CorreLog SIEM Agent for z/OS

Installation and Operation

http://www.correlog.com info@correlog.com

CorreLog SIEM Agent for z/OS
Installation and Operation

See also Appendix A: Notices.

Table of Contents

Section 1: Introduction

This manual provides instructions for installing and operating the CorreLog SIEM Agent for z/OS software.

The mainframe Agent program (The Agent) is installed and executes in one or more mainframe LPARs[1], and continuously monitors mainframe SMF activity. The Agent reformats specified SMF records and forwards them as Syslog[2] messages to a standard Syslog server or console[3] of the customer's choice.

[1] LPAR, pronounced "EL-par," means "logical partition," basically a virtualized mainframe. If you are not familiar with mainframes you may read LPAR simply to mean "mainframe."

[2] The Syslog protocol is a standard for logging messages from computers and similar devices. It was invented in the 1980s by Eric Allman and is the subject of Internet Engineering Task Force (IETF) RFC 3164 and subsequent RFCs. See http://en.wikipedia.org/wiki/Syslog. The text of the RFC is here http://www.ietf.org/rfc/rfc3164.txt.

[3] The correct RFC 3164 term is Syslog *collector*.

Note that the traditional mainframe use of the term Syslog or SYSLOG refers familiarly to z/OS console message facilities in general, or more properly to "a data set residing in the primary job entry subsystem's spool space … used by application and system programmers to record communications about problem programs and system functions."[4] This manual however uses the term Syslog to refer to the message streams traditionally produced by UNIX systems, routers, and the like, and documented in IETF RFC 3164 and subsequent RFCs. See **Syslog Messages** below.

The Agent's use is not limited to the CorreLog Syslog Server, and there is no mainframe-agent-specific software that must be installed on the CorreLog Windows Syslog server, or any other Syslog console or "intermediate" machine.

The Agent package includes a z/OS program called CZASEND. CZASEND may be used – typically in a batch (JCL) job – to a send text of the user's choice as a Syslog message. CZASEND operates independently of the Agent, although it is intended to share the Agent's parameter file. In fact, you can use CZASEND even if you do not use the Agent.

This manual is intended for system administrators responsible for installing the software components on the Mainframe platform. This information will also be of interest to program developers and administrators who want to extend the range of their Syslog console's role within an enterprise to include z/OS events.

For information on features of the CorreLog server, refer to the "CorreLog User Reference Manual", which is provided as embedded document in all versions of the CorreLog system, or visit our Web site at www.CorreLog.com.

Technical Support – Contacting CorreLog

To contact CorreLog for technical support, please call 1-800-CORRELOG (1-800-267-7356) and press 2, or send an e-mail to support@CorreLog.com.

CorreLog z/OS Agent Overview

Generally speaking Syslog consoles, including the CorreLog server, monitor Syslog and/or SNMP trap messages sent by managed devices. Syslog messages are generally sent by UNIX systems, routers, and many other computer and computer-like systems.

[4] *MVS Planning: Operations*, © 1988, 2008 International Business Machines Corporation.

However, traditional (non-UNIX) z/OS (like Microsoft Windows!) has no “built-in” component that transmits standard Syslog messages. In order to monitor mainframe events, in particular events from z/OS System Management Facilities (SMF), the Agent must be installed as described in this manual.

System Management Facilities (SMF) is a standard component of z/OS that collects data on system activities, and is typically used for accounting, security, and performance monitoring. SMF records are collected by the Agent program and transmitted via UDP/IP (IPv4 or IPv6) to the CorreLog Server or the Syslog console of the customer’s choice. The Agent program operates by installing a z/OS “installation exit” that monitors z/OS system exits IEFU83, IEFU84, and IEFU85. (See the IBM manual “z/OS MVS Installation Exits.”)

The steps in the installation of the Agent are detailed in Section 2 of this manual. The Agent includes extensive facilities to specify which SMF records are forwarded as Syslog messages, and how they are to be formatted before forwarding. Customization of CZAGENT is described in Section 3 of this manual. The parameter file that is used to specify configuration options is described in detail in **Parameter File Reference** in "CorreLog SIEM Agent for z/OS Configuration Reference."

dbDefender for DB2

dbDefender for DB2 is an optional feature of the CorreLog Agent for z/OS that automatically captures IBM DB2 events that must be monitored for PCI DSS and similar regulatory compliance. dbDefender is described primarily in the following sections of this manual: **PCI DSS and Other Regulatory Standards**, **The SMF DB2 Statement**, and **DB2 Traces for Database Access Monitoring** in "CorreLog SIEM Agent for z/OS Configuration Reference."

dbDefender supports DB2 Version 9.1, DB2 10 and DB2 11.

PCI DSS[5] and Other Regulatory Standards

The Agent may be used as part of a compliance program for PCI DSS, Sarbanes-Oxley, HIPAA, Graham-Leach-Bliley, IRS Publication 1075, and/or FISMA. All of these regulatory standards are concerned with the integrity and security of data, and the Agent may be used to audit file and database access.

[5] The Payment Card Industry Data Security Standard. See https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

The following are some of the activities that must be audited under one or more of these regulatory standards, and the associated the Agent facility. These sorts of capabilities are sometimes called Database Activity Monitoring or File Integrity Monitoring. In the following descriptions, “SMF 42” refers to the SMF 42 statement: see **The SMF 42 Statement**; “SMF 80” refers to the SMF 80 statement: see **The SMF 80 Statement**; “SMF DB2” refers to the SMF DB2 statement: see **The SMF DB2 Statement** all in **Parameter File Reference** in "CorreLog SIEM Agent for z/OS Configuration Reference;" and **DB2 Traces for Database Access Monitoring**, also in "CorreLog SIEM Agent for z/OS Configuration Reference."

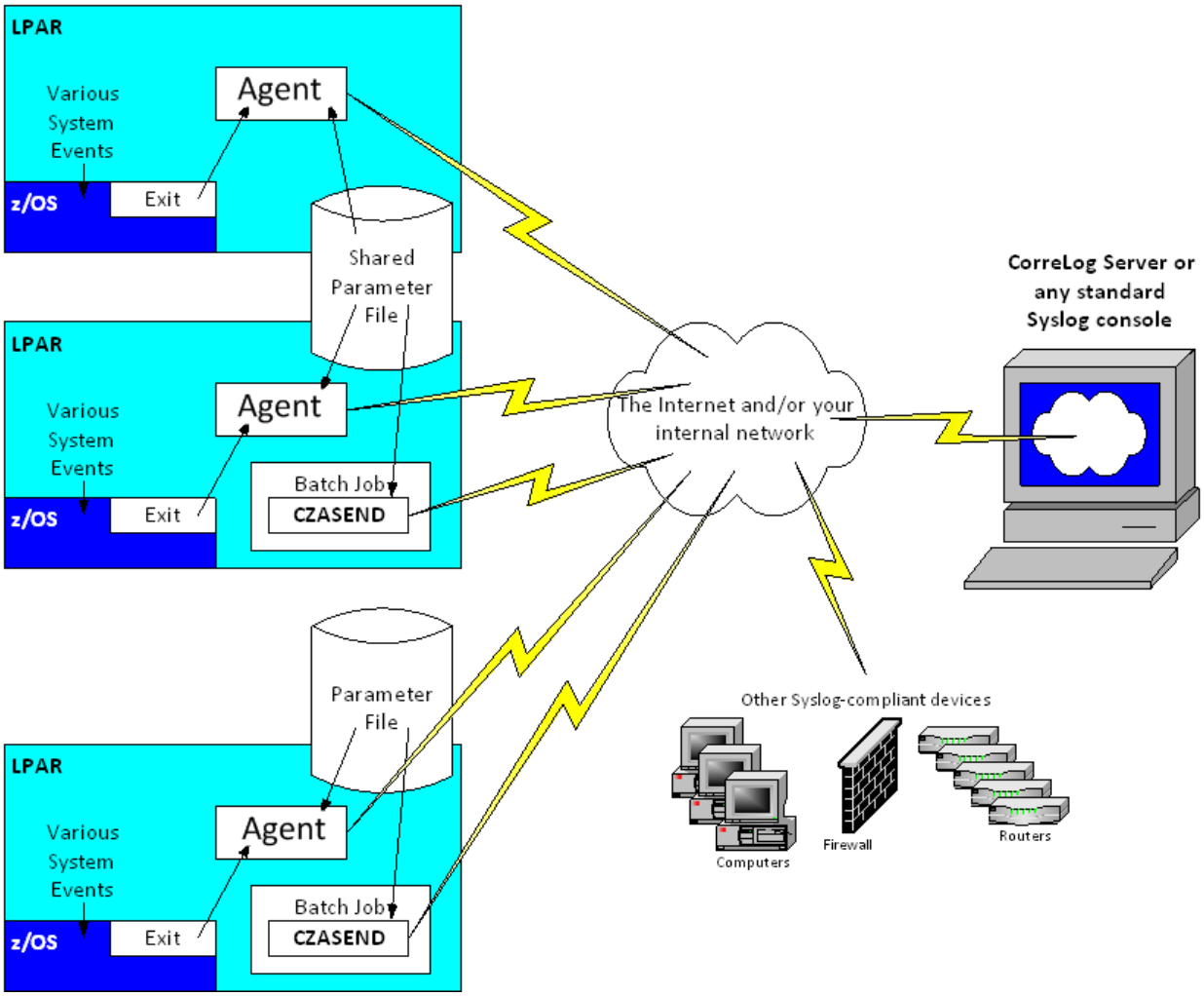
- Privileged User Monitoring: SMF DB2 IFCID(361)
- Invalid Logical Access Attempts: SMF 80 and SMF DB2 IFCID(140)
- Creation and Deletion of System Level Objects: SMF DB2 IFCID(97)
- Data Access: SMF 80 EVENT(.0) and SMF DB2 IFCID(143 144 145). Specify AUDIT(ALL) for the appropriate RACF dataset profiles.
- File Integrity: SMF 42 and SFM 80 EVENT(.0). SMF 42 can potentially notify you of changes to system libraries. Specify AUDIT(ALL(UPDATE)) for the appropriate RACF dataset profiles.
- Backup and Recovery: SMF DB2 IFCID(24 25)

z/OS Security Products

There are three commonly used z/OS security products: RACF, CA ACF2, and CA Top Secret. RACF (Resource Access Control Facility), properly the IBM z/OS Security Server RACF, is a product of IBM. CA ACF2 and CA Top Secret are products of CA Technologies (formerly Computer Associates). All provide roughly comparable security services, and all write roughly comparable SMF records. The Agent supports all three security products.

