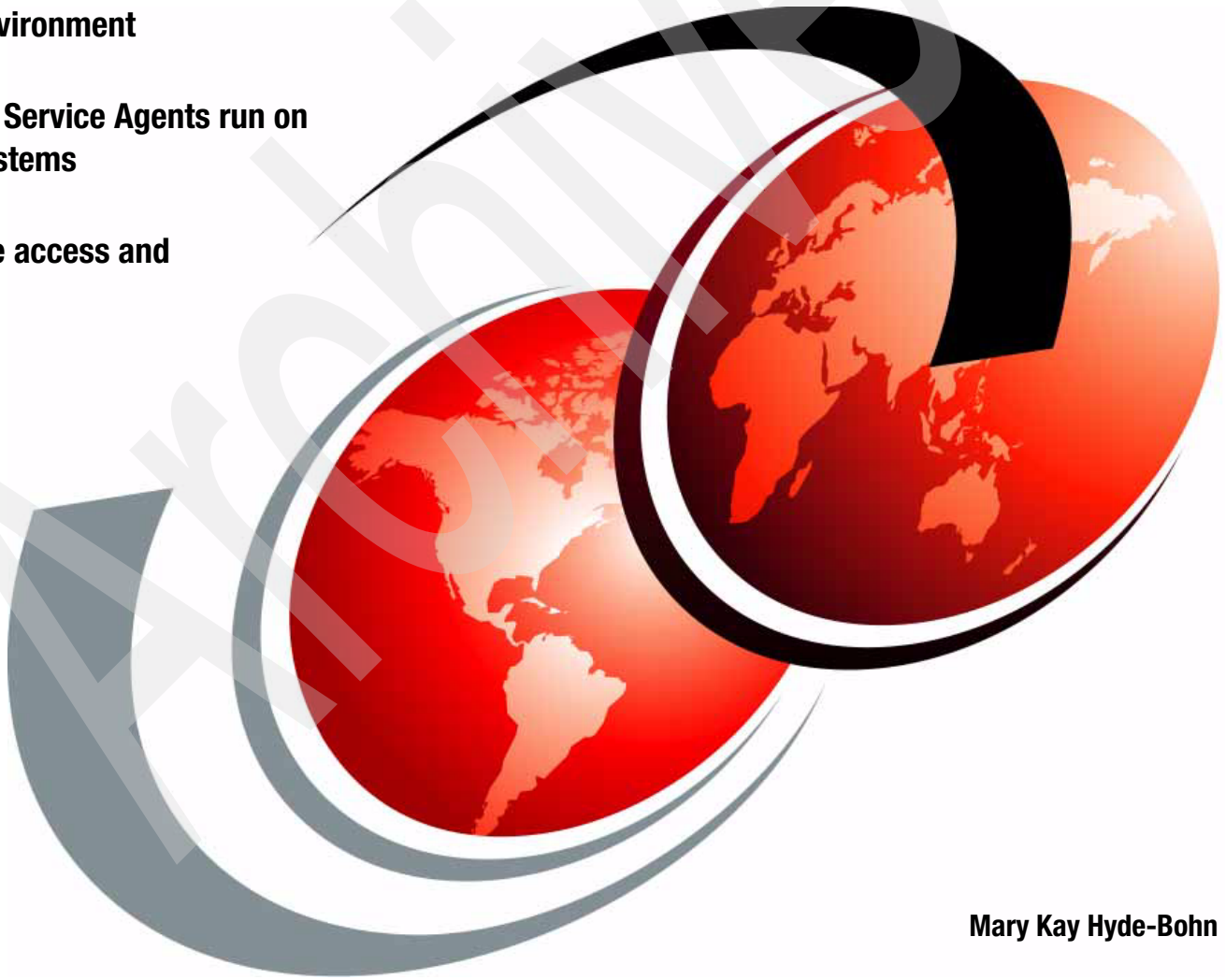
IBM

IBM Electronic Services

Support using Automation and Web Tools

- Simplify and enable faster support for your IT environment
- Electronic Service Agents run on all IBM systems
- Worldwide access and utilization



Mary Kay Hyde-Bohn

Redbooks

ibm.com/redbooks

International Technical Support Organization

IBM Electronic Services: Support using Automation and Web Tools

September 2007

SG24-6323-01

Note: Before using this information and the product it supports, read the information in “Notices” on page vii.

Second Edition (September 2007)

This edition applies to products within or enabled by IBM Electronic Services.

Contents

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 matter 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 you.

This information could include 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.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM application programming interfaces.

Trademarks

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

Redbooks (logo)  ®
eServer™
iSeries®
i5/OS®
xSeries®
z/OS®
zSeries®
z9™
AIX®
DFSORT™
DS8000™
Electronic Service Agent™
ESCON®
HACMP™
IBM®
MVS™
OS/390®
POWER™
POWER4+™
POWER5™
Redbooks®
RACF®
RETAIN®
RS/6000®
S/390®
Service Director™
System i™
System i5™
System p™
System x™
System z™
System z9™
Workplace™

The following terms are trademarks of other companies:

Acrobat, and Portable Document Format (PDF) are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Java, JDK, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Pentium, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

Preface

What is IBM® Electronic Services? Why do you need it? Where do you get it? When and how do you use it? How will this help your electronic support relationship with IBM? Find the answers to these questions and more details about *IBM Electronic Services* in this IBM Redbooks® publication.

The goal of IBM Electronic Services is to simplify your support relationship to make it easier and faster to do business with IBM. Through automation and Internet access, Electronic Services integrates the IBM Support community with your company staff and your IT environment. The two major components are IBM Electronic Service Agent™ (Service Agent) and the IBM Electronic Services Web site.

IBM Electronic Services reaches across all IBM systems in all countries or regions where IBM does business. Electronic Services can provide the electronic support relationship for a single machine environment or a multinational complex of many servers.

This book is intended for IT management, system operators, and other individuals who work for and with IBM clients. Prior to reading this book, you need a thorough understanding of your computer system and networking environments.

The team that wrote this book

This IBM as produced by the IBM Electronic Services global organization. Assistance was provided by the International Technical Support Organization (ITSO), Rochester Center.

Thanks to the following people for their contributions to this project:

Electronic Services Executive team:

- R. Kent Holcomb, Electronic Services Director
- Bob A. Haataia, Electronic Services executive team
- John Speacht, Electronic Services executive team

ITSO: LindaMay Patterson, ITSO Project Leader

Content:

- Linda Allen, Electronic Services Web strategist
- Eve Berman: Hardware Management Console (HMC)
- M. Lauren Bragg, Terry Ulmer, and Ivaylo N. Blajev: System x™
- Eliot T. Burris, Mike A. Edwards, and Ivica Vardic: System z™
- Kent Eastley, Craig Mull, and Eve Berman: System p™
- Scott Fredericksen, Service Agent Strategist
- Mary Kay Hyde-Bohn: IBM Redbooks publication coordinator
- Mark McDonnell and Sandra Westling: System i™

Become a published author

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You

will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our booksto be as helpful as possible. Send us your comments about this bookor other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review IBM Redbooks publication form found at:

  ibm.com/redbooks

- Send your comments in an e-mail to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Summary of changes

This section describes the technical changes made in this edition of the IBM book. This edition might also include minor corrections and editorial changes that are not identified.

Summary of Changes
for SG24-6323-01
for IBM Electronic Services: Support using Automation and Web Tools
as created or updated on September 13, 2007.

September 2007, Second Edition

This revision reflects the addition, deletion, or modification of new and changed information described below.

New information

The new information includes:

- New tools on the Electronic Services Web site
- Electronic Service Agent (ESA) Connectivity
- ESA support for Linux®

Changed information

The changed information includes:

- Expanded uses of ESA information on the Electronic Services Web site
- Updated Web site tools
- Security and privacy information
- Updates to Service Agent new versions
- Expanded information on Hardware Management Console (HMC) ESA

1

Welcome to IBM Electronic Services

During the course of reading this book, you learn about IBM Electronic Services:

- What IBM Electronic Services is
- Where to get more information about IBM Electronic Services
- When and how to use IBM Electronic Services
- How IBM Electronic Services enables your electronic support relationship with IBM

The goal of IBM Electronic Services is to simplify your support relationship and make it easier and faster to do business with IBM.

This chapter focuses on two key components of IBM Electronic Services:

- IBM Electronic Service Agent (ESA)
- IBM Electronic Services Web site

This chapter presents an overview of how these components interrelate, how they support each other, and how they provide input to other IBM organizations.

Subsequent chapters give you information about the uses of ESA information within IBM tools, specific categories on the Electronic Services Web site, and the reference information for each Service Agent.

1.1 Electronic Services

Electronic Services is an IBM support approach made up of Electronic Service Agent and the Electronic Services Web site, as illustrated in Figure 1-1. Electronic Service Agent (ESA) submits hardware problems and collects service information. Both submissions are transmitted automatically within protected firewalls into the IBM structure. This information is visible for your use and for those users you authorize on the Electronic Services Web site. Organizations within IBM can use the same information or results to assist you with support functions, solution delivery, and planning.

This structure works in any IBM system client environment: System i, System p, System x, or System z platforms with their respective operating systems (OSs) and Linux.

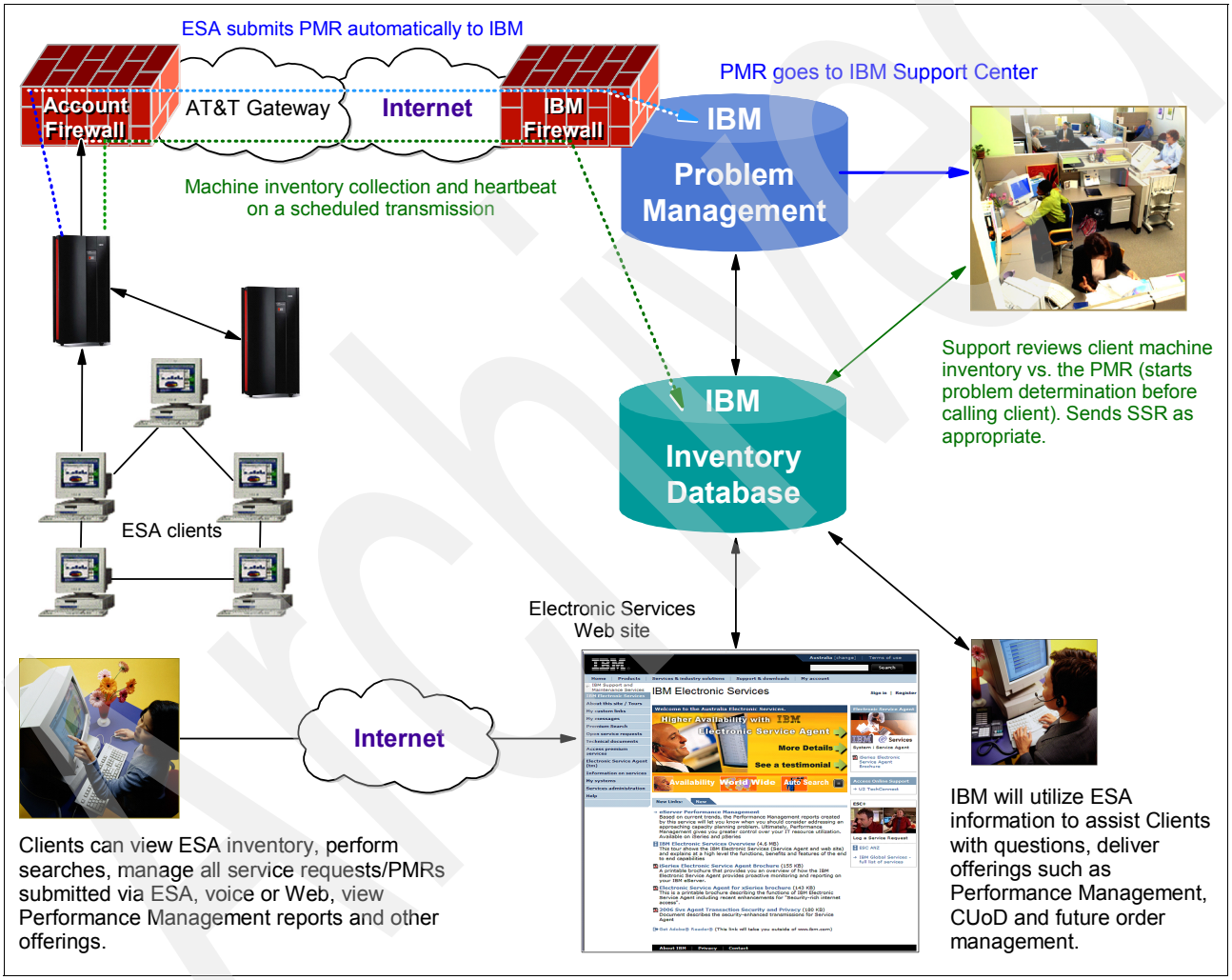


Figure 1-1 eServices overview

1.2 Electronic Services are necessary

Electronic Services provides an electronic collaboration between you and IBM, so that IBM can offer better support of your information technology (IT) environment. The goal of IBM Electronic Services is to simplify your support relationship by making it easier and faster for you to do business with IBM.

Electronic Services brings the following benefits to your organization:

- Client systems might have higher availability due to shorter problem resolution time and less downtime.
- All elements are easy to activate, easy to use, available on all IBM platforms, available globally, and secure.
- Client problem information and service information are readily available to the IBM Support Community through an internal Web site.
- Electronic Services enables personalized services, such as My Systems, My Search, Performance Management, Electronic Technical Services (ETS) including Alert, Maintenance Level Comparison Reports (MLCR), and Capacity Upgrade on Demand (CUoD).
- ESA can submit hardware problems automatically with additional error data.
- ESA works with other IBM tools to identify a potential fix or create an action plan for the IBM Support Center.
- IBM and Business Partners can provide the best, personalized support and guidance using the ESA information.
- 7x24 Web site enables your systems to potentially have higher availability due to shorter problem resolution time and less downtime:
  - View or print your ESA information for business or technical analysis.
  - Search IBM technical databases using your ESA information to filter results.
  - Review IBM technical resources or access IBM service offerings.
  - Submit hardware or software service requests.
- Peace of mind knowing that IBM is there to ensure that your systems run smoothly.

Information about all the Electronic Services elements are available at the Electronic Services Web site in flash tours, informational PDFs, or actual download files:

`https://www.ibm.com/support/electronic`

1.3 Privacy and security of Electronic Services

Here are several brief descriptions of the layers of security and privacy that are used by Electronic Services, how IBM provides privacy for your information as viewed on the Web site, and how IBM secures the transmission from your systems to IBM:

- The secure ESA transmission to IBM is described in Chapter 5, “IBM Electronic Service Agent and the Hardware Management Console security” on page 51, with descriptions of the communication methods available for each platform. The ESA transactions are subject to IBM Security rigorous guidelines and updated frequently.
- The IBM ID entered during ESA activation is the *account contact* for any other IBM IDs that will be associated with that system. (You use this same IBM ID in many of the IBM Web sites.) You control who can view and use the ESA information, for example, your IT department staff, extended staff, and Business Partners. On the Electronic Services Web site in the Services Administration category, you can add more IBM IDs, select more systems per IBM IDs, and remove IBM IDs from systems.
- The machine inventory information collected by ESA is typically collected by speaking with clients during phone calls with the IBM Support Center, pre-sales specialists, administrative clerks, and other groups within IBM. These IBM groups now have electronic

access to the information so that they can prepare and perform advance problem determination and more efficiently serve IBM clients.

The ESA inventory information includes:

- Your support contact information, including names, phone numbers, and e-mail addresses
- System utilization, performance, system failure logs, part feature codes, part number, part serial number, part locations, software inventory, operating system applications, program temporary fixes (PTFs), the maintenance level, and configuration values

Inventory information does not include:

- Collection or transmission of any of your company's financial, statistical, or personnel data
- Client information
- Your business plans

- ESA can provide a *call home* mechanism for other IBM offerings that you might select in the future. The information collected by these offerings is covered by separate agreements, for example, for Performance Management and Capacity Upgrade on Demand offerings.

1.4 Electronic Service Agent

The Electronic Service Agent is a *no charge* software tool that resides on your system to monitor events and transmit system inventory information to IBM. It ships with many IBM systems without an additional charge. For other systems, it can be downloaded from the Electronic Services Web site or ordered free of charge. The platform-specific chapters, starting with Chapter 4, "IBM Electronic Service Agent" on page 41, give details about installation and activation of ESA for each IBM system platform.

ESA's two key functions, automatic hardware problem reporting and service inventory information collection, enable proactive and predictive services, as well as faster problem resolution and call avoidance. ESA tracks and captures machine inventory, hardware error logs, and automatically reports hardware problems to IBM if the server is under a service agreement or warranty. The information is available to you, your authorized users, and IBM representatives.

You can add your IBM Business Partner representative to your authorized users by adding their IBM ID to your list of authorized users.

Table 1-1 on page 5 outlines the features and benefits of ESA hardware reporting by IBM hardware platforms.

Table 1-1 ESA automatic hardware reporting

Feature	System i	System p	System x	System z
Report hardware problems and send error data.	Yes	Yes	Yes	Yes
Collect the extended error data.	Yes	Yes	No	No
Consult the knowledge base for additional fix information.	Yes	Yes	No	Yes
Collect the system logs.	Yes	No	No	No
Determine part numbers.	Yes	Yes	Yes	Yes
Notify IBM service support representative (SSR).	Yes	Yes	Yes	Yes

ESA hardware reporting enhances client satisfaction and has these benefits:

- Confidence knowing your system is being monitored
- Less time spent explaining problems to the IBM support community
- Higher availability through faster problem resolution
- Better call routing because more information is known up front
- Getting the right part the first time saves time
- Higher quality and effectiveness of support
- Ability to view Service Agent information on the Web
- Leveraging IBM resources

Table 1-2 outlines the features and benefits of the inventory collection function by IBM hardware platforms.

Table 1-2 ESA machine inventory collection

Feature	System i	System p	System x	System z
Hardware inventory and system Configuration	Yes	Yes	Yes	I/O only
Software inventory	Yes	Yes	Yes	Yes
PTFs (software fixes)	Yes	Yes	Yes	Yes

The benefits of ESA machine inventory collection are:

- Access current system configuration easily to assist in problem determination
- Call out the accurate parts
- Identify accurate hardware and software fixes
- Enable marketing to assess needs and requirements
- Enable customized solutions for marketing and sales
- Ensure accurate billing

Table 1-3 outlines the features and benefits of transmission security. Electronic Service Agent communicates with IBM through a secure connection using encryption and authentication, with Internet or a dial-up connection using AT&T Global Network Services. You can ensure your privacy and the security of your machine inventory information and problem submission record, both in the transmission and usage of your information inside IBM. In Chapter 6, "IBM Electronic Service Agent: Connectivity for System i and System p" on page 69, you see more detailed information and graphics showing these connection styles.

Table 1-3 ESA transmission security

Feature	System i	System p	System x	System z
Connect to IBM using HTTPS	Yes	Yes	Yes	Yes
Connect to IBM using the Internet	Yes	Yes	Yes	Yes
Connect to IBM using Dial-up	Yes	Yes	Yes	Yes
Proxy/Firewall support	Yes	Yes	Yes	Firewall only

The benefits of ESA transmission security are:

- There are a variety of connection options to satisfy most client configurations.
- All connections are secure.
- All communications are encrypted.
- All communications are authenticated.

1.5 Electronic Services Web site

The Web component of IBM Electronic Services offers a single location for you to access many IBM Internet service and support capabilities. You can also view and use the ESA inventory information. This is a global site, which is tailored to 65 countries (regions) and national languages, with visibility to the services offered by IBM in that country or region.

The Electronic Services Web site offers:

- A single portal for hardware and software information and reference materials
- My Systems to view and use ESA service information in customized reports, such as hardware and software inventory, fixes, and system parameters
- My Search facility that uses Electronic Service Agent information to provide customized results for your specific machines from the IBM reference databases
- A single place to submit a service request for either hardware or software, in any country
- My Messages to receive information for specific platforms or individual profile definition
- Access to Web-delivered premium services, such as Performance Management or Enhanced Technical Support (ETS) contracted services
- My Links to customize the Web view by your selections of IBM system platforms
- Tutorials or demonstrations provided for all major areas of the Web site

Table 1-4 shows the features available for each IBM system platforms.

Table 1-4 Electronic Services Web site: My Systems view of ESA inventory

Feature	System i	System p	System x	System z
Hardware inventory and system configuration	Yes	Yes	Yes	No
System inventory	Yes	Yes	Yes	Yes
PTFs (software fixes)	Yes	Yes	Yes	Yes

The benefits of the My Systems view of the Electronic Services Web site are:

- Easy Web access to current system configuration assists in problem determination even when your system is unavailable.
- The My Systems view enables comparison of inventory across multiple systems.
- This view provides customized reports for printing and record keeping.
- You control the access so that you can add or remove users on the Web.

Table 1-5 shows the features available for each of the IBM systems when using ESA information during a My Search query.

Table 1-5 Electronic Services Web site: My Search using Service Agent

Feature	System i	System p	System x	System z
Filter by installed fixes	Yes	Yes	Yes	Yes
Filter by operating system type	Yes	Yes	Yes	FMID
Filter by installed products	Yes	Yes	Yes	Yes

The benefits of My Search using Service Agent information are:

- Search based on what you have installed with the release level and fixes.
- Reduce irrelevant search results to help you focus on what applies to your system.
- Save searches so that you can quickly search for documents of interest and related to your system inventory.

Table 1-6 shows the options available in the Service Request area of the Electronic Services Web site.

Table 1-6 Electronic Services Web site Service Request

Feature	Americas	Asia	Europe
Hardware	Yes	Yes	Yes
Software	Yes	Yes	Yes
Unique country or region offering titles	Yes	Yes	Yes

The benefits of the Service Request area of the Electronic Services Web site are:

- You can access many Web tools from one location.
- You can use these tools for submitting or checking status on a service request instead of calling IBM support.
- Tutorials are available for hardware or software submissions.

2

Use of Service Agent information

In this chapter, you explore many uses for your IBM Electronic Service Agent (ESA) information. Be sure to consult with your account team for recent updates to existing offerings, new offerings, or new solutions.

This chapter discusses the use of ESA information by IBM organizations, Web tools or offerings, and processes. The value to your company is to have ESA information available 24x7 to support your operations, your staff, the IBM support community, and future planning. The increased use or wider use of ESA information is continually updated based on client suggestions of where this information can help you with self-assistance or help IBM provide support with greater ease and efficiency.

The machine information you can see and use is based on your IBM ID. You can add your IBM ID when activating the Service Agent code, request a specific machine serial to be associated with your IBM ID on the Electronic Services Web site, or add an IBM ID to view your machines using the Electronic Services Web site.

2.1 Where ESA information is at work

Electronic Service Agent (ESA) information is found at many levels inside IBM, helping to improve your support experience and provide the best support possible. The locations or solutions listed are the current locations. However, solutions and locations are expanding each month, so be sure to check with your account team.

2.2 Automatic hardware problem submission

The prompt resolution of Service Requests or Problem Management Reports (PMRs) is a challenge to both you and to IBM. We both want to obtain the latest information to help find the best solution to a problem in the most prompt manner.

When ESA detects a hardware problem and submits it to IBM, it brings along additional information about the problem, the system operations at the time of the problem, and other information, based on the type of system submitting the problem. The problem is routed to the local support center for that system. Based on your contract coverage, the IBM Support Center will contact you about your situation with a possible action plan.

The IBM Support community has access to your ESA inventory information, as well as the information that came with the problem, so they have more information to use in problem determination and resolution than in previous years.

2.3 Viewing Service Agent information

The My Systems category in the Electronic Services Web site is where you can view your machine inventory that is collected and transmitted by ESA. The same information is visible to the IBM Support community for use in problem determination. There are a wide variety of uses for these reports, such as asset control, insurance documentation, disaster planning, hardware consistency within your corporation, future planning, and software planning.

You select the machines that you want to include in the reports. The list displayed is of the machines that are associated with your IBM ID. The selection table includes a column with the date of the last inventory transmission to IBM so that you know how current the information is that is provided in the reports.

The reports are available for sorting within columns and printing or downloading in several formats, and they are based on each platform. Each report has header information that includes the inventory and the heartbeat dates for reference. This information is available to the IBM Support community on an internal site.

We describe these reports in detail in 3.5.2, “Select reports” on page 20.

2.4 My Search

The My Search tool that is available on the Electronic Services Web site uses the ESA information to filter your search for an individual system. It enables you to search the IBM technical support knowledge bases that provide informational APARs, FAQs, white papers, and other document types.

Note: A Demonstration Experience is provided on the Electronic Services Web site. You will be able to assign two machine types to your IBM ID and be able to experience the search capabilities yourself. See the Electronic Services Web site information in 3.1, “IBM Electronic Services Web site overview” on page 14 for details.

The basic steps of the My Search are:

1. You enter the search keyword or keywords.
2. Select the system that you want to use for filtering the results from the **Select systems** table.
3. You can increase the filter for the search by specifying fixes that are on the system, products that are installed, and operating system type and level. The filters vary by platform.

2.5 Performance Management reports

Performance Management automates many of the functions that are associated with capacity planning and performance analysis. You activate Service Agent and it automatically collects and transmits system utilization information. This information can include CPU disk utilization, response time, throughput, and application and user usage.

The result is the capacity planning and performance analysis reports and graphs that provide a crisp picture of your current system operating efficiencies. Based on current trends, these reports let you know when to consider rectifying an approaching capacity planning problem. Performance Management puts you in control, as opposed to your system being in control of you. The reports might be free or fee-based depending on your platform. The System i and System p platforms offer Performance Management. More details about these reports are available in *A Systems Management Guide to Performance Management for i5 and p5 Systems*, SG24-7122. View this book at:

`http://www.redbooks.ibm.com/`

2.6 Capacity Upgrade on Demand

Capacity Upgrade on Demand (CUoD) enables you to dynamically activate one or more processors on your IBM system as your business peaks dictate. You can activate inactive processors that are already installed on your server on a temporary or permanent basis.

Electronic Service Agent provides the vital product data (VPD) from your server helping to create the activation code necessary to activate inactive processors on your server. It also provides continuing VPD information:

- *CUoD* allows you to install inactive CUoD processors and memory at an extremely attractive price and then bring new capacity online quickly and easily.
- *On/Off CUoD* allows self-managed temporary activation of CUoD processor and memory resources. You can turn on and then turn off resources as needed. The system monitors the amount and duration of the activations and generates a usage report. Billing for the activations is based on the usage report.

- *Reserve CUoD* allows you to have optimized, automatically managed temporary activation of CUoD processors. You purchase a block of 30 Processor Days of usage time and then assign inactive processors to the shared processor pool. The server then automatically manages the workload and only charges against the Processor Day account when the workload requires over 100% of the base (permanently activated) processing power.
- *Trial Capacity Upgrade on Demand* helps you meet an immediate need for additional resources or to give inactive processor and memory resources a test run. To enable a trial, the user must register the server at the CUoD Web site and request an activation code. The user then uses the code to activate the trial on the registered server.

  For more information about Capacity Upgrade on Demand, go to this Web site:

  `http://www.ibm.com/servers/eserver/about/cod/about/index.html`
- *Capacity BackUp* provides emergency processing capacity for up to 30 days in the event that you lose capacity in part of your operation. It helps you recover by adding reserved capacity on a designated system. Capacity BackUp is intended for companies that require an off-site disaster recovery machine at an extremely affordable price. Using On/Off Capacity on Demand capabilities, Capacity BackUp offerings have a minimum set of inactive processors that can be used for any workload. They also have a large number of inactive processors that can be used at no charge in the event of a disaster.

2.7 Enhanced Technical Support

Enhanced Technical Support (ETS) is available in many countries as a single offering with several components or in separate offerings using the ESA information as a reference for customized support. The grouping of IBM tools and services varies by country. Check with your local account team for availability.

In Europe for example, refer to this IBM Web site:

`http://www.ibm.com/services/uk/index.wss/offering/its/a1007320`

On this Web site, you can read about examples of what is available in the ETS relationship:

- Support for all common IT environments including IBM server and storage platforms, IBM middleware and strategic other equipment manufacturer (OEM) products, for example, Linux, Microsoft®, and Cisco
- Proactive advice by professional account advocates using state-of-the-art tools
- Access to the cross-European knowledge pool of support center engineers with direct access to worldwide laboratories
- A coordinated support service to reduce cost by optimizing availability and preventing any unplanned disruptions
- A consistent service level throughout Europe

3

IBM Electronic Services Web site

The Electronic Services Web site supports 65 countries (regions) in 23 languages, with more countries added each year. This is your Web portal for all IBM Support activities with links for planning purposes, self-assist using Electronic Service Agent (ESA) information to filter results, technical document libraries, service request submission, viewing ESA information reports, and access to offerings and tools that use ESA information.

This chapter explains the IBM Electronic Services Web site categories and features, including PDFs, demonstration opportunities, and links to many IBM information sources. This chapter gives you the opportunity to learn how to use and view the Service Agent information from systems associated with your IBM IDs. You can customize the Web site and receive personalized messages from IBM through this Web site.

You might find it helpful to open a Web browser and follow along viewing your country's Electronic Services Web page:

`http://www.ibm.com/support/electronic`

3.1 IBM Electronic Services Web site overview

The Electronic Services Web site evolved from a single platform, single country, single language site in 1999 to a site that reaches many countries (in their national language) and serves many platforms. Today you are able to view ESA inventory reports, use My Search to get results from IBM databases filtered by your machines, open service requests, customize the site to your preference, and receive support messages by platform or individual. You will take a look at the major categories and the information or tools available.

Note: Several of the categories use the IBM registration ID (IBM ID) for authentication and privacy to determine the relationship to systems (using machine serial numbers) and the ESA information.

The Electronic Services Web site is located at:

`http://www.ibm.com/support/electronic`

When you are on the Web site and select your country, your first view is the IBM Electronic Services welcome and news page. Figure 3-1 shows the Australian news page. This chapter provides sample views in the English language. The left side of view is the list of major categories; the middle section has animation that highlights Submit a service request, Service Agent, and My Search activities and benefits. Just beneath the movie are two tabs: New Links and New Offerings, which provide links that are new to your country's site. On the right side of the Web page are more links to information for you from your local IBM team.

Figure 3-1 Australian Web site

3.2 Your IBM ID

Your IBM Registration ID is your single sign-on or single point of access to IBM web applications that use IBM Registration. You need just one IBM ID and one password to access any IBM Registration-based application. Furthermore, your information is centralized so you can update it in a convenient and secure location. The benefits of having an IBM Registration ID will increase over time as more and more IBM applications migrate to IBM Registration. Because IBM Electronic Services is a registration-based application, you need an IBM ID for IBM Electronic Service Agent. Several categories on the Electronic Services Web site, including My Systems and My Search, use this IBM ID for authentication. You also need this IBM ID to view information that has been reported to IBM through the IBM Electronic Service Agent. For your IBM ID, you can use the user ID for a profile that you already have set up on other IBM Web sites, or you can use the user ID you already have associated with your machine, for example, during Service Agent activation.

Several activities ensure that only authorized users can view and use the Service Agent information:

- Service Agent code must be activated on a machine so that it can transmit inventory information.
- A representative from your company must register their IBM ID during the activation process.

  The first person to register is the administrator who has the ability to add, remove, or approve additional IBM IDs. Additional IBM IDs can be added using the ESA client fields after activation. The ESA chapters show examples of the field.
- A new IBM ID user who requests access to a machine's information completes a request on the Electronic Services Web site under the Services Administration category. This request goes to the administrator of the machine serial number. The administrator must approve the request before any access is given.

For more information about the IBM ID or to create or update your IBM ID, go to this Web page:

https://www.ibm.com/account/myibm/profile.do

Figure 3-2 shows an example of the IBM ID sign-on page on this Web site.

Figure 3-2 IBM ID sign-on page

3.3 About this site/Tours

The About this site/Tours category provides animated tours and documents describing various elements of Electronic Services. All these documents are available for download and use later.

Figure 3-3 shows the tours and PDFs available on the Australian Overview tab.

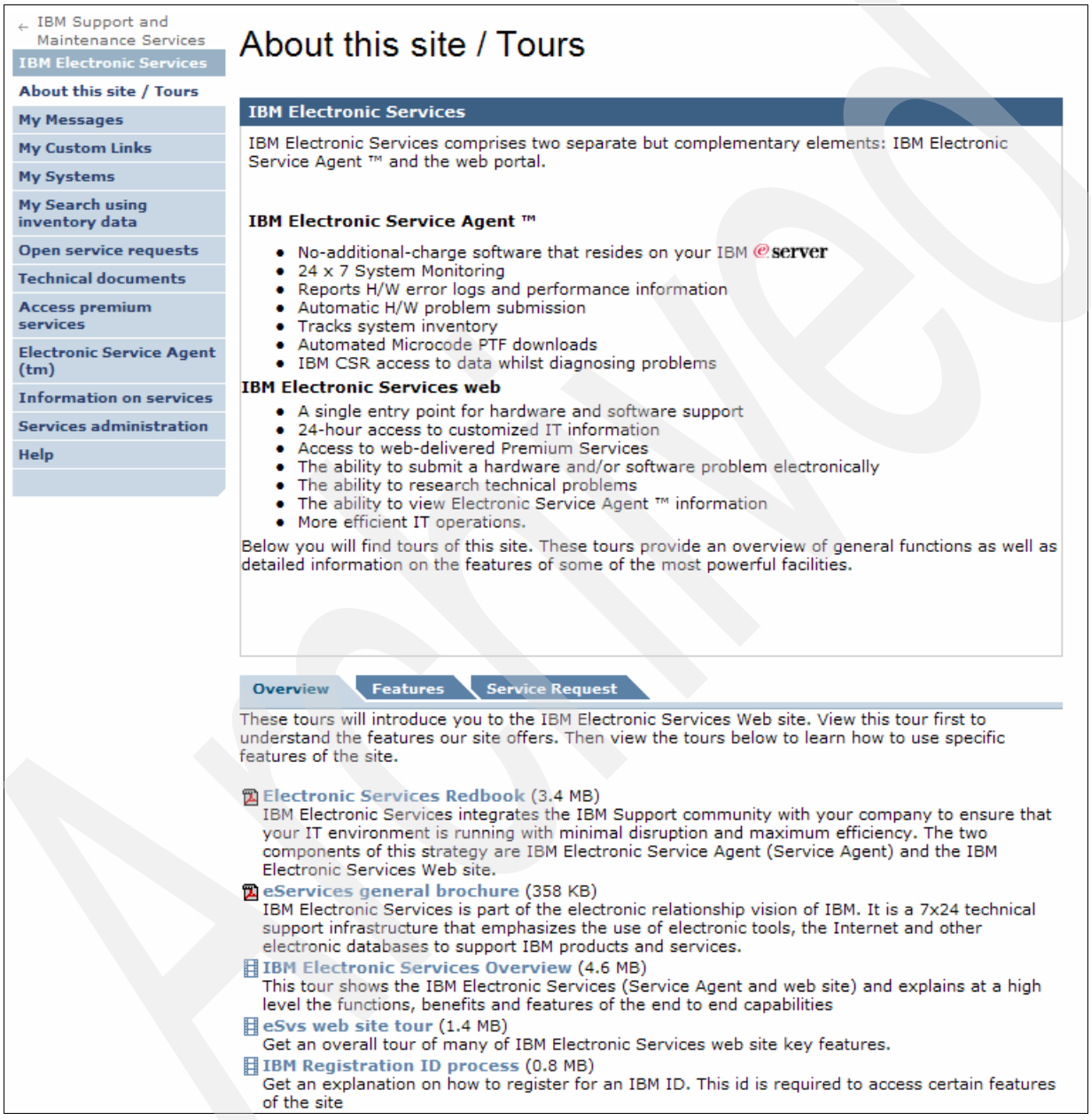


Figure 3-3 Australian About this site/Tours view

3.4 My messages and My custom links

My messages and My custom links are the areas where you can customize your view of the Electronic Services Web site. You indicate which types of messages and notifications you want to see delivered to a mailbox within this site or to your e-mail address. Figure 3-4 shows you an example of this capability.

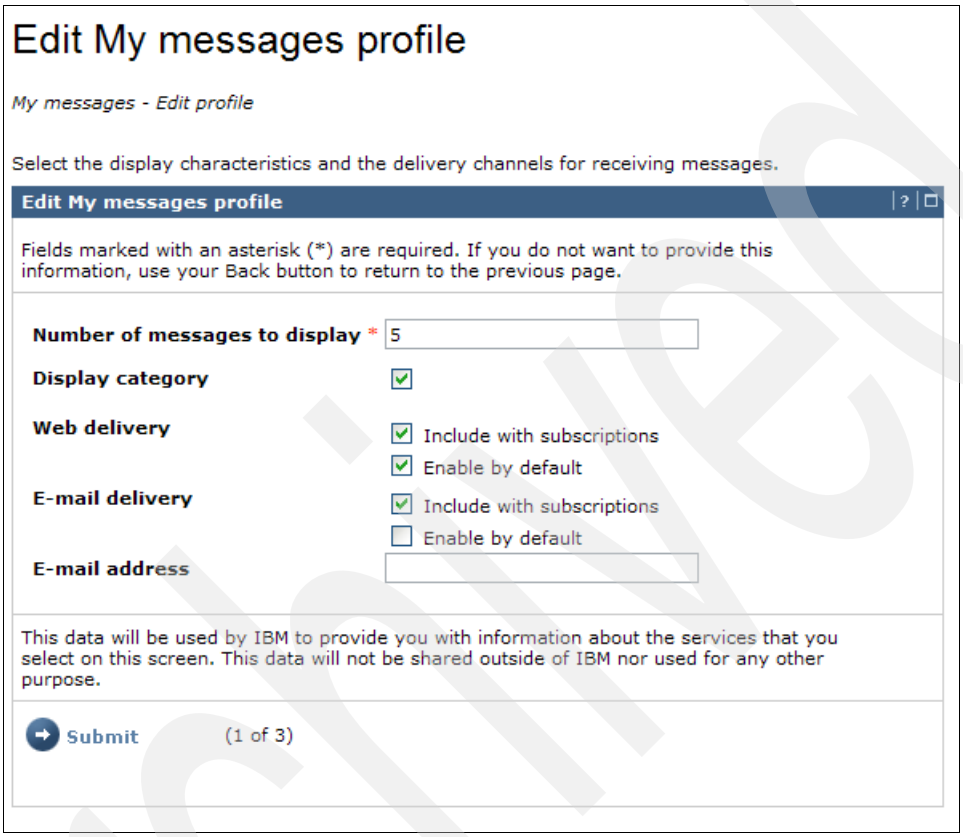


Figure 3-4 Create My messages profile

You can also customize your view of the Web site to show just those links that relate to your system or systems. The average number of links per country (region) on this Web site is over 100. With your own profile, you limit the links to those that relate to the platform or platforms that you have selected, as shown in Figure 3-5.

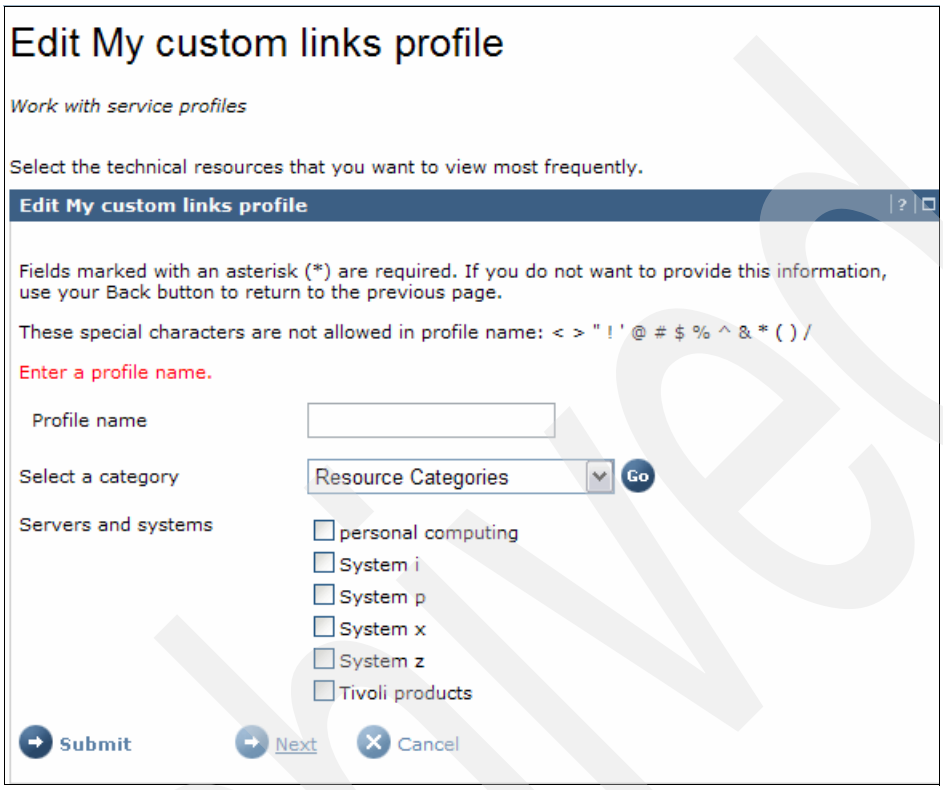


Figure 3-5 My custom links: Create the profile

3.5 My systems

My systems is the area of the Web site that provides your ESA information reports. As mentioned before, your IBM ID is associated with the machine serial numbers that you are able to view and use. This association is done during the activation of Service Agent or a request made later in the Services Administration section of the Web site.

Note: The IBM Support community has visibility to similar reports through an internal site.

3.5.1 Select systems

To begin using My Systems, select the machines that you want to include in the reports by checking those systems in the Identified Systems list. Figure 3-6 shows an example of the “Select system” table. It displays the machine serial numbers that are authorized for the IBM ID used in the session. The table includes a column with the date of the last inventory transmission to IBM so that you know how current the information is that is provided in the reports. The heartbeat time stamp is displayed when that is more current than the latest inventory update.

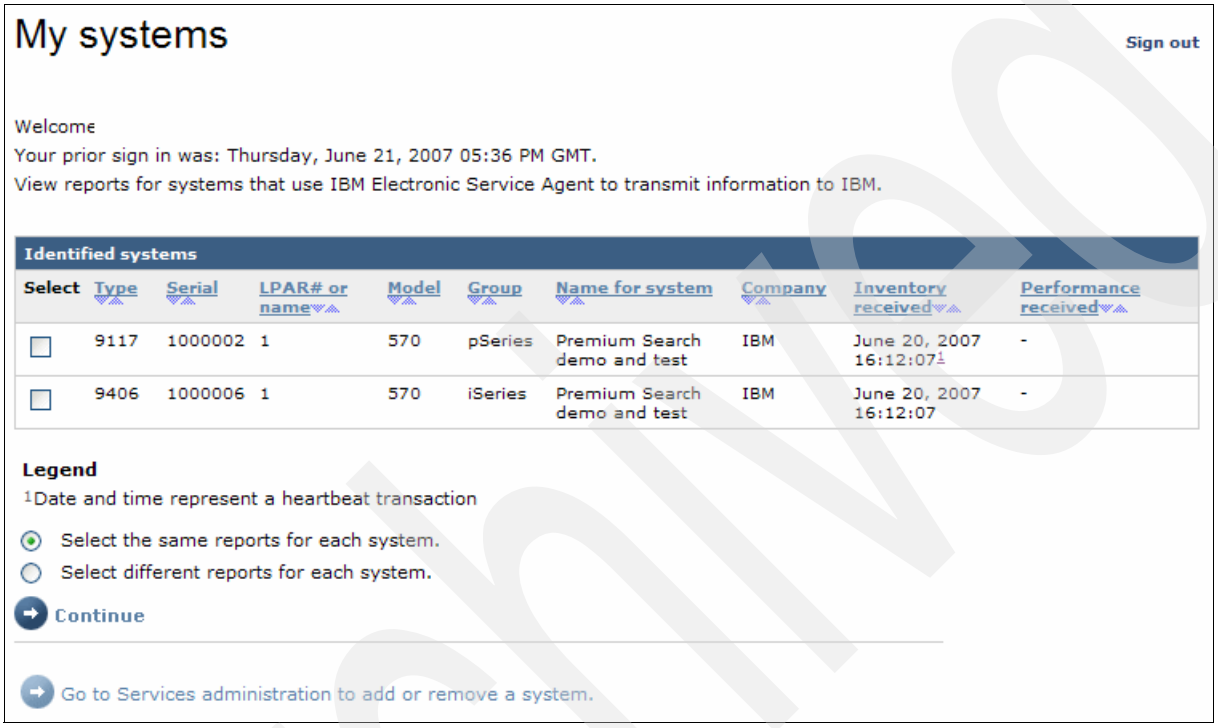


Figure 3-6 Select a system view

After you have selected your system, the report selections reflect the unique system type.

3.5.2 Select reports

Based on the sample systems in Figure 3-6 on page 19, you see sample Select report views. Figure 3-7 identifies the reports that are available for System i platforms.

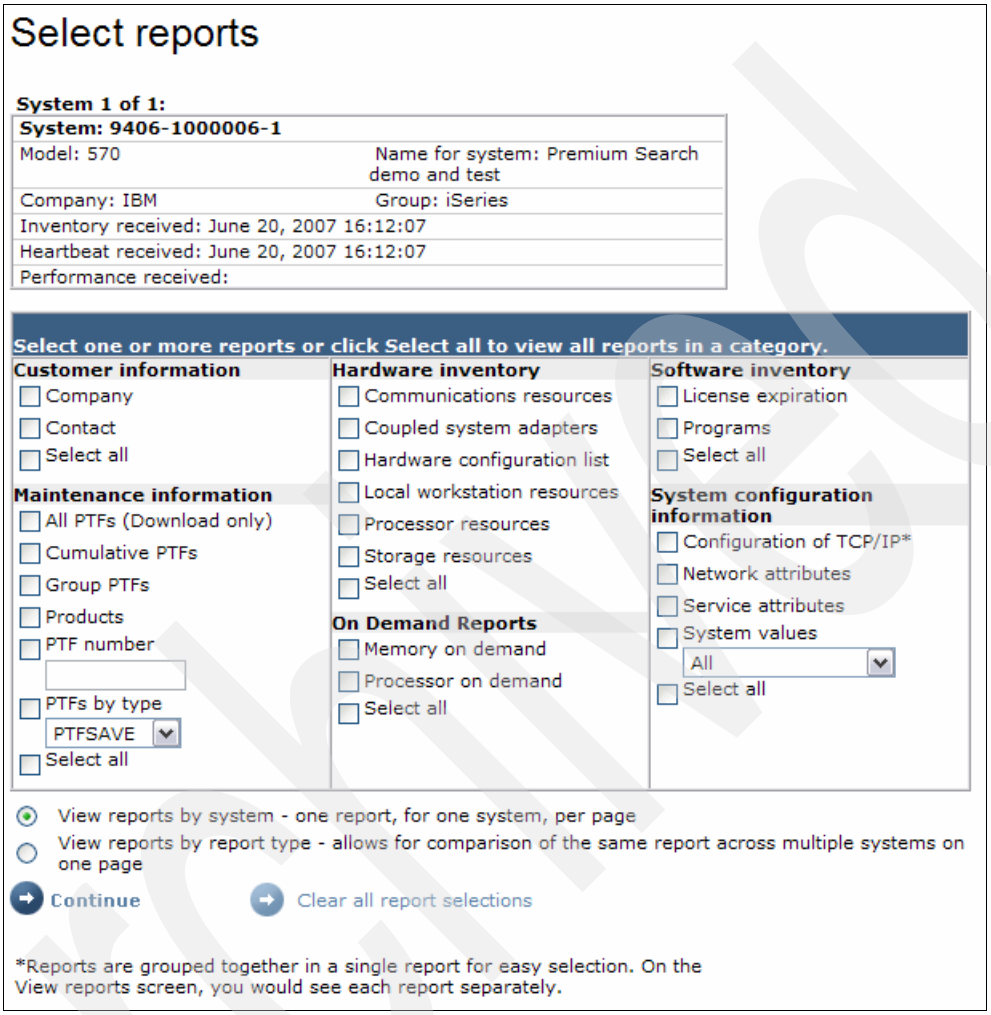


Figure 3-7 Report selection for System i platforms

Figure 3-8 identifies the reports for System p platforms. Note that these systems have reports for stand-alone devices or for those devices in an Hardware Management Console (HMC) environment. Certain reports are environment specific and do not include information if it is inappropriate.

