

Data Collection Guideline for SAPC

Ericsson Service-Aware Policy Controller

Operating Instructions

Copyright

© Ericsson AB 2018. 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	General	1
2	Workflow	2
3	Mandatory Data	3
3.1	Data Collection	3
3.1.1	Collecting Application and Platform Logs	3
4	Data Collected Based on Specific Problem Types	6
4.1	Database General Problems in the SAPC	6
4.2	Active-Standby Geographical Redundancy Problems in the SAPC	6
4.3	Active-Active Geographical Redundancy Problems in the SAPC	6
4.4	Software License Problems in the SAPC	7
5	Other Useful Information	8
5.1	Performance Data Collector Reports	8
5.1.1	Daily Report	8
5.1.2	Monthly Report	8
5.1.3	Health Check Report	8
6	Appendix A: Severity/Priority	9





1 General

The purpose of this document is to instruct what troubleshooting data to collect and enclose in a Customer Service Request (CSR). This guideline also instructs the needed procedure to collect the needed information.

Product Scope

This guideline is applicable to the following product releases:

- SAPC 1.1 and later product releases.

Prerequisites

Not Applicable.

Related Data Collection Guidelines

Not Applicable.



2 Workflow

The workflow for collecting troubleshooting data is as follows:

Steps

1. Collect mandatory data that is needed in connection to any problems experienced. See [Mandatory Data](#) on page 3.
2. Collect specific data based on the type of problem that is experienced. See [Data Collected Based on Specific Problem Types](#) on page 6.
3. Collect other useful information in case that is available within acceptable amount of time and effort. See [Other Useful Information](#) on page 8.



3 Mandatory Data

This section describes how to collect data that is mandatory for every type of problems related to the SAPC.

The data described in this chapter must always be included in a CSR.

3.1 Data Collection

To collect the required data, perform the following procedure:

Steps

1. Collect all application and platform essential data with the `sapcCollectInfo` commands script.

3.1.1 Collecting Application and Platform Logs

The `sapcCollectInfo` command script collects the essential data from the whole SAPC system, including the following:

Software repository list:

Software level running in the SAPC system.

Core MW information and SAPC logs:

Collect Core MW information.

Collect the SAPC logs, further information in Logging Events.

PMF files:

SAPC performance and measurements.

SAPC configuration files:

SAPC components configuration.

Last restore

Last System Data Restore executed.

IMM configuration

SAPC cluster configuration.

SAPC current state

Collect the log execution of `sapcHealthCheck` command script.

DBS logs files

Collect the log files of the DBS component.



DBS heap statistics

Collect the DBN record heap statistics.

Core Dump Files

Core dump files are generated when certain faults, such as segmentation faults, occur.

Stderr files

All Third Parties which are used by the SAPC give us the standard error output to a file per process.

C-diameter logs files

Collect the log files of the C-diameter component.

RMF information

SAPC cluster configuration in Resource Management Framework.

SS7 CAF information

Collect the log files of the SS7 CAF component.

Do the following to collect the previous logs:

Steps

1. Log on to the COM CLI of the SAPC as described in [System Administrator Guide](#)
2. Execute `sapcCollectInfo` as follows:

Caution!

The following command consumes high amount of storage space, in `/cluster/storage`

```
sapcadmin@SC-1:~> sudo sapcCollectInfo
```

Note: The execution of `sapcCollectInfo` takes about 5–20 minutes.

3. The command output file (`sapc_collect_info_<date>_<time>.tgz`) is located in the following folder:

`/cluster/storage`

The output of the command must be similar to the next example:

Example

```
sapcadmin@SC-1:~> sudo sapcCollectInfo
```

```
-----  
Collecting information from cluster  
-----
```




```

Collecting repository list
Collecting SwM & SwInventory information
Collecting cmw-collect-info
Logs archived in /cluster/storage/sapc_collect_info_2017-11-28_15-20-52/cmw-collect-info.tar.gz.
Collecting measurements
Collecting configuration files
Collecting information about last restore
No information about restore.
Collecting IMM configuration
Dumping current IMM state to XML file /cluster/storage/sapc_collect_info_2017-11-28_15-20-52/immdump.→
xml using XMLWriter
Collecting healthcheck information
Collecting DBS logs
Collecting DBS heap statistics
Collecting core dump information (level all)
No cores found
Collecting stderr files
Collecting C-Diameter logs
Collecting RMF information
Collecting SS7 CAF information
Information collected on file (also link 'sapc_collect_info.tgz' updated):
/cluster/storage/sapc_collect_info_2017-11-28_15-20-52.tgz
-----
Collection finished
-----

```

The size of **tgz** output file is variable, generally between 1GB-3GB.