System Block Diagram

The relationships among the various parts of the CorreLog SIEM Agent for z/OS software are depicted in the diagram below.



- The Agent program installs a z/OS “installation exit” program on each z/OS LPAR on which it is run. It reformats SMF records as standard Syslog messages and sends them via your IP network to a CorreLog server or any standard Syslog console.
- The CZASEND program may optionally be used in any batch job, or called from your programs, to send custom Syslog messages to your Syslog console.
- The Parameter File contains various parameters used by the Agent and CZASEND, such as the IP address of the Syslog console.

How to Use This Manual

- **Section 2: Installation** should be used to install your CorreLog SIEM Agent software on one or more z/OS LPARs.

- **Section 3: Configuration** describes how to configure your CorreLog SIEM Agent software initially, and includes procedures for testing as you go along.
- **Section 4: Agent Operation** describes how to set up the Agent in your z/OS system.
- **Section 5: CZASEND Operation** describes how to use the CZASEND program from your batch jobs or from within your installation's COBOL or other programs to send custom Syslog messages to your Syslog console.

Section 2: Installation

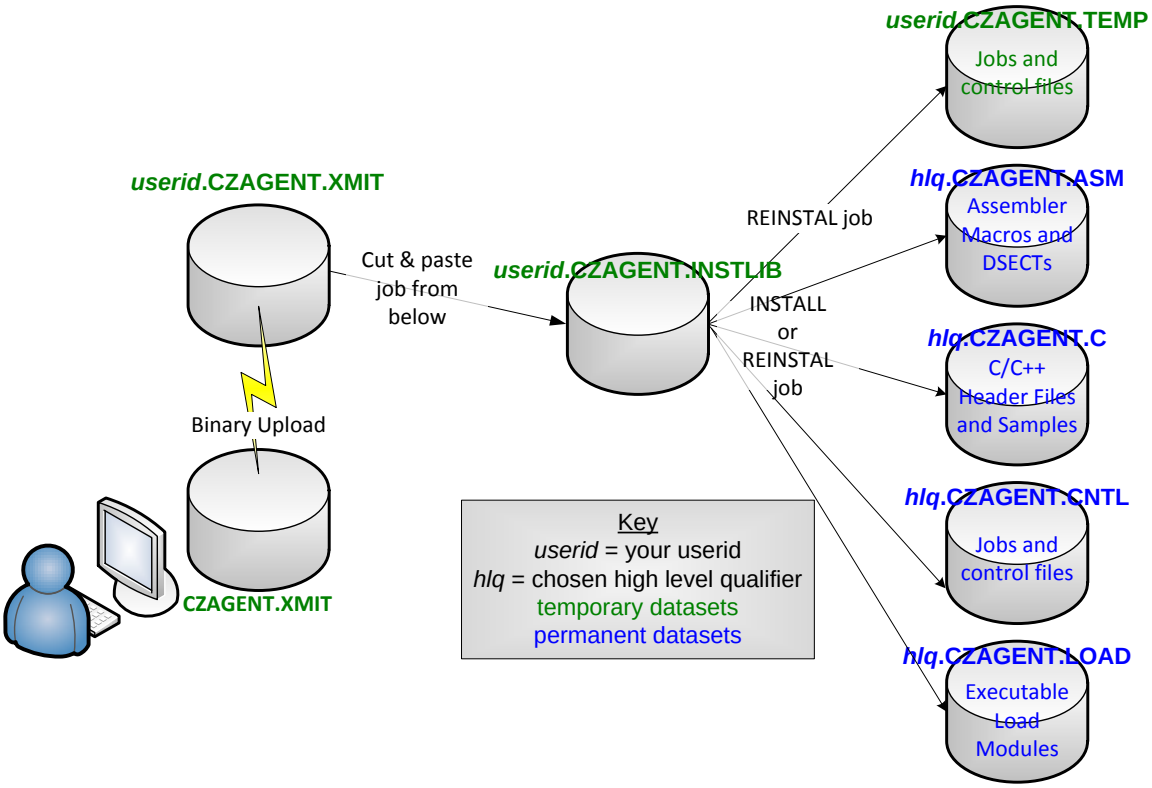
Re-Installation Considerations

If you are re-installing the Agent, such as after receiving a new release from CorreLog, you may skip the Planning step below and proceed directly to Installation Steps. *Re-installation as directed below will not over-write your customized control files.* If you are re-installing the Agent over a production installation you may wish to consider the RUNMODE=TEST parameter of START, documented under **The Start or S Command**.

Planning

You must decide on a high-level qualifier (HLQ) for the Agent datasets. This is the highest-level node name under which the Agent datasets will be cataloged on your LPAR. If you are not familiar with your installation's cataloging requirements then you may wish to consult someone who is. *You must have the access rights to write to datasets with your chosen HLQ*. If you wish to defer this decision then you can simply use your TSO userid initially; there are no conflicts in dataset names if *hlq* is the same as *userid*. From this point forward we will refer to this node name as *hlq*.

Installation Overview



Installation Steps

The CorreLog SIEM Agent for z/OS Package is delivered as a compressed or "zip" file. The installation is a fairly typical non-SMP/E software installation. The installation steps are as follows:

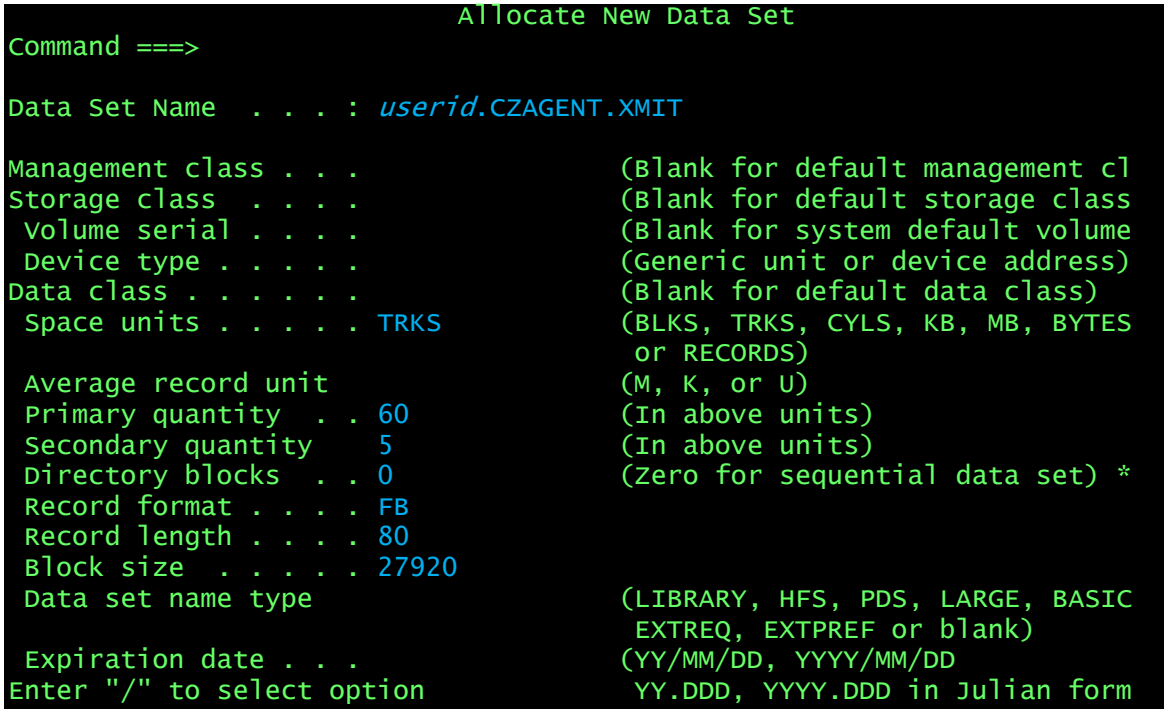
Obtain the installation package from your CorreLog salesperson or as directed by CorreLog support.

If you will be using the Agent and not just CZASEND obtain a LICENSE statement from your CorreLog salesperson.