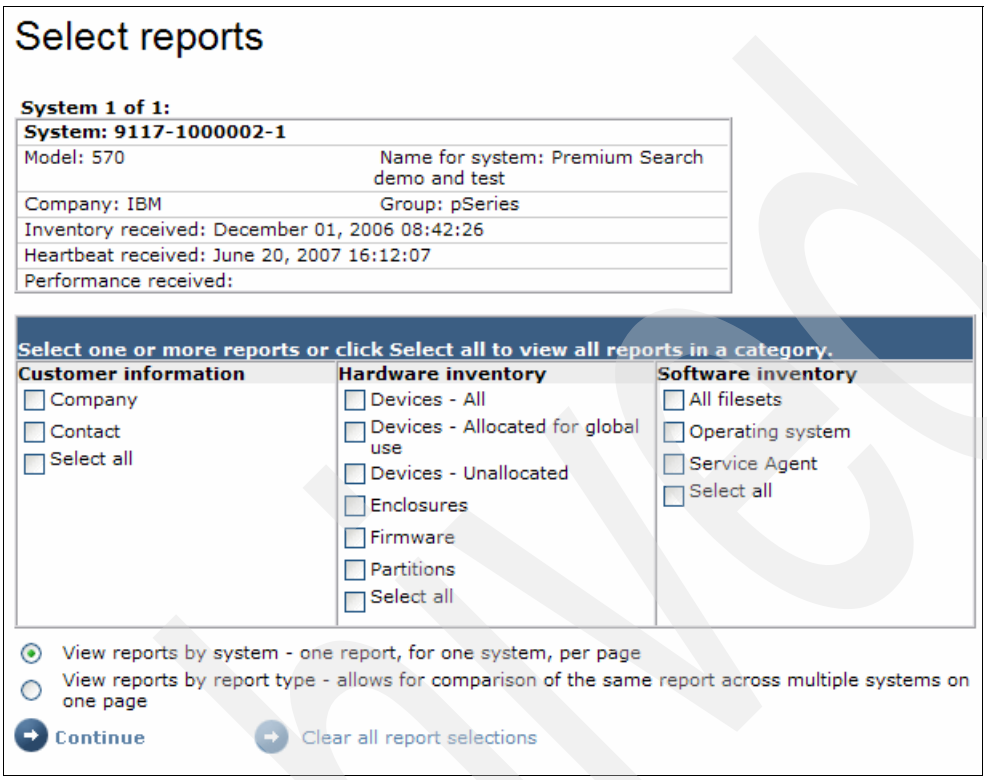
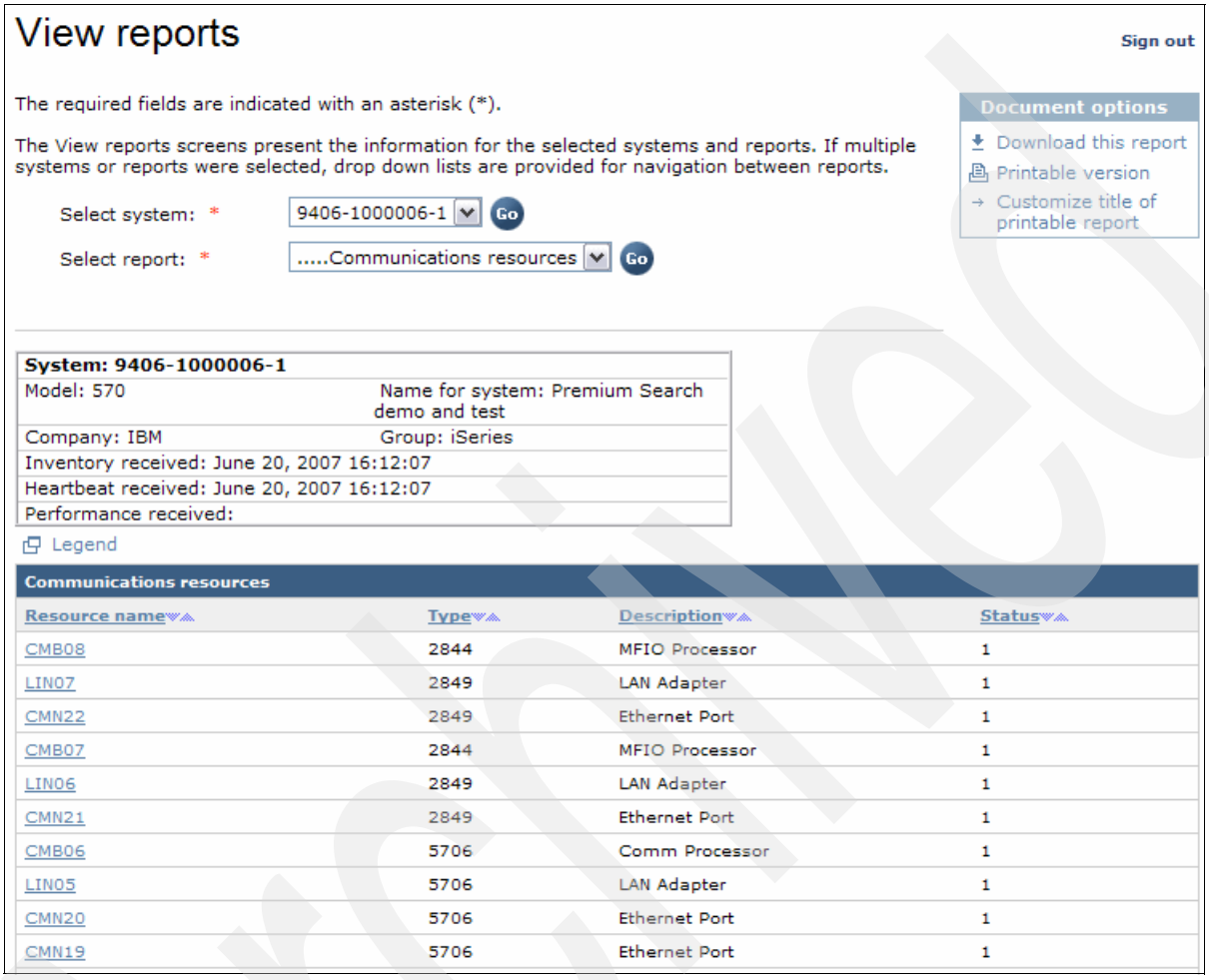


Figure 3-8 Report selection for System p platforms

Figure 3-9 is a sample of the reports. The Communications resources report for System i platforms was selected. You can view this report on the window or select a resource and see another layer of detail. If you prefer, you can download or print the report and get all the detailed information.



View reports

Sign out

The required fields are indicated with an asterisk (*).

The View reports screens present the information for the selected systems and reports. If multiple systems or reports were selected, drop down lists are provided for navigation between reports.

Document options
Download this report
Printable version
Customize title of printable report

Select system: * 9406-1000006-1 Go

Select report: * .....Communications resources Go

System: 9406-1000006-1	
Model: 570	Name for system: Premium Search demo and test
Company: IBM	Group: iSeries
Inventory received: June 20, 2007 16:12:07	
Heartbeat received: June 20, 2007 16:12:07	
Performance received:	

Legend

Communications resources

Resource name	Type	Description	Status
CMB08	2844	MFIO Processor	1
LIN07	2849	LAN Adapter	1
CMN22	2849	Ethernet Port	1
CMB07	2844	MFIO Processor	1
LIN06	2849	LAN Adapter	1
CMN21	2849	Ethernet Port	1
CMB06	5706	Comm Processor	1
LIN05	5706	LAN Adapter	1
CMN20	5706	Ethernet Port	1
CMN19	5706	Ethernet Port	1

Figure 3-9 Communications resources report

Figure 3-10 shows the detail under the first resource: CMB08. You can also print or download this report.

Figure 3-10 Hardware details report for Communications resource: CMB08

3.5.3 My Search using inventory data

My Search combines the function of search and the value of inventory data collected by the Service Agent to provide advanced searching over the technical knowledge base of service and support information. Using My Search and the inventory data, you are able to eliminate search results that do not apply to your system and to include search terms that apply specifically to your system.

The search can:

- Include or exclude certain keywords or phrases
- Specify the operating system release or a product
- Include or exclude installed fixes

The function to exclude all installed fixes eliminates search results that describe fixes that are found on your system. If you are researching a problem that you believe might be a defect that requires a code fix, enter search terms to describe your problem and choose the filter to exclude all installed fixes. The search is designed to show only fixes that apply to your system.

Figure 3-11 shows you the main view of the category. There are sections that you can select to execute a search, go on a tour, experience a demonstration, and read testimonials. The *Execute a Search* section takes you right into the search definition window.

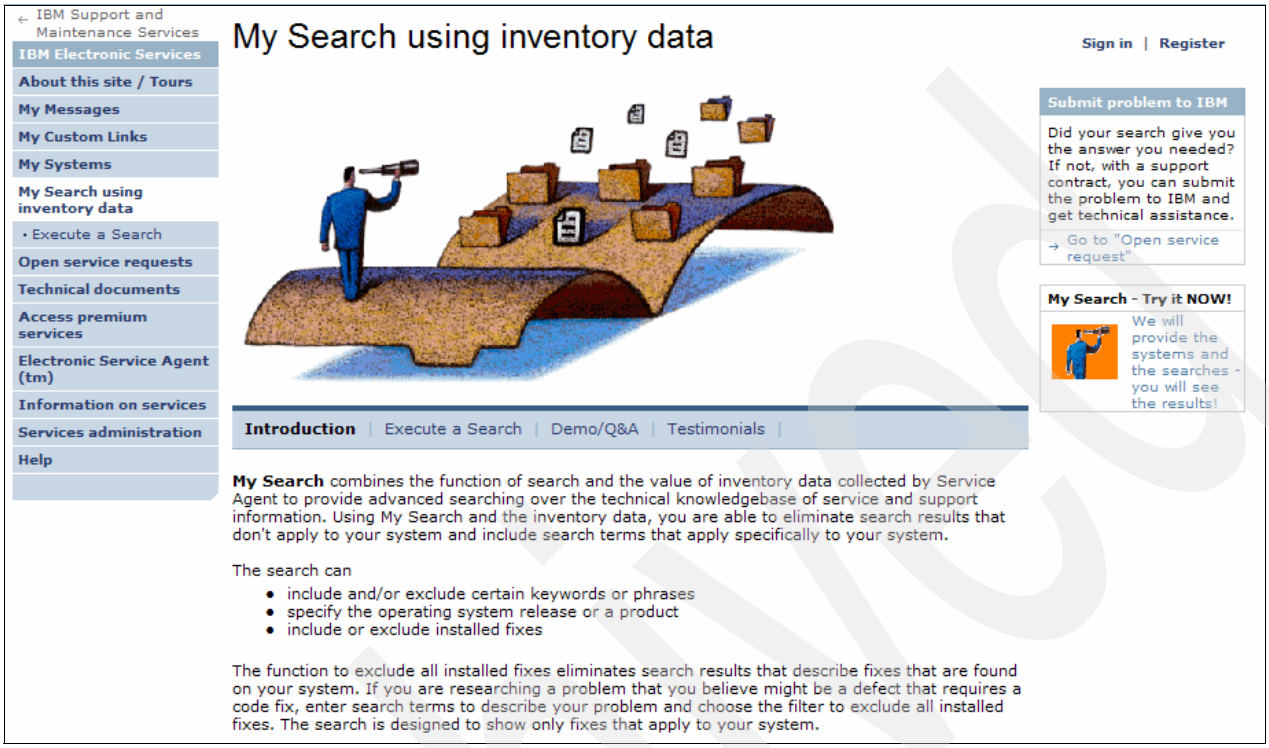


Figure 3-11 My Search main view

IBM recommends that if you do not already have Service Agent activated and associated with your IBM ID that you take advantage of the My Search demonstration experience.

My Search Demo experience

To view the My Search Demo experience:

1. Select either the Demo section or other links that point to the Demo experience.
2. You log in with your IBM ID if you have not already.
3. You see a window that explains that two systems (a System i and a System p) will be associated with the IBM ID. The system information looks familiar, because we used the same systems in the My systems section.

Try your own search keywords and include filters for those systems or select a saved search provided under My saved searches. For each system, one saved search uses no filtering and the other search filters with the inventory data. Notice the difference that it makes to filter the search based on the inventory data. With filtering, the results are often reduced so that you can quickly investigate the situation instead of seeing hundreds of irrelevant results.

Note: These systems are available for My systems, but they are not available for service request submission. When the systems are no longer needed, you can delete them from your profile using Services administration.

Now that you have machines associated to your IBM IDs, try searching.

Figure 3-12 shows our search terms: `java virtual machine`.

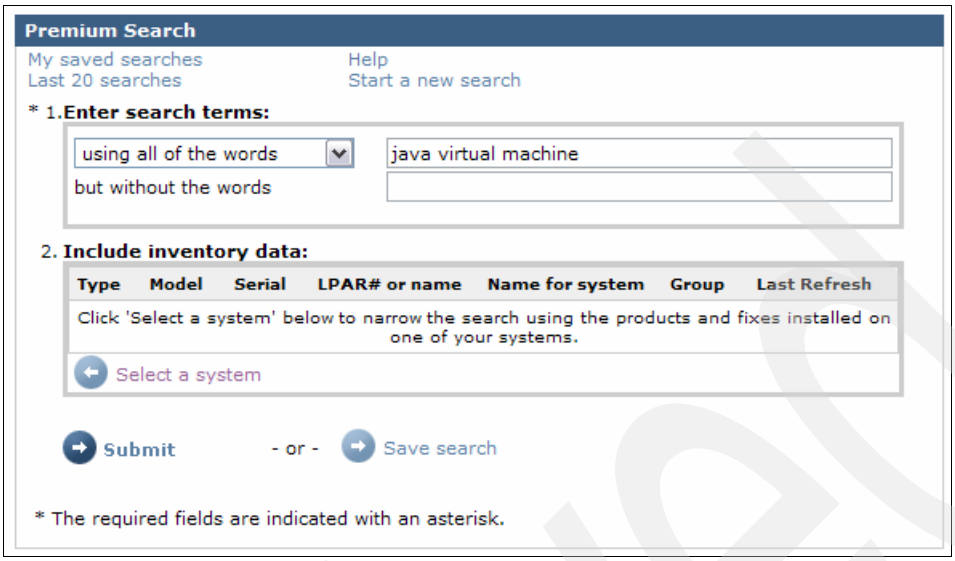


Figure 3-12 Search terms

Next, you select the system, `9406 10-10006`, to filter the results as shown in Figure 3-13.

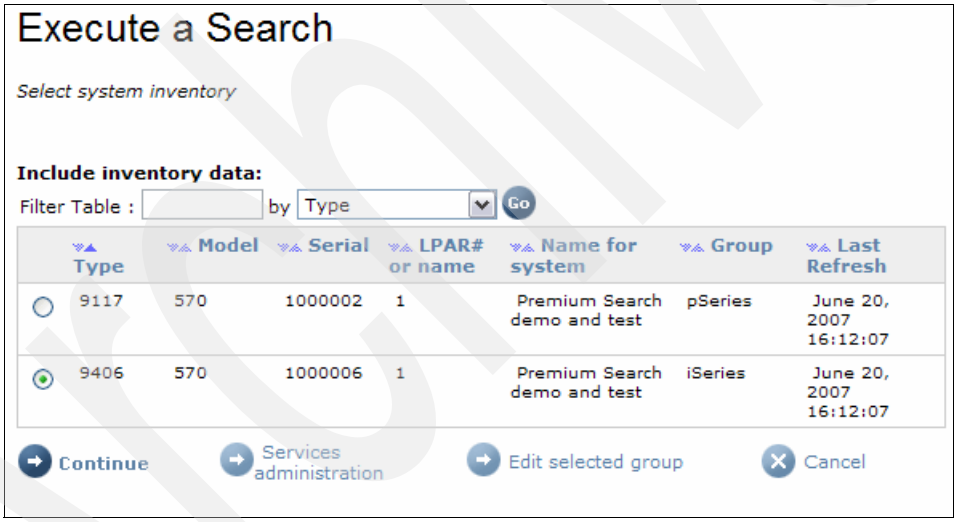


Figure 3-13 Selecting the system to use for the filter

Next, you can select additional filters. The window prefills with the operating system on this system, which is i5/OS® V5R3, as shown in Figure 3-14. You can filter the search by specifying fixes that are on the system, products that are installed, and operating system (OS) type and level. The filters vary by platform.

If you search for a fix to an IBM defect, you can exclude all the fixes that you already have installed, greatly reducing the number of fixes. You can also include a product from the list of products installed on the system. The search includes the component ID or FMID (of the System z platform) for the product selected.

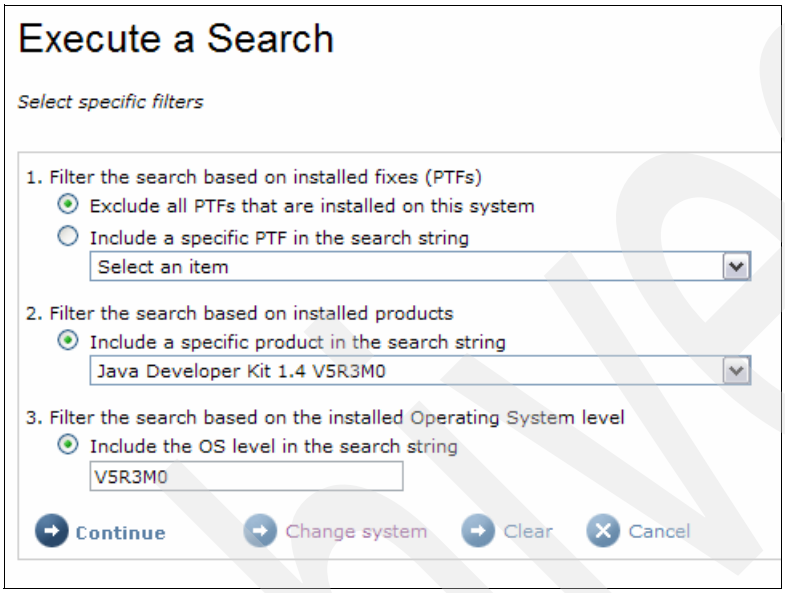


Figure 3-14 Selecting the filters

Figure 3-15 shows how you can confirm all the search factors. You do have an opportunity to adjust the filter selection. When you are ready, click **Submit** to begin the process.

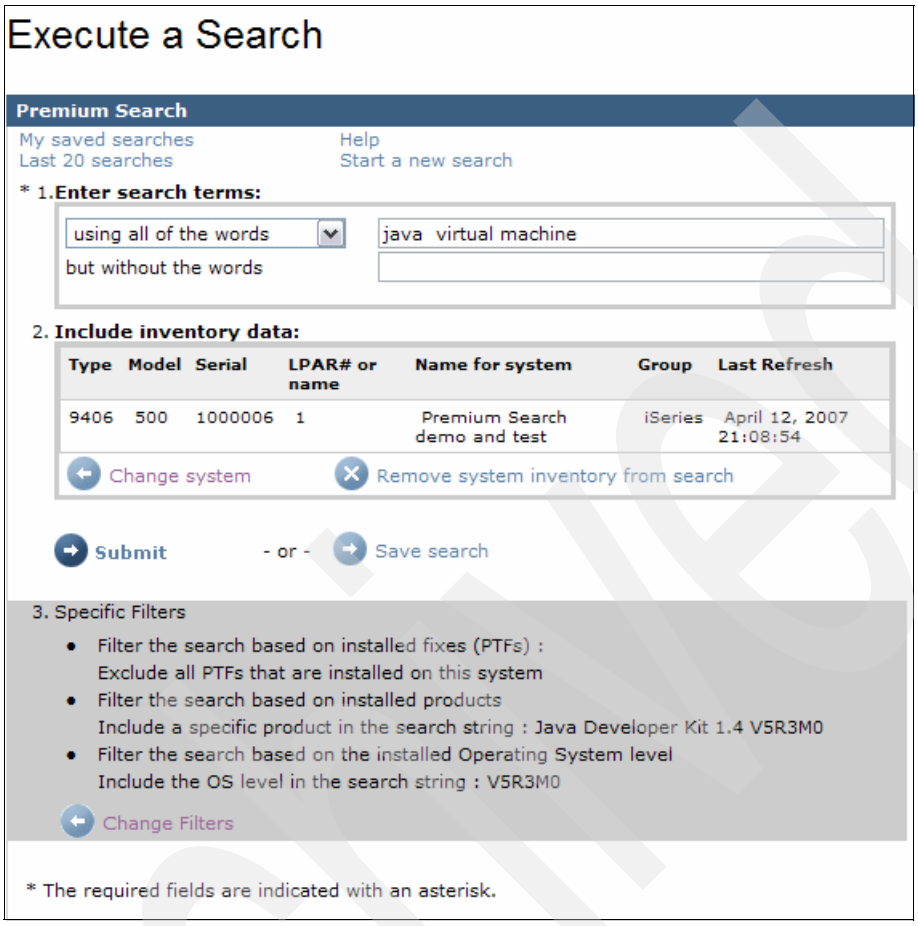


Figure 3-15 Confirming filters

The search engine searches for all relevant results. Figure 3-16 on page 28 and Figure 3-17 on page 29 demonstrate the effectiveness of using Service Agent information in My Search queries. The search text is `java virtual machine` on a 9406.

For comparison purposes, Figure 3-16 shows all the results (no filtering) for the search text `java virtual machine` as 3,578 items.

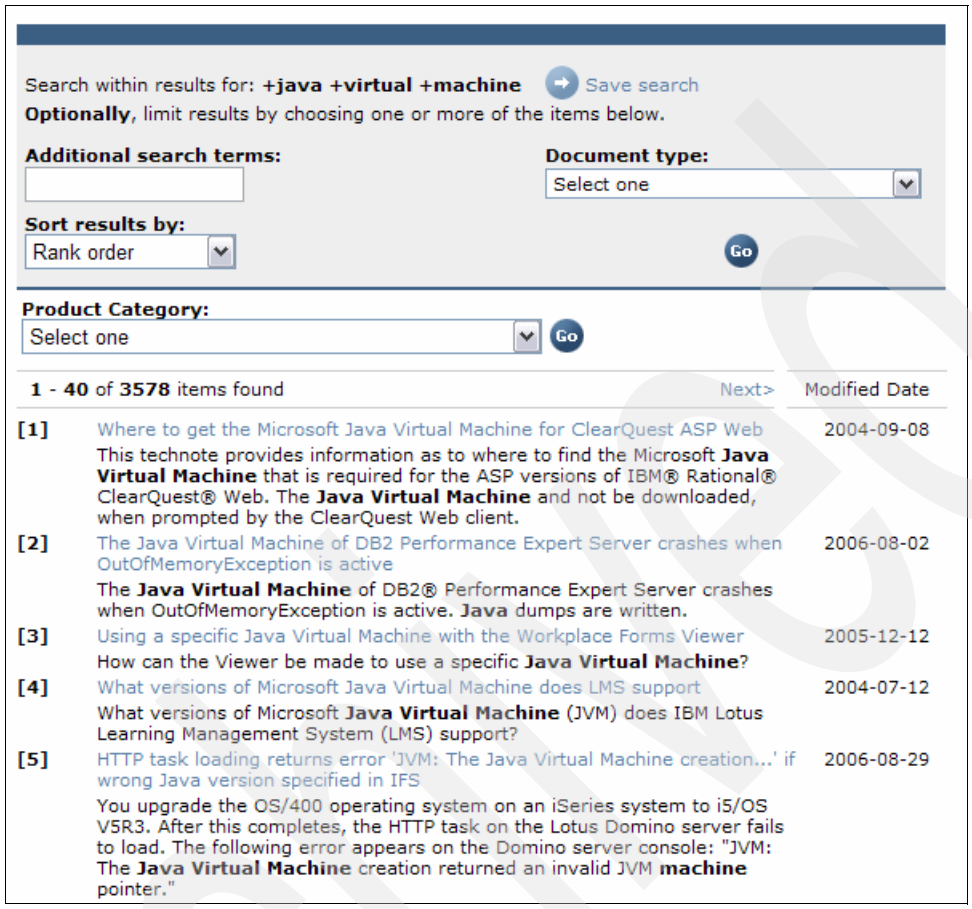


Figure 3-16 Results without providing any filter for the search

Using all the possible filters, system inventory, OS, and product filtering, Figure 3-17 shows the results of the search, four items. Several of the result items are items that have been translated into Japanese text.

Figure 3-17 Results using system information, products, and OS level: Four items

3.6 Open service requests

The *Open a service request* category enables you to submit a hardware or software service request electronically. Each country (region) has a list of selections for both hardware and software. You can submit problems to any of the countries on the drop-down list. The self-guided tours in the *About this site/Tours* category have samples of each type of service request.

Figure 3-18 shows the main page for submitting problems to Australia, from Australia. The first field on this view is to determine which country receives the service request. After the country is selected, the lists for hardware and software are presented for that country. The hardware list is shown in this example.

You are taken to the product submission site or window for details about your request.

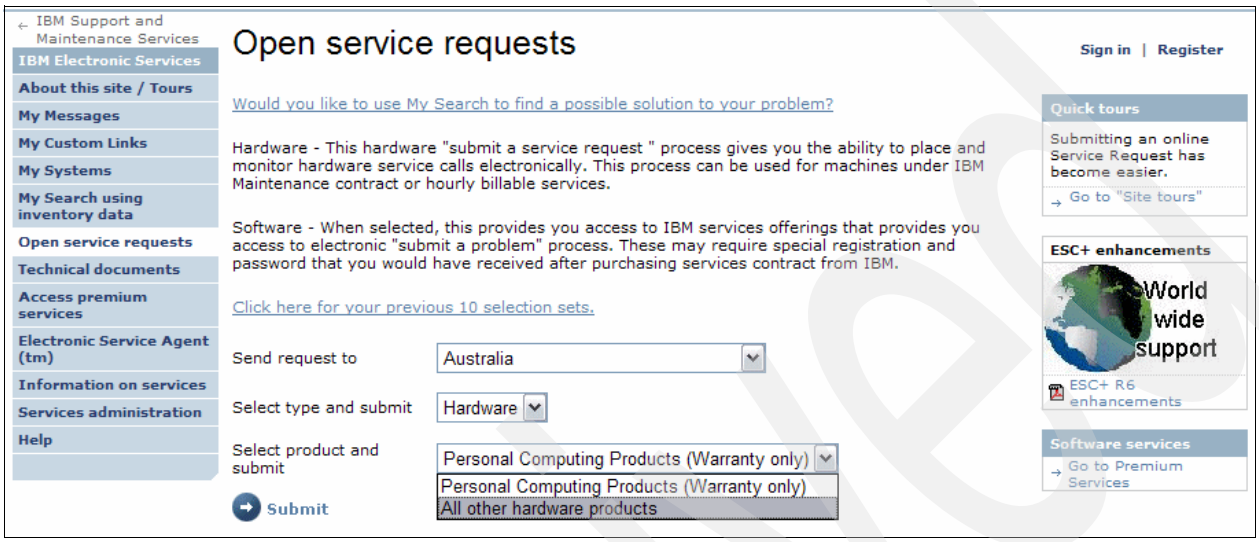


Figure 3-18 Australian view of hardware products

Figure 3-19 on page 31 shows the list of software products.

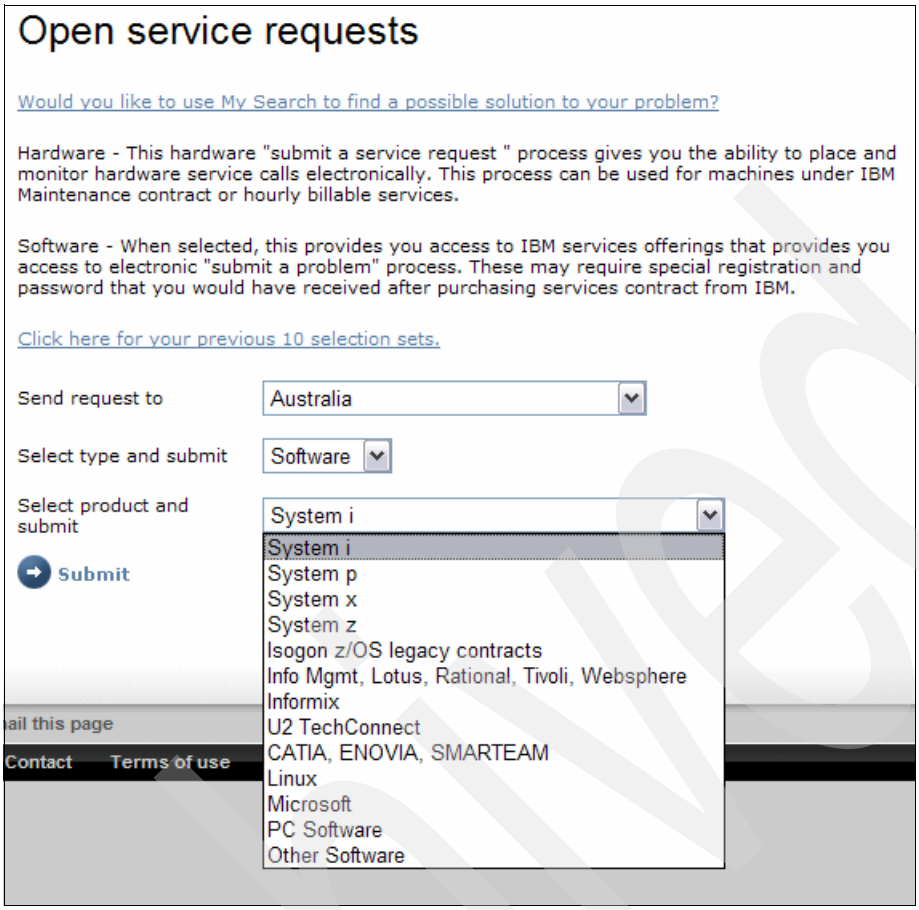


Figure 3-19 Australian software products

3.7 Technical documents

Technical documents is the library of many links within the IBM vast collection of information. Figure 3-20 on page 32 shows the topics that are available for Australia.

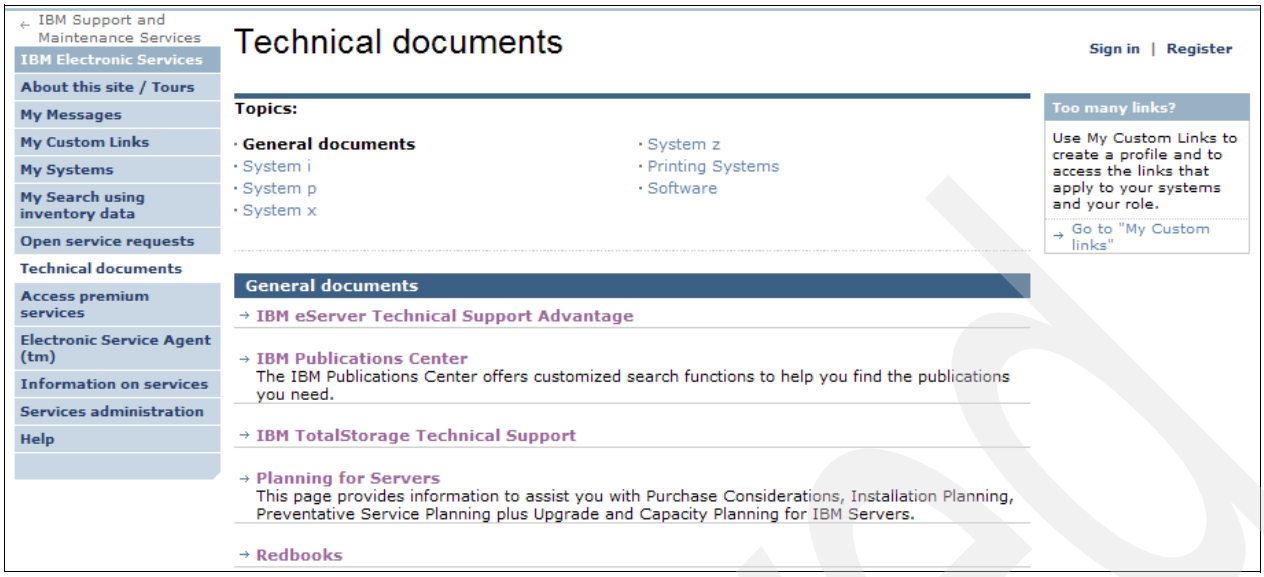


Figure 3-20 Technical documents category

3.8 Access premium services

The *Access premium services* category provides you with the information or links to the many IBM Support and Services offerings in your country. Figure 3-21 shows the non-Web offerings for Australia. Consult your country view of these categories and your account team, because the availability and diversity of offerings vary by country.

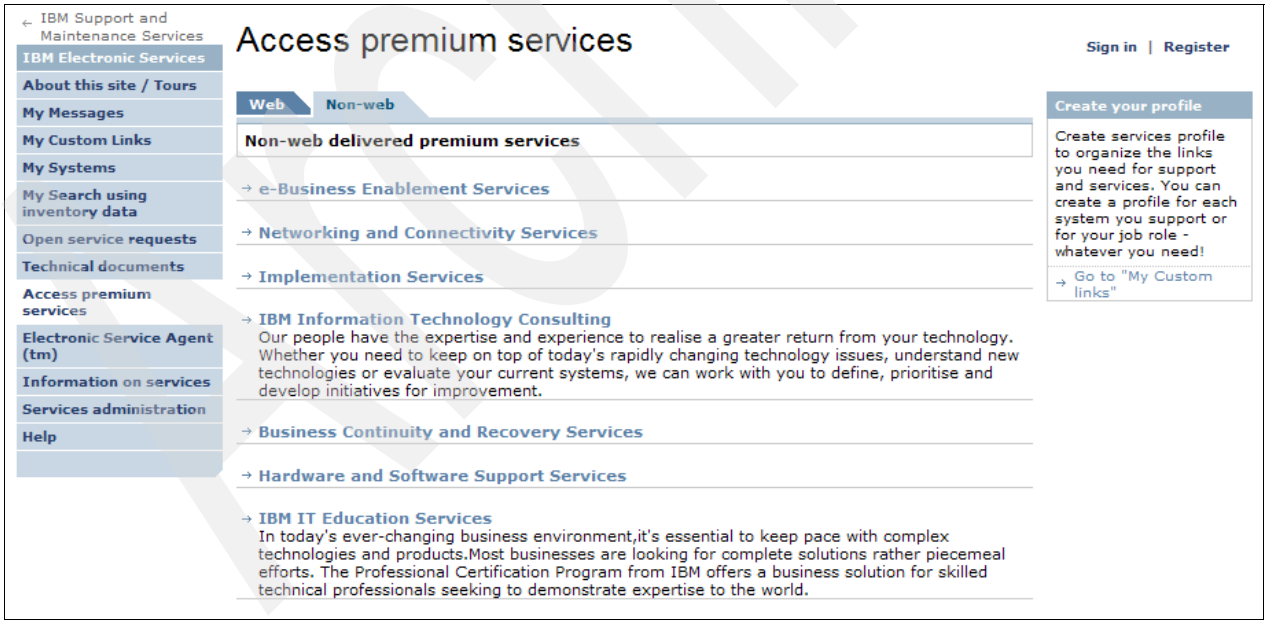


Figure 3-21 Premium Services and information about services

3.9 Electronic Service Agent

The *Electronic Service Agent* category contains all the background information about each of the Electronic Service Agents. There are informational brochures, connectivity guides, security and privacy documents, success stories, actual code to download (if the ESA code is not already shipped with the operating system), user guides, readme files, and tours. Figure 3-22 is the main view of the category.

Figure 3-22 Service Agent category main view

The *Learn about* section has all the high level information that you might want to read about each Service Agent. Figure 3-23 shows the results when you click **Learn about** → **Security Information**.

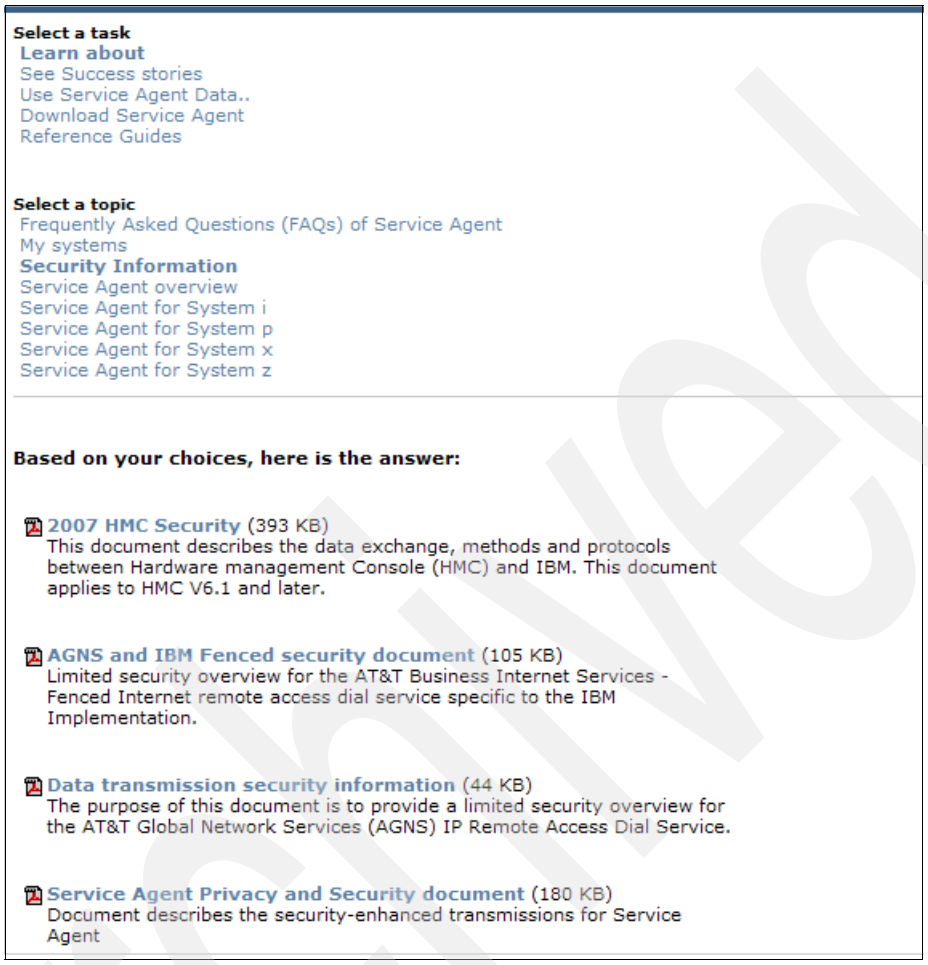


Figure 3-23 Learn about → Security Information topic

See Success stories has short articles from a variety of industries and platforms. Figure 3-24 shows the *General interest* topic.

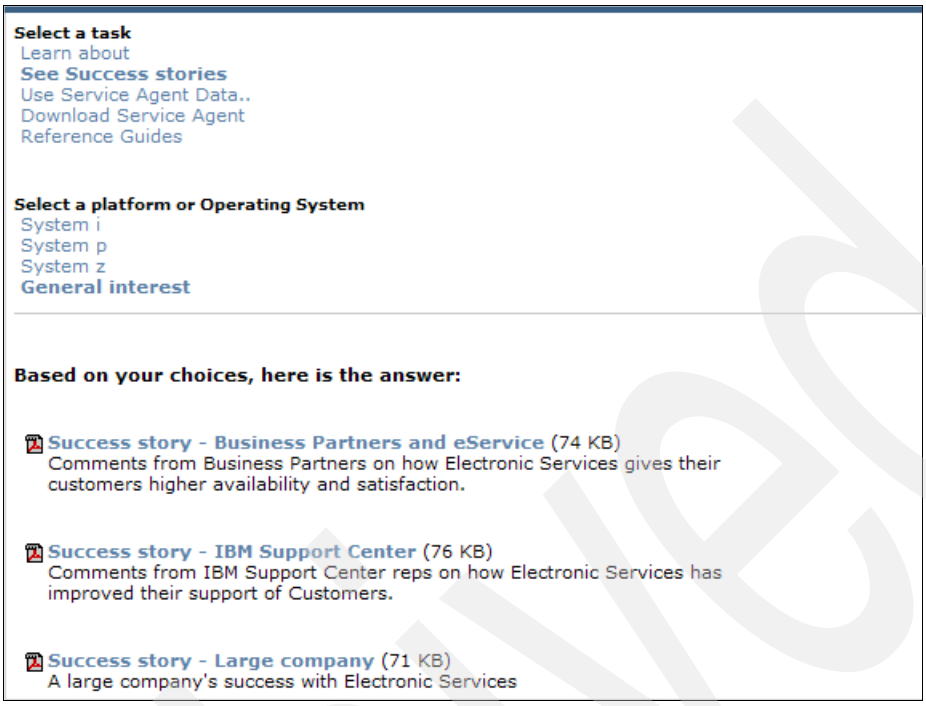


Figure 3-24 See Success stories → General interest

In the *Use Service Agent Data* topic, you see various tools and offerings that are enabled by Service Agent. These include the Electronic Services Web site categories of My Systems and My Search. The ESA inventory information gives this function customized results that are used for improving your operations and system performance. Figure 3-25 shows the listings under **Use Service Agent Data** → **Performance Mgmt**.

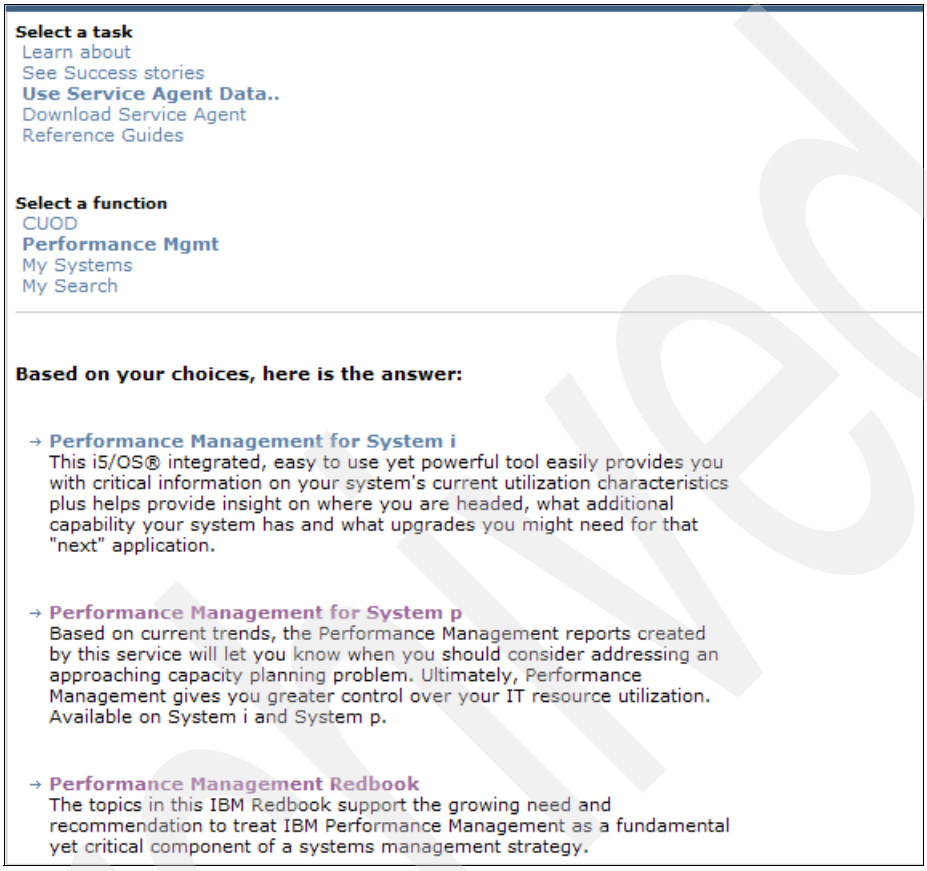


Figure 3-25 Use Service Agent Data → Performance Mgmt

The *Download Service Agent* topic shows you by platform where to find the ESA code, either with the operating system package or available from download from the Web. In Figure 3-26, the topic is open to the System x platform and Standalone - Linux. The download package zip file contains the ESA code, user guide, readme file, and response file.

Figure 3-26 Download System x and Linux

The *Reference Guides* topic includes many ESA User Guides, as well as related ESA documents. Drilling down into the System x for Linux download package, Figure 3-27 shows the Reference Guides listed under that same platform and OS.

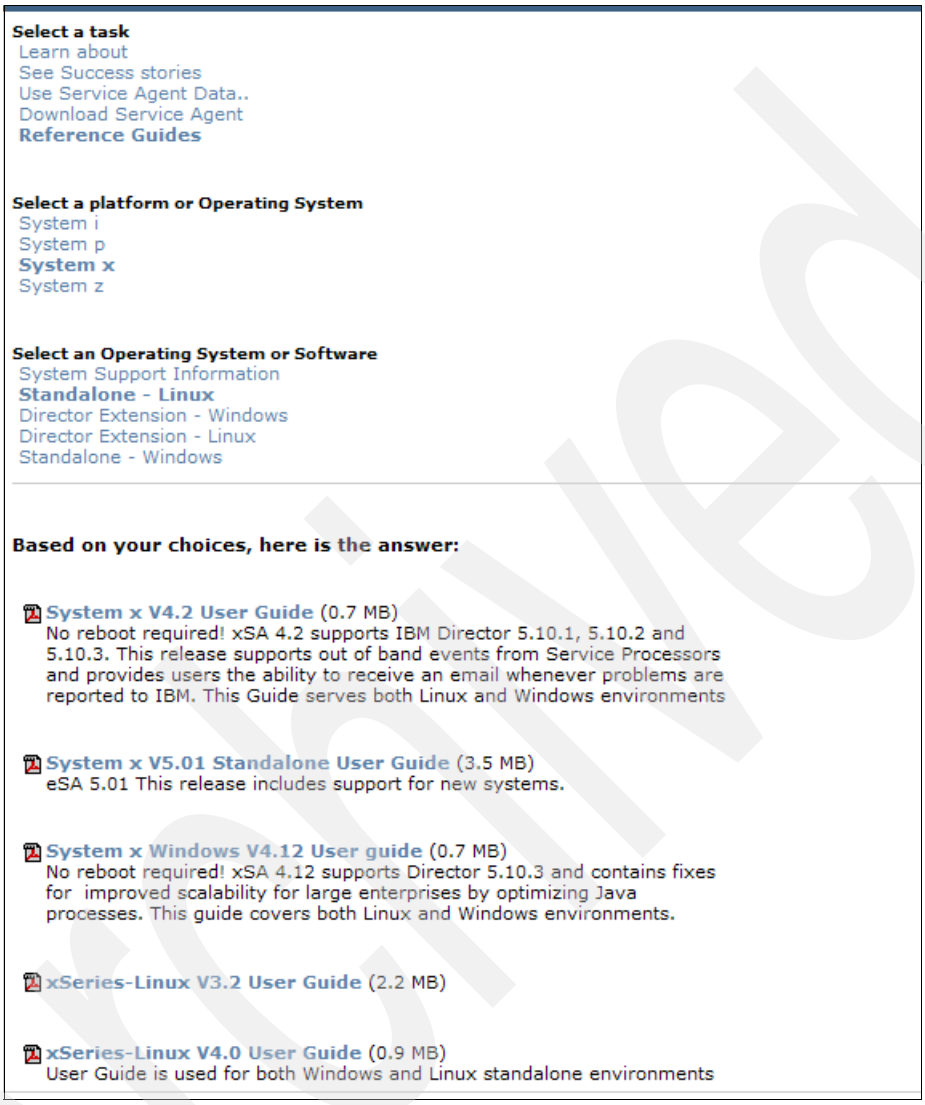


Figure 3-27 Reference guides for System x and Standalone - Linux

3.10 Services administration

The *Services administration* category enables you to do any administrative tasks related to the Electronic Services Web site, as either a user or an administrator. You can link to this area when in My Search or in My systems and:

- Add new Customer numbers that relate to new contract coverage.
- Request new systems that have activated ESA in order to add them to your IBM ID.
- Remove systems from your IBM ID.
- Perform administrator tasks if you are an ESA Administrator for a system.

Figure 3-28 on page 39 shows the main view if you are a user, not an administrator.

