1 Ordering	3
1.2 Delivery	4
1.3 Documentation	4
2 Software extensions	4
3 Technical information	5
3.1 Resource requirements	5
3.2 Software configuration	5
3.3 Product installation	5
3.4 Product use	6
3.5 Discontinued functions (and those to be discontinued)	7
3.6 Incompatibilities	7
3.7 Restrictions	8
3.8 Procedure in the event of errors	9
4 Hardware requirements	9
5 Firmware levels	9

1 General

BS2000 systems can be coupled together to form a functional network using the HIPLEX¹ MSCF (HIPLEX MULTI-SYSTEM-CONTROL-FACILITY).

HIPLEX MSCF is a compatible further development of the product MSCF and replaces the previous MSCF versions as of BS2000/OSD V3.0A.

The partners in the MSCF network only have to form a subset of a BCAM network. The network can comprise up to 164 systems, where each must be accessible under a unique SYS ID.

Operating system functions such as catalog access and starting ENTER jobs, which were originally intended for just a single BS2000 system, are now supported for all computers in the network.

HIPLEX MSCF also allows Cross Coupled Systems (XCS), the high performance and high availability network.

This Release Notice is a summary of the major extensions, dependencies and operating information with respect to HIPLEX MSCF V11.0A under the BS2000 operating system.

The release level is that of February 2017.

This and other current Release Notices are shipped on the SoftBooks DVD and are available online at <http://manuals.ts.fujitsu.com>.

If one or more previous versions are skipped when this product version is used, the information from the Release Notices and README files of the previous versions must also be noted.

Please note:

Each version of HIPLEX MSCF can be used only together with a given version of BS2000 OSD/XC. In order to emphasize this fact, the main version of HIPLEX MSCF is now equal to the version of BS2000 OSD/XC which is required to run this HIPLEX MSCF version.

To achieve this, the HIPLEX MSCF versions V9.0 and V10.0 have been skipped.

The predecessor version of HIPLEX MSCF V11.0 is V8.0.

1.1 Ordering

HIPLEX MSCF V11.0A can be ordered from your local distributors.

The product is supplied subject to a single payment or payment by installments.

¹ HIPLEX® is a registered trademark of Fujitsu Technology Solutions GmbH

1.2 Delivery

The HIPLEX MSCF V11.0A files are supplied via SOLIS.

The following delivery groups are part of the HIPLEX MSCF V7.0A delivery scope:

MSCF V20.0A
NSM V20.0A
XCS-TIME V20.0A

The current file and volume characteristics are listed in the SOLIS2 delivery cover letter.

1.3 Documentation

The BS2000 documentation is available in German and English on DVD with the title BS2000 SoftBooks. The DVD is part of the delivery, but additional copies may be ordered separately.

The documentation is also available on the internet at

<http://manuals.ts.fujitsu.com>.

Manuals which are displayed with an order number can also be ordered in printed form.

The HIPLEX MSCF V6.0A manual remains valid for HIPLEX MSCF V11.0A. The subsequent changes and extensions to the manual can be found in the README file for the product, which is also available on the SoftBooks DVD as well as on the internet.

The basic BS2000 manuals are also required for operating HIPLEX MSCF.

2 Software extensions

HIPLEX MSCF V11.0 has been adapted to run under BS2000 OSD/BC V11.0. This includes the evaluation of the new pubset attribute **ALTERNATE-MASTER**:

This attribute is relevant for pubsets which have both, master and backup master, explicitly specified.

Up to now, only the system specified as master has been allowed to execute the first master import, thus initiating pubset operation. The backup master has just been a replacement in case the current master fails during ongoing operation.

Now, the attribute ALTERNATE-MASTER may entitle the backup master to initiate pubset operation if the master doesn't do so.

A detailed description of the new attribute is included in the BS2000 "commands" manual, because it is set by the BS2000 command SET-PUBSET-ATTRIBUTES and displayed by the BS2000 command SHOW-PUBSET-ATTRIBUTES.

3 Technical information

3.1 Resource requirements

Depending on the installation parameters used in IMON, 3,300 to 8,500 PAM pages of disk space is required to install HIPLEX MSCF.

Additionally, 18 PAM pages for the file SYS.PVS.SHARER.CONTROL are required on the pubres of each shared pubset.

HIPLEX MSCF is able to run even on the smallest BS2000 servers with a nominal power of 12 RPF. However, MSCF internally uses fix time intervals to monitor the pubset partners and therefore needs 12 RPF in each single interval, not only in statistic average.

To ensure this, the nominal power assigned to a VM2000 guest system must be higher. Depending on the server power, the number of guest systems, the relation of their CPU quotas, and the length of the MSCF interval (which depends on the selected FAIL-DETECTION-LIMIT), up to nominal 48 RPF may be necessary for running MSCF smoothly.

3.2 Software configuration

HIPLEX MSCF V11.0A will run on BS2000 OSD/BC V11.0A. Additional prerequisite is the product openNet Server that must be purchased.