On a Windows or other platform with ".zip" support right-click on the file and extract the components to a folder of your choice.

Sign on to the mainframe LPAR on which you will be testing. The remainder of this discussion assumes you will be using TSO and ISPF. Allocate a sequential dataset with an FB record format, a record length of 80, and any legal blocksize (an even multiple of 80 no more than 32720). Name it *userid*.CZAGENT.XMIT where *userid* is your TSO user ID. (It is a temporary file and will be deleted in a

later step.) The following screen shows how you might do this with ISPF function 3.2. *Note that you must pre-allocate this file as described; you must not let FTP or 3270 file transfer allocate the file with default characteristics.*



Using FTP or 3270 file transfer, upload the file CZAGENT.XMIT from the folder where you unzipped it to *userid*.CZAGENT.XMIT (the dataset you just created in the preceding step). *You must select a binary upload.*

Copy and paste the following JCL into an ISPF editor. (If you have trouble pasting into your 3270 emulator from a PDF the file is also available with the unzipped files from the step above as InitialJCL.txt.) Edit the job statement to conform to your installation's standards. Submit the job. It should run to a completion code of zero. If it does not, resolve the error and re-submit the job. If you cannot resolve the error, call CorreLog for technical support.

```
//useridR    JOB   ,'CZAGENT Install',
//    MSGCLASS=H,NOTIFY=&SYSUID,CLASS=A,REGION=0M
//RECEIVE  EXEC PGM=IKJEFT01,DYNAMNBR=10
//SYSPRINT DD   SYSOUT=*
//SYSTSPRT DD   SYSOUT=*
//SYSTSIN  DD   *
 RECEIVE INDSNAME(CZAGENT.XMIT)
 DATASET(CZAGENT.INSTLIB)
/*
```

You may now delete *userid*.CZAGENT.XMIT if you wish.

If this is an initial installation, then edit *userid*.CZAGENT.INSTLIB(INSTALL). If this is a re-installation, then edit *hlq*.CZAGENT.CNTL(REINSTAL). If necessary edit the job statement to conform to your installation's standards and change all *userid* to your user ID and all *hlq* to your chosen high-level qualifier. Submit the job. *Exit from the editor.* It should run to a completion code of zero. If it does not, resolve the error and re-submit the job. If you cannot resolve the error, call CorreLog for technical support.

> Note that because of how TSO ENQs datasets the job will probably not run unless you exit from the editor.

You may now delete *userid*.CZAGENT.INSTLIB if you wish.

The REINSTAL job will not overwrite your exiting *hlq*.CZAGENT.CNTL members (which you may have edited to customize the Agent). However in some circumstances certain modifications may be necessary or advisable in order to accommodate or take advantage of new Agent features. You may be advised in an installation memo to inspect certain members of userid.CZAGENT.TEMP and possibly merge certain statements into your existing members. If not, or when you have completed that task, you may delete *userid.*CZAGENT.TEMP if you wish.

The installation of the Agent software is complete. You should now move on to **Section3: Configuration.**

Section 3: Configuration

Planning for Configuration

You must know the IP address of your CorreLog server or other Syslog console (and the port address if it is not the standard 514). *The software will not work at all if you do not specify this address correctly. If you are not sure of the IP address of your Syslog console, you will save yourself a lot of headaches if you determine the correct address before proceeding*.

Your CorreLog server or other Syslog console must actually be running. You should have access to (be able to look at) the captured Syslog messages or have access to someone who does.

If you are planning to utilize the full agent (as opposed to only CZASEND) then you must have the authority to APF-authorize[6] a dataset, or have access to someone who does. You will not be able to finish testing the Agent without APF authorization. You will also need the authority to add cataloged procedures to your SYS1.PROCLIB concatenation, and you may need the authority to update members of your SYS1.PARMLIB concatenation, or have access to someone who does.

[6] The Authorized Program Facility (APF) is a facility of z/OS that allows installations to identify datasets that contain system or user programs that potentially can use sensitive system functions. APF is described in the IBM publications "z/OS MVS Initialization and Tuning Reference" and "z/OS MVS Programming: Authorized Assembler Services Guide."

If you will be testing the Agent you must have the authority to issue z/OS console commands, or have access to someone who does. To determine if you have this authority go to SDSF (any panel) and type **`/D IPLINFO`**. If you receive about ten lines of response detailing the last IPL then you have the authority to issue console commands. If you receive an error message then you do not.

Tailoring the Installation for a Proprietary Syslog Extension

ArcSight CEF

If you will be using the Agent and/or CZASEND with ArcSight CEF, begin your testing by tailoring the following members of *hlq*.CZAGENT.CNTL (where *hlq* is the "high level qualifier" chosen during installation) as indicated in the table below. (To "comment out" a line, type an asterisk in column 3 so the line begins //*; to uncomment a line, remove the asterisk in column 3 so the line begins with // and a blank.)

Member	Comment out	Uncomment
CZAGENT	`//  PARMS=CZAPARMS`	`//* PARMS=CZAPCEF`
CZAGNJOB	`//  SET  PRMS=CZAPARMS`	`//* SET  PRMS=CZAPCEF`
CZASEND	`//  SET  PRMS=CZAPARMS`	`//* SET  PRMS=CZAPCEF`

IBM Security QRadar

If you will be using the Agent and/or CZASEND with IBM Security QRadar, begin your testing by tailoring the following members of *hlq*.CZAGENT.CNTL (where *hlq* is the "high level qualifier" chosen during installation) as indicated in the table below. (To "comment out" a line, type an asterisk in column 3 so the line begins //*; to uncomment a line, remove the asterisk in column 3 so the line begins with // and a blank.)

Member	Comment out	Uncomment
CZAGENT	`//  PARMS=CZAPARMS`	`//* PARMS=CZAPLEEF`
CZAGNJOB	`//  SET  PRMS=CZAPARMS`	`//* SET  PRMS=CZAPLEEF`
CZASEND	`//  SET  PRMS=CZAPARMS`	`//* SET  PRMS=CZAPLEEF`

QRadar should automatically discover and create a log source for the Agent. Follow the instructions in the IBM manual "IBM Security QRadar DSM

Configuration Guide" under the section "CorreLog Agent for z/OS." You should be able to find this publication at www.ibm.com/support.

Splunk

If you will be using the Agent and/or CZASEND with Splunk, begin your testing by tailoring the following members of *hlq*.CZAGENT.CNTL (where *hlq* is the "high level qualifier" chosen during installation) as indicated in the table below. (To "comment out" a line, type an asterisk in column 3 so the line begins //*; to uncomment a line, remove the asterisk in column 3 so the line begins with // and a blank.)

Member	Comment out	Uncomment
CZAGENT	`//  PARMS=CZAPARMS`	`//*  PARMS=CZAPSPLN`
CZAGNJOB	`//  SET  PRMS=CZAPARMS`	`//*  SET  PRMS=CZAPSPLN`
CZASEND	`//  SET  PRMS=CZAPARMS`	`//*  SET  PRMS=CZAPSPLN`

Fields Definitions Files

Most of the Agent's SMF record type and field definitions are read from an external schema called the Fields Definitions Files. Modifying these files is an advanced topic; most customers have no need to modify them. They are documented in a separate CorreLog Agent manual, "Defining Your Own Fields." The main Fields Definitions file may be specified on Agent startup and defaults to the CZDEFINE member of the dataset defined by the CZAPARMS DD statement.

Parameter File

The parameter file is normally the CZAPARMS member of the *hlq*.CZAGENT.CNTL dataset (where *hlq* is the "high level qualifier" you specified during installation). For ArcSight CEF compatibility, use the member CZAPCEF. For IBM QRadar compatibility, use the member CZAPLEEF. For Splunk integration, use the member CZAPSPLN. For IBM QRadar compatibility, use the member CZAPLEEF. The changes to do so are described in the section above.

However, you may have multiple parameter files of whatever z/OS-legal names you choose. The parameter file for CZASEND is specified with the CZAPARMS DD statement. The parameter file for the Agent is specified with the CZAPARMS DD statement and the START or MODIFY command. CorreLog recommends

that you use the single parameter file member named CZAPARMS, CZAPCEF, CZAPLEEF or CZAPSPLN until you become familiar with the software.

You will need to customize the SERVER statement in the parameter file. You will also need to insert a LICENSE statement supplied by CorreLog, and you may wish to configure the events to be forwarded with SELECT. All of these steps are detailed immediately below. You should probably leave the other statements of the supplied parameter file as-is until you become more familiar with the software, at which point you should refer to **Parameter File Reference** in "CorreLog SIEM Agent for z/OS Configuration Reference."

Configuring the Syslog Server Address

You must at a minimum edit the parameter file and specify the IP address of the Syslog console or CorreLog server. You must also specify the IP port number if it is not the standard Syslog default, port 514. The IP address and optional port are specified on the SERVER statement in the parameter file as a hostname or in standard IPv4 “dotted” format, for example

```
SERVER   123.48.0.160
```

or

```
SERVER   serverx.ourshop.com:10514
```

(Parameter file statements are free format. You may use any reasonable number of spaces between the word SERVER and the IP address. The IP address and optional port must be punctuated as shown with no embedded blanks.)

