IBM Security zSecure Service Stream Enhancement for IBM Operations Analytics for z Systems (IOAz)

Documentation updates

IBM Security zSecure Service Stream Enhancement for IBM Operations Analytics for z Systems (IOAz)

Documentation updates

Chapter 1. About this document

This document lists updates to the IBM® Security zSecure™ documentation as a result of the Service Stream Enhancement (SSE) for IBM Operations Analytics for z Systems (IOAz) - APAR OA52273. All updates apply to IBM Security zSecure Version 2.2.1.

The following IBM Security zSecure publications for V2.2.1 were updated:

zSecure CARLa-Driven Components Installation and Deployment Guide
: Chapter 10. Setup of zSecure Admin Access Monitor was updated.

zSecure Admin and Audit for RACF User Reference Manual
: Chapter 10. RACF Access Monitor: the introduction was updated.

zSecure Messages Guide
: Several messages were added.

Note: Referenced topics that have not changed are not included in this document. You can find them in the publication that the chapter applies to.

Chapter 2. *IBM Security zSecure CARLa-Driven Components Installation and Deployment Guide*

This chapter lists the documentation updates for the *zSecure CARLa-Driven Components Installation and Deployment Guide* as a result of the SSE for IOAz enhancements.

Chapter 10. Setup of zSecure Admin Access Monitor was updated:

- Section "Installation and post-installation requirements": a bullet was added.
- Section "Definition of security resources and permissions": a bullet was added.
- Section "Optional customization for analytics preprocessing" was added.
- Section: "DEBUG command": the syntax was updated
- Section: "REPORT command": the syntax was updated

"Installation and post-installation requirements"

The following bullet was added:

- If you want to use an analytics application, for example IBM Operations Analytics for z Systems (IOAz), to report about events that zSecure Access Monitor collects, you must perform additional configuration steps. These are described in section "Optional customization for analytics preprocessing".

"Definition of security resources and permissions"

The following bullet was added:

- If you are activating analytics preprocessing, ensure that the started task user ID has authorization to create and remove files from the specified analytics directory. Also, the started task user ID must have at least read access to the input files that are specified in the analytics configuration member C2PAMANC.

"Optional customization for analytics preprocessing" (new)

zSecure Access Monitor can provide preprocessed access records for use by an analytics product like IBM Operations Analytics for z Systems (IOAz). The records are saved in a UNIX file and can be retrieved by one of the Analytics components. To enable this process, several additional steps have to be performed.

To enable zSecure Access Monitor to provide preprocessed access records, perform the following customization steps:

- Define a UNIX directory where Access Monitor can store the files. The started task user ID must have sufficient authority to create and remove files in this directory.
- Specify analytics keywords and parameters in the Access Monitor configuration member.
- Configure your analytics application to retrieve records from the UNIX work directory.

Prepare a directory for storing analytics data

The analytics data is saved as a CSV file. These CSV files are kept for the specified number of days and then automatically removed (default is 5 days). The directory must have sufficient space to store the summarized access data. On average, the amount of disk space required for each day is 50% of the disk space of the daily collection data sets that are specified through C2PAMCLT.

If you run Access Monitor on multiple systems and use a shared USS file system, you must specify a dedicated directory for each system. In the Access Monitor configuration file, you can use system symbols in the name of the specified USS directory. System symbols must be specified in uppercase for correct substitution.

Like any UNIX directory, the directory must have both an owning user and an owning group. It is easiest to assign the user ID and group of the C2PACMON started task as the owner of this directory. You might want to create a dedicated USS file system for this directory and use an automount policy. The following is an example UNIX command to create the work directory:

```
mkdir -m 750 /u/c2pacmon
```

To specify the owner, you can use a command that is similar to the following example:

```
chown c2psuser:sysaudit /u/c2pacmon
```

If you specify a different user or group as owner, ensure that the C2PACMON started task user ID has sufficient authority to create and remove files in the specified directory.

Update C2PACMON configuration files

When you have created the directory for the analytics files, update the C2PACMON configuration members. There are two members that must be changed:

- Copy member C2PAMANC from SCKRCARL to your Access Monitor configuration data set (as indicated by symbol C2PACPRM in your CKRPARM member). The C2PAMANC member contains the CARLa specification of the RACF input source and the name of a daily refreshed CKFREEZE data set. For more information about the daily CKFREEZE data set, see section “Use of a fresh CKFREEZE and UNLOAD each day” in Chapter 8. Setup for production. During an initial install, member C2PAMANC is copied to the CKRPARM data set as part of job CKRZPOST.
- Member C2PAMP (or the one indicated by parameter PPARM in the C2PACMON procedure) must contain statements to activate and configure the analytics file creation process. Activation is through the use of the `ANALYTICS` keyword on the `REPORT` statement. Configuration can be done through the specification of sub-keywords and parameters on the `ANALYTICS` keyword. For more information on the syntax of the `REPORT` statement, see section “Configuration commands”.