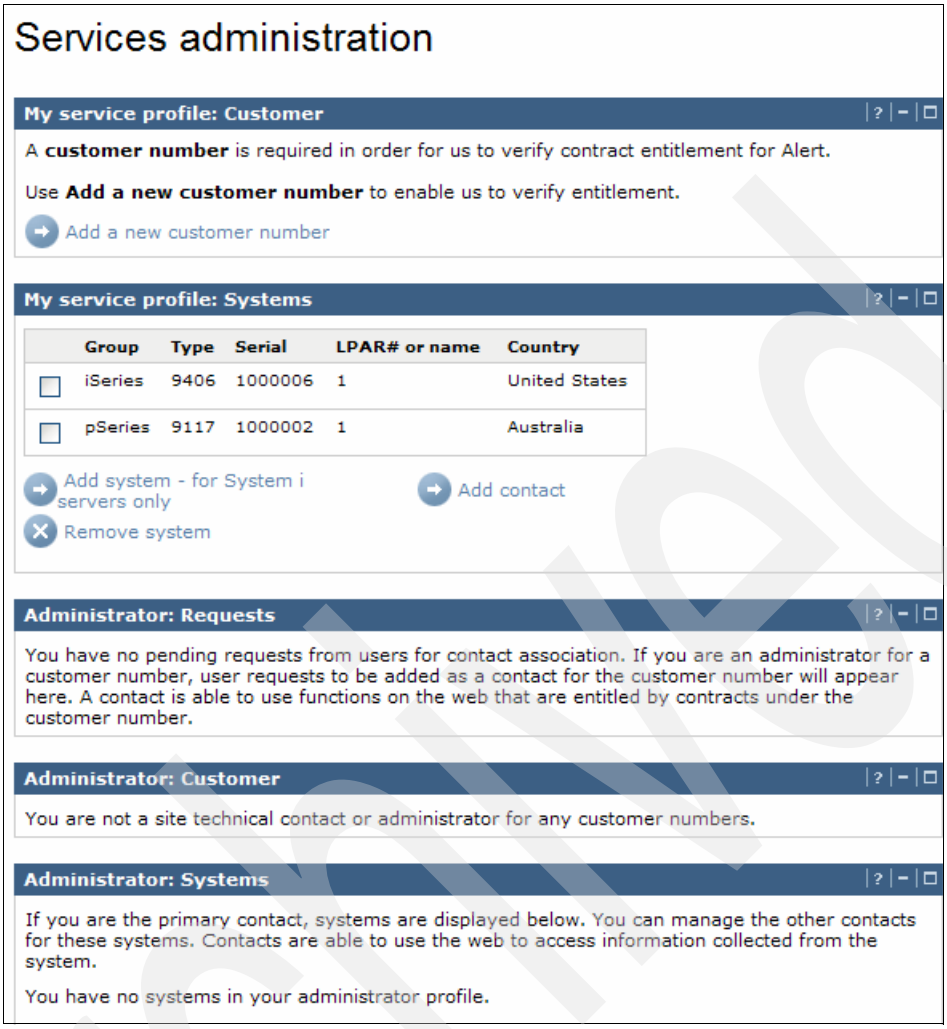


Figure 3-28 Services administration: User view

In **My service profile: Customer**, the person who is the primary contact can add the customer number to this section. You must be the person listed in the IBM contract as the primary contact. This person can also authorize other users to be contacts for the customer number.

In the **My service profile: Systems** portion of the view, you can add new IBM IDs to use and view your list of systems. You can select one or several systems to add to an IBM ID. Figure 3-29 shows the window after you have selected the machines to add to an IBM ID. After you have added the IBM ID and click **Submit**, you get a success or fail message based on a valid IBM ID.

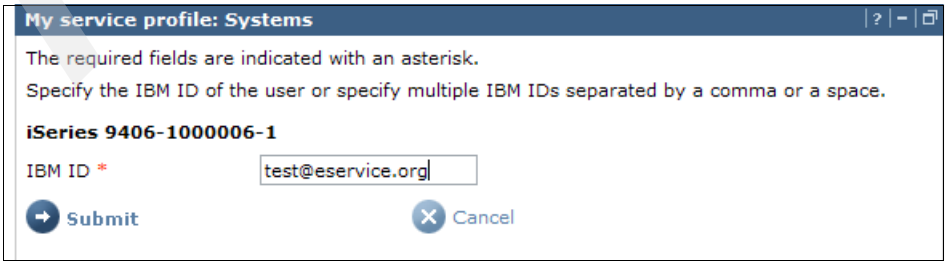


Figure 3-29 Services administration: Add a contact

4

IBM Electronic Service Agent

IBM Electronic Service Agent supports several functions. This chapter highlights these functions and describes the current environments in which you can use them. Detailed information for each platform is described later in this book.

4.1 Electronic Service Agent overview

The first product in the Service Agent family, Service Director™ SubSystem (Service Director or SDSS), was introduced in 1987. It monitored direct access storage device (DASD) input/output (I/O) attached to a S/390® platform. Over the years, the scope of platform coverage now works with or is integrated into five operating systems. IBM clients in over 64 countries (regions) can activate Electronic Service Agent.

The following list outlines the current Electronic Service Agents. Because there are periodic updates on each platform, refer to the Service Agent User Guide for the latest listing of machine types and operating system coverage:

- Electronic Service Agent for System i
- Electronic Service Agent for System p
- Electronic Service Agent for Linux on System p
- Electronic Service Agent for System x
- Electronic Service Agent for Linux on System x
- Electronic Service Agent for System z

Figure 4-1 shows how the Service Director span of functions has evolved into the current Service Agent functions.

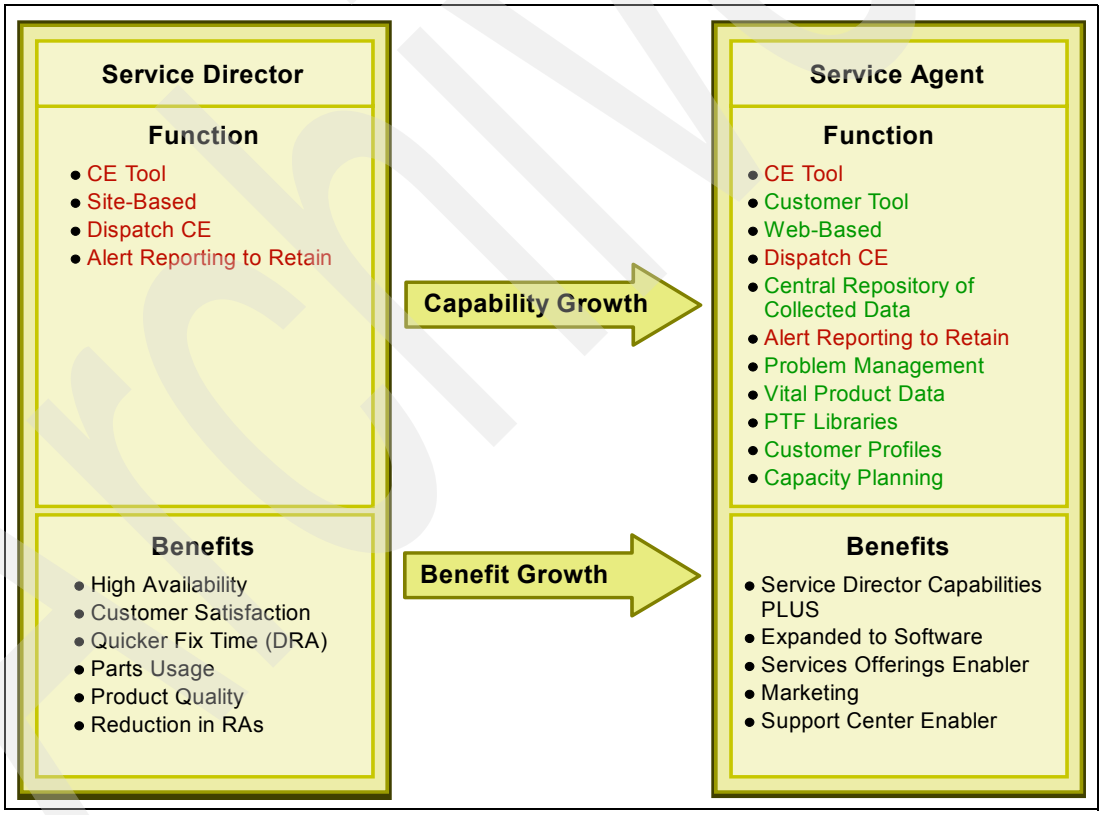


Figure 4-1 Service Director growth into Service Agent

4.2 Environments

Service Agent is available on each IBM system product line for stand-alone and network environments. The secure communication options range from modems to the Internet. Figure 4-2 provides an example of a stand-alone environment.

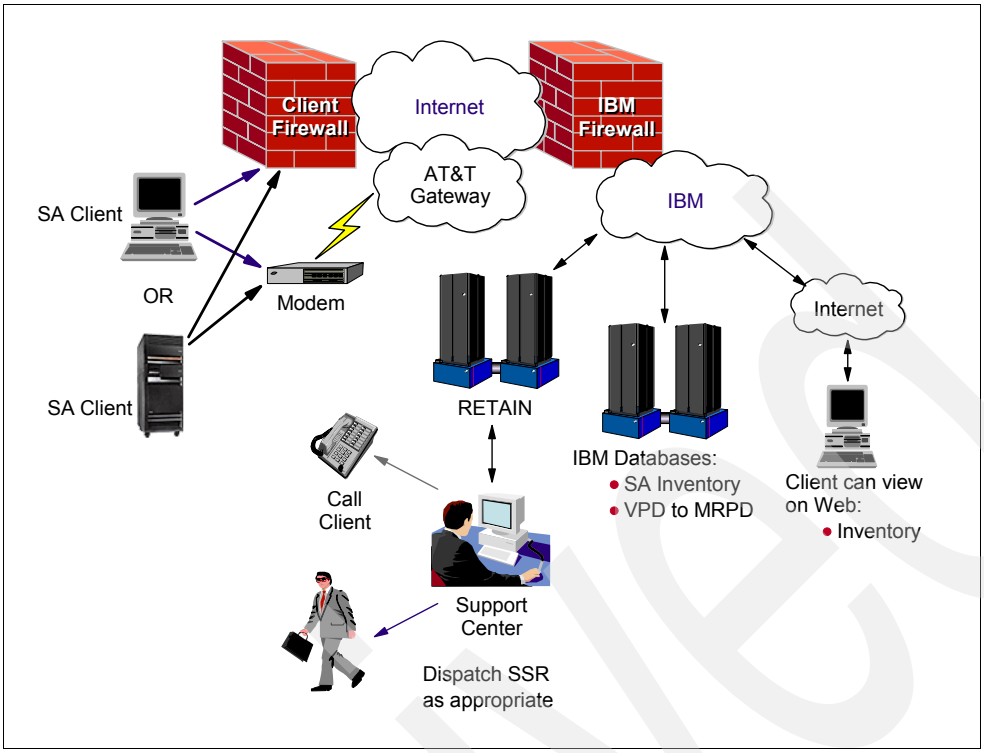


Figure 4-2 Generic stand-alone network

Figure 4-3 shows an example of a network environment. In this environment, Service Agent flows inside complex networks and helps to manage the complexity with automatic hardware problem submission and inventory collection.

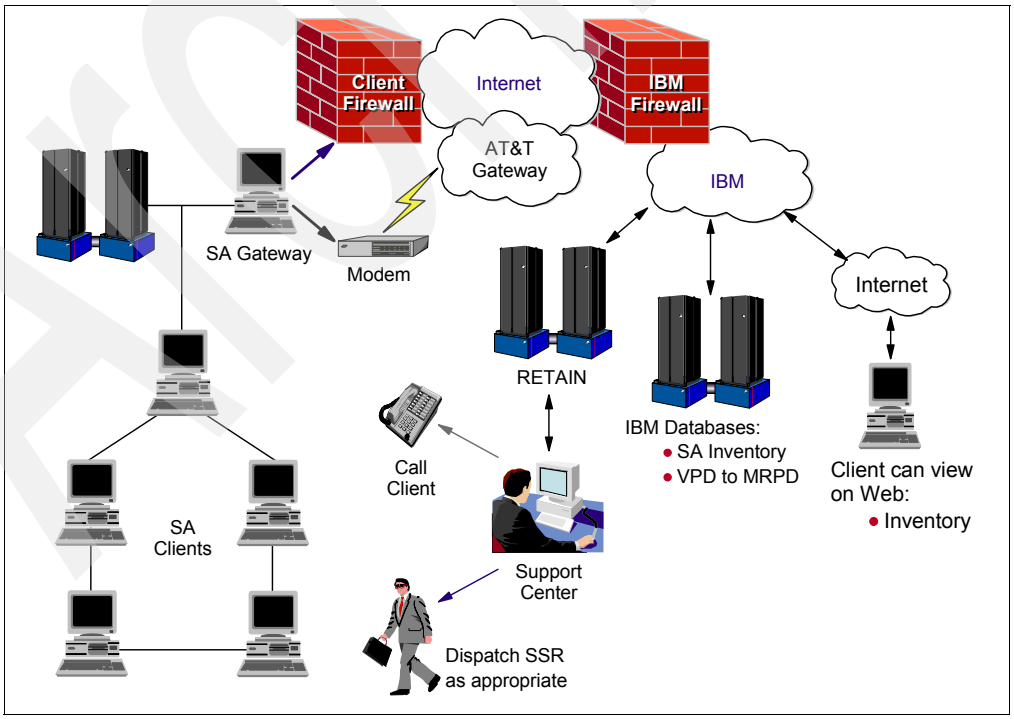


Figure 4-3 Generic complex network

4.3 Where to install and activate IBM Electronic Service Agent

IBM Electronic Service Agent can run on a variety of operating systems and system platforms:

- i5/OS
- AIX®
- Linux on System p, System i, or System x
- Windows® on System x
- Hardware Management Console (HMC)
- z/OS®

For any system platform, there can be one or more operating systems. No matter which system platform you have, how many partitions are configured, or which operating systems are running, IBM Electronic Service Agent must be installed and activated on each partition, operating system, and HMC.

4.3.1 Functions by operating system

To have total coverage, IBM Electronic Service Agent needs to be running on every system, every partition, and on every HMC. The functions provided by IBM Electronic Service Agent vary based on the environment, including the network. For example, if your system is running two partitions of AIX and two partitions of i5/OS, the HMC reports platform errors for the system and partition errors for the AIX partitions. IBM Electronic Service Agent on each i5/OS partition reports partition errors for the partition on which it is running. To have total coverage (for this example), IBM Electronic Service Agent needs to be running on the HMC, each i5/OS partition, and each AIX partition.

Table 4-1 shows the functions provided by the various Service Agents (SAs) based on platform and system configuration.

Table 4-1 Service Agents by platform and OS

Operating System	Report platform errors	Report partition errors	Report service information	Automatic fix download
i5/OS stand-alone	SA on i5/OS	N/A	Yes	Yes
i5/OS partition with an HMC	SA on the HMC	SA on i5/OS	Yes	Yes
AIX stand-alone	SA on AIX	N/A	Yes	No
AIX partition with an HMC	SA on the HMC	SA on the HMC	Yes	No
Linux stand-alone (Power)	SA on Linux	N/A	Yes	No
Linux partition with an HMC (Power)	SA on the HMC	SA on the HMC	Yes	No
HMC	Reports errors for itself and reports all platform errors	Reports partition errors for AIX and Linux platforms	Yes	No

Operating System	Report platform errors	Report partition errors	Report service information	Automatic fix download
Windows stand-alone	SA on Windows	N/A	Yes	No
Windows Director Extension	SA on Windows	N/A	Yes	No
Linux stand-alone (X86)	SA on Linux	N/A	Yes	No
Linux Director Extension (X86)	SA on Linux	N/A	Yes	No
z/OS	Handled by the z/OS HMC	N/A	Yes	Yes
Storage: DS8000™	SA on Storage	N/A	Yes	No
n series	Reported by n series call home (Auto support)	N/A	Yes	N/A

4.3.2 Service information

The following figures show the service information collected and sent to IBM by various Service Agents based on the operating system or the system. These figures show that a partition is controlled by an HMC, and the HMC is connected to it.

Table 4-2 shows the service information collected and sent to IBM by the various Service Agents for the System i platforms.

Table 4-2 System i or i5/OS service information

Operating system	Hardware information	Software information	Other information
Service Agent for i5/OS (stand-alone or partition)	► Hardware resources ► IPL type ► Disk details ► ASP ► Consolidated hardware information ► System configuration ► Vital product data (VPD)	► Software resources ► Software license ► Software license usage information ► Fixes ► Fix groups	► Service attributes ► Network attributes ► TCP/IP domain information ► TCP/IP status: IPv4 and IPv6 ► TCP/IP attributes: IPv4 and IPv6 ► TCP/IP network interface: IPv4 and IPv6 ► TCP/IP network routes: IPv4 and IPv6 ► TCP/IP Point-to-Point Protocol (PPP) setting ► System register

Table 4-3 shows the service information collected and sent to IBM by the various Service Agents based on the System p platform, AIX, or Linux operating system.

Table 4-3 Service information for System p platform, AIX, or Linux

Operating System	Hardware information	Software information	Other information
Service Agent for AIX stand-alone	► Hardware information ► Vital product data (VPD) ► Workload Manager information (WLM)	► Installed software ► Fixes	► PM AIX data ► SNAP data ► File system information ► Printer information ► System network information ► TCP/IP information
Service Agent for AIX partition	N/A	► Installed software ► Fixes	N/A
Service Agent for Linux stand-alone (Power)	► Hardware information ► Vital product data (VPD)	► Installed software ► Fixes	► PM AIX data ► SNAP data ► File system information ► Printer information ► System network information ► TCP/IP information
Service Agent for Linux - partition (Power)	N/A	► Installed software ► Fixes	N/A

Table 4-4 shows the service information collected and sent to IBM by the various Service Agents based on System i or System p platform's use of HMC.

Table 4-4 Service information based on System i platform's or System p platform's use of HMC

Operating System	Hardware information	Software information	Other information
HMC	► Complete information for each partition, including unallocated hardware ► Hardware and other information for AIX and Linux (Power) partitions	Information about itself, AIX, and Linux (Power) partitions	N/A

Table 4-5 shows the service information collected and sent to IBM by the various Service Agents based on the System x platform and Windows or Linux operating system.

Table 4-5 Service information for System x for Windows and Linux

Operating System	Hardware information	Software information	Other information
Service Agent for Windows (stand-alone or Director Extension)	► BIOS ► Processor ► Memory ► Hard drives ► ServeRaid drives ► Power ► Service processor and PCI adapters	► Device drivers ► Installed programs	► Machine location ► Company information ► Contact details
Service Agent for Linux (stand-alone or Director Extension X86)	► BIOS ► Processor ► Memory ► Hard drives ► ServeRaid drives ► Power ► Service processor and PCI adapters	► Installed packages ► Patches	► Machine location ► Company information ► Contact details

Table 4-6 shows the service information collected and sent to IBM by the various Service Agents based on the System z platform or z/OS operating system.

Table 4-6 Service information for System z or z/OS

Operating System	Hardware information	Software information	Other information
Service Agent for z/OS	► Selected I/O hardware failures ► I/O statistical data ► Tape media maintenance	► Installed software ► Fixes	► Contact information ► System registration

4.4 Privacy and security of your information

For details about the privacy and security of your information, refer to the document, *Transmission Security Information Inventory Information Privacy*, from the following Web site:

`https://www.ibm.com/support/electronic`

This document provides a high-level view of the security features during the Electronic Service Agent inventory transmission between a client system and the IBM infrastructure. It also provides a brief description of inventory information. The following sections highlight key information from this document.

4.4.1 Privacy

The service information that is gathered from client systems is typically collected by speaking with clients during phone calls with the IBM Support Center, pre-sales specialists, administrative clerks, and other groups within IBM. These IBM groups have electronic access to the information so that they can prepare, perform advance problem determination, and more efficiently serve IBM clients.

Note: In certain IBM organizations, the representatives are not full-time IBM employees, or they might be vendors who work under IBM direction and contract. These staff members are subject to same privacy and security guidelines as any IBM employee.

The inventory information includes:

- Your support contact information, including names, phone numbers, and e-mail addresses
- System utilization, performance, system failure logs, part feature codes, part number, part serial number, part locations, software inventory, operating system applications, program temporary fixes (PTFs), the maintenance level, and configuration values

Using platform-specific commands, authorized IBM employees can view all inventory information about the system.

Inventory information does not include:

- Collection or transmission of any of your company's financial, statistical, or personnel data
- Client information
- Your business plans

In addition, Service Agent can provide a *call home* mechanism for other IBM offerings that you might select in the future. The information collected by these offerings is covered in separate agreements, for example, the Performance Management and Capacity Upgrade on Demand offerings.

4.4.2 Transmission security

Electronic Service Agent has the ability to collect service information and transmit it to IBM on a scheduled basis:

- All Service Agent transactions are outbound requests secured by encryption (Hypertext Transfer Protocol Secure (HTTPS) or POST).
- Service Agent has *no* inbound capability. Service Agent client code cannot accept incoming connection attempts. For example, the Service Agent client initiates a connection with IBM, similar to a Web browser, and then IBM replies. However, IBM never initiates a connection to a client environment.

During the activation and setup of Electronic Service Agent, the client can select to transmit this information either through the Internet or the AT&T Global Network Services (AGNS) phone connection. The Service Agent code has the appropriate information to use for either communication method. Both of these transmission paths use Secure Sockets Layer (SSL) and TCP/IP protocols. Service Agent uses the client's connectivity environment, including any firewalls that the client has established.

Figure 4-4 shows a summary of the connection into IBM. The nature of maintaining a high-level security posture dictates that IBM and AGNS do not divulge in-depth details regarding the management of security: tools, processes, and audits.

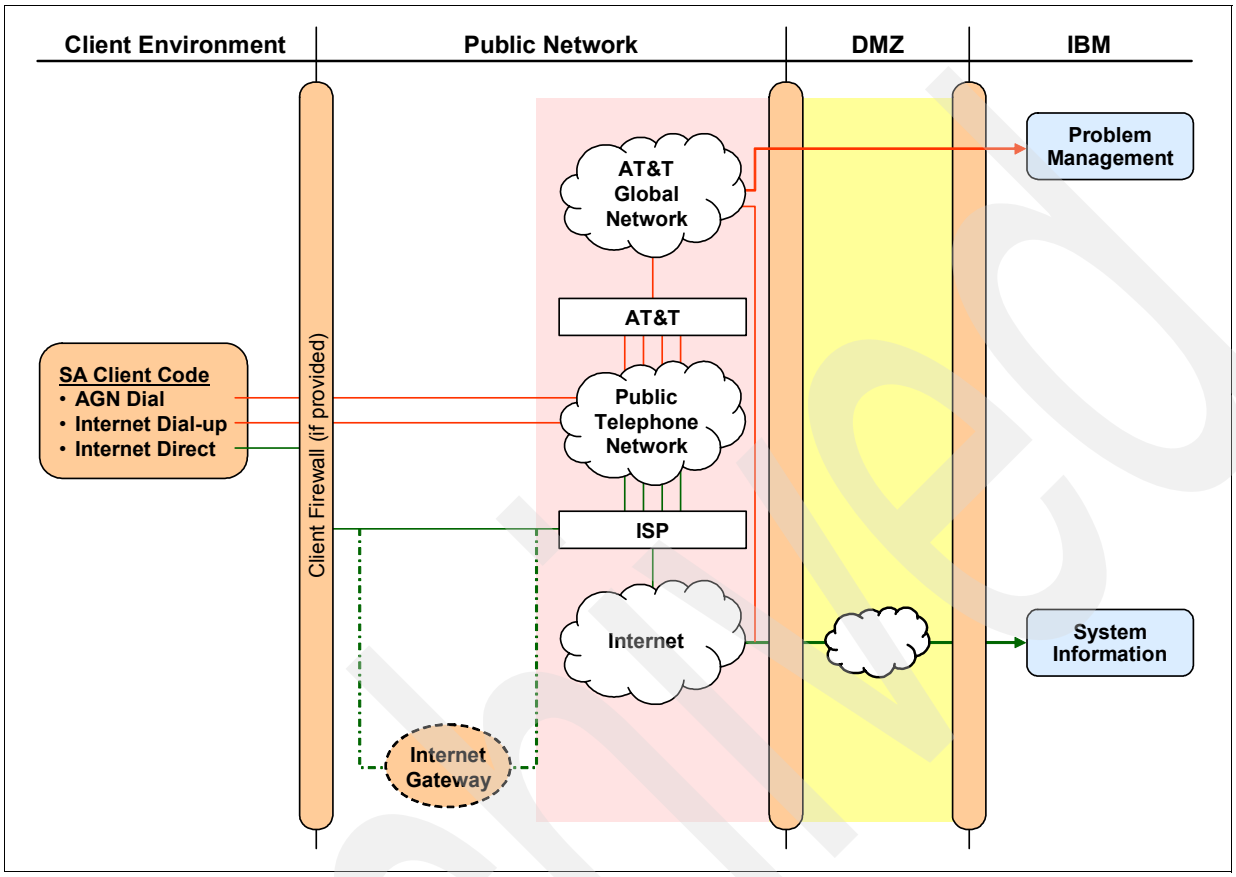


Figure 4-4 Service Agent transaction environment

Internet

Note: The Internet provider relationship and connection are the responsibility of the client.

For the authentication of transmission, system IDs and passwords are generated for the client system every six months by the server using an algorithm. The passwords are not visible to the user. A user can request that a new password is generated, if deemed necessary.

If you select the Internet path to send your Service Agent service information, the following process applies:

1. Service Agent collects the information to be transmitted and queues for transmission at the scheduled time.
2. At the appropriate time, you establish an Internet connection using system IDs and passwords that were created previously.
3. An SSL connection is established between your system and IBM.
4. Service Agent inventory information flows to the IBM destination (predetermined by the Service Agent code).
5. Upon arrival at IBM, the inventory is transferred to the appropriate IBM database.

Telephone AT&T Global Network Service transmission

You can use the AGNS TCP/IP Remote Access Service (Secure IP) as a limited use network service provider. This is a point-to-point dial connection, which has a specific IBM account with AGNS. The information is encrypted prior to entering the AT&T network. No party on the AT&T network can decrypt the information. The information is decrypted only inside IBM firewalls by the appropriate application.

AT&T provides a document that describes their communication process with Service Agent. Refer to the document, *Transmission Security Information Inventory Information Privacy*, from the following Web site:

`https://ibm.com/support/electronic`

If you select the AGNS path for your Service Agent service information, the following process applies:

1. You have a modem connected to your system.
2. Service Agent collects the information to be transmitted and queues for transmission at the appropriate time.
3. The system dials the AGNS Local Interface Gateway (LIG) at the appropriate time and establishes a connection using an AGNS ID and password.
4. An SSL connection is established with IBM through the AGNS LIG.
5. Service Agent inventory information flows to the IBM destination (predetermined by the Service Agent code).
6. Upon arrival at IBM, Service Agent inventory is transferred to the appropriate IBM database.

5

IBM Electronic Service Agent and the Hardware Management Console security

The transmission of Service Agent (SA) or Hardware Management Console (HMC) information is performed by a security-rich process. Depending on the connection options available, the transaction is by modem or in many networks, through the Internet. Allowing access between the Internet and the client's network raises security and privacy concerns, which we address in this chapter.

The following information and any updates are available on the Electronic Services Web site:

https://www.ibm.com/support/electronic

5.1 SA transmission security

The transmission of Service Agent information is performed by a security-rich process. Depending on the connection options available, the transaction is by modem or in many networks, through the Internet. Allowing access between the Internet and the client's network raises security and privacy concerns, which we address in this document.

IBM takes many actions to provide security-enhanced transmissions for Service Agent transactions:

- *Outbound transmission only*: The client Service Agent initiates communications and does not allow any inbound connection attempts. There are no applications "listening" to the TCP/IP port to establish a session.
- *Public key encryption*: Service Agent uses a 128-bit public key encryption mechanism to maintain the integrity and the authenticity of data exchanged between the Service Agent and IBM. Service Agent uses Secure Socket Layer (SSL)-based encryption and decryption.
- *Enrollment*: The first communication to IBM after activation is to request a unique ID and password for each machine monitored. This ID is not visible; it is only between your machine and IBM. The ID is generated by an algorithm using machine specific information. IBM, using this ID and password to authenticate the client machine, authenticates each subsequent communication.
- *Machine information only*: Machine or error information is sent. Service Agent does not access or transmit any other information that is on the monitored machines. The client license agreement clarifies the type of information that is transmitted.

5.2 SA connection options

This is a list of the connection options for Service Agent at this time. Each Service Agent User Guide provides the latest connection options for that platform.

Note: Not all options described below are available for all platforms. Reference the respective Service Agent User Guide**.**

5.2.1 Modem

Service Agent access through a modem:

- Service Agent uses the AT&T Global Network Services (AGNS) dialer for modem access.
- Service Agent provides the AGNS ID and password, which is supplied electronically in the background. The client is not able to view this information. This is an exclusive account for Service Agent.
- Service Agent uses these user IDs for point-to-point communications.
- A Dynamic IP address is assigned for each logon session.
- Service Agent does not accept incoming calls to the modem.
- The information is encrypted prior to entering the AGNS network. No party on the AGNS network can decrypt the information. The information is decrypted only inside IBM firewalls by the appropriate application.

- AGNS has provided a document describing their communication process with Service Agent. You can read this document on the Electronic Services Web site:

  https://www.ibm.com/support/electronic

Modem transmission example

The details of a modem transmission example (as shown in Figure 5-1) are:

1. The client has a modem connected to the system.
2. Service Agent collects the information to be transmitted and queues for transmission at the appropriate time.
3. System dials the AGNS Local Interface Gateway (LIG) at the appropriate time and establishes a connection using AGNS ID and password.
4. SSL connection is established with IBM through the AGNS LIG.
5. Service Agent inventory information flows to the IBM destination (predetermined by Service Agent code).
6. Upon arrival at IBM, Service Agent information is transferred to the appropriate IBM database.

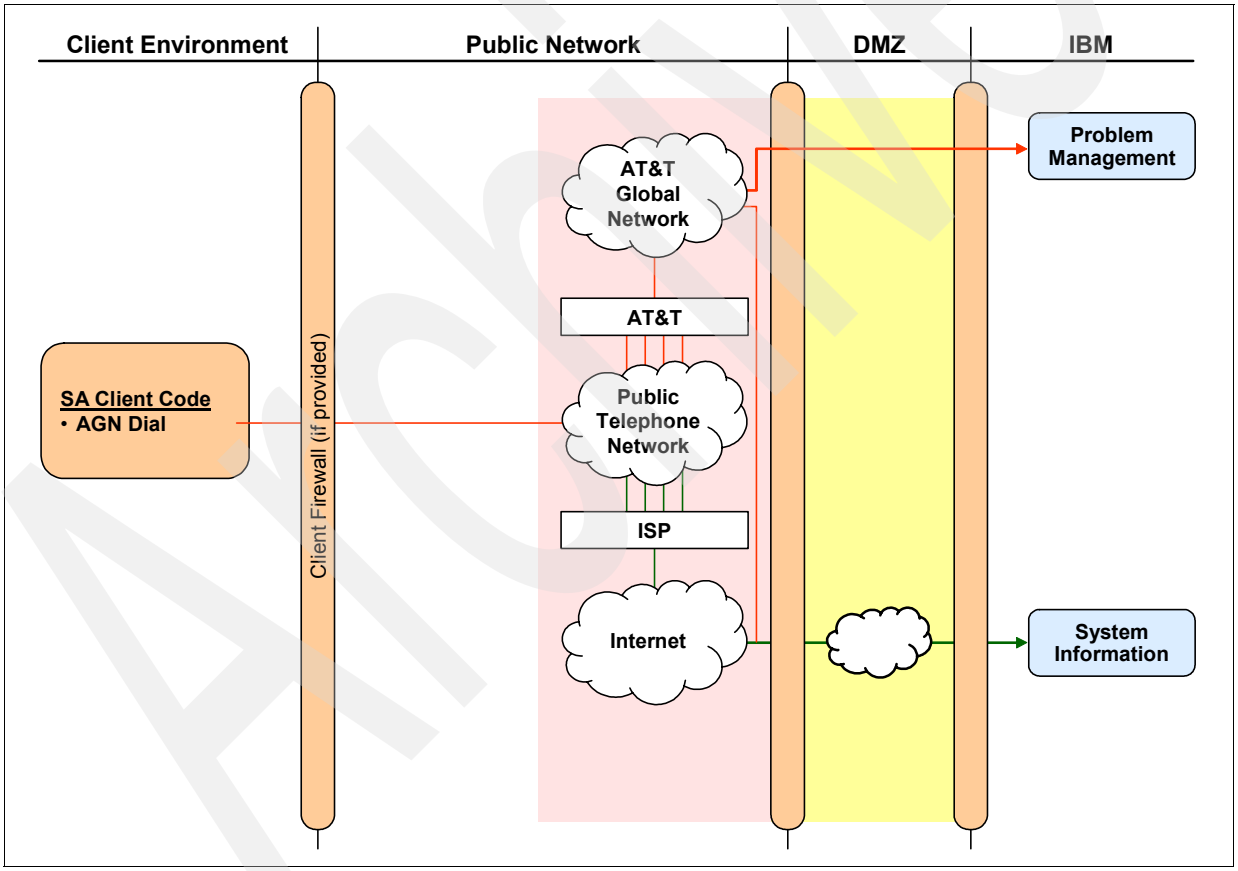


Figure 5-1 Modem connection example

5.2.2 Internet HTTPS

Service Agent access using Internet HTTPS considerations are:

- Service Agent uses HTTPS, which utilizes SSL 128-bit encryption and TCP/IP protocols.
- You can configure Service Agent to work with firewalls and authentication proxies.
- Service Agent only initiates the HTTPS communications; it does not respond.
- The Internet provider relationship and connection are the responsibility of the client.

Internet transmission example

Service Agent collects the information that is transmitted and queues it for transmission at the scheduled time. These steps show an example of Service Agent using an Internet transmission (as shown in Figure 5-2):

1. At the appropriate time, client Service Agent code establishes the Internet connection using System IDs and passwords that were created previously.
2. The SSL connection is established between the client system and IBM.
3. Service Agent information flows to the IBM destination (predetermined by Service Agent code).
4. Upon arrival at IBM, Service Agent information is transferred to the appropriate IBM database.

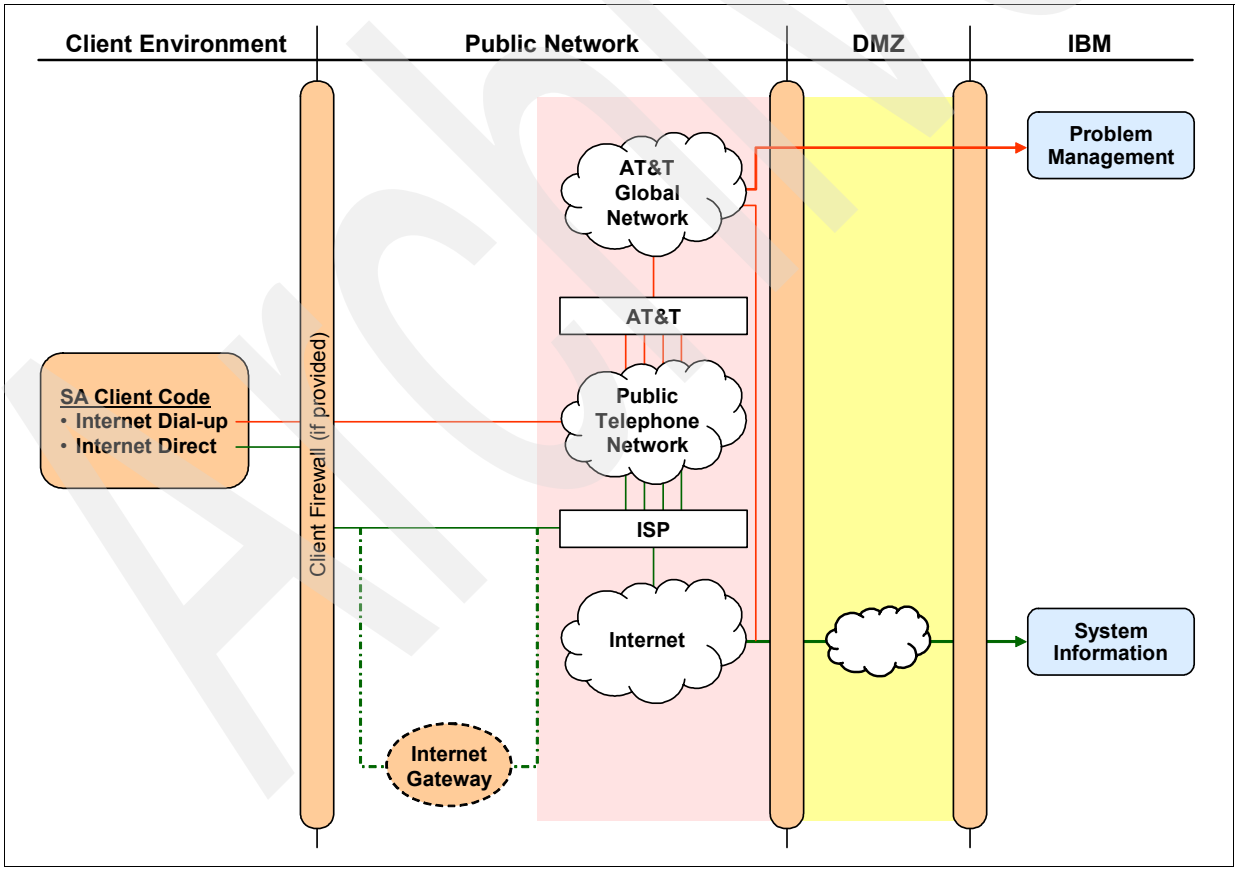


Figure 5-2 Internet connection

5.2.3 Internet Virtual Private Network

A Virtual Private Network (VPN) gives users the privacy of a separate network over public lines by substituting encryption and other security measures for the physically separate network lines of traditional private networks. VPNs require the configuration of an access device, either hardware-based or software-based, to set up a channel in a security-enhanced environment. In the case of Service Agent, it is software-based:

- VPN access uses Layer 2 Tunneling Protocol (L2TP) safeguarded with IPSec.
- Internet Key Exchange (IKE) is used to perform the initial authentication and to establish the security parameters to use when encrypting the information that will flow between the client's system and the IBM server.
- The Challenge Handshake Authentication Protocol (CHAP) is utilized as part of establishing the L2TP tunnel. This is to perform a second level of authentication.
- There is a firewall, which filters traffic to allow access to specific IP addresses and ports, behind the IBM VPN gateways to which the tunnels are established. When a tunnel is established with the VPN gateway, Electronic Service Agent then establishes a socket session to a specific port. When a socket is established, Electronic Service Agent sends up a logon record.

VPN transmission example

These steps are an example of Service Agent using a VPN transmission (as shown in Figure 5-3):

1. Service Agent collects the information and queues for transmission at the scheduled time.
2. At the appropriate time, client Service Agent code establishes an Internet connection using System IDs and passwords created previously.
3. The VPN connection is established between the client system and IBM.
4. The Service Agent information flows to the IBM destination (predetermined by Service Agent code).
5. Upon arrival at IBM, Service Agent information is transferred to the appropriate IBM database.

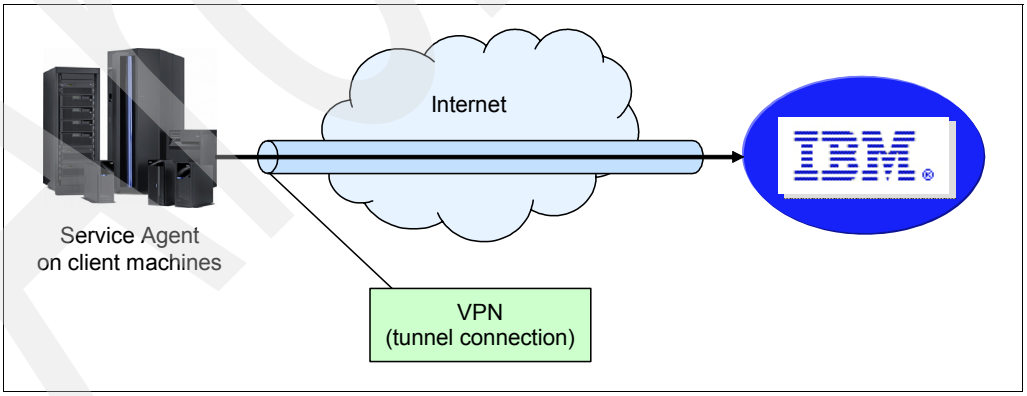


Figure 5-3 VPN example

Firewall considerations

When the Service Agent uses a VPN connection for transmission with a firewall between the client network and the Internet, you must configure the firewall to allow Service Agent to connect to IBM.

Service Agent establishes connections to these TCP/IP addresses:

- 207.25.252.196: The IBM Boulder VPN server
- 129.42.160.16: The IBM Rochester VPN server

You must enable the following ports and protocols:

- Protocol ESP
- Protocol UDP port 500
- Protocol UDP port 4500

5.3 SA and HMC privacy of client information

The inventory information that is gathered from client systems is information that is typically collected verbally from clients during phone calls with the IBM Support Center, pre-Sales specialists, administrative clerks, and other groups within IBM that work with the client to provide the best possible service (technical or administrative). These IBM groups have electronic access to the information so that they can prepare, do advance problem determination, and more efficiently serve IBM clients.

Inventory information includes your contact information, including names, phone numbers, and e-mail addresses; system utilization, performance, system failure logs, part feature codes, part number, part serial number, part locations, software inventory, operating system applications, PTFs, maintenance level, and configuration values. You can view all of the inventory information on the system using platform-specific commands.

Inventory information does not include the collection or transmission of any of your company's financial, statistical, or personnel data, client information, or your business plans.

In addition, Service Agent might also provide a "call home" mechanism for other IBM offerings that you might select in the future. The information collected by those offerings is covered in separate agreements.

5.4 Hardware Management Console (HMC)

This section describes data that is exchanged between the Hardware Management Console (HMC) and the IBM Service Delivery Center (SDC) and the methods and protocols for this exchange. All the functionality that is described here refers to HMC Version 6.1.0 and higher.

The HMC uses various methods for communicating back to IBM to match different client environments. This section outlines all the different ways in which you can configure an HMC to communicate with IBM.

5.4.1 HMC outbound configurations

You use outbound configurations to configure the HMC to connect back to IBM. The HMC uses its ability to connect to IBM for various situations, including reporting problems, downloading system fixes, reporting inventory, and transmitting error data.

Modem connectivity

Figure 5-4 on page 57 shows a typical dial environment. This configuration allows the HMC to use a modem to dial the AT&T global network and connect to the IBM POWER™ processor-based systems. The HMC automatically detects the modem when it boots up.

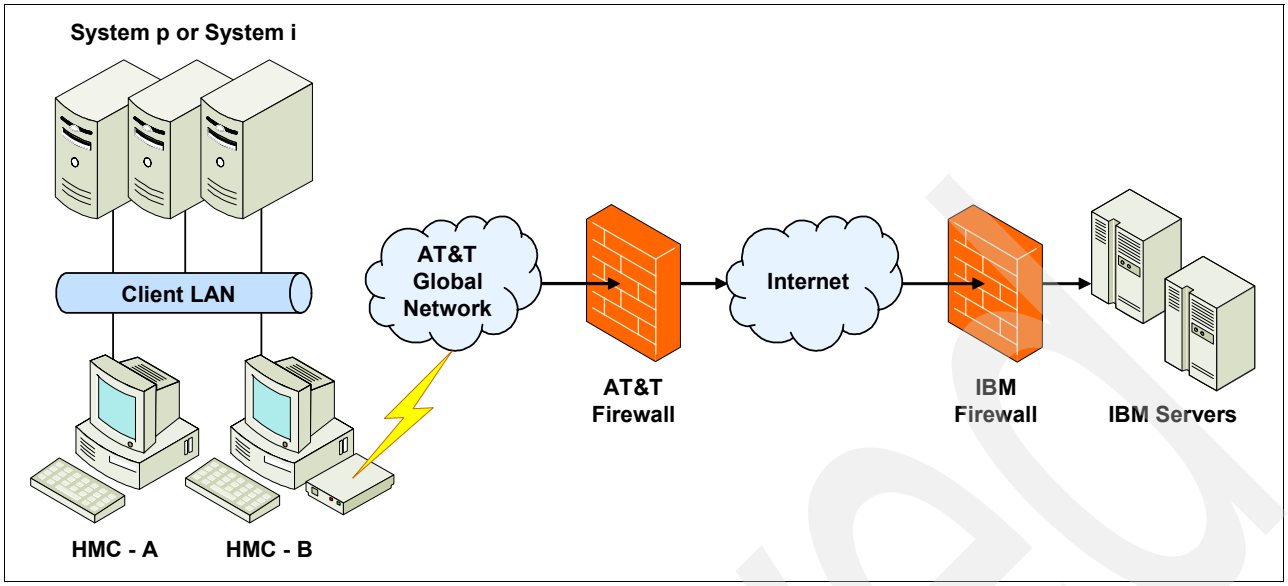


Figure 5-4 HMC modem connection example

In this example, the HMC uses one of the configured phone numbers to dial the modem to connect to the AT&T Global Network. After the modem connects, the HMC authenticates itself and establishes a Point-to-Point Protocol (PPP) session between the modems. Finally, after the PPP session finishes, AT&T allows IP connections through a "Fenced Internet," which completes the network between the HMC and the IBM servers.

All the communications between the HMC and the IBM servers are handled through TCP sockets. These sockets always originate from the HMC and use Secure Sockets Layer (SSL) to encrypt the data that is sent back and forth.

The "Fenced Internet" connection uses a firewall to limit access between the HMC and the Internet. Specifically, it allows communication only between the HMC and a list of IBM IP addresses. All other access to and from the Internet is blocked.

Note: The client can also configure the HMC's internal firewall, which also applies to IP connections over the modem.

Internet connectivity

In Figure 5-5 on page 58, the HMC uses a client-provided Internet connection to connect to the IBM servers. All the communications are handled through TCP sockets (which always originate from the HMC) and use SSL to encrypt the data that is being sent back and forth.

For this type of configuration, the client can optionally use a second network card to physically separate the local system network from the Internet-enabled network.

For the HMC to communicate successfully, the client's external firewall must allow established TCP packets to flow freely on port 443. The use of Source Network Address Translation (SNAT) and masquerading rules to mask the HMC's source IP address are both acceptable. The firewall can also limit the specific IP addresses to which the HMC can connect.

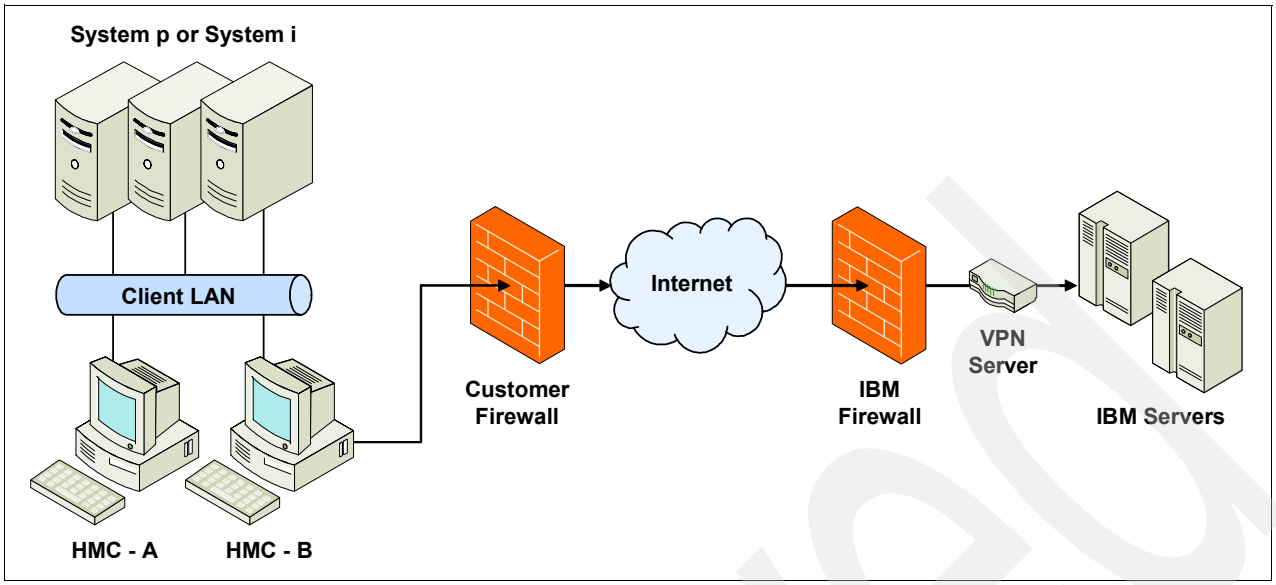


Figure 5-5 HMC connecting to IBM without a proxy server

Optionally, you can also enable the HMC to connect to the Internet through a client-configured proxy server, as shown in Figure 5-6.

To forward SSL sockets, the proxy server must support the basic proxy header functions (as described in RFC #2616) and the CONNECT method. Optionally, you can configure basic proxy authentication (RFC #2617) so that the HMC authenticates before attempting to forward sockets through the proxy server.