Configuring Your Required Events with SELECT

The parameter files supplied by CorreLog configure, by default, a large number of event types: security events, operational events, file integrity events, and so forth. Your installation may want to forward all of those events to your SIEM, or it may not. You can easily control which types of events are formatted and forwarded by the Agent by commenting or uncommenting the SELECT statements near the top of the parameter file. Near the top of the parameter file you will see several lines similar to the following:

```
  SELECT SMF(80 ACF2)              ; Security events
; SELECT SMF(30 119)               ; TSO signon events
; SELECT SMF(15 42 64)             ; File integrity events
  SELECT SMF(14 15 30 42 64)       ; Operational events
; SELECT SMF(110)                  ; CICS events
; SELECT SMF(119)                  ; TCP/IP Events
; SELECT SMF(DB2)                  ; DB2 events
```

Uncomment (overtype the semicolon with a blank) the SELECT statements for the events you wish to receive; comment out (begin the line with a semicolon) the SELECT statements for the events you do not wish to receive. For your initial testing you may wish to receive all possible events. See **The SELECT Statement** in **Parameter File Reference** in "CorreLog SIEM Agent for z/OS Configuration Reference" for a full description of SELECT. You can also “fine-tune” which events you format by changing the configuration statements for the various SMF record types such as with the SMF 80 EVENTS parameter.

Configuring Agent Licensing

If you will be using the Agent and not just CZASEND then you must obtain a LICENSE statement from CorreLog support. Carefully paste it *without any changes* into the parameter file member between the two lines that read

```
; Insert the LICENSE statement between these two lines
```

Do not make any changes to the operands of the LICENSE statement. (Blanks between parameters are not significant.) For example, if your organization name is spelled incorrectly, do not change the LICENSE statement; instead contact CorreLog for a new LICENSE statement.

If the Agent is already running, then the Agent must re-read the parameter file in order for a new LICENSE statement to become effective. You may if you wish stop and re-start the Agent, or wait until it restarts at your next scheduled IPL; it is not, however, necessary to do so. You can make the Agent re-read its parameter file (without missing a single event) by entering the z/OS MODIFY console command

F *procname*,PARMS(parmfile)

where *procname* is the name of your Agent started task (typically CZAGENT) and parmfile is your parameter file member name, typically CZAPARMS, CZAPCEF or CZAPSPLN as described above.

Configuring CZASEND

There is a JCL procedure (PROC) in hlq.CZASEND.CTNL named CZASEND. It may be used to facilitate the use of the CZASEND program. (See **Section 5: CZASEND Operation**.) You should customize this procedure and add it to your SYS.PROCLIB concatenation. (Alternatively you may use a JCLLIB statement in each job that uses CZASEND, or incorporate the statements found in the CZASEND prodcedure directly into your jobs.)

Edit the CZASEND member of hlq.CZAGENT.CNTL. Change all *hlq* to your chosen high level qualifier. You may change the CZAPRINT statement as desired; typically it references a held SYSOUT class.

CorreLog recommends that you copy CZASEND to a dataset in your SYS1.PROCLIB concatenation, or have some who is authorized do so.

If you are only going to be using CZASEND and not the Agent then your configuration is complete and you should skip ahead to **Section 5: CZASEND Operation**.

Checking the Configuration of SMF

In order for the Agent to receive the required record types from SMF, you must make certain of three things:

- that SMF is configured to invoke exits IEFU83, IEFU84, and IEFU85 (EXITS parameters)
- that SMF is configured to collect and write the appropriate record types (TYPE parameters). SMF configuration is controlled by “the SMFPRMxx member of SYS1.PARMLIB.”
- That TN3270 is configured to write the appropriate records.

If the above bullets mean little to you, then a description of the SMF parameters is beyond the scope of this manual; please consult with the person at your installation who is responsible for SMF and TCP/IP configuration.

Fortunately, the Agent diagnoses most mis-matches between the Agent configuration and the SMF configuration, with messages such as the following:

```
CZA0277W The following specified subsystems are NOT configured to
write SMF Type 18 records: SYSSTC. Some events will be missing
from Syslog
```

CZA0286W SUBSYS(TSO,EXITS(IEFU85)) not specified in SYS1.PARMLIB(SMFPRMxx). Some events will be missing from Syslog

CZA0287W SUBSYS(OMVS,EXITS or [NO]TYPE coded in SYS1.PARMLIB(SMFPRMxx) but OPTIONS SUBSYS(SYSOMVS) not specified in CZAPARMS. Some events will be missing from Syslog

SMFPRMxx specifies this information using a "two-level" scheme: you can specify parameters for z/OS as a whole using the **SYS(EXITS/NOEXITS** and **SYS(TYPE/NOTYPE** statements, and you can override those parameters on a subsystem by subsystem basis using **SUBSYS(xxx,EXITS/NOEXITS** and **SUBSYS(xxx,TYPE/NOTYPE**. *CorreLog highly recommends the use only of the system-wide statement SYS; otherwise you are at risk of missing important events.*

If any of the requirements below is not met, edit (or ask the appropriate system programmer to edit) appropriately your SMFPRMxx member in the SYS1.PARMLIB and then issue the console command SET SMF=xx (or /SET SMF=xx from SDSF) where xx is the last two characters of the appropriate SMFPRMxx member name.

Refer to the table below as you read about the EXITS and TYPES parameters.

Event Type to be Forwarded	SUBSYS	Record Types
Job, jobstep, started task, TSO session, and other "unit of work" start and end	Any; corresponds to the type of work	30
DFSMS PDS(E) changes	Any	42
Security events	Any	80 (RACF and TSS), 230 (or other as specified in ACF2)
DB2 events	Any	100, 101, and 102
CICS events	STC	110
TCP/IP and FTP events	Any, typically OMVS, TSO or STC	119

Also, if there are any SUBSYS statements of any kind in SMFPRMxx then be sure to read the description of the SUBSYS parameter of the OPTIONS statement in **Parameter File Reference** in "CorreLog SIEM Agent for z/OS Configuration Reference." It is highly recommended that you code SUBSYS(ALL) or allow SUBSYS to default.

EXITS Parameters

You must enable exits IEFU83, IEFU84 and IEFU85 for all of the events you wish to monitor. You can enable them for z/OS as a whole or on a subsystem by subsystem basis. *CorreLog highly recommends that you enable them on a system-wide basis; otherwise you are at risk of missing important events.*

Issue the console command **`D SMF,O`** (or **`/D SMF,O`** from SDSF). Check the **`D SMF,O`** output to make sure that at least one of the following is true:

- **`SYS(EXITS`** and **`SYS(NOEXITS`** are both *not* specified.
- **`SYS(EXITS(IEFU83`**, **`IEFU84`**, and **`IEFU85`** are specified, and there are no **`SUBSYS(xxx,EXITS`** or **`NOEXITS`** statements for any of the subsystems that you wish to monitor. (Recommended.)
- **`SUBSYS(xxx,EXITS(IEFU83`**, **`IEFU84`**, and **`IEFU85`** are specified for all of the subsystems that you wish to monitor.

TYPE Parameters

You must enable the writing of the appropriate SMF record types for the events you wish to monitor. You can enable them for z/OS as a whole or on a subsystem by subsystem basis. *CorreLog highly recommends that you enable them on a system-wide basis; otherwise you are at risk of missing important events.*

Issue the console command **`D SMF,O`** (or **`/D SMF,O`** from SDSF). Check the **`D SMF,O`** output to make sure that both of the following are true:

- **`SYS(TYPE`** and **`SYS(NOTYPE`** are both omitted,
  OR
  `SYS(TYPE` is specified and the specification includes all of the desired record types. (Recommended.)
  OR
  `SYS(NOTYPE` is specified and the specification does *not* include any of the desired record types.
- There are no **`SUBSYS(xxx,TYPE`** or **`NOTYPE`** statements for any of the subsystems that you wish to monitor (Recommended),
  OR
  `SUBSYS(xxx,TYPE` is specified for each of the subsystem and record type combinations that you wish to monitor, and **`SUBSYS(xxx,NOTYPE`** is

not coded specifying any of the subsystem and record type combinations that you wish to monitor.

TCP/IP and TN3270 Parameters

You must make certain that the TCP/IP profile is configured to write Type 119 records for the TCP/IP events you wish to audit. (The TCP/IP profile dataset is the dataset referenced by the //PROFILE DD statement in the cataloged procedure that is used to start TCP/IP.) The default is NO for most or all of the record types, so you should make certain that your TCP/IP profile contains a statement something like

```
SMFCONFIG TYPE119 FTPCLIENT TCPINIT TCPTERM TN3270CLIENT
```

If it does not edit the dataset, insert or edit the statement and save the dataset. You will have to stop and re-start TCP/IP for the statements to take effect, a step that must be deferred to a weekend evening or an IPL. (If the file already contains an SMFCONFIG statement that does not specify TYPE119, or that specifies TYPE118, it is okay to leave it in place, but you might inquire whether anyone in your organization actually requires SMF Type 118 records, which are general considered to be obsolete.)

You must make certain that the TN3270 profile is configured to write Type 119 records for the start and end of TN3270 sessions. (The TN3270 profile dataset is the dataset referenced by the //PROFILE DD statement in the cataloged procedure that is used to start TN3270.) These records are critical for enabling you to correlate security violations by TSO users back to the TCP/IP address from which they connected. The profile must contain the statements

```
SMFINIT TYPE119
SMFTERM TYPE119
```

If it does not edit the dataset, insert the statements and save the dataset. You will have to stop and re-start TN3270 for the statements to take effect, but you can probably defer that restart until a convenient time. (If the file already contains SMFINIT STD and SMFTERM STD statements it is okay to leave them in place, but you might inquire whether anyone in your organization actually requires SMF Type 118 records, which are generally considered to be obsolete.)