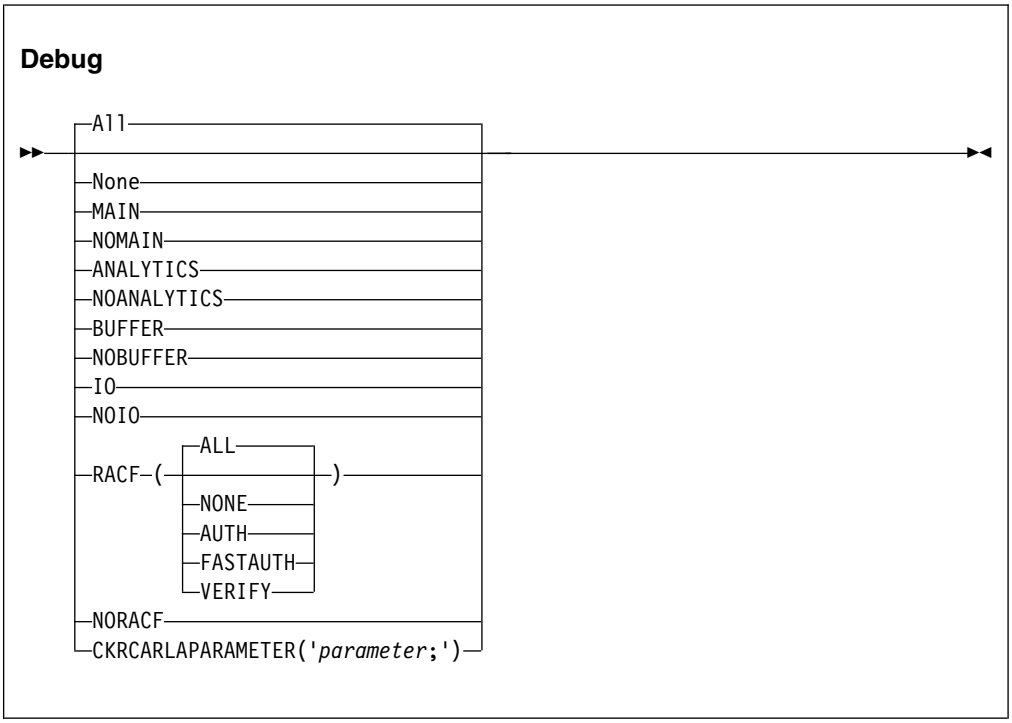
Configure CDP to retrieve and forward data to IOAz

IBM Operations Analytics for z Systems (IOAz) uses its Common Data Provider (CDP) component to retrieve records from the z/OS UNIX log files. The CDP component must be configured to identify the directory where the files are located, and the naming pattern for the files.

The naming pattern of the CSV files created by zSecure Access Monitor is `/u/c2pacmon/AccMon.D??????.T????.csv`, where */u/c2pacmon* is the directory name that is specified in the C2PAMP configuration member.

"DEBUG command"

The syntax was updated:



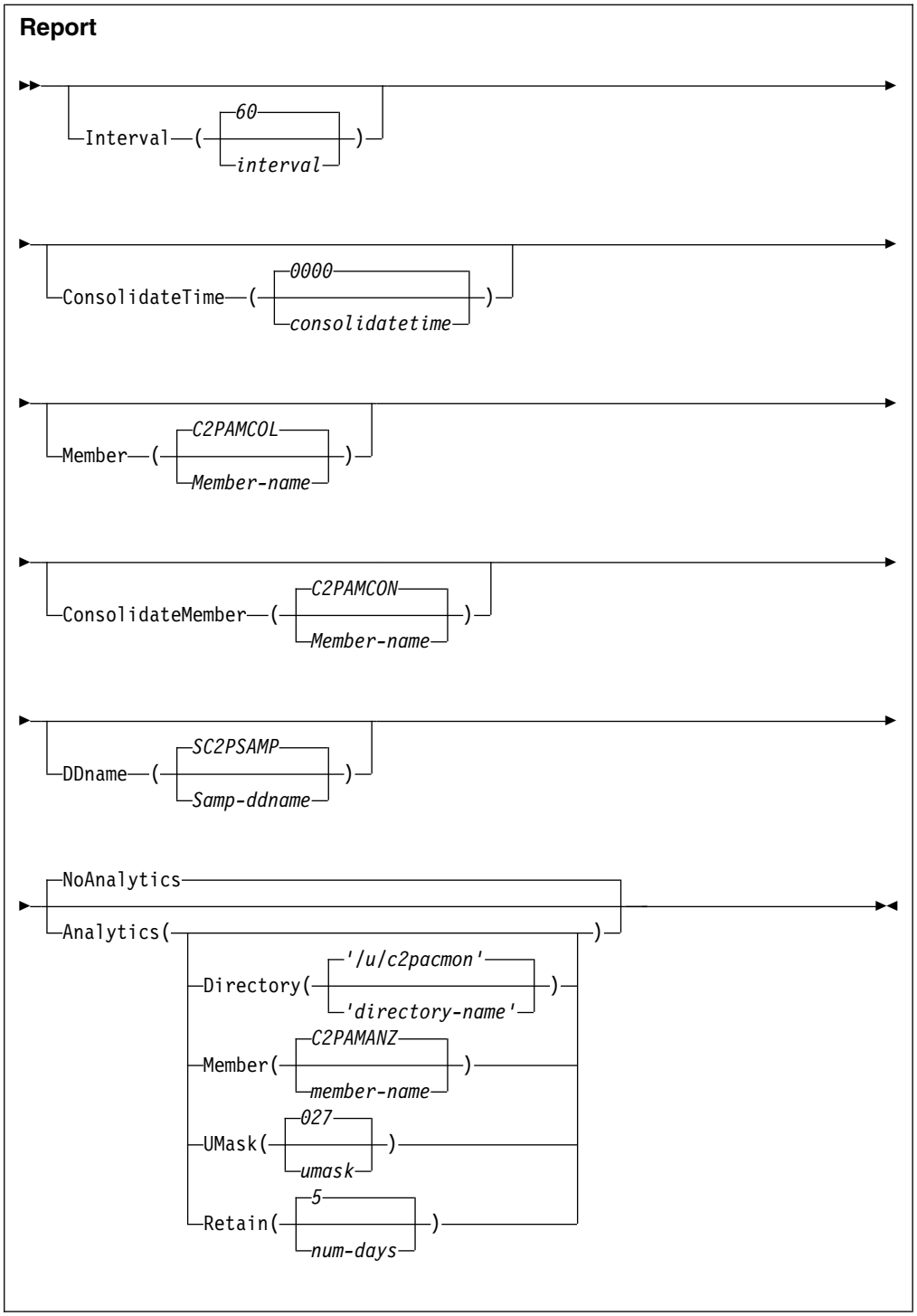
The following descriptions were added:

ANALYTICS
Write diagnostic messages related to analytics file processing to the console.

NOANALYTICS
Do not write diagnostic messages related to analytics file processing to the console.

"REPORT command"

The syntax was updated:



The following descriptions were added:

Analytics

Specifies that a daily file with statistical information is created. This daily file is intended for further processing by an analytics program like IBM Operations Analytics for z Systems (IOAz). Specifying this keyword on the REPORT statements activates this support using default parameters. You can

override these defaults by specifying one or more of the following keywords. You can repeat the `REPORT ANALYTICS` statement as often as needed to specify all four keywords.

Directory
Specifies the z/OS UNIX directory where the prepared files are stored. The C2PACMON started task user ID must have sufficient authority to create and remove files in this directory. The directory that you specify must be entered between quotes. It must start with a slash ("/") and not end with a slash. If you are sharing the C2PACMON configuration file between systems, you must ensure that every C2PACMON started task uses a different directory. You can use system symbols in the directory name, for example `&SYSCLONE`. System symbols must always be specified in uppercase.

Note: The configuration statements do no support continuation lines. You can abbreviate keywords using the normal TSO conventions (for example abbreviate DIRECTORY to Dir).

If you do not specify a value, the default directory name is **/u/c2pacmon**.

Member
Specifies the CARLa member that contains the statements to process the access records in a format that is suitable for use by an analytics program. The default member C2PAMANZ is supplied in the SCKRCARL data set. It imbeds member C2PAMANC that must be configured before use. Member C2PAMANC is contained in the data set that is indicated by symbol C2PACPRM in your CKRPARM member.