The size of log files is generally between 100-900 MB.

For further information about the use of the command, execute it with the help switch (sudo sapcCollectInfo -h).



4 Data Collected Based on Specific Problem Types

The data described in this chapter must be included in a CSR, depending on what type of problem is experienced.

4.1 Database General Problems in the SAPC

Steps

Useful Information

1. Include any data that could be useful for the analysis of the reported problem. The possible cause of fault, abnormal behaviors detected in network, or adjacent nodes are additional useful information. More logs and information for the particular problem can be collected, according to [Troubleshooting Guide](#).

4.2 Active-Standby Geographical Redundancy Problems in the SAPC

Any problem affecting the replication in the Active-Standby Geographical Redundancy.

Steps

Data to Be Collected

1. Access to both SAPC (Active and Standby) by SSH through VIP_OAM as *sapcadmin* user and follow the instructions in [Collecting Application and Platform Logs](#) on page 3.

4.3 Active-Active Geographical Redundancy Problems in the SAPC

Any problem affecting the replication in the Active-Active Geographical Redundancy.

Steps

Data to Be Collected



1. Access to both SAPC (Preferred and Non-Preferred) by SSH through VIP_OAM as *sapcadmin* user and follow the instructions in [Collecting Application and Platform Logs](#) on page 3.

4.4 Software License Problems in the SAPC

Problem Description

Any problem related to software license installed on the License Manager.

Steps

Data to Be Collected

1. To extract the information related to installed software license, follow the procedure described in [View License Information](#).
2. To activate and collect LM Traces, follow [Enabling LM Trace](#) section, in [LM Troubleshooting Guideline](#).



5 Other Useful Information

The data described in this chapter could be included in a CSR, depending on what type of problem is experienced and within acceptable amount of time and effort.

5.1 Performance Data Collector Reports

PDC collects performance information from the SAPC regularly and generates reports. PDC could also be used on demand without having to wait scheduled daily or monthly planned execution. There are three main types of reports: daily logs, monthly packages, and specific health check snapshots.

5.1.1 Daily Report

PDC *collect* operation gets the information from PMF files and creates the daily reports. Include any data that could be useful for the analysis of the reported problem. More information could be read at [Performance Data Collection](#).

5.1.2 Monthly Report

PDC *package* operation gets the information from daily reports and creates a monthly *tar.gz* file. More information could be read at [Performance Data Collection](#).

5.1.3 Health Check Report

PDC *healthcheck* operation compiles the SAPC health check information into an XML report. More information could be read at [Performance Data Collection](#).



6 Appendix A: Severity/Priority

The correct priority ensures that critical problems are fixed before less critical problems, therefore it is crucial to apply the following guidelines. It is important to observe that for an Emergency and High priority CSR that requires immediate attention, First Line Support (FLS) has to call the Global Front Office when the fault is present. Another important point related to CSR priority is that when the priority is not clear for both parts (FLS and Second Line Support (SLS)), they have to discuss it and get an agreement defining a common priority from start. The FLS can increase priority owing to commercial reasons at any time.

Note: If a discrepancy exists between the definition of Severity (Emergency/ High/Medium/Low) in this document and the WLA/SLA agreed upon by the customer and Ericsson, the latest takes precedence.

— Severity Emergency

Emergency call, severe impact on critical End Customer or on many customers, affecting network operation both technically and economically, requires immediate emergency action. Severe faults are affecting the total network operation, system functionality, or security affecting the reliability of the service. Commercial and economical impact or both, for example, no charging or traffic handling or both.

This must be logged as an Emergency CSR in SMS and followed by a phone call to the Global Front Office. If there is an emergency situation, all parties work actively until the system is in service or the emergency situation has a preliminary solution acceptable to the customer.

Emergency faults are the following:

- More than 30% of traffic failures continuously taking place.

— Severity High:

A severe fault or disturbance affecting a specific area of functionality, but not the whole system. For example, a certain function is disabled, is giving incorrect results or is not acting according to the specifications. When Operation and Maintenance are inaccessible, system security is malfunctioning but not deemed at risk, issues of commercial and / or financial impacts are also recognized as high severity.

High severity fault is the following:

- More than 30% of traffic failures on a single occasion.

— Severity Medium:

Medium severity problems have minor customer impact and thus require lower priority action. These faults have minor impact on the functionality of



the product, for example single units blocked with small traffic disturbance, display errors and failures that cause handling errors.

Medium severity faults are the following:

- Less than 30% of traffic failures.
- Malfunctioning but without end-user impact.

— Severity Low:

The SLS is accessed to get general consultation. This inquiry not has to be related to any fault in the End-Customers network / Network Elements.

Low Severity faults are the following:

- Missing information.
- Configuration matters.