Other Subsystem Parameters

You must also configure subsystems such as CICS and DB2, and your security subsystem (RACF, ACF2 or Top Secret) to write the appropriate SMF records. For DB2 only, you can configure the Agent to have DB2 start the required traces

(SMF record types) automatically: see the discussion of the **STArt** parameter under **The SMF DB2** Statement in **Parameter File Reference** in "CorreLog SIEM Agent for z/OS Configuration Reference." A description of how to configure z/OS subsystems is beyond the scope of this manual; consult the appropriate IBM documentation.

RACF and Similar Authorizations and Permissions

Authorizing the Agent Load Library

You must APF-authorize the load library in which the Agent resides.

For the purposes of testing you can use the **`SETPROG APF`** console command, which will authorize the library *only until the next IPL*[7]. First, you must determine the volume on which the library resides. From ISPF enter the command

```
TSO LISTDS 'hlq.CZAGENT.LOAD'
```

Note the last line of output which is the “volume serial number” of the disk on which the library resides. Press enter to clear the *** on your display. Go to SDSF and type /+ and press Enter. Type

```
SETPROG APF,ADD,DSN=hlq.CZAGENT.LOAD,VOL=volser
```

in the popup window here *hlq* is the high-level qualifier you selected and *volser* is the volume serial number noted above, and press Enter. If you have typed the command correctly you will receive a response acknowledging that z/OS has added the library to the authorized library list.

You will not want to have to repeat this procedure after every IPL so on the longer term you should add the library to the permanent authorized library list in SYS1.PARMLIB. The procedures to do so are beyond the scope of this manual. If you are not familiar with the procedure at your installation then you should contact someone who is.

z/OS Communication Server (TCP/IP) and OMVS Segments

The CorreLog z/OS Agent and CZASEND utilize z/OS Communication Server for TCP/IP and/or UDP services. All programs that utilize z/OS Communication Server require a “z/OS UNIX security context,” commonly referred to as an “OMVS segment” for the owning user ID (whether they run as batch programs,

[7] “IPL” stands for Initial Program Load and is the mainframe term for “re-boot.”

started tasks, or under the UNIX shell). Your installation may choose to set up a separate OMVS segment for the specific user IDs under which the Agent and CZASEND will run, or they may set up a single default OMVS segment. A suitable OMVS segment may already be in place for your user ID and/or the user ID under which started tasks run. If not, then you should read **Requirement for an OMVS segment** in the *IBM z/OS Communication Server IP Configuration Guide* and follow the steps outlined there.

If the Agent or CZASEND is executed by a user ID without an OMVS segment it will fail immediately with the RACF message (or equivalent ACF2 or Top Secret message)

```
ICH408I USER(xxxxxx ) GROUP(xxxxxx   ) NAME(xxxxx xxxxxx )
CL(PROCESS ) OMVS SEGMENT NOT DEFINED
```

Facility Class Permissions for CSVDYNEX

The user ID under which the Agent runs must have SAF UPDATE authority to the CSVDYNEX FACILITY class. A full tutorial on RACF commands is beyond the scope of this manual, but something similar to the following is recommended:

```
PERMIT CSVDYNEX.** CLASS(FACILITY) ID(user) ACCESS(UPDATE)
SETROPTS RACLIST(FACILITY) REFRESH
```

Where *user* is the user ID or RACF group name for the Agent started task.

The equivalent commands should be entered for CA ACF2 or CA Top Secret if your installation uses either of those products instead of RACF.

DB2 MONITOR2 Privileges

If you will be using the dbDefender feature of the Agent to monitor DB2 *and using the SMF DB2 START* option, then the Agent's user ID must have MONITOR2 privileges for each DB2 subsystem specified. Use a DB2 command similar to the following:

```
GRANT MONITOR2 TO authid
```

Where *authid* is the Authorization ID for the Agent started task.

Testing the Agent

The Agent as a Job

Edit the sample job in *hlq*.CZAGENT.CNTL(CZAGNJOB) (where *hlq* is the "high level qualifier" chosen during installation). Change the job statement to conform to your installation's requirements. Change all *hlq* to your high-level qualifier. Make certain that the **`//CZAPARMS DD`** statement references the correct parameter dataset.

Submit the job. If you receive a JCL error or if CZAGNJOB completes immediately try to resolve the problem by referring to the messages in the CZAPRINT dataset. If you cannot resolve it, contact CorreLog for technical support.

If the Agent is working correctly then the job will not end. You should have a functioning Agent. Go to SDSF and type

`/F jobname,STATS(SEND)`

on the command line where *jobname* is the name you chose for the CZAGNJOB job statement. If you go to your CorreLog server or Syslog console you should see several Syslog messages with the Agent statistics. You should also start to see TSO logon messages and perhaps security violation messages (depending on how busy your LPAR is). If you don't see any TSO logon or security violation messages, try logging off of your TSO session and logging back on. You should see a message reporting your logon on the Syslog console. If not then you should contact CorreLog for technical support.

Go to SDSF and type **`/P jobname`** on the command line where *jobname* is the name you chose for the CZAGNJOB job statement. *Important – do not use the P "action character" from SDSF.* The job should end normally.

The Agent as a Started Task

Edit the sample procedure *hlq*.CZAGENT.CNTL(CZAGENT). Change *hlq* to your chosen high-level qualifier. Check the //CZAPARMS DD statement, which should refer to the hlq.CZAGENT.CNTL dataset as a whole, not to a particular member. Check the CZADIAG and CZAPRINT DD statements; normally they should refer to a held SYSOUT class. Copy, or have someone authorized to do so copy, the member CZAGENT to a dataset in your SYS1.PROCLIB concatenation.

Go to SDSF and type

```
/S CZAGENT
```

If you go to the SDSF DA panel you should see the CZAGENT started task. (You may have to type PREFIX CZA* and/or OWNER *.) If not, try going to the H or O panel. Browse the CZAPRINT dataset. If errors are reported, attempt to resolve them and re-start CZAGENT. If there are no errors, you may verify proper operation using the same tests as described above for the Agent as a job.

Troubleshooting

Agent Completely Fails to Start with No CZAPRINT Listing

Almost certainly a JCL error in the cataloged procedure. Check the console log and/or SDSF for the error.

Agent Terminates Immediately

Did you receive ABEND U4093 Reason Code 90? Please refer to the section above **z/OS Communication Server (TCP/IP) and OMVS Segments**.

Check the CZAPRINT dataset for errors. Look for messages with identifiers ending in E, S or C (such as CZA0207S). Look up the message in "CorreLog SIEM Agent for z/OS Messages and Codes" (see **Appendix B: Bibliography**) and attempt to resolve the error. Contact CorreLog for technical support if you cannot resolve the error on your own.

Agent Runs but no Messages Received by SIEM

Does message **`CZA0028E Return code 1127 received from TCP/IP function connect(), EDC8127I Connection timed out`** appear in CZAPRINT? This or a similar message indicates that the SIEM is not running, not configured to receive TCP/IP messages on the specified or default port, or is unreachable due to firewall or similar issues. You will need to resolve this issue with your network staff.

Check message CZA0274I (usually about the fifth message in CZAPRINT) to make certain the Agent is using the intended parameter file. If not, attempt to resolve any configuration issues.

If your SERVER statement in the parameter file specifies PROTO(UDP), or has no PROTO parameter, then the most likely cause is an incorrect IP address or port, or a firewall is blocking connectivity. Attempt to resolve the problem. Remember that with UDP, there will be absolutely no error indicated on the LPAR if the IP address is incorrect or unreachable.

If your SERVER statement specifies PROTO(TCP) and there are no CZA0028E messages, then the agent's Syslog messages are almost certainly reaching *some* destination. Perhaps you have two SIEM consoles and have specified an incorrect address? Perhaps the SIEM is receiving the messages but they are not being displayed? Contact CorreLog for technical support if you cannot resolve the error on your own.

Messages Received by SIEM, but Some Expected Messages Missing

Stop the Agent and look at the CZAPRINT listing. Do you see message CZA0277W, CZA0278W, CZA0286W or CZA0287W (near the beginning of the listing)? If so, it indicates that the specified SMF record type(s) is not being produced. Refer to **TYPE Parameters** under **Checking the Configuration of SMF** above.

Do you see message CZA0217W (near the end of the listing)? Does it mention IEFU83 driven, IEFU84 driven or IEFU85_driven? If so, it probably indicates that the specified exit is not enabled in SYS1.PARMLIB. Refer to **EXIT Parameters** under **Checking the Configuration of SMF** above.

Consider the effect of SELECT statements. See **Configuring Your Required Events with SELECT** above.

Still having a problem?

Contact CorreLog for support.

Adding the Agent to your IPL Procedures

You will want to add the Agent to your standard IPL procedures so that it is not necessary to start it manually after every IPL. The Agent should be started after TCP/IP is operational. The Agent will wait for TCP/IP to initialize unless OPTIONS NOTCPWAIT is specified (see **The OPTIONS Statement** in **Parameter File Reference** in "CorreLog SIEM Agent for z/OS Configuration Reference"). The Agent will output message CZA0247I to indicate that it is waiting; if you wish you may terminate the Agent in this situation with the console STOP command.