For the HMC to communicate successfully, the client's proxy server must allow connections to port 443. The proxy server can also limit the specific IP addresses to which the HMC can connect.

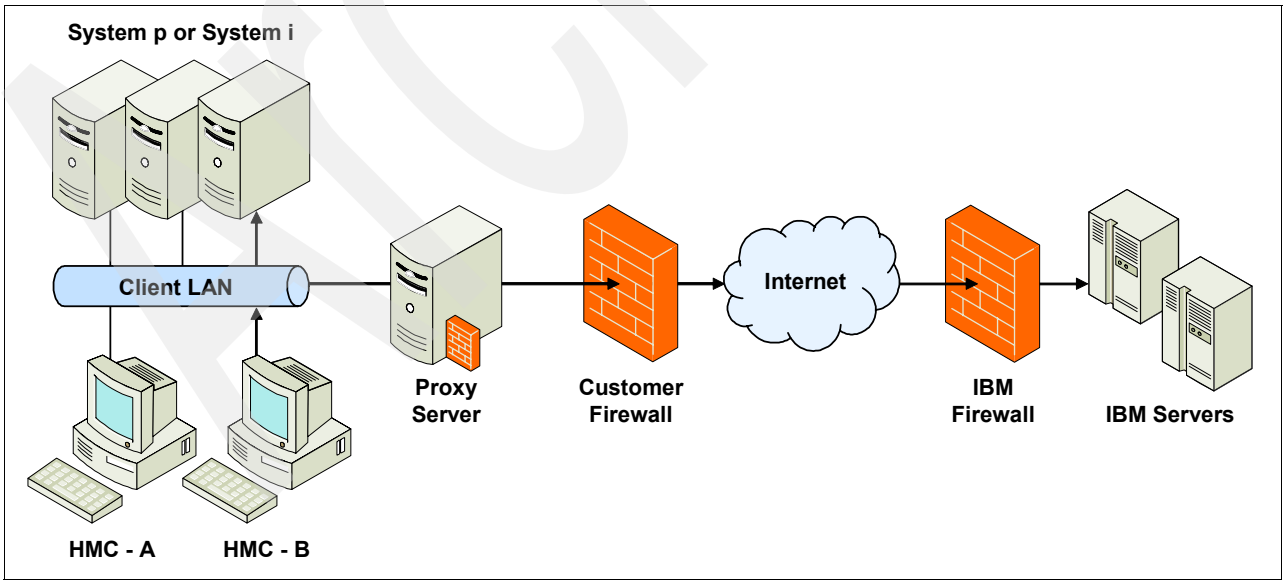


Figure 5-6 HMC connecting to IBM using a client-provided proxy server

Internet Virtual Private Network (VPN) connectivity

Figure 5-7 shows the HMC connecting to IBM using an Internet VPN. This is similar to the Internet Connectivity in Figure 5-5 on page 58, except that the connections are tunneled inside of another network layer.

In this example, the HMC connects through the client-provided Internet connection by the default route. For this type of configuration, the client can optionally use a second network card to physically separate the local system network from the Internet-enabled network.

Before the HMC tries to connect to the IBM servers, it first establishes an encrypted VPN tunnel between the HMC and the IBM VPN server gateway. The HMC initiates this tunnel using Encapsulated Security Payload (ESP, Protocol 50) and User Datagram Protocol (UDP). After it is established, all further communications are handled through TCP sockets, which always originate from the HMC.

For the HMC to communicate successfully, the client's external firewall must allow traffic for protocol ESP and port 500 UDP to flow freely in both directions. The use of SNAT and masquerading rules to mask the HMC's source IP address are both acceptable, but port 4500 UDP must be open in both directions instead of protocol ESP. The firewall can also limit the specific IP addresses to which the HMC can connect.

Note: The client can also configure the HMC's internal firewall, which applies to IP connections that go through the VPN tunnel.

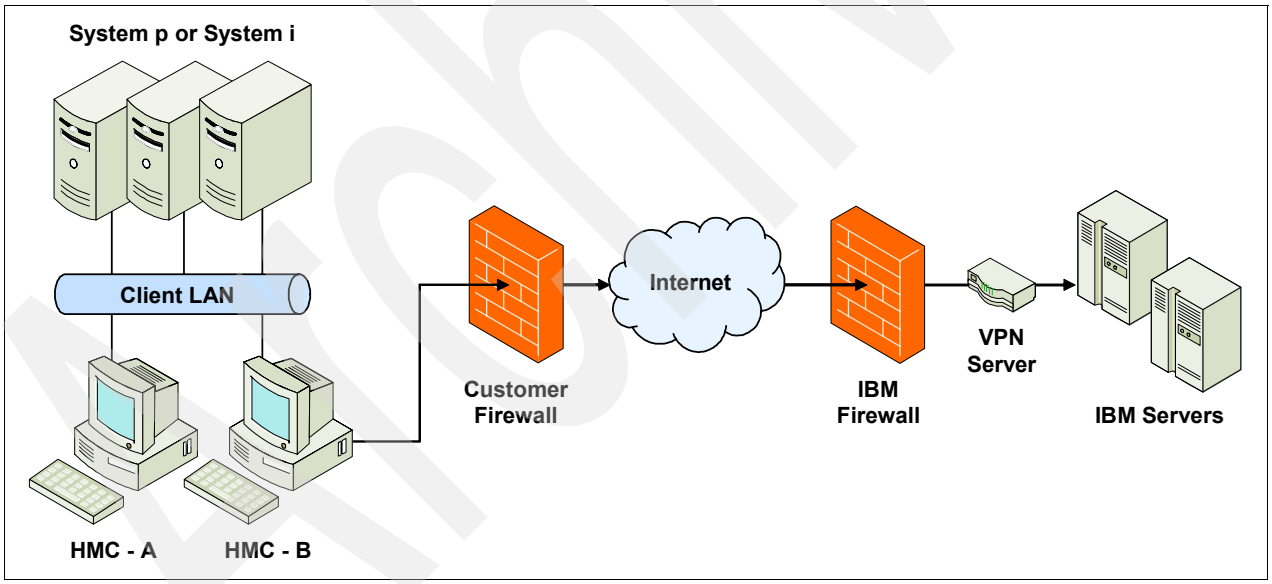


Figure 5-7 HMC connecting to IBM using Internet VPN

Pass-through server connectivity

Configuring pass-through server connectivity allows an HMC to borrow a shared VPN connection or modem from a properly configured i5/OS partition.

Multi-hop VPN

Figure 5-8 on page 60 shows a configuration that allows the HMC to use the multi-hop VPN capability of a client's i5/OS partition.

Before the HMC tries to connect to the IBM servers, it first establishes an unencrypted Layer 2 Tunneling Protocol (L2TP) tunnel to the i5/OS partition and requests the creation of an encrypted VPN tunnel between the partition and the IBM VPN server. The HMC initiates this tunnel using a UDP socket. After it is established, all further communications are handled through TCP sockets, which always originate from the HMC.

For the HMC to communicate successfully, the HMC must be able to open a 2-way UDP socket to the i5/OS partition on port 1701. Additionally, the client must configure the client's external firewall to allow the partition to properly establish the VPN tunnel to IBM.

Note: The client can also configure the HMC's internal firewall, which also applies to IP connections that go through the VPN tunnel.

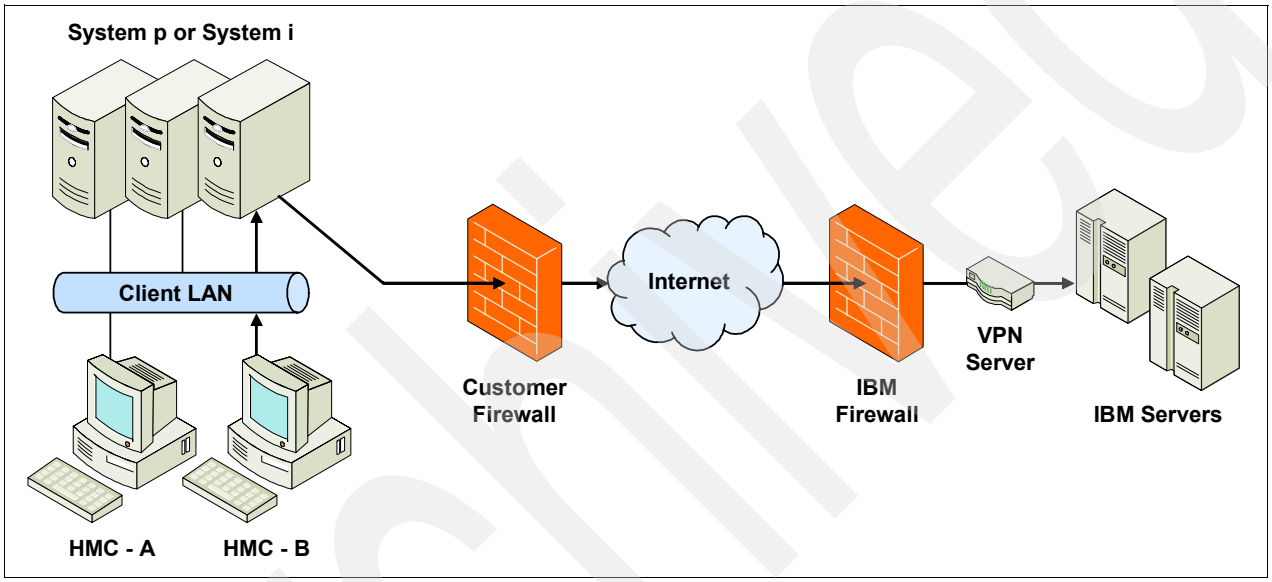


Figure 5-8 HMC using the multi-hop VPN

Remote modem

Figure 5-9 on page 61 shows a configuration in which the modem that the HMC uses is shared with a client's i5/OS partition.

Before the HMC tries to connect to the IBM servers, it first establishes an unencrypted L2TP tunnel to the i5/OS partition and requests the establishment of a modem connection to the AT&T Global Network. The HMC initiates this tunnel using a UDP socket. After the modem connection is established, the HMC authenticates itself and establishes a PPP session between the dialed AT&T modem and itself. Finally, after the PPP session finishes, AT&T allows IP connections through a "Fenced Internet," which completes the network between the HMC and the IBM servers.

All the communications between the HMC and the IBM servers are handled through TCP sockets. These sockets always originate from the HMC and use SSL to encrypt the data that is being sent back and forth.

The "Fenced Internet" connection uses a firewall to limit access between the HMC and the Internet. Specifically, it allows communication only between the HMC and a list of IBM IP addresses. All other access to and from the Internet is blocked.

Note: The client can also configure the HMC's internal firewall, which also applies to IP connections over the modem.

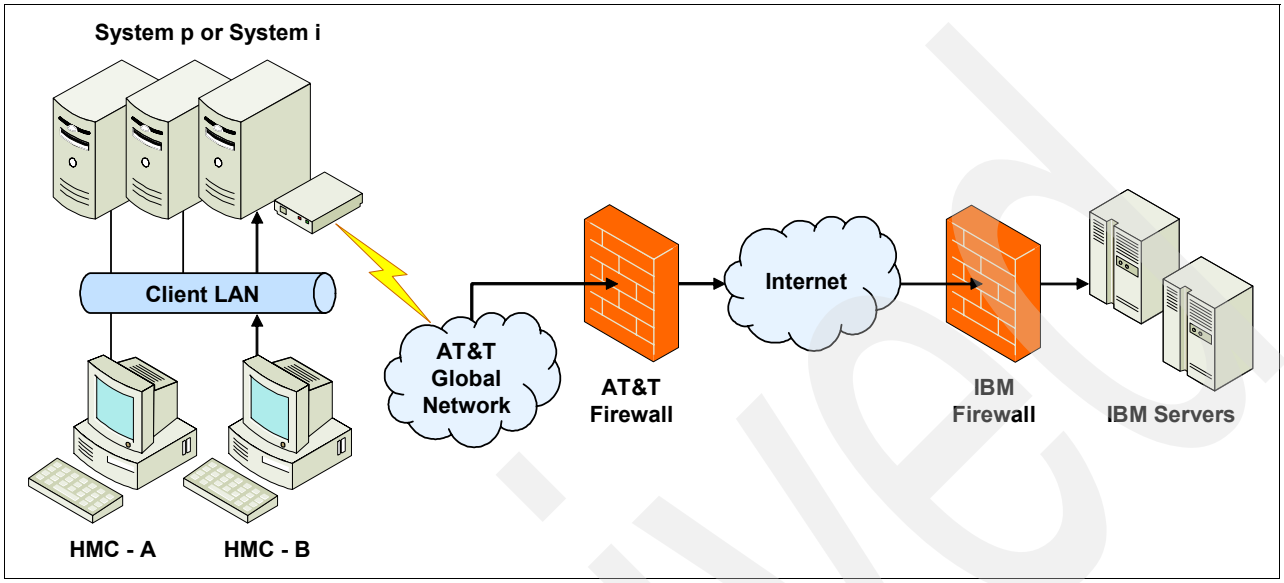


Figure 5-9 Shared modem example

5.4.2 HMC inbound configurations

Inbound connectivity configurations allow an IBM service support representative (SSR) to connect from IBM directly to your HMC or the systems that the HMC manages. The following sections describe two approaches to remote service. Both approaches only allow a one-time use after enabling.

Modem

Figure 5-10 on page 62 shows an inbound configuration using a modem.

For remote service over a modem, the modem must be set up to accept incoming phone calls. An IBM representative then logs in to a special server and uses that to dial directly into the client's modem. After the modem answers, a PPP session is initiated, and the IBM representative must authenticate using credentials based on the value that the client entered into the PPP address field on the Customize Inbound Connectivity panel.

After the PPP session is successfully initiated, the HMC creates an alternate IP address and attaches it to the virtual PPP network device for each partition to which the client allows access. Special routing rules are then put in place to route network packets to those IP addresses and over to the intended partition.

Finally, if the client has disabled access to the HMC, firewall rules are put in place to block all traffic that goes to the HMC. If the client has allowed access to the HMC, the firewall blocks all traffic except for packets targeting the ports outlined in 5.3, "SA and HMC privacy of client information" on page 56. Note that these rules override any rules that the client set through the Customize Network Settings panel.

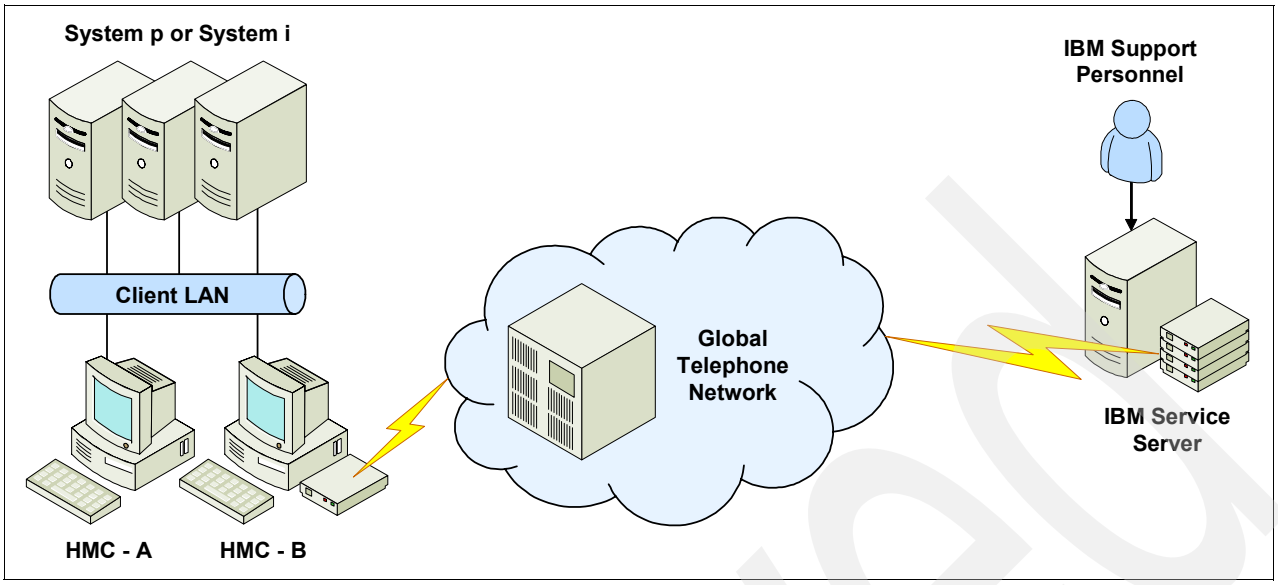


Figure 5-10 Inbound connectivity using a modem

VPN

Figure 5-11 on page 63 shows an inbound configuration using VPN.

A remote service VPN session can be initiated over a modem, Internet VPN, or a pass-through i5/OS partition. At least one of these methods of connectivity must be configured through the Outbound Connectivity panel.

To initiate the VPN session, the HMC connects into the IBM VPN server as described in 5.2.3, “Internet Virtual Private Network” on page 55. A client who configures the Outbound Internet VPN to use the existing Internet connection must ensure that the firewall has been properly configured to allow connections to the servers listed in “Firewall considerations” on page 55.

After the VPN session has been initiated, the HMC initiates additional L2TP+PPP tunnels for each partition to which the client allows access. Special routing rules are then put in place to route network packets on those tunnels over to the intended partitions.

Finally, if the client has disabled access to the HMC, firewall rules are put in place to block all traffic that goes to the HMC. If the client has allowed access to the HMC, the firewall blocks all traffic except for packets targeting the ports outlined in “Firewall considerations” on page 55. Note that these rules override any rules that the client set through the Customize Network Settings panel.

After the VPN session has been fully established, an authorized IBM Service Representative logs in to the IBM Service Server and connects to the HMC through the VPN session. The IBM Service Server has a special firewall in place that keeps the client’s VPN session completely separate from the IBM intranet. Access to the client’s VPN session through the IBM Service Server is possible only through the use of special tools that require special authorization and knowledge to use.

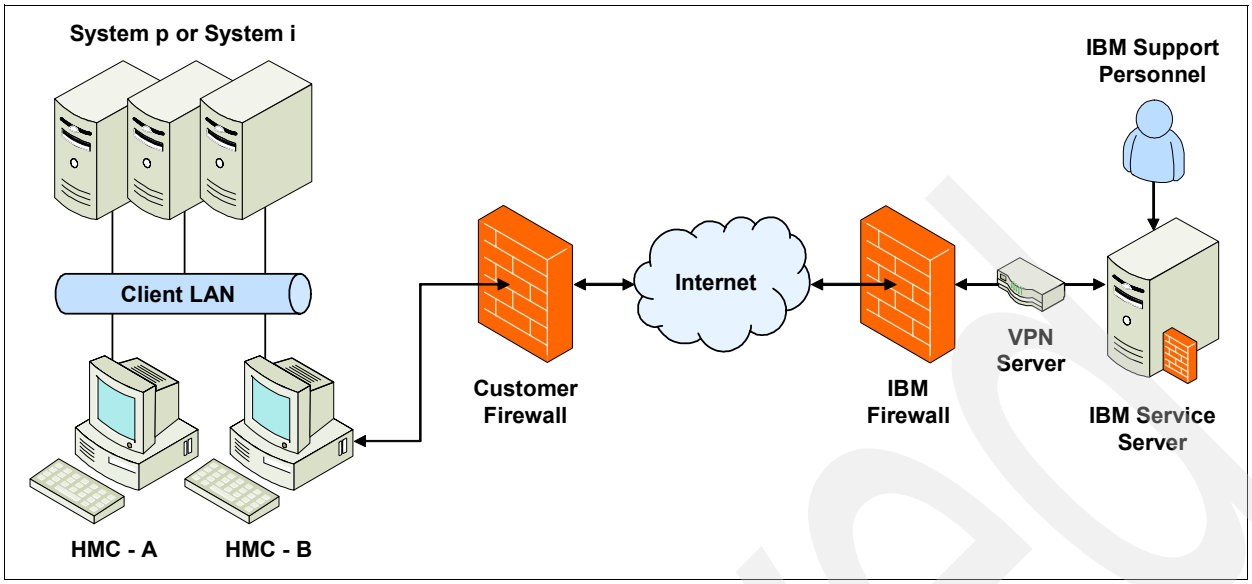


Figure 5-11 Inbound connectivity using VPN

5.5 HMC protocols and encryption

This section describes the protocols, encryption algorithms, and security that the various communication methods use. It is intended to be a conceptual overview, not to provide implementation details for particular technologies.

5.5.1 AT&T Global Network

When the HMC tries to connect to IBM using one of the phone numbers available from the Outbound Connectivity Modem panel, it is dialing into the AT&T Global Network Fenced Internet Remote Access Dial Service.

After the HMC's modem successfully connects into one of AT&T's Local Interface Gateways (LIGs), it initiates a PPP session and authenticates with the server using a special account and user ID that are sent using Password Authentication Protocol (PAP). Upon successful authentication, the LIG assigns the HMC a dynamic IP address from a pool for the duration of the connection.

All packets that flow through the LIG from the HMC are inspected to ensure that the source of the packet is the assigned IP address and that the destination matches one of the authorized IBM servers or to one of the utility services provided by AT&T (such as domain name servers). Return packets that flow through the LIG back to the HMC must have destinations that match the assigned IP addresses, and the source must match the IBM server with which the IP addresses communicate. Any packets not matching these criteria are discarded.

5.5.2 SSL

The SSL sockets used by the HMC are actually Transport Layer Security (TLS) sockets (sometimes referred to as *SSLv4*). The initial handshake uses a public/private asymmetric 1024-bit key. After the handshake, they negotiate the bulk encryption depending on the IBM server to which a connection is being made. IBM systems in the SDC use a symmetric 128-bit Rivest Cipher 4 (RC4) encryption or a symmetric 256-bit Advanced Encryption Standard (AES) encryption.

5.5.3 VPN

The VPN connection that is used by the HMC is an IP Security (IPSec) implementation in tunnel mode over a UDP socket that uses L2TP+PPP encapsulation for the actual data transmission. The VPN key exchange is done using Internet Key Exchange (IKE), which is authenticated as part of the ESP encryption using a Pre-Shared Key (PSK). The ESP encryption uses a 192-bit Triple DES (3DES) encryption key with a 160-bit Message Digest Algorithm 5 (MD5) hash authentication key. The authentication and encryption keys are renegotiated at a random time interval around every 30 minutes.

After the IPSec tunnel has been properly established, the HMC creates an L2TP tunnel between the VPN server and itself. Within that tunnel, the HMC then establishes one or more PPP sessions that the server authenticates using the Challenge Handshake Authentication Protocol (CHAP). All further HMC data sockets are then opened over one of the established PPP sessions.

5.6 HMC data and information

This section outlines what data is sent and the reasons for sending data when the HMC connects to the IBM Service Delivery Center.

The reasons for connecting to IBM are:

- Reporting a problem with the HMC or one of the systems that it manages back to IBM
- Downloading fixes for systems that the HMC manages
- Reporting inventory and system configuration information back to IBM:
  - The client's problem and system inventory information are readily available to the IBM Support Community, which helps reduce problem resolution time.
  - The client can view the client's inventory on the Electronic Services Web site. The reports are unique by hardware platform.
  - The Electronic Services Web site enables searching IBM technical databases using your Electronic Service Agent information to filter results.
- Sending extended error data for analysis by IBM
- Repairing and verifying system parts and enclosures
- Reporting heartbeat and status of monitored systems
- Sending performance and utilization data for system I/O, network, memory, and processors

5.6.1 Data sent to IBM

Table 5-1 on page 65 is a list of the files that can be sent to IBM, plus short descriptions of the contents of those files. Along with the information contained in these files, the HMC also sends back client contact information, machine model and serial numbers, and debug traces for HMC software. None of the information or debug data that is sent to IBM contains client data.

Table 5-1 Files sent to IBM

File	Description
actzuict.dat	Tasks performed
hmc.eed	HMC code level obtained from **`lshm c -V`** and connection information obtained from **`lssysconn -r all`**
iqyvpd.dat	Configuration information associated with the HMC
iqyvpdc.dat	Configuration information associated with the HMC
iqyycom0.log	HMC firmware log information backlog0
iqyycom1.log	HMC firmware log information backlog1
iqyycom2.log	HMC firmware log information backlog2
iqyylog.log	HMC firmware log information
PMap.eed	Partition map obtained from **`lshsc -w -c machine`**
problem s.xml	XML version of the problem opened on the HMC for the HMC and the server
sys.eed	Output from the following commands: ► **`lssyscfg -r cage`** ► **`lssyscfg -r frame`** ► **`lsdump -e $machine -s a`** ► **`lsdump -e $machine -s b`** ► **`lshsc -i -a >> managedSystems`** ► **`lssyscfg -r lpar`** ► **`lshwres -r proc -- level lpar`** ► **`lshwres -r mem -m $machine --level lpar`** ► **`lshwres -r io -m $machine --rsub type slot`** ► **`lsdump -m $machine`** ► **`lssyscfg -r sys -m $machine`** ► **`lssyscfg -m $machine -r sys`** ► **`lssyscfg -m $machine -r lpar`** ► **`lssyscfg-m $machine -r sysprof`**
machType-Model_Serial.VPD.xml	Configuration information associated with the managed system
filetype.machineSerial.dumpID - *yyyymmddhhmmss*	Dump file type set to one of the following: ► SYSDUMP for a platform system dump ► FSPDUMP for a FipS Service Processor dump ► BMCDUMP for a BMC SP dump ► SMADUMP for a SMA dump ► PWRDUMP for a power subsystem dump ► LOGDUMP for a platform event log entry dump ► RSCDUMP for a platform resource dump These dumps do not contain any client-related information.

5.7 HMC additional considerations

Next, we describe additional HMC information that is available to you.

5.7.1 IBM server address list

An HMC uses the following internet protocol (IP) addresses when the client configures it to use Internet connectivity. All connections to these IP addresses use port 443 TCP.

For the Americas, use:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.200
- 207.25.252.204

For other than the Americas, use:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.200
- 207.25.252.205

Note: When configuring a firewall to allow an HMC to connect to these servers, the client only needs the IP addresses specific to the client's region.

5.7.2 VPN server address list

The HMC uses these IP addresses when it is configured to use Internet VPN connectivity. All connections use protocol ESP and port 500 UDP, or ports 500 and 4500 UDP when a Network Address Translation (NAT) firewall is used.

VPN servers for all regions:

- 129.42.160.16
- 207.25.252.196

5.7.3 Remote service HMC port list

When an inbound remote service connection to the HMC is active, only the following ports (shown in Table 5-2) are allowed through the firewall for TCP and UDP.

Table 5-2 Ports list

Port	Comments
22, 23, 2125, and 2300	These ports are used for access to the HMC.
9090, 9735, 9940, and 30000-30009	These ports are used for the Web-based System Manager.

5.7.4 Multiple HMCs

This section describes an environment with multiple HMCs configured with outbound connectivity.

Discovery and inter-console communication

Consoles have the ability to discover and communicate with each other. A console discovers other consoles by using a UDP broadcast (port 9900) on the subnet of each configured network card. A console also discovers any other console managing the systems that it manages. A console establishes communication with any discovered console by using an SSL socket (port 9920) with Diffie-Hellman key exchange.

Call home servers

A console automatically forwards its *call home* requests to any discovered console that is configured as a call home server. When more than one call home server console is available, a brokering process involving inter-console communication selects a console to handle each request. Failures are automatically retried at remaining call home server consoles.

6

IBM Electronic Service Agent: Connectivity for System i and System p

This connectivity chapter contains the complete list of tasks needed to set up connectivity to service and support. You might have already completed many of these tasks (during initial server setup, for example). You can use this information to verify that the tasks were completed correctly.

6.1 Where to install and activate IBM Electronic Service Agent

IBM Electronic Service Agent can run on a variety of operating systems and system platforms:

- i5/OS
- AIX
- Linux
- Windows
- Hardware Management Console (HMC)
- z/OS

For any system platform, there can be one or more operating systems. No matter which system platform you have, how many partitions are configured, or which operating systems are running, IBM Electronic Service Agent must be installed and activated on each partition, operating system, and HMC.

The functions provided by IBM Electronic Service Agent vary based on the network environment. For example, if your system platform is running two partitions of AIX and two partitions of i5/OS, the HMC reports platform errors for the system and partition errors for the AIX partitions. IBM Electronic Service Agent on each i5/OS partition reports partition errors for the partition on which it runs. To have total coverage, IBM Electronic Service Agent needs to run on the HMC, each i5/OS partition, and each AIX partition.

6.2 Before you begin

This chapter defines *direct Internet connection* as access to the Internet from a logical partition, server, or HMC by direct or indirect access. *Indirect* means that you are behind a Network Address Translation (NAT) firewall. *Direct* means that you have a globally routable address without an intervening firewall (which blocks the ports that are needed for communication to service and support).

6.2.1 Determine your connectivity method

In this section, we recommend options for your connectivity method.

If you have an HMC and have multiple logical partitions

In this case, we recommend:

- For the HMC, use either direct Internet or a dial-up connection to connect the HMC to service and support.
- For logical partitions:
  - For AIX or Linux logical partitions, hardware errors are reported through the HMC by using the connection method provided for the HMC.
  - For i5/OS logical partitions, use one of the following methods (listed in the recommended order):
    - Direct Internet from each logical partition: This method allows larger fix files to pass through the connection to the server. Each logical partition can receive the fixes that it needs. It is also faster than modem dial-up connection.
    - Shared direct Internet through one of the i5/OS logical partitions: This method also allows larger fix files to pass through the connection to the server. It allows

connectivity to be concentrated through one server or logical partition, which simplifies firewall rules. It is also faster than modem dial-up connection.

- Shared dial-up connection through one of the i5/OS logical partitions: If you do not have direct or shared direct Internet, you might choose to use a shared dial-up connection. It is slower and restricts the file size that can pass through the connection.

If you do not have an HMC and logical partitions

Your options if you do not have an HMC and logical partitions are:

- For AIX or Linux, use direct Internet, Secure Sockets Layer (SSL), or direct dial-up connection.
- For i5/OS, use direct or shared direct Internet, or a direct or shared dial-up connection.

6.3 Prerequisites

The following list describes various connection types.

Note: Work with the network administrator if necessary.

Internet connections:

- For HMC environments, and for i5 servers in a non-HMC environment, ensure the following ports are open for communication:
  - Protocol UDP ports 500 and 4500 with the following IP addresses:
    - Boulder: 207.25.252.196 and Rochester: 129.42.160.16
  - ESP (protocol 50) with the following IP addresses:
    - Boulder: 207.25.252.196 and Rochester: 129.42.160.16
- For p5 servers in a non-HMC environment, ensure the following port is open for communication:
  - Protocol TCP port 443 with the following IP addresses:
    - Boulder: 207.25.252.200 and Rochester: 129.42.160.48
- If multiple logical partitions are sharing an Internet connection, you need the IP addresses or host names created for TCP/IP and for virtual Ethernet.

Dial-up:

- For dial-up (modem) connection, determine the necessary configuration settings, including:
  - Local area code
  - Pre-dial information, such as dialing “9” to dial outside the network
  - Use of commas if delayed dialing is needed

TCP/IP:

- Ensure that TCP/IP is set up and configured correctly. If not, work with the network administrator and your operating system documentation.

6.4 Ensure that your physical network is set up correctly

To ensure that your physical network is set up correctly, perform the following steps:

1. Verify the physical connection between the service processor and the HMC.

   The service processor is part of your platform hardware and monitors hardware attributes and conditions on your server. The service processor is controlled by server firmware (Licensed Internal Code) and does not require an operating system to perform its tasks.

   The connection to the service processor is recommended for all servers, whether or not you have logical partitions. This connection is represented in Figure 6-1.

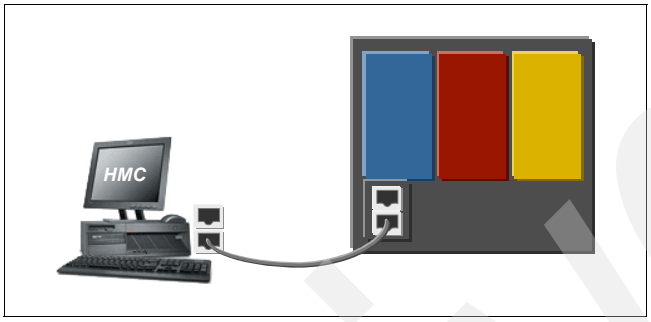


Figure 6-1 The Ethernet connection between your HMC and the service processor on your server

2. Verify the physical connection between the HMC and the operating systems.

   Note: This step is optional for i5/OS.

   This connection allows your operating systems to communicate with your HMC. How you set up this connection depends on your configuration:

   – If your server is in its manufacturing default configuration, you make this connection when you set up your server.

   – If your server has multiple logical partitions, you must ensure that your HMC can communicate with each logical partition and that the logical partitions can communicate with each other. You set up these connections as you create your logical partitions.

     Note: The *manufacturing default configuration* is the original configuration of the managed system. All of the resources on the managed system are assigned to a single logical partition. You can install an operating system on the single logical partition and use the managed system in this non-partitioned state.

   You can use either of the following methods. Both of the networking methods require basic TCP/IP configuration on your logical partitions. For instructions to configure TCP/IP, see your operating system documentation:

   – Have an Ethernet adapter for one logical partition (this can be the service partition for i5/OS) and then use virtual Ethernet to enable the logical partitions to communicate with each other and with the HMC. This option is the preferred option, because it requires that you have only one physical adapter in the system. Figure 6-2 on page 73 shows the Virtual Ethernet connection between your logical partitions and the physical Ethernet connection between your service partition and the HMC.

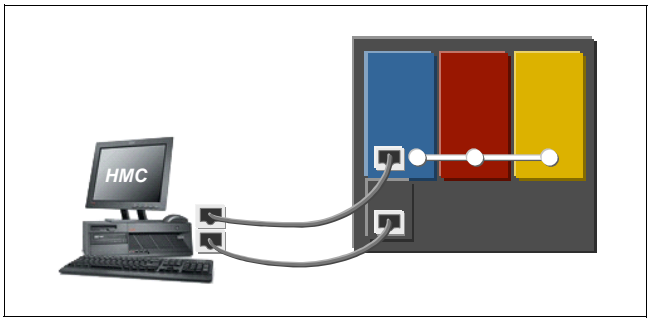


Figure 6-2 Virtual Ethernet connection between logical partitions and the physical Ethernet connection

– Have a LAN adapter for each logical partition and then have a physical connection between each logical partition and the HMC. This option requires that you have a router and a physical LAN adapter for each logical partition. Figure 6-3 shows this configuration.

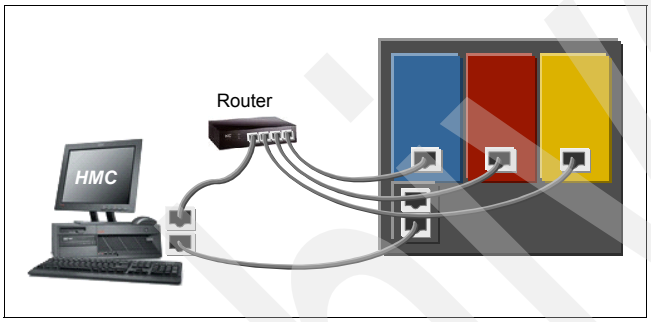


Figure 6-3 Physical Ethernet connections between logical partitions and your HMC through a router

3. Verify the physical connection from your site to service and support. This connection enables you to report hardware problems and other server information to service and support. It also enables you to receive fixes electronically from service and support as shown in Figure 6-4.

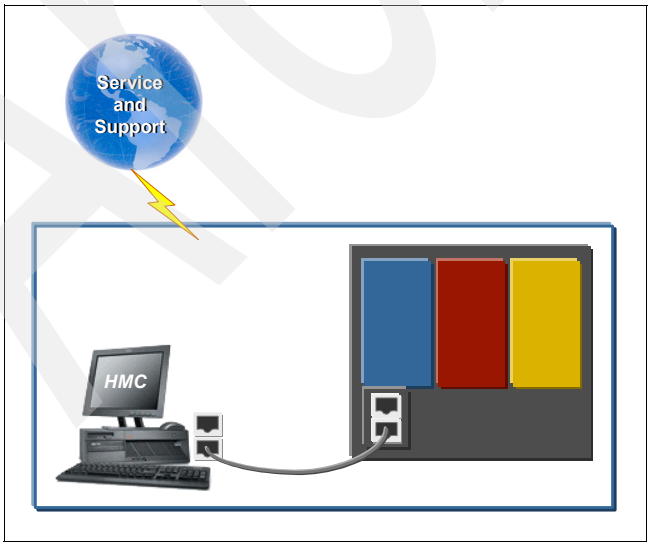


Figure 6-4 The connection between service and support for a company with a server and an HMC

6.5 Obtain or verify an IBM ID

You need an IBM ID to register IBM Electronic Service Agent on the HMC and for IBM Electronic Service Agent on the operating systems, including AIX, i5/OS, and Linux. You also need this IBM ID to view information that has been reported to IBM through the IBM Electronic Service Agent.

If you are a client, perform the following steps:

1. Using a Web browser, go to the My IBM Profile Web site at:

   https://www.ibm.com/account/profile

2. Verify that you are registered:
   - If you are registered, “Welcome back” appears on the Web site. Or, you can select **Sign in** and see if your e-mail address is recognized.
   - If you are not registered, select **Register** and fill out the registration form.
3. Record your IBM ID (the e-mail address that you registered). You will need the ID during 6.6, “Verify the HMC service settings”.

If you are a service provider, ask the client for their IBM ID. You will need the IBM ID during 6.6, “Verify the HMC service settings”. The simplest way to verify that the HMC service settings are set up correctly is by using the Guided Setup wizard.

Note: If you have not set up your server, do that now. See the Initial server setup topic in the eServer Hardware Information Center. For details, refer to Task 15. Access additional resources.

6.6 Verify the HMC service settings

To verify the HMC serice settings, install the operating systems on your server or logical partitions:

1. Access the Guided Setup wizard using the HMC interface:
   a. In the navigation area, select the HMC with which you want to work.
   b. Click **Information Center and Setup Wizard**.
   c. In the contents pane, click **Launch the Guided Setup Wizard**. The Guided Setup wizard steps you through the tasks that are required to set up your HMC, including the tasks that are required to set up your service environment.

      Note: You can ignore the tasks that are unrelated to service and support, such as setting the date and time.

2. Ensure that the following service tasks are completed correctly:
   - Configuration of the network settings
   - Client contact information for service-related activities
   - Configuration of connectivity for service-related activities. Choose one or more of the following types of connectivity for this procedure:
     - VPN: When configuring the HMC’s network settings for connecting using direct or indirect Internet, you must configure the HMC with a default gateway to access the Internet. Select **HMC Management** → **HMC Configuration** → **Customize**

Network Settings. Ensure that the Default Gateway Information field has a Gateway address listed and that a selection is made in the Gateway device field (for example, `any`).

- HTTPS (HMC Release 5.2) Support for Proxy Servers
- Dial-up

– Configuration of Service Focal Point settings

3. Test the connection from the HMC:
   a. In the HMC navigation area, open **Service Applications** → **Remote Support** → **Customize Outbound Connectivity**.
   b. Select the tab for the type of outbound connectivity that you want for your HMC:
      - Local Modem
      - Internet VPN
      - HTTPS
      - Pass-Through Systems
   c. Click **Test** and then click **Start**.
   d. If the test fails, continue with the next step.
   e. Ensure your country or region is listed. Select **Service Applications** → **Remote Support** → **Customize Customer Information**. Ensure that your country (region) is selected from the drop-down list.

7

IBM Electronic Service Agent for System i

The IBM Electronic Service Agent for System i automatically ships with the System i platform without an additional charge. It is designed to monitor events and transmit system inventory information to IBM. Service Agent has been available on the System i platform since 1992 under the name Service Director and as Service Agent since 2000.

This chapter is written for system administrators who are familiar with or have a working knowledge of IBM i5/OS system.

7.1 Where to install and activate IBM Electronic Service Agent

IBM Electronic Service Agent can run on a variety of operating systems and system platforms:

- i5/OS
- AIX
- Linux
- Windows
- Hardware Management Console (HMC)
- z/OS

For any system platform, there can be one or more operating systems. No matter which system platform you have, how many partitions are configured, or which operating systems are running, you must install and activate IBM Electronic Service Agent on each partition, operating system, and HMC.

The functions provided by IBM Electronic Service Agent vary based on the network environment. For example, if your system platform is running two partitions of AIX and two partitions of i5/OS, the HMC reports platform errors for the system and partition errors for the AIX partitions. IBM Electronic Service Agent on each i5/OS partition reports partition errors for the partition on which it is running. To have total coverage, IBM Electronic Service Agent needs to run on the HMC, on each i5/OS partition, and on each AIX partition.

7.2 IBM Electronic Service Agent V5R4 for System i platform

IBM Electronic Service Agent for System i platform is designed to reduce the downtime when a hardware or software problem occurs or is predicted to occur. Detected hardware failures are sent immediately to the IBM Support Center. The regular schedule of collecting machine inventory information (also known as *service information* on this platform) enables support representatives or representatives of your organization to quickly confirm the machine's configuration.

IBM Electronic Service Agent V5R4 is integrated into the base i5/OS V5R4 operating system (5722-SS1). It includes the following features:

- Secure Internet access to IBM through Hypertext Transfer Protocol Secure (HTTPS)
- Access to IBM through an authenticating proxy
- Easy configuration using wizards
- Reporting of certain software problems

For information about IBM Electronic Service Agent activation, use, connectivity, and troubleshooting, see the IBM Electronic Service Agent topic in the i5/OS Version 5 Release 4 Information Center:

`http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/rzaji/service_agent.htm`

7.3 Stand-alone system compared to partitioned system

Hardware and software problems are reported through two paths, depending on your hardware environment:

- Stand-alone (non-partitioned) system:
  - Service Agent reports hardware problems and software problems to IBM.

- Partitioned system:
  - Service Agent for System i detects partition errors for the i5/OS partition on which it is running and reports the problems to IBM.
  - Service Agent for System i detects software errors for the i5/OS partition on which it is running and reports the problems to IBM.
  - Service Agent on the HMC detects platform errors for the system and partition errors for the AIX and Linux partitions and reports the problems to IBM.

The service information collected by Service Agent varies based on the configuration of the system.

The machine inventory collection function of Service Agent for System i platform collects system information about memory, hard disk drives or RAID drives, Peripheral Component Interconnect (PCI) adapters, and communications information. You can view Service Agent Inventory at the following Web site using your IBM ID as authentication:

https://www.ibm.com/support/electronic

Figure 7-1 shows a System i multi-partition environment reporting to the HMC.

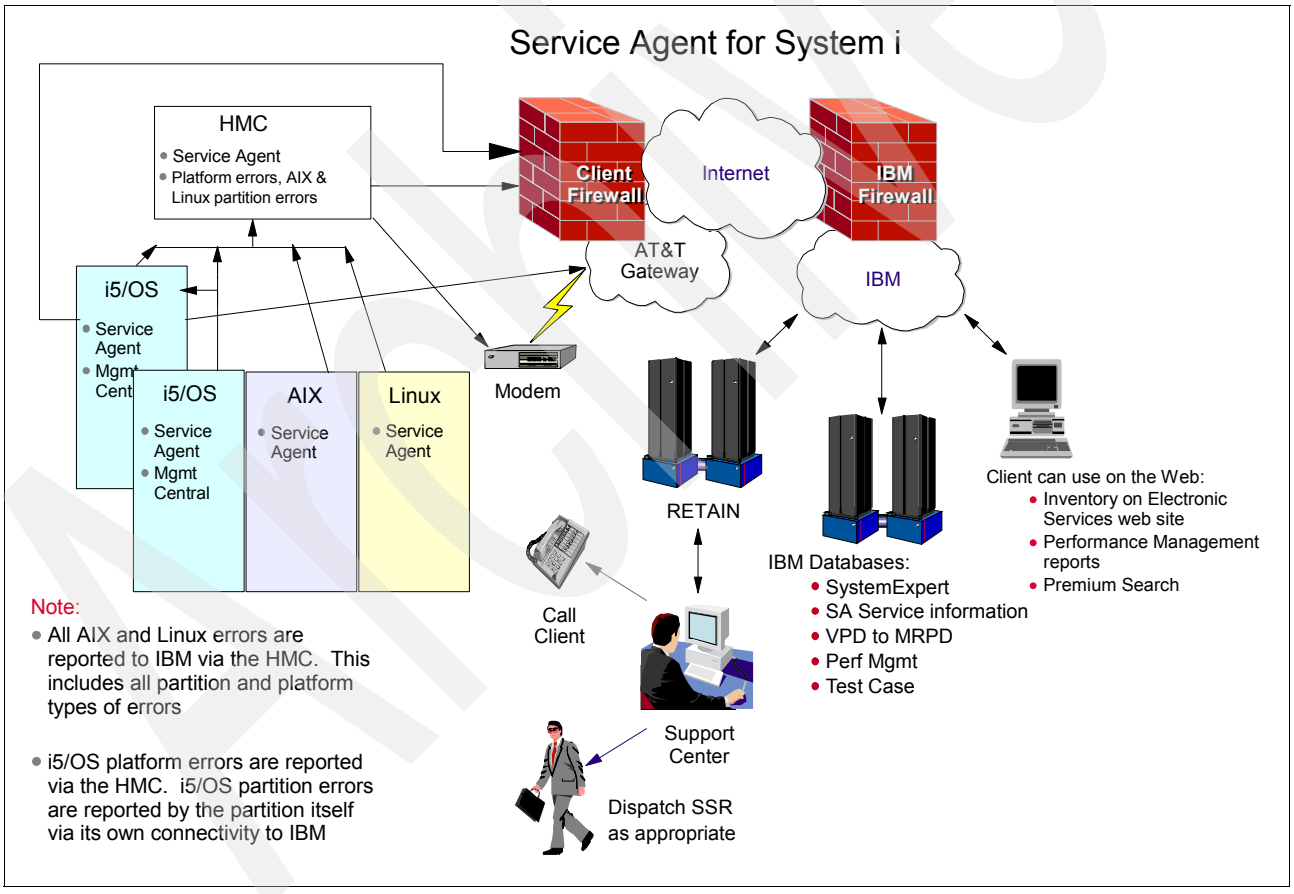


Figure 7-1 System i multi-partition environment

7.4 Interaction with other components

Service Agent for System i interacts with several system software components (as shown in Figure 7-2 on page 80) in order to provide coverage for your system. These components

include Electronic Customer Support (ECS), Connection Manager (Universal Connection), Management Central, Problem Log Manager, Database, and Java™. Service Agent also interfaces with components within the IBM back-end infrastructure, such as the Electronic Services Problem Service Provider and the Profile Service Provider.