The job variables subsystem, that also has to be purchased, is required in order to use the full functional scope.

3.3 Product installation

Installation of the product HIPLEX MSCF with the installation monitor IMON is mandatory. The information concerning installation in the delivery cover letter and in the product documentation must be followed as well as the information given below.

The necessary inputs and the sequence of the installation are described in the IMON documentation.

Note:

If the file `SYSPAR.MSCF.200` exists on the system, it will remain unchanged. The file of the same name in the delivery is then cataloged by IMON under the name `SYSPAR.MSCF.200.NEW` instead.

After the product has been successfully installed using IMON, the following must be observed:

- If the MSCF subsystem is to be started automatically in BS2000 startup, the start time of MSCF must be set to `*BEFORE-SYSTEM-READY` in the generated subsystem catalog (default name: `SYS.SSD.CAT.X`) and, if required, another MSCF configuration file must be specified as the `SUBSYSTEM-INFO-FILE`. This requires that BCAM is also started via the parameter `service` prior to `SYSTEM READY`.
- The preset value for the MSCF configuration parameter `FAIL-DETECTION-LIMIT` is 176 seconds for reasons of compatibility. When using the `SNAPSHOT` function, it is recommended to increase this value to 528 seconds.
A prerequisite for this is that the value is agreed with the network partners (see 3.4 "Product use").

3.4 Product use

For compatibility, the presets of all MSCF configuration parameters correspond to those of older MSCF versions. If necessary, it is recommended to assign other values to the following parameters in the MSCF configuration file:

- FAIL-DETECTION-LIMIT = 352 / 528
To be absolutely certain of preventing MSCF connections from being (temporarily) dropped during a SNAP dump, FAIL-DETECTION-LIMIT must be set to at least 528. This is particularly recommended in an XCS network with RECOVERY-START = *AUTOMATIC since a connection failure in this case would cause an MSCF-ABORT on one of the systems concerned.
If partners without a common shared pubset are monitored, there is a risk with FAIL-DETECTION-LIMIT < 352 that MSCF will detect the partner as failed within the SNAPTIME and initiate reconfiguration measures (there is real danger of a SETS MCS1300 if RECOVERY-START=*AUTOMATIC).
Note:
The FAIL-DETECTION-LIMIT must be the same on all partners in order to set up CCS connections.
- RECOVERY-START = *[CONSISTENT-]BY-OPERATOR / *SECURE
If *AUTOMATIC is set, there is a danger of an abnormal system termination with SETS MCS1300 if a connection to a partner is lost at roughly the same time as a write error to the watchdog file(s) of the common shared pubset(s) occurs.
In particular, *AUTOMATIC should never be used if the connections and the disks used by MSCF are routed via the same FC switch.
- TRACE-FILE = *STD
The trace file is just about indispensable for diagnosing MSCF problems. The additional load on the system caused by writing the traces is not measurable during normal operation. The file should be changed at regular periods (e.g. weekly) with the command:
MODIFY-MSCF-ENVIRONMENT TRACE-FILE = *STD

The master of a shared pubset should always be a system that is running the latest versions of BS2000/OSD and MSCF. This is also the basic requirement to enable the slave systems to use new components of the network functionality in these versions.

A master role for a shared pubset can be assigned with the SET-PUBSET-ATTRIBUTES command.

If the product SECOS is used, all members of an SPVS network should have the same version. The following must be noted if this is not possible:

- If SECOS is not running on the master of an SPVS, it is generally not possible to use SECOS functions for access to this pubset.
- If the master and slave are using different versions of SECOS, the functionality of the local SECOS version of the accessing system always applies for access to the pubset, regardless of whether it is the master or slave (for example: if a "default protection" has been set up for the pubset, it applies only for the user of the pubset on which SECOS as of V3.0A is running; for all users with earlier SECOS versions, on the other hand, the default system values apply).

In an XCS network, it is strongly recommended that ALL systems are connected to a radio clock. This is the only way to guarantee that the global XCS time in the network, the local SVP time of all machines and the real time always nearly match.

On every system without its own radio clock connection, the SVP time of the local server may significantly diverge from the system and the net time. This can lead to problems under unfavourable conditions:

- with a new IPL:
With an IPL via the SVP, the system time is initialized with the system SVP time. If the SVP time lags behind the system time that was valid before the IPL, an apparently negative time jump may occur. In this case, a system startup is only possible by executing a dialogue startup with the UNLOCK option and manually initializing the system time (or after waiting until the time difference has elapsed).
- when a system enters the network:
If a system wishes to enter an XCS network, its system time must be synchronized with network time. Differences between system and network time therefore result in lengthy delays when entering the network.
Differences greater than 15 minutes cannot be compensated at all. Entering the network is only possible for this system with corrected system time (new IPL with changed SVP time or manual time input).
- when temporarily leaving the network:
If the system time of a system leaving the network differs by less than 15 minutes from the local SVP time, BS2000 starts to adjust the system time to the SVP time. When re-entering the network, the problems described above may therefore also occur.