You should choose a method of automatic startup that is suitable for your installation's needs. Recommending a specific method is outside the scope of this manual. Some of the methods that might be appropriate to your installation include

- The COMMNDxx member of your SYS1.PARMLIB concatenation (see the IBM manual “z/OS MVS Initialization and Tuning Reference”).
- A $VS command in your JESx initialization dataset (commonly referred to as a JES init deck). See the IBM Manual “z/OS JES2 Initialization and Tuning Reference” or “z/OS JES3 Initialization and Tuning Reference.”
- The MPFLSTxx member of your SYS1.PARMLIB concatenation (see the IBM manual “z/OS MVS Initialization and Tuning Reference”).
- The TCP/IP AUTOLOG facility (see the IBM manuals “z/OS Communications Server IP Configuration Reference” and “z/OS Communications Server IP Configuration Guide.”
- Your console automation system.

Orderly Termination of the Agent

You should also make provisions for the orderly shutdown of the Agent during a z/OS shutdown or re-IPL. The Agent should be terminated with a STOP command before terminating TCP/IP, however, *if you issue the STOP command and TCP/IP has already terminated or become unavailable the Agent should terminate without waiting for TCP/IP*. In an emergency it is permissible to cancel the Agent and no harm to the system should result. However, it is only recommended that you cancel the Agent in an emergency or before a shutdown or re-IPL. If you re-start the Agent after cancelling it and without an intervening IPL then you may have to use the FORCE parameter. See **Restarting the Agent after an Unexpected Failure**.

Section 4: Agent Operation

See **How to Read the Syntax Diagrams** in "CorreLog SIEM Agent for z/OS Configuration Reference" for a description of the notation used in the command syntax diagrams.

Running the Agent as a Started Task

The procedures for running the Agent as a started task are largely detailed under **Section 3: Configuration**, **Testing the Agent**. JCL similar to the following is required to run the Agent as a started task. This JCL is provided in *hlq*.CZAGENT.CNTL as member CZAGENT.

```
//CZAGENT  PROC PARMS=CZAPARMS,RUNMODE=PROD,INSTALL=,VERBOSE=,
//   TRACE=
//CZAGENT  EXEC PGM=CZAGENT,TIME=1440,REGION=4096K,
//   PARM=('&VERBOSE,TRACE(&TRACE),CZAPARMS(&PARMS)',
//         'MODE(&RUNMODE &INSTALL)')
//STEPLIB  DD  DSN=hlq.CZAGENT.LOAD,DISP=SHR
//CZAPARMS DD  DSN=hlq.CZAGENT.CNTL,DISP=SHR
//CZADIAG  DD  SYSOUT=H
//CZAPRINT DD  SYSOUT=H
//SYSUDUMP DD  SYSOUT=H
//         PEND
```

Note that that CZAPARMS must specify an entire PDS or PDSE (single dataset or a concatenation, LRECL=80, RECFM=FB) and not a member, i.e., *hlq*.CZAGENT.CNTL, not *hlq*.CZAGENT.CNTL(*member*). Note also that the

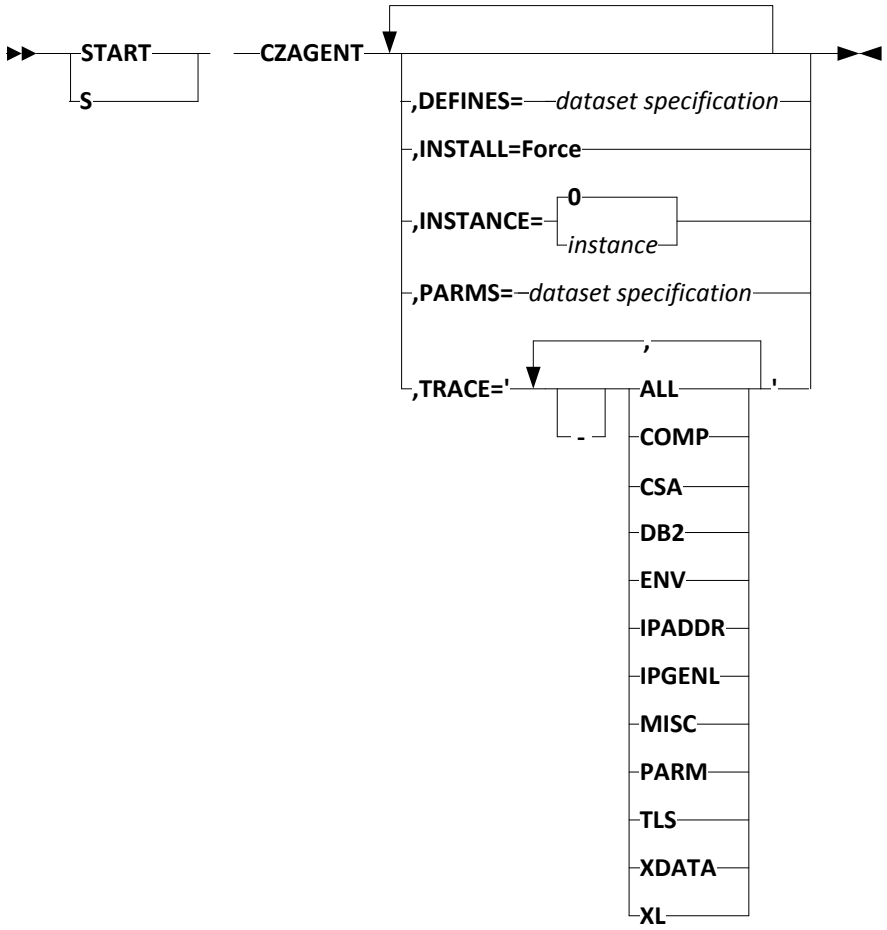
agent and its exit *must* be loaded from STEPLIB, not from some other DD such as JOBLIB, nor from the link pack concatenation.

Restarting the Agent after an Unexpected Failure

Should the Agent experience an unexpected failure (or should you end the Agent by canceling it rather than with the STOP command, which is *not* recommended) it should be possible to restart the Agent with no difficulties using the START command with the INSTALL=FORCE parameter. Do not alter the OPTIONS SUBSYS parameter between a non-orderly termination of the Agent and a FORCE restart. If you wish to alter the SUBSYS parameter after an unexpected failure, first start CZAGENT INSTALL=FORCE, then shut it down with a STOP command, and then make your desired changes to OPTIONS SUBSYS.

The Start or S Command

The START (abbreviated S) command is used to initiate the Agent as a started task. The format of the START command for the Agent is



Note that one or more blanks are required after START or S and before CZAGENT, but there must be no embedded blanks before, between or within the optional parameters.

DEFINES=dataset specification

Specifies the name of the primary fields definitions file. See **Fields Definitions File**. As the fields definitions file is an input file, a specification of * (SYSOUT) is invalid, and the output variable symbols are not supported. z/OS command processing uppercases unquoted command operands, so to specify a zFS file specify, for example,

```
S CZAGENT,PARMS='/u/myfiles/czaparms'
```

The default PDS(E) is DD:CZAPARMS, that is, the library specified by the CZAPARMS DD statement. If DEFines is omitted it defaults to DD:CZAPARMS(CZDEFINE).

INSTALL=FORCE

Should be used only after an unexpected failure (see **Restarting the Agent after an Unexpected Failure**) or as directed by CorreLog technical support.

FORCE will not cause any harm if used unnecessarily *assuming the Agent is not already running in the specified RUNMODE*. Avoid using FORCE habitually or routinely because if you inadvertently use FORCE when the Agent is already running in the specified RUNMODE it will cause unpredictable problems.

If START CZAGENT with FORCE runs into certain unexpected situations it attempts to clean them up but also reports them and then terminates with an error. However, a second attempt at FORCE might succeed because the unexpected situation has previously been resolved. So if FORCE fails, you should try it again up to two or three times. You should see a different error on the subsequent failure; if not, further retries are pointless.

INSTANCE=instance

Specifies an Agent "instance number" between 0 and 7 inclusive. Specifying an instance allows you to start more than one "copy" of the Agent in a single LPAR. The multiple instances run completely independently and could specify different SIEM collectors, different SMF records, different formatting options, and so forth. If you specify the number of an instance that is already running you will receive an error message. If you omit INSTANCE it defaults to 0.

PARMS=dataset specification

Specifies the name of the primary parameter file. As the parameter file is an input file, a specification of * (SYSOUT) is invalid, and the output variable symbols are not supported. The default PDS(E) is DD:CZAPARMS, that is, the library specified by the CZAPARMS DD statement. If PARMS is omitted it defaults to DD:CZAPARMS(CZAPARMS). This file is described in **Parameter File Reference** in "CorreLog SIEM Agent for z/OS Configuration Reference."

TRACE='trace_specifications'

Specfies that the Agent is to output additional diagnostic messages and the types of diagnostic messages, in the CZAPRINT dataset. TRACE may be

useful for diagnosing certain problems. If TRACE is completely omitted then all tracing is turned off.

Specify zero or more of the trace specifications in the table below (in any order), surrounded by single quotation marks and separated by commas. Prefix any of the specifications with "-" (a minus sign) to indicate negation. For example TRACE='ALL –XL –ENV' indicates all TRACE output *except* that related to translation and the operating environment.