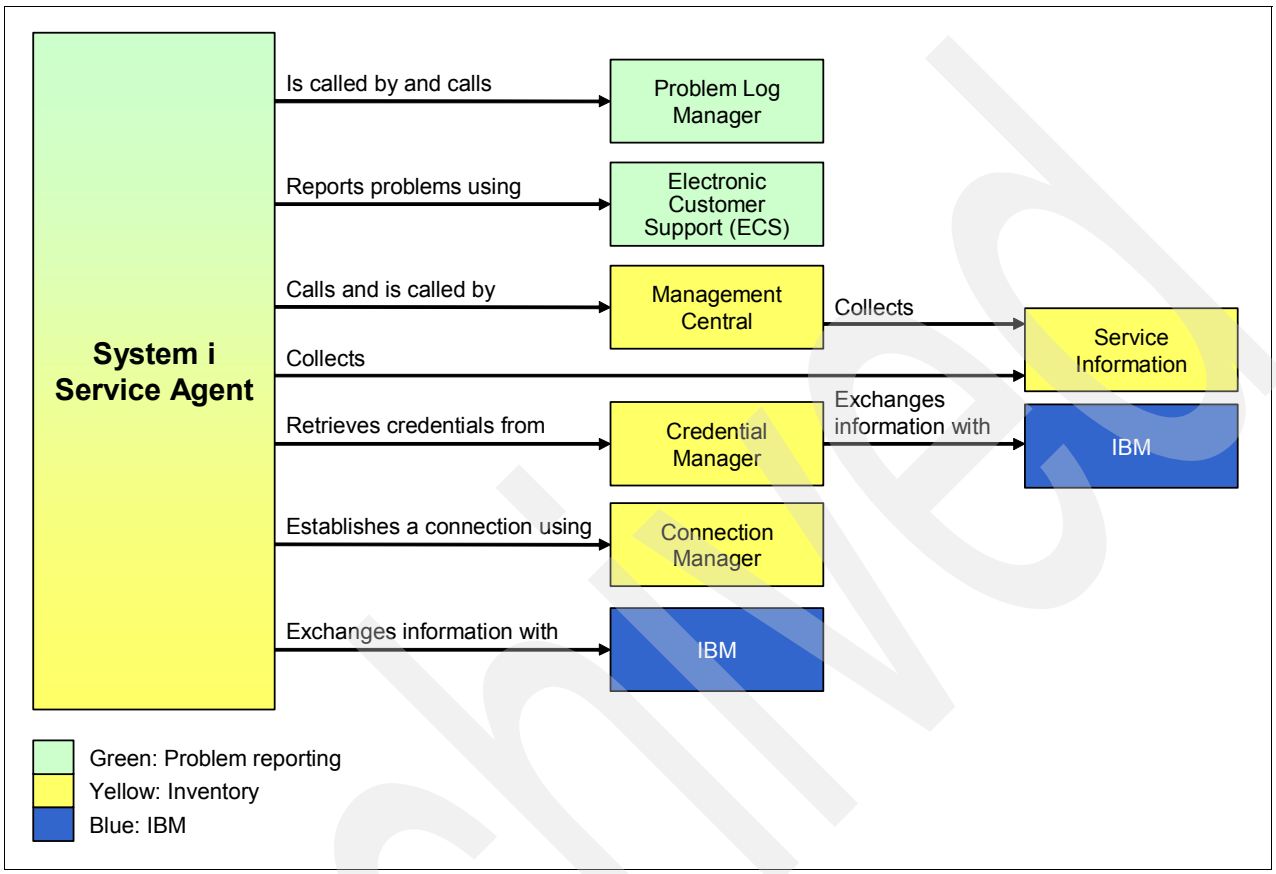


Figure 7-2 How Service Agent works with other components

7.5 Activation

Service Agent must be activated before it can report problems or send service information to IBM. For instructions about how to activate Service Agent, see the Information Center articles: “Pre-Activation checklist” and “Activation steps and troubleshooting,” at this Web page:

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=/rzaji/service_agent.htm

With the inclusion of Service Agent into i5/OS, it is not possible to uninstall Service Agent; however, you can disable Service Agent. To disable Service Agent, from the Service Agent main menu, select Change Service Agent attributes (option 1) and set the Enable parameter to *NO.

7.6 Connectivity

There are many ways to configure Service Agent and its connectivity in a network. The recommended method is to use a direct Internet connection. A direct Internet connection

provides the largest bandwidth for improved performance in the transmission of information to IBM. It is the most efficient connection type.

In the case where you use a modem, we recommend that you use the internal modem by having it logically attached to each partition so that all partitions can share the modem as a single connectivity point to IBM. You can configure Service Agent on i5/OS to use a modem on any partition or the modem on the HMC.

For information and scenarios about connectivity options, see the i5/OS Information Center topic on Universal Connection, which is located at:

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=/rzatj/kickoff.htm

7.6.1 Service Agent in a network

Automatic hardware problem reporting and service information collection are started in separate tasks. When using a centralized approach, we recommend that you activate problem reporting first.

Problem reporting

In a network environment, Service Agent and System Manager/400 (SM/400) can work together to report problems to IBM through a central system. It is important to note:

- On the central system (Service Provider):
  - Service Agent must be activated.
  - Service Agent must be configured to accept problems from remote systems (Service Requesters).

    This is controlled by a Service Agent attribute on the central system. To change this attribute, from the Service Agent main menu, select **Change Service Agent attributes (option 1)**. The command parameter Report remote problems must be set to ***YES**.
  - The Activation password (also entered using the Change Service Agent attributes menu option) must be supplied. Contact your IBM Service Representative to obtain the activation password.
- On each endpoint system (Service Requester):
  - Service Agent must be activated.
  - Service Agent must be configured to report problems to a central system (Service Provider).

    This is controlled by a Service Agent attribute on each endpoint system. To change this attribute, from the Service Agent main menu, select **Change Service Agent attributes (option 1)**. The command parameter “Report problem to” must specify the control point name and the network ID of the central system (Service Provider).

There are several Software Knowledge Base articles (as shown in Table 7-1 on page 82) that are useful to configure Service Agent and System Management/400 to work together to provide centralized problem reporting.

Table 7-1 Software Knowledge Base articles for System Manager/400

Document title	Document number
“Installation, Configuration, and Start-Up for System View System Manager/400”	14720929
“System View System Manager/400 Communication Requirements”	14425526
“Logging Remote Problems Using System Manager and Service Agent”	20310946

For more information about configuring and using System Manager, refer to the document, *System Manager Use*, SC41-5321, at this Web site:

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/books/sc415321.pdf

Service information

In a network environment, Service Agent and Management Central can work together to collect and send service information to IBM through a central system.

Management Central on the central system provides an Extreme Support wizard to help you configure the collection and transmission of service information to IBM. For instructions about configuring Extreme Support to use Service Agent, see the i5/OS Information Center topic entitled Configure Extreme Support.

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=/rzaji/rzajiextsptcfg.htm

Figure 7-3 on page 83 shows iSeries® Navigator and Extreme Support on your system.

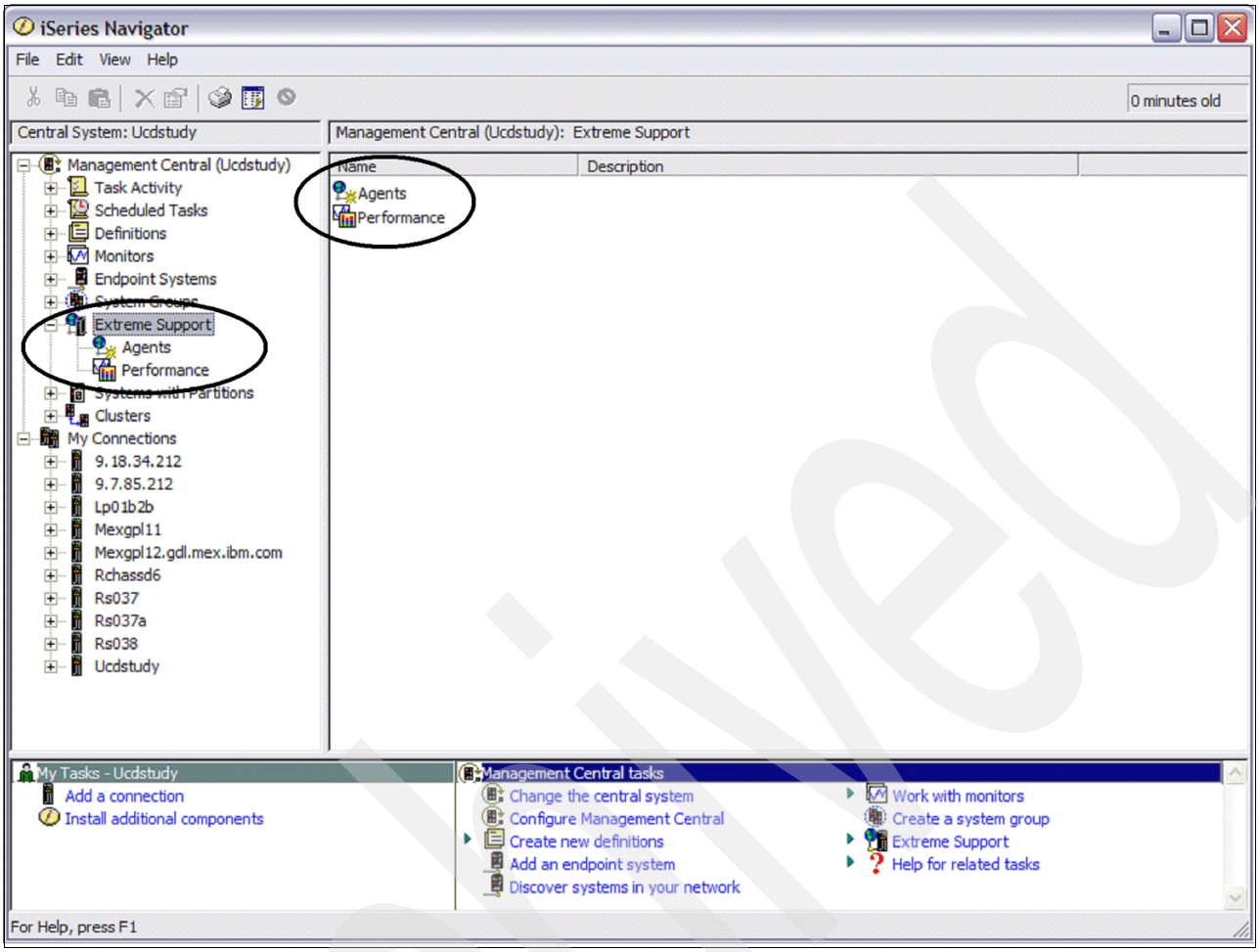


Figure 7-3 Management Central, Extreme Support menus

For information about using Management Central, see the i5/OS Information Center topic about Management Central:

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=/rzaih/rzaih1.htm

When Service Agent is activated, jobs are scheduled to handle the collection and transmission of service information. If iSeries Navigator and Management Central are also used to schedule the collection and transmission of service information, the result can be duplicate processing. To avoid this duplication, after you have successfully scheduled the collection and transmission of service information through iSeries Navigator, enter the following command on each endpoint system:

```
RMVJOBSCDE JOB(QS9SA*) ENTRYNBR(*ALL)
```

This command removes the service information collection and transmission jobs that were created during the initial activation of Service Agent. Each time that the Service Agent attributes are changed, the service information and collection jobs are added.

7.7 User Interface: Character-based compared to GUI

The user interface for Service Agent consists of a native user character-based interface (“green screen” or 5250 application) and a graphical user interface (GUI). You can use the native user interface to access all aspects of Service Agent: problem reporting and service information collection. You can use the GUI to access service information collection, but not problem reporting.

The GUI provides for centralized service information collection. Service Agent leverages Management Central for this centralized service information collection. Centralized service information collection allows service information to be collected from multiple endpoint systems to a central system. The service information is then sent from the central system to IBM.

The GUI is part of iSeries Navigator and is found as an agent under Extreme Support, as shown in Figure 7-4.

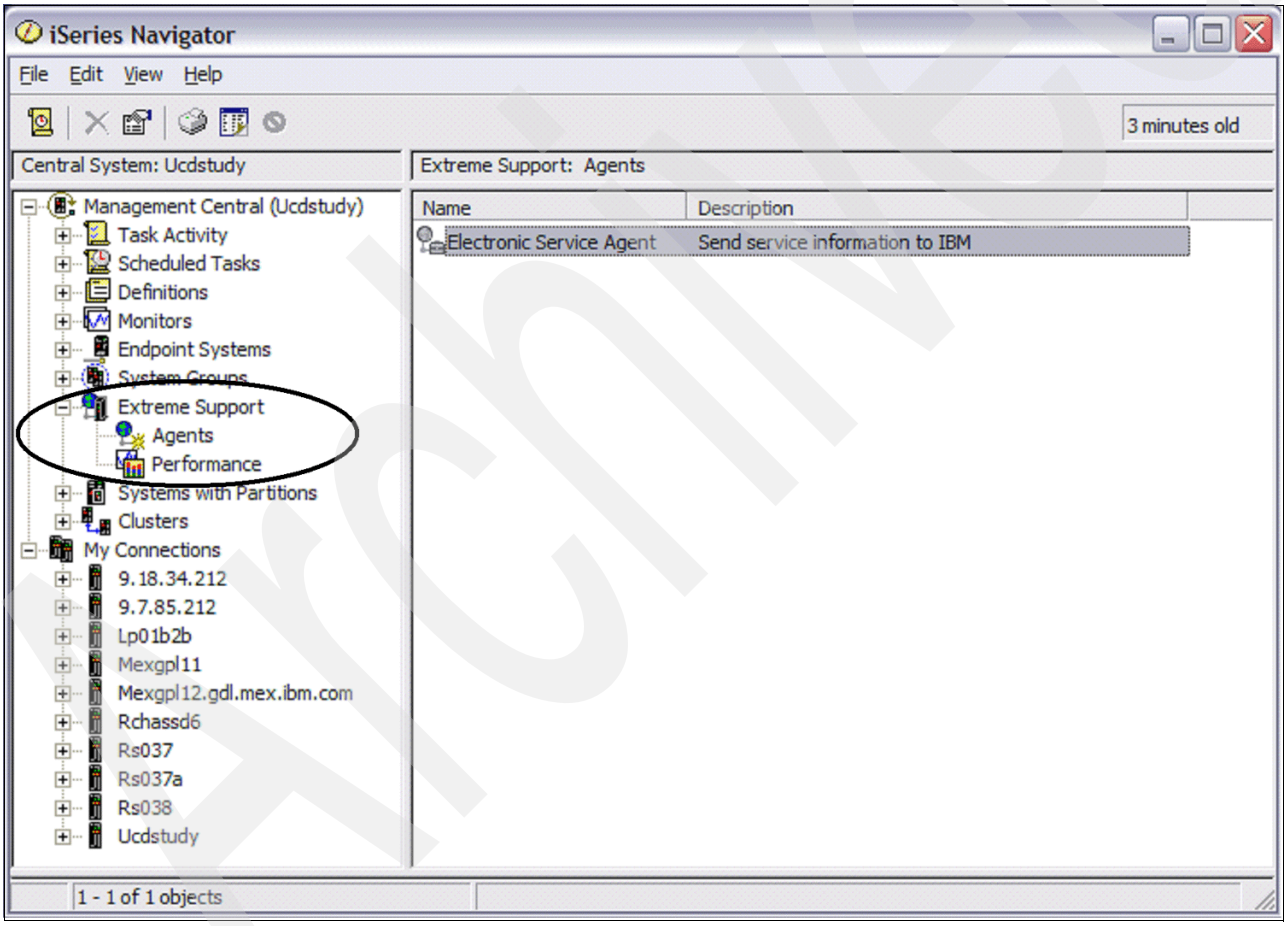


Figure 7-4 iSeries Navigator, Extreme Support Agents

The Service Agent main menu (“green screen”), as shown in Figure 7-5 on page 85, is used to update the configuration, authorize your IBM ID for the system, view reports or logs, send test problems, and send service information manually. To access the Service Agent main menu, enter:

```
GO SERVICE
```

```
   1. Change Service Agent attributes
   2. Run service information collection
   3. Authorize users to access service information

Information
   4. Display problem reporting information
   5. Display service information collection
   6. Display service registration information
   7. Reports

Jobs
   8. End jobs
   9. Start jobs
  10. Work with jobs

Problem determination
  11. Change Service Agent job logging
  12. Change product activity log analysis
  13. Work with Service Agent spooled files
  14. Display audit log
  15. Send test problem
  16. Work with threshold table
  17. Verify Service Agent connection
  18. Service Configuration menu
```

Figure 7-5 Service Agent for System i main menu

7.8 Keeping Service Agent current

There are several ways to make it easy to ensure that you have the most recent Service Agent code:

- Auto PTF
- Group PTF
- Subscription Service
- Recommended Fixes Web page

7.8.1 Auto PTF

Auto PTF checks the system or logical partition to determine if PTFs deemed critical by IBM Service and PTFs needed to ensure Service Agent's well-being are on the system or logical partition. If PTFs are needed, fix request entries containing the PTF numbers to order are created in the Problem Log, and the fix requests are sent to IBM. You can control whether Auto PTF is enabled or not, and if enabled, the day on which it runs, and whether it downloads PTFs, PTF cover letters only, or nothing. These controls are part of the Service Agent attributes and can be changed by selecting from the Service Agent main menu, Change Service Agent attributes. The command parameter is *Auto PTF*.

7.8.2 Group PTF

A group PTF is a collection of PTFs that are related to a single function, such as Service Agent. This collection is identified by a single PTF number so that the entire collection is easy to manage. You can order and install the entire collection of PTFs that are important for Service Agent on V5R4 by ordering and applying PTF SF99316. Like cumulative PTF packages, group PTFs are updated periodically as new fixes become available that affect the

function. The IBM Electronic Service Agent group PTF helps you ensure that you have the most recent PTFs for Service Agent and for components upon which Service Agent depends. PTFs in the Service Agent group include those for ECS, Connection Manager (Universal Connection), Management Central, and Java.

7.8.3 Subscription Service

Subscription Service for System i5™ provides technical bulletins on various support topics including changes and updates to group PTFs. You can subscribe to the topics in which you are interested, and when new or updated bulletins become available, an e-mail is sent with the technical bulletins and links to more information.

The Service Agent group PTF is included in the IBM System i Subscription Service. You can add the IBM Electronic Service Agent group to your current list of group PTF notifications to receive when updates occur in the group. Register for the V5R4 (and V5R3) IBM Electronic Service Agent notifications using the following steps:

1. Go to the Support for System i Web site, located at:

   `http://www.ibm.com/servers/eserver/support/iseries/index.html`
2. Select **System i5 Subscription Service** under the Popular Links category.
3. Select the **Subscribe/Setup** tab.
4. Select **Continue** to sign in with your IBM ID.
5. If you do not have an IBM ID, use the IBM ID link to register for one.
6. After signing in, check the box next to the IBM Electronic Service Agent group.
7. Click **Save preferences data** to save your update.

7.8.4 Recommended Fixes Web page

You can get the latest fix information directly from the Rochester Support Center without a telephone call. You can locate the fix for a specific problem or obtain the latest fixes for IBM Electronic Service Agent.

The following link is for the IBM System i Recommended Fixes Web page. At this page, select your release and then select a topic of IBM Electronic Service Agent:

`http://www.ibm.com/eserver/iseries/support/s_dir/slkbase.nsf/recommendedfixes`

7.9 Controls

There are several settings that control the way Service Agent reports problems, tests connectivity to IBM, and notifies you of its activities. You can change these settings to fit your environment.

7.9.1 Threshold table

Service Agent uses the threshold table to determine the action to take for problem log and product activity log entries. Based on the origin of the error, the Active indicator or the threshold value is used to determine if an error is reported to IBM.

When a problem surfaces in the problem log, the Active indicator in the threshold table is used to determine whether the problem needs to be reported to IBM. Service Agent reports errors for a device System Reference Code (SRC) that is active. If the SRC is not in the

threshold table, whether the problem must be reported has been predetermined by Licensed Internal Code processing.

When a problem surfaces in the product activity log, the threshold value in the threshold table is used to determine whether the problem needs to be reported to IBM. Service Agent reports errors for an active SRC that have occurred the specified number of times within a seven day period. If the threshold value is 0, the error is not reported from the product activity log. Service Agent analyzes the product activity log periodically throughout the day. The frequency of the analysis is controlled by a Service Agent attribute. Analysis can be enabled or disabled and the interval, including the time at which analysis is to begin, can be changed. To change the product activity log analysis settings, do the following:

1. From the Service Agent main menu, select **Change Service Agent attributes (option 1)**.
2. Press Enter to display additional settings.
3. For product activity log analysis, enter the desired values.

You can change the threshold table using the threshold table editor. You can add, remove, or change devices and SRCs. This includes changing the active indicator and the threshold value for a device SRC. To change the threshold table, from the Service Agent main menu, select **Work with threshold table (option 16)**.

7.9.2 Delay problem reporting

This new function helps avoid unnecessary interruptions to your operations. Every SRC reported by the system does not require immediate action. One example of SRCs that do not require immediate action are predictive (non-failure) SRCs, such as those which notify you that the DASD cache batteries need replacement during the next 90 days. The battery end-of-life SRCs reported and handled outside of normal business hours result in unnecessary interruptions to your operations.

To avoid unnecessary interruptions and to avoid the concerns that these SRCs cause for your off-shift personnel, it is preferable to report these SRCs the next business day and to schedule replacement at a future date.

IBM Electronic Service Agent provides a way for you or your IBM Service Representative to set parameters that allow SRCs to be reported only during normal business hours. If the SRC occurs off-hours, reporting is delayed until the next business day.

To ensure that you have this functionality, install the latest Service Agent PTFs.

How the delay function works

To enable the delay function, a new command, Delay Service Agent Problem, is available. To use it:

1. On the command line, enter the command DLYSRVAGTP.
2. Next, press F4 (prompt).

You see the parameters as shown in Table 7-2 on page 88.

Table 7-2 Delay Problem reporting parameters

Parameter name	Comments
Enable	*Yes enables the delay function. Group B SRCs are reported only on the specified report days between the report start time and the report end time (normal business hours). If the SRC occurs outside of the specified days and times, the error is held until a reporting day and time is reached. A parameter value of *NO disables the delay function. Errors are reported as they occur. The default is *YES.
Report day	The days during which Group B SRCs are reported. If an SRC occurs on a day that has not been specified, the error is held until a reporting day is reached. A parameter value of *ALL means all days of the week. The default is *MON *TUE *WED *THU *FRI.
Report start time	The time of day that defines the start of normal business hours. Group B SRCs can be reported to IBM between the report start time and the report end time. Restriction: Start time and end time must both be either before midnight or after midnight. The default is 08:00.
Report end time	The time of day that defines the end of normal business hours. Group B SRCs can be reported to IBM between the report start time and the report end time. Restriction: Start time and end time must both be either before midnight or after midnight. The default is 17:00.

A new threshold table group value of “B” identifies SRCs that need to be reported to IBM only during normal business hours. Figure 7-6 shows a Group B SRC in the Service Agent threshold table. Installing the PTF that provides this function also updates the threshold table.

```
                    Work with Device SRCs

Device . . . . . :   2748

Type options, press Enter.
   1=Add   2=Change   4=Remove

Opt  SRC   Active  Threshold  Group  Description
Changed

     3400   Yes        0             STG I/O ADAP ERROR
     8009   Yes        0        B    CACHE BATT EXP 90 DAYS
Yes
```

Figure 7-6 Service Agent threshold table for Group B SRCs

7.9.3 Service Agent activity

You can receive notifications about Service Agent activity, or you can use the menu options to display information about problem reporting activity and service information collection activity.

Notifications

You can receive notification of Service Agent activity through i5/OS messages. Notifications are sent for activities, such as reporting a problem or analyzing the problem activity log. Notifications are also sent when Service Agent is unable to complete a task, such as reporting a problem to IBM.

To specify the user IDs to receive notifications:

1. From the Service Agent main menu, select **Change Service Agent attributes (option 1)**.
2. Press Enter to display additional settings.
3. For Notify user ID, enter the user IDs to receive the notifications.

In addition to any user profiles you specify, the system operator (QSYSOPR) and QSRV user profiles also receive messages. It is not possible to prevent notifications from being sent to these user profiles.

Problem reporting

To display Service Agent problem reporting activity, select from the Service agent main menu, Display problem reporting information. Figure 7-7 is a screen capture showing a sample of this information.

```
                    Display Problem Reporting Information

Auto report  . . . . . . . . . . . . . :   *YES

Auto report retry:
   Retry  . . . . . . . . . . . . . . . :   *YES
   Frequency  . . . . . . . . . . . . . :    15
   Number of times to retry . . . . . . :     3
   Notify user  . . . . . . . . . . . . :   *YES


 Problem                 Assigned                 -----Created------
 ID          Status      Number     Origin        Date      Time
 0701230399  Reported    66123      LOCAL         01/15/07  17:28:07
 0701225624  Prepared                LOCAL         01/12/07  07:27:49
 0701225363  Prepared                LOCAL         01/12/07  07:23:17
 0701161970  Reported    65653      LOCAL         01/11/07  18:03:01
 0701160209  Prepared                LOCAL         01/11/07  17:32:16
 0701157210  Reported    65645      LOCAL         01/11/07  16:39:54
 0700866092  Reported    50862      LOCAL         01/08/07  17:54:44
 0700866091  Reported    50631      LOCAL         01/08/07  10:41:48
                                                                    More...
 F3=Exit    F6=Print    F11=Alternate view    F12=Cancel
```

Figure 7-7 SA main menu, Display Problem Reporting Information

In addition to these columns, the following information is provided by the Alternate views (F11):

- Last attempt date and time
- Number of attempts
- Last change date and time
- Whether service information was sent or not

Service information

You can display Service Agent service information collection activity by selecting from the Service agent main menu, Display service information collection. Figure 7-8 is a screen capture showing a sample of this information.

```
                    Display Service Information Collection

System or logical partition  . . . . . :   *LOCAL


Schedule:
  Collect time . . . . . . . . . . . . . :   10:55:00
  Send time  . . . . . . . . . . . . . . :   10:55:00

Collect  . . . . . . . . . . . . . . . . :   *NO


Service               -----Last run-----  ----Last send-----
 Information           Date      Time      Date      Time
 SOFTWARE              07/14/06  17:14:36  07/14/06  17:14:43
 SFWLIC                07/14/06  17:14:46  07/14/06  17:14:43
 WRKORDINF             07/14/06  17:14:48
 SFWAUDLOG             07/14/06  17:14:50  07/14/06  17:14:53
 PTF                   07/14/06  17:14:55  07/14/06  17:15:21
 PTFGRP                07/14/06  17:15:29  07/14/06  17:15:33
 SYSVAL                07/14/06  17:15:35  07/14/06  17:15:38
                                                              More...
 F3=Exit    F6=Print    F11=Alt. view    F12=Cancel
 (C) COPYRIGHT IBM CORP. 2003, 2005.
```

Figure 7-8 Service Agent main menu, Display Service Information Collection

In addition to these columns, the *Last collect date and time* is provided by the alternate view (F11).

Audit log

The audit log contains information about Service Agent activity and errors that have been encountered. Entries include starting the Service Agent monitoring jobs, detecting an error, reporting or bypassing an error, and successful and unsuccessful attempts to connect to IBM. This information is in English. Its purpose is to assist IBM support personnel in problem determination. Figure 7-9 on page 91 is a sample from an audit log.

```
000001 06/10/25 10:02:39  QS9PRBSND : Service Call Successful for Problem 06298.
000002                    PMR is 24596.
000003 06/10/25 10:02:39  QS9PRBSND : Collect PAL Service Information for PMR: 24596
000004 06/10/25 10:02:42  QS9PRBSND : Command failed: SBMJOB CMD(WRKSRVAGT
000005                    TYPE(*SRVINF) COLSRVINF(*NO) SNDSRVINF(*YES) SRVINF(*PRBID))
000006                    JOB(QSJPRBRPT) USER(HAGEN) errno 0
000007 06/10/25 10:04:06  QS9PRBMON: NOT ACTIVE ON PROBLEM 0629834567: B600 710
000008 06/10/25 10:04:10  QS9PRBMON: NOT ACTIVE ON PROBLEM 0629834571: B600 710
000009 06/10/25 10:04:13  QS9PRBMON: NOT ACTIVE ON PROBLEM 0629834573: B600 710
000010 06/10/25 10:10:04  NO SERVICE CALL FOR PROBLEM ID = 0629834907 DUE TO MULTIPLE
000011                    CALL BLOCK PLACED AT 06/10/25 09:58:53
000012 06/10/25 10:13:52  QS9PRBMON: NOT ACTIVE ON PROBLEM 0629835125: B600 710
000013 06/10/25 10:14:46  QS9PRBMON: NOT ACTIVE ON PROBLEM 0629835177: B600 710
000014 06/10/26 15:06:05  QS9PRBMON: NOT ACTIVE ON PROBLEM 0629951844: B600 710
000015 06/10/27 14:09:14  QS9PALMON  job starting.
000016 06/10/27 14:09:19  QS9PRBMON  job starting.
```

Figure 7-9 Service Agent audit log sample

7.9.4 Automatic connection verification (Heartbeat)

Service Agent provides a way to automatically periodically test the connection to IBM. At the specified interval, Service Agent connects to IBM and sends a transaction to indicate that the connection was successful.

The interval is controlled by a Service Agent attribute. To specify the interval for the automatic connection verification test:

1. From the Service Agent main menu, select **Change Service Agent attributes (option 1)**.
2. Press Enter to display additional settings.
3. For Connection verification timer, enter the specified interval in days.

7.9.5 Line control

It is possible for the service configuration to share a resource with other applications on the system. When this is the case, for service configurations that use a line description, Service Agent can vary off a line that is in connect pending status that shares the same resource as the service line description. No other action is taken for any other line status. After Service Agent has completed its use of the resource, the line is returned to the state in which Service Agent found it prior to using it.

The service line varies based on the type of service configuration. If the Universal Connection (TCP/IP) is used for the service connection, then line description QESPPLIN is used; otherwise, it is an SDLC connection and line description QESLINE is used. In the case of the Universal Connection, if it is configured to use a Virtual Private Network (VPN), then line control is not used, and Service Agent does not attempt to vary off the line.

You can control whether line control is enabled or not, and if enabled, the configuration objects associated with the resource that it is allowed to vary off. These controls are part of the Service Agent attributes and can be changed by selecting from the Service Agent main menu, Change Service Agent attributes. The command parameter is Line control.

7.10 Software problem reporting

Service Agent reports software problems detected by the i5/OS Service Monitor, which is a service function that is used to monitor the system for specific conditions. The Service Monitor uses policy information to determine which problems to process. The policy information defines the behavior for identifying and reporting software problems. When a problem is reported, if no solution is found, Service Agent automatically sends the primary problem documentation to IBM. Documentation consists of primary and secondary information. The secondary documentation is not sent automatically.

If IBM Support requires the secondary documentation, it can be sent manually (as shown in Figure 7-10):

1. From the Service Agent main menu, select **Run service information collection (Option 2).**
2. Change the following parameters to the specified values:
   - Service information: `*PRBID`

     This indicates that service information corresponding to a specific problem is to be processed.
   - Problem identifier: Specify the problem log ID for the problem
   - Information for a problem: `*SECONDARY`

```
                    Work with Service Agent (WRKSRVAGT)

Type choices, press Enter.

Collect information  . . . . . .   *YES          *YES, *NO
Send information . . . . . . . .   *YES          *YES, *NO
Service information  . . . . . > *PRBID         *ALL, *PRBID
              + for more values
Problem identifier . . . . . .   0417737041     Character value, *ALL
Information for a problem  . . .   *SECONDARY    *ALL, *PRIMARY, *SECONDARY

                                                                      Bottom
F3=Exit    F4=Prompt    F5=Refresh    F12=Cancel    F13=How to use this display
F24=More keys
```

Figure 7-10 Command prompts for software problem reporting

7.11 Batch activation

You can activate IBM Electronic Service Agent in a batch environment. This is helpful for environments with many systems. You can write a program to perform the activation steps that otherwise occur manually.

For details, including a sample program, see the i5/OS Information Center Service Agent topic entitled Batch activation, at:

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=/rzaji/batch_activation.htm

7.12 Authorizing users to view or use service information

Authorized users can view or use service information for a system through the Electronic Services Web site. To authorize users to view or use service information for a specific system, from the Service Agent main menu on that system, select **Authorize users to access service information (option 3)**. Enter the IBM ID to authorize.

To obtain an IBM ID for use on many IBM Web sites, go to:

https://www.ibm.com/account/profile/us?page=reg

7.13 HMC Service Agent

Four major components make up the Service Agent environment on HMC machines:

- The *Electronic Server System (ESS)* process runs only on the gateway HMC. The ESS handles all requests for data input and retrieval from the centralized database.
- The *On Demand Server (ODS)* process runs on all HMCs that are defined and handles all Service Agent communication activities for that host. The ODS sends data to the ESS process as necessary or makes a request to Service Agent Connection Manager (SACM) to call IBM. Events from the Service Focal Point (SFP) are reported to IBM directly using an Internet connection or a modem that is attached to the gateway server. Service Agent calls IBM to report that it is healthy one time in every health-check interval.
- *Service Agent Connection Manager* is a stand-alone process. You can configure it to communicate with IBM using an existing Internet connection or modem. It can exist on any HMC or stand-alone System i5 machine and can support multiple Service Agent Gateway connections.
- The *User Interface* allows you to set up and define HMCs that Service Agent monitors. The graphical user interface (GUI) is invoked from *Web-based System Manager (WSM)* by:
  a. Select **Service Agent** from the Service Applications.
  b. From the WSM service menu, you select **TASKS** for the Service Agent User Interface.
  c. You use the User Interface for advanced functions and customization of the system, as well as to configure complex systems and multilevel networks.

7.13.1 Planning

Establish the overall HMC environment before you activate Service Agent. Do not start Service Agent processes if the network is not configured on the gateway or your HMC.

Review and complete the following items:

1. On new installations, the HMC host name is a default name. Assign it a new name that suits the client's network environment.
2. On the HMC gateway, ensure that the modem and phone line are connected if they are used. Check the physical connections to determine that they are connected.
3. If you use the Internet, make sure that the HMC has connectivity to the network.

4. If HMC is a client, start Service Agent only after the network is set up properly.
5. After the host name is assigned, determine the type of Service Agent to apply: gateway or client.

Figure 7-11 shows the HMC high-level activation flow.

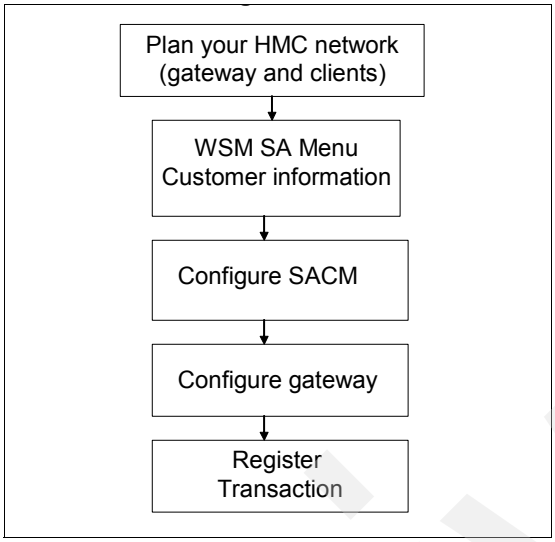


Figure 7-11 HMC Service Agent activation flow

7.13.2 Installation and activation

HMC machines have Service Agent installed as part of the HMC code. Service Agent appears on the HMC menu.

Complete the following steps to activate HMC Service Agents.

1. In the Navigation Area on the HMC menu, select **Service Applications** → **Service Agent**, as shown in Figure 7-12 on page 95.

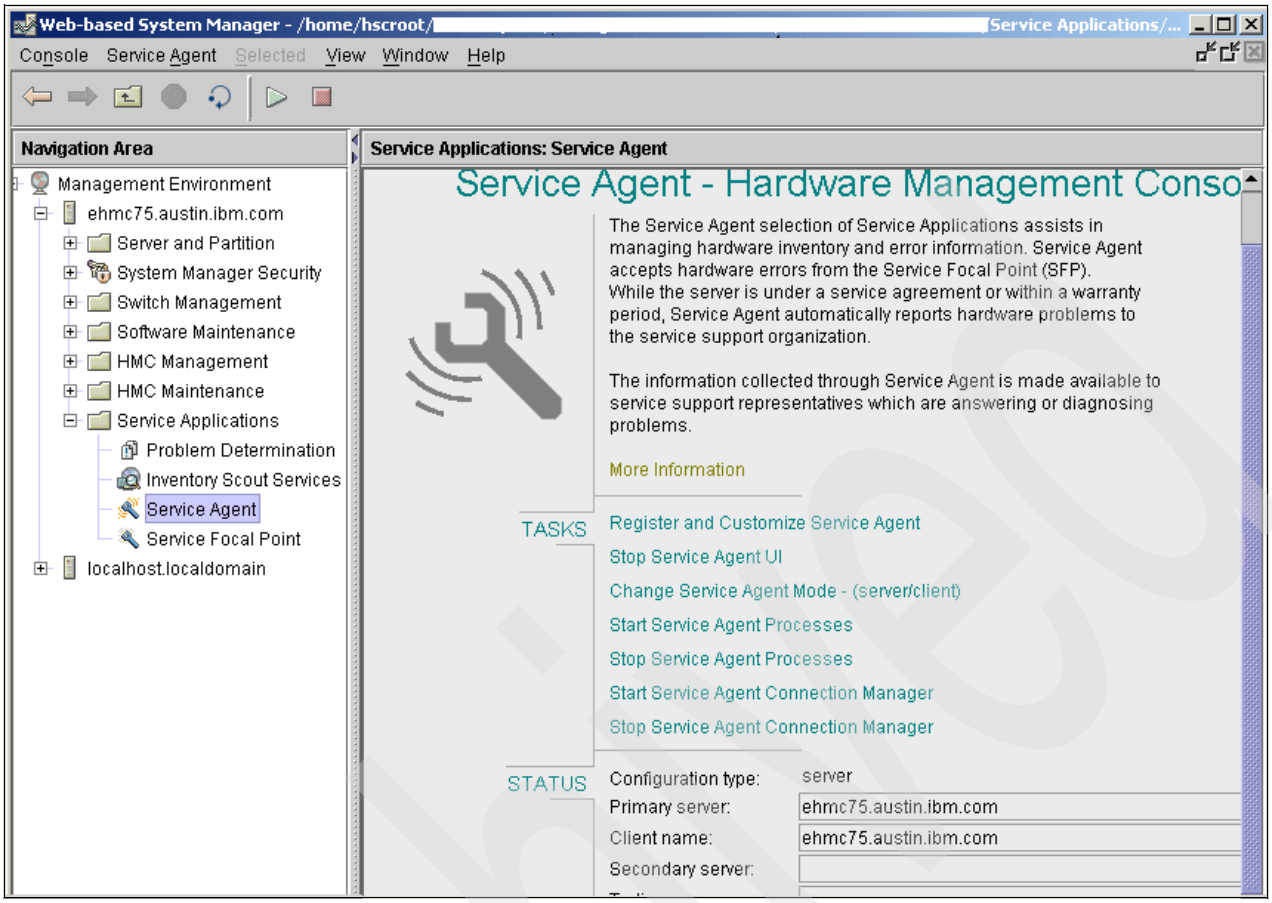


Figure 7-12 HMC Service Agent menu

2. Service Agent detects whether it is activated. If it is not, you see the window shown in Figure 7-13. Verify or update the information, and then click **Continue**.

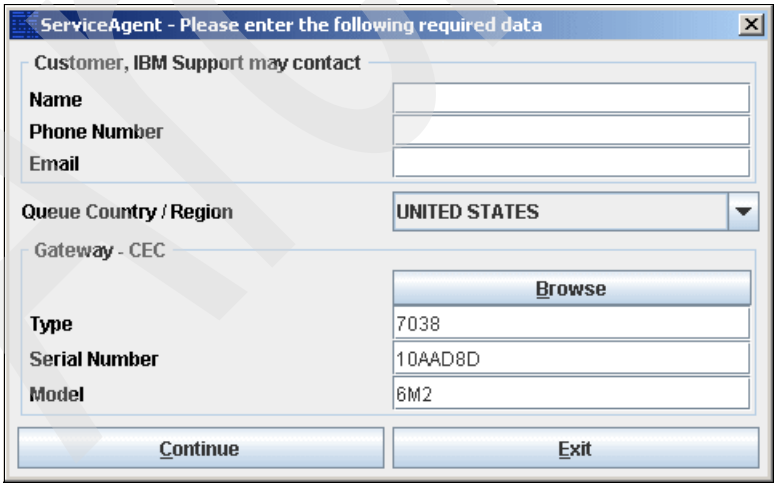


Figure 7-13 HMC Service Agent activation wizard (Part 1 of 2)

3. Now you see the window shown in Figure 7-14. Type the requested information and click **OK**.

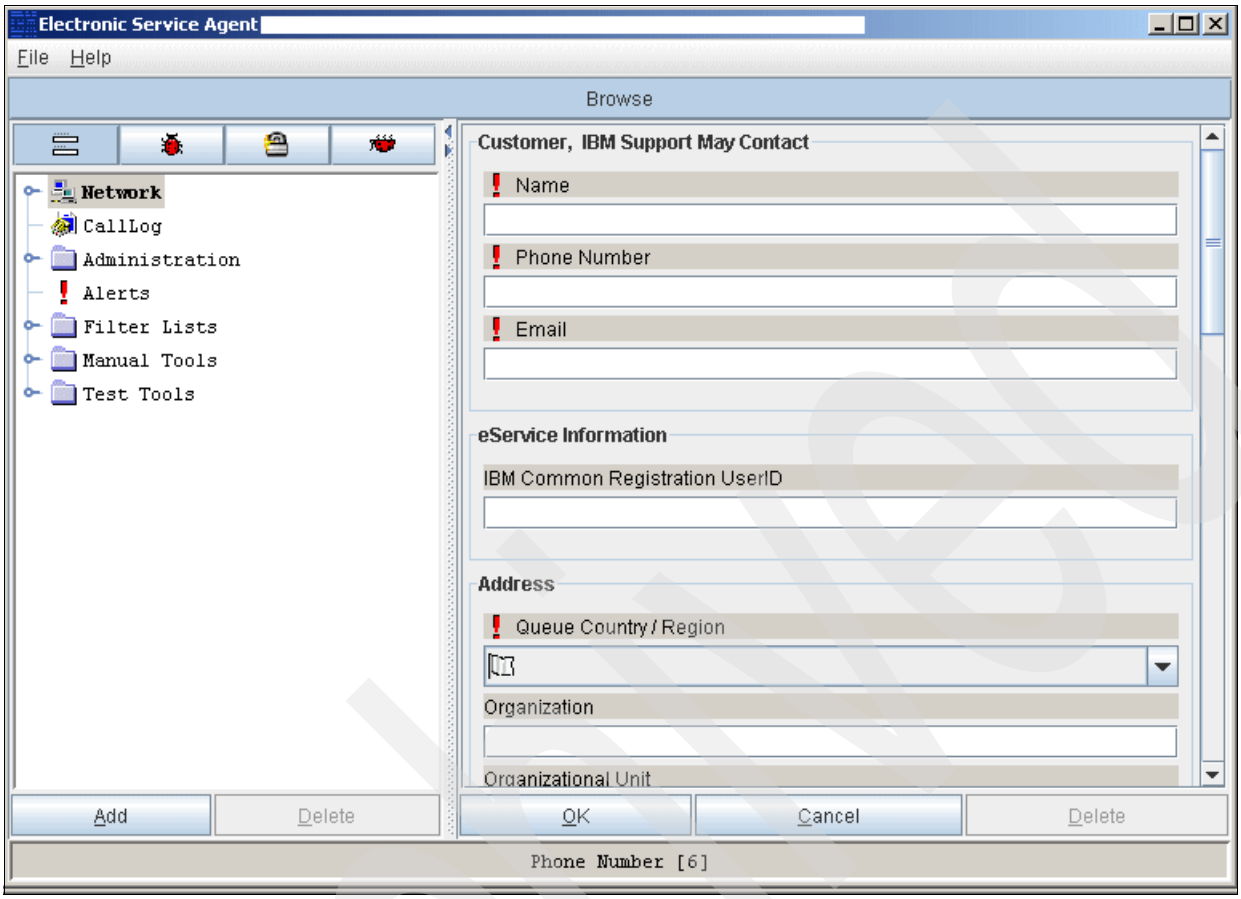


Figure 7-14 HMC Service Agent activation wizard (Part 2 of 2)

7.13.3 Maintenance

You update the HMC Service Agent with new releases of HMC code. Selecting **Service Applications** → **Service Agent** invokes the HMC Service Agent GUI from the WSM.

The Service Agent menu has two major sections, TASKS and STATUS, as shown in Figure 7-12 on page 95:

- In the TASKS section, you start and stop a process, change the function, update the host name, and access the user interface.
- In the STATUS section, you see information about how this HMC is configured (server/client) and the status of the Service Agent processes.

8

IBM Electronic Service Agent for System p

This chapter provides background and information about Service Agent on the System p platform. This chapter is for users and system administrators who are familiar with or have a working knowledge of AIX and RISC architecture as it pertains to basic operation of IBM System p.

8.1 Electronic Service Agent on System p

Service Agent on the System p platform began with Service Director on RS/6000® in 1994. It served as a problem detection and submission tool on desktop Models 7011 through 7015 in the United States. During the past decade, more models and function have been added, hence the migration to the Service Agent title in 2001.

Electronic Service Agent for System p is now available on all models of the System p platform in all countries (regions). Today, the Service Agent for System p submits problems automatically and collects machine inventory information for both the stand-alone and the Hardware Management Console (HMC) environments.

The following information is from the current *Electronic Service Agent for System p User Guide,* SC38-7105, and *Electronic Service Agent for System p Hardware Management Console (HMC)*, SC38-7107. Refer to these user guides for comprehensive information about these subjects. All the Service Agent graphical user interface (GUI) help text is directly from the user guides.

8.1.1 Overview of Service Agent on System p

Figure 8-1 shows how your environment has the potential for a stand-alone configuration, HMC machines in a configuration, or both types of configuration.

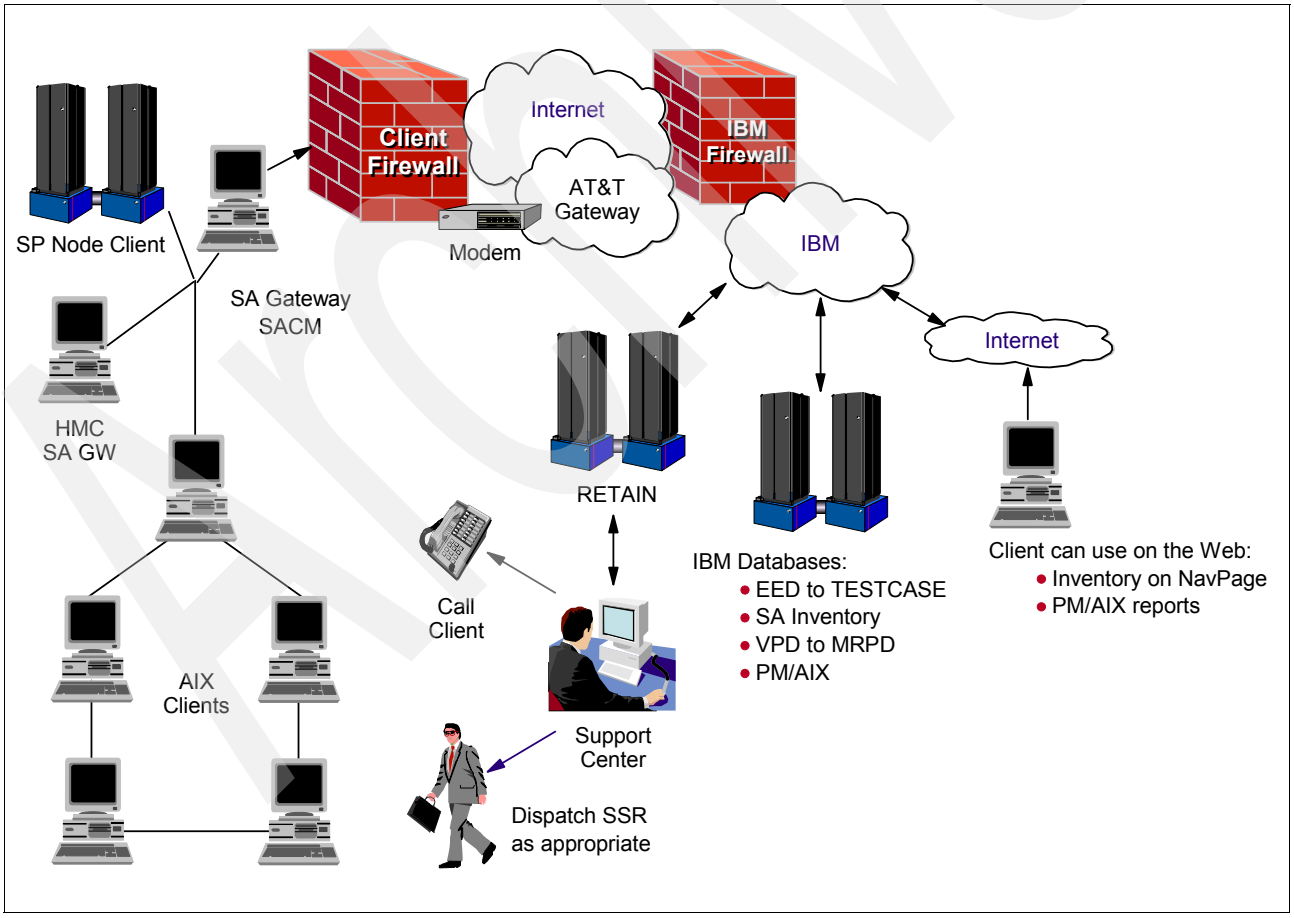


Figure 8-1 Service Agent for System p network view

Service Agent is flexible, and you can configure it to your environment. Service Agent works with clients by reporting through AIX gateways or the HMC client to the HMC gateway. All Service Agent communication flows through the Service Agent Connection Manager (SACM) on either AIX or the HMC host to IBM.

The choices of communication to IBM are either modem or Internet. The automatic problem submission path and the inventory paths are through secure firewalls that go into the appropriate IBM databases. You can use IBM Web sites to view the Service Agent inventory, Performance Management reports, and other offerings. The HMC Web-based System Manager (WSM) and System Management Interface Tool (SMIT) present Service Agent menus or interfaces.

