IBM Electronic Service Agent
for
IBM zSeries and IBM S/390
Version 1 Release 2
User's Guide
SC38-7104-02

June 10, 2013

Note

Before using this information and the product it supports, read Appendix F, “Notices and Trademarks” on page 89.

FIRST Edition 2001

SECOND Edition 2002

This edition applies to Version 1 Release 2 of Electronic Service Agent for zSeries and S/390, product number 5655-F17, and to all subsequent releases and modifications until otherwise indicated in new editions

Contents

Figures

Summary of Changes

This topic summarizes the recent changes made to this document.

Second Edition, June 2013 with APAR PM90105

This publication has been revised to reflect the withdrawal of functionality for sending IBM Customer Configuration Collector (CCC) data, i.e. External transaction of Electronic Service Agent.

Host software prerequisties update

Host software prerequisites section on page 10 have been revised with applicable version of Modification Program Extended (SMP/E) for z/OS.

Ordering Service Agent

This publication has been revised with ordering Service Agent information. See 2.5, "Chapter 2 - Service Agent installation" on page 3 for details.

Related publications update

This publication has been revised with related publicatons on page X.

Second Edition, April 2012 with APAR PM57608

This publication has been revised to support the functional changes introduced with Electronic Service Agent APAR PM57608.

The Apache Software License notice and JDOM License notice are removed from Appendix F. Notices and Tradmarks section since both software products are no longer required by Electronic Service Agent and hence are removed from the product package.

This publication has been updated with currently supported SDK for z/OS, Java Technology Edition versions.

How to control Device List for hardware data collection

This publication has been revised to provide additional information on how to control which devices are eligible for hardware data collection and reporting. See “Excluding devices from hardware data collection and reporting” on page 17 and “Including devices for hardware data collection and reporting” on page 18.

Second Edition, February 2008 with APAR PK60847

This publication has been revised to support the functional changes introduced with Electronic Service Agent APAR PK60847.

The changes relating to Hardware applications using communications by Direct Connection are described in overview on 4.0, “Chapter 4 - Hardware data collection and reporting” on page 14.

Second Edition, June 2007 with APAR PK42978

This publication has been revised to support the functional changes introduced with Electronic Service Agent APAR PK42978. This APAR edited some panels and revised some procedures used in the Dialog.

In page 30, the use of envvars variables for transmission of hardware is redefined.

In page 44, changes in operation are described which are forced by the removal of the requirement for enablement of Hiper/PE. That is, Hiper/PE is no longer only available to customers who have purchased certain software contracts ("ETS" in EMEA and "Swxcel Enterprise Edition" in the US) but is available to all.

In page 46, the revision of the Advanced (Authorize Web Users) screen to provide more clarity for usage instructions is described.

Second Edition, December 2006 with APAR PK35167

This publication has been revised to support the functional changes introduced with Electronic Service Agent APAR PK35167. This APAR provided functionality for Direct Connection Proxy Server authentication support.

In page 11, the use of this APAR is mandated.

In page 29, the use envvars variables for this option is defined.

Second Edition, December 2006 with APAR PK34970

This publication has been revised to reflect the changes made when the Performance Collection capabilities were removed from Electronic Service Agent.

All of the changes were text removals. They were concentrated mainly in 5.0, "Chapter 5 - Software and Hiper data collection and reporting" on page 25.

Second Edition, October 2006 with APAR PK28406

This publication has been revised to support the functional changes introduced with Electronic Service Agent APAR PK28406. This APAR provided functionality for sending IBM Customer Configuration Collector (CCC) data using the collection and reporting facilities of ESA.

The following summarizes changes made to this edition:

- In 5.0, "Chapter 5 - Software and Hiper data collection and reporting" on page 25 et al, changes to panels and operations have been made to configure, schedule and force the reporting of CCC data under the transaction name "External."
- In "Forcing data collection" on page 39, changes that allow hardware, external and Hiper/PE transactions to be manually forced have been made.
- In 6.0, "Chapter 6 - Service Agent management" on page 70, the procedures for starting and stopping Service Agent Tasks have been further explained.
- In page /IMPCON/, the conditions under which an import for Hiper/PE is done is explained.
- In page 47, an explanation of Group ID and its usage is made.

Second Edition, September 2006

This publication has been revised to support the functional changes introduced with the Hardware Management Console for the z9 Enterprise Complex (EC).

The following summarizes changes made to this edition:

- In 3.0, "Chapter 3 - System Prerequisites" on page 5, enabling Service Agent using the z9 HMC is discussed.

Second Edition, March 2006 with APAR PK18451

This publication has been revised to support the functional changes introduced with Electronic Service Agent APAR PK18451. This APAR provided functionality for Hardware Data Collector (HMC communication mode) to delete a remote file from theHMC.

The following summarizes changes made to this edition:

- In Appendix C, "Hardware data collection and reporting task" on page 81, the Hardware Data Collector HESRDLOG now includes an additional parameter in support of deleting a remote file from the HMC. Please see REMOTE DELETEFILE parameter in section C.1, "How the parameters work with the Hardware Data Collector program" on page 81.

Second Edition, December 2005 with APAR PK15210

This publication has been revised to support the functional changes introduced with Electronic Service Agent APAR PK15210. This APAR provided functionality for sending data directly for clients host to IBM using HTTP over SSL secured connection.

The following summarizes changes made to this edition:

- In 3.0, "Chapter 3 - System Prerequisites" on page 5, the system and software prerequisites for direct connection is outlined in a tabular format.
- In 4.0, "Chapter 4 - Hardware data collection and reporting" on page 14, collecting and sending data directly to IBM using module HESHWRDL is discussed.
- 5.0, "Chapter 5 - Software and Hiper data collection and reporting" on page 25 is changed to describe the new direct connection method; how to customize and enable it.
- Appendix C, "Hardware data collection and reporting task" on page 81 is changed to describe the Hardware Data Collector parameters that are applicable to direct connection and HMC connection.

Second Edition, June 2005 with APAR PK06867

This publication has been revised to support the functional changes introduced with Electronic Service Agent APAR PK06867. This APAR provided functionality for processing logrec data from TPF and VM systems also referred to as offloaded EREP history data sets.

The following summarizes changes made to this edition:

- In 4.0, "Chapter 4 - Hardware data collection and reporting" on page 14, the processing of logrec from TPF and VM systems is discussed. See section "Processing EREP offloaded history data sets from TPF, VSE and VM systems" on page 18. for additional information.
- In Appendix C, "Hardware data collection and reporting task" on page 81, the Hardware Data Collector now includes additional parameters in support of logrec from TPF and VM systems. Please see INTERVAL EREPWAIT and READ EREPDSN parameters in section C.1, "How the parameters work with the Hardware Data Collector program" on page 81.

Second Edition, March 2005 with APAR PQ96746

New functionality is added to the z/OS Service Agent to support HIPER/PE reporting and OMIS. Service Agent can now electronically notify customers of critical software fixes (HIPER APARs) and PTFs in Error (PEs) as well as the ability to electronically download the fixes for these problems. This AHA (Automatic Hiper Alert) report and PTF delivery feature is available to customers who have purchased certain software contracts ("ETS" in EMEA and "Swxcel Enterprise Edition" in the US).

The following summarizes changes made to this edition:

- 5.0, "Chapter 5 - Software and Hiper data collection and reporting" on page 25 is changed to describe how to configure and enable it.

About this guide

This guide provides information on the usage of the Electronic Service Agent for zSeries and S/390 program product. The guide contains:

- Overview information
- Setup and prerequisite information
- Installation instructions
- Configuration instructions
- Usage information

Who should read this guide?

This guide is intended for zSeries and S/390® system software administrators and support staff responsible for the installation, configuration, and activation of Electronic Service Agent for IBM zSeries and IBM S/390. Throughout this guide, Electronic Service Agent for IBM zSeries and IBM S/390 is also referred to as Service Agent.

Personnel responsible for installing and configuring the Service Agent for hardware data collection and reporting should be familiar with or have a working knowledge of zSeries and S/390 architectures, MVS system commands and SMP/E installation skills.

Personnel responsible for installing and configuring the Service Agent for software and data collection and reporting should be familiar with or have a working knowledge of zSeries and S/390 architecture, MVS system commands, the installation's SMP/E CSI (Consolidated Software Inventory) structure, the UNIX System Services environment.

Related information

The following publications, program directories, or Web sites may be useful to you while working with Service Agent.

Program Directory for Electronic Service Agent for zSeries and System/390	GI11-2492-03
SMP/E for z/OS User's Guide	SA22-7773
SMP/E for z/OS Commands	SA22-7771
SMP/E for z/OS Reference	SA22-7772
SMP/E for z/OS Messages, Codes and Diagnosis	SA22-7770
z/OS Unix System Services User's Guide	SA22-7801
z/OS MVS JCL Reference	SA22-7597
z/OS MVS JCL User's Guide	SA22-7598
z/OS MVS Initialization and Tuning Reference	SA22-7592
Hardware Management Console Operations Guide Version 2.9.1	SC28-6857
Note: All s/390 publications can be found at the website: http://www.ibm.com/servers/eserver/zseries/zos/bkserv/	

1.0 Chapter 1 - What is Service Agent?

Electronic Service Agent for IBM zSeries and IBM S/390 is a program product owned by International Business Machines Corporation or one of its subsidiaries (IBM), and is copyrighted and licensed, not sold. Service Agent is a no-charge, orderable, installable program product that runs on z/OS or z/OS.e operating systems.

Electronic Service Agent for zSeries and S/390 is intended to replace the Service Director/2 (SD/2) for collection hardware i/o errors and reporting to IBM.

Electronic Service Agent for zSeries and S/390, combined with network centric architecture provides information to IBM service and support personnel that results in improved service delivery to the customer. When enabled by you, this code collects selected data and transmits it to IBM periodically. It communicates with IBM using the Hardware Management Console or directly using secure HTTP over SSL (HTTPS) with APAR PK15210 installed.

Service Agent has an optional service which will electronically notify customers of critical software fixes (Hiper APARs) and PTFs in Error (PEs) as well as the ability to electronically download the fixes for these problems. The AHA (Automatic Hiper Alert) report and PTF delivery feature is available to all customers who have installed APAR PK42978. Throughout this document, Hiper and Hiper/PE are used interchangeably unless otherwise specified.

Service Agent may be enabled to collect information from the zSeries and S/390 environment, including:

- Selected I/O hardware failures from z/OS system. EREP offloaded history files from TPF, VSE and VM systems can also be processed by Service Agent
- I/O statistical data
- Installed IBM z/OS software information
- Installed service for IBM z/OS software

The collected information can then be used to provide improved customer support and tailored service offerings.

For additional information and benefits refer to the Electronic Service Agent Brochure at

ftp://ftp.software.ibm.com/s390/serviceagent

2.0 Chapter 2 - Service Agent installation

This chapter explains how to obtain the Service Agent program product and recommendations for installing and activating Service Agent in your environment.

2.1 Installation recommendations

The installation, configuration and activation tasks required to enable data collection and reporting to IBM by Service Agent for your hardware, and software resources are presented in this guide so that each data type can be enabled for data collection and reporting individually from each other. This approach allows you to implement functionality of Service Agent in a phased-in fashion. The five data types for which information can be collected and reported on are:

- Hardware
- Software
- Hiper

2.2 Collecting and reporting data to IBM

Each Service Agent data type (Hardware, Software and Hiper)
has its own data collection and reporting considerations.

Hardware data should be collected for each instance of a LOGREC data set. So, for each system that has its own LOGREC, a Hardware Data Collector started task needs to be running to collect hardware data. When the LOGREC is a LOGSTREAM, only one instance of the Hardware Data Collector task should be running on **any one** of the systems that is connected to the LOGREC logstream.

Software and Service (PTFs) data which make up the software data type can be collected from any system that has addressability to the SMP/E CSI containing information about the installed products and service on the system. There may be circumstances where all systems do not have addressability to the required resources (for example, GLOBAL CSI). In these cases, software and service information cannot be collected. IBM recommends that in a situation where system images are cloned - where multiple system images are the same based on one system performing the SMP/E target and distribution library management, software data collection should be enabled on only one of the similar systems.

Hiper data is collected from the same CSIs processed for Software and Service (PTFs) data and as such, follows the same rules in terms of system addressability to CSIs and image cloning issues. Hiper collected data is used by IBM for AHA (described earlier) reports and PTFs delivery.

2.3 Enabling and disabling data collection and reporting

To enable data collection and reporting for a specific Service Agent data type, the definition and activation steps documented in this guide must be followed. If you are not planning to enable data collection for a specific data type immediately after installation of Service Agent, it is not necessary to perform the associated definition and activation steps until such time that data collection and reporting for the data type is desired.

Each Service Agent data type may be disabled at anytime after data collection and reporting has been enabled.

For instructions regarding enabling of data collection and reporting for the hardware data type, see 4.0, “Chapter 4 - Hardware data collection and reporting” on page 14.

For instructions regarding enabling data collection and reporting for the software and hiper data types, see 5.0, “Chapter 5 - Software and Hiper data collection and reporting” on page 25.

2.4 Multi-system installation recommendations

In a multi-system environment, you must pay careful attention to the deployment of Service Agent throughout the enterprise. IBM's recommendation is to first install, customize and configure Service Agent on one of the participating systems. After activating Service Agent on the base system, you can then phase in deployment to your other participating systems.

For more information:

- See 5.1, “Customizing and configuring software data collection and reporting in a multi-system environment” on page 32.
- See 4.1, “Customizing and configuring hardware data collection and reporting in a multi-system environment” on page 16.

2.5 Ordering Service Agent

Service Agent is installed using SMP/E and can be ordered as a standalone program product or in one of the following IBM Custom Build package offerings:

- 5751-CS5 IBM ProductPac/MVS
- 5751-CS6 IBM FunctionPac/MVS
- 5751-CS4 IBM SystemPac/MVS
- 5751-CS3 MVS Custom-Built PDO (CBPDO)
- 5751-CS9 ServerPac

All Custom Build offerings are offered for Internet delivery in countries where ShopzSeries product ordering is available. Internet delivery reduces software delivery time and allows you to install software without the need to handle tapes. For more details on Internet delivery, refer to the ShopzSeries help information at

http://www.software.ibm.com/ShopzSeries

You choose the delivery method when you order the software. IBM recommends Internet delivery. In addition to Internet and DVD, the supported tape delivery options include:

- 3590
- 3592

2.6 Program Services

The following product has been updated to a new service level by Software Manufacturing.

Product: ELECTRONIC SERVICE AGENT

Date: APRIL, 2008

The program FMID(s) have been updated to a new service level and have been assigned a new SOURCEID.

FMID(s)	SOURCEID
HESV120	SMC0812

Contact your IBM representative for specific information about available program services.

2.7 Installing Service Agent as a standalone program product

Prior to installing the Service Agent, review the Program Directory for IBM Electronic Service Agent for IBM zSeries and IBM S/390 (GI11-2492-03) which comes with the standalone-tape.

2.8 Installing Service Agent using a packaged offering

Refer to the instructions in the installation guide for the specific packaged offering to install Service Agent.

2.9 What to do if Service Agent installation fails

Report failures of Service Agent installation using your normal IBM software support channel.

3.0 Chapter 3 - System Prerequisites

The Program Directory (GI11-2492-03) for Electronic Service Agent for IBM zSeries and IBM S/390, Section 5.0 Installation Requirements and Considerations identifies the system requirements for installing and activating Service Agent. You must read the Program Directory and satisfy the listed prerequisites before attempting to install and activate Service Agent on the operating system.

This chapter discusses Service Agent communication modes and prerequisite activities that need to be verified or completed prior to installing and activating Service Agent. These prerequisites are broken into two categories:

- Hardware prerequisites (HMC communication mode only)
- Software prerequisites

3.1 Communication Modes: HMC and Direct

z/OS Service Agent provides 2 modes of communication with IBM:

1. HMC communication mode which is the traditional communication mode. Data is forwarded by the z/OS Service Agent client (using the FTP protocol) to the HMC Service Agent and subsequently to IBM.
2. Direct communication mode (APAR PK15210). Data is forwarded directly to IBM from the z/OS Service Agent client using a secure connection. The secured connection is implemented using HTTPS. This implementation removes dependency on HMC to have a separate LAN connection for Service Agent use. All Service Agent's components are enhanced to use this feature: software and hardware.
3. HMC Service Agent also provides two methods of communication with IBM:
   a. Traditional dial up mode.
   b. LAN/Internet connection mode available only on z9 zSeries systems.

Note

All the subsequent steps associated with Hardware prerequisites are NOT required if you plan to employ Direct Communication mode with IBM.

3.2 HMC Connectivity

1. If you have more than one Hardware Management Console, choose **one** that you want to use for working with the Service Agent program. This is called your focal Point Hardware Management Console.
2. The focal point Hardware Management Console needs to be attached to the Customer LAN and its IP address needs to be accessible to every operating system where the Customer wishs to install and run Service Agent. There are three methods for achieving the above condition:
   a. Connect the Hardware Management Console to the Customer LAN via a bridge or otherwise.
   b. Connect the Hardware Management Console to the Customer LAN using a second LAN adapter. This method will allow the host MVS systems to FTP the data to the HMC via the Customer LAN but does not expose the HMC functions to the Customer LAN. The HMC will use a private network on the other LAN adapter to communicate with its managed systems.
   c. Install a separate Hardware Management Console on the Customer LAN. This Hardware Management Console will need to have its own phone line and will not be a part of the Processor complex.

3.3 Hardware prerequisites

OS/2®-based HMC only

1. The requisite LIC for the 2064 Hardware Management Console is Driver 38 and above, currently either EC J10091 (ECA189) or EC J10092 (ECA188).

   Other systems are supported on Driver 26W with MCL 040 EC F99933. Contact your local IBM Service Representative for more details.

   Notes:

   a. The modem communications on the Hardware Management Console must be set for ASYNC in order to use Service Agent. Service Agent **will not** work with SDLC or SNA communications.

   b. Verify Company and Account Information resident on the focal point Hardware Management Console.

      The IBM CE should have already entered the necessary Account Information on the focal point Hardware Management Console workstation. To verify the Company and Account information:

      1) Logon to **SYSPROG** and select **Console Actions.**

      2) Select **Customize Account Information**. There are two tabs (**Company** and **Account**). The company information can be changed here or it can be changed later on during the Service Agent Enablement function. Changing the data now affects the whole Hardware Management Console, whereas changing the data later affects only the Service Agent section.

      The Account data can be viewed for accuracy, but may only be changed by an IBM CE. If there is any question about the data, call your CE for verification. For automatic dispatching of an IBM CE, the voice phone number you provide needs to be one that has been registered with IBM Service (1-800-426-7378).

2. Verify Automatic Service Call Reporting Automatic Service Call Reporting must be enabled if the focal point Hardware Management Console is going to place calls to RETAIN. If Automatic Service Call Reporting is not enabled, I/O hardware errors are not reported to RETAIN and no CE will be dispatched. To verify if Automatic Service Call Reporting is enabled:

   - Select **Customize Dial Information**.
   - Ensure the box ***Authorize Automatic Service Call Reporting*** is checked.

z9 HMC only

1. The Hardware Management Console for the z9 Enterprise Complex (EC) is a completely new design from the existing HMC available on zSeries servers. It is sometimes referred to as "The Next Generation HMC." The z9 EC HMS is no longer an OS/2®-based system but a closed platform that only supports the HMC application and will not allow the installation of any other applications. Existing prior generation HMCs cannot be used to manage a z9 EC.

   The z9 EC HMC also supports the following zSeries and S/390 processors when at the right driver and MCL level:

   a. zSeries 990 at Driver 55 with MCL 132 to EC J13486

   b. zSeries 890 at Driver 55 with MCL 132 to EC J13486

   c. zSeries 900 at Driver 3G with MCL 194 to EC J11213

   d. zSeries 800 at Driver 3G with MCL 194 to EC J11213

   e. Parallel Enterprise Server - Generation 5 and 6 at Driver 26 with the following MCLs:

      1) MCL 174 to EC F99918

      2) MCL 009 to EC J11172

      3) MCL 009 to EC J10392

4) MCL 006 to EC J11920

Notes:

1. The outbound communications on the Hardware Management Console must be set to use either the local modem (for dialing out) or an existing Internet commection.

   a. Logon to **SYSPROG**
   Hardware Management Console (Version 2.9.0) is displayed at the top of the screen verifying that this is the z9 HMC

   b. Select **Console Actions**

   c. Select **Hardware Management Console Settings**

   d. Select **Customize Outbound Connectivity**

   e. Check the box **Enable local system as a call-home server**

   f. Select either the **Local Modem** or **Internet** tab depending on whether you want the HMC to phone home using the local modem or existing Internet connection.

      1) If **Local Modem** selected, then check the box **allow local modem dialing for service**.

      2) If **Internet** selected, then check the box **allow existing Internet connection for service**.

2. Verify Company and Account Information resident on the focal point Hardware Management Console.
   The IBM CE should have already entered the necessary Account Information on the focal point Hardware Management Console workstation. To verify the Company and Account information:

   a. Logon to **SYSPROG**
   Hardware Management Console (Version 2.9.0) is displayed at the top of the screen verifying that this is the z9 HMC

   b. Select **Console Actions**

   c. Select **Hardware Management Console Settings**

   d. Select **Customize Customer Information**. There are three tabs (**Administrator**, **System** and **Account**). The company information can be changed here, or it can be changed later on during the Service Agent Enablement function. Changing the data now affects the whole Hardware Management Console, whereas changing the data later affects only the Service Agent section.

   The Account data can be viewed for accuracy, but may only be changed by an IBM CE. If there is any question about the data, call your CE for verification. For automatic dispatching of an IBM CE, the voice phone number you provide needs to be one that has been registered with IBM Service (1-800-426-7378).

3. Verify Automatic Service Call Reporting

   Automatic Service Call Reporting must be enabled if the focal point Hardware Management Console is going to place calls to RETAIN. If Automatic Service Call Reporting is not enabled, I/O hardware errors are not reported to RETAIN and no CE will be dispatched. To verify if Automatic Service Call Reporting is enabled:

   a. From the **Hardware Management Console Settings** select **Customize Remote Service**.

   b. Ensure the boxes **Enable Remote Service Requests** and **Authorize Automatic Service Call Reporting** are checked.

Note

All the subsequent steps associated with Enabling the HMC are NOT required if you plan to employ Direct Communication mode with IBM.

3.4 Enabling the Hardware Management Console for Service Agent use

Note

The steps you are about to complete pertain only to Service Agent and do not have any effect on the way the focal point Hardware Management Console reports errors on processors.

OS/2®-based HMC only

1. Verify or obtain the IP address of the focal point Hardware Management Console
   a. Logon as **ACSADMIN**
   b. Go to **Console Actions**
   c. Select **Hardware Management Console settings**
   d. The IP address is displayed in this panel.
   Record this IP address. You will need it to configure the other Service Agent components.
2. Under *Console Actions*, select **Enable Hardware Management Console Services**. It is recommended to enable this focal point Hardware Maintenance Console as a **Phone Server**, if there is a phone line connected to it.
3. Under *Console Actions*, select the icon titled ***Enable zSeries Electronic Service Agent***. A multi-page legal agreement panel is displayed, which requires acceptance (**I Agree**) (for best performance, use the page up and page down keys to view). Near the top of the first page, the current status of Service Agent is displayed. If Service Agent is currently enabled, it tells you the user ID and date it was enabled.

   Note

   If you do not agree to the terms in the panel, you may select **Cancel** or **Discontinue** and Service Agent will not be enabled.

4. After selecting **I Agree**, a second panel is displayed. Verify the information in the lower fields is complete and accurate, especially the voice phone number. For automatic dispatching of an IBM CE, this phone number must be the same as the one registered with IBM Service (1-800-426-7378). This information is used by IBM Service to contact you if you should have a failure on IBM maintained hardware.

   Then select **Continue**.
5. The next panel has two check boxes. You may allow Service Agent to process I/O error data, or Software (Software and Service (PTFfs) data as configured on host), or both. Check the applicable boxes. The operating system sends the data to the focal point Hardware Management Console using FTP. The user ID is set as esa390 and is not changeable.

   After supplying a password for this user ID, select **Continue**.