UMask
Specifies the UMASK that is in effect when creating new files in the specified directory. The default value 027 resets write access for the group and resets all access for other users.

Retain Specifies the number of days that the analytics files are retained before being deleted automatically. The specified value must be in the range of 2 to 99 days. The default value (5) allows several days for the analytics product to pick up the files. Expiration of files is automatic and based on the date and time stamp in the file name.

Chapter 3. *IBM Security zSecure Admin and Audit for RACF User Reference Manual*

This chapter lists the documentation update for the *zSecure Admin and Audit for RACF User Reference Manual* as a result of the SSE for IOAz enhancements.

The following information was added for the introduction for Chapter 10. RACF Access Monitor:

zSecure Access Monitor can provide preprocessed access records for use by an analytics product like IBM Operations Analytics for z Systems (IOAz). The records are saved in a UNIX file and can be retrieved by one of the analytics components. To enable this process, several configuration steps must be performed. For more information about required configuration, see section "Optional customization for analytics preprocessing" in *zSecure CARLa-Driven Components Installation and Deployment Guide*.

Chapter 4. *IBM Security zSecure Messages Guide*

This chapter lists the documentation updates for the *zSecure Messages Guide* as a result of the SSE for IOAz enhancements.

The following messages were added:

C2P0340I Access Monitor prepares files for Analytics processing

Explanation: This message is part of the response to the console operator `DISPLAY` command. It indicates that the collected access records are preprocessed for use by an analytics application.

C2P0341I Analytics CARLa member is *member-name*

Explanation: This message is part of the response to the console operator `DISPLAY` command. It shows the member name that contains the CARLa statements that are used to create the analytics files.

C2P0342I Analytics directory is *directory-name*

Explanation: This message is part of the response to the console operator `DISPLAY` command. It shows the directory name that is used to store the analytics files.

C2P0343I Analytics file umask is *umask*

Explanation: This message is part of the response to the console operator `DISPLAY` command. It shows the umask that is in effect when creating the analytics files.

C2P0344I Analytics file retention is *num-days* **days**

Explanation: This message is part of the response to the console operator `DISPLAY` command. It shows the number of days that the analytics files are saved until they are automatically removed.

C2P0496I Debug Analytics is activated

Explanation: This debug-only message is issued to indicate that special diagnostic messages that are related to the processing of analytics files are issued.

C2P0497I Debug Analytics is deactivated

Explanation: This debug-only message is issued to indicate that special diagnostic messages that are related to the processing of analytics files are not issued.

C2P0498E Unlink failed rv=*return_value* **rc=***return-code* **rs=***reason-code*

Explanation: Expiration of the Analytics directory failed because an error occurred during the BPX1UNL service. Check the BPX1UNL return-code and reason-code why the unlink failed. This message is followed by message C2P0499I showing the file that could not be deleted.

System action: Execution continues, but files in the output directory are not deleted.

C2P0499I *path-name*

Explanation: This message is a continuation of message C2P0498E. It shows the path name of the file that could not be deleted.

C2P0529E Open dir failed rv=*return_value* **rc=***return-code* **rs=***reason-code*

Explanation: Expiration of the analytics directory failed because the directory could not be opened.

System action: Execution continues, but files in the output directory are not deleted.

User response: Check the BPX1OPD *return-code* and *reason-code* to see why opening failed.

C2P0530I Analytics CARLa member is *member-name*

Explanation: This debug-only message is issued to confirm the member name that is specified for the analytics CARLa.

C2P0531E Invalid analytics directory *directory-name*

Explanation: The specified directory name does not adhere to the documented restrictions. It must start with a slash (/) and cannot end with a slash.

C2P0532I Using default analytics directory /u/c2pacmon

Explanation: An invalid directory name was specified. Therefore, the default directory `/u/c2pacmon` is used.

C2P0533I Analytics directory is *directory-name*

Explanation: This debug-only message is issued to

confirm the directory name that is specified for the analytics files.

C2P0534I Analytics umask is *umask*

Explanation: This debug-only message is issued to confirm the umask in effect when creating the analytics files.

C2P0535I Analytics file retention period is *num-days* **days**

Explanation: This debug-only message is issued to confirm the number of days that analytics files are kept until they are automatically removed.

C2P0536I Invalid analytics file retention period, using default value 5 days

Explanation: The retention period that is specified is either too small or too large. The default retention period of five days is used instead.

C2P0537I Expired analytics file *file-name*

Explanation: This debug-only message is issued to indicate that the analytics output file *file_name* is expired and has been deleted.

Printed in USA