Specification	Type of diagnostic messages
ALL	All
COMP	SMF record compression-related processing
CSA	CSA initialization
DB2	DB2-related processing
ENV	The z/OS operating environment
IPADDR	IP address processing
IPGENL	IP general
MISC	Miscellaneous
PARM	Parameters
TLS	SSL/TLS-related events
XDATA	Transmitted data (generates a fairly voluminous number of messages)
XL	Translation (generates a fairly voluminous number of messages)

Start Command Responses

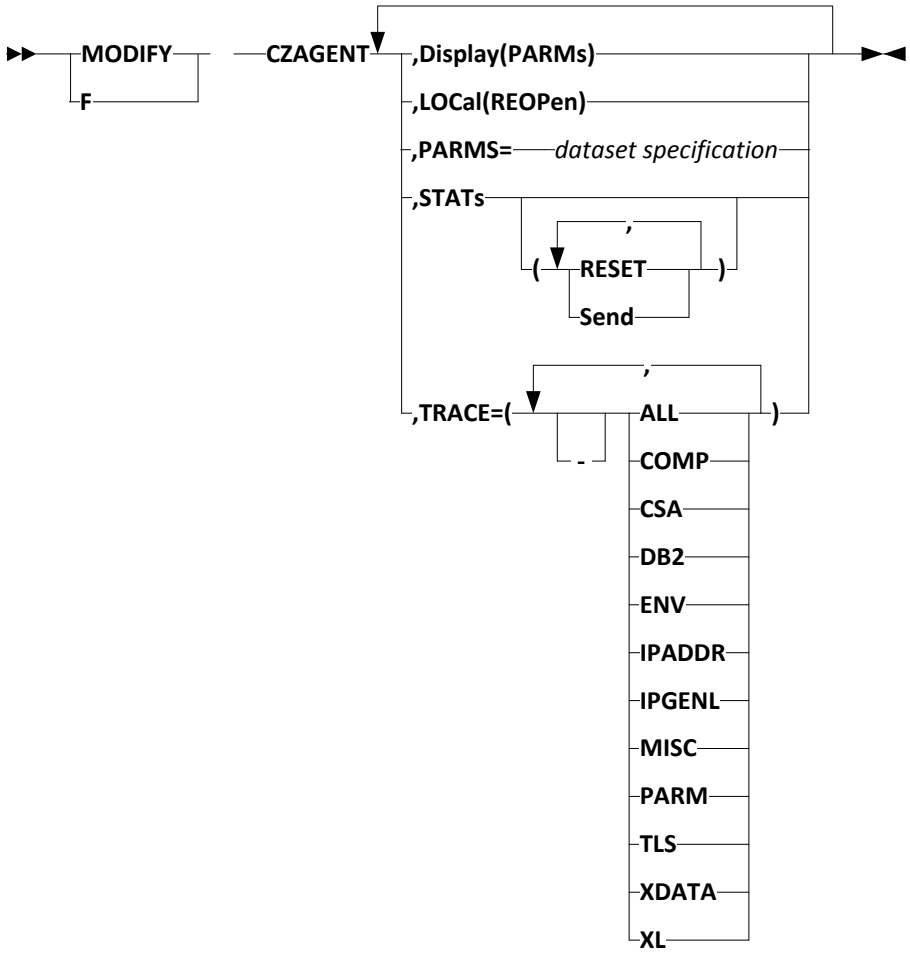
If the Agent initialization is successful the response to the START command will be

```
CZA0202I CorreLog SIEM Agent for z/OS: z/OS Syslog Agent, Vv-r-m
CZA0205I Initialization successful as Instance n; ready to forward Syslog messages
```

In the event of errors diagnostic messages will be issued to the console and to CZAPRINT. For some errors additional information may be available in CZAPRINT beyond what is displayed on the console.

The Modify or F Command

The MODIFY (abbreviated F) command is used to change the Agent's operating parameters or to display the Agent's statistics. The displayed statistics may optionally be transmitted as a Syslog message. The format of the MODIFY command for the Agent is



Note that one or more blanks are required after MODIFY or F and before CZAGENT, but there must be no embedded blanks before, between or within the optional parameters.

Display(PARMs)

Causes the Agent to display the currently active settings for the parameters of LOCAL, OPTIONs, and SERVER. The values are displayed on the console and in CZAPRINT in the format

```
CZA0251I LOCAL
CZA0251I     DATASET (*)
CZA0251I     FOLD    (133)
CZA0251I   NOMOD
Etc.
```

LOCal(REOPen)

Specifies that the Agent is to close and re-open the LOCAL Syslog dataset. Before using this command you should consider the effect of the use or absence of system variable symbols in the specified dataset name, and the use or absence of MOD. For example, REOPEN *may* be meaningless for a dataset specified with MOD because additional records will simply be appended to the already-open dataset. If REOPEN is specified for a local MVS dataset without the &HHMMSS. variable symbol in its name and without MOD, the Agent will overwrite the existing dataset and any existing messages will be lost.

PARMs(dataset specification)

Specifies a dataset from which the Agent is to take new operating parameters. As the parameter file is an input file, a specification of * (SYSOUT) is invalid, and the output variable symbols are not supported. z/OS command processing uppercases unquoted command operands, so to specify a zFS file specify, for example,

```
F CZAGENT,PARMS=('/u/myfiles/czaparms')
```

or

```
F CZAGENT,'PARMS=(/u/myfiles/czaparms)'
```

The default PDS(E) is DD:CZAPARMS, that is, the library specified by the CZAPARMS DD statement. If PARMs is omitted it defaults to DD:CZAPARMS(CZDEFINE).

This file is described in **Parameter File Reference** in "CorreLog SIEM Agent for z/OS Configuration Reference."

Parameter processing “starts over” each time you read in a parameter file with MODIFY CZAGENT,PARMS with the exception of OPTIONS TRACE, SUBSYS, and QUEUE. Every parameter assumes its default value except for the three parameters named. OPTIONS QUEUE and SUBSYS are ignored during MODIFY processing; to change their values you must stop and re-start the Agent; to change the setting of TRACE you must explicitly specify TRACE. So if the Agent is running with a LOCAL dataset, FORMAT(ALL), and an SMF 119 statement, and you read in a new

parameter file with FORMAT, LOCAL, and SMF 119 omitted, then FORMAT assumes its default value of ERGONOMIC, the LOCAL dataset is closed, and no further SMF 119 records are formatted and transmitted. (See **Parameter File Reference** in "CorreLog SIEM Agent for z/OS Configuration Reference" for a discussion of the specific parameters mentioned.)

STATs

STATs(RESET,Send)

Causes the Agent to display message CZA0215I with counts of SMF records processed and similar statistics on the console and in the listing on CZAPRINT. If RESET is specified then the various statistical counters are reset to zero after being displayed. If SEND is specified then the statistics are also transmitted to the CorreLog server or other Syslog console as Syslog messages. SEND may be abbreviated as S. The various statistics are documented in **Counters** in "CorreLog SIEM Agent for z/OS Configuration Reference."

TRACE(trace_specifications)

Specfies that the Agent is to output additional diagnostic messages and the types of diagnostic messages, in the CZAPRINT dataset. TRACE may be useful for diagnosing certain problems. If TRACE is completely omitted or specified as TRACE() then it defaults to the previous state of TRACE; if TRACE(-ALL) is specified then all tracing is turned off.

Specify zero or more of the trace specifications in the table below (in any order), surrounded by parentheses and separated by commas. Prefix any of the specifications with “-” (a minus sign or hyphen) to indicate negation. For example, if TRACE(ALL) is currently in effect then specifying TRACE(-XL -ENV) indicates all TRACE output *except* that related to translation and the operating environment.

Specification	Type of diagnostic messages
ALL	All
COMP	SMF record compression-related processing
CSA	CSA initialization
DB2	DB2-related processing
ENV	The z/OS operating environment
IPADDR	IP address processing
IPGENL	IP general

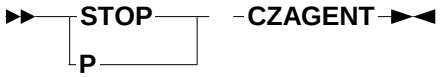
Specification	Type of diagnostic messages
MISC	Miscellaneous
PARM	Parameters
TLS	SSL/TLS-related events
XDATA	Transmitted data (generates a fairly voluminous number of messages)
XL	Translation (generates a fairly voluminous number of messages)

After processing TRACE, the Agent will display the trace specifications then in effect. To simply display the current trace specifications, enter

```
F CZAGENT,TRACE()
```

The Stop or P Command

The STOP (abbreviated P) command is used to stop the Agent. The format of the STOP command for the Agent is



Note that one or more blanks are required after STOP or P and before CZAGENT. The STOP command has no parameters.

When the STOP command is accepted by the Agent it will send a message (CZA0234I) to the Syslog console, display statistics on both CZAPRINT and the Syslog console, and terminate:

```
CZA0212I STOP command accepted
CZA0234I Termination in progress
CZA0042I SIEM Agent for z/OS completed, completion code n
```

Section 5: CZASEND Operation

CZASEND is a simple program that will send a single Syslog message of your choosing to your configured Syslog server. CZASEND may be included in any batch job or called from a COBOL or other application program. The Syslog message may be specified as a parameter or read from a file.