   Note

   Record this password for later use. You will need it during configuration of the Service Agent collection attributes

6. Select a time when you would like Service Agent to send accumulated I/O statistical data to IBM. Service Agent must send data to IBM at least once a day. When you are done, select **Finish**. If Service Agent was disabled prior to this action, a Service Agent call will be sent to IBM to confirm registration of this focal point Hardware Management Console.

Note

Service Agent is disabled using this same icon. At the bottom of the legal panels, select **Discontinue** to prevent the focal point Hardware Management Console from sending Service Agent data to IBM. Be sure to deactivate the corresponding Service Agent software on the z/OS images as well.

z9 HMC only

1. Verify or obtain the IP address of the focal point Hardware Management Console
   a. Logon as **ACSADMIN**
   b. Select **Console Actions**
   c. Select **Hardware Management Console settings**
   d. Select **Customize Network Settings**
   e. Select **LAN Adapters**
   f. If there are 2 LAN adapters, there will be 2 IP addresses displayed. You may need to verify with your network support personnel which IP address is connected to the customer LAN. Record this IP address. You will need it to configure the other Service Agent components.
2. Under **Console Actions**, select the icon titled "Enable zSeries Electronic Service Agent." A multi-page legal agreement panel is displayed, which requires acceptance (**I Agree**) (for best performance, use the page up and page down keys to view). Near the top of the first page, the current status of Service Agent is displayed. If Service Agent is currently enabled, it tells you the user ID and date it was enabled.

   Note: If you do not agree to the terms in the panel, you may select **Cancel** or **Discontinue** and Service Agent will not be enabled.
3. After selecting **I Agree**, a second panel called the **Data Selection** Panel is displayed. The **Data Selection** panel is comprised of 4 sections as follows:
   a. Data Types: This has 2 check boxes which specifies the data types that Service Agent is allowed 2 process:
      1) *IBM I/O Device Error data.* This indicates that Service Agent is to process hardware error data from logrec.
      2) *IBM I/O Device Error Data.* This indicates that Service Agent is to process Software data - Software and Service (PTFs) data.

      Please check the applicable boxes as desired.
   b. **FTP Password**: If you are not using Direct Connection to transmit data directly to IBM from the host then supply an FTP password. Service Agent will send data to the HMC using FTP. Please note that the user ID is set as *esa390* and is not changeable.

      Note: If you are not using Direct Connection then record this password for later use. You will need it during configuration of the Service Agent collection attributes.
   c. **Transfer Time**: Select a time when you would like Service Agent to send accumulated I/O statistical data to IBM. Service Agent must send data to IBM at least once a day.
   d. **FTP Access**: If you are not using Direct Connection, you can create an FTP access table to specify the IP addresses of only those systems that can FTP data to this HMC. When you are done, select **OK**. If Service Agent was disabled prior to this action, a Service Agent call will be sent to IBM to confirm registration of this focal point Hardware Management Console.

```
FTP Access

Set the addresses of the systems that are to be allowed to
FTP data into this Hardware Management Console, or select
to allow access for any system.

X Allow FTP access from any address

Select  TCP/IP Address  Comment
   _    9.23.246.231    XENA


|Add|     |Remove|
```

Note: Service Agent is disabled using this same icon. At the bottom of the legal panels, select **Discontinue** to prevent the focal point Hardware Management Console from sending Service Agent data to IBM. Be sure to deactivate the corresponding Service Agent software on the z/OS images as well.

Direct Connectivity

Service Agent (with PTF UK13197) can transmit your data (to IBM) either using the HMC or directly from the z/OS host using your existing Internet connection. This Internet connection uses a security rich transmission mode which employs HTTP over SSL (HTTPS).

Some installations might prefer the direct mode because it saves having to configure a separate LAN connection to the HMC for Service Agent use as well as remove the dependency on the HMC.

3.5 Host Software prerequisites

1. Ensure your Driving System has one of the following installed (Driving System is defined as the system used to install the Service Agent program):

Program Number	Product Name and Minimum VRM / Service Level
5655-G44	IBM System Modification Program Extended (SMP/E) for z/OS 3.5.x

2. Refer to the Program Directory for a list of mandatory and functional prerequisites required on your Target System for Service Agent. The target system is defined as the system on which the Service Agent program will be installed.

   See the IBM Publication Center to view the Program Directory located at:

   http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi

   Mandatory Requisites

   The mandatory requisites listed in the Program Directory must be satisfied for any of the data types chosen to be enabled for data collection and reporting. The mandatory requisites are the minimum requirements for the Service Agent product to run.

   Functional Requisites

   The functional requisites that must be satisfied are based on the Service Agent data types that are enabled for data collection and reporting.

   IBM 31-bit SDK for z/OS, Java Technology Edition product must be installed on the target system if one of the following is true:

- Software data type is enabled for data collection and reporting
- Hiper/PE is enabled for data collection and reporting
- Direct communication mode (non-HMC) using HTTPS is employed

The following verions of IBM 31-bit SDK for z/OS, Java Technology Edition are currently supported.

- IBM 31-bit SDK for z/OS, Java 2 Technology Edition, V5 (5655-N98)
- IBM 31-bit SDK for z/OS, Java Technology Edition, V6 (5655-R31)
- IBM 31-bit SDK for z/OS, Java Technology Edition, V6.0.1 (5655-R31)
- IBM 31-bit SDK for z/OS, Java Technology Edition, V7 (5655-W43)

Notes:

Installation and configuration of the JAVA products is not required if only Hardware data collection and reporting is desired and the method of communication with IBM is through the HMC (non-direct).

IBM recommends that the latest TCP/IP and JAVA service levels applicable to your operating system be applied to ensure successful communication between the components of Service Agent and IBM.

If a proxy server is used in non-HMC Direct Communication mode, APAR PK35167 must be applied.

3. Ensure that SMP/E DDDEF entries exist for the following libraries when Service Agent is installed:
   - CEE.SCEELKED
   - CEE.SCEELKEX
   - SYS1.CSSLIB
   - ISP.SISPLOAD

   Note

   Service Agent uses the CALLLIBS function provided in SMP/E to resolve external references during installation.

4. Ensure you have enough space allocated for Service Agent to run.

Total DASD Space Required by Electronic Service Agent	
Library Type	Total Space Required
Target	80 tracks 3390
Distribution	112 tracks 3390
HFS	10 MB

Non-SMP/E permanent and temporary data sets are required to run Service Agent.

For a list of non SMP/E permanent datasets and their sizes, refer to the Program Directory GI11-2492-03, figure title "*Storage Requirements for Electronic Service Agent Non-SMPE datasets*."

5. TCP/IP must be installed and configured on the zSeries or S/390 host system(s).
6. TCP/IP (LAN) path must exist between the focal point Hardware Management Console and z/OS images for Service Agent data transmission. **This step is not required if direct communication mode is employed**.
7. It is recommended that there is a communications line (telephone line) connected to the focal point Hardware Management Console, and that the Hardware Management Console be configured as a Phone Server. (See the Hardware Management Console documentation). **This step is not required if direct communication mode is employed**.

System and software prerequisites required for HMC communication mode

Different components related to Electronic Service Agent for zSeries 5655-F17 program product	HW errors Reporting prereqs	SW Inventory Collection prereqs	Hiper/PE service prereqs
Operating System: any supported level of z/OS and z/OS.e	X	X	X
LAN connection between HMC and host via TCP/IP	X	X	X
Installation of Service Agent program product 5655-F17 on host system using SMP/E	X	X	X
Activation of Service Agent on HMC	X	X	X
Hardware Management Console: • HMC Driver 26+MCL or >= Driver 38 • Modem setup asynchroneous (TCP/IP)	X	X	X
IBM or OEM TCP/IP with FTP enabled	X	X	X
IBM Security Server or equivalent ISV product	X	X	X
31-bit SDK for z/OS, Java 2 Technology Edition, V5 or later		X	X
UNIX System Services enabled and activated	X	X	X
ISPF/PDF - Invoke ESA dialog to define SMP/E CSI		X	X

System and software prerequisites required for Direct communication mode

Different components related to Electronic Service Agent for zSeries 5655-F17 program product	HW errors Reporting prereqs	SW Inventory Collection prereqs	Hiper/PE service prereqs
Operating System: any supported level of z/OS and z/OS.e	X	X	X
LAN/Internet system host connection to ISP provider	X	X	X
Installation of Service Agent program product 5655-F17 on host system using SMP/E	X	X	X
IBM or OEM TCP/IP	X	X	X
IBM Security Server or equivalent ISV product	X	X	X
31-bit SDK for z/OS, Java 2 Technology Edition, V5 or later	X	X	X
ISPF/PDF - Invoke ESA dialog to define SMP/E CSI	X	X	X

4.0 Chapter 4 - Hardware data collection and reporting

Hardware data can be setup to collect hardware i/o errors data using one of the following programs/tasks:

- HESRDLOG - collects and sends data to HMC on regular interval. Does not support direct connection to IBM over Internet.
- HESHWRDL - collects data which is sent using direct connection through HESEVEM and HESSCAN.

The Hardware Data Collector started task first begins by reading a data set (***hlq.***HESPARMS) for its operating parameters. LOGREC is then read on a five minute cycle, saving hardware records in a temporary dataset (***hlq.***HESTEMP in HESRDLOG, ***hlq.***HW in HESHWRDL). State information is written to the dataset (***hlq.***HESSTATE). When critical data has been read,

- HESRDLOG will forward the contents of ***hlq.***HESTEMP via HMC/FTP to the IBM Server and, if successful, empty the HESTEMP file in preparation for further processing. If the forwarding is not successful, HESRDLOG will retain the contents of HESTEMP to add to and forward later when the HMC becomes free.
- HESHWRDL will rename the temporary data set from ***hlq.***HW to ***hlq.***HW.Dddhhmm.EREPDATA (where dd is the day of the month, hh is the hour and mm is the minute), reallocate a new temporary data set and continue processing. HESEVEM and HESSCAN will transmit the timestamped data set to the IBM Server.

Write To Operator (WTO) messages are utilized to inform the operator of critical error conditions. Job status information can be found in the spooled output ddname HESPRINT for both HESRDLOG and HESHWRDL and spooled output from HESSCAN's SYSPRINT as well as Dialog History can be used for HESHWRDL transmission status information.

Below is a summary of the steps to configure and activate the Hardware Function of Service Agent upon the completion of the SMP/E installation of Service Agent.

- Allocate data sets required by the Hardware Data Collection and Reporting function of Service Agent in dataset ***hlq.***SHESJCL
- APF-authorize the Service Agent load library dataset (***hlq.***SHESLMOD)
- Update and add Service Agent procedures to SYS1.PROCLIB
- Add a step in the EREP JCL job to run and capture Service Agent data
- Create started task IDs and started task entries in the STARTED RACF class for HESRDLOG/HESHWRDL using the supplied sample job in dataset ***hlq.***SHESSAMP
- Start the hardware collection by starting the HESRDLOG/HESHWRDL procedure in the SYS1.PROCLIB dataset.

Customizing and configuring for hardware data collection and reporting via HESRDLOG.

1. Run the HESALCHW job provided in ***hlq.***SHESJCL. Update the high level qualifier in the JCL to match that of your installation standards.

> **Note**
>
> Every system that is going to report hardware error data MUST HAVE THE FOLLOWING DATA SETS ALLOCATED, UNIQUE FOR THAT SYSTEM. In a shared DASD environment, to ensure its uniqueness for each system image, this is generally done using different high level or 2nd level qualifiers. Example:
>
> ***hlq.***system name.HESPARMS

Running this job allocates and populates the following data sets required by the hardware data collection and reporting function of Service Agent:

- ***hlq.***HESSTATE -Data set stores pointer information for selected hardware module.
- ***hlq.***HESPARMS - Parameter dataset for hardware module.
- ***hlq.***HESTEMP -Data set for temporary storage of hardware records.

2. APF-authorize the Service Agent load library dataset ***hlq.***SHESLMOD. This is done by adding the authorization for the data set in PROGxx in SYS1.PARMLIB. A sample HESAPF can be found in ***hlq.***SHESSAMP.
3. Add and update Hardware Collector procedure in SYS1.PROCLIB, setting the high level qualifiers to match those that you have specified in the HESALCHW job. Sample hardware procedures (both HESRDLOG and HESHWRDL) are provided in data set ***hlq.***SHESSAMP.

   This must be done on every system that has a LOGREC data set or DASD-only log stream. In a sysplex that utilizes a coupling facility logstream to manage the LOGREC, you only have to create the hardware started task on one of the images connected to the log stream.
4. To protect against the possibility of Service Agent missing an I/O device record in the error recording data set (i.e. SYS1.LOGREC), the following job step should be added to the start of any EREP job that results in the clearing of the error recording data set (ZERO=Y):

```
//HESRDLOG EXEC PGM=HESRDLOG,
// PARM='ENV HLQ=hlq, EREP' <==hlq of user datasets
//*                          allocated with jcl HESALCHW in step #1
//STEPLIB DD DISP=SHR,DSN=hlq.SHESLMOD <==hlq of load libraries
//* which you specified during SMP/E i nstallation
//* of the Service Agent product
```

> **Note**
>
> This invocation of the hardware collection module results in an immediate reading of the error recording data set (i.e. SYS1.LOGREC), after which control is returned to the Environmental Record Editing and Printing Program (EREP) job.

5. Define the hardware task in either the RACF started procedures table (SPT) or in RACF CLASS (STARTED). The HESSTHW sample job shipped in dataset ***hlq.***SHESSAMP creates a started task entry for HESRDLOG/HESHWRDL using the RACF STARTED CLASS. This entry is assigned the TRUSTED RACF status.

> **Note**
>
> The HESSTHW sample job defines the hardware started task with the RACF attribute of TRUSTED. This allows hardware collection task to access the data sets required for hardware data collection and reporting in the z/OS environments, without any specific RACF permissions.

   If you decide not to define these tasks as TRUSTED, then refer to the table in Appendix A, "Security authority required by Service Agent" on page 74 to find out the minimum authority required by the hardware collection task to access its required resources.

> **Note**
>
> As of z/OS 1.4, services that use TCP/IP (specifically FTP) requires USS and thus an OMVS segment. Consequently, the HESSTHW job includes an OMVS segment if you plan to use and activate the Hardware collector task.

6. Additional HESRDLOG customization step Edit section 1 of each ***hlq.***HESPARMS dataset that you allocated in Step 1 with the HESALCHW JCL. Specify the correct IP address and FTP password in your environment:

```
REMOTE HOST = #IP name or addr.
REMOTE PASSWORD = # from HMC
```

Note

Use the Focal Point Hardware Management Console IP Address and FTP password obtained while performing the steps in 3.4, "Enabling the Hardware Management Console for Service Agent use" on page 8.

4.1 Customizing and configuring hardware data collection and reporting in a multi-system environment

When an error occurs, the system records information about the error in either the LOGREC data set or a sysplex-wide LOGREC log stream. The diagnostic information provides a history of all hardware failures, selected software errors, and selected system conditions. Since an installation can consist of only coupling facility log streams, only DASD-only log streams, only LOGREC data sets, or a combination thereof, the hardware collection started task is designed to work with LOGREC data sets or LOGREC log streams. Service Agent customization for hardware collection implementation is the same, regardless of the LOGREC recording medium that is being used. The only stipulation is the number of instances of the hardware collection started task that is activated. This is dependent on the type of LOGREC recording medium that is being used and this is described in the ensuing sections.

Note

IBM does not recommend running mix modes hardware data collection in your complex. Either employ the HMC to forward data to IBM, using HESRDLOG task and HMC SA; or forward data directly to IBM from the client host using HESHWRDL and HESSCAN tasks.

Steps 1-5 of the previous section need to be repeated for every system where the hardware collection task is activated.

Note

To determine the current LOGREC recording medium in use on your system, type the following command at the MVS console:

```
DISPLAY LOGREC,CURRENT
```

If log stream is the recording medium, then the following is displayed:

```
IFB090I 16.57.55 LOGREC DISPLAY 092
   CURRENT MEDIUM = LOGSTREAM
      MEDIUM NAME = SYSPLEX.LOGREC.ALLRECS
         STATUS = CONNECTED
```

If a LOGREC data set is the recording medium, then the following is displayed:

```
IFB090I 16.57.55 LOGREC DISPLAY 066
   CURRENT MEDIUM = DATASET
      MEDIUM NAME = SYS1.CPAC.LOGREC
```

The Medium Name for the LOGREC data set will be different, depending on the name that you have established.

Multi-system environment using LOGREC data sets

In a multi-system environment where LOGREC data sets are to be used for the error and environmental recording, you must have an instance of the hardware collection task running on each system that has a LOGREC data set allocated.

Multi-system environment using DASD-only log streams

In a multi-system environment where DASD-only log streams are to be used for the error and environmental recording, you need to have an instance of the hardware collection task running on each system that has a DASD-only log stream allocated. Since DASD-only log streams are single system in scope, only one system can connect to a DASD-only log stream.

Multi-system environment using coupling facility log stream

In a multi-system environment where the coupling facility log stream is to be used for the error and environmental recording, only a single instance of the hardware collection task should be running on any one of the systems that is connected to the coupling facility log stream. Since the coupling facility log stream provides a single repository for all of the MVS images in a sysplex, activating the hardware collection started task for hardware collection and reporting on more than one system results in duplicate data, duplicate service calls, and erroneous tape statistical data being presented to the IBM CE.

It is the responsibility of the installation to ensure that only one instance of the hardware collection task is attached to the coupling facility log stream in a sysplex, as no checking is done for multiple instances of hardware collection reading the coupling facility log stream in a sysplex.

Modifying hardware data collection and reporting task parameters

The hardware collection started task is controlled through the use of parameters, keywords and variables that can be assigned a value and passed to the hardware collection program. Many of these parameters are intended for use only under IBM direction. See C.1, “How the parameters work with the Hardware Data Collector program” on page 81 for details on the usage of parameters, keywords and variables by the hardware collection started task.

TCP/IP considerations

- If you are running multiple IP stacks in your environment and would like to include a specific IP stack and its configuration parameters to hardware collection module then you must add a SYSTCPD DD statement in the hardware collection procedure pointing to the TCPDATA information as follows:

  ```
  //SYSTCPD DD DISP=SHR,DSN=tcpdata
  ```

  where tcpdata is the name of the file containing the TCPDATA configuration.

- Similarly, if you need to include specific FTP parameters then you should also add a SYSFTPD DD statement in the hardware collection procedure pointing to the FTP.DATA information as follows:

  ```
  SYSFTPD DD DISP=SHR,DSN=ftpdata
  ```

  where ftpdata is the name of the file containing the FTP configuration.

Excluding devices from hardware data collection and reporting

You may want to exclude a device or a number of devices from Service Agent. For example, if an installation has mixed (IBM and non-IBM) vendors that have the same device type (i.e. 3390, 3490, etc.) then all non-IBM devices appear as an IBM device type. You may wish to exclude non-IBM devices by device address in order to limit processing to only IBM devices.

To exclude (no data will be sent to IBM, nor will a service representative be dispatched) a device or multiple devices, complete the following step:

1. Edit the HESPARMS dataset and go to Section 2. Create one of the following entries:

```
READ CUA=(N0121)           - to exclude device address 0121.
READ CUA=(N033X)           - to exclude device addresses 0330 through 033F
READ CUA=(N0120:N024F) - excludes all devices between 0120 and 024F.
```

Including devices for hardware data collection and reporting

All devices are implicitly included. In the event there are only a couple of device types to be reported, you may find it easier to use the include parameter instead of the exclude function (as shown above).

Note

If you include a device, you must code a statement for every device type you want included.

To include a single device type:

1. Go to the end of Section 3 of the HESPARMS dataset to see the examples. (The # sign is a comment flag.) Make the following change:

```
READ DEVICE=(3390,2027,20) - the format is (device type, OBR code, MDR code)
```

Note

All devices for specified device type are included unless a device or multiple devices are excluded by device address.

The "EREP Reference" manual provides detailed information regarding the OBR and MDR codes under sections "OBR Codes" and "MDR Codes." These sections contain tables to help you cross-reference OBR/MDR codes and devices.

You cannot limit processing to only IBM devices by coding a device type in the include parameter because the OBR and MDR codes are the same for both IBM and non-IBM devices.

Processing EREP offloaded history data sets from TPF, VSE and VM systems

With APAR PK06867 installed, Logrec data from TPF, VSE and VM systems that has been offloaded to an EREP history file using the EREP program, can be processed by the Hardware Data Collector.

The Hardware Data Collector will read the EREP file in its entirety looking for records of interest just as it would for online Logrec/Logstream. Following the initial processing of offloaded EREP history files, the Hardware Data Collector will start a repeated cycle of alternately processing online Logrec/Logstream and offloaded EREP history files.

There are two parameters, specified in the HESPARMS data set that drive the processing of offloaded EREP history files as follows:

1. Specifying the unique qualifier(s) that comprise the EREP data set(s) to be processed.

   In Section 2 of the HESPARMS data set you will see the following example (the # sign is a comment flag).

   ```
   READ EREPDSN=EREP.HISTORY - partial qualifier of EREP history file(s)
   ```

   The qualifier(s) specified are combined with the environment high level qualifier to compose the name of the fully qualified EREP history file.

   Example:

If PARM='env ***hlq***.SYS4.DEV' is specified in the Hardware Data Collector task a catalog search will be performed looking for all partially qualified data set(s) starting with 'SYS4.DEV. EREP.HISTORY'.

All data set(s) found including 'SYS4.DEV.EREP.HISTORY' will be considered as candidates for processing.

2. Specifying the time interval to check for presence of offloaded EREP history data set(s).

   In Section 3 of the HESPARMS data set you will see the following example (the # sign is a comment flag).

   ```
   INTERVAL EREPWAIT = 14400 - seconds to wait between EREP reads
   ```

   This is the default and specifies that every 14400 seconds (4 hours), the Hardware Data Collector will check to see if there are any offloaded EREP data set(s) to be processed.

Activating hardware data collection and reporting using HESRDLOG task

Activate the hardware data collection and reporting task by issuing the following MVS START command:

```
S HESRDLOG
```

For the very first start, IBM suggests that you add the VERBOSE variable to the ENV keyword passed as a parameter to the HESRDLOG program. The HESRDLOG started task JCL should look like the following example. A sample is provided in ***hlq***.SHESSAMP:

```
//HESRDLOG PROC HESSPREF=HESV120,HESUPREF=HESV120 <====
//*
//*
//HESRDLOG EXEC PGM=HESRDLOG,TIME=1440,DYNAMNBR=300,REGION=0M,
// PARM='ENV HLQ=&HESUPREF.,VERBOSE' (be sure to include the single quotes)
//STEPLIB DD DISP=SHR,DSN=&HESSPREF..SHESLMOD
```

In a sysplex where the LOGREC is a LOGSTREAM, only one instance of the HESRDLOG task should be running on any one of the systems that is connected to the LOGREC logstream. Due to the nature of the LOGSTREAM, data is reported from all of the images connected to the LOGSTREAM in the sysplex. No checking is done for multiple instances of HESRDLOG reading the LOGREC LOGSTREAM in a sysplex.

It is the responsibility of the installation to make sure only one HESRDLOG task is attached to the LOGREC LOGSTREAM in a sysplex. **Activating the HESRDLOG started task for hardware data collection and reporting on more than one system results in duplicate data, duplicate service calls, and erroneous tape statistical data being presented to the IBM CE**.

Activating modified hardware data collection and reporting task parameters immediately

You may make changes in the ***hlq***.HESPARMS dataset, and have the changes take effect immediately, by issuing the MODIFY command. When this command is issued, it causes HESRDLOG to reread the ***hlq***.HESPARMS dataset before the next run cycle takes place. The command syntax is:

```
MODIFY HESRDLOG,REREAD
   or
F HESRDLOG,REREAD
```

Verifying the hardware data collection and reporting task (HESRDLOG) has started correctly

For the very first start, we suggest adding the VERBOSE parm. Compare the output log HESPRINT with the example below. The PARM statement in the started task JCL would look like this:

```
// PARM='ENV HLQ=hlq,VERBOSE'
```

When started, the program tries to allocate the ***hlq.*** HESPARMS data set. It reads in the parameters from ***hlq.***HESPARMS. The next step is to verify that an FTP logon operation can be completed with the focal point Hardware Management Console. If successful, the program then ascertains the name of the LOGREC, allocates ***hlq.***HESSTATE and ***hlq.***HESTEMP, reads the LOGREC, and writes to ***hlq.***HESSTATE and ***hlq.***HESTEMP if needed. Finally the datasets are released, and the program goes into the five minute wait state.

