

File Management, Number of Files in FileGroup Exceeded

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2014–2016. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Alarm Description	1
1.2	Prerequisites	2
2	Procedure	3



File Management, Number of Files in FileGroup Exceeded



1 Introduction

This instruction concerns alarm handling.

It is assumed that a Managed Element (ME) function called `Function2` produces files that are regularly transferred and deleted by some external system. The produced files are stored in a directory represented by a file group called `Function2Files`, which is monitored by a file group policy `alarmHighFileNumber`. When the number of files in this file group exceeds the defined limit, an alarm is raised.

1.1 Alarm Description

The possible alarm causes and fault locations are explained in Table 1.

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
Too many files in a file group	The total number of files in a file group has exceeded a threshold according to a file group policy	The total number of files in a file group has exceeded a configured threshold. Some ME or management system functionality responsible for deleting the files is misbehaving.	Network problems	Eventually the ME can lack storage space
			ME function	
			External system	

The alarm attributes are listed and explained in Table 2.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	131073
Managed Object Class	<i>FileGroup</i>
Managed Object Instance	<code>ManagedElement=<node_name>,SystemFunctions=1,FileM=1,LogicalFs=1,FileGroup=<file_group_id></code>



Table 2 Alarm Attributes

Attribute Name	Attribute Value
Specific Problem	File Management, Number of Files in FileGroup Exceeded
Event Type	other (1)
Probable Cause	x733ResourceAtOrNearingCapacity (343)
Additional Text	The number of files exceeded threshold level <i><thresholdHigh></i> in ManagedElement= <i><node_name></i> , SystemFunctions=1, FileM=1, LogicalFs=1, FileGroup= <i><file_group_id></i>
Perceived Severity	thresholdSeverity, which is one of the following: <ul style="list-style-type: none">• critical (3)• major (4)• minor (5)• warning (6)

1.2 Prerequisites

This section provides information on the documents, tools, and conditions that apply to the procedure.

1.2.1 Documents

This instruction references the following documents:

- *Data Collection Guideline*

1.2.2 Tools

No tools are required.

1.2.3 Conditions

Before starting this procedure, ensure that the following conditions are met:

- A File Management, Number of Files in FileGroup Exceeded alarm is raised.
- The user has appropriate access rights to the *FileGroup* Managed Object (MO).
- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.



2 Procedure

Do the following:

1. Check the connection to the external system using `ping` and `traceroute`.
2. Is the external system reachable in a delay lower than 10 seconds?

Yes: The file collection process can be interrupted because of some fault in the external system. Request the external system administrator to act on the fault.

No: The network can have a configuration fault. Request the network administrator to act on the fault.

3. Navigate to *FileGroup* MO indicated by the alarm attribute Additional Text, for example:

```
>dn ManagedElement=NODE06ST, SystemFunctions=1, FileM=1, LogicalFS=1, FileGroup=Functions2Files
```

4. Check which policy is applicable to the MO:

```
(FileGroup=Functions2Files)>show reservedByPolicy
```

The following is an example output:

```
reservedByPolicy="ManagedElement=NODE06ST, =>
SystemFunctions=1, FileM=1, FileGroupPolicy=>
alarmHighFileNumber"
```

5. Navigate to the *FileGroupPolicy* MO, for example:

```
(FileGroup=Functions2Files)>dn ManagedElement=NODE06ST,
SystemFunctions=1, FileM=1, FileGroupPolicy=alarmHighFileNumber
```

6. Observe the defined value for `thresholdLow` in the identified policy:

```
(FileGroupPolicy=alarmHighFileNumber)>show -m
ThresholdMonitoring
```

The following is an example output:

```
ThresholdMonitoring=warningAt10
  monitoredAspect=QUANTITY
  thresholdHigh=11
  thresholdLow=5
  userLabel="More Than Ten Files in File Group"
```



Note: If there are several *ThresholdMonitoring* MOs, find the `thresholdHigh` value corresponding the alarm, then observe the associated `thresholdLow` value.

7. Is it appropriate to manually delete the files in the *FileGroup* MO without loss of important data?

Yes: Continue with Step 8.

No: The external system is expected to delete these files automatically. Once this has happened, proceed with Step 10.

8. Identify the files that can be deleted to decrease the number of files in the file group to or below the `thresholdLow` value:

```
>dn ManagedElement=NODE06ST, SystemFunctions=1, FileM=1, LogicalFs=1, FileGroup=Functions2File
```

```
(FileGroup=Functions2File) >show
```

The following is an example output:



```
FileGroup=Functions2Files
internalHousekeeping=false
files="Functions2File.cfg"
  fileType="cfg"
  modificationTime="2014-11-20T13:33:57"
  size=108
files="Functions2File_20141025_210916.cfg"
  fileType="cfg"
  modificationTime="2014-10-25T21:09:16"
  size=108
files="Functions2File_20141025_210925.log"
  fileType="log"
  modificationTime="2014-10-25T21:09:27"
  size=0
files="Functions2File_20141025_211150_20141025_212046.log"
  fileType="log"
  modificationTime="2014-10-25T21:20:46"
  size=7168
files="Functions2File_20141025_212046.cfg"
  fileType="cfg"
  modificationTime="2014-10-25T21:20:46"
  size=108
files="Functions2File_20141027_175033_20141027_175714.log"
  fileType="log"
  modificationTime="2014-10-27T17:57:14"
  size=2048
files="Functions2File_20141027_175714.cfg"
  fileType="cfg"
  modificationTime="2014-10-27T17:57:14"
  size=108
files="Functions2File_20141027_180112_20141027_185409.log"
  fileType="log"
  modificationTime="2014-10-27T18:54:09"
  size=4096
files="Functions2File_20141027_185409.cfg"
  fileType="cfg"
  modificationTime="2014-10-27T18:54:09"
  size=108
files="Functions2File_20141028_184309.cfg"
  fileType="cfg"
  modificationTime="2014-10-28T18:43:09"
  size=108
files="Functions2File_20141120_133357.log"
  fileType="log"
  modificationTime="2014-11-20T14:34:10"
  size=5120
```

9. Delete each identified file:

```
(FileGroup=Functions2File) > config
```

```
(config-FileGroup=Functions2File) > removeFile  
Functions2File_20141025_211150_20141025_212046.log
```

The system returns `true` after a successful deletion operation. The system returns `false` when the operation fails. The operation fails when the file does not exist or is in use.

```
(config-FileGroup=Functions2File) > commit
```

10. Is the alarm cleared?

Yes: Proceed with Step 13.

No: Proceed with Step 11.

11. Perform data collection, refer to *Data Collection Guideline*.



12. Consult the next level of maintenance support. Further actions are outside the scope of this instruction.
13. Job is completed.