The HMC WSM menus allow control and setup of Service Agent. The Service Agent User Interface (SAUI) is used for various functions, such as setting local user notification entries, customizing the system, and displaying local Service Agent information. You start and stop the application, as well as perform basic configuration, through the WSM menu.

The SMIT-derived menus in an AIX environment enable you to control management of the application and select the user interface. They also display the application status.

8.1.2 Key tasks and functions

The Electronic Service Agent functions include:

- Use of Internet access or modem phone line connection to IBM
- Automatic problem analysis and submission based on defined thresholds
- Automatic client notification and view of hardware event logs of any automatic problems
- High-availability cluster multiprocessing (HACMP™) support for full fallback, including high-availability cluster workstation (HACWS) for 9076
- Vital product data (VPD) or machine inventory information sent to IBM
- Software product information install and fix sent to IBM
- Capacity Upgrade on Demand (CUoD) enabled on non-HMC servers
- Using Performance Management, automatic reporting of PM/AIX data to IBM

8.1.3 Machine types and models that are eligible for Service Agent

Service Agent supports all System p machine types. This includes the 9076 (SP) or cluster configurations. All machine types that have concurrent diagnostics installed and are under IBM warranty or maintenance contracts (for problem submission) are eligible.

8.1.4 Service Agent Connection Manager

One of the major improvements or simplifications in Version 3.1 is the introduction of the SACM. The SACM is a stand-alone process that can be configured to communicate with IBM using an existing Internet connection or modem. This application installs with the Service Agent AIX code on the Service Agent gateway, but it can be installed as stand-alone code on any supported platform. It can exist on any HMC or stand-alone AIX machine and can support multiple Service Agent gateway connections.

The features that enable enhanced security, as shown in Figure 8-2, help to:

- Provide firewall support using either a proxy service or provide for traffic to pass through a Network Address Translation (NAT) device, such as a Cisco PIX Firewall
- Provide a single point of exit from the client environment
- Ensure Inter-Enterprise Security (IES) compliance

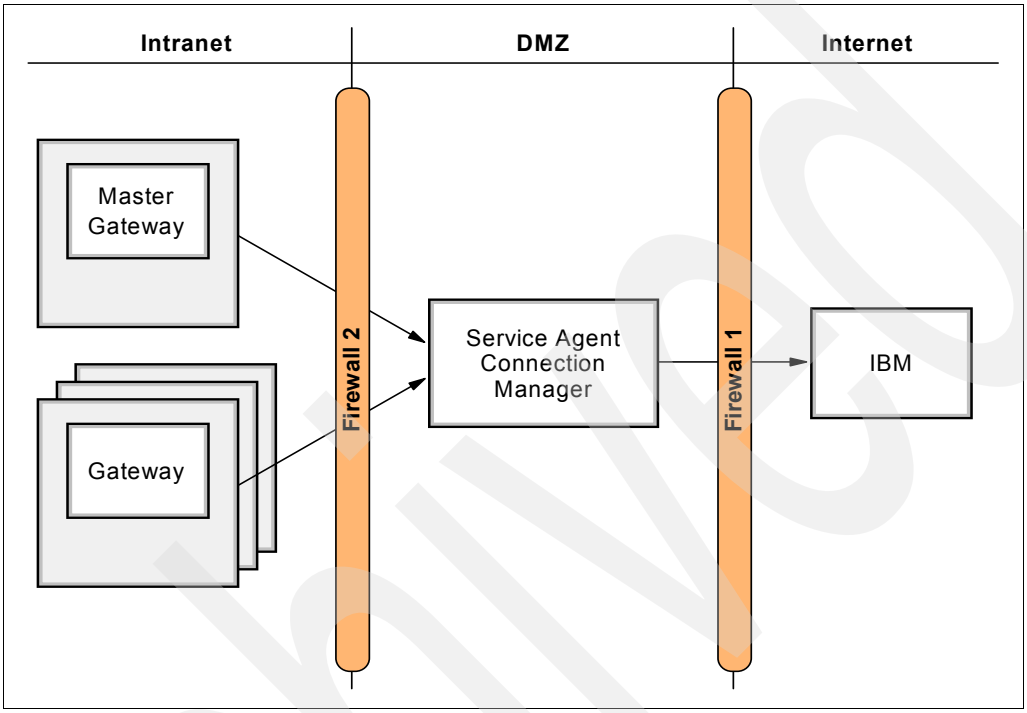


Figure 8-2 Sample configuration using firewalls and SACM

8.2 Stand-alone environment: Planning and prerequisites

Early planning can save you valuable time and prevent aggravation later. Understanding how to set up the Service Agent application to best cover your information technology (IT) environment makes the Service Agent experience much more enjoyable.

Consider the following items to assist in your decision making and placement of the Service Agent components:

- Ensure that your System p is at AIX Version 4.2.1 or higher with concurrent diagnostics installed. IBM diagnostics must be installed on every monitored machine. Error logging and error log analysis must be enabled.
- Java is required on all monitored machines. Java for AIX V4.3.3 or higher is on the system disk. You obtain Java from another source for machines with AIX versions earlier than 4.3.3.
- Note the correct memory needed for various components of Service Agent:
  - The minimum GUI is 10 MB. The maximum is 32 MB.
  - For a 50 system network, 20 MB are required.
  - For a 100 system network, 25 MB are required.
  - Electronic Server System (ESS) requires 64 MB.
  - On Demand Server (ODS) requires 64 MB.

- Ensure that the person who is installing Service Agent has root authority on the gateway machine. This person must have access to a root-authorized window while installing Service Agent.
- All communications between the Service Agent gateway and IBM are now encrypted and secure using Java Secure Sockets Layer (SSL) regardless of the communication method that is selected:
  - Is an existing high-speed Internet access available to communicate with IBM? If no Internet access is available, then you must meet all dialer prerequisites.
  - Is a modem required? Only outbound calls are required by Service Agent, so you must disable the auto answer capability of the modem. Refer to the local procedures in your country (region) for asynchronous modem requirements for speed and error correction.
- Determine which host best supports the Connection Manager.
- Identify whether Service Agent needs to support any High Availability (HA) configurations.
- Verify whether an HMC host name and network are established and defined.
- Determine the number of Service Agent gateway machines that need to be set up to cover the various client hosts:
  - All client configurations must exist in their respective Service Agent gateway databases.
  - For multiple gateway configurations, build the first Service Agent gateway and then export the database to a temp file. Import the temp file database to the second or third gateway as needed.
  - Set up only one Service Agent gateway as a master gateway for each Service Agent Connection Manager (SACM).
- Service Agent needs to know the host name, machine type, model, serial number, and processor ID (field is auto-filled) to monitor managed machines. Service Agent V3.1 attempts to automatically discover the machine type, model, and serial number after the host name is given.

8.2.1 Service Agent code installation and activation

You can obtain the Service Agent code, user guides, and readme files from several sources:

- The AIX Expansion Pack is a collection of additional applications and tools. All complement the AIX operating system with additional packaged software at no additional charge. An Expansion Pack is included with every new order when media is selected.
- The IBM FTP site also provides information about this topic:

  `ftp://ftp.software.ibm.com/aix/service_agent_code/AIX`

8.2.2 Installation

You install the Service Agent code on your system. Then you activate it to start the tasks. Next you untar the svcagent.tar file into the directory from which you want to install it. The restoration of the archive file creates a new sa subdirectory with svcagent modules.

Note: You can install V3.1 over previous versions of Service Agent for System p. Your machine list, communications files, and database remain the same. We recommend that if you migrate from Service Agent V2.4 or earlier, you use the clean installation procedure:

1. To save the configuration, save the current Service Agent gateway database.
2. Remove the current version of Service Agent.
3. Install the new version of Service Agent.
4. To restore the configurations, import the saved Service Agent gateway database.

There are two methods to install Electronic Service Agent:

- Install from the SMIT:
  a. Log on to the gateway server as `root` or sign on using a root-authorized user ID.
  b. To activate the SMIT, type (in lowercase) **`smit`**
  c. Select **Software Installation and Maintenance** → **Install and Update Software** → **Install and Update from Latest Available Software**.
  d. Type the INPUT device/directory (or select install media) and click **OK**.
  e. From the SOFTWARE list, select **svcagent** to do a complete install. Click **OK**.
  f. View the install Summary message result column to ensure that it indicates *Success*.
  g. After the Service Agent program installs, select **DONE**. Depending on your version of AIX, you do this either by clicking DONE, selecting DONE from a list of options, or pressing a PF key shown at the bottom or your display.
  h. Select **CANCEL** to return to the SMIT display.

  You have successfully installed Service Agent.
- Install from a command line:
  a. Log on to the gateway server as `root` or sign on using a root-authorized user ID.
  b. Type the following command **`inutoc /tmp/sa`** and replace *tmp* with the directory where you saved Service Agent.
  c. If this is a new installation, type the command **`installp -YacXd /tmp/sa svcagent`**
  d. Check the installation summary message result column to ensure that it indicates *Success*. Figure 8-3 shows a sample view of the summary message.

```
Installation Summary

Name                        Level           Part        Event       Result
svcagent.cm                 3.0.0.0         USR         APPLY       SUCCESS
svcagent.cm                 3.0.0.0         ROOT        APPLY       SUCCESS
svcagent.client             3.0.0.0         USR         APPLY       SUCCESS
svcagent.client             3.0.0.0         ROOT        APPLY       SUCCESS
svcagent.server             3.0.0.0         USR         APPLY       SUCCESS
svcagent.server             3.0.0.0         ROOT        APPLY       SUCCESS
svcagent.help.en_US         3.0.0.0         USR         APPLY       SUCCESS
```

Figure 8-3 SMIT menu summary results view

You have successfully installed Service Agent.

8.2.3 Activation

Figure 8-4 on page 103 shows the steps to activate Service Agent for System p in a stand-alone environment.

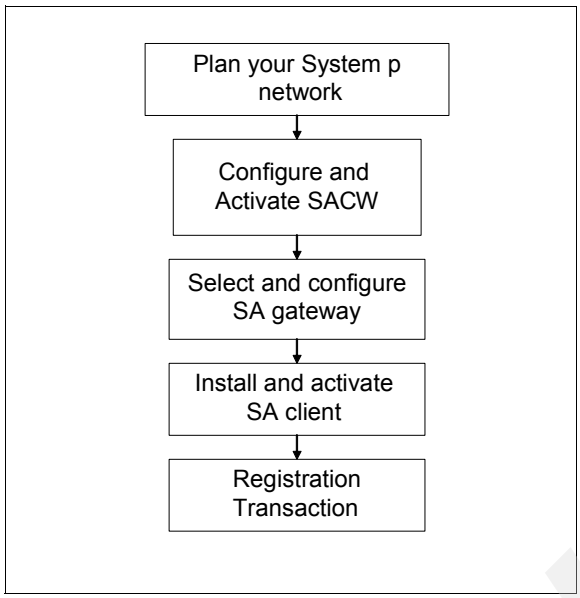


Figure 8-4 Service Agent for System p stand-alone activation flow

After the application is successfully installed, you must manually configure and start the Service Agent processes. This occurs only after the initial or new installation. The upgrade process does not require this step, because Service Agent is already running.

Determining what to configure and start depends on what is installed. Each step uses SMIT Service Agent menus. Figure 8-5 on page 104 shows a sample SMIT main Service Agent menu.

1. Create a new Service Agent gateway:
   a. In the SMIT menu, select **Service Agent** to access the Service Agent menu.
   b. In the SMIT main Service Agent menu, select **Manage Service Agent Connection Manager**.
   c. Then, select **Configure Service Agent Connection Manager**.

Note: The defaults are: *localhost* for host name, *1198* for socket, and *secure* setting. If SACM points to a specific host, the fields must be updated with the correct information. The SACM process must be started before using the Service Agent gateway.

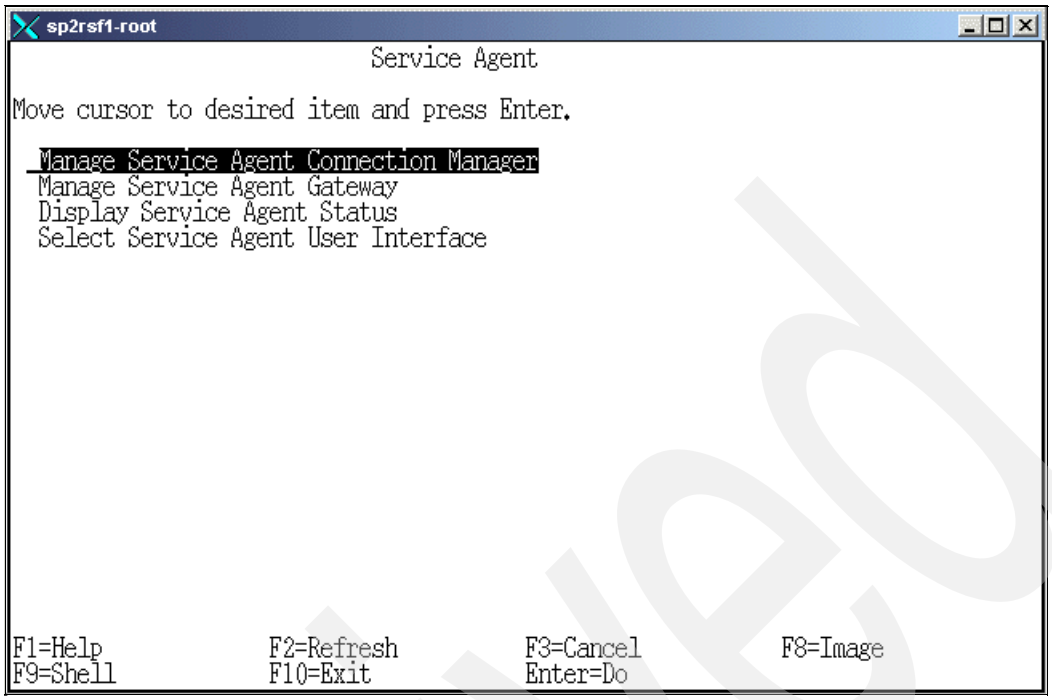


Figure 8-5 SMIT main Service Agent menu

d. Click **OK**.

e. Click **Done**.

f. Return to the SMIT main Service Agent menu.

g. Select **Manage Service Agent Gateway** → **Select Configure Service Agent Gateway** to start the Service Agent gateway processes. Add the inittab entries for the database and the ods script. The default host name of the Service Agent gateway server is the default configured host name. Click **OK**.

h. Click **Done**.

2. Install the Service Agent client code:

> **Note:** This step is required only if you manually installed the svcagent.client module on another host after the Service Agent gateway host is activated. This step is not required if code is applied to the client from the Service Agent gateway.

a. From the SMIT menu, select **Manage SA Client**.

b. Configure the client first. The host name is the default. Change it to match the host name in the database if it is different. Enter the password for root to match the Service Agent gateway password.

c. Define the primary (required), secondary, and tertiary server host names, as appropriate.

d. Click **OK**.

e. Click **Done**.

8.2.4 Maintenance

Electronic Service Agent has several operational user interface views (ASCII and GUI) that you can access from the SMIT menu. These views include Select Problem Determination, Service Agent, and Select Service Agent User Interface, which is shown in Figure 8-6.

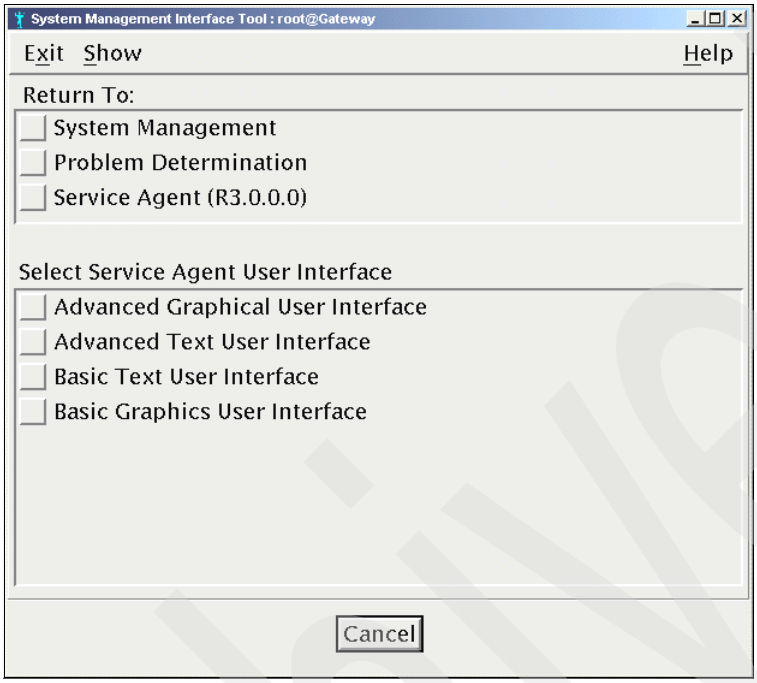


Figure 8-6 SMIT menu: Select Service Agent User Interface

The basic menu

When you select the basic menu GUI (shown in Figure 8-7 on page 106), you see several fields for customer contact information when you are using the GUI for the first time. Fields with exclamation marks (!) are mandatory and must be completed for the machine location. IBM communicates with your company and location based on the information in these fields. Incomplete or inaccurate information delays responses from IBM.

The select list located on the left side contains fields that are completed as you proceed through a guided process. Help for each of these selections is provided in the upper right side of the view. The lower right side of the view contains the specific fields within each selection.

When you complete the eService Information field with your IBM ID, your ID is authorized to view Service Agent information on the Electronic Services Web site and use the information in the Premium Search queries.

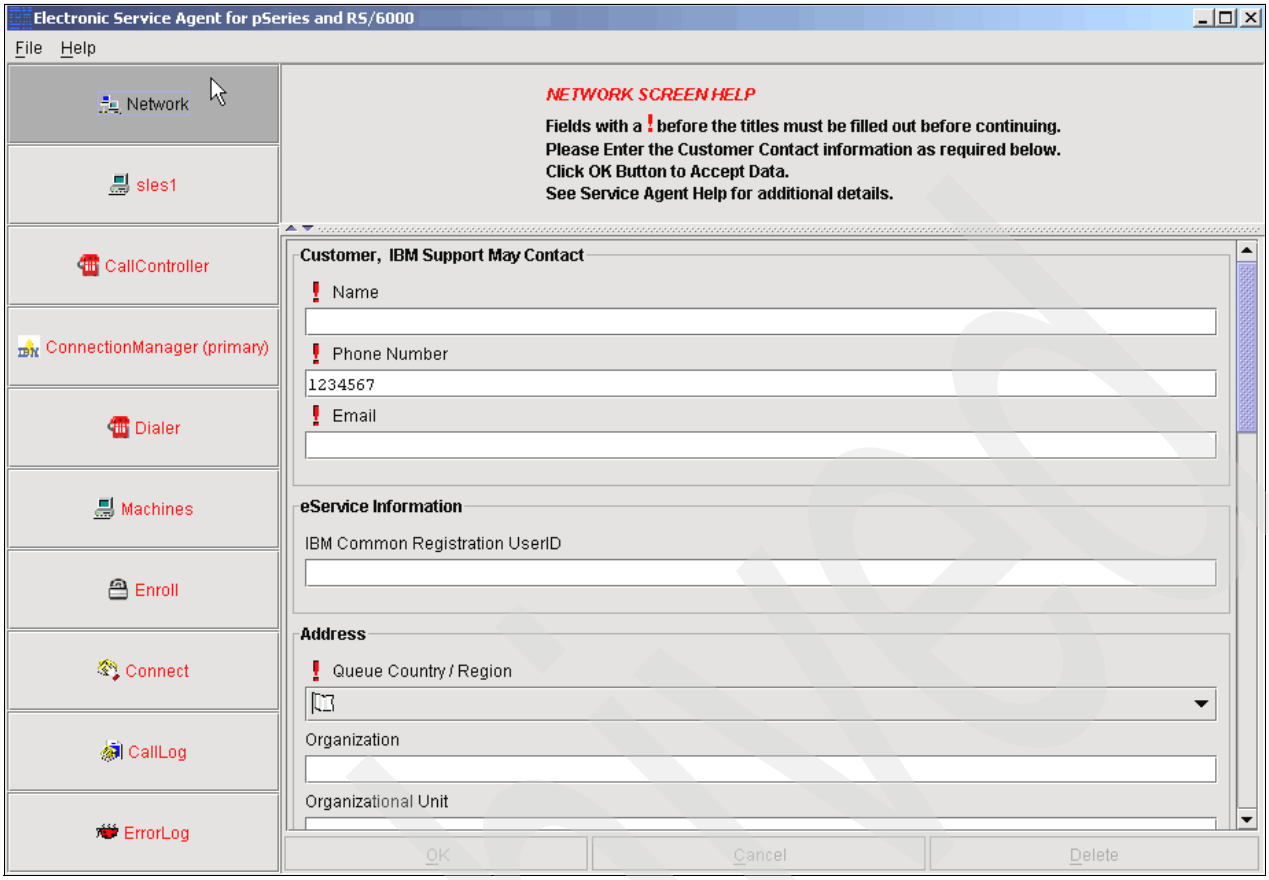


Figure 8-7 Service Agent for System p basic main menu

The Call Log (shown in Figure 8-8) displays the results of connections and transmissions to IBM. By viewing this log during the dialing or initial phase of a connection, you see real-time updates being logged. When a connection is made and requests are transmitted, a summary count of the request types and whether they were transmitted successfully are logged. The summary counts overlay the description entries made during the connection phase.

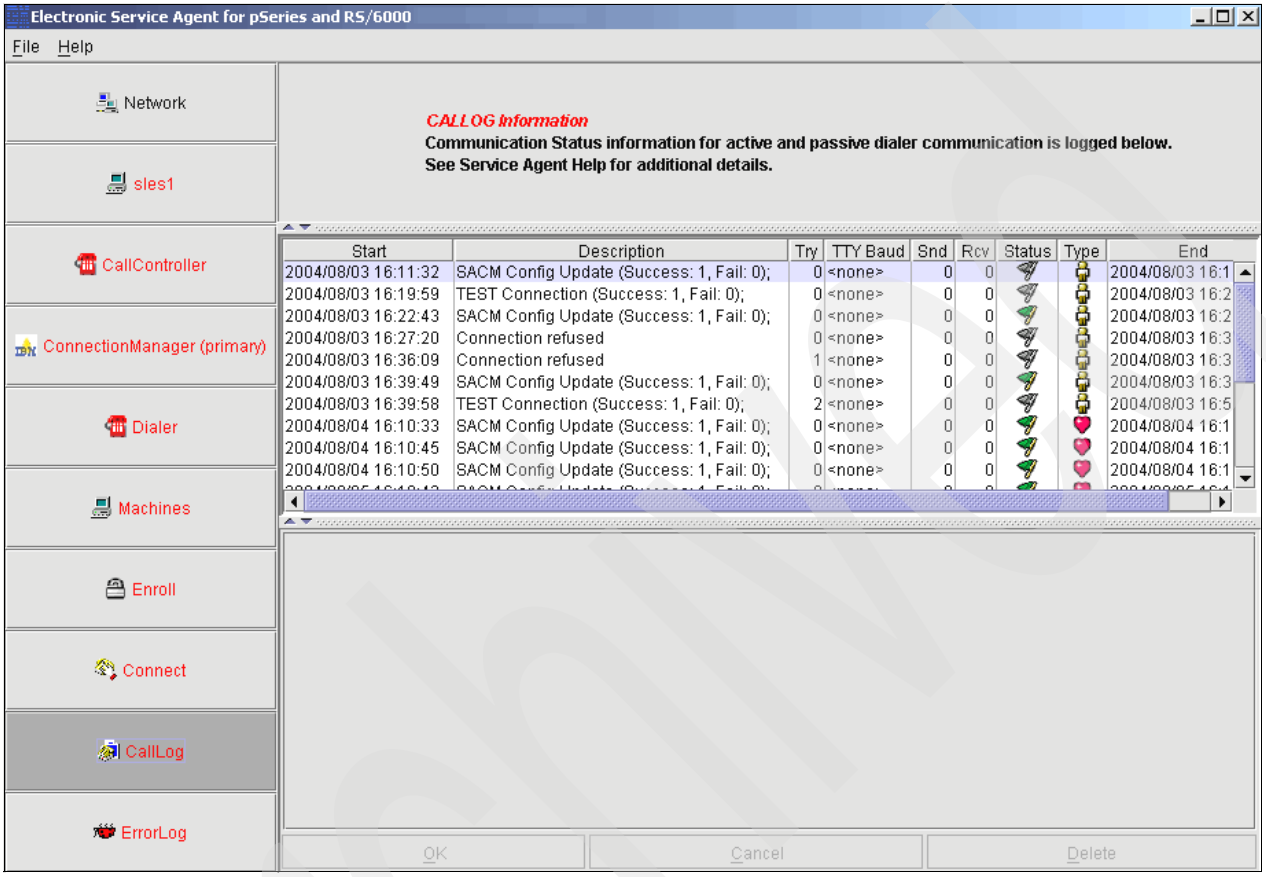


Figure 8-8 Service Agent for System p basic menu Call Log view

The other selections, such as the various logs and connection view, that are in the left navigation bar are used in activation or maintenance tasks.

Advanced menu

The advanced menu (shown in Figure 8-9) provides selections that handle the complex system configuration steps and maintenance tasks. Sample tasks include:

- Adding SP nodes to 9076 cws
- Setting thresholds, filters, and alerts
- Using manual tools for testing and sending information to IBM
- Purging information
- Viewing real-time monitoring of code clients and alerts

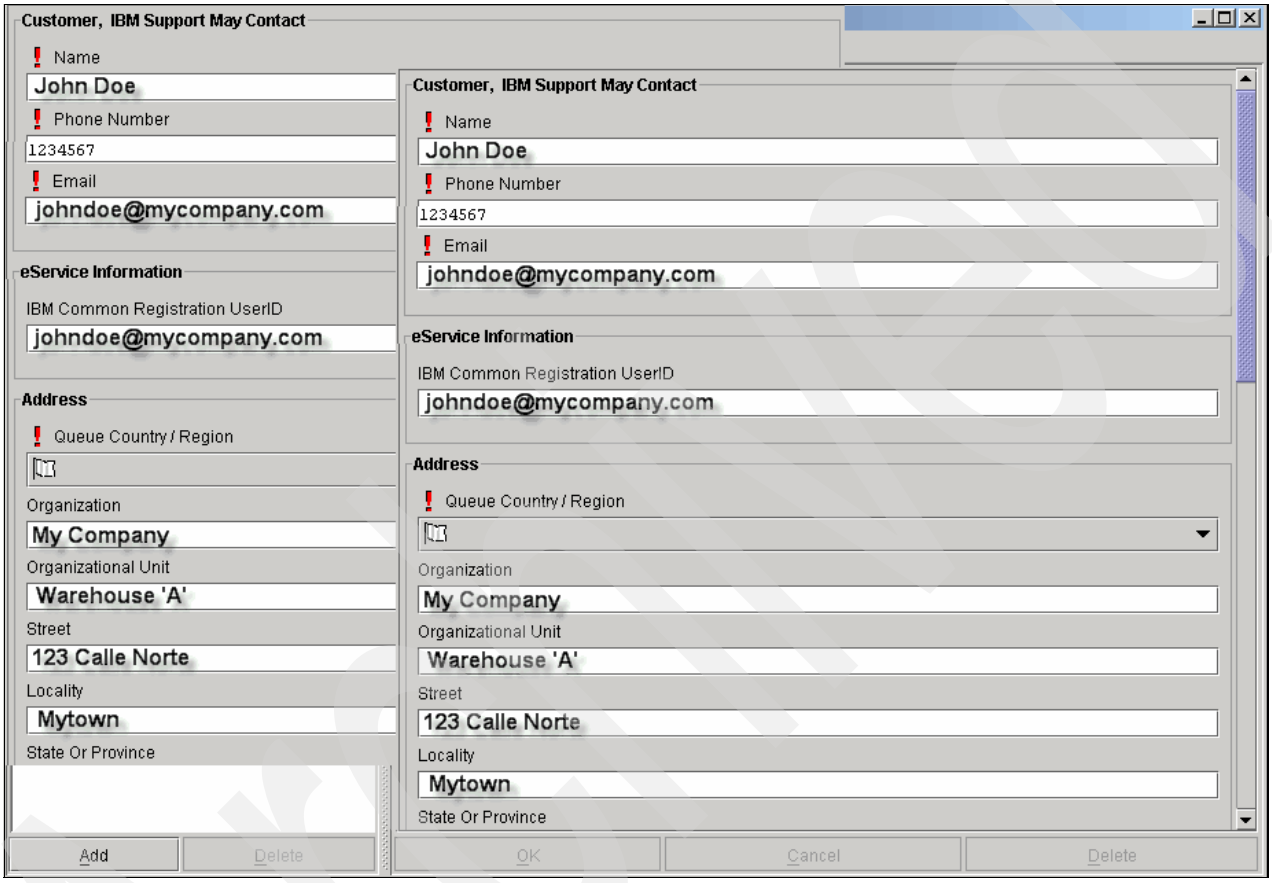


Figure 8-9 pService Agent advanced menu

For more information under each properties folder, you use the four symbols on the upper left side, as shown in Figure 8-10.

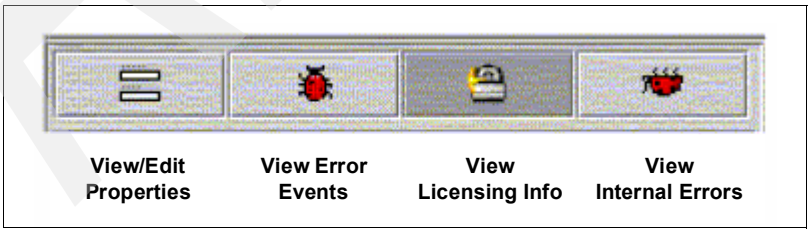


Figure 8-10 System p Service Agent advanced menu: Property symbols

For example, when you select Network properties, the View Licensing Info icon displays the licensing, Heartbeat status (green flag or red X), and lock status (red X) on all monitored machines as shown in Figure 8-11.

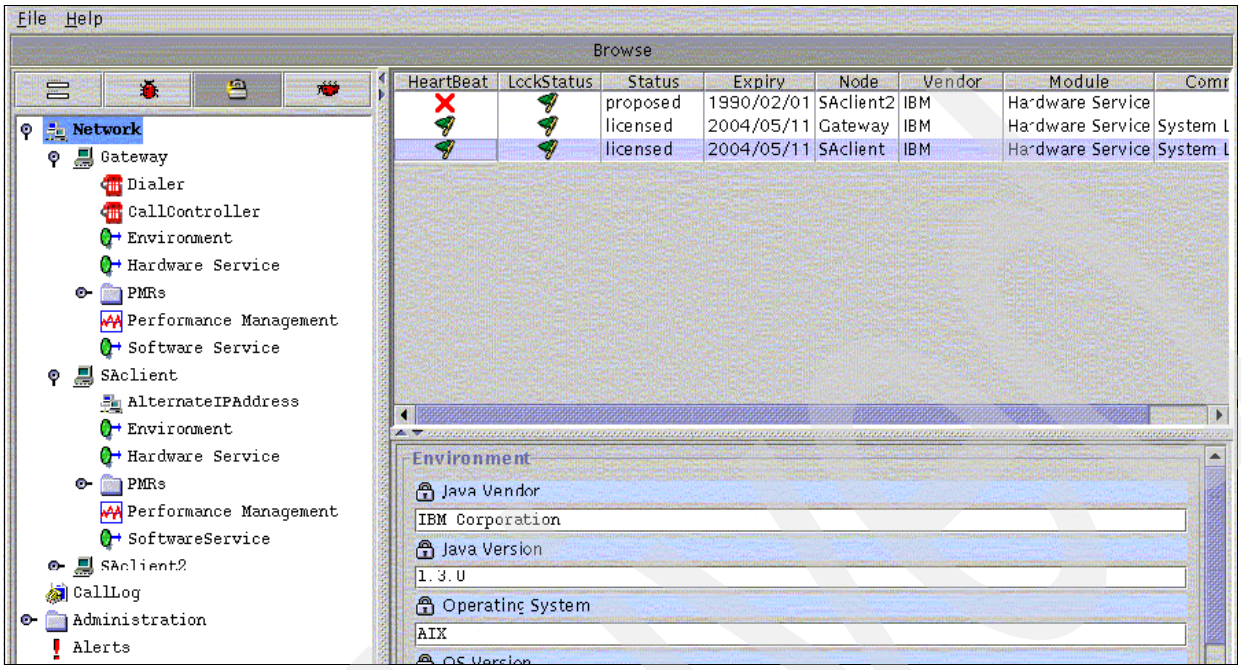


Figure 8-11 System p Service Agent advanced menu: Expanded sample

You can configure e-mail alerts on the advanced menus shown in Figure 8-12 and Figure 8-13 on page 111. You can customize various e-mail alerts for particular users. For example, you might want to notify employee A about CAUTIONS and notify employee B of INTERNAL ERRORS. Typically, only one e-mail alert is necessary for any of the events that might happen on any of the systems that use this gateway.

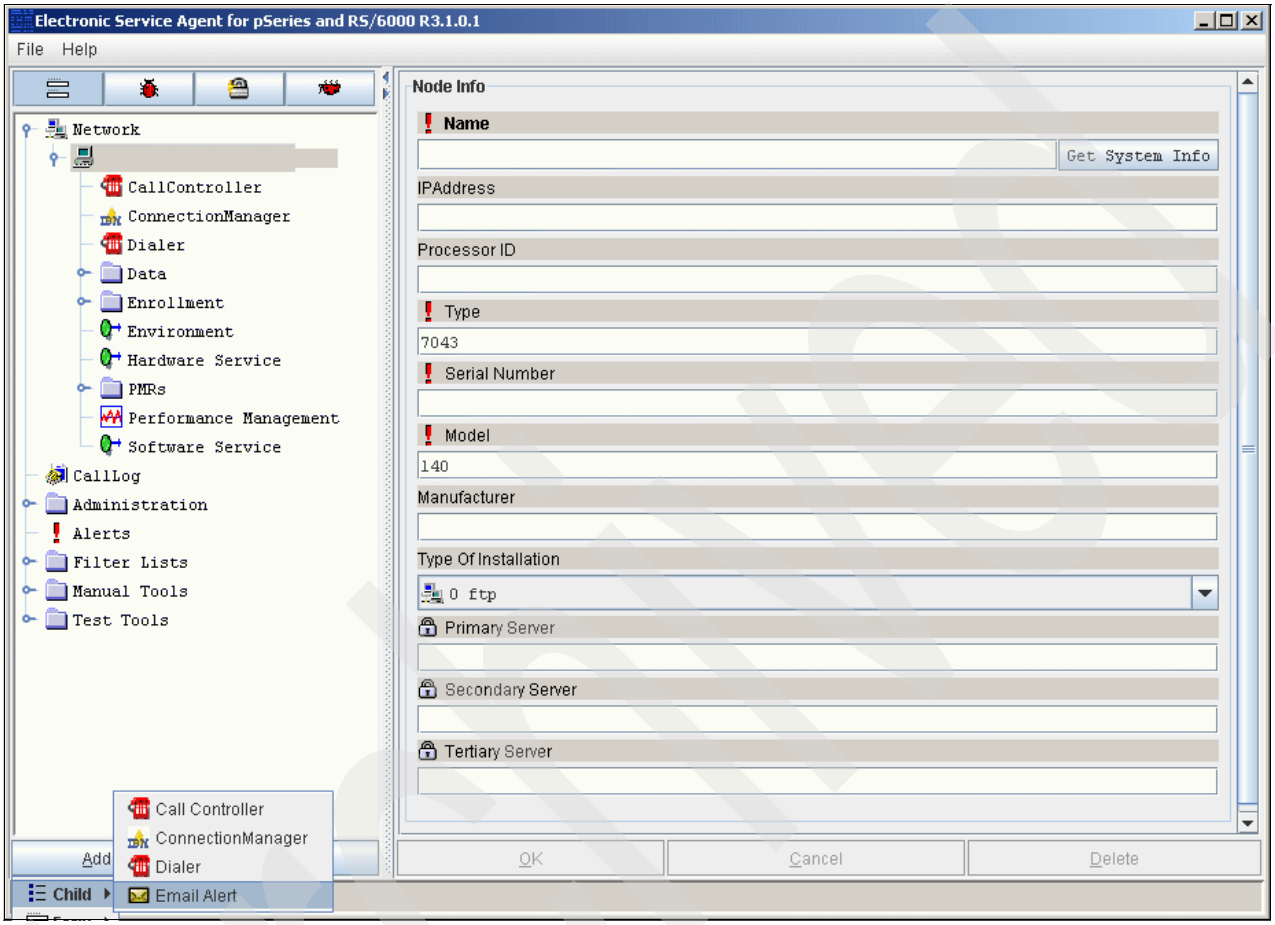


Figure 8-12 Advanced menu: First view of e-mail setup

The advanced menu provides more configuration options, as shown in Figure 8-13 on page 111.

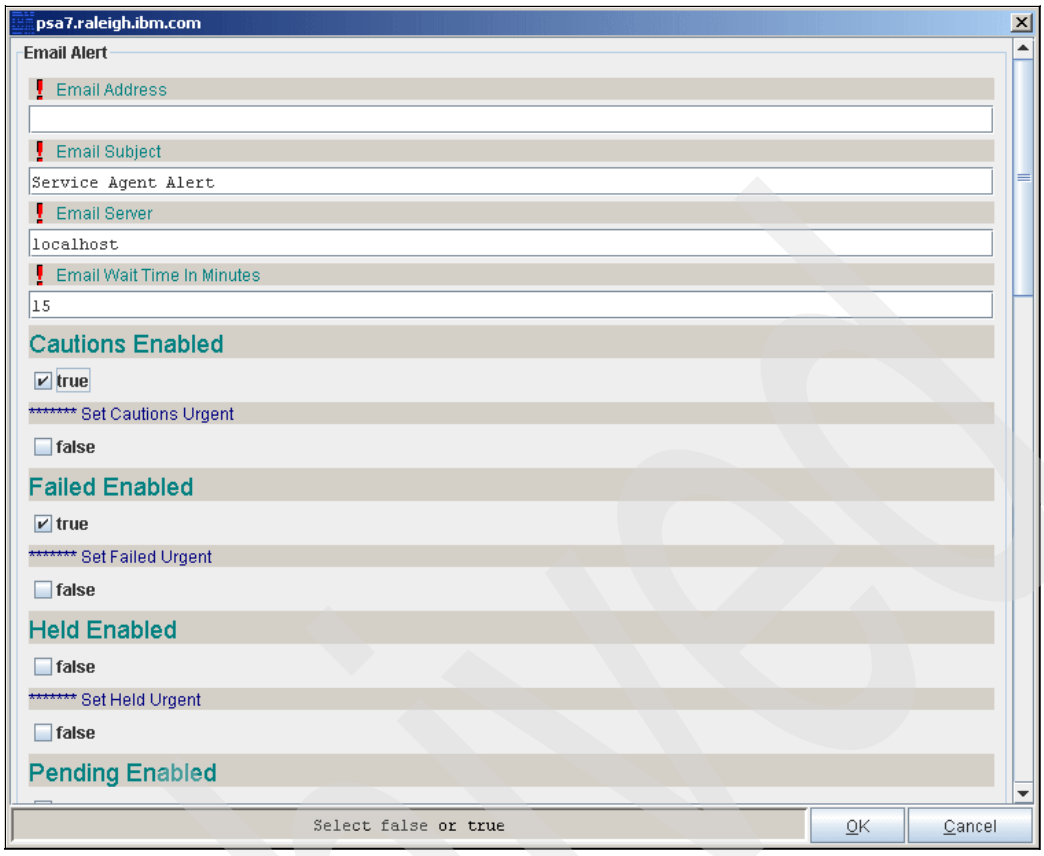


Figure 8-13 Advanced menu: Second panel of e-mail setup

Selecting Performance Management on the advanced menu shown in Figure 8-14 informs you of the status of the selected host. The same area displays the schedule for information collection and transmission to IBM.

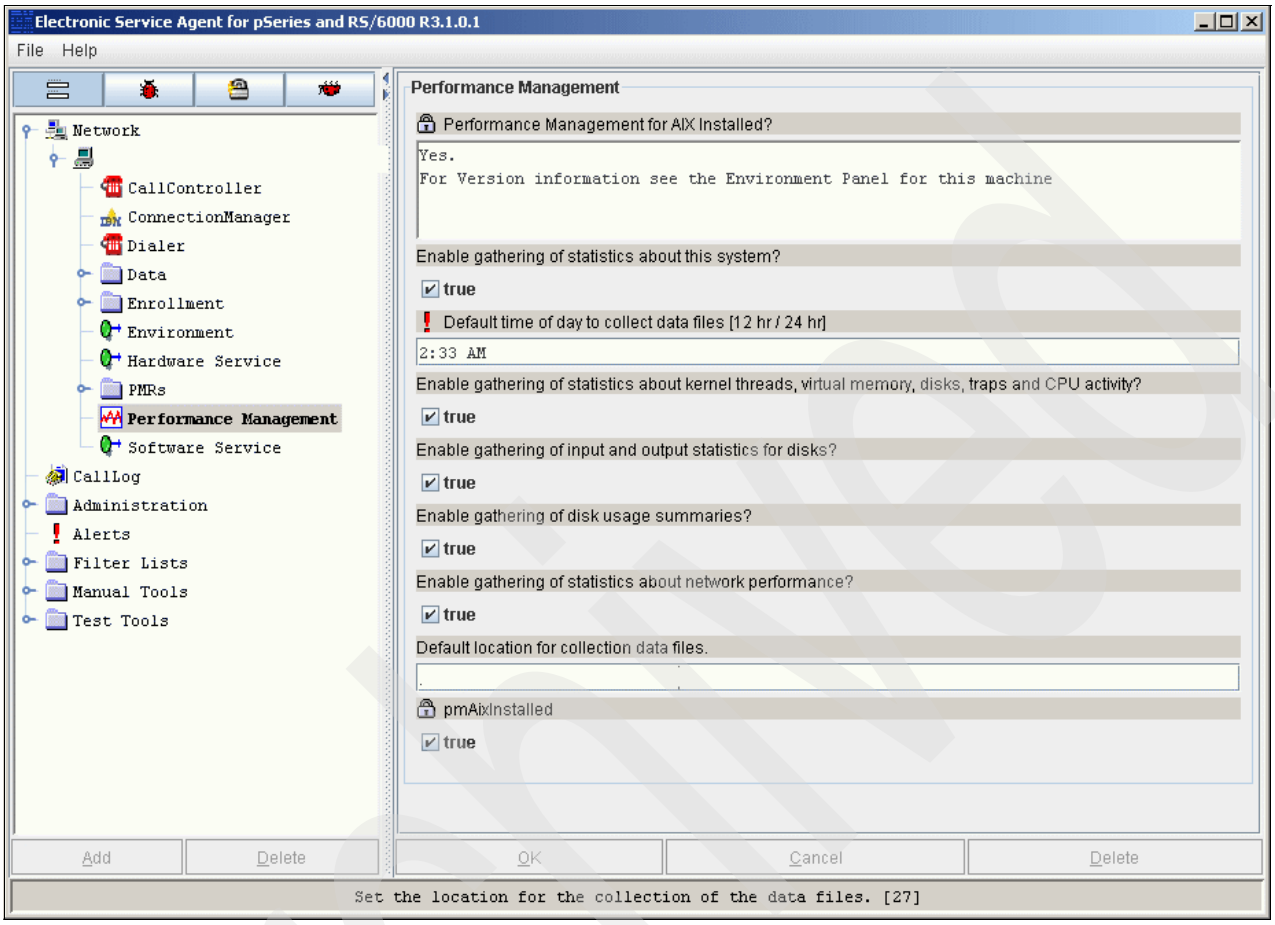


Figure 8-14 Advanced menu: Performance Management expanded

8.2.5 Stopping and restarting Service Agent

There might be times when you want to stop or restart the Service Agent daemon process. There are multiple places and steps to perform the stop and restart. This section provides a summary of the necessary tasks. For specific details, refer to *Electronic Service Agent for System p User Guide*, SC38-7105.

Places to stop Service Agent

You can stop Service Agent in any of these areas:

- On the gateway server, ESS, ODS, and SACM (where the Service Agent database resides)
- On the monitored machine, ODS only (clients that report to the gateway server)
- On the stand-alone AIX server, SACM (Connection Manager server) only

Places to restart Service Agent

After you stop the Service Agent daemons, you restart them on both the gateway server and the monitored machines:

- Restarting the Service Agent daemons on the gateway server creates new inittab entries for the ESS, ODS, and SACM daemon processes. If Connection Manager is not on this gateway, it is not started.
- Restarting the Service Agent daemon on the monitored machines creates a new inittab entry for the ODS daemon.
- Restarting the Service Agent Connection Manager creates a new inittab entry for the SACM daemon process that restarts the server's Service Agent Connection Manager process.

8.3 HMC: Planning and prerequisites

Four major components make up the Service Agent environment on HMC machines:

- The *Electronic Server System* process runs only on the gateway HMC. The ESS handles all requests for data input and retrieval from the centralized database.
- The *On Demand Server* process runs on all HMCs that are defined and handles all Service Agent communication activities for that host. The ODS sends data to the ESS process as necessary or makes a request to SACM to call IBM. Events from the Service Focal Point (SFP) are reported to IBM directly using an Internet connection or a modem that is attached to the gateway server. Service Agent calls IBM to report that it is healthy, one time in every health-check interval.
- The *Service Agent Connection Manager* is a stand-alone process that you can configure to communicate with IBM by using an existing Internet connection or modem. It might exist on any HMC or stand-alone AIX machine and can support multiple Service Agent gateway connections.
- The *User Interface* allows the user to set up and define HMCs that Service Agent monitors. The GUI is invoked from the WSM when you select Service Agent from the Service Applications. Then in the WSM Service menu, you select TASKS for Service Agent User Interface. It is used for advanced functions and customization of the system, as well as configuration for complex systems and multilevel networks.

Important: You must establish the HMC environment prior to activating Service Agent. Do not start the Service Agent processes if the network is not configured on the gateway or client HMC.

Here are several items to review:

- On new installations, the HMC host name is a default name. Be sure to assign a new name to fit your network environment.
- On the HMC gateway, ensure that the modem and phone line are connected if you use them. Check the physical connections to determine whether they are connected.
- If you use the Internet, make sure that HMC has connectivity to the network.
- If HMC is a client, start Service Agent only after the network is set up properly.
- After assigning a host name, determine whether to apply a gateway or client Service Agent.

Figure 8-15 shows the high-level activation process.

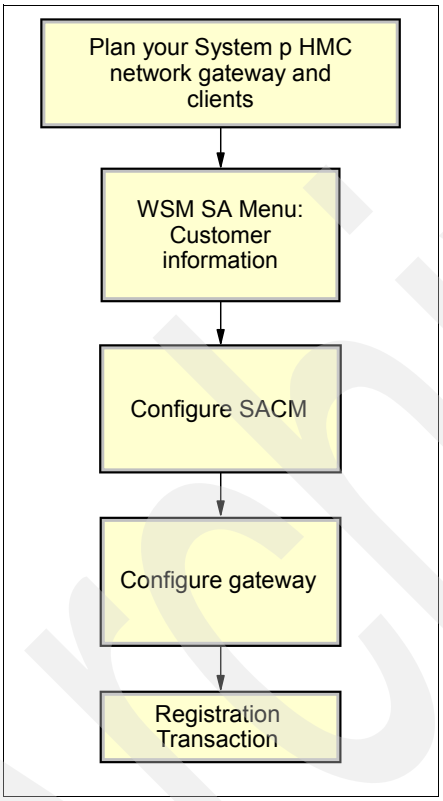


Figure 8-15 System p HMC activation flow

8.3.1 Installation and activation

HMC machines have Service Agent installed as part of the HMC code and on the HMC main menu under Service Applications. You update Service Agent with new releases of HMC code.