The important statements in the example output (shown below) are highlighted with ====>>>>.

```
HES80999I 01-25 103508 HESRDLOG 20001220 14:59:59 01.01.00
HES80001I 01-25 103508 5655-F17 (C) Copyright IBM Corp. 2000,2002.
HES80001I 01-25 103508 All Rights Reserved.
HES80001I 01-25 103508 US Government Users Restricted Rights -
HES80001I 01-25 103508 Use, duplication or disclosure restricted by
HES80001I 01-25 103508 GSA ADP Schedule Contract with IBM Corp.
HES80001I 01-25 103508 Licensed Materials - Property of IBM.
HES80001I 01-25 103508

====>>>> This next line is the PARM card from the started task

HES80002I 01-25 103508 Command Line: ENV HLQ=TEST,VERBOSE.

====>>>> read of HESPARMS This is actually the Keyword and
         Variable values in AFFECT

HES80109I 01-25 103508 File HESPARMS was read: 131 records.
HES80021I 01-25 103508 Parm value: env hlq= SDTEST2.
HES80021I 01-25 103508 Parm value: env disable= N
HES80021I 01-25 103508 Parm value: env enable= N
HES80021I 01-25 103508 Parm value: env scan= N
HES80021I 01-25 103508 Parm value: env query= N
HES80021I 01-25 103508 Parm value: env erep= N
HES80021I 01-25 103508 Parm value: env verbose= Y
HES80021I 01-25 103508 Parm value: env debug= N
HES80021I 01-25 103508 Parm value: env estae= Y * Provided on PARM, not in HESPARMS
HES80021I 01-25 103508 Parm value: env wto= N
HES80021I 01-25 103508 Parm value: env abend= N

====>>>> next 3 lines are values assigned for the focal point
         Hardware Management Console

HES80021I 01-25 103508 Parm value: remote host= 9.99.999.999
HES80021I 01-25 103508 Parm value: remote user= esa390
HES80021I 01-25 103508 Parm value: remote password= ******
HES80021I 01-25 103508 Parm value: remote checkw= 600
HES80021I 01-25 103508 Parm value: remote send= 14400
HES80021I 01-25 103508 Parm value: remote warning= 3600
HES80021I 01-25 103508 Parm value: remote failc= 5
HES80021I 01-25 103508 Parm value: remote old= 1
HES80021I 01-25 103508 Parm value: remote transmit= N
HES80021I 01-25 103508 Parm value: remote fileext= .sod
HES80021I 01-25 103508 Parm value: remote oldext= .SOD
HES80021I 01-25 103508 Parm value: remote clear= N
HES80021I 01-25 103508 Parm value: remote path=
HES80021I 01-25 103508 Parm value: remote filename= mvsg
HES80021I 01-25 103508 Parm value: remote passive= Y
HES80021I 01-25 103508 Parm value: #remote localfile= 'TEST.HESTEMP'
HES80021I 01-25 103508 Parm value: interval wait= 300
HES80021I 01-25 103508 Parm value: interval records= 10000
HES80021I 01-25 103508 Parm value: interval busyw= 60
HES80021I 01-25 103508 Parm value: interval busyc= 1
HES80021I 01-25 103508 Parm value: interval iterations= 0
HES80021I 01-25 103508 Parm value: interval spool= 7
HES80021I 01-25 103508 Parm value: read startdate= 0101025F
HES80021I 01-25 103508 Parm value: read starttime= 00000000
HES80021I 01-25 103508 Parm value: read startttrz= 00000000
HES80021I 01-25 103508 Parm value: #read records entries=5
HES80021I 01-25 103508 Parm value: read records=(30*)
HES80021I 01-25 103508 Parm value: read records=(90:91)
HES80021I 01-25 103508 Parm value: read records=(a2)
HES80021I 01-25 103508 Parm value: read records=(a3*)
HES80030I 01-25 103508 Setting Spool timer interval of 604800 seconds.

====>>>> Start of FTP check

HES80164I 01-25 103508 Checking remote HMC availability.
HES80110I 01-25 103508 File INPUT was written: 4 records.
HES80109I 01-25 103510 File OUTPUT was read: 19 records.
```

```
HES80109I 01-25 103510 File HESTEMP was read: 0 records.

=====>>>> If there are no errors, you should see this next line

HES80165I 01-25 103510 Starting readlog loop.
HES80109I 01-25 103510 File HESSTATE was read: 1 records.
HES80160I 01-25 103510 Time data: 0101025F00000000, 0101025F09285079, 0101025F10334442.
HES80159I 01-25 103510 TTRz data: 00000000, 00001200, 00001300.
HES80109I 01-25 103510 File HESDATA was read: 19 records.
HES80110I 01-25 103510 File HESTEMP was written: 16 records.
HES80110I 01-25 103510 File HESSTATE was written: 1 records.

=====>>>> This is the end of the first read cycle.
         The program begins a wait.

HES80031I 01-25 103510 Begin Interval Wait of 300 seconds.
```

If the program does not appear to be working, and your output does not match the highlighted sections, add the DEBUG parm to the started task parm card. Adding the DEBUG parm provides much more detail about the actual data set allocations. The name of the LOGREC data set will also be found in the output. Verify that the LOGREC name is correct, and that the three datasets get allocated.

Activating hardware data collection and reporting using a HESHWRDL task in a local system

In a sysplex where the LOGREC is a LOGSTREAM, only one instance of the HESHWRDL task should be running on any one of the systems that is connected to the LOGREC logstream. Due to the nature of the LOGSTREAM, data is reported from all of the images connected to the LOGSTREAM in the sysplex. No checking is done for multiple instances of HESHWRDL reading the LOGREC LOGSTREAM in a sysplex.

It is the responsibility of the installation to make sure only one HESHWRDL task is attached to the LOGREC LOGSTREAM in a sysplex. Activating the HESHWRDL started task for hardware data collection and reporting on more than one system results in duplicate data, duplicate service calls, and erroneous tape statistical data being presented to the IBM CE.

A "Local" system is a system that does both collecting and reporting of hardware errors; that is, it contains both HESHWRDL and HESEVEM.

In a situation where there is only one LOGREC, a single "Local" system is sufficient.

In a new installation of the Hardware application, a "Local" system should be implemented first as follows:

1. Set the envvars environment variables for the "Local" system. Some examples are as follows: (see page 30).
   - *ibmhes.external.erepdata.collector-interval=60*
   - *ibmhes.erepdata.dataset.prefix=ZSA*
   - *ibmhes.external.erepdata.collector=Y*
   - *ibmhes.erepdata.dataset.cleanup=Y*
2. Enable Service Agent to transmit hardware data to IBM (with APAR PK15210 installed). This is done by selecting Option 3.8 Schedule of the Service Agent ISPF Dialog and specifying Y in the Collect Hardware Data field.
3. Activate the hardware data collection and reporting task by issuing the following MVS START command:

   ```
   S HESHWRDL
   ```

   For the very first start, IBM suggest that you add the VERBOSE variable to the ENV keyword passed as a parameter to the HESHWRDL program. The HESHWRDL started task JCL should look like the following example. A sample is provided in ***hlq.*** SHESSAMP:

```
//HESHWRDL PROC HESSPREF=HESV120,HESUPREF=ZSA.S01 <====
//*
//*
//HESHWRDL EXEC PGM=HESHWRDL,TIME=1440,DYNAMNBR=300,REGION=0M,
// PARM='ENV HLQ=&HESUPREF.,VERBOSE' (be sure to include the single quotes
//STEPLIB DD DISP=SHR,DSN=&HESSPREF..SHESLMOD
```

Processing externally collected EREP data from Remote Systems

See "Activating hardware data collection and reporting using a HESHWRDL task in a local system" on page 21 for a description of "Local" and "Remote" systems.

Remote systems may transmit their data in two ways:

1. Ensuring that the collected logrec data file EREPDATA is written to shared DASD that's accessible by both the HESHWRDL data collector and the HESEVEM transmitting component. p.For example, one can set up HESALCHW for the HESHWRDLs so that they are initiated from ZSA.N01.HESPARMS, ZSA.N02.HESPARMS, ZSA.N03.HESPARMS, etc., producing ZSA.N01.HW.D030848.EREPDATA, ZSA.N02.HW.D030852.EREPDATA, ZSA.N03.HW.D030919.EREPDATA, etc. and each of the EREPDATA files will be transmitted.
2. If a shared-DASD environment is not possible, a sample system to use MVS FTP to transmit to the "local" system can be found in ***ftp://ftp.software.ibm.com/s390/serviceagent***

Activating modified hardware data collection and reporting task parameters immediately

You may make changes in the ***hlq.***HESPARMS dataset, and have the changes take effect immediately, by issuing the MODIFY command. When this command is issued, it causes hardware task to reread the ***hlq.***HESPARMS dataset before the next run cycle takes place. The command syntax is:

```
MODIFY HESHWRDL,REREAD
or
F HESHWRDL,REREAD
```

Verifying the hardware data collection and reporting task (HESHWRDL) has started correctly

For the very first start, we suggest adding the VERBOSE parm. Compare the output log HESPRINT with the example below. The PARM statement in the started task JCL would look like this:

```
// PARM='ENV HLQ=hlq,VERBOSE'
```

When started, the program tries to allocate the ***hlq.***HESPARMS data set. It reads in the parameters from ***hlq.***HESPARMS. If successful, the program then ascertains the name of the LOGREC, allocates ***hlq.***HESSTATE and ***hlq.***HESTEMP, reads the LOGREC, and writes to ***hlq.***HESSTATE and ***hlq.***HESTEMP if needed. Finally the datasets are released, and the program goes into the five minute wait state.

The important statements in the example output (shown below) are highlighted with ====>>>>.

```
====>>>> The first line is the compile date (yyyymmdd),
         time and latest PTF level

HES80999I 12-19 180005 HESHWRDL 20051209 13:20:57 01.02.00 UK09779.
HES80001I 12-19 180005 5655-F17 (C) Copyright IBM Corp. 2005,2005.
HES80001I 12-19 180005 All Rights Reserved.
HES80001I 12-19 180005 US Government Users Restricted Rights -
HES80001I 12-19 180005 Use, duplication or disclosure restricted by
HES80001I 12-19 180005 GSA ADP Schedule Contract with IBM Corp.
HES80001I 12-19 180005 Licensed Materials - Property of IBM.
HES80001I 12-19 180005

====>>>> This next line is the PARM card from the started task
```

```
HES80002I 12-19 180005 Command Line: ENV HLQ=HESR130.FUNCTEST,VERBOSE
HES80003I 12-19 180005 open_file.
HES80109I 12-19 180005 File HESPARMS was read: 177 records.
HES80107I 12-19 180005 File HESPARMS is being Dynamically freed.
HES80003I 12-19 180005 %%%logrec_select_dflt.
HES80021I 12-19 180005 Parm value: env hlq= HESR130.FUNCTEST.
HES80021I 12-19 180005 Parm value: env disable= N
HES80021I 12-19 180005 Parm value: env enable= N
HES80021I 12-19 180005 Parm value: env scan= N
HES80021I 12-19 180005 Parm value: env query= N
HES80021I 12-19 180005 Parm value: env erep= N
HES80021I 12-19 180005 Parm value: env trace= N
HES80021I 12-19 180005 Parm value: env verbose= Y
HES80021I 12-19 180005 Parm value: env debug= Y
HES80021I 12-19 180005 Parm value: env authmode=N
HES80021I 12-19 180005 Parm value: env estae= Y * Provided on PARM, not in HESPARMS
HES80021I 12-19 180005 Parm value: env wto= Y
HES80021I 12-19 180005 Parm value: env abend= N
HES80021I 12-19 180005 Parm value: remote checkw= 600
HES80021I 12-19 180005 Parm value: remote send= 14400
HES80021I 12-19 180005 Parm value: remote warning= 3600
HES80021I 12-19 180005 Parm value: remote failc= 5
HES80021I 12-19 180005 Parm value: remote old= 1
HES80021I 12-19 180005 Parm value: remote clear= N
HES80021I 12-19 180005 Parm value: remote filename= XENA
HES80021I 12-19 180005 Parm value: #remote localfile='HESR130.FUNCTEST.HESTEMP'
HES80021I 12-19 180005 Parm value: interval wait= 300
HES80021I 12-19 180005 Parm value: interval Erepwait= 14400
HES80021I 12-19 180005 Parm value: interval records= 10000
HES80021I 12-19 180005 Parm value: interval busyw= 60
HES80021I 12-19 180005 Parm value: interval busyc= 1
HES80021I 12-19 180005 Parm value: interval iterations= 0
HES80021I 12-19 180005 Parm value: interval spool= 7
HES80021I 12-19 180005 Parm value: read erepdsn=
HES80021I 12-19 180005 Parm value: read startdate= 0105200F
HES80021I 12-19 180005 Parm value: read starttime= 00000000
HES80021I 12-19 180005 Parm value: read startttrz= 00000000
HES80021I 12-19 180005 Parm value: #read records entries=5
HES80021I 12-19 180005 Parm value: read records=(30*)
HES80021I 12-19 180005 Parm value: read records=(90:91)
HES80021I 12-19 180005 Parm value: read records=(a2)
HES80021I 12-19 180005 Parm value: read records=(a3*)
HES80030I 12-19 180005 Setting Spool timer interval of 604800 seconds.
HES80165I 12-19 180005 Starting readlog loop.
HES80109I 12-19 180005 File HESSTATE was read: 0 records.
HES80161I 12-19 180005 Scanning LOGSTREAM from: FROM=(2005/200,00:00:00),LOCAL.
HES80178I 12-19 180005 Processing Logrec from z/OS system
HES80160I 12-19 180005 Time data: 0105200F00000000, 0105353F00143918, 0105353F15340586.
HES80159I 12-19 180005 TTRz data: 00000000, 00000000, 00000000.
HES80003I 12-19 180005 close_file.
HES80109I 12-19 180005 File HESDATA was read: 3208 records.
HES80110I 12-19 180005 File HESTEMP was written: 350 records.
HES80107I 12-19 180006 File HESTEMP is being Dynamically freed.
HES80161I 12-19 180006 Scanning LOGSTREAM from: FROM=(2005/200,00:00:00),LOCAL.
HES80179I 12-19 180006 350 records passed filtering.
HES80003I 12-19 180006 %%%send_file.
HES80167I 12-19 180006 Sending file with 350 records.
HES80003I 12-19 180006 local_file: 'HESR130.FUNCTEST.HESTEMP'.
HES80003I 12-19 180006 rename_file: HESR130.FUNCTEST.XENA.EREPDATA.
HES80063I 12-19 180006 Erep data set "'HESR130.FUNCTEST.HESTEMP'" was renamed to "HESR130.FUNCTEST.XENA.EREPDATA".

=====>>>> The HESEVEM task is notified and subsequently dispatches
         the HESSCAN task to retrieve the data collected

HES80003I 12-19 180006 Event Manager dispatched for Hardware request.
HES80110I 12-19 180008 File HESSTATE was written: 1 records.
HES80107I 12-19 180008 File HESSTATE is being Dynamically freed.

=====>>>> This is the end of the first read cycle. The program begins a wait.

HES80031I 12-19 180008 Begin Interval Wait of 300 seconds.
```

There is more output than that presented here such as allocation / de-allocation output. This is left out for brevity purposes. You can also start HESHWRDL in DEBUG mode which provides less output. VERBOSE mode implies DEBUG as well. VERBOSE is useful for discovering errors.

If the program does not appear to be working, and your output does not match the highlighted sections, add the VERBOSE parm to the started task parm card. Adding the VERBOSE parm provides much more detail about the actual data set allocations. The name of the LOGREC data set will also be found in the output. Verify that the LOGREC name is correct, and that the three datasets get allocated.

5.0 Chapter 5 - Software and Hiper data collection and reporting

Software information is collected from the SMP/E CSI data on a daily basis based on configuration values. Collected software information is compared with previously collected information and if changed, will be formatted and sent to IBM.

Hiper data is collected from either a subset of, or the same SMP/E CSIs specified for software information. The collection schedule is based on an interval (in weeks) as outlined by the configuration values.

Collected data is formatted in a temporary XML file and sent, using FTP, to the focal point Hardware Management Console or directly to IBM using HTTPS. The temporary file is sent by Hardware Management Console Service task, which checks regularly for any information to be sent to IBM. A response XML file is generated describing the status of the data sent to IBM. The response file is parsed, analyzed and logged by Service Agent.

Service Agent verifies the success of information received and stored by IBM. In case of an error, Write To Operator (WTO) messages are utilized to inform the operator of critical error conditions and the error is logged in ERRLOG inventory. Job status information can be found in the spooled output ddname SYSPRINT.

Software and Hiper data is collected and transmitted using configuration values supplied by a user using the Service Agent Dialog. Externally collected data is transmitted using the same values.

Below is a summary of the steps to configure and activate the Software and Hiper data collection and reporting function of Service Agent upon the completion of the SMP/E installation of the Service Agent:

- Allocate data sets required by the Software Data Collection and Reporting function of Service Agent by modifying and running the sample HESALCSW job provided in data set ***hlq.***SHESJCL
- APF-authorize the Service Agent load library using sample provided in data set ***hlq.***SHESSAMP(HESAPF)
- Authorize Service Agent programs for Service Agent Dialog usage by modifying the IKJTSOxx member in SYS1.PARMLIB. The sample is provided in data set ***hlq.***SHESSAMP(HESTSO)
- APF-authorize Java DLL libraries used by Service Agent. The sample job is provided in data set ***hlq.***SHESSAMP(HESJAVA).
- Create started task entries in the RACF STARTED class profile for HESEVEM and HESSCAN. The sample job is provided in data set ***hlq.***SHESSAMP(HESSTSW).
- Update and add Service Agent procedures HESMAIN, HESEVEM and HESSCAN to SYS1.PROCLIB. The sample procedures HESMAIN, HESEVEM and HESSCAN are provided in data set ***hlq.***SHESSAMP.
- Determine the 31-bit SDK for z/OS, Java Technology Edition to be used by Service Agent. Verion 5.0 and up is currently supported.
- Verify/update environment variables in the ../usr/lpp/esa/esa1.2/envvars file:
  - CLASSPATH and LIBPATH for SDK for z/OS, Java Technology Edition, V5 and up.
  - Time zone
  - Service Agent System call variables
- Customize Service Agent Dialog ISPF interface.
- Configure Service Agent using Service Agent Dialog.
- Start the Verify transaction to verify connection to IBM.
- Enable scheduled collection for Data Types of your choice.

- Enable software data collection and reporting.
- Enable Hiper/PE collection and reporting.
- Optionally enable hardware collection if you activated HESHWRDL hardware collection task.

Customizing and configuring for Software Data Collection and Reporting

Note

Perform the following sections and steps only if software data collection and reporting are to be enabled.

Follow the steps below to have your Service Agent environment customized:

1. Run the HESALCSW job provided in ***hlq.***SHESJCL. Update the high level qualifier in the JCL to match your installation standards. However, it is important that the high level qualifier you specify in the HESALCSW job must be the same as the high level qualifier which you specify during the configuration of Service Agent using the Service Agent Dialog user interface. With APAR PK15210 installed, this high level qualifier must also be the same as that used in the HESHWRDL task (ENV ***hlq.***parameter).

   Note

   For multi-systems or sysplex users, a unique set of the following user-defined data sets has to exist in every z/OS image from which you want Service Agent to collect and transmit data.

   Running this job allocates and populates the following data sets required by Service Agent:

   - CONFINV - Configuration inventory used to store Service Agent customization parameters.
   - CUSTINV - Customer inventory used to store collected software and service data.
   - DIALLOG - Service Agent Dialog activity is logged here.
   - ERRLOG - Repository where errors are logged for diagnostic purposes.
   - HELPINV - HELP inventory where help texts for ISPF dialogs are stored.
   - WKSPINV - WORKSPACE inventory where all datasets attributes are stored. The scanner uses these attributes to perform dynamic allocation during its execution
   - WORKINV - Repository where each unit of work (or called work element) is stored.
   - WORKLOG - History or log of all performed or performing work.

   If you plan to use SMS to manage allocated data sets, read section "Using SMS to manage software data" on page 31 before updating and running the HESALCSW job.

2. APF-authorize the Service Agent load library dataset ***hlq.***SHESLMOD. This is done by adding the authorization for the data set in PROGxx in SYS1.PARMLIB. A sample HESAPF can be found in ***hlq.***SHESSAMP.
3. Update PARMLIB member IKJTSOxx to add the required Service Agent programs to the list of authorized programs in TSO. A sample member HESTSO is provided in data set ***hlq.***SHESSAMP.
4. APF-authorize Java DLL libraries used by Service Agent. Run HESJAVA job supplied in ***hlq.***SHESSAMP to mark the selected Java libraries as APF-authorized.

   Note

   Note: Whenever you refresh the Java run-time libraries you must run this job again to APF-authorize selected Java libraries as APF-authorized.

5. Set up started tasks for HESSCAN and HESEVEM.

Create user IDs and STARTED class entries for HESSCAN and HESEVEM. A sample can be found in member HESSTSW in ***hlq.***SHESSAMP.

Note

The HESSTSW sample job defines the Service Agents started tasks with the RACF attribute of TRUSTED. This allows Service Agent to create and access Service Agents data sets in both the MVS and Unix environments, without any specific RACF permissions. If you decide not to define these tasks as trusted, see Appendix A, "Security authority required by Service Agent" on page 74.

6. Modify the sample procedures HESSCAN, HESEVEM, and HESMAIN supplied in ***hlq.***SHESSAMP to reflect your installation's naming conventions. Remember that the high-level qualifiers must match those that you have specified in the HESALLOC and HESALCSW allocation jobs. In addition, it is essential that you update the _CEE_ENVFILE parameter to point to the right directory where envars in located. After that, add the procedures to SYS1.PROCLIB.
7. Determine the IBM 31-bit SDK for z/OS, Java Technology Edition to be used by Service Agent. Verion 5.0 and up is currently supported. Use UNIX command JAVA -FULLVERSION to determine what Java SDK level is installed.
8. Verify CLASSPATH and LIBPATH Java environment variables for SDK for z/OS, Java Technology Edition, V5 and up in /usr/lpp/esa/esa1.2/envvars. If there are updates to be made, perform the following:
   - Create a directory for the environment variables file (for example, etc/esa120)
   - Copy the environment variables file envvars from /usr/lpp/esa/esa1.2 to the environment directory created by you.
   - Update the envvars file with the correct JVM library locations and product jar files.
   - Verify and update time zone environment variables if necessary:

     Update /etc/esa120/envvars with the correct time zone setting. Refer to previous step (directly above) to have /etc/esa120 directory created. The current setting is for Eastern Standard Time. If the setting is omitted, default is GMT0 (Greenwich Mean Time). The format of the TZ environment variable is:

     ```
     TZ=standardHHdaylight
     ```

     Standard - An alphabetic abbreviation for the local standard time zone.

```
MIT Midway Islands Time
HST Hawaii Standard Time
AST Alaska Standard Time
PST Pacific Standard Time
PNT Phoenix Standard Time
MST Mountain Standard Time
CST Central Standard Time
EST Eastern Standard Time
IET Indiana Eastern Standard Time
PRT Puerto Rico and US Virgin Islands Time
CNT Canada Newfoundland Time
AGT Argentina Standard Time
BET Brazil Eastern Time
CAT Central African Time
GMT Greenich Mean Time
ECT European Central Time
EET Eastern European Time
ART (Arabic) Egypt Standard Time
EAT Eastern African Time
MET Middle East Time
NET Near East Time
PLT Pakistan Lahore Time
IST India Standard Time
BST Bangladesh Standard Time
VST Vietnam Standard Time
CTT China Taiwan Time
JST Japan Standard Time
ACT Australia Central Time without Daylight Savings Time
AET Australia Eastern Time with Daylight Savings Time
SST Solomon Standard Time
NST New Zealand Standard Time
```

HH - The time offset westward from the Greenwich Time. Use leading minus sign (-) to indicate offset eastward of GMT.