In an XCS network without a radio clock, the system time of the network members (the network time) may significantly diverge from the real (official) time after a lengthy operation period.

In an XCS network with more than one radio clock, time information may appear contradictory when reaching network members without radio clock due to transfer inaccuracies. As a result, the accuracy of time synchronization may decrease.

Further notes on use can be found in the manual.

Courses for BS2000 are offered by Fujitsu Technology Solutions (<http://training.ts.fujitsu.com>). MSCF is part of the BS2ADMIN2 course.

3.5 Discontinued functions (and those to be discontinued)

None.

3.6 Incompatibilities

None.

3.7 Restrictions

The POSIX file systems /root and /var should not be stored on the shared pubset; otherwise, manual POSIX termination would be necessary to export the pubsets concerned. This could cause a blockage, especially for the automatic reconfiguration of MSCF (RECOVERY-START = *AUTOMATIC), since it is not possible to terminate MSCF until all shared pubsets have been exported.

Creating additional snapsets for shared pubsets, on which POSIX file systems are located, should be avoided. If this cannot be avoided, the following should be observed:

Such pubsets are mostly imported before starting POSIX, because that is when POSIX can only automatically mount the file systems located on it. However, in this case the snapsets are not put into operation (because for this purpose POSIX and SHC-OSD would already have to be operational at the time of the import). If a master change takes place later for a pubset with inactive snapsets, the new master makes up for putting them into operation. However, the master cannot process any other requests for this pubset during this time!

In the case of multiple problems (e.g. loss of connection to all VMs of a server or a location) this can result in the blockade of the MSCF reconfiguration. We therefore strongly recommend you to explicitly put into operation the snapsets of all shared pubsets, which are already imported before starting POSIX and SHC-OSD, e.g. with /SHOW-SNAPSET-CONFIGURATION <pubset>.

A BS2000 system sets the cluster reconfiguration lock of MSCF before it is possibly stopped for a longer period of time – e.g. when moving a VM (VM2000 command MOVE-VM) or during Live Migration. The lock prevents the partners in the network from classifying the affected system as “failed”.

The lock does not prevent applications on the network partners from continuing to attempt to send messages to the MSCF of the system that is at a standstill. Such attempts to send are repeated at TCP protocol level approximately for a minute (TCP Retransmit). If transmission does not succeed in this time, TCP disconnects the connection without MSCF being able to have any influence.

This is why actions that result in the stopping of the system and the setting of the cluster reconfiguration lock should always be scheduled for times with a low load.

When using SECOS in an LCS network, job variables on REMOTE imported pubsets can only be created when the SECOS function "default protection" is deactivated explicitly by specifying PROTECTION-ATTR=*STD. Otherwise, any attempt to create a job variable will be rejected with error message JVS044C.

3.8 Procedure in the event of errors

If problems occur with HIPLEX-MSCF, the following documents will be required for diagnostics:

- An accurate description of the error condition indicating if and how the error can be reproduced.
- If available, system dump / SLED
- CONSLOG log after entering the following commands

```

/SHOW-SUBSYSTEM-STATUS MSCF
/BCSHOW APPLICATION=$MRSAPP,SH=ROUTE
/BCSHOW APPLICATION=$MRSAPPS,SH=ROUTE
/BCSHOW APPLICATION=$MRSAPP4,SH=ROUTE
/BCSHOW APPLICATION=$MRSAPP5,SH=ROUTE
/BCSHOW APPLICATION=$MCSNLX,SH=ROUTE (only in XCS network)
/BCSHOW APPLICATION=$MCSNSM,SH=ROUTE (only in XCS network)
/SHOW-MSCF-CONFIGURATION INFORMATION=*ALL
/SHOW-SHARED-PUBSET
/SHOW-XCS-OCCUPATION (only in XCS network)
/SHOW-MASTER-CATALOG-ENTRY SELECT=*SHARED
/SHOW-MASTER-CATALOG-ENTRY SELECT=*MASTER-CHANGE-ERROR
/SHOW-PUBSET-PARAMETERS INFORMATION=*PUBSET-OCCUPATION

```
- SERSLOG file
- MSCF configuration file (default: SYSPAR.MSCF.200)
- MSCF trace file
- Output of /SHOW-SUBSYSTEM-ATTRIBUTES MSCF, INF=*ALL

The error must be reported to the appropriate service provider.
A PERLE error report will be opened for Second Level Support.

A Teleservice connection with callback option or an AIS Connect access is essential for diagnostics. If this is not available, the service provider is entitled to invoice additional services rendered.

4 Hardware requirements

HIPLEX MSCF itself has no hardware dependencies.
All devices and central units that are supported by BS2000 OSD/XC V11.0 can be used.

5 Firmware levels

HIPLEX MSCF has no firmware dependencies.