In CEF mode, CZASEND messages have a Header Signature ID of “CZASEND User Message”; a Header Name of “User Message”; and an extension of

```
cat=CZASEND cs1Label=User Message cs1=Message text
```

The description below assumes you have added the CZASEND procedure (PROC) to your SYS1.PROCLIB concatenation as described above in **Configuring CZASEND**. If you have not then you will have to add the statement

```
//PROCLIB JCLLIB ORDER=hlq.CZAGENT.CNTL
```

to each job that uses the CZASEND procedure. Alternatively you may incorporate the JCL statements found in CZASEND directly into your jobs. A description of how to do so is beyond the scope of this manual.

CZASEND will return a completion code to the job or the calling program. See "CorreLog SIEM Agent for z/OS Messages and Codes" (see **Appendix B: Bibliography**) for the possible return codes and their meanings.

In the very simplest case, code an EXEC statement for CZASEND omitting PARM= specifying text to be sent as a Syslog message. The text must be enclosed in single quotes.

```
//VSIMPLE   EXEC CZASEND
```

A Syslog message consisting of the Job and Step names will be sent to your CorreLog server or other Syslog console with a severity of Notice. (All CZASEND Syslog messages are sent with a Facility code of 1, user-level messages.)

In the next simplest case, code an EXEC statement for CZASEND with PARM= specifying text to be sent as a Syslog message. The text must be enclosed in single quotes.

```
//SIMPLE   EXEC CZASEND,PARM='Update Completed'
```

The text you specify will be sent to your Syslog console with a severity of Notice. The operand of PARM= is limited by z/OS to 100 characters in length.

If the text contains a quotation mark then you must code it as two quotation marks:

```
//QUOTES   EXEC CZASEND,
//     PARM='Billing didn''t complete - notify Phil'
```

(The text will appear on the CorreLog server or other Syslog console with only a single quotation mark.)

Optionally you may prefix the message with a token signifying a Syslog severity:

```
//SEVERITY EXEC CZASEND,
//     PARM='ERROR Database update failed'
```

Any blanks between the token and the message text are removed. See **Syslog Severities** in "CorreLog SIEM Agent for z/OS Configuration Reference."

You may abbreviate the token to the portion in upper case in the table in **Syslog Severities**. The token may be coded in upper, lower, or mixed case. For example, you could indicate a severity of WARNING by coding WARN, Warn, or warning.

If PARM= is omitted but a DD statement for CZAMSG is provided, CZASEND will obtain the message text from the dataset referenced by the DD statement CZAMSG. CZAMSG may refer to a sequential dataset, a PDS member, or an HFS or zFS file. The file may be any valid z/OS record format, record length, and block size.

```
//FILEDFLT EXEC CZASEND
//CZAMSG   DD   DSN=MY.MESSAGE.LIBRARY(MESSAG01),DISP=SHR
```

The message dataset – MY.MESSAGE.LIBRARY(MESSAG01) in this example – contains a message in the same format as PARM=, including an optional severity, except that the text is limited to about 1400 rather than 100 characters and quotes should not be doubled. The message is always treated as text; do not code CZAMSG() in the file. The message may span multiple records. Any trailing blanks on CZAMSG records are deleted; leading blanks are not. So MESSAG01 might contain

```
Warning Severe errors were detected during the
 update of the customer database W52KZTFH.#QIKKWMY.
UPIBPG21.YLBGY1ZB
 Open a ticket for the customer database team
 immediately.
```

Alternatively you may specify a message file in the PARM= operand in any of several formats:

```
//FILEDD  EXEC CZASEND,PARM='CZAMSG(dataset specification)'
```

See **Dataset Specifications** in **Parameter File Reference** in "CorreLog SIEM Agent for z/OS Configuration Reference" for the supported dataset specification formats. As it is an input file, * (SYSOUT) is not allowed, nor are the output file variable symbols. The default PDS(E) is the dataset referred to by the CZAPARMS DD statement, without the member name. If the CZAPARMS DD statement does not reference a PDS(E) member then there is no default PDS(E).

You may invoke CZASEND from within a COBOL or other application program, or from a Rexx script. At run time you must provide DD statements for CZAPARMS, CZAPRINT, and a STEPLIB that contains CZASEND. If the use of a DD statement for the message is implied by the passed parameter, then you must provide a DD statement for CZAMSG or any DD statement referenced by CZAMSG(DD:).

You may pass a parameter to CZASEND with any of the formats described above (or omit the parameter to use the CZAMSG DD). The following is a demonstration COBOL program that invokes CZASEND. Note the use of the “bridge” stub CZASENDL because of the requirements of Language Environment.

```
IDENTIFICATION DIVISION.
PROGRAM-ID. CZASCOB.
ENVIRONMENT DIVISION.
DATA DIVISION.
WORKING-STORAGE SECTION.
77  CZASEND-PROG  PIC X(8)  VALUE 'CZASENDL'.
01  SYSLOG-MESSAGE.
  05  MESSAGE-LENGTH COMP PIC S9(4).
  05  MESSAGE-TEXT.
    10  SEVERITY  PIC X(15) VALUE 'INFO'.
    10  FILLER    PIC X(29)
          VALUE 'Customer update completed. '.
    10  REC-COUNT PIC ZZZ,ZZ9.
    10  FILLER    PIC X(18) VALUE ' records inserted.'.

PROCEDURE DIVISION.
    MOVE 38569 TO REC-COUNT.
    MOVE LENGTH OF MESSAGE-TEXT TO MESSAGE-LENGTH.
    CALL CZASEND-PROG USING SYSLOG-MESSAGE.
    STOP RUN.
```

To invoke CZASEND from a Rexx script, refer to the following example.

```
/* Rexx program to test and demonstrate CZASEND */
Parm = "Notice Hello from a Rexx program"
ADDRESS LINKMVS "CZASEND Parm"
```

Appendix A: Notices

Trademarks

dbDefender is a trademark and CorreLog® is a registered trademark of CorreLog, Inc.

The following terms are trademarks of International Business Machines Corporation in the United States or other countries or both:

DB2®
IBM®
MVS
Q1 Labs®
QRadar®
RACF
System z
z/OS®
zSeries®

ACF2® and Top Secret® are registered trademarks of CA Inc.

ArcSight is a trademark of Hewlett-Packard Development Company, L.P.

Netscape® is a registered trademark of AOL® Inc.

PCI Security Standards Council is a trademark of The PCI Security Standards Council LLC.

Splunk® is a registered trademark of Splunk, Inc.

UNIX® is a registered trademark of The Open Group.

Windows® is a registered trademark of Microsoft Corporation.

Other company, product, or service names may be trademarks or service marks of others. No association with CorreLog, Inc. is implied.

Appendix B: Bibliography

CorreLog SIEM Agent for z/OS Application Program Interface

This manual is intended for an advanced programmer who will be interfacing some other product to the CorreLog SIEM Agent for z/OS using the Agent's Application Programming Interface One, referred to therein as "the API" or "API 1." This manual assumes a thorough knowledge of programming in the z/OS Assembler or C/C++ language.

CorreLog SIEM Agent for z/OS Configuration Reference

This manual is a reference for system administrators and programmers who will be configuring, operating and maintaining the CorreLog SIEM Agent for z/OS.

The topics covered in this manual include:

- Configuring the Agent to suit particular business requirements or a particular SIEM (security console).
- Including or omitting the processing of SMF record types already defined to Agent. For example, you can turn SMF Type 42 formatting and forwarding on or off without using the information in this manual.

- Including or omitting, or changing the order of, fields in the formatted messages sent by Agent.
- Changing the case of field tags. For example, SMF80REA may be identified as Reas, reas or REAS.
- Changing the delimiters that surround fields in the formatted Syslog messages.
- Changing many other characteristics of Agent's processing or the format of forwarded messages.

CorreLog SIEM Agent for z/OS Defining Your Own Fields

This manual is intended for an advanced programmer, administrator or security analyst who will be creating or modifying the definition of Agent fields.

Using the information in this manual, you can

- Define additional SMF record types for the agent to process (subject to some limitations). For example, you could define the processing of SMF Record Type 4, which is not currently supported by the agent.
- Define additional fields in new or existing SMF record types. For example, you could define the fields of SMF Record Type 4, or additional fields in SMF Record Type 80 (which is already supported by the agent).
- Change the characteristics of existing fields. For example, the field SMFXXSID, the system identifier common to all SMF records, is defined as a character field with the tag SID. You could redefine it as a hex field, or redefine its tag as SysID.
- Change other information associated with fields. For example, the X'01' bit of SMF Type 80 field SMF80REA is displayed as "GLOBALAUDIT". You could change that to "Audited (Global)".

CorreLog SIEM Agent for z/OS Installation and Operation

Read me first! This manual is the starting point for system administrators and programmers who will be installing the CorreLog SIEM Agent for z/OS.

The topics covered in this manual include:

- Initial installation and re-installation.
- Initial configuration of the Agent to suit a particular SIEM (security console).
- Day to day operation of Agent including starting and stopping the task.
- Including or omitting the processing of SMF record types already defined to Agent. For example, you can turn SMF Type 42 formatting and forwarding on or off with the information in this manual.

CorreLog SIEM Agent for z/OS Messages and Codes

This manual provides a detailed description of the messages and return codes of the CorreLog SIEM Agent for z/OS programs, *with the exception of the return codes of the Application Program Interface (API) which are documented in the Application Program Interface Manual*.

Index