Daylight - An abbreviation for the local daylight savings time zone.

You can use the samples below for your local time setting:

- For Pacific Time: TZ=PST8PDT
- For UK: TZ=GMTODES
- For Central European Time zone: TZ=CET-1DST

Note

It's imperative that the time zone setting reflects the same system time used on the z/OS host machine. Service Agent components (namely those written in Java and C/C++) utilize this time setting, but other components (those written in Assembler) will use the z/OS host system time. Discrepancies between both time settings will lead to different reporting times among Service Agent module, affecting the chronological sequence of logs as well as hampering debugging.

9. Verify and update Service Agent System calls environment variables if necessary. Service Agent environment variables are identified in the "envvars" file by the "ibmhes" prefix. Please note that the envvars file is created in step 8 (directly above). Please uncomment (remove the # sign) for those variables that you will need. The environment variables used by the Service Agent are as follows:

   Environment variables for ESA Java Component

   - *ibmhes.home=/usr/lpp/esa/esa1.2*

     This is the default home directory for the HESSCAN Started Task.

   - *ibmhes.dtd=/usr/lpp/esa/esa1.2/dtd*

This is the home directory for all DTD files required by the HESSCAN Started Task for parsing XML response files.

- *ibmhes.data=/usr/lpp/esa/esa1.2/data*

  This is the default working directory for the HESSCAN Started Task. Working files are written to this directory by Service Agent; accordingly, this directory must be writable. If you decide to change the default directory, the files in this directory must always be copied to your new directory after every Service Agent upgrade. The HESMKDIR exec that is shipped with Service Agent sets the permission bits to 755. This setting assumes that Service Agent is the owner of the directory and thus has full access (Read, Write and Search). If Service Agent is defined as a RACF TRUSTED task or as a superuser (UID 0), then the setting is not important. If you decide not to define this task as TRUSTED, see Appendix A, "Security authority required by Service Agent" on page 74.

- *ibmhes.log=/usr/lpp/esa/esa1.2/log*

  This is the default Service Agent log directory. Files are written to this directory by the Service Agent and as such, its directory must be writable. The HESMKDIR exec that is shipped with the Service Agent correctly sets the permission bits to 755. This setting assumes that the Service Agent is the owner of the directory and so has full access (Read, Write and Search). If the Service Agent is defined as a TRUSTED task or a superuser (UID 0), then the setting is not important. If you decide not to define this task as trusted see Appendix A, "Security authority required by Service Agent" on page 74.

Environment variables for Communication

- HMC Connection - FTP Mode

  This variable must be defined if Dialog panel 3.3 shows FTP mode is in use -- that is, Direct Communication=N.

  - *ibmhes.ftp.mode=PASSIVE*

    This variable is used for sending data with the HMC and is the default Service Agent FTP connection mode. It can be set to either PASSIVE or ACTIVE; note that ACTIVE mode should not normally be set; it can cause problems with fire walls.

- Direct Communication Mode

  These variables will be used if Dialog panel 3.3 shows Direct Communication=Y. They are provided by IBM and should not be changed.

  - *ibmhes.url=https://207.25.252.200:443/support/electronic/itssdr/IESproxy.wss*

    This parameter is IBM IP address URI for Service Agent direct connection using your existing Internet connection.

  - *Ibmhes.jks=/usr/lpp/esa/esa1.2/IES.jks*

    This parameter is Service Agent supplied Java Key Store certificate required on IBM server side for sending data directly to IBM using your existing Internet connection.

- Direct Communication Proxy Definitions

  The HTTP proxy or the SOCKS proxy environment variables are used only if proxy servers are in use in your Internet communications setup. Define one or the other.

  The following are the parameters for the HTTP proxy:

  - *ibmhes.http.proxyHost*

    This parameter defines an IP address if Service Agent must use an HTTP Proxy server for Direct Communication.

  - *ibmhes.http.proxyPort*

    This parameter defines a port for the HTTP Proxy server.

If the proxy requires authentication then remove the comment sign from the following and add the required information.

- *ibmhes.http.username*

  This parameter defines an user name for the HTTP Proxy server.

- *ibmhes.http.password*

  This parameter defines a password for the HTTP Proxy server.

The following are the parameters for the SOCKS proxy:

- *ibmhes.socks.proxyHost*

  This parameter defines an IP address if Service Agent must use a SOCKS Proxy server for Direct Communication.

- *ibmhes.socks.proxyPort*

  This parameter defines a port for the SOCKS Proxy server.

If the proxy requires authentication then remove the comment sign from the following and add the required information.

- *ibmhes.socks.username*

  This parameter defines an user name for the SOCKS Proxy server.

- *ibmhes.socks.password*

  This parameter defines a password for the SOCKS Proxy server.

Environment variables for some Data Collection

These variables are used only if Hardware transactions is enabled in Dialog panel 3.8.

- Hardware Collection
  - *ibmhes.external.erepdata.collector=Y/N*

    This variable specifies whether externally collected logrec data (i.e. logrec data collected by the Hardware Data Collector running on a system other than the sending system) is to be processed and transmitted to IBM.

  - *ibmhes.erepdata.dataset.cleanup=Y/N*

    This variable specifies whether Service Agent will remove an EREPDATA file when it has been successfully transmitted. This variable is ignored is ignored if ibmhes.erepdata.dataset.prefix is not assigned.

  - *ibmhes.erepdata.dataset.prefix*

    This optional variable sets the high-level qualifier for all EREP data sets. If this variable is not assigned, the High Level Qualifier defined in Dialog option 3.3 will be used.

  - *ibmhes.external.erepdata.collector-interval=60*

    Specifies the number of minutes (60 - 1440) that Service Agent is to wait, before checking for externally collected erep data.

10.

Note

Run IVP sample job HESHIVP in SHESSAMP library to verify the environment variables customization. If the IVP fails, check for error messages in output, make appropriate changes and rerun until successful completion.

11. Customize Service Agent Dialog ISPF Interface.

The Service Agent Dialog interface must be customized before you can use the Service Agent Dialog to complete required configuration steps for collecting and reporting software data.

IBM recommends for you to include the Service Agent load library in your ISPLLIB or STEPLIB concatenation of your logon procedure. If not, the load library needs to be included in your Linklist.

Modify an existing ISPF selection panel (for example, ISR@PRIM), to include the following:

```
) BODY

E Electronic Service Agent

) PROC

&ZSEL = TRANS(&ZCMD,;
....
E, CMD(%HESCMAIN)

....)
```

HESCMAIN CLIST will allocate product ISPF libraries using ISPF LIBDEF services.

Note

Make copy of the HESCMAIN CLIST provided in ***hlq.***SHESEENU and set &HESSPREF and &HESUPREF variables based on your Service Agent allocation jobs. Additional information is provided in the HESCMAIN CLIST.

12. Invoke the Service Agent Dialog (HESMAIN program) and complete required Service Agent configuration steps.

Note

If you are a first-time user, you must bring up the Service Agent Dialog to accept the Licence Agreement and go through the registration and enrollment process before you can configure and use Service Agent.

The Service Agent Dialog configuration steps are described in detail in "Service Agent Dialog overview" on page 33.

Using SMS to manage software data

SMS can be used to manage Service Agent software data sets, including all MVS data sets created dynamically by Service Agent.

SMS manages data sets through the use of four constructs called data class, management class, storage class, and storage group. Automatic class selection (ACS) routines can be used to either validate or choose the constructs used for each data set, or both.

The HESALCSW job provides allocation for both SMS and non-SMS environments. If you decide to use SMS, then modify the job providing the storage class name. Detailed information is provided as comments in this job. The storage class assigned by you in this job must be provided during the configuration of Service Agent. SMS storage class value for Service Agents dynamically created data sets are specified in the Storage class field of the Service Agent Dialog panel. This value is used if the SMS active field of the Service Agent Dialog contains Y. For additional information, see "Customizing and configuring for Software Data Collection and Reporting" on page 26.

The dynamically created data sets use a high level qualifier specified by you in the High Level Qualifier field of the Service Agent Dialog.

Note

There is currently no provision in Service Agent for management class specification for dynamically created data sets, consequently a default management class will be assigned by your ACS routines. If the assigned default management class is not appropriate for your system, update your management class routine to assign a management class that reflects your storage management policy.

5.1 Customizing and configuring software data collection and reporting in a multi-system environment

In a multi-system environment, you must pay careful attention to the deployment of Service Agent throughout the enterprise. IBMs recommendation is to first install, customize and configure Service Agent on one of the participating systems. After activating Service Agent on the base system, you can then have a phased in deployment to other participating systems. The following topics can assist you in where and how Service Agent should be deployed.

The following sections and steps are only performed if software, hiper/PE data collection will be enabled.

For multi-systems or sysplex users, a unique set of user-defined data sets have to exist in every z/OS image for which you want Service Agent to collect and transmit data. Consequently, you will need to repeat Steps 1-6, 8-11 as described in "Customizing and configuring for Software Data Collection and Reporting" on page 26.

Note

If shared HFS is in use for the JAVA DLL libraries then step 4 is not required to be repeated for those systems that access the shared HFS.

Shared HFS

As of OS/390 R9, all file systems that are mounted by a system participating in shared HFS are available to all participating systems. You must not assume that with shared HFS, two systems can share a common HFS data set for /etc, /tmp, /var, and /dev. This is not the case. Even with shared HFS, each system must have specific HFS data sets for each of these file systems. The file systems are then mounted under the system-specific HFS.

Similarly, Service Agent HFS ../data and ../log directories cannot beshared between different systems and must be located in a system-specific HFS data set such as /etc. The following example can be used to define a system-specific HFS for your shared HFS environment:

Define the /etc first level directory as a symbolic link to /$SYSNAME./etc,A BPXPRMxx member thats used across the entire sysplex (IBM recommendation) would have the following coded:

```
BPXPRMxx
.
SYSPLEX(YES)
.
MOUNT FILESYSTEM(OMVS.&SYSNAME..ETC)
TYPE(HFS) MODE(RDWR) NOAUTOMOVE
MOUNTPOINT(/&SYSNAME./etc)
.
```

The statement /$SYSNAME./etc will resolve to /sysname/etc during parmlib processing, where sysname is the actual system name.

Customize Service Agent envvars to use the defined symbolic link.

```
../esa120/envvars
.
# HES WORK directory
 ibmhes.data=/etc/esa120/data
# HES LOG directory
 ibmhes.log=/etc/esa120/log
```

For each system image using the shared HFS, and where Service Agent is to be activated, create required /sysname/etc/esa120/data and ../log directories.

Software data collection considerations - shared CSI

In a situation where system images are cloned, it is recommended that the software data collection be enabled on only one of these systems.

An example of such a system is an installation where multiple system images are the same, based on one system performing the SMP/E target and distribution library management. The system chosen for collection has to have access to the SMP/E CSI. The selected target zones should reflect the maintenance currently installed on these images.

In order to collect all software data for all systems, the active zones representing these systems would have to be selected. For example:

Systems A is the base system, where all SMP/E product installation and maintenance is installed.

Systems B and C are cloned from system A.

Since system A has access to all SMP/E CSIs, software data collection would be enabled on this system. In order to collect software data for all systems, active zones related to A,B and C should be selected when configuring Service Agent on system A.

Restriction is placed on including multiple global CSIs with zones sharing the same name. In this case a separate instance of Service Agent would have to be activated on another system that has access to these global CSIs. If access to the global CSI is only available on one system, then only one of the duplicate zones can be selected.

If a system image is not participating in software data collection or does not have access to the SMP/E CSIs, then you need to disable software collection on this image.

Service Agent Dialog overview

Service Agent Dialog can be used to perform the following functions:

- Configuring Service Agent
  - Set run time environment options
  - Set data collection and reporting attributes
- Operational control of the Service Agent tasks
  - Start and stop Service Agent
  - Verify connection to IBM
  - Verify system registration information
  - Request immediate (nonscheduled) Software data collection and reporting
- Monitoring Service Agent tasks
  - Monitoring transactions in progress

  - History (work, dialog and error) logs
- Authorize Web Users - optional configuration

5.2 The initial use of Service Agent

The initial use of Service Agent requires you to do the following:

- Read and accept the Service Agent license agreement
- Configure Service Agent providing the following information:
  - Company, Location and Customer Data
  - System user description
  - Service Agent run time environment options
- Configure Service Agent collection attributes
  - System Inventory data
- Verify system registration information
- Enable Service Agent automatic (scheduled) data collection, and select collection data type (software and/or hiper).

Configuring for software data collection and reporting

You must configure certain elements of Service Agent. In doing so, you are setting an environment in which Service Agent can begin to run. Complete the following steps:

1. Access the Service Agent Dialog.

   Note

   If you need assistance using the Service Agent Dialog, press the ***PF1*** function key. Pressing ***PF1*** takes you to help text relevant to your current panel.

   The Service Agent Dialog performs edit checking on selective input fields. It ensures that all required fields are complete. If, for whatever reason, you have made a mistake during input, an error message will appear. While the error message is present, you can press the Shift key plus the ***PF1*** function key to obtain additional information about the meaning of the message.

2. Read and accept the license agreement. (Once the agreement is accepted it is not displayed nor accessible again.) In the current version of the Service Agent Dialog, no print function is provided to print the agreement. After accepting the agreement, press ***PF3*** key to continue with the customization.
3. From the Electronic Service Agent Main Menu, select option 3, Configure Service Agent Collection Attributes.

   Note

   Because this is the first time Service Agent has been accessed on your system, all options except option 3 are unavailable. You must provide values for the parameters on the Configure Service Agent Collection Attributes menu before you can access other options from the Electronic Service Agent Main Menu.

4. From the CONFIGURE SERVICE AGENT COLLECTION ATTRIBUTES menu, select options 1, 2, 3 and 4. as these are required by Service Agent to operate. Complete all the required (indicated by an *) fields on those screens (pressing the ***Enter*** key saves the data and pressing the ***PF3*** key returns you to options menu).
5. In option 3.3 (Service Agent configuration) populate required fields in the following sections:

- Service Agent configuration data

  If SMS active is Yes (Y), this means you would like to have the allocation of the data sets used by Service Agent managed by SMS. In this case, you must provide a value for the Storage Class.

  If SMS active is No (N), this means you do not want to have the allocation of the data sets used by Service Agent managed by SMS. In this case, you must provide a value for the VOLSER.

  The field Generic Unit type is defaulted to SYSALLDA. This is for Service Agent to allocate temporary data sets. Modify this value according to your installations standards.

  The field High Level Qualifier is defaulted to HESV120. Data sets used during the running of Service Agent are allocated using this high level qualifier on SMS managed volume or volume which you specified earlier.

  Note

  The High Level Qualifier input here should match the user specified (hesupref) high level qualifier which you specified in the HESALCSW job.

- Connection to IBM

  Select Direct connection or HMC connection

  If HMC connection specified then do the following:

  Enter the IP address of the focal point Hardware Management Console. You must also enter the FTP password of the focal point Hardware Management Console as the password for the esa390 user ID.

  You will be prompted to verify the password.

  Note

  This is the password you first encountered when completing the prerequisites for the focal point Hardware Management Console. See 3.4, “Enabling the Hardware Management Console for Service Agent use” on page 8 for more information on passwords.

- Event Manager and Scanner data

  The scanner and the event manager will always be started in a normal mode. Debug mode causes the generation of much SYSPRINT output—only useful for diagnostic reasons should problems arise. Do not modify this field unless instructed by IBM Support personnel.

6. In option 3.4 (System Information), provide system user description and verify system registration information to make sure that the system matches the one for which you want to collect and report data.
7. Select option 3.5 (Software Inventory), if Software collection will be enabled. The panel allows you to create, modify and view global CSI list (SMP/E Consolidated System Inventory) for which you would like Electronic Service Agent to collect data.

   At least one GLOBAL data set has to be entered and the maximum is 20.

   Consolidated System Inventory (CSI) GLOBALS are used by Service Agent to collect software and service data. When working with System Inventory you will be viewing two displays (System Inventory and CSI Zone Names):

   a. Configure Service Agent Collection Attributes - Software Inventory

      The Configure Service Agent Collection Attributes - Software Inventory display lists all the CSIs that have been defined and shows the number of zones in the CSI and the number of selected zones for which data is collected. CSIs, which you defined in this display, undergo a catalog search to ensure that they exist in your system.

      Select a Global CSI; the Configure Service Agent Collection Attributes - CSI Zone Names display appears.

Note

Following restriction exists:

- Maximum number of global CSIs selection is restricted to 20.

b. Configure Service Agent Collection Attributes - CSI Zones.

The Configure Service Agent Collection Attributes - CSI Zones display lists all the zones defined to a particular CSI. From this panel you can specify to Service Agent, the zones from which you wish to collect data. You do this by choosing a Line command of S (Select) to select a zone or D (Deselect) to deselect a zone.

If a zone has been Selected, a Y is displayed between the ZoneName and the Data Set Name fields. If a zone had been Deselected, the field between ZoneName and Data Set Name is blank.

Note

Following restrictions exist:

- Duplicate zone name selection is not allowed from different global CSIs although this supported by SMP/E.
- Maximum number of zones selection is restricted to 100.
- DLIB zones selection MUST be accompanied by related TARGET zone pair selection. Reporting on DLIBs only is not supported by the product.

8. To enable the automatic collection for data types of your choice, see "Enabling Service Agent to automatically collect and transmit data" on page 44.

Configuring for Hiper report and PTF delivery

Hiper report and PTF delivery (collectively referred to as AHA - Automatic Hiper Alert) is a function that electronically notifies customers of critical software fixes (HIPER APARs) and PTFs in Error (PEs), as well as the ability to electronically download the fixes for these problems. This function is available to all customers who have installed APAR PK42978.

Configuring AHA first requires performing steps 1-7 of "Configuring for software data collection and reporting" on page 34. In other words, Software Inventory collection must be enabled and SMP/E target zones must be selected for Inventory collection prior to continuing with the following additional steps.

1. Verify that zones selected for Software Inventory (opt 3.5) collection include the zones for which AHA is desired. If not, add additional zones as required. The implication is that AHA can only be enabled for zones which have been selected for Software Inventory collection.
2. Select option 3.7 (Automatic Hiper Alert) , if AHA is to be enabled. This will provide the following display:

   Configure Service Agent Collection Attributes - Automatic Hiper Alert

   The Configure Service Agent Collection Attributes - Automatic Hiper Alert display, lists all the zones and their associated CSIs for which AHA is desired. You do this by choosing a Line command of:

   - R (Report) to select a zone for AHA reporting only
   - P (PTFs) to select a zone for both AHA reporting (notification of critical fixes), as well as delivery of these installable critical fixes, based on installed FMIDs and PTFs.
   - D (Deselect) to deselect a zone.

   If a zone has been selected for AHA reporting only, a Y is displayed under the Reports name field. If a zone has been selected for PTFs, a Y is displayed under both the Reports and PTFs fields, since this implies both AHA reporting and delivery of hiper PTFs. Conversely, if a zone has been Deselected for AHA then an N is placed under the respective field (Report and/or PTFs).

3. To enable the automatic collection for AHA see "Enabling Service Agent to automatically collect and transmit data" on page 44.

Verifying the communication connection to IBM

Option 7, from the Service Agent Main menu, displays the status of your last and second last verification request. The first time you access Option 7 the display appears as shown below:

```
------------------- Verify Service Agent Connection --------------------------

PRIM Cmds:(VERify)


Current verification
   Status: Connection verification in progress

   Requested:        Completed:
      Date                 Date  00
      Time                 Time  00:00:00



Last verification
   Status: Never performed

   Requested:        Completed:
      Date                 Date  00
      Time                 Time  00:00:00



Command ==> ____________________________________________________________
```

Figure 1. Verify Service Agent Connection - Empty Panel

Notice the status displayed in the Current and Last verification fields. Current verification is never requested before. Last verfication is never performed.

To verify your Service Agent connection:

1. Select Option 7 from the Service Agent Main Menu.
2. From the command line, type VER and press the ***Enter*** key.

   If you see a message indicating the Service Agent Scanner and Event Manager tasks are not active, Press the ***Enter*** key to confirm and start the Service Agent Data Collect and Send task.

   You will see a message indicating the Scanner and Event Manager are now active.

   Press the ***Enter*** key to run the VERIFY command.
3. You will be returned to the Main menu and the following message will be displayed:

   `HES20005I Your request to VERIFY the service connection was SENT.`

   It will take approximately 5 minutes for HMC communication mode and a few seconds if you have specified Direct Connection.

   Note

   On the Service Agent Main Menu, Service Agent status should read: Verify connection initiated.

4. You will be notified by a TSO message after about five to six minutes indicating if the verify transaction completed successfully or not. Return to Option 7, Verify Service Agent Connection to view the result of the connection.

Note

The system enrollment transactions will be performed to enroll your system before any other transaction can be send to IBM. To check if the system is successfully enrolled go to option 3.4 System Information and check the field System enrolled: Yes/No.

If it is not successful check Error Log for more information regarding the problem, you may want to retry or contact IBM. A successful verification displays as follows:

```
------------------- Verify Service Agent Connection ---------------------------

PRIM Cmds:(VERify)


Current verification
   Status: Verify ran successfully

   Requested:        Completed:
      Date  2006-07-17      Date  2006-07-17
      Time  14:43:12 Time 14:49:12



Last verification
   Status: Verify ran successfully

   Requested:        Completed:
      Date  2006-07-10      Date  2006-07-13
      Time  12:24:44 Time 20:55:35



Command ==> ____________________________________________________________
```

Figure 2. Verify Service Agent Connection - Filled Panel

Forcing data collection

A Force Collection overrides any automatic scheduling of data collection you may have configured.

To perform a Force collection:

1. From the Service Agent Main Menu, select Option 5, Run Service Agent Data Collectors. The following display appears:

```
------------------ Run Service Agent Data Collectors -------------------------

Service Agent is .....................: enabled
   Hardware data collection is ........: disabled
   Software data collection is ........: disabled
     Hiper/PE automatic reporting is ..: disabled

Next scheduled activity:
   Collect and send time   12.20.00   (hh.mm.ss)


Force immediate action:
                       Collect
   Data types          Delta /   Refresh
      Software           N          N       (Y/N)
                       Send data for follwing transactions:
      Hiper/PE                      N       (Y/N)
      Hardware                      N       (Y/N)


 ____________________________________________________________________________
 HES20030W You are about to override the scheduled time and have the data
 collection and transmission invoked immediately. Choose from the list above
 which data collectors you would like to invoke immediately and what action
 to have on them.
 ____________________________________________________________________________
Command ==> ____________________________________________________________________
```

Figure 3. Run Service Agent Data Collectors

2. In the Force field, select the Data types for which you want to Force a collect and Send by placing a Y in the appropriate field.
3. Press the ***Enter*** key to run the Force collection and transmission.