1. In the Navigation Area on the HMC main menu, select **Service Applications** → **Service Agent** (Figure 8-16).

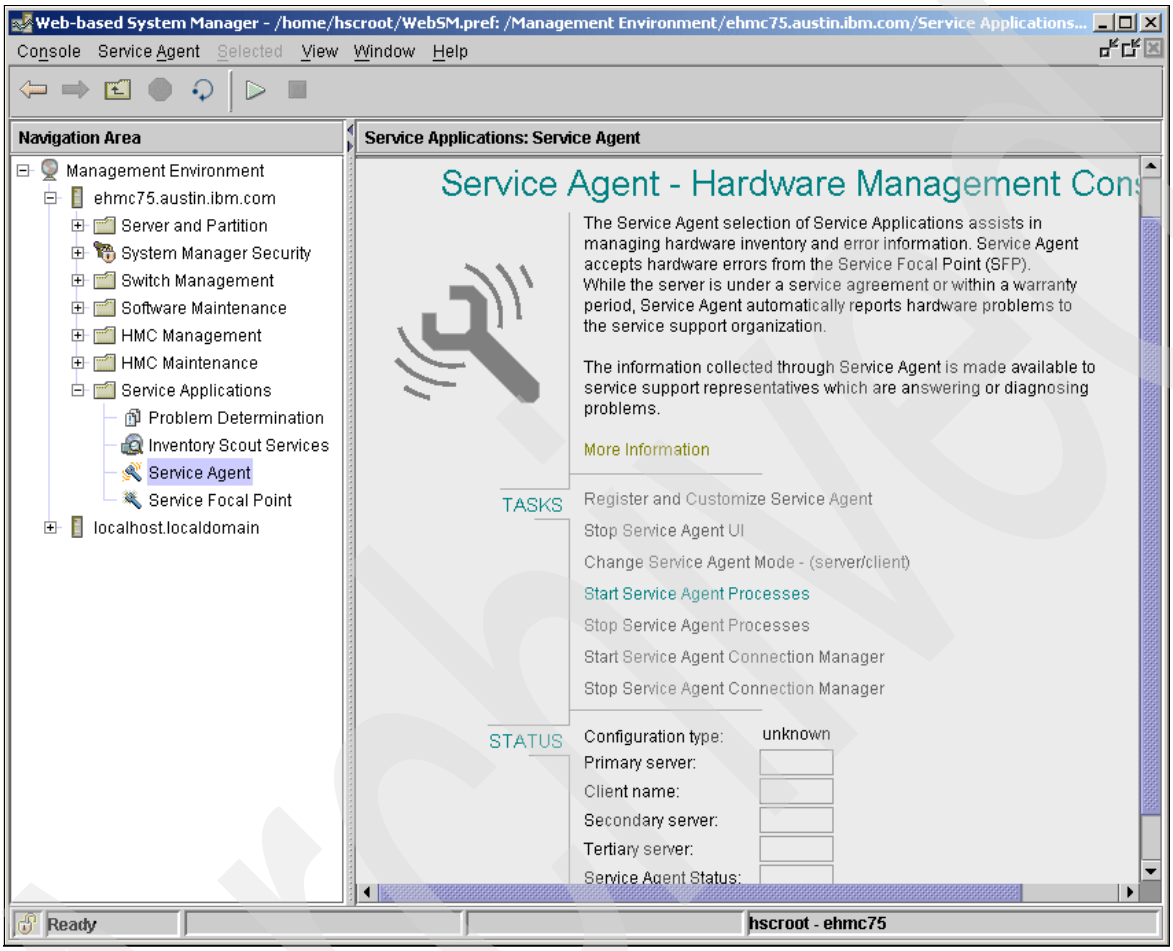


Figure 8-16 HMC main menu: First visit

2. Service Agent detects whether it has been activated. If not, you see the window shown in Figure 8-17. Verify or update the information and select **Continue**.

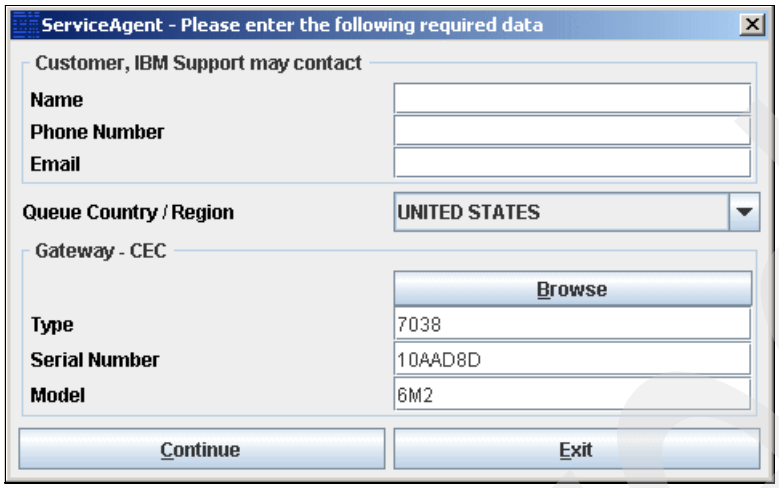


Figure 8-17 HMC Service Agent activation wizard (Part 1 of 2)

3. In the next window (shown in Figure 8-18), enter the requested information and click **OK**.

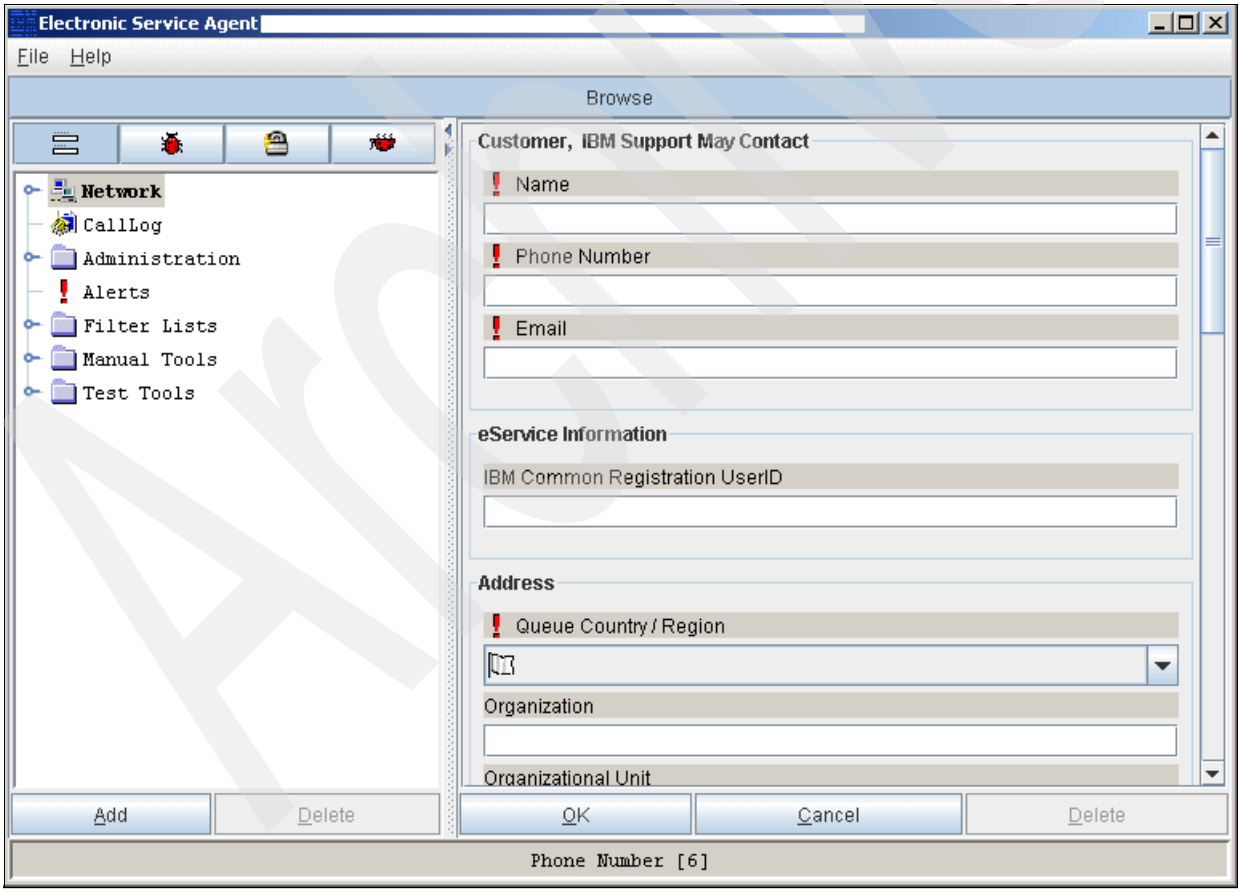


Figure 8-18 HMC Service Agent activation wizard (Part 2 of 2)

8.3.2 Maintenance

To invoke the Service Agent GUI in WSM, you select **Service Applications** → **Service Agent**. The Service Agent menu (shown in Figure 8-19) shows the two main sections: TASKS and STATUS:

- The TASKS section is where you start and stop the processes, change the function or update the host name, and access the user interface.
- The STATUS section informs you about the configuration of this HMC (server/client) and the status of the Service Agent processes.

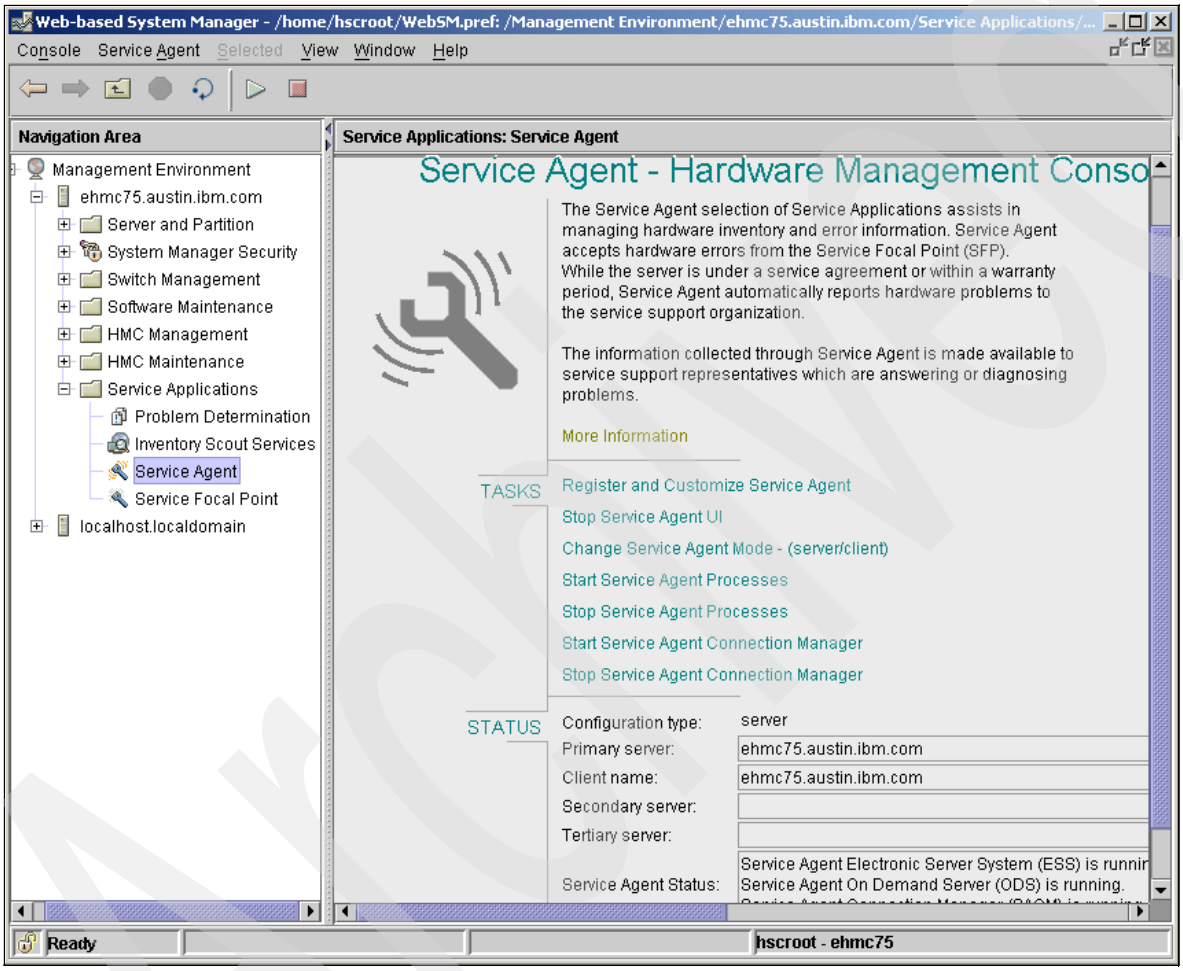


Figure 8-19 HMC main menu with Service Agent expanded

8.3.3 Stopping and restarting a process

You have the flexibility to stop and restart Service Agent on the gateway server.

Stopping Service Agent

When you stop the Service Agent, you end the normal Service Agent daemon processes and remove the inittab entries. If the SACM is running on this gateway server, it is not stopped automatically. To stop it, complete these tasks:

1. On the HMC User Interface, select **Service Agent Panel**.
2. Select **Stop Service Agent processes**.
3. Select **Stop SACM**, if appropriate.

Restart Service Agent

After you stop the Service Agent daemons, you restart them on both the gateway server and the client machines. If the SACM is stopped on the gateway server, you can restart it from the menu.

The Service Agent menu selections create new inittab entries for the ESS and ODS daemons, which restart the gateway HMC Service Agent processes. The ODS daemon is started on a client HMC and automatically starts a SACM process, if present. To restart Service Agent, follow these steps:

1. On the HMC User Interface, select **Service Agent Panel**.
2. Select **Start Service Agent processes**.

9

IBM Electronic Service Agent for Linux on the System i, System p, and System x platforms

This chapter provides background and information about the Electronic Service Agent for Linux on several platforms. This chapter is intended for system administrators who are familiar with or have a working knowledge of Linux on these platforms, Linux system commands, and the System Resource Controller.

9.1 Electronic Service Agent

Service Agent enhances your use of Linux in the System p environment by providing the capability to submit automatic hardware problems and to monitor the system inventory.

The following information is from the *Electronic Service Agent for Linux User Guide,* SC38-7109. Refer to this user guide for comprehensive text about the topics covered in this chapter. All the Service Agent GUI help text is taken directly from that user guide.

9.1.1 Overview of Service Agent for Linux on System p

In the overview of the System p environment shown in Figure 9-1, you see the client Linux environment has the potential for stand-alone and gateway configurations. All Service Agent communication flows through the *Service Agent Connection Manager (SACM)*.

The choices of communication to IBM are either modem or Internet. The automatic problem submission path and the inventory paths are through secure firewalls into the appropriate IBM databases. You can use the Electronic Services Web site to view the Service Agent inventory.

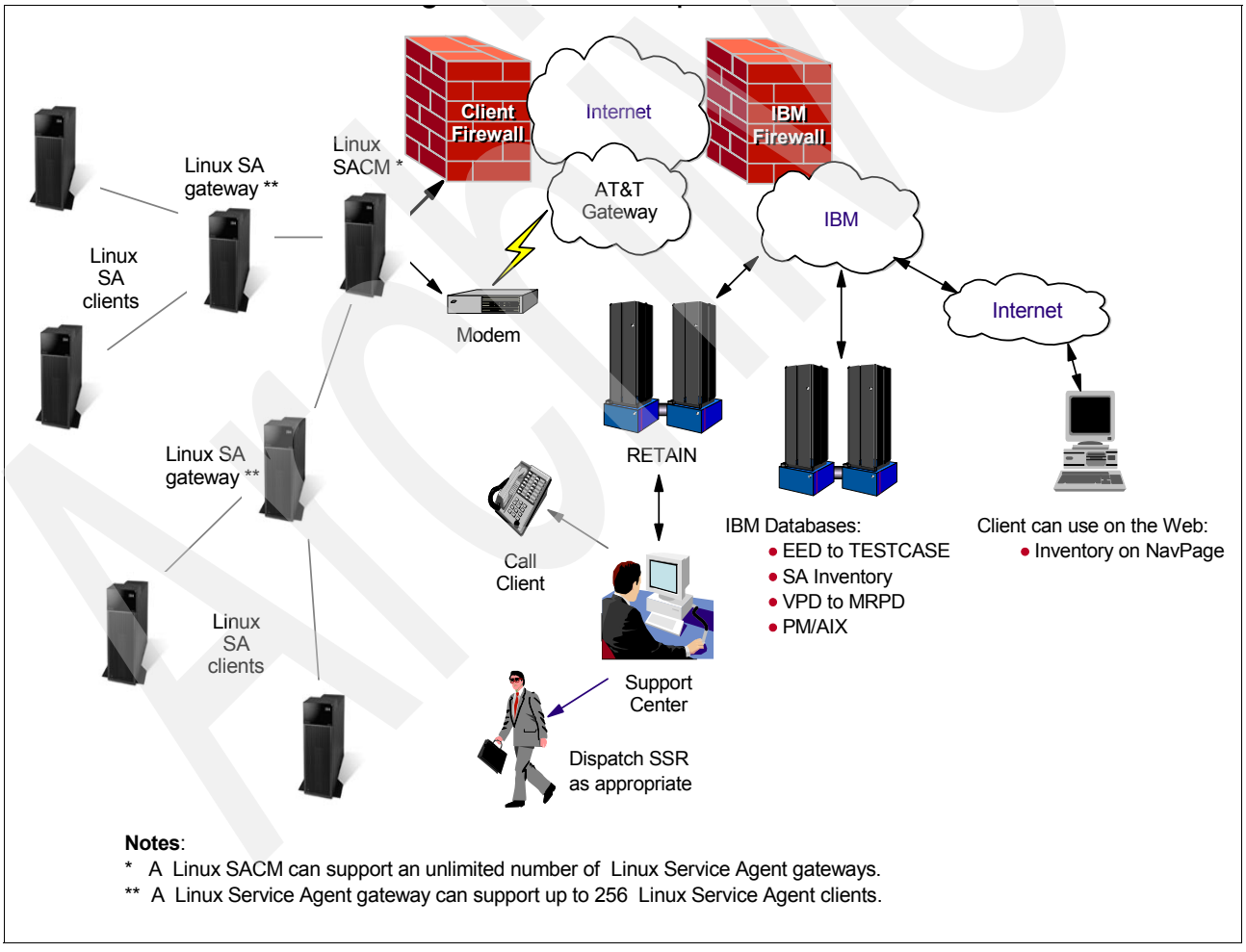


Figure 9-1 Linux Service Agent overview

9.1.2 Machine types and models that are eligible for Service Agent

Electronic Service Agent for Linux on System p supports SUSE Linux Enterprise Server (SLES) Version 8 with Service Pack 3 and SLES Version 9. The machines must be under IBM warranty or maintenance contracts.

9.1.3 Service Agent Connection Manager

The SACM is a stand-alone process that can be configured to communicate with IBM using an existing Internet connection or modem. This application is installed with the Service Agent code on the Service Agent gateway. However, it can be installed as stand-alone code on any supported platform. It can exist in a stand-alone machine and can support multiple Service Agent gateway connections.

Figure 9-2 shows a sample configuration using firewalls and SACM and the features that enable enhanced security and offer the following advantages:

- Provide firewall support using either a proxy service or provide for traffic to pass through a Network Address Translation (NAT) device, such as a Cisco PIX Firewall
- Provide a single point of exit from the client environment
- Ensure Inter-Enterprise Security (IES) compliance

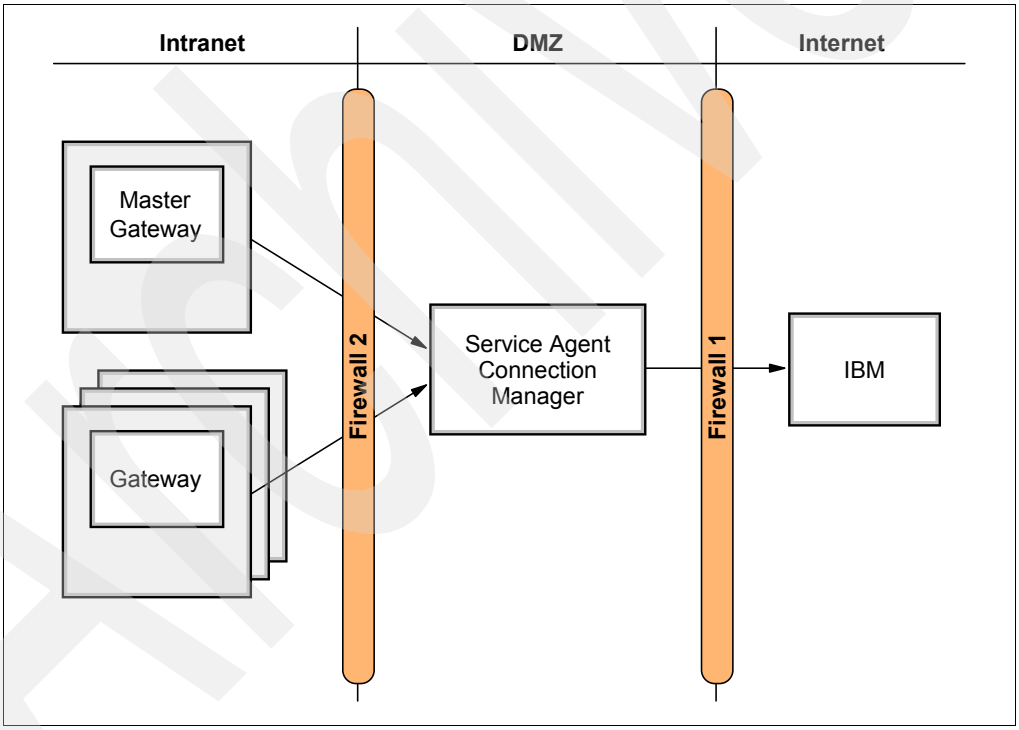


Figure 9-2 Sample configuration using firewalls and SACM

9.2 Planning, installation, and activation

Early planning can help save you valuable time and help minimize aggravation later. Understanding your information technology (IT) environment and planning the activation of the Service Agent application makes your time more efficient and effective.

Figure 9-3 on page 122 shows an overview of the activation steps.

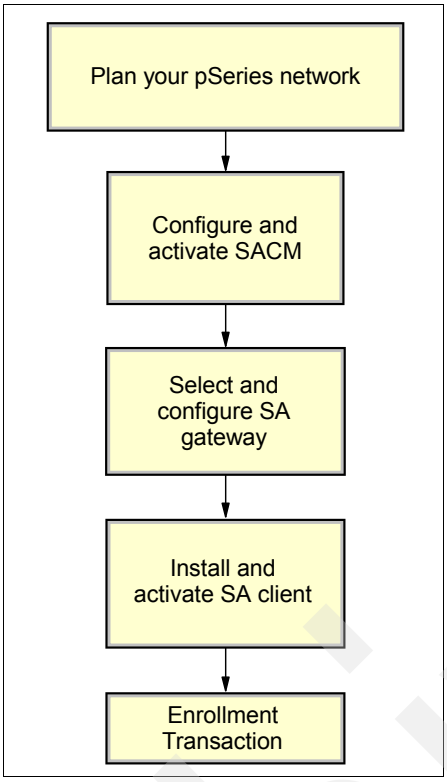


Figure 9-3 Linux Service Agent activation flowchart

9.2.1 Planning

Four major components or processes make up the Service Agent application:

- The *Electronic Server System* (ESS) process runs only on the Service Agent gateway server or servers. It handles all requests for data input and retrieval from the centralized database.
- The *On Demand Server* (ODS) process runs on both the gateway and monitored machines. It handles all Service Agent monitoring and communication activities for that host. The ODS retrieves and sends data to the ESS process as necessary.
- *Service Agent Connection Manager* is a stand-alone process that is configured to communicate with IBM using an existing Internet connection or modem. It can exist on any Linux on POWER in your environment and can support multiple Service Agent gateways concurrently.
- The *User Interface* or interfaces is available for both basic or advanced users through text or GUI. The Basic User Interface is designed to allow a first-time user to configure the Service Agent system with as little user input as possible, using predefined defaults for a single-level network environment. The Advanced User Interface provides advanced functions and enables customization of the system as well as configuration for complex systems and multilevel networks.

Use the following planning list to help you through the process:

1. Plan your Service Agent environment to determine the placement and the number of Service Agent gateways and the location of monitored machines.
2. Plan your Service Agent Connection Manager:
   - Determine which host is best.

- SACM can be installed on any System p Linux host. It does not have to be a Service Agent gateway.
- SACM can be controlled by a designated master Service Agent gateway.
- Communication to and from the SACM host can pass through secure firewalls.
- SACM can support an unlimited number of gateways.
- A gateway can support up to 256 clients.

3. Ensure that the administrator who is installing Service Agent has root authority on all target machines.
4. If you are on a System p platform using POWER4+™ technology, ensure that your Linux installation is SLES 8.1 SP3 or later.
5. If you are on a System p platform using POWER5™ technology, ensure that your Linux installation is at SLES 9.0 or later.
6. Java is required on all Service Agent machines (SACM, gateway, and client). All supported Linux on POWER distributions come with a version of Java installed by default. Service Agent is equipped to use the default Java installation.
7. Install the appropriate IBM Linux Service Aids Toolkit. This toolkit provides the utilities required to service System p systems running IBM-supported versions of the Linux operating system. Service Agent requires you to download the packages from the Linux Service Aids Toolkit Web site and install them *in this order* on all Service Agent machines:

   a. librtas
   b. ppc64-utils
   c. lsvpd
   d. IBMinvscout
   e. diagela
   f. System Resource Controller (SRC)

   You can obtain more information about the IBM Linux Service Aids Toolkit at:

   `http://techsupport.services.ibm.com/server/lopdiags`
8. Install IBM diagnostics on every monitored machine.
9. Make sure that the System p machine type, model, and serial number are listed with an IBM RETAIN® database.
10. Ensure that the gateway server has remote File Transfer Protocol (FTP), SSH, or both types of capabilities for all monitored machines.
11. Determine whether you are using an existing Internet connection or modem.
12. Prepare for e-mail alerts. The host on which the e-mail alert is placed must have e-mail service that is available either locally or through an attached network.
13. Obtain managed systems information. This includes the host name, machine type, model, serial number, and processor ID. Service Agent attempts to discover the information after the host name is provided. If the auto-discovery process is unsuccessful, manually start the installation.

9.2.2 Installation

Service Agent consists of several RPM format packages. You must install each component in the correct location. Table 9-1 on page 124 lists the items to install.

Table 9-1 Linux Service Agent components to install

Component	RPM name
Service Agent Connection Manager	svcagent.cm-1.0.0-x.ppc64.rpm
Service Agent Gateway	svcagent.server-1.0.0-x.ppc64.rpm
Service Agent Client	svcagent.client-1.0.0-x.ppc64.rpm
Service Agent Localized Messages	svcagent.msg.<*locale*>-1.0.0-x.ppc64.rpm For example, svcagent.msg.en_US-1.0.0-x.ppc64.rpm
Service Agent Help	svcagent.help.<*locale*>-1.0.0-x.ppc64.rpm For example, svcagent.help.en_US-1.0.0-x.ppc64.rpm

Download Service Agent code from the IBM FTP site to your machine using these steps:

1. Log in (or **su**) to root on a System p.
2. To access the tmp directory, type:

   ```
   cd /tmp
   ```

3. Access the FTP site:

   ```
   ftp ftp.software.ibm.com.
   ```

4. Log in to the server. For your login name (user ID), enter `anonymous`. For your login password, enter your *e-mail address.*
5. Set the file transfer type to binary. Type:

   ```
   bin
   ```

6. Access the path where the Service Agent code is stored. Type:

   ```
   cd /linux/service_agent_code/LINUX
   ```

7. Retrieve the Service Agent code:

   ```
   get svcagent_ppclinux.tar
   ```

8. Retrieve the Acrobat® format of the Service Agent User's Guide:

   ```
   get svcUG_ppclinux.pdf
   ```

9. End your FTP session:

   ```
   quit
   ```

10. Transfer the file in binary if necessary to the machine that you want to be the Service Agent gateway server.
11. Untar the svcagent_ppclinux.tar file into the directory from which you want to install it.

You have now created an SA directory that contains all of the installp modules.

Most clients install the Service Agent Connection Manager and Service Agent gateway on the same machine. The following steps illustrate this type of configuration:

1. Install SACM:
   a. Log in to your designated Service Agent Connection Manager as `root` or sign on using a root-authorized user ID.
   b. Change to the tmp directory or the location where you placed the Service Agent Connection Manager package:

      ```
      cd /tmp/sa
      ```

c. Type the following command:

```
rpm –i svcagent.cm-1.0.0-x.ppc64.rpm
```

You have successfully installed Service Agent Connection Manager.

2. Install the Service Agent gateway:
   a. Log in to your designated Service Agent gateway as `root` or sign on using a root-authorized user ID.
   b. Change to the tmp directory or the location where you placed the Service Agent gateway (server) package.

```
cd /tmp/sa
```

   c. Install the client package:

```
rpm –i svcagent.client.1.0.0-x.ppc64.rpm
```

   d. Install the msg package:

```
rpm –i svcagent.msg.en_US-1.0.0-x.ppc64.rpm
```

   e. Install the help package:

```
rpm –i svcagent.help.en_US-1.0.0-x.ppc64.rpm
```

   f. Install the server package:

```
rpm –i svcagent.server.1.0.0-x.ppc64.rpm
```

The Service Agent processes are not active when the initial installation completes. You must configure Service Agent manually after you install the code components.

9.2.3 Activation

Service Agent for Linux is under the control of the SRC. The following steps explain how to configure your environment using the SRC.

Tip: The SRC master daemon (/sbin/srcmstr) must be running. Make sure that this line is in /etc/inittab:src:2345:respawn:/sbin/srcmstr.

1. Start SACM.

```
startsrc -s sacm
```

2. Configure the gateway system.

```
/usr/svcagent/bin/sagatewayconfig
```

3. Accept the Customer License Agreement.
4. The gateway and client processes start on this machine.
5. To start Service Agent, type:

```
startsrc -g svcagent
```

Use the Advanced GUI for test and enrollment transactions.

9.3 Maintenance

Electronic Service Agent has two layers of operational menus: *basic* and *advanced*.

9.3.1 Basic menu

The basic menu (shown in Figure 9-4) displays several fields for customer contact information when you use the graphical user interface (GUI) for the first time. Complete these fields accurately, because IBM communicates with your company based on the information that is in these fields. Incomplete or inaccurate information delays a response from IBM.

When you complete the eService Information field with an IBM ID, that ID is authorized to view the Service Agent information on the Electronic Services Web site and to use Premium Search queries.

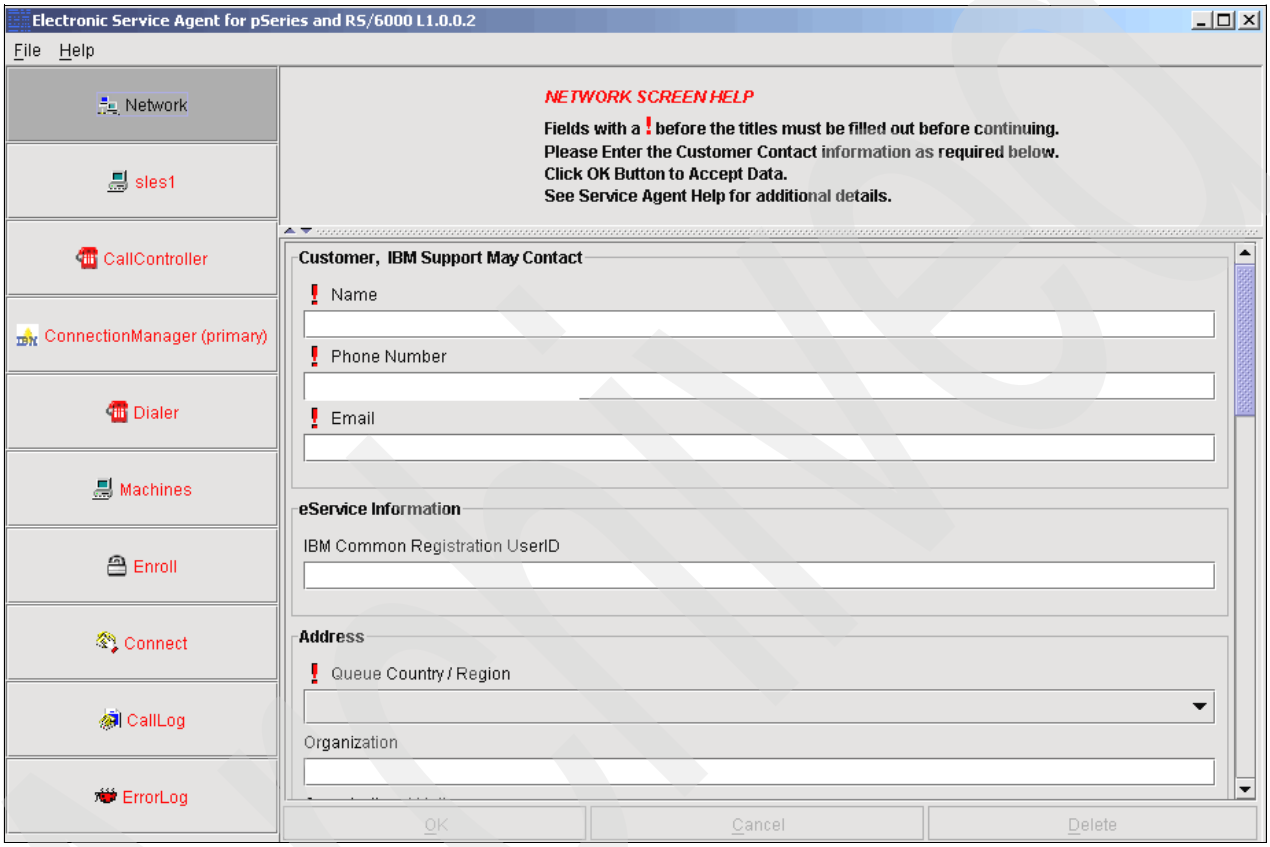


Figure 9-4 Service Agent for Linux: Basic menu

The Call Log shown in Figure 9-5 displays the results of connections and transmissions to IBM. By viewing this log during the dialing or initial phase of a connection, you see real-time updates being logged. After a connection is made and requests are transmitted, a summary count of the request types and whether they were transmitted successfully are logged. The summary counts overlay the description entries that were made during the connection phase.

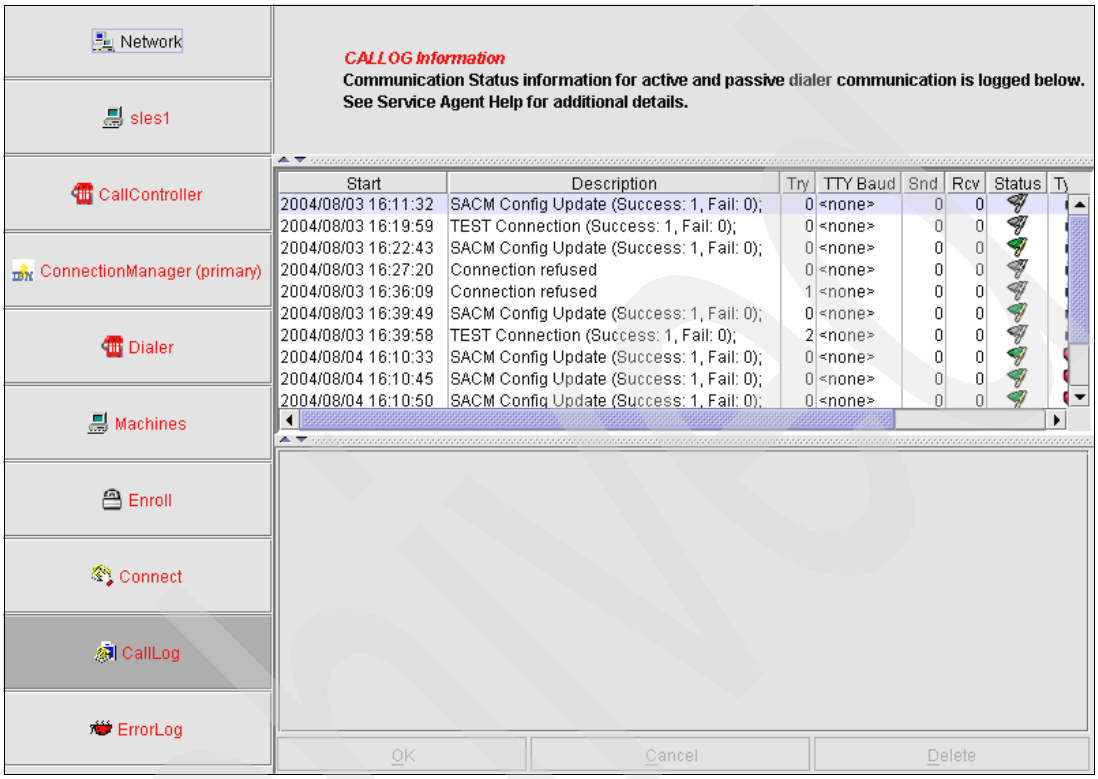


Figure 9-5 Service Agent for Linux: Basic menu Call Log

Advanced menu

The advanced menu (shown in Figure 9-6) is used after you define the gateway server host type and serial number fields. All functions available within the basic interface are a subset of the functions that are available in the advanced interface.

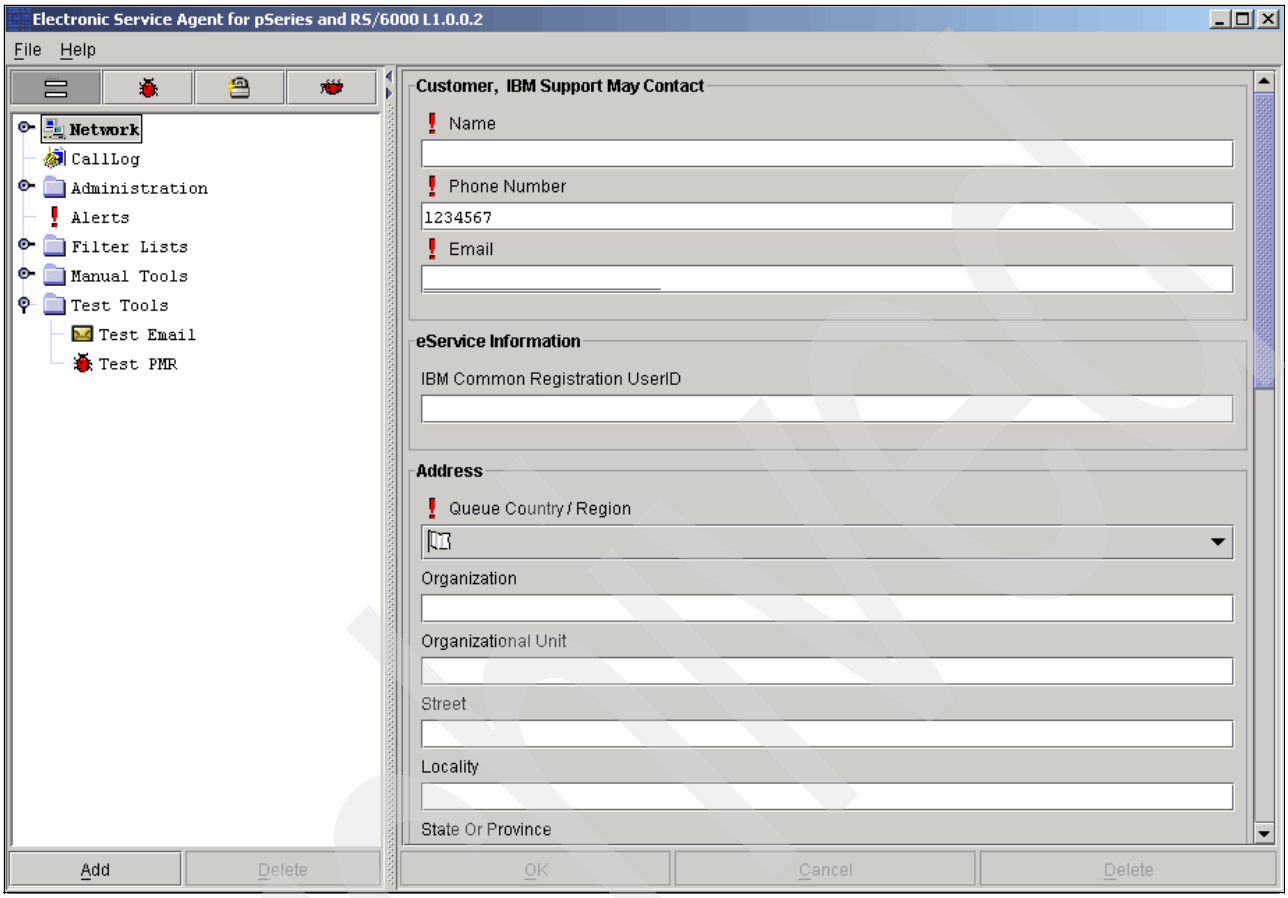


Figure 9-6 Service Agent for Linux: Advanced menu

9.4 Mixed partition configurations

The System p server and Electronic Service Agent can operate with a variety of configurations using AIX and Linux operating systems. The Service Agents do not communicate directly to each other. However, they can share a gateway SACM. Figure 9-7 on page 129 shows a sample configuration.

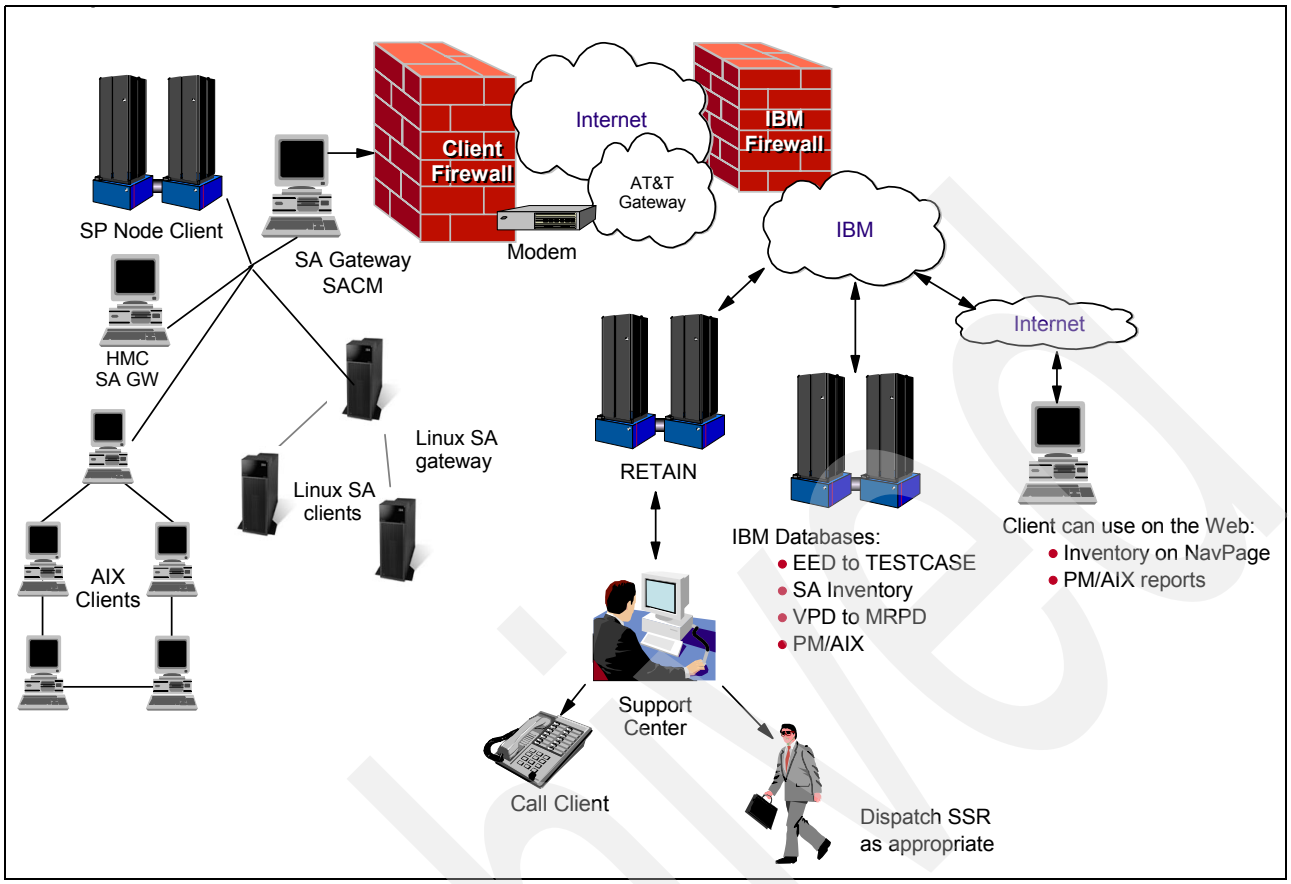


Figure 9-7 System p network with Linux and AIX Service Agents

The following samples describe how Service Agents can operate in these configurations.

Linux operating system (OS) environments have the following characteristics:

- Linux OS SACM
- Linux OS gateways
- Hardware problems automatically transmitted to IBM
- Hardware inventory collected and transmitted to IBM

AIX OS environments have the following characteristics:

- AIX OS SACM
- AIX OS gateways
- Hardware problems automatically transmitted to IBM
- Hardware inventory collected and transmitted to IBM
- Software inventory collected and transmitted to IBM

9.5 Service Agent for Linux on System x

The Electronic Service Agent for System x for Linux or Windows in a stand-alone environment or Director Extension environment use the same user guides and readme file. The following text is from the readme file of the most recent ESA for System x. You can obtain the code, user guides, and readme file from the Electronic Services Web site:

`http://www.ibm.com/support/electronic`

9.5.1 Stand-alone environment

On Linux, installation and deinstallation of Electronic Service Agent is restricted to users with *root* authority. Access to programs providing control over Electronic Service Agent requires the use of a special user account *esadmin*.

Electronic Service Agent on Linux requires that IBM Director Agent Linux Version 5.10 or later is installed and running. Before you install IBM Director Agent on Linux, make sure that you have installed all of the necessary device drivers. This might require installing service processor device drivers or the IBM LM78 and SMBus device drivers for Linux:

1. Ensure that all monitored servers have the correctly configured machine type, model, and serial number.
2. Ensure that the person installing Electronic Service Agent has *root* authority.
3. Create the ServiceAgent group and user. Type the following commands as *root*:

   ```
   #groupadd esa
   #useradd -m esadmin -p welcome
   ```

4. Make sure that the cron daemon is running from a command prompt. Type the following command as *root*:

   ```
   # /etc/init.d/crond status
   ```

5. If the cron demon is running, this message appears:

   ```
   crond (pid 1603) is running...
   ```

6. If the cron demon is not running, issue the following command to start it:

   ```
   # /etc/init.d/crond start
   ```

7. Edit the sudoers file to allow the /opt/IBM/DSA/collectall (IBM inventory collector) to be executed by esadmin without a password.
8. From a command prompt, type the following command as *root*:

   ```
   #/usr/sbin/visudo
   ```

9. Append the following line to the end of the file:

   ```
   esadmin   ALL=(ALL)     NOPASSWD: /opt/IBM/DSA/collectall
   ```

9.5.2 IBM Director Extension

The general requirements for the Director Extension are:

1. Ensure that all monitored servers have the correctly configured machine type, model, and serial number.
2. Ensure that the person installing Electronic Service Agent has *Administrative authority*.
3. Ensure that all monitored servers are under warranty or under an IBM Service agreement.
4. Ensure that IBM Director has completed the initialization of the physical inventory for the machines to be supported by Electronic Service Agent by checking the physical inventory using the IBM Director console.

All supported systems must be initialized prior to Electronic Service Agent enrollment:

- Ensure that you have supplied accurate contact information when configuring Electronic Service Agent.
- It is particularly important that you configure the location details of your managed systems accurately. *Recording location details incorrectly delays IBM service delivery.* Similarly, if you record your managed systems' location details incorrectly, IBM service

representatives will not be dispatched to the correct site location after a hardware problem is reported.

Installing files on Linux

To install Electronic Service Agent on your IBM Director Server:

Remember: The installation requires *Administrator* privileges.

1. Log in as the user *root*.
2. Enter **cd** to the directory where you stored the installation program.
3. Execute the following command:

   ```
   ./5639-n89-de50.bin
   ```

4. At the Electronic Service Agent Setup panel, click **Next** to continue with the program setup.
5. If you accept the terms and conditions of the License Agreement, click **Yes** to continue with the setup program.
6. Click **Finish** to complete the installation.

10

Service Agent for the Hardware Management Console

The *Hardware Management Console (HMC)* has a unique Service Agent (SA). You use the HMC in the System i, System p, and System z environments. This chapter contains information for each of these environments.