4. You will see a panel showing what data types are going to be collected and sent.

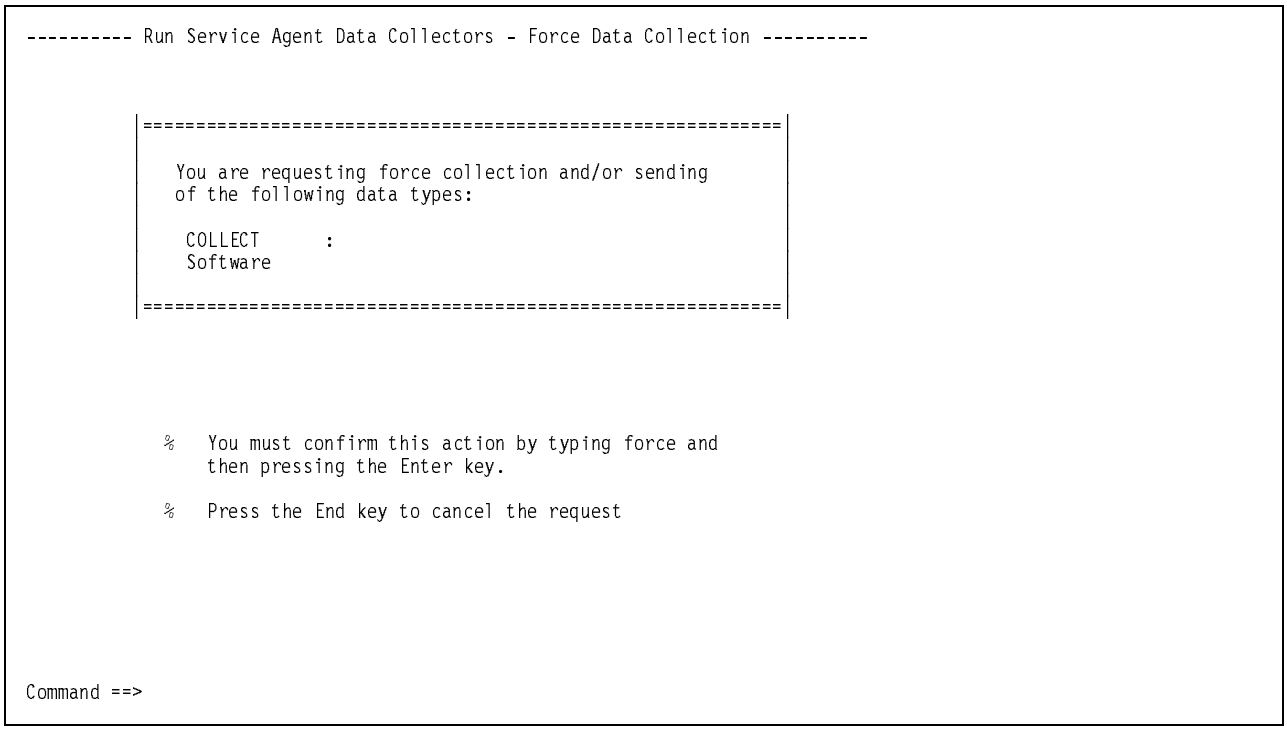

Figure 4. Run Service Agent Data Collectors - Force Data Collection

5. Type the Force command and press the ***Enter*** key to continue.

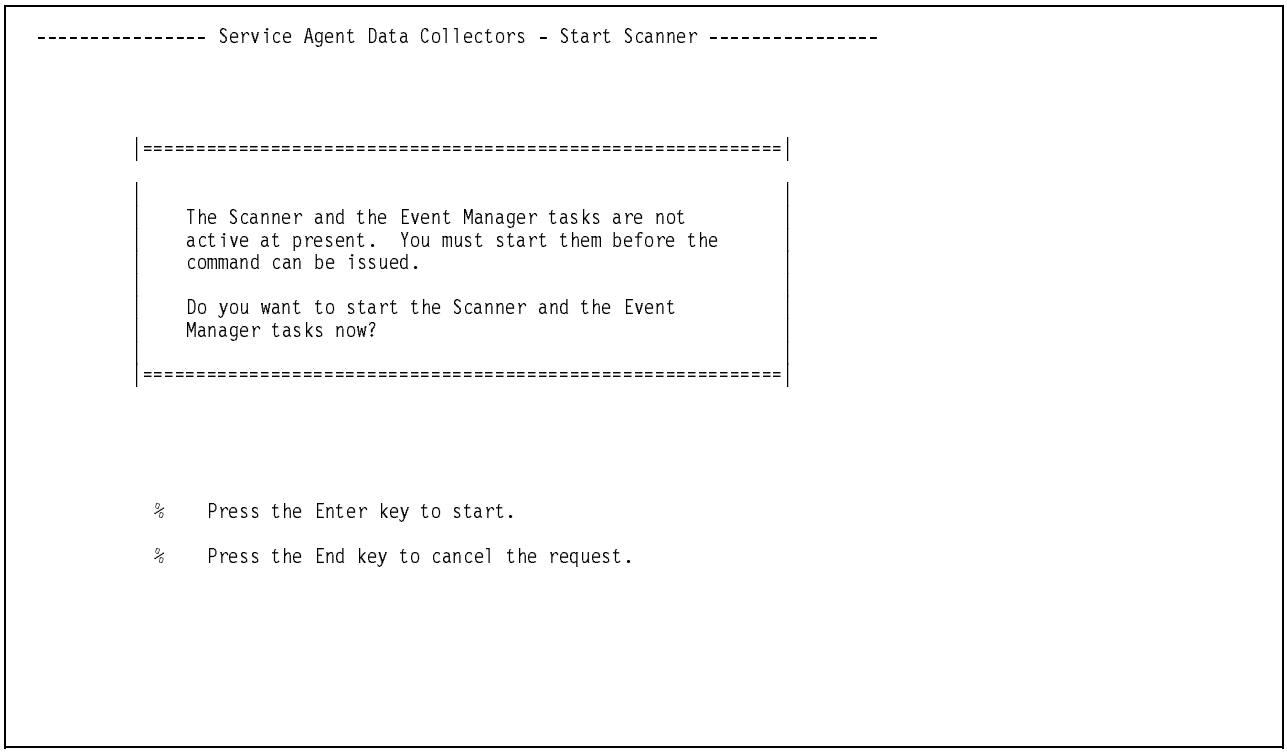

Figure 5. Run Service Agent Data Collectors - Start Scanner

When you see a message indicating the Event Manager and Scanner are not active respond accordingly. Following, you will see a message indicating the Scanner is now active.

6. Press the ***Enter*** key to run the Force command.
7. Press the ***PF3*** key to return to the Main menu.

Note

On the Service Agent Main menu, Service Agent status should read: Force Command Initiated.

Verifying the forced and scheduled data collection

To verify your collections:

1. Select Option 4, Display Service Agent Data Collectors.
2. Check the Last Collect and Last Send fields.

   They should have a date and time value. The Last Collect value is the date and time the collection completed. The Last Send value is the date and time that Service Agent received an acknowledgment from the IBM Data Receiver that it received the data. See the Last Collect and Last Send fields in the display below:

```
---------------- Display Service Agent Data Collectors -----------------------

PRIM Cmds:(Alternate)

Service Agent is .....................: enabled
   Hardware data collection is ........: disabled
   Software data collection is ........: enabled
     Hiper/PE automatic reporting is ..: disabled

Schedule:
   Collect and send time: 14.40.00 (hh.mm.ss)


                  -- Last Collect ---        ---- Last Send ----
Collector:    Date       Time            Date       Time
   Hardware I/O   2006-07-20 12.55.50        2006-07-20 12.56.03
   Software       2006-07-23 14.42.17        2006-07-21 14.42.39
     Hiper/PE     2006-06-06 17.30.05        2006-06-06 17.45.34




Command ==> ____________________________________________________________
```

Figure 6. Display Service Agent Data Collectors

3. At the command line type A to display the date and time of last software delta collection. No delta information is available for the initial run of software collection.

4. Press ***PF3*** to return to the Service Agent Main Menu.

```
---------------- Display Service Agent Data Collectors ------------------------

PRIM Cmds:(Previous )

Service Agent is .....................: enabled
   Hardware data collection is .......: disabled
   Software data collection is .......: enabled
     Hiper/PE automatic reporting is ..: disabled

Schedule:
   Collect and send time: 14.40.00 (hh.mm.ss)


                  --- Last Change ---
Collector:    Date       Time


   Software       2006-07-20 10.20.04




Command ==> ____________________________________________________________
```

Figure 7. Display Service Agent Data Collectors - Alternate

Enabling Service Agent to automatically collect and transmit data

Service Agent can be enabled to perform data collection and reporting automatically on a predetermined schedule for the software data type. It can also be enabled to transmit logrec data collected by the Hardware Data Collector to IBM. When enabled for automatic data collection and reporting the Service Agent will initiate data collection and reporting at a user specified or default time each day for the software data type.

The Enable Service Agent scheduled collection parameter needs to be set to Y (Yes) to enable automatic data collection and reporting on a scheduled basis.

After the Service Agent scheduled collection function is enabled, the software data type automatic data collection and reporting is enabled by default. You can also individually disable or enable data collection and reporting for the software types. To change the Enable Service Agent scheduled collection function to Y (Yes):

1. From the Service Agent Main Menu, select Option 3, Configure Service Agent Collection Attributes.
2. Select Option 8, Schedule.
3. Change the Enable Service Agent scheduled collection field value to Y as shown in the display below:

```
------ Configure Service Agent Collection Attributes      Enter required field

Enable Service Agent scheduled collection.... Y  (Y/N) (*)

Collect hardware data ....... Y  (Y/N) (*)
Collect software data ....... Y  (Y/N) (*)
   Request Hiper/PE report .. Y  (Y/N) (*)


Schedule time for software data type when enabled:
   Collect and send time: 14.40.00 (*) (hh.mm.ss)

Schedule Hiper/PE report and/or PTF delivery frequency when enabled:
   Frequency :      2  (*)   (1-8)   every  2  weekly intervals


(*) Required                                      Press the Enter key to save




Command ==> ____________________________________________________________
```

Figure 8. Configure Service Agent Collection Attributes - Schedule

Once you change the Enable Service Agent scheduled collection field to Y, Collect time, Send time, and Day of week will be set to default values. These values are used by Service Agent to determine when to initiate automatic daily data collection and transmission.

Note

The collect hardware data field must be set to Y if hardware error data is to be sent to IBM.

The default assigned data collection and reporting time values for the software data type are: current local time minus two hours for data collection and current local time minus one hour for data reporting.

Activate Service Agent tasks using option 1 on the Main Menu to allow automatic scheduled collection of the data. See “Starting Software and Hardware (from HESHWRDL) Data Collection and Reporting” on page 70.

4. Enabling Hiper reporting and PTF delivery.

   Request Hiper/PE report: N (Y/N)

The default value for this parameter is N (No). This parameter is visible only if zones have been previously selected for AHA, otherwise this field is disabled. Once you have changed the Request Hiper/PE report to Y and pressed the ***Enter*** key, the AHA frequency field is displayed under Schedule Hiper/PE report and/or PTF delivery

a. Frequency: This specifies the interval in weeks of the next scheduled report.

5. If you want to disable software collection:

   Collect software data: Y (Y/N)

   The default value for this parameter is Y (Yes). This parameter will be visible only if you previously enabled Enable Service Agent scheduled collection, otherwise this option is disabled. If the parameter collect software data is set to N, that means that the Service Agent will NOT automatically collect and transmit software data.

6. Press the ***Enter*** key to save the data.

7. Press the ***PF3*** key to return. If Service Agent tasks have been activated and if Hiper schedule has been enabled, then Hiper reporting and/or PTF delivery will be scheduled according to the frequency interval specified by you.

Optional advanced configuration option: Authorize Web Users

The Configure Service Agent Collection Attributes - Advanced display allows you to authorize users to access web site data for the system enrolled by this Service Agent.

```
-------- Configure Service Agent Collection Attributes - Advanced -------------


Authorize Web Users

IBM provides a web site where you can view details of the systems you have
enabled for Electronic Services.  To authorize users to access this information
enter one or two IBM Registration user IDs.

   User ID 1.  _____________________________
           2.  _____________________________

   Last authorization request sent on 2007-05-01.18.02.55  UTC for User ID(s)
   johndoe@domain.com


To view details of the systems and to perform further User ID maintenance,
please view www.ibm.com/support/electronic

                                                Press the Enter key to submit
                                                authorization request




Command ==> ____________________________________________________________
```

Figure 9. Configure Service Agent Collection Attributes - Advanced

Fields

The two input fields on this panel are intended to accept one user ID each. These user IDs must be in IBM Common Registration format.

After entry, validation will be done remotely by IBM. If any one of the fields is deemed invalid a message will be sent to your TSO logon ID to that effect giving a reason code as follows:

```
9970 - length of given user ID is invalid
9972 - illegal character within given user ID
```

The entire process may take some minutes to complete. After a successful validation, authorized user IDs and your user ID will be saved in the dialog activity log; also, the next time this panel is used the Last Authorization text will show the date and time of the authorization and the authorized user IDs that were submitted last time.

Note: If you currently have two user IDs and you wish to change only one of them, both the changed and the unchanged must be entered.

Saving Data

Data is saved by pressing the ***Enter*** key. Pressing the End key will not save your changes.

System Information

The Configure Service Agent Collection Attributes - System Information display lists all system and hardware information used to identify the system where Service Agent is running.

The field System User Description must be entered. This is the name you will use to identify your system when you are reading Service Agent application reports.

```
-------------- Display System Registration Information  -----------------------

CPU Information:               System Information:
   Type:            2066          System name: XENA
   Model:           004           OS level:    z/OS 01.04.00 HBB7707
   Serial number:   123D0         SYSPLEX name: MONO
                                      Hardware name: R2066
   Manufacturer:    IBM           System enrolled: Yes
   Plant of manufacture: 02

LPAR Information:              System Input:
   LPAR name:       XENA          System User description: (*)
   LPAR number:     8             XENA Development System_________________
                                      ________________________________________
                                      ________________________________________

                                  Hardware data collection only:
                                     System Group ID: 0004____
                                     System Registered: Yes
                                  Last updated  2006-07-19 07:22:20

(*) Required                                      Press the Enter key to save




Command ==> ____________________________________________________________
```

Figure 10. Display System Registration Information

The field **System Group ID** for Hardware data collection is displayed when direct communication has been configured and hardware collection is enabled. Its main purpose is to allow you to select reporting of your hardware I/O errors on the same or different zSeries systems or z9 Servers in Service Agent summaries.

The field becomes editable when you are configuring, but haven't yet enrolled, ESA for hardware collection by HESHWRDL on a system which is using direct connection and which is on a different physical box (a different Type/Serial number) than those enrolled previously. If there have been no other physical boxes enrolled for this purpose previously, then leave this field blank and a new System Group ID will be assigned for you on initial enrollment. If not, you will have the option of entering a System Group ID that has been previously assigned to your complex; or leave it blank, in which case another System Group ID will be assigned.

Once this assignment has been done, each LPAR that you enroll for hardware collection by HESHWRDL on the same physical box will be assigned the same Group ID automatically.

Using the Service Agent Dialog user interface

The Service Agent Dialog has a Main Menu and thereafter sub-menus that allow you to manage your Service Agent work. You will need to explore the options on the Main Menu to obtain a feel for the user interface.

Note

Help is available for all Service Agent panels. To access help text press the ***PF1*** key, and to exit from help text press the ***PF3*** key. Help text is scrollable, to go down press the ***PF8*** key and to go up press the ***PF7*** key.

The following is the Service Agent Main Menu:

```
---------------- Electronic Service Agent Main Menu --------------------------

Select the option of your choice:

   1  Start     Service Agent
   2  Stop      Service Agent

   3  Configure Service Agent Configuration

   4  Display   Service Agent Data Collectors

   5  Run       Service Agent Data Collectors

   7  Verify    Service Agent Connection to IBM

   H  History   Service Agent History Logs
   R  Report    View Automatic Hiper Alert reports

   X  Exit


Service Agent status: not active                    mode: enabled




Command ==> ____________________________________________________________
```

Figure 11. Electronic Service Agent Main Menu

The Service Agent Dialog performs edit checking on selective input fields. It also ensures that all required fields are complete. If, for whatever reason, you have made a mistake during input, an error message appears. If the message appears in the top right hand corner of your screen you can press the Shift key plus the ***PF1*** function key to obtain additional information about the meaning of the message.

Start option Starts two dependent tasks: Event Manager and Scanner. This option is only enabled when you have configured Service Agent -- i.e., you provided all required configuration information. The Scanner task will be started up and active only if there is work requested by a user or a scheduled collection data event. After completing requested work it will shut itself down. Starting a Service Agent which is disabled (no scheduled data collection) will result in a message indicating that and both tasks will shutdown.

If you have enabled Service Agent to run in an automatic mode using option 3.8 (Configure->Schedule), you can optionally add started command HESMAIN to your COMMNDxx member in SYS1.PARMLIB if you want to have the Scanner and Event Manager started automatically during system initialization. For example:

```
COM = 'S HESMAIN,ESAPARM=START'
```

See “Starting Software and Hardware (from HESHWRDL) Data Collection and Reporting” on page 70.

Stop option Stops the Event Manager and Scanner tasks if is active. This option is only available when you have configured Service Agent This option allows you to suspend or stop data collection and data transmission for all Service Agent data types in a controlled manner. The Scanner shuts down only after it finishes work currently being processed.

Alternatively, you can stop the tasks from the operator console using following command on the MVS console:

```
COM = 'S HESMAIN,ESAPARM=SHUTDOWN'
Or, using STOPSA command on the Service Agent Dialog command line on
the Main Menu.
```

See 6.3, “Stopping Service Agent started tasks” on page 71.

Configure option Displays a further sub-menu, allowing you to view and provide values for Service Agent parameters needed by the Event Manager and the Scanner to work properly.

Display option The Display option displays the following information:

- The customer specified scheduled times for data collection and data transmission for all Service Agent data types.
- For each Service Agent data type:
  - The last data collection and last data transmit date and time.
  - For software data type, the last date and time where a change in the inventory data has been detected and collected. A change in the inventory implies that changes to the inventory have occurred since the last time the inventory data was collected.

Run option Enables immediate processing of selected data types. In disable mode, Service Agent is started if it is not active in order for the immediate processing to be begin.

Verify option Verifies the physical and logical connection to the focal point Hardware Management Console and IBM. In disable mode, Service Agent is started if it is not active in order for the verify connection processing to be begin.

History option Provides a further sub-menu where you can view all logs created by Service Agent (i.e., Work log, Error log and Dialog activity log).

Report option Displays the following information related to AHA:

- number of requested HIPER reports
- AHA request submitted date
- AHA report received date

Exit option Ends the current session of the Service Agent dialog.

Status Bar The status bar appears directly below the option. It provides the current status of Service Agent.

Mode Service Agent can operate in three modes: 1) non-configured 2) enabled and 3) disabled. The Mode field is directly to the right of the Status bar

Not-configured mode The first time you access Service Agent, before any configuration is done, the mode appears as not-configured.

Once you have configured the Service Agent parameters, there are only two possible modes Service Agent can be in: disabled or enabled.

Enabled mode Service Agent performs collection and transmission of data automatically as defined by a schedule assigned by the user. Software and service data is collected and sent daily. Automatic collection and transmission are enabled when you provide a Y to the prompt below (This prompt is found under option 3, Configure Service Agent Collection Attributes - Schedule).:

Enable Service Agent scheduled collection: Y (Y/N) (*)

Disabled mode Service Agent will not perform any automatic collection or transmission of data. Collection or transmission only happens when requested (or forced) by the user. Service Agent is in a disabled mode when you provide a "N" to the prompt below (This prompt is found under option 3, Configure Service Agent Collection Attributes - Schedule.):

Enable Service Agent scheduled collection: N (Y/N) (*)

Help Help is available for all Service Agent panels. To access help text press the ***PF1*** key, and to exit from help text press the ***PF3*** key. Help text is scrollable, to go down press the ***PF8*** key and to go up press the ***PF7*** key.

Split screen mode Service Agent makes use of the full screen (all 24 lines are utilized). The best results are obtained when not using the split screen mode when invoking Service Agent.

Service Agent commands The following commands can be used to monitor and control the Service Agent collection and reporting:

- MONitor command - Displays list of work elements currently being processed by Service Agent in a Work Inventory Panel.
- STARTSA command - Starts Service Agent.
- STOPSA command - Stops Service Agent.

All the above commands can only be run from the Service Agent Main Menu command line and are available when Service Agent is either enabled or disabled but not before it is configured.

History Logs The Service Agent History Logs display presents options that allow you to view Work and Error Inventory logs, and the Dialog Activity Log.

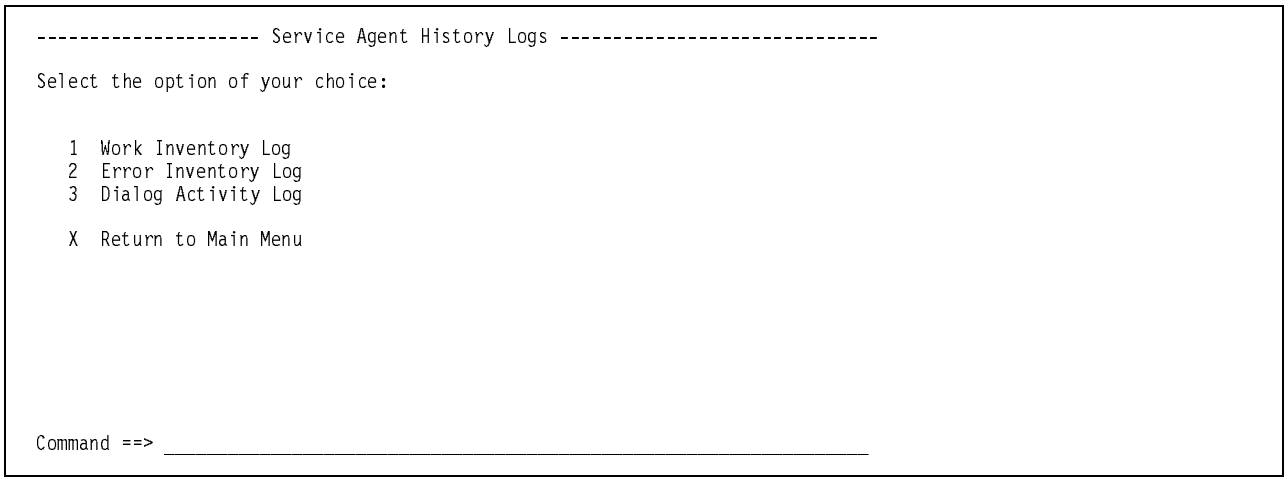

Figure 12. Server Agent History Logs

Allows you to select and display one of the following Service Agent Logs:

Work Inventory Log All service agent transactions' steps are logged in the Work Log. It is used to track the number of transactions performed by the Service Agent and their completion status. The Work Log summery displays all collections performed, how long did each one of them take, and how they completed.

The Work Inventory Log option provides two log views - one for the summary of Work history entries and the other for complete display of all history entries.

Error Inventory Log If for any reason a transaction did not complete successfully, it is logged in the Error Log. Error Log tracks phase or step of the transaction failed, with what error code, and what was the accompanying error message. Error Log dialog allows users to see Service Agent errors without going to the SDSF output. Choosing the Error Inventory Log option start the Error Inventory Log display.

Dialog Activity Log Information about actions performed in the dialog and by who are logged in the Dialog Log. Choosing the Dialog Activity Log option starts the Dialog Activity Log display.

X Return to Main Menu

Work History - Filter The Work History - Filter display allows you to specify the search criteria which are used to extract a subset of log records to be displayed. If you do not specify any search criteria a default of ALL summary records is used.

```
----------------------- Work History - Filter -------------------------------

Specify View Criteria:

   Summary or entire
      work log   ==> s            s - summary
                                  e - entire


Specify Search Criteria:

   Date entered  ==> *           (yyyy-mm-dd)

   Data type     ==> *           (Enroll, Software, Ping,
                                  Hardware, Hiper)




                                                Press the Enter key to view




Command ==> ____________________________________________________________
```

Figure 13. Work History - Filter

Fields All fields on this panel are of input type and are in character format.

The Summary or entire work log field must contain either an s or an e.

The Date entered field must contain either an asterisk (*) to represent all records, or a date specified in yyyy-mm-dd format If a date is specified, the search criteria will be defined as equal to or following that date.

The Data type field must contain either an asterisk (*) to represent all records, or a valid data type spelled exactly as displayed in the examples in brackets (Software, Hiper, Verify or Enroll. Case is ignored).

Saving Data The filters are applied by pressing the ***Enter*** key. The ***End*** key will not apply the filters.

Work History The Service Agent's Summary Work History display allows you to view a summary of Service Agent's work history, specifically the elapsed time and the start and end time-stamps.

```
------------------ Service Agent's Summary Work Histor Row 449 to 480 of 1,931

PRIM Cmds:(SET L F N P SORT)
LINE Cmds:<Error log Select>

                                  |Elapsed |Start Date/Time|End Date/Time
S PID   DataType CollType Status        |hh:mm:ss| yymmdd hhmmss |yymmdd hhmmss
- ----- -------- -------- -------------- --------  ------ ------  ------ ------
_ 09339 SOFTWARE REFRESH  received       00:00:51 130605 120445 130605 120536
_ 09338 PING     INITIAL  received       00:00:48 130605 120057 130605 120145
_ 09337 SOFTWARE DELTA    no-delta       00:00:23 130605 111121 130605 111144
_ 09336 SOFTWARE DELTA    no-delta       00:00:27 130604 111122 130604 111149
_ 09335 SOFTWARE DELTA    no-delta       00:00:24 130603 111131 130603 111155
_ 09334 SOFTWARE DELTA    no-delta       00:00:27 130602 111120 130602 111147
_ 09333 SOFTWARE DELTA    no-delta       00:00:27 130601 111120 130601 111147
_ 09332 HARDWARE EREPDATA received       00:00:14 130531 135750 130531 135804
_ 09331 SOFTWARE DELTA    no-delta       00:00:23 130531 135415 130531 135438
_ 09330 SOFTWARE REFRESH  received       00:00:47 130531 135037 130531 135124
_ 09329 HIPER    REPORT   received       00:00:28 130531 134723 130531 134751
_ 09328 ENROLL   UPDATE   received       00:00:12 130531 134705 130531 134717
_ 09327 ENROLL   UPDATE   received       00:00:11 130531 134647 130531 134658
_ 09326 HARDWARE EREPDATA received       00:00:13 130531 123810 130531 115238

Command ==> _____________________________________________ Scroll ==> CSR_
```

Figure 14. Service Agent's Summary Work History

PID This column displays the Package Identification Number that was or is in process.

DataType This column displays the type of data for the package that was processed. The values may be:

- Enroll - User or System Enrollment
- Software- Software
- Hardware- Hardware
- Ping - Connection Verification
- Hiper - AHA

Request This column displays the request as follows:

- Acrenew - Access code renewal
- Delta - Change after initial collection
- Initial - Initial collection
- Refresh - Complete refresh of data after the initial
- Update - Update of Enrollment information
- Report - AHA report request

Status This column displays the final result of the function. For functions which have not fully completed the status field displays current phase the process is in prefixed by 'act'. The values may be:

**** failed **** processing of the package completed in error

incomplete processing of the package has not ended yet, package may be waiting for send time

no-delta no delta was found between this and last collection, and no transmission of data was required.

received processing for the package has completed successfully (request was received by IBM).

act-phase processing for the package is progress name

Elapsed Time This column displays the calculated elapsed time for the function, and it is the time between the beginning of the first phase and the beginning of the last phase for the particular package.

Detailed Work History Using Select line command on the summary page and selecting a transaction, you will get the detailed work history log displayed for that transaction. The history log shows all phases that the was run during processing the transaction.

```
------------------ Service Agent's Detailed Work History ----- Row 1 to 6 of 6

PRIM Cmds:(SET L F N P SORT)

  D a t e     T i m e    PID     DataType  CollType   Phase    Status
  ----------  --------   -----   --------  --------   -------- --------
  2006-02-09  13.24.16   01463   SOFTWARE  REFRESH    INIT     ACTIVE
  2006-02-09  13.24.19   01463   SOFTWARE  REFRESH    COLLECT  ACTIVE
  2006-02-09  13.24.35   01463   SOFTWARE  REFRESH    FORMAT   ACTIVE
  2006-02-09  13.24.40   01463   SOFTWARE  REFRESH    READY    HOLD
  2006-02-09  13.24.43   01463   SOFTWARE  REFRESH    TRANSMIT ACTIVE
  2006-02-09  13.25.00   01463   SOFTWARE  REFRESH    RECEIVED HOLD
******************************** Bottom of data ********************************




Command ==> ____________________________________________________ Scroll ==> CSR_
```

Figure 15. Service Agent's Detailed Work History

Date This column displays the Date the phase of the request was started.

Time This column displays the Time the phase of the request was started.

PID This column displays the Package Identification Number that was in process.

DataType This column displays the type of data for the package that was processed. The values may be:

- Enroll - User or System Enrollment
- Software- Software
- Hardware- Hardware
- Ping - Connection Verification
- Hiper - AHA

Request This column displays the request that the function was fulfilling.

- Acrenew - Access code renewal
- Delta - Change after initial collection
- Initial - Initial collection
- Refresh - Complete refresh of data after the initial
- Update - Update of Enrollment information
- Report - AHA report request

Phase This column displays the initial phase of the operation. The values may be:

- Init - Initialize and allocate data sets required for this data type.
- Collect - Collection of inventory data is in process.
- Compare - Comparing data from previous transmission. Valid only for software data type.
- Format - Formatting of XML data for sending to IBM is in process.
- Ready - Work element is ready for transmission.

- Send - FTP send is in process.
- Resend - FTP send is in process.
- Nodelta - Work element will be deleted. Inventory has not changed since last collection.
- Validate - Validation of response from IBM is in progress.
- Received - Positive acknowledgment has been received. Work element will be deleted.
- Delete - Refresh has been requested but package has not been successfully received. Work element and work data sets will be deleted.

Status This column displays the initial status of the phase on which the scanner is working.

Phase Status This column displays the status of the process:

- Active - function is active for this work element
- Hold - function is waiting to be activated
- Error - function finished unsuccessfully

Error History The Service Agent's Error History display allows you to view Service Agent's error history. Use the Verbose mode to see complete error message text.

```
--------------------- Service Agent's Error History ---- Row 1 to 33 of 2,111

PRIM Cmds:(SET L F N P SORT VErbose)
LINE Cmds:<Select>

  D a t e    T i m e  PID    DataType  CollType  Program   Phase     RetC Rtry
  ---------- -------- -----  --------  --------  --------  --------  ---- ----
_ 2013-02-25 14.34.13 09228  SOFTWARE  REFRESH   HESJNIF   FORMAT    8
_ 2013-02-25 12.35.10 09227  SOFTWARE  REFRESH   HESJNIF   FORMAT    8
EssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssN
e -------------- Service Agent's Error History - Detail -------------------- e
e                                                                             e
e Package ID:             Data type:           Date: 2013-02-14  RC:          e
e Program name: HESJNIT   Phase name: BEATERR   Collect type:                 e
e                                                                             e
e Error message:                                                              e
e HES30046E HESSCAN is unable to reach IBM Server and will be shutdown.       e
e                                                                             e
e                                                                             e
e                                                                             e
DssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssM
_ 2013-01-25 07.57.16 00056  HARDWARE  EREPDATA  HESHWTRN  COLLECT   16
_ 2013-01-25 06.56.34 00053  HARDWARE  EREPDATA  HESHWTRN  COLLECT   16
_ 2013-01-25 05.56.03 00050  HARDWARE  EREPDATA  HESHWTRN  COLLECT   16
_ 2013-01-25 04.55.30 00047  HARDWARE  EREPDATA  HESHWTRN  COLLECT   16
_ 2013-01-25 03.54.58 00044  HARDWARE  EREPDATA  HESHWTRN  COLLECT   16
_ 2013-01-25 02.54.25 00041  HARDWARE  EREPDATA  HESHWTRN  COLLECT   16
_ 2013-01-25 01.53.54 00038  HARDWARE  EREPDATA  HESHWTRN  COLLECT   16
```

Figure 16. Service Agent's Error History

Date This column displays the Date the error occurred

Time This column displays the Time the error occurred

PID This column displays the Package Identification Number that was in process when the error occurred.

DataType This column displays the type of data that was processed. The values may be:

- Enroll - User or System Enrollment
- Software- Software
- Hardware- Hardware
- Ping - Connection Verification
- Hiper - AHA

Request This column displays the request that the function was fulfilling.

- Acrenew - Access code renewal
- Delta - Change after initial collection
- Initial - Initial collection
- Refresh - Complete refresh of data after the initial
- Update - Update of Enrollment information
- Report - AHA report request

Phase This column displays the initial phase of the operation. The values may be:

- Init - Initialize and allocate data sets required for this data type.
- Collect - Collection of inventory data is in process.

- Compare - Comparing data from previous transmission. Valid only for software data type.
- Format - Formatting of XML data for sending to IBM is in process.
- Ready - Work element is ready for transmission.
- Send - FTP send is in process.
- Resend - FTP send is in process.
- Nodelta - Work element will be deleted. Inventory has not changed since last collection.
- Validate - Validation of response from IBM is in progress.
- Received - Positive acknowledgment has been received. Work element will be deleted.
- Delete - Refresh has been requested but package has not been successfully received. Work element and work data sets will be deleted.

Program This column displays the name of the program operating.

RetC This column displays the return code of the error.

Rtry This column displays the number of times Service Agent attempted to perform the same function.

PRIMARY COMMANDS

VErbose This command may be abbreviated to VE. The table is redisplayed showing also error text for each entry in the log. This display mode will remain active until a TERSE command is issued.

Dialog Activity Log The Service Agent's Dialog Activity History allows you to view the Dialog activity history.

```
---------------- Service Agent's Dialog Activity History Row 1 to 34 of 3,111

PRIM Cmds:(SET L F N P SORT VErbose)

D a t e    T i m e  W Log Detail                                      UserId
---------- -------- - ---------------------------------------------- --------
2013-06-05 12.03.18 U Force COLLECT & SEND requested for: SOFTWARE    AWU
2013-06-05 11.58.48 U Verify connection to IBM has been requested     AWU
2013-05-31 13.56.28 U Force  requested for:                           AWU
2013-05-31 13.56.03 U Service Agent start requested                   AWU
2013-05-31 13.55.45 U Service Agent shutdown requested                AWU
2013-05-31 13.55.21 U Service Agent shutdown requested                AWU
2013-05-31 13.52.55 U Force COLLECT & SEND requested for: SOFTWARE    AWU
2013-05-31 13.49.16 U Force COLLECT & SEND requested for: SOFTWARE    AWU
2013-05-31 13.46.44 U Configuration information has been updated      AWU
2013-05-31 13.45.26 U Force  requested for: COLLECT & SEND            AWU
2013-05-31 13.45.18 D Service Agent started to be ready to perform... AWU
2013-05-31 13.43.46 U Configuration has been updated                  AWU
2013-05-31 13.43.19 I Import task started                             HESCONF
2013-05-31 13.43.19 I Import parameters parsed                        HESCONF
2013-05-31 13.43.19 I All current data read                           HESCONF
2013-05-31 13.43.18 U Import task started                             AWU
2013-05-31 13.43.05 U License agreement has been accepted by AWU      AWU
2013-05-31 13.43.00 U Service Agent dialog invoked first time AWU     AWU
2013-05-31 13.43.00 D Initialization of inventories has been compl... AWU
2013-05-31 13.41.40 U Service Agent shutdown requested                AWU
2013-05-31 13.40.22 I Export task started                             HESCONF
2013-05-31 13.40.22 I Export parameters parsed                        HESCONF
2013-05-31 13.40.22 U Export task started AWU                         AWU
2013-05-31 12.36.50 U Force  requested for:                           AWU

Command ==> _____________________________________________ Scroll ==> CSR_
```

Figure 17. Service Agent's Dialog Activity History

Date This column displays the date the activity occurred.

Time This column displays the time the activity occurred.

W(ho) This column displays who initiated action/request. Could be user (U), Dialog (D) or Import/Export function.

UserId This column displays the user-identification of the user who started the activity.

PRIMARY COMMANDS

VErbose This command may be abbreviated to VE. The table is redisplayed showing also error text for each entry in the log. This display mode will remain active until a TERSE command is issued.

Reports - View Automatic Hiper Alert reports The Service Agent's Reports menu allows you to receive and view AHA reports and Hiper/PE installable PTFs.

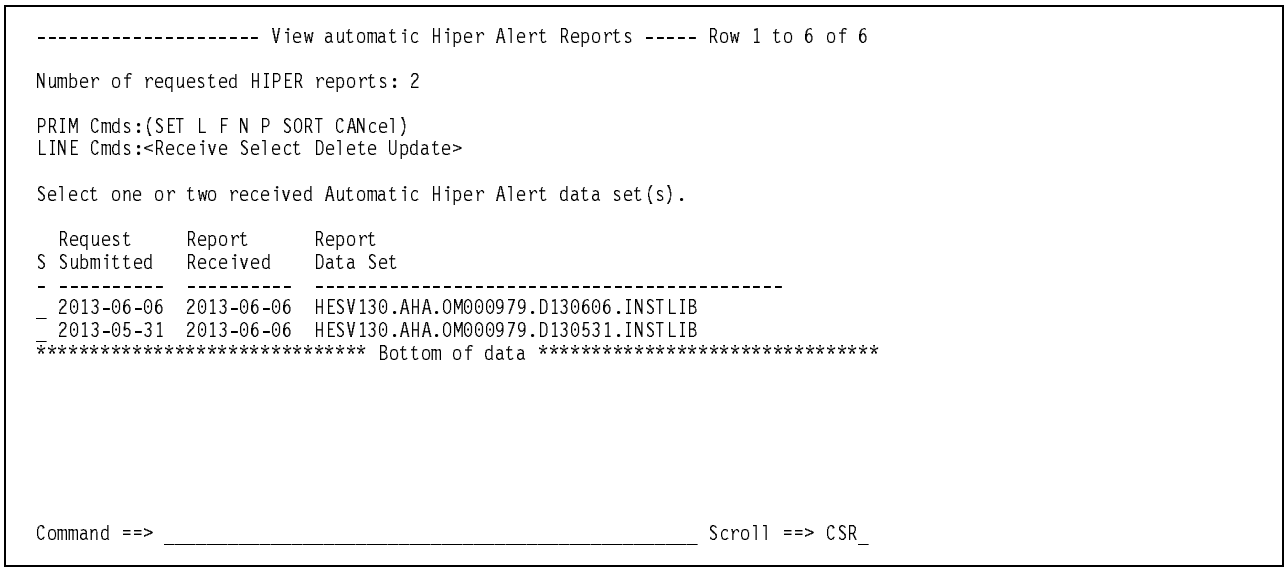

Figure 18. View Automatic Hiper Alert reports

End date of AHA reporting

Request submitted Date that AHA request was submitted

Report Received Date that AHA report was received

Report Data Set Data Set containing AHA report

LINE COMMANDS

R R(eceive) AHA reports into a data set for viewing

S S(elect) received AHA reports for viewing

D D(elete) AHA reports from the display menu. The actual AHA report file remains intact, only the selection is removed from the menu.

Automated Hiper Alert Automated HIPER Alert panel is the main navigation panel for viewing your requested Hiper/PE report and selected information in it.

- It allows for selecting individual PTF reports, CSI report and reach ahead report.
- Individual PTF reports detail installable and not installable Hiper PTFs, resolved and unresolved PE PTFs, and installable HOLD PTFs.
- Elements of CSI is a summary report that lists date of service select, profile number, and a list of entries in the CSI.
- Reach ahead report lists PTFs which are available but not installed on your system.

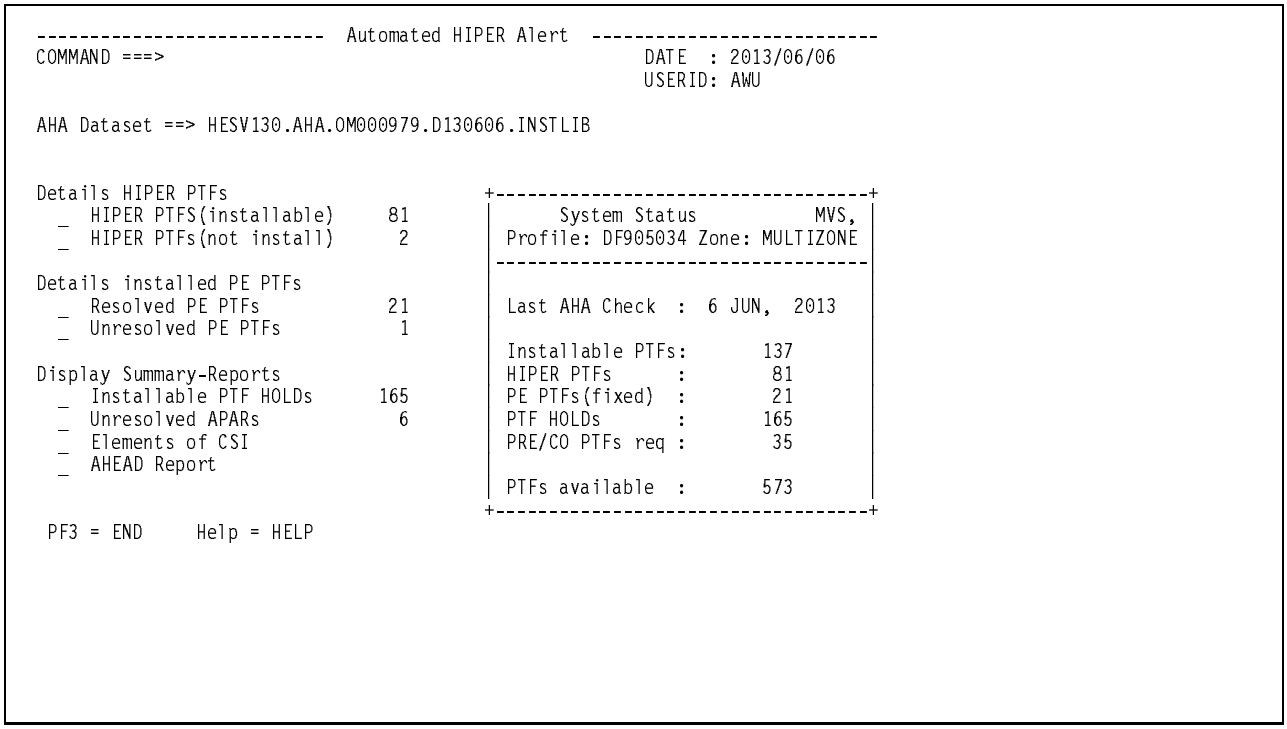

Figure 19. Automated Hiper Alert

The panel features a summary of all PTF counts that are found. To select a report type any character next to the report heading.

Automated Hiper Alert Summary Info Automated HIPER Alert summary panel displays, in a table format, all PTFs for the selected report and allows view access to each individual PTF from the list.

The display can be sorted on a specific column by providing a letter from the menu bar in the space next to the bar.

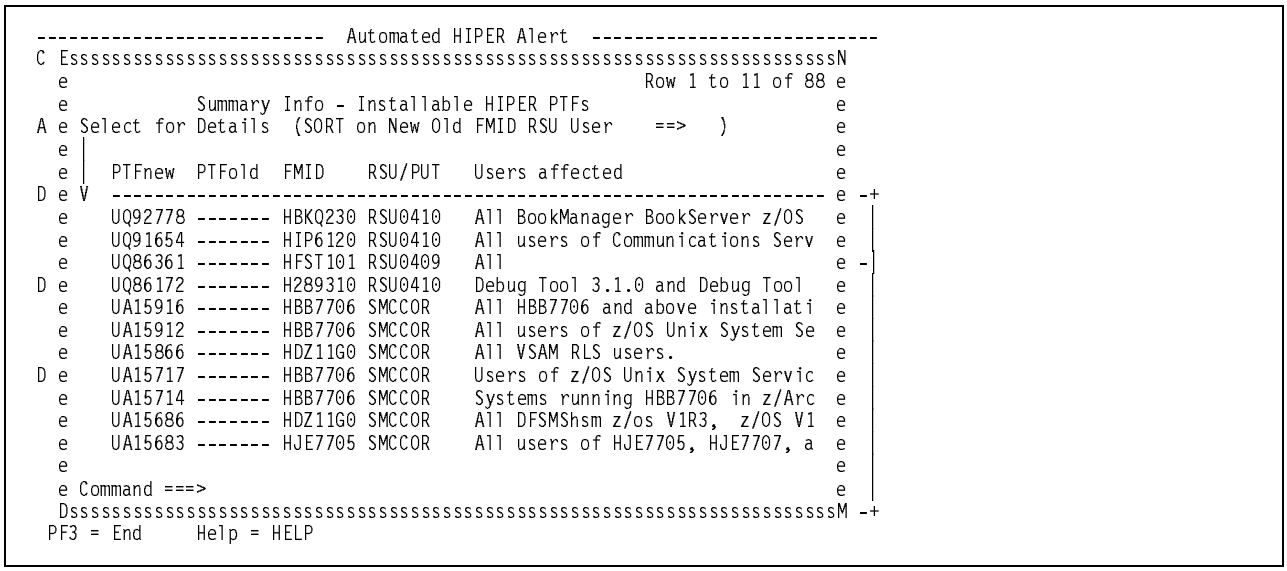

Figure 20. Automated Hiper Alert Summary Info

Depending on the report selected the column content may change and the change will be reflected in the column heading.

To select a PTF type 's' next to the PTF's name

Automated Hiper Alert PTFs with HOLD action Automated HIPER Alert has option to list all Installable PTFs with HOLD. The panel displays, is in a table format, and allows view access to each individual PTF from the list.

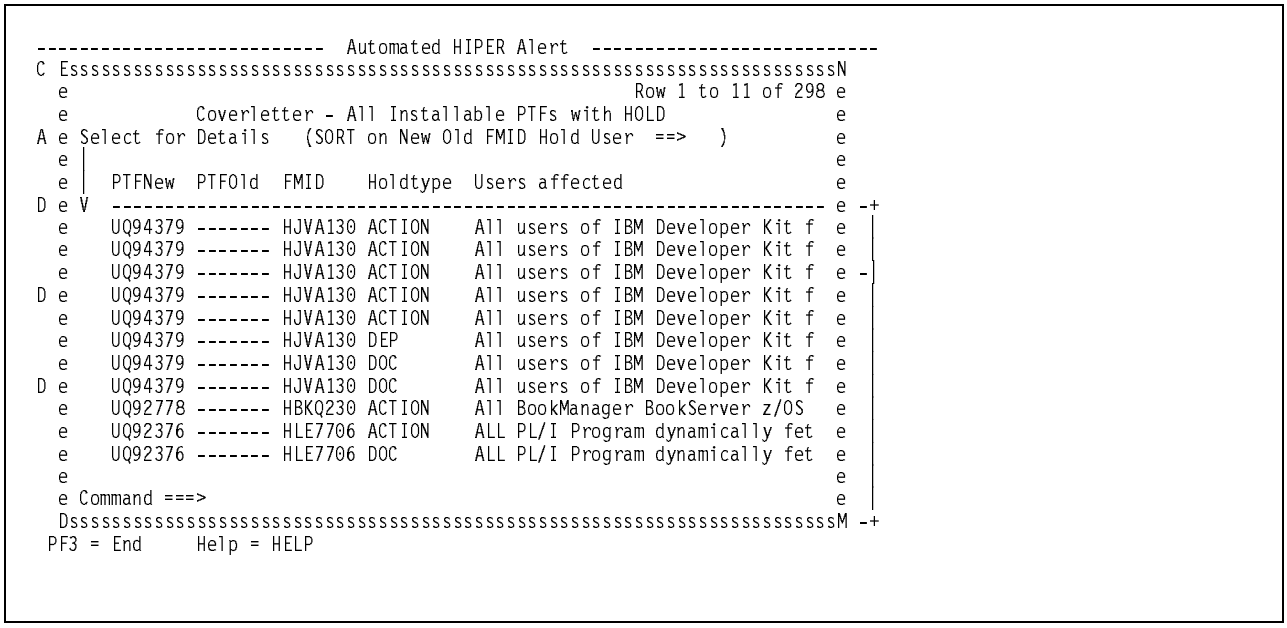

Figure 21. Automated Hiper Alert PTFs with HOLD action - 1

```
 EDIT ---- ALEXS.SPFTEMP1.CNTL ---------------------- Line 00000000 Col 001 080
 --------------------------- Automated HIPER Alert ---------------------------
 DF900326   Installable PTF UQ94379  - Holdtype = ACTION    JANUARY 10, 2005
 ------------------------------------------------------------------------------
******************************** Top of Data ********************************

  -------- COVER LETTER FOR PTF UQ94379 ------------

    PROBLEM DESCRIPTION(S):
      PQ95576 -
        ****************************************************************

1       * USERS AFFECTED: All users of OS/390 SDK 1.3.1           *
        ****************************************************************
        * PROBLEM DESCRIPTION: APARs                               *
        *                      Fixed                                   *
        *                      =====                                   *
        *                      PQ89101                                 *
        *                                                              *
        *                      Common Code defects fixed.              *
        *                      ==========================              *
        *                                                              *
        *                      CMVC                                    *
        *                      Name   Abstract                         *
        *                      60441  IBM_XE_COE_NAME doesn't work for *
        *                             jited method                     *
        *                      65745  Incorrect floating point values  *
        *                             returned with JIT ON             *
        *                      66537  Deferred Packets Problem         *
        *                      67881  Unexplained                      *
        *                             IllegalMonitorStateException     *
        *                      68383  Append timestamp.pid to the      *
        *                             tracefile file name              *
 COMMAND ===>                                          SCROLL ===> CSR
```

Figure 22. Automated Hiper Alert PTFs with HOLD action - 2

Export/Import function

The Export/Import function enables customers to clone or customize their Sysplex deployment of the Service Agent program product, and/or backup their existing Service Agent configuration inventory data file. The Export/Import function can be invoked online using the Service Agent Dialog interface or in batch mode using JCL provided in the ***hlq***.HESSAMP library in the HESCONF member.