10.1 The Service Agent and HMC on System i and System p

Four major components make up the Service Agent environment on HMC machines:

- The *Electronic Server System (ESS)* process runs only on the gateway HMC. The ESS handles all requests for data input and retrieval from the centralized database.
- The *On Demand Server (ODS)* process runs on all of the defined HMCs and handles all Service Agent communication activities for that host. The ODS sends data to the ESS process as necessary or makes a request to Service Agent Connection Manager (SACM) to call IBM. Events from the Service Focal Point (SFP) are reported to IBM directly using an Internet connection or a modem that is attached to the gateway server. Service Agent calls IBM to report that it is healthy, one time in every health-check interval.
- *Service Agent Connection Manager* is a stand-alone process. You can configure it to communicate with IBM using an existing Internet connection or modem. It can exist on any HMC or stand-alone System i5 machine and can support multiple Service Agent Gateway connections.
- The *User Interface* allows you to set up and define the HMCs that Service Agent monitors. The graphical user interface (GUI) is invoked from Web-based System Manager (WSM) by selecting Service Agent from the Service Applications. Then from the WSM service menu, you select TASKS for the Service Agent User Interface. Utilize the User Interface for advanced functions and customization of the system, as well as to configure complex systems and multilevel networks.

10.1.1 Planning your HMC environment for Service Agent

Establish the overall HMC environment before you activate Service Agent. Do not start Service Agent processes if the network is not configured on the gateway or your HMC.

Review and complete the following items:

1. On new installations, the HMC host name is a default name. Assign it a new name that suits the client's network environment.
2. On the HMC gateway, ensure that the modem and the phone line are connected if you use them. Check the physical connections to verify that the modem and the phone line are connected.
3. If you use the Internet, make sure that the HMC has connectivity to the network.
4. If HMC is a client, start Service Agent only after you set up the network properly.
5. After you assign the host name, determine the type of Service Agent to apply: gateway or client.

Figure 10-1 on page 135 shows the HMC high-level activation flow.

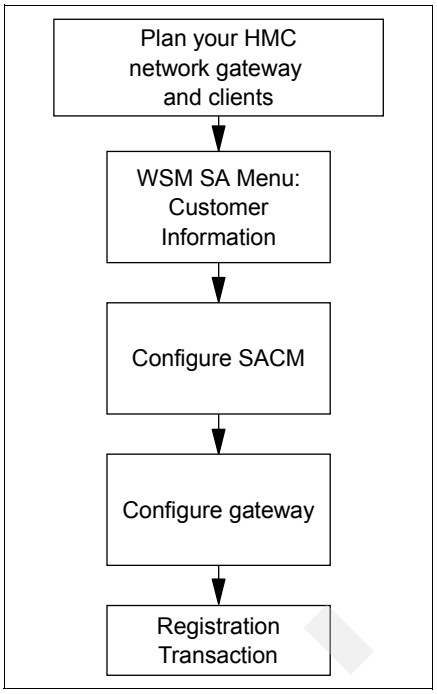


Figure 10-1 Service Agent HMC activation flow

10.1.2 Installation and activation

On HMC machines, Service Agent is installed as part of the HMC code. Service Agent appears on the HMC menu.

Complete the following steps to activate HMC Service Agents:

1. In the Navigation Area of the HMC menu, select **Service Applications** → **Service Agent**, as shown in Figure 10-2 on page 136.

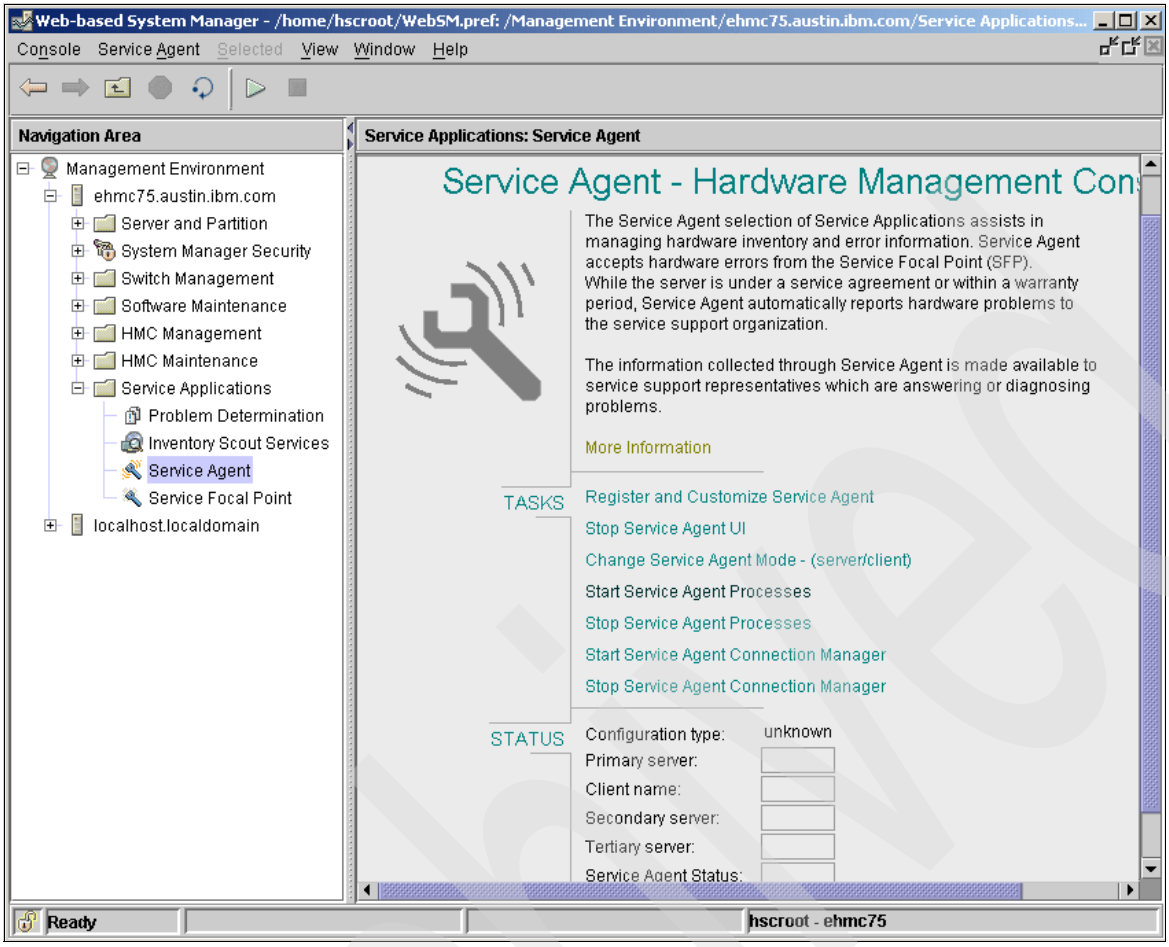


Figure 10-2 HMC main menu: Service Agent selected

2. When you select Service Agent under the Service Applications on the HMC Service Agent menu (Figure 10-3), Service Agent detects whether it is activated. If it is not activated, you see the window shown in Figure 10-3. Verify or update the information, and then click **Continue**.

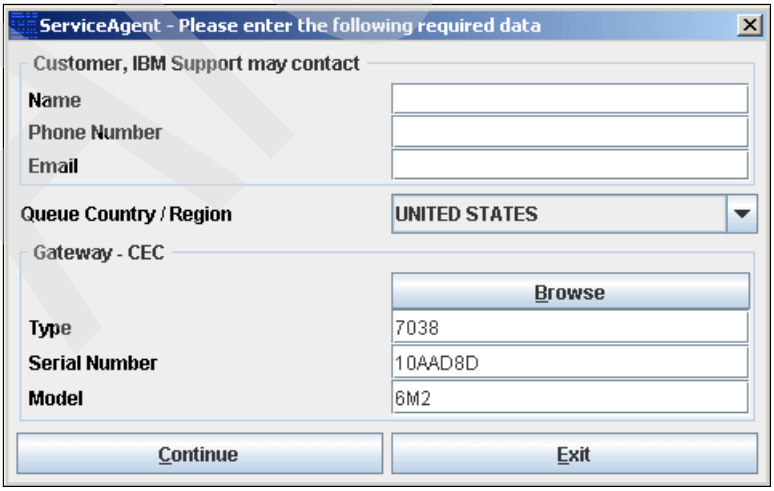


Figure 10-3 HMC SA information panel

3. Next you see the window that is shown in Figure 10-4, the HMC Service Agent activation wizard. Type the requested information and click **OK**.

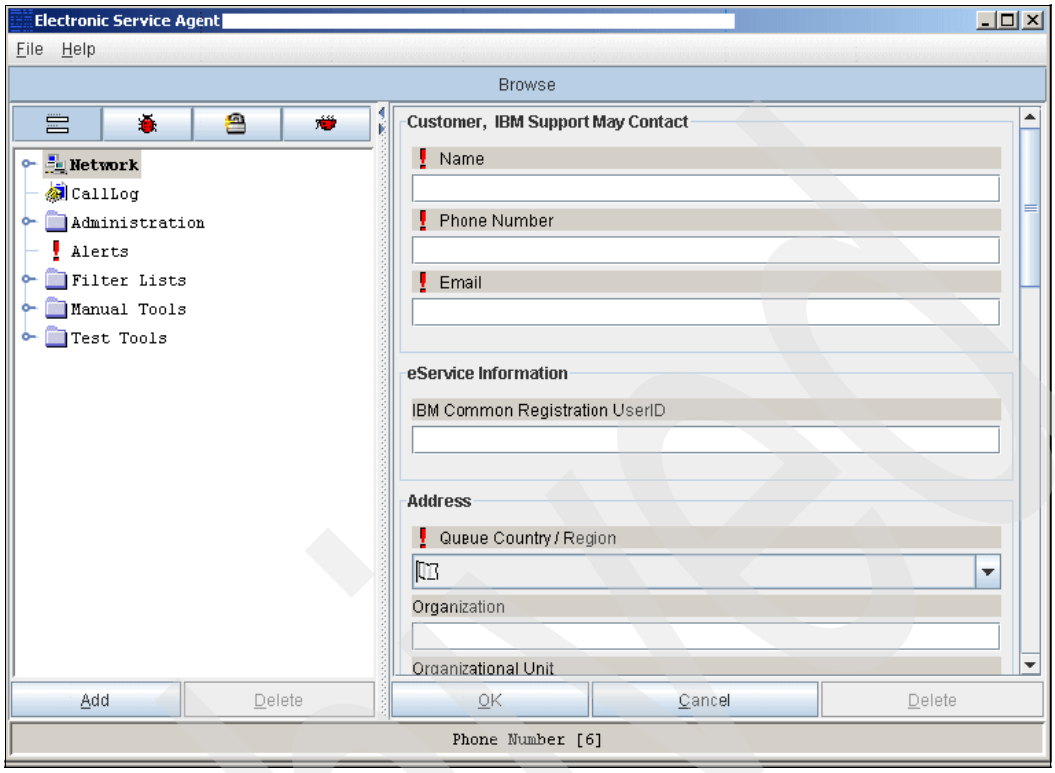


Figure 10-4 HMC SA wizard

10.1.3 Maintenance

The HMC Service Agent is updated through new releases of HMC code. The HMC Service Agent GUI is invoked from the WSM when you select **Service Applications** → **Service Agent**.

The Service Agent menu consists of two major sections: TASKS and STATUS, as shown in Figure 10-5 on page 138.

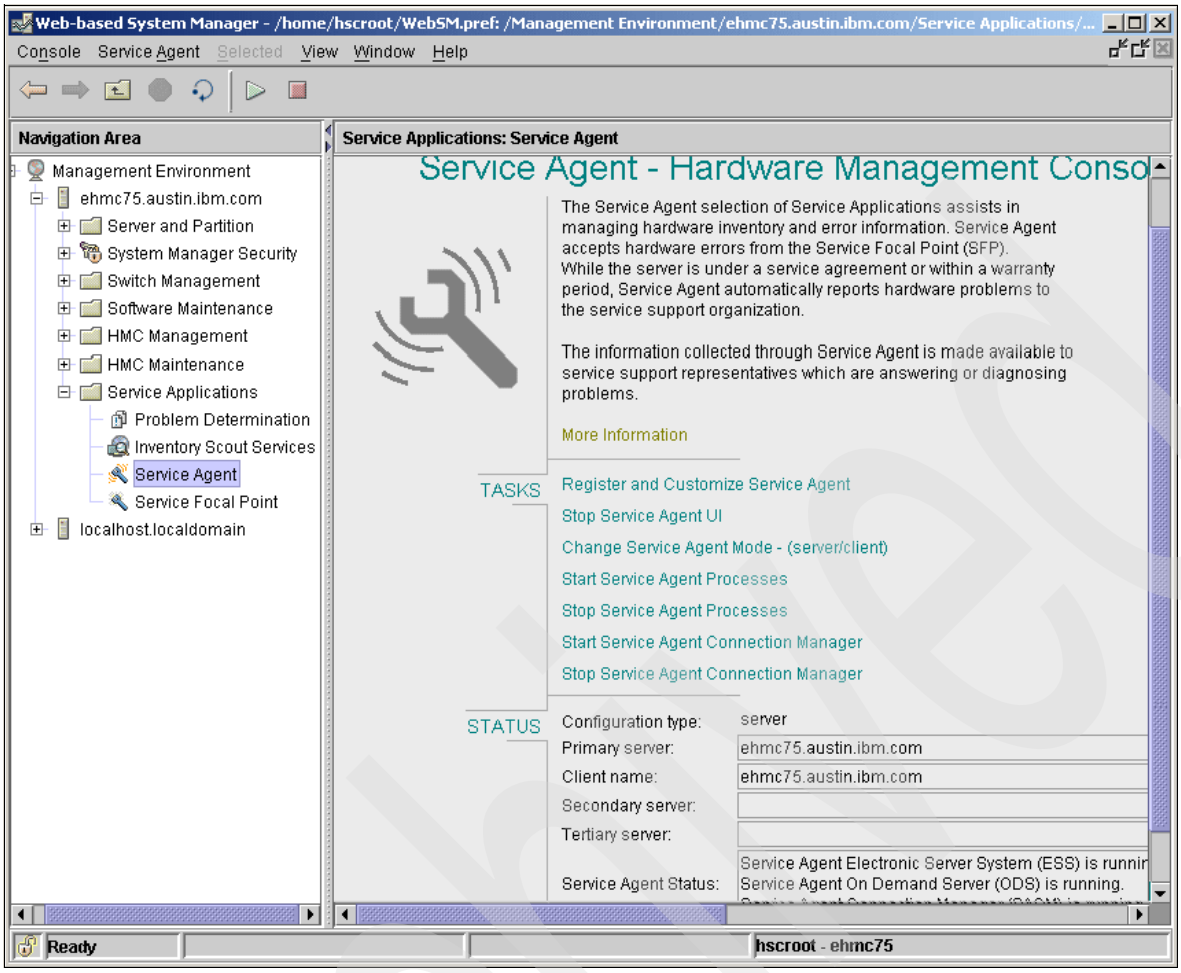


Figure 10-5 HMC SA menu expanded

In the TASKS section, you start and stop a process, change the function, update the host name, and access the user interface.

In the STATUS section, you see information about how this HMC is configured (server/client) and the status of the Service Agent processes.

10.2 Electronic Service Agent for System z

Electronic Service Agent for System z has two functions: automatic hardware problem reporting of connected I/O devices and system inventory collection for monitored systems. With these functions, Electronic Service Agent for System z can monitor, track, and capture system inventory and hardware errors.

Electronic Service Agent for System z (zSA) is designed to reduce the downtime of IBM input/output (I/O) devices when a hardware problem occurs or is predicted to occur. Detected I/O hardware failures are sent immediately to the IBM Support Center. When system problem descriptions and inventory information are available to IBM Service or Support Center representatives, they can better assist in diagnosing problems. With the early knowledge about potential problems provided by the Electronic Service Agent, IBM can proactively respond to clients and can assist in maintaining higher availability and performance.

Service Agent is also designed to transmit, on a scheduled basis, performance and service inventories to IBM. This information allows IBM support or authorized client representatives to obtain and view necessary information. Service Agent for System z is designed to work with z/OS Version 1.4 and higher.

Electronic Service Agent for System z has been enhanced with several new features, including secure data transmission, direct communication mode with IBM, and additional data collection capabilities.

Several of these features require Hardware Management Console (HMC) Version 2.9 and higher, which is available with the IBM System z9™ Server.

Figure 10-6 shows a sample System z and Service Agent environment.

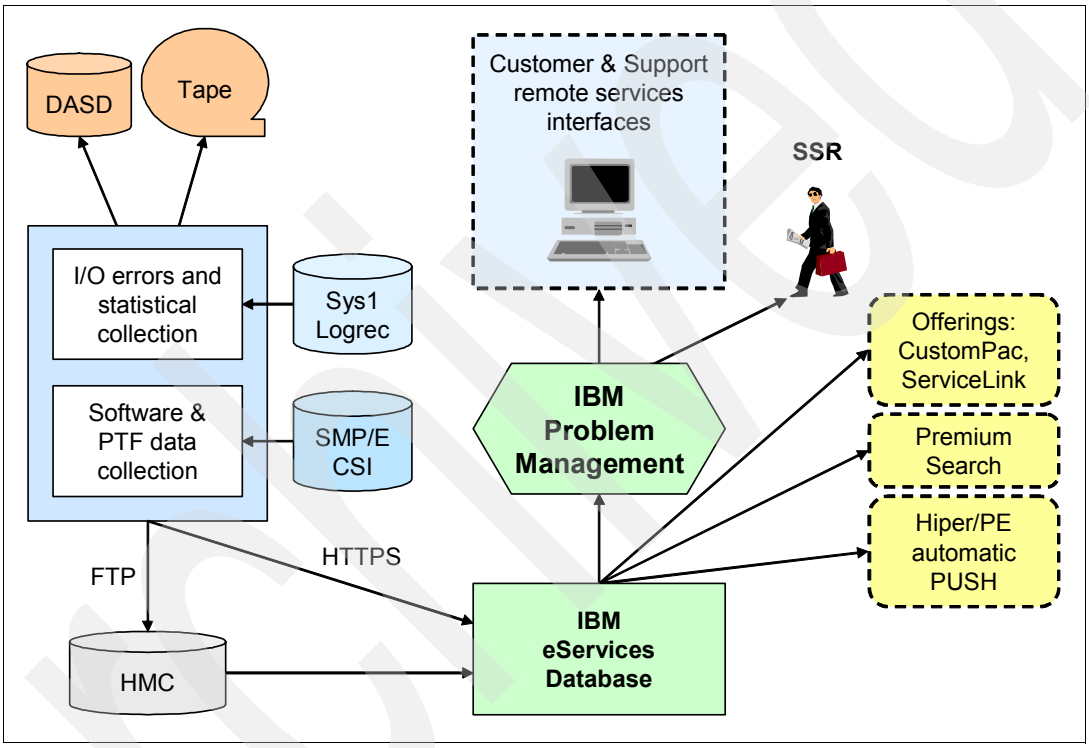


Figure 10-6 Service Agent for System z overview

10.3 HMC activation

Clarification: The following steps are for Service Agent processes. These steps do not have any relationship to the focal point HMC that reports errors on processors.

To activate the HMC Service Agent, follow these steps:

1. Log on as *ASCADMIN*.
2. The HMC menu (shown in Figure 10-7) opens. In the Views pane, select **Console Actions**.
3. Now the HMC menu displays options in the Console Actions Work Area. The Console Actions Work Area is shown in Figure 10-7. Select **Hardware Management Console Settings**.

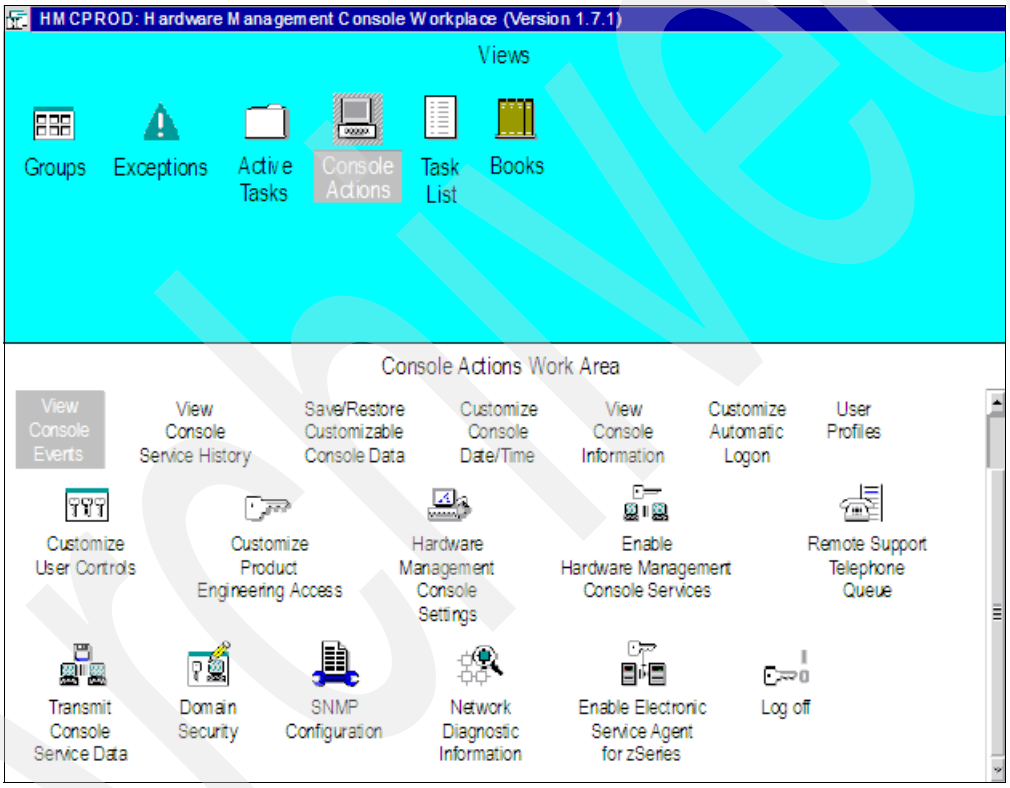


Figure 10-7 HMC Workplace™

4. A pop-up window opens on the HMC menu and displays an IP address. Record the address. You need this address to complete a field in the Service Agent collection attributes. Then click the upper left corner and select **Close** to close this pop-up window.
5. In the Console Actions Work Area in Figure 10-7, select **Enable Electronic Service Agent for zSeries®**.
6. The Service Agent License Agreement window shows in Figure 10-8 on page 141. To continue with the Service Agent activation process, page through the agreement and select **I AGREE**.

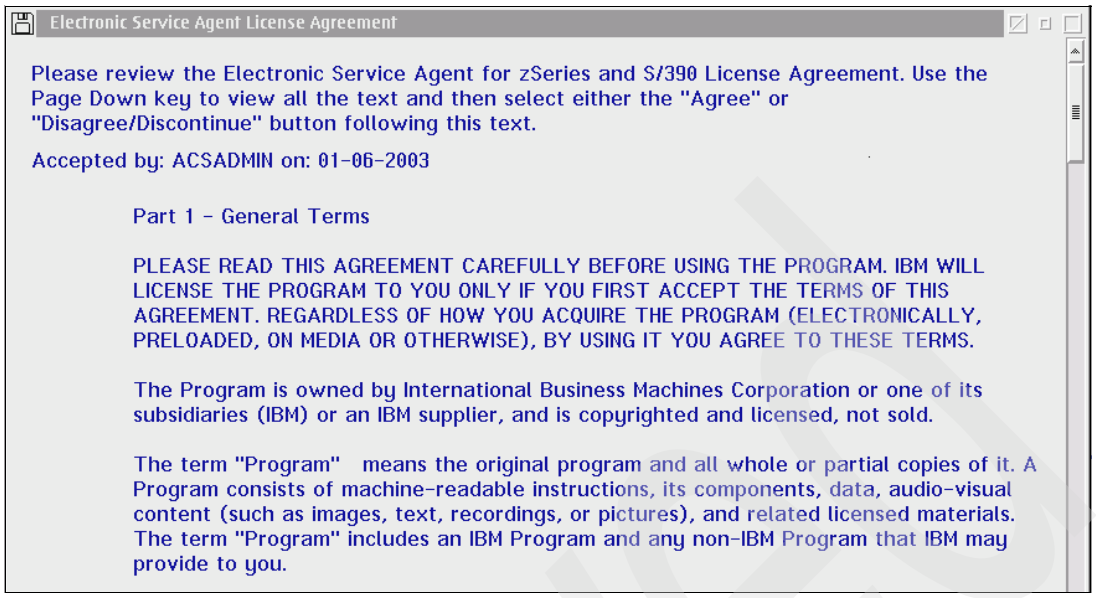


Figure 10-8 Service Agent for System z: License Agreement window

7. In the next window (shown in Figure 10-9), client contact information is used to register this HMC with Service Agent and IBM. IBM uses this information to communicate regarding service requests. Change or correct any of the client information as necessary. Click **Continue**.

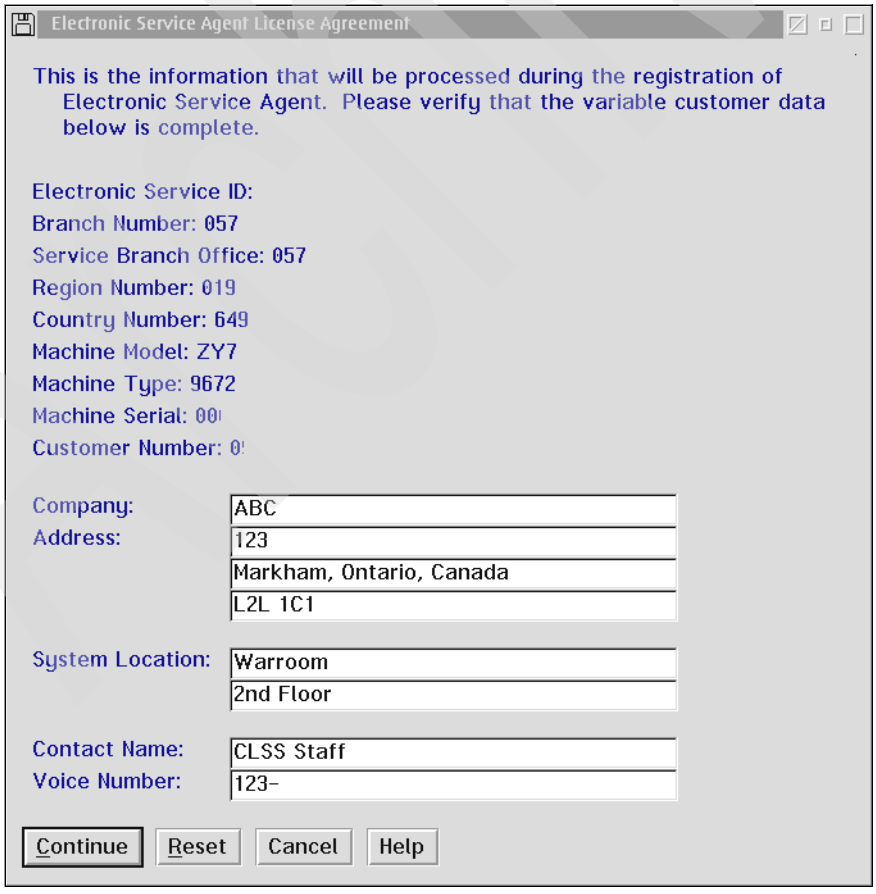


Figure 10-9 Service Agent for System z: Updating client information

8. In the next window (shown in Figure 10-10), you enable or disable subsections of the Service Agent, and you set the FTP password that is used by the OS/390® software to send information to the HMC. Select the types of data that you want collected and forwarded to IBM. Enter an FTP password, which you also must enter into the OS/390 software. Click **Continue** when you are finished.

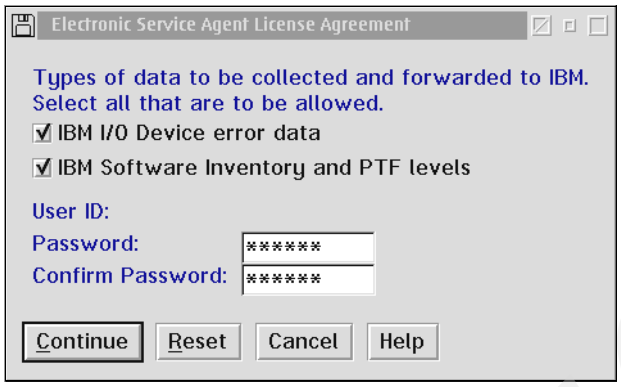


Figure 10-10 Service Agent for System z: Enabling or disabling the types of data to send to IBM

9. In the next window, select the time of day for the daily transmission of the inventory information that is sent to IBM. Click **Finish** to complete the configuration process and to store the data within the HMC.
10. The HMC sends the automatic registration transaction to IBM. You must complete this transaction before IBM can accept any problem data or inventory transactions.
11. Add a step in the EREP JCL job to run and capture Service Agent data.
12. Create started task IDs and started task entries in the STARTED RACF® class for HESRDLOG using the supplied sample job.
13. Configure Service Agent by editing the dataset hlq.HESPARMS. Change the HMC IP address and HMC FTP password to match that of your installation.
14. Start the hardware collection. Start the HESRDLOG procedure in the SYS1.PROCLIB dataset.
15. Enable a scheduled collection for the data types of your choice.
16. Enable the collection and reporting for software data, performance data, or both.

Now, you have activated the HMC for Service Agent.

11

IBM Electronic Service Agent for System x

The IBM Electronic Service Agent (SA) for System x automatically ships with the System x platform without an additional charge. SA monitors events and transmits system inventory information to IBM. SA has been available since 2000 for the IBM Director environment and available for the stand-alone environment since 2003.

This chapter is about the IBM Electronic Service Agent for System x.

11.1 IBM Electronic Service Agent for System x

IBM Electronic Service Agent for System x is designed to reduce the downtime when a hardware problem occurs or is predicted to occur. Detected hardware failures are sent immediately to the IBM Support Center. The regular schedule of inventory checks enables support representatives or client representatives to quickly check the machine's configuration.

Service Agent is designed to work an all models of the System x product line. Support for new servers is available typically after General Availability of the new machines in order to allow for proper testing. The System x Service Agent user guides and readme file show the current listing for each release. The user guides and readme file are on the Electronic Services Web site under Service Agent Reference Guides:

- For the stand-alone environment version of the user guide, go to:

  http://www.ibm.com/support/electronic/serviceagent
- For the Director Extension version of the user guide, go to:

  http://www.ibm.com/support/electronic/serviceagent

Automatic hardware problem detection

Service Agent both detects and generates hardware problem events. Service Agent is pre-configured to detect specific hardware failure base events that are generated by managed systems that are enabled and enrolled for Service Agent.

Service information collection

The inventory function of Service Agent for System x collects system information about memory, hard disk drives or RAID drives, peripheral component interconnect (PCI) adapters, communication information, and environments, such as power, fan, and temperature. You can view service information for monitored systems at the following Web site, using your IBM ID for authentication:

https://www.ibm.com/support/electronic

11.1.1 The stand-alone environment

The stand-alone environment on the System x platform (shown in Figure 11-1 on page 145) has the ability to work with any system management tool. The Service Agent has all of the modules that are needed to monitor, gather, and report events and inventory. Major features are:

- Secure Internet access to IBM through the Hypertext Transfer Protocol Secure (HTTPS)
- Restricted use of Service Agent to users with Windows Administrative rights
- Access through Service Agent to IBM through an authenticating proxy
- Easy installation and configuration by using wizards
- History panel with historical details of significant system events, including enrollment history, inventory history, and Problem Management Record (PMR) history
- Installation can be done without a system reboot.
- Lightweight application uses minimum system resources.

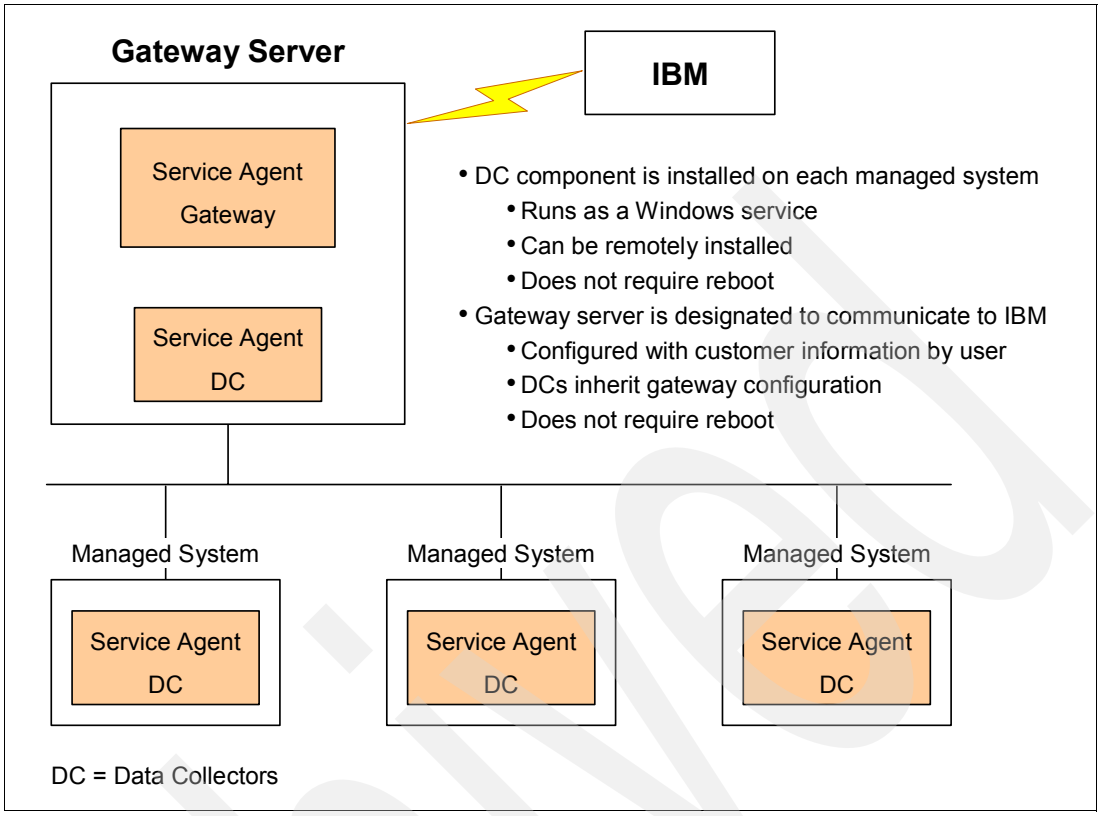


Figure 11-1 Stand-alone environment

11.1.2 IBM Director Extension

Service Agent is an extension to the IBM Director management application. Install Service Agent on your IBM Director Server as shown in Figure 11-2 on page 146. You do not need to install Service Agent on each of your managed systems.

This agent monitors your System x servers for hardware errors. Hardware errors that meet certain criteria for criticality are reported to IBM. Service Agent also administers hardware and software inventory collections and reports inventory changes to IBM. All information is transmitted through a secure link and stored in a secure IBM database.

The information technology (IT) administrator must have a working knowledge of IBM Director when working with Service Agent. If more in-depth knowledge of IBM Director is required, refer to:

`http://www.ibm.com/systems/management/director/`

The features of Electronic Service Agent Director Extension are:

- The releases are concurrent with each version of Director
- It supports the Windows and Linux versions that are supported by Director.
- The Director Extension supports all System x machines that are supported by Director.

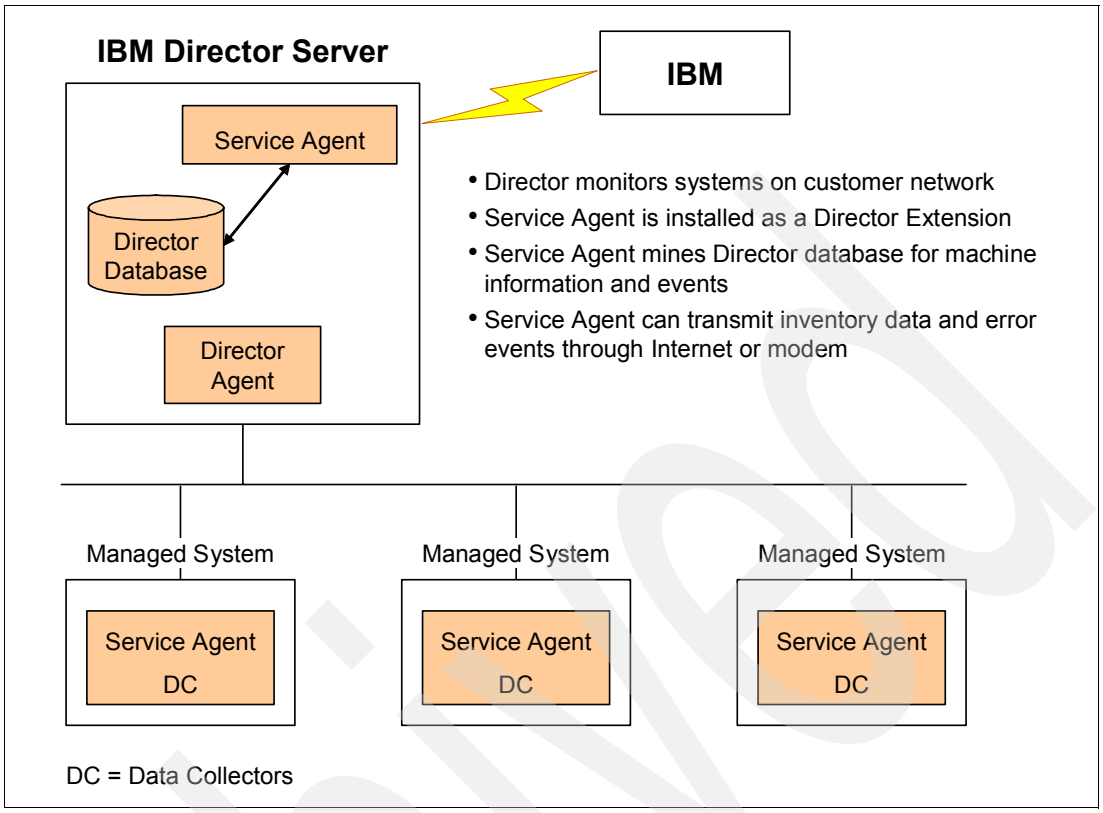


Figure 11-2 IBM Director Extension view

11.2 Stand-alone planning, installation, and activation

The Service Agent code is available for download from the Electronic Services Web site under Service Agent, **Download ESA**:

`http://www.ibm.com/support/electronic/serviceagent`

Important: Service Agent automatically detects if it is installed in a stand-alone environment or in an IBM Director environment. If it is installed in an IBM Director environment, you must ensure that Service Agent is installed on the IBM Director Management Server.

Figure 11-3 on page 147 shows the flow of the Service Agent installation and activation process.

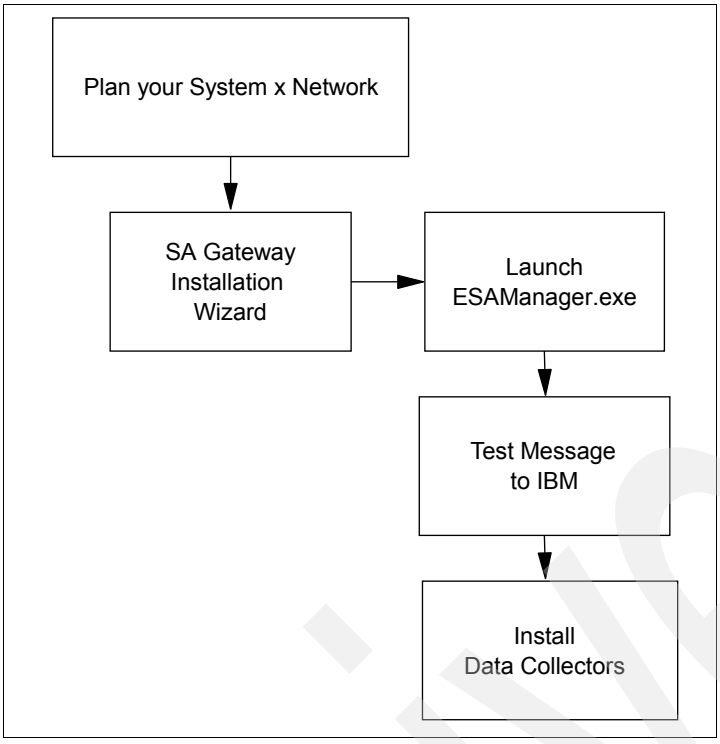


Figure 11-3 System x stand-alone activation flowchart

11.2.1 Planning

Early planning can save you valuable time and prevent confusion and delays later. Understanding how to set up the Service Agent application to best cover your IT environment makes the experience much more effective.

Consider these items assist you as you make Service Agent decisions:

- Ensure that the person who installs Service Agent has Windows *Administrative authority.*
- Ensure that the person who installs Service Agent has an IBM ID to enter on the Advanced tab.
- Ensure that the gateway machine and all monitored servers are under warranty or an IBM Service Agreement.
- Ensure that you supply accurate contact information when configuring Service Agent.
- Configure the location details of your gateway and managed systems accurately. IBM Service Delivery depends on this information in order to deliver timely service, including callbacks and the dispatch of the field personnel.

Important tip: Install the gateway before you install the Data Collectors.

Table 11-1 on page 148 lists the system requirements to consider for the stand-alone system.

Table 11-1 System requirements for a stand-alone environment

Operating system	All versions of Windows and Linux supported by Director Agent
Microprocessor	x86 (Pentium® or higher)
Hard disk space	110 MB available: The gateway requires 100 MB, plus 10 MB per Data Collector
Modem or Internet access	Required for gateway machine
Monitor	Super VGA monitor with the screen resolution set at 800 x 600 (minimum), small font setting, and 256 colors

11.2.2 Installation wizard

The installation wizard leads you through the installation process, beginning with the window shown in Figure 11-4:

Requirement: You must install and configure the gateway before installing the Data collectors. Electronic Service Agent stand-alone environment does not require a reboot of either the gateway or the data collectors.

1. In the first wizard window that opens, select your installation type. In this example, we select **Gateway**. Click **Next**.

Figure 11-4 Stand-alone installation wizard

2. In the next window, select the preferred language from the drop-down list to view the Service Agent License Agreement. Click **Next**.
3. Select the option to accept the terms of the agreement. Click **Next**.
4. The next window prompts you to specify the directory placement of the Service Agent code. Accept the default or select **Browse** for a new location. After you specify a location, click **Next**.
5. The next window confirms your directory selection. If you agree, click **Next**.

6. Installation Wizard begins to install Service Agent. The wizard shows a window with a progress bar so you can see the progress of the installation.

7. After installation, launch the *eSAManager.exe*. Click the icon on the desktop or use Start Programs.

   Tip: You will be able to configure data collection systems after the gateway machine is properly configured.

8. To continue installation on the rest of the machines in your enterprise, run the installation wizard for each machine. This time, select **Data Collection** on the first wizard window (shown in Figure 11-4 on page 148) for the installation type. No restart or reboot is needed after installation.
9. After the installation is complete on the last (or only) machine, the System Status panel (shown in Figure 11-5) of the configurator program appears. Select **Automatically detect Gateway System** to have the Data Collector configure itself, if the Data Collector is on the same network as the gateway. If the Data Collector is on a separate network, select the **Manually enter the port and network information** option. Select **Next**.

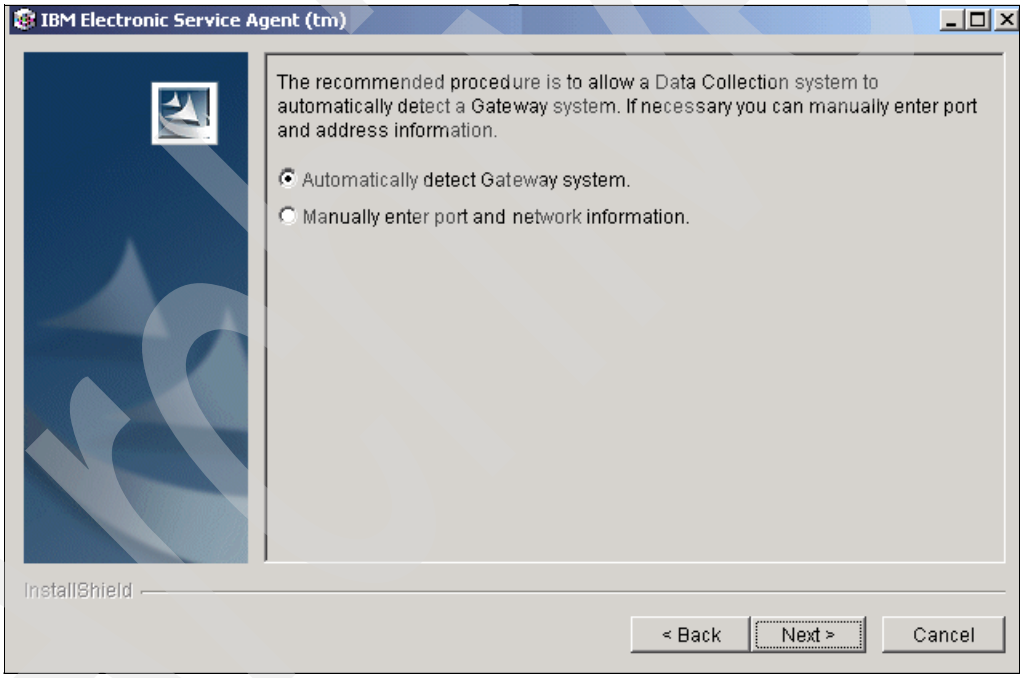


Figure 11-5 Data collection configuration panel

10. When the task completes, there is a completion display (as shown in Figure 11-6 on page 150) with the message that `Electronic Service Agent has now been installed on this system`. To close the wizard, click **Finish**.

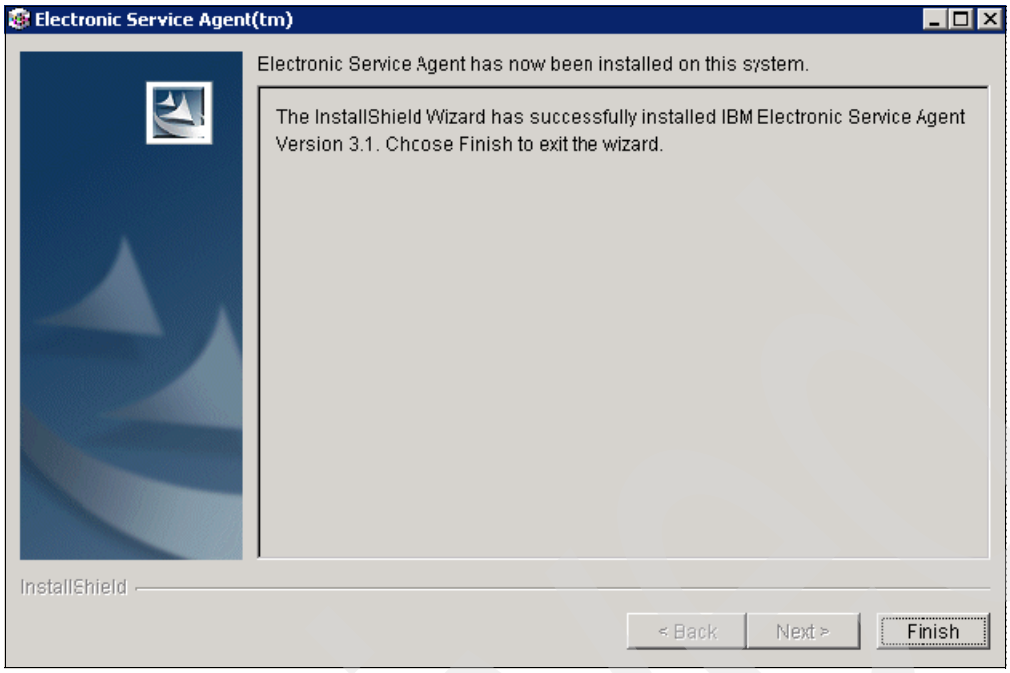


Figure 11-6 Service Agent configuration completion window

11.2.3 Upgrade information

To upgrade an existing Service Agent, follow these steps:

1. Download the new Service Agent files.
2. Install Service Agent on your gateway. You must upgrade the gateway before you upgrade the Data Collectors.

   A downlevel gateway cannot handle transactions from Data Collectors that have a new Electronic Service Agent release. A higher level gateway can handle downlevel Data Collector transactions.
3. Invoke the installation wizard. It detects that you have an existing Service Agent and uses existing configuration files. You do not need to launch eSAManager.exe unless your configuration needs to be updated during this upgrade.

11.2.4 Configuration and maintenance

The Service Agent Configuration Manager provides the user-controlled functions of Service Agent. These functions provide you with the ability to perform actions, such as naming the callback contact and identifying the location of a monitored machine. If all monitored machines are located in one subnet, have the same callback contact, and are in the same physical location, you only need to configure the gateway, because all of the monitored machines inherit the gateway configuration.

If any monitored machines have different