The Import function can be used in batch mode during IPL time to update the Service Agent software data collection configuration in cases where the Global CSI names need to be changed. This new capability removes the need for using the Service Agent Dialog to make required modifications on each affected system. The Import function can be run during IPL time using a prepared configuration import file. This eliminates a need to logon to the system to make required changes using the dialog.

The Export function collects all required Service Agent configuration information and saves the data in a predefined XML format. The resulting dataset can be easily modified to update an existing or to create a new configuration inventory file. Using either the Service Agent Dialog or batch JCL, you have the option of selecting which configuration data will be exported from the following list:

```
Select EXPORT data:
  User Information (Y/N)
  Service Agent configuration (Y/N)
  Data Collection configuration (Y/N)
  Enrollment information (Y/N)
```

User Information Enrollment information entered in options 3.1; 3.2 and 3.4.

Service Agent configuration Configuration information provided in options 3.3.

Data Collection configuration Configuration information provided in options 3.5.

Enrollment information The default is set to No. Existing Enrollment Information should only be exported when a backup of the current configuration inventory file is desired or for use during a system recovery situation where an existing configuration inventory file is needed.

The Import function transfers exported data to another Service Agent configuration inventory file. An Import function can be performed on an already configured (pre-primed) or not yet configured (non-primed) Service Agent configuration inventory file. Using either the Service Agent Dialog or the batch JCL, you have an option to select which configuration data will be imported from the following selection list:

```
Select IMPORT data:
  User Information (Y/N)
  Service Agent configuration (Y/N)
  Data Collection configuration (Y/N)
  Enrollment information (Y/N)
```

The Import function will validate the selected data and update the target fields in the current configuration inventory file. Note that for complete Hiper/PE import and export requires the selection of both Service Agent and Data Collection configurations.

The results of each Export or Import invocation are reported and saved in a user provided data set name. Major export events and import updates to the new configuration inventory file are logged into the Dialog Activity Log database which can be viewed using the Service Agent Dialog.

Upon successful completion of an Import function, a report will indicate the status of the Service Agent. The status can be either **configured** or **not configured**. If the report indicates that the Service Agents status is **configured** the Service Agent collection process can be started immediately. If the report indicates that the Service Agents status is **not configured** you have to use the Service Agent Dialog to add or correct configuration data before you can start any type of collection. (The report and the Dialog will indicate which data is incorrect or missing.)

Online mode

To invoke the Export or Import function, type **export** or **import** on the command line in the Service Agent Dialog Main Menu panel and follow the instructions that are displayed. A generated report will be displayed in browse mode upon completion of the function.

EXPORT command will start a process to collect user selected categories of data from a Service Agent configuration inventory file (CONFINV) and export data into an export file in predefined XML format.

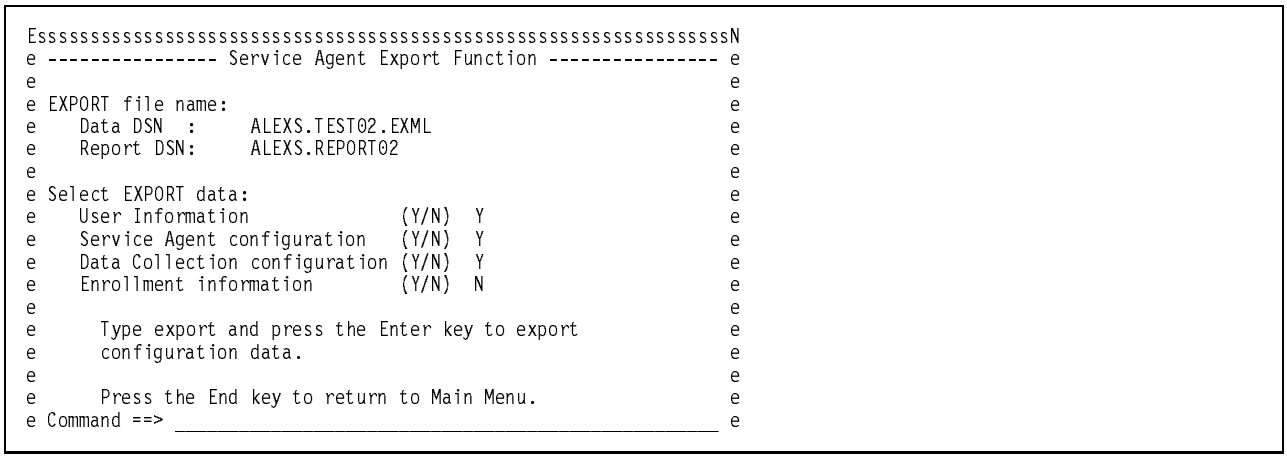

Figure 23. Service Agent Export Function

The exported data can be modified and used later in the Import process. The Export command allocates two data sets; an exported configuration data file and an Export report file.

IMPORT command will start a process to initialize (i.e. populate) or to overwrite a Service Agents configuration inventory information.

The Import process reads a user provided data set (usually one from an Export process), validates its contents and update the appropriate information in the target configuration inventory file. The input data is in XML format and can be modified to further tailor the content of the required configuration inventory data before a new image of Service Agent is created.

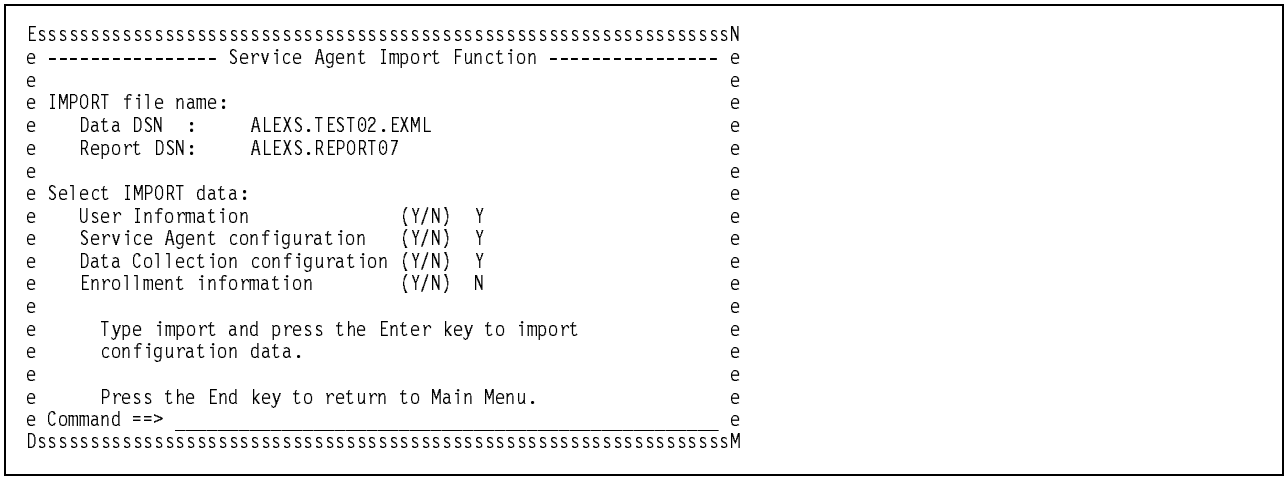

Figure 24. Service Agent Import Function

The command allocates an import report data set.

Batch mode

Export or Import function is also supported in the batch mode. Sample job is provided in the SHESSAMP sample library member **HESCONF**.

Export Modify the SYSTSIN DD to specify PARM('/EXPORT BATCH'). The CONFXML DD should allocate to a new export data set or point to an existing data set which will be overwritten.

Import Modify the SYSTSIN DD to specify PARM('/IMPORT BATCH'). The CONFXML DD should point to an existing data set with exported data. In SYSIN DD specify what types of information you want to process and import:

```
//SYSIN DD *
USERDATA(Y)
SERVICEAGENTCONFIG(Y)
DATACOLLECTIONCONFIG(Y)
ENROLLINFORMATION(N)
/*
```

A generated report will be saved in the HESXRPT DD in SYSPRINT upon completion of the function. You can browse the output in SDSF.

Error Codes

```
2,“Value is blank. Field not updated.”
3,“Value is too long. It will be concatenated to max size.”
4,“IP address is invalid. Field not updated.”
5,“Global CSI data set is not found.”
6,“Data set name is not suffixed by CSI.”
7,“Zone does not exist in specified CSI.”
8,“Dlib zone's related target zone not selected.”
9,“Can't find related info for this Dlib zone.”
10,“Time entry is invalid. Make sure it's between 000000 and 235959.”
11,“Country code is invalid.”
12,“Country code type is invalid.”
13,“Reserved.”
14,“Time zone is invalid.”
15,“State or province is invalid.”
16,Access code is invalid.
17,“Company email is invalid. Use name@company.com format.”
18,“Contact email is invalid. Use name@company.com format.”
```

6.0 Chapter 6 - Service Agent management

6.1 Activating Service Agent

Follow the instructions on 4.0, "Chapter 4 - Hardware data collection and reporting" on page 14 for standalone hardware and follow the instructions on 5.2, "The initial use of Service Agent" on page 34 for software, hiper/pe and hardware (from HESHWRDL).

6.2 Starting Service Agent started tasks

In normal operation, the started tasks HESEVEM, the Event Manager, and HESRDLOG, the stand-alone Hardware collector and reporter, will run continuously until shut down (see 6.3, "Stopping Service Agent started tasks" on page 71 below). HESHWRDL, the Hardware collector, will also run continuously until shut down. Started task HESSCAN, the Scanner, which collects software, hiper/pe and hardware (in HESHWRDL) and reports software, hiper/pe and hardware (from HESHWRDL), will only execute if HESEVEM identifies that it is time to collect and/or send data.

Starting Standalone Hardware Data Collection and Reporting

See "Activating hardware data collection and reporting using HESRDLOG task" on page 19.

Starting Software and Hardware (from HESHWRDL) Data Collection and Reporting

After enabling Service Agent data collection, the next step is to activate the Service Agent started tasks. If the Service Agent tasks are not activated, automatic data collection will not be initiated.

The Service Agent tasks can be started in one of the two following ways:

1. Using Service Agent Dialog Start option
   This is option 1 on the Main Menu.
   Or, using STARTSA command
   On the the Service Agent Dialog Main Menu type STARTSA command to activate Service Agents started tasks.
2. Using the MVS console
   The Service Agent started tasks can be activated by the following MVS commands:
   - If Hardware has not been activated then enter the following:

     ```
     START HESMAIN,ESAPARM=START or
     S     HESMAIN,ESAPARM=START
     ```

     Upon successful activation, the following messages are displayed on the console log:

     ```
     IEF695I START HESEVEM WITH JOBNAME HESEVEM IS ASSIGNED TO USER HESEVEM , GROUP SYS1
     $HASP373 HESEVEM STARTED
     HES25100I EVENT MANAGER IS NOW ACTIVE
     ```

   - If Hardware has been activated then enter the following:

     ```
     START HESMAIN,ESAPARM=STARTALL or
     S     HESMAIN,ESAPARM=STARTALL
     ```

     Upon successful activation, the following messages are displayed on the console log:

```
IEF695I START HESEVEM WITH JOBNAME HESEVEM IS ASSIGNED TO USER HESEVEM , GROUP SYS1
$HASP373 HESEVEM STARTED
IEF695I START HESHWRDL WITH JOBNAME HESHWRDL IS ASSIGNED TO USER HESHWRDL , GROUP SYS1
$HASP373 HESHWRDL STARTED
HES25100I EVENT MANAGER IS NOW ACTIVE
```

In all cases, the Service Agent tasks remain active only if you have enabled Service Agent for automatic collection and reporting of data.

6.3 Stopping Service Agent started tasks

Stopping Standalone Hardware Data Collection and Reporting

The started task HESRDLOG controls standalone hardware data collection and reporting. Hardware data collection and reporting can be stopped by using any of the following commands:

```
MODIFY HESRDLOG,STOP or
F      HESRDLOG,STOP or
STOP   HESRDLOG
```

The MVS CANCEL command can be used as a last resort if the task does not respond to the stop commands.

Stopping Data Collection and Reporting

Data collection and reporting can be stopped by using any of the following commands on the MVS console:

- If Hardware has not been activated then enter the following:

  ```
  START HESMAIN,ESAPARM=SHUTDOWN or
  S     HESMAIN,ESAPARM=SHUTDOWN
  ```

- If Hardware has been activated then enter the following:

  ```
  START HESMAIN,ESAPARM=SHUTALL or
  S     HESMAIN,ESAPARM=SHUTALL
  ```

The MVS CANCEL command can be used as a last resort if the tasks do not respond to the shutdown commands.

Preferably, the started tasks are stopped using the Service Agent Dialogs option 1 on the Main Menu or the STOPSA command.

6.4 What to do if you upgrade your system

For a normal system upgrade with no changes to any of the three identifiers (CPU serial number and plant of manufacture, Model type, and System name (the 8-char SYSNAME)), IBM recommends that you perform a force collection using Service Agent to refresh the data.

With large amounts of change in installed products and service levels, a delta collection (obtained using normal Service Agent scheduled activity) takes an excessively long period of time to process. Performing a force collection for software information provides a refresh of the Software data type.

6.5 What to do if you change system identifiers

IBM uses the following identifiers to identify the data collected from your system:

- CPU serial number and plant of manufacture
- Model type
- System name (the 8-char SYSNAME)

If any one of these identifiers are changed (for example, SYSNAME changes because of a system replacement), Service Agent initiates a full refresh collection for Software Inventory data if it is enabled for Software collection.

Appendices

Appendix A. Security authority required by Service Agent

The HESSTHW and HESSTSW sample jobs define the Service Agents started tasks with the RACF attribute of TRUSTED. This allows Service Agent to create and access Service Agent data sets in both the MVS and Unix environments without any specific RACF permissions. If you decide not to define these tasks as TRUSTED, then the following table shows the minimum authority required by the Service Agents Started Tasks for each of the listed resources.

Hardware resource authorization requirements

Service Agent Started Tasks	Service Agent Resources	Authority Required
HESRDLOG/ HESHWRDL	MVS Data Sets:	RACF Resource Access:
	FTP.DATA	READ
	HESPARMS	READ
	HESTEMP	ALTER
	HESSTATE	ALTER
	SHESLMOD	READ

Table 1. RACF Authorization Required for Resources Used by Service Agent

Software data collection and reporting resource authorization requirements

Service Agent Started Tasks	Service Agent Resources	Authority Required
HESEVEM	MVS Data Sets:	RACF Resource Access:
	CONFINV	UPDATE
	SHESLMOD	READ
	RACF Resource	
	OPERCMDS(MVS.SEND)	READ
HESSCAN	MVS Data Sets:	RACF Resource Access:
	CONFINV	UPDATE
	CUSTINV	ALTER
	DFSPARM	READ
	ERRLOG	UPDATE
	FTP.DATA	READ
	WKSPINV	READ
	WORKINV	UPDATE
	WORKLOG	UPDATE
	SHESLMOD	READ
	User Catalog	UPDATE
	RACF Resource	
	OPERCMDS(MVS.SEND)	READ

Service Agent Started Tasks	Service Agent Resources	Authority Required
	UNIX Directories (see envvars file)	UNIX Access Write Write

Table 2. RACF Authorization Required for Resources Used by Service Agent

Appendix B. Understanding Service Agent

What does Service Agent do?

When Service Agent is installed, configured, and enabled to collect information from the zSeries or S/390 environment, Service Agent provides the following functions:

Hardware collection and reporting:

- Reports severe I/O device errors and requests service when appropriate.
- Collects I/O device statistical data and customer system configuration data that is transmitted to IBM for use in support of service related activities.

Software collection and reporting:

- Transmits software and service data based on a defined schedule or on demand when more frequent updates are needed. The data that is transmitted to IBM is then used and made available for viewing by web based services offered by IBM.

Hiper collection and reporting:

- Employs a pull and push methodology in transmitting data to IBM (on a defined schedule) and delivering Hiper reports and/or PTFs to the customer.

B.1 Understanding the Service Agent Application work flow when data are sent to HMC to forward data to IBM

How does Service Agent work?

The Electronic Service Agent for zSeries and S/390 consists of two major components:

- Product 5655-F17 installed on your z/OS system. It is comprised of Service Agent Dialog and data collection/data sending modules. This component is SMP/E-installable and distributed as an orderable program product. The primary function of this component is to allow the customer to configure and tailor the Service Agent data collection with attributes that are unique and tailorable to the installation. Once the data is collected from the operating system resources and processed, the data is formatted for transmission using File Transfer Protocol (FTP) to the installation's focal point Hardware Management Console that has been configured to serve as the focal point for Electronic Service Agent processing and transmission to IBM.
- The focal point Hardware Management Console-based Electronic Service Agent component receives the collected I/O device error and statistical data, system software and PTF from the operating system component.

  The focal point Hardware Management Console analyzes and filters I/O device error and statistical data. Statistical summaries are accumulated, duplicate reports are counted and service needs are analyzed. If a device reports an error that requires IBM service, a request is sent to RETAIN and all accumulated statistical data is sent to IBM. An IBM CE is dispatched if required.

  For system software and PTF data received from the operating system component, all analysis, filtering and transmission formatting are performed by the operating system component. The Hardware Management Console component verifies the file format and sends the data to IBM.

Once the collected data is received by IBM, a customer may view their data through new and enhanced remote electronic web-based service offerings. Contact your IBM representative to obtain more information about electronic services offerings, provided by IBM, that allow customers to view and utilize their collected data.

The following diagram depicts the activity and flow of data that Service Agent manages.

It shows the types of data (I/O Error data, Software and PTF data) collected, how and to where that data is transmitted, where that data is stored, and how you can view that data.

Figure 25. Service Agent Activity Flow

1. The primary function of the operating system (z/OS) based Service Agent Data Collection component is to allow the customer to configure and tailor the Service Agent data collection component with attributes that are unique and tailorable to the installation. The types of data that may be enabled for collection from the S/390 environment include:
   - Selected I/O hardware failures
   - I/O Statistical data
   - System configuration data
   - Installed IBM z/OS software information
   - Installed service for IBM z/OS software

2. Once the data is collected from the operating system resources (such as SYS1.LOGREC and installation selected CSIs) and processed, the data is formatted for transmission and sent using File Transfer Protocol (FTP) to the installations Hardware Management Console that has been configured to serve as the focal point for Electronic Service Agent Analysis processing and transmission to IBM.
3. The Hardware Management Console-based Electronic Service Agent Analysis component receives the collected I/O device error and statistical data, system software and PTF data from the operating system component.
4. For all I/O device incidents that require IBM service, the Hardware Management Console based Service Agent Analysis component sends a request to RETAIN and sends accumulated I/O statistical data to the IBM Electronic Service database. The IBM RETAIN system will open problem records and dispatch SSRs based on the error data received.

   For system software and PTF data received from the operating system component, all analysis, filtering and transmission formatting are performed by the operating system component. The Hardware Management Console analysis component verifies the file format, and sends the data to the IBM Electronic Services database.
5. The data sent to the IBM Electronic Services database resides in the eService repository infrastructure and is available for use by eService based offerings as well as other IBM exclusive electronic services offerings.

B.2 Understanding the Service Agent Application work flow when data are sent directly to IBM

The Service Agent Sending component which previously only used the FTP protocol to transmit data to the HMC Service Agent, has been enhanced to support a secure Internet connection directly between the z/OS owning system client and IBM. The secured connection is implemented using secure HTTP over SSL (HTTPS) , which is provided by JSSE (Java Secure Socket Extension) components and digital certificates.

This approach is flexible and secure. Flexible in that it now provides 2 modes of communication for customers using HMC to forward data or sending data directly from the host to IBM. This implementation removes the requirement for the HMC to have a separate LAN connection for Service Agent use. This will now allow Service Agent to transmit data to IBM unfettered from HMC dial up time and size restrictions (5 minutes timeout and less than 2MB transaction size). All Service Agents components are enhanced to use this feature, software and hardware. Secure in that it also adheres to all IBM IES requirements. The method of communication is customer determined and as before, communication will be initiated by the Service Agent clients either through dynamic user requests or predetermined times.

The following diagram illustrates the 2 ways that zSeries Service Agent will communicate with IBM:

1. HMC communication using FTP via a secure dial connection
2. Direct connection via HTTPS.

Figure 26. Service Agent to IBM Communication

Customers who select direct connection as a communication mode will enable them to securely send data from their host to IBM without dependency on the HMC connection. This communication is fully IBM IES compliant. Sending data to IBM using HMC Service Agent, will continue to exist in 2 flavours for the foreseeable future:

1. IBM IES compliant mode using either dial up or LAN/internet connection available only on z9 zSeries systems.
2. Not fully IES compliant mode, OS/2 based dialup only available on previous zSeries systems.

Service Agent code on z9 HMCs is also enhanced to support a secure connection, providing additional capability for forwarding data either over LAN/internet or dial up to IBM. Additional filtering capability is provided for FTP access to ensure that only Service Agent owning systems are eligible to send data to the HMC. This functionality is not downward compatible to OS/2 based HMCs, making them still not fully IES compliant. These customers can be advised to switch to direct connection from the host, assuming that they have required prerequisites and an Internet connection.

B.3 Understanding data types

Data types, as used by the Service Agent program, consist of the following:

- Software data type

  Software data type information consists of SMP/E CSI data gathered during the installation of software products and services. A software data type includes the following data pertaining to a product:

  - Program Product number
  - Program Product name
  - Program Product feature(s)
  - Software element ids (fmids) related to the feature(s)
  - Rework date for software element (fmid)
  - Zones name and type in which the software element resides

- CSIs name in which the zone resides
- Service element id (ptf number)
- Software element id (fmid) the service is in relation with
- Date whereby service is SMP/E received, applied and accepted
- Target zone in which service is applied
- Dlib zone in which service is accepted

- Hiper data type

  Hiper data type provides electronic notification of critical software fixes (HIPER APARs) and PTFs in Error (PEs) available for the customer's specific z/OS environment, as well as the ability to electronically download the fixes for these problems.

- Enrollment data type

  Enrollment data type information consists of user and system data. An enrollment data type includes the following data.

  - Contact information
  - Company information
  - Location information
  - Authorized Web ids
  - Machine id and Access code for the system
  - Company name for the system

  As administrator of Service Agent, you can collect and send this data to IBM. The collect actions can be done anytime you want to or you can configure the Service Agent program to do the collection and transmission of the data automatically.

Appendix C. Hardware data collection and reporting task

C.1 How the parameters work with the Hardware Data Collector program

The Hardware Data Collector started task comes in 2 flavours:

1. HESRDLOG module which is used for HMC communication mode
2. HESHWRDL module which is used for Direct connection mode

Both tasks, unless otherwise stated, are controlled by the same set of parameters, keywords and variables that can be assigned a value and passed to the respective program. Many of these parameters are intended for use only under IBM direction and are documented as such in the shipped HESPARMS data set.

All of the modifiable program parameters are found in the ***hlq.***HESPARMS data set. As of APAR PK18451, a single HESPARMS data set is shipped in support of both Direct Connection and HMC Communication mode. Parameters that are not required for one mode are commented out. The parameters consist of a keyword, followed by the variable name and then the assigned value.

When the Hardware Data Collector program is started, the ENV HLQ= keyword and variable needs to be specified on the JCL parm card, so Hardware Data Collector can find the ***hlq.***HESPARMS dataset. The ***hlq.***HESPARMS dataset is then read. The ***hlq.***value must correspond with the high level qualifier value specified in the HESALCHW allocation job run as part of the steps performed to customize and configure the Service Agent for hardware data collection and reporting.

The Hardware Data Collector program reads all the keywords and variables specified on the PARM in the started task JCL. The keyword and variable values specified on the PARM can be used to override any parameter from the ***hlq.***HESPARMS dataset. Some of the variables have default values coded in the Hardware Data Collector program itself. The priority order is as follows:

- Program default values, if applicable, are overridden by;
- ***hlq.***HESPARMS dataset values, which are overridden by;
- Started task JCL PARM

The following table lists the most commonly used keywords and variables. Typically, only the ENV keyword is passed in the started task JCL.

Keyword	Variable Name	Default	Explanation
ENV ENVIRON-MENT	HLQ		Hiqh-level qualifier for location of HESxxxxx datasets.
	EREP		Invoked from EREP JCL. Causes a one-time job execution.
	DEBUG		Adds informational statements to JES output.
	VERBOSE		Same as above, with more details.
	WTO	YES	WTO=N disables WTO (write to operator) messages.
REMOTE	These REMOTE Parameters are used in HMC communication mode only		
	DELETEFILE	NO	Prior to sending the new remote file, delete the old remote file, if found on the HMC. Remote file is the logrec error data file (Remote Filename + Remote Fileext) that is sent to the HMC.
	FILEEXT	.SOD	File extension of EREP error data file that's written to the HMC. This file extension MUST NOT be changed. The HMC looks for this file when sending data to IBM.
	HOST		IP Name or decimal.dotted address.
	CHECKW	600	Number of seconds to wait after FTP failure on initial start of program. If still failing, then program ends with WTO.
	PASSWORD		Password for the FTP userid. Set using ACSADMIN on HMC
	FILENAME specifies the unique name (maximum 8 characters) of the repository file containing the logrec error records. • In HMC mode, the filename is suffixed with the REMOTE FILEEXT value and sent to the HMC. • In Direct Connection mode, the filename will be prefixed by the ENV HLQ and suffixed with EREPDATA to create a data set on the z/OS host that's transmitted to IBM.		
	FILENAME	&SYSNAME	
INTERVAL	WAIT SLEEP	300	Seconds to wait between read cycles.
	SPOOL	7	Number of days to accumulate in HESPRINT before spooling the output to a new joblog.
READ	STARTDATE	TODAY	Julian date. YYYYDDD
	STARTTIME	00000000	Time in 24 hr format. hhmmsstt.
	RECORD	30*,90,91,RECORD A2,A3*	Type of records of interest. Records marked with * cause an immediate SEND to occur.
	DEVICE	table	Table of included devices to find. Syntax is device type, OBR code, MDR code.
	CUA	table	Table of excluded devices by device address (Nxxx). Coded same as EREP.

In the PARM field, multiple Variable Names for the same Keyword are delimited by a comma. Multiple Keywords are delimited by a semicolon. For example,

```
// PARM=ENV HLQ=hlqual.mdlqual.,VERBOSE,WTO=N; INTERVAL SLEEP=600;
// REMOTE FILENAME=SYSA'
```

Or, if you are using a started task entitled HESRDLOG and you are starting from TSO, you may use a colon instead of the semicolon to avoid the concatenation symbol ";." For example,

```
/S HESRDLOG,ESAPARM='env debug,verbose,wto=n:interval wait=900:REMOTE filename=sysb'
```

Note

For started task HESHWRDL (Direct Connection), the debug parameter is a subset of the verbose parameter. In other words, specifying verbose would include the verbose trace statements as well as the debug trace statements as follows:

```
/S HESHWRDL,ESAPARM='env verbose,wto=n:interval wait=900:REMOTE filename=sysb'
```

You can control which devices are eligible for data collection. By default, ALL devices that write error records (Type 30,90,91,A3) to LOGREC are included. If you have I/O that is not on IBM maintenance, you can exclude individual devices, or blocks of devices, using the ***hlq***.HESPARMS data set. Refer to Excluding devices from hardware data collection and reporting for more information.

The HESPRINT/SYSPRINT Job Log

Output from the Hardware Data Collector started task is kept in the job log HESPRINT for HMC communication and SYSPRINT for Direct connection. This appendix explains some of the more common messages that are found in the Hardware Data Collector output stream. This is an example of a HESPRINT job log, but is also applicable to SYSPRINT as well. All of the output messages start with HES.

Comments are inserted in the following example HESPRINT job log for explanation. Comment lines start with a ====>>>>:

```
HES80999I 01-26 134713 HESRDLOG 20001220 14:59:59 01.01.00.

====>>>> 01-26 is the month-date and 134713 is the timestamp of
         13:47:13

HES80001I 01-26 134713 5655-F17 (C) Copyright IBM Corp. 2000,2002.
HES80001I 01-26 134713 All Rights Reserved.
HES80001I 01-26 134713 US Government Users Restricted Rights -
HES80001I 01-26 134713 Use, duplication or disclosure restricted by
HES80001I 01-26 134713 GSA ADP Schedule Contract with IBM Corp.
HES80001I 01-26 134713 Licensed Materials - Property of IBM.
HES80001I 01-26 134713
HES80002I 01-26 134713 Command Line: ENV HLQ=TEST1..

====>>>>From the parm card of the JCL.

HES80164I 01-26 134713 Checking remote HMC availability.

====>>>> This is the FTP check

HES80166I 01-26 134716 Sending extant data.

====>>>> A previous HESRDLOG task had ended, and data was still in
HESTEMP, so it is sent.

HES80167I 01-26 134716 Sending file with 73 records.

====>>>> Number of I/O records that are being FTP'd to the
         Hardware Management Console

HES80165I 01-26 134720 Starting readlog loop.
HES80162I 01-26 134720 Start ttrz > End ttrz.

====>>>> This message is indicating that the next track we
         expected to read, is greater than what LOGREC has. This
         indicates an EREP CLEAR may have been executed (99.9%
         likely).

HES80157I 01-26 134720 Data loss detected: from 0101026F05053093 to 0101026F06102441

====>>>> This is probably not an error! The message indicates that
         the timestamp of the last record read from the previous
         cycle was 05:05:30.93, on Julian day
         026. However, the first record in LOGREC is
         06:10:24.41 on day 026. This occurs
         because an EREP CLEAR is done every day around
         06:00. If you see this message, and an EREP
```

```
         CLEAR was not submitted, then you may have an
         error condition that needs to be investigated.

HES80167I 01-26 151226 Sending file with 137 records.
HES80034I 01-26 191246 Send Interval(14400) exceeded(14415).

====>>>> The REMOTE SEND parameter timer has
         tripped. No data was sent in the past 4 hours, so
         if there is any data in HESTEMP, it will be sent
         now.

HES80167I 01-26 191246 Sending file with 85 records.
HES80034I 01-26 231311 Send Interval(14400) exceeded(14418).
HES80167I 01-26 231311 Sending file with 156 records.
HES80034I 01-27 031343 Send Interval(14400) exceeded(14427).
HES80167I 01-27 031343 Sending file with 205 records.
HES80167I 01-27 031851 Sending file with 6 records.
HES80034I 01-27 071920 Send Interval(14400) exceeded(14423).
HES80167I 01-27 071920 Sending file with 132 records.
HES80034I 01-27 111939 Send Interval(14400) exceeded(14414).
HES80167I 01-27 111939 Sending file with 76 records.
HES80034I 01-27 151956 Send Interval(14400) exceeded(14413).
HES80167I 01-27 151956 Sending file with 33 records.
HES80034I 01-27 192016 Send Interval(14400) exceeded(14415).
HES80167I 01-27 192016 Sending file with 64 records.
HES80167I 01-27 200523 Sending file with 13 records.
HES80034I 01-28 000553 Send Interval(14400) exceeded(14419).
HES80167I 01-28 000553 Sending file with 212 records.
HES80167I 01-28 002602 Sending file with 22 records.
HES80167I 01-28 010609 Sending file with 49 records.
HES80167I 01-28 013117 Sending file with 22 records.
HES80167I 01-28 032129 Sending file with 139 records.
HES80167I 01-28 032634 Sending file with 9 records.
HES80167I 01-28 033138 Sending file with 6 records.
HES80034I 01-28 073159 Send Interval(14400) exceeded(14416).
HES80167I 01-28 073159 Sending file with 181 records.
HES80034I 01-28 113220 Send Interval(14400) exceeded(14416).
HES80167I 01-28 113220 Sending file with 89 records.
HES80034I 01-28 153235 Send Interval(14400) exceeded(14411).
HES80167I 01-28 153235 Sending file with 28 records.
HES80167I 01-28 191251 Sending file with 31 records.
HES80034I 01-28 231311 Send Interval(14400) exceeded(14416).
HES80167I 01-28 231311 Sending file with 118 records.
HES80034I 01-29 031331 Send Interval(14400) exceeded(14415).
HES80167I 01-29 031331 Sending file with 184 records.
HES80162I 01-29 060347 Start ttrz > End ttrz.
HES80157I 01-29 060347 Data loss detected: from 0101029F05582711 to 0101029F06020511
HES80034I 01-29 071352 Send Interval(14400) exceeded(14416).
HES80167I 01-29 071352 Sending file with 242 records.
HES80034I 01-29 111434 Send Interval(14400) exceeded(14431).
HES80167I 01-29 111434 Sending file with 190 records.
HES80034I 01-29 151508 Send Interval(14400) exceeded(14428).
HES80167I 01-29 151508 Sending file with 87 records.
HES80167I 01-29 180527 Sending file with 82 records.
HES80034I 01-29 220556 Send Interval(14400) exceeded(14421).
HES80167I 01-29 220556 Sending file with 52 records.
HES80167I 01-30 014633 Sending file with 99 records.
HES80167I 01-30 021641 Sending file with 9 records.
HES80167I 01-30 031656 Sending file with 41 records.
HES80112I 01-30 060226 File HESDATA is busy (allocated to another job or user).

====>>>> HESDATA (the LOGREC) is busy (EREP is
         running). We will wait 1 minute and try again.  If the
         busy condition doesn't free, HESRDLOG will issue a WTO
```

```
         and end.

HES80162I 01-30 060326 Start ttrz > End ttrz.
HES80162I 01-30 060827 Start ttrz > End ttrz.
HES80157I 01-30 060827 Data loss detected: from 0101030F05533846 to 0101030F06061010
HES80034I 01-30 071831 Send Interval(14400) exceeded(14483).
HES80167I 01-30 071831 Sending file with 90 records.
HES80167I 01-30 075338 Sending file with 3 records.
HES80167I 01-30 080844 Sending file with 10 records.
HES80167I 01-30 082854 Sending file with 8 records.
HES80167I 01-30 102419 Sending file with 84 records.
HES80034I 01-30 142440 Send Interval(14400) exceeded(14416).
HES80167I 01-30 142440 Sending file with 113 records.
HES80034I 01-30 182506 Send Interval(14400) exceeded(14415).
HES80167I 01-30 182506 Sending file with 43 records.
HES80034I 01-30 222526 Send Interval(14400) exceeded(14416).
HES80167I 01-30 222526 Sending file with 48 records.
HES80167I 01-31 012102 Sending file with 82 records.
HES80167I 01-31 032125 Sending file with 75 records.
HES80112I 01-31 060150 File HESDATA is busy (allocated to another job or user).
HES80162I 01-31 060250 Start ttrz > End ttrz.
HES80162I 01-31 060750 Start ttrz > End ttrz.
HES80162I 01-31 061251 Start ttrz > End ttrz.

====>>>> There are three messages in a row, every
         5 minutes. No data was written to LOGREC during the
         06:01:50 until sometime after
         06:07:50. Message below shows the record was
         written at 06:10:12.45

HES80157I 01-31 061251 Data loss detected: from 0101031F05561753 to 0101031F06101245
HES80034I 01-31 072256 Send Interval(14400) exceeded(14481).
HES80167I 01-31 072256 Sending file with 98 records.
HES80167I 01-31 091315 Sending file with 39 records.
HES80034I 01-31 131352 Send Interval(14400) exceeded(14429).
HES80167I 01-31 131352 Sending file with 147 records.
HES80034I 01-31 171412 Send Interval(14400) exceeded(14414).
HES80167I 01-31 171412 Sending file with 49 records.
HES80034I 01-31 211434 Send Interval(14400) exceeded(14417).
HES80167I 01-31 211434 Sending file with 56 records.
HES80034I 02-01 011619 Send Interval(14400) exceeded(14501).
HES80167I 02-01 011619 Sending file with 71 records.
HES80167I 02-01 031659 Sending file with 70 records.
HES80112I 02-01 060247 File HESDATA is busy (allocated to another job or user).
HES80162I 02-01 060347 Start ttrz > End ttrz.
HES80157I 02-01 060347 Data loss detected: from 0101032F05564788 to 0101032F0603
HES80167I 02-01 064852 Sending file with 132 records.
HES80167I 02-01 082907 Sending file with 39 records.
HES80167I 02-01 083416 Sending file with 3 records.
HES80167I 02-01 083922 Sending file with 6 records.
HES80167I 02-01 100954 Sending file with 63 records.
HES80034I 02-01 141026 Send Interval(14400) exceeded(14425).
HES80167I 02-01 141026 Sending file with 136 records.
HES80167I 02-01 145036 Sending file with 38 records.
HES80167I 02-01 145036 Sending file with 38 records.
```

Appendix D. Downloading Hiper report/PTFs from FTP Boulder

The following Hiper note is e-mailed to the ESA user when the AHA order has been processed and is ready to be downloaded from the FTP Boulder Server.

Your Service Agent Hiper/PE service check order is ready to be downloaded

Order Number OM000979 is completed at 09:55 04/05/18.

Your order is now ready to be downloaded. Please download your file(s) as soon as possible for the file(s) will be removed from the FTP server after 15 days.

1. Download data set(s) from IBM FTP server

Please right-click on the links then select "Save Target As..." for IE or "Save Link Target As..." for Netscape to initiate the download process.

FILE NAME	FILE DESCRIPTION	LRECL	BLKSIZE	DATA SET TYPE	TERSED
INSTLIBP	Install Library	1024	6144	PO	Yes
PACKPTF	Tersed PTF File	1024	6144	PS	Yes

2. Upload data set(s) to your host

The following instructions detail the steps for uploading data set(s). The instructions are based on the data set type as illustrated in the table above. Please pay attention to these columns LRECL, BLKSIZE, DATA SET TYPE and TERSED of the above table. You have to use appropriate parameter settings for FTP upload process.

1. ***Sequential Data Set (DATA SET TYPE: PS)***

   a. We assume that you use an interactive FTP session on your workstation. If you are going to use FTP software, please consult with your local help-desk for the parameters configuration before you start the transfer.

   b. Initiate a FTP session with your host.

   c. Make sure that the transfer mode is BINARY. For example: ftp>binary

   d. Set appropriate parameters for LRECL, BLKSIZE, and RECFM. For example: ftp> quote site recfm=FB lrecl=80 blksize=3120

   Note: ALL FILES MUST BE TRANSFERRED WITH RECFM=FB

   e. Upload the file to host.

   For example: ftp> put <src> <dsn>

   where <src> is the name of the file you have downloaded, for example, instlib.exe <dsn> is the name of the MVS data set.

2. ***Partition Data Set (DATA SET TYPE: PO)***

   Follow step a. to step e. for sequential data set.

   f. If TERSED is Yes, go to step 3. Else issue the following TSO command to restore file to the original format.

   For example: receive inda(<dsn>)

   where <dsn> is the name of MVS data set you specified during file upload

3. ***Additional Step For Tersed Files (TERSED: Yes)***

   Files are packed (tersed) to reduce the file sizes. Please unterse files with the instructions below.

   If you do not have the TRSMAIN program, click here to get a copy of the module.

   - Run sample job hlq.SHESSAMP(HESUNTRS) to unterse the files or click here for a copy of sample JCL.

4. ***Receive and review order Hiper reports in Service Agent Dialog***

   After files are received on the host, rename them to mach the following naming convention:

   hlq.AHA. OM000979.D040518.INSTL, for the report library and hlq.AHA. OM000979.D040518.INSTPTF, for PTF data set.

   This data sets name you will be asked to provide in the Service Agent Dialog, View Automatic Hiper Alert option.

Note

If you have any problem, please send an e-mail to cpacis@ca.ibm.com to report your problem.

Appendix E. Service Agent Dialog Status and Mode Messages

.

Status	Mode	Meaning	Available Options	Possible actions
N/A	Not Configured	First time into Service Agent	3. Configure	Configure Service Agent.
Active - idle Active - processing	Enabled	1. Service Agent started tasks are active, waiting or performing work. 2. Service Agent Configured for automatic collect/transmit.	2. Stop 3. Configure 4. Display 5. Run 7. Verify 9. History	Normal operation of the Service Agent. Scheduled collection and transmission.
	Disabled	1. Service Agent started tasks are active performing work for a force request or enrollment update. 2. Service Agent is **not** set for automatic collect/transmit.	2. Stop 3. Configure 4. Display 5. Run 7. Verify 9. History	Service Agent shuts down automatically after processing is finished
Active - idle Scanner Shutdown	Enabled	1. Service Agent is active. Waiting to perform work. One of the two Service Agent tasks - the Scanner is **not** active. Waiting to be started by the Event Manager. 2. Service Agent Configured for automatic collect/transmit	2. Stop 3. Configure 4. Display 5. Run 7. Verify 9. History	Normal operation of the Service Agent. Scheduled collection and transmission.
Not Active	Enabled	1. Service Agent started tasks are **not** active now. No work can be performed unless they are started. 2. Service Agent is set for automatic collect/transmit	1. Start 3. Configure 4. Display 5. Run 7. Verify 9. History	Start Service Agent using dialog. Automatic collection and transmission can only take place when the Service Agent tasks are active.
	Disabled	1. Service Agent started tasks are not active now. No work can be performed unless they are started. 2. Service Agent is **not** set for automatic collect/transmit	1. Start 3. Configure 4. Display 5. Run 7. Verify 9. History	The forced collection or verify transactions trigger Service Agent to be started. Service Agent shuts down automatically after processing is finished.
Event Manager not active	Enabled	One of the two Service Agent tasks - the Event Manager is **not** active. Service Agent **cannot** function normally.	1. Start 2. Stop 3. Configure 4. Display 9. History	Investigate problem. Stop and start Service Agent again. Call IBM if unable to resolve the problem

Appendix F. Notices and Trademarks

F.1 Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject mater described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to your.

This information could contain technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of information which has been exchanged, should contact:

IBM Corporation
Department 80D
P.O. Box 12195
3030 Cornwallis
Research Triangle Park

NC 27709
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM international Program License Agreement or any equivalent agreement between us.

F.2 Trademarks

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

IBM

RS/6000

Electronic Service Agent

S/390

zSeries

OS/390

z/OS

Microsoft, Windows, Windows NT and Windows XP are trademarks or registered trademarks of Microsoft Corporation.

Java is a trademark of Sun Microsystems

CMF is a registered trademark of BMC Software, Inc.

Other company, product, and service names may be trademarks or service marks of others.

Glossary

Definition of Terms

You need to be familiar with the following terms that are used in this manual:

AHA. Automatic Hiper Alert. The term used to refer to the Electronic Service Agent function that electronically notifies customers of critical software fixes - (HIPER APARs) and PTF in error, as well as the ability to electronically download the fixes for these problems.

APAR. Authorized Program Analysis Report

Collection Frequency. Elapsed time and collection frequencies for various data types are as follows:

- Software - daily
- I/O error data - read every five minutes and sent when a critical error is detected

Collector Type. The type of collection initiated by the S/390 client itself. The types are:

INITIAL - Initial first time collection

DELTA - Delta Updates

REFRESH - Subsequent complete refresh after the initial collection

Configuration Inventory. A file structure where customization parameters (input using Service Agent Dialog) are stored.

Customer Inventory. A file structure where customer's collected and delta data are stored.

CSI. Consolidated Software Inventory. The SMP/E data set that contains information about the structure of a user's system as well as information needed to install the operating system on a user's system.

Data Type. Type of data to be collected and/or transmitted (for example: Software, Verify, Enroll, I/O error data) to IBM.

DDDEF entry. An SMP/E entry containing the information SMP/E needs in order to dynamically allocate a particular data set it may need to process SMP/E commands.

Debug Mode. Debug Mode is turned on in order to get a trace of the collect/transmit transactions. SYSPRINT messages will be collected to allow for in-depth investigation if the need arises.

Delta. Differences in data between the current customer inventory data and the previously collected data. Delta is only applicable for Software data type.

Direct Connection. Customers who select direct connection as a communication mode are able to securely send data from their host to IBM through the internet without dependence on the HMC connection. This communication is fully IBM IES compliant.

Electronic Service Agent. See 1.0, “Chapter 1 - What is Service Agent?” on page 1.

Enrollment. The type of transaction used to transmit system and user information to IBM for registration. Also used to send web user id authorization requests. IBM assigns unique machine id and a renewable access code.

Event Manager. The Event Manager is responsible for the following Service Agent activities:

- The scheduling of data collection and/or data transmission, as determined by the values you supply during Service Agent configuration.
- Communicate to the Scanner to perform required activities when the scheduled times for collection, transmission and validation arrive.
- Communicate to the Scanner to perform required activities when a Force command is issued using the Service Agent dialog. Force command, in the context of Service Agent, means that you force a collection and transmission of data using Service Agent. More detailed information is provided later in this manual about the Force command.

Export/Import Function. Enables customers to clone or customize their Sysplex deployment of Service Agent program, and/or backup their existing Service Agent configuration data.

Focal Point Hardware Management Console. The Hardware Management Console that you want to designate as the console to receive the data generated by the Service Agent program is known as the focal point Hardware Management Console. It is recommended, but not required, that this console also be a Hardware Management Console phone server, having a modem and dedicated phone line attached.

Force Command. A command used to force a one time collection and/or transmission of data to IBM. If the scanner is not active when the FORCE command is run, a prompt is displayed to have it started.

FTP - File Transfer Protocol. FTP is the process whereby collected data is transmitted from the S/390 host to the focal point Hardware Management Console.

FTP password. Your FTP password is modifiable at your discretion. Service Agent uses this password when it logs onto the focal point Hardware Management Console to FTP collected information.

Note: Do not change the value of this password using the Service Agent Dialog without verifying that the new value matches the value set for the Service Agent application on the focal point Hardware Management Console.

FTP user ID. Your FTP user ID is "esa390." This userid is fixed and cannot be modified. It is used by Service Agent to logon to the focal point Hardware Management Console during the FTP operation.

Hardware Data Collector. There are two tasks which do hardware data collection:

HESRDLOG - which uses the focal point Hardware Management Console to FTP the data to the IBM Service Bureau.

HESHWRDL - which requests the Event Manager to transmit the data using Direct Connection facilities.

Help Inventory. A file structure which contains help text for the dialog displays.

HIPER. High impact or pervasive APAR

IBM Service Agent Server (SAS). The Service Agent Server (SAS) is located at the IBM company. Your collected data is stored and analyzed there by IBM

PE. Program error PTF. A PTF that has been found to contain an error.

PTF. Program Temporary Fix. A temporary solution to or bypass of a problem that may affect all users and that was diagnosed as the result of a defect in a current unaltered release of the program. In the absence of a new release of a system or component that incorporates the correction, the fix is not temporary but is the permanent and official correction.

RETAIN. A database, accessible through Information/Access, that contains information about APARs and PTFs. The customer version of this database is called the Customer Service Support Facility (CSSF).

Scanner. The Service Agent Service Delivery Module coordinates all activities pertaining to the collection and transmission of data types under its control.

TCP/IP address. Transmission Control Protocol/Internet Protocol address is. the IP address of the focal point Hardware Management Console.

Work Element. Unit of Work is identified by a unique Package ID (PID) assigned by the Scanner. A unit of work normally represents a unit of an instance of a data type. There are 6 package types. They are:

- Software (with Service levels PTFs)
- Hardware
- Enroll
- Verify
- Hiper

A new collection of any of the seven data types is assigned an unique Package ID to identify its uniqueness in the system. The Package ID always starts with PID followed by a 5 digit number. As an example, the output file of a software collection will be identified by the following convention in the system:

```
Software.PID00714.xml
```

There are altogether 11 possible phases, reflecting the different stages which the package can be in.

Work Inventory. A file structure where work elements are temporarily stored during processing.

XML. Extensible Markup Language. A language used for data transfer. Format of data transfer is governed by dtd (data definition).

Index

F

H

I

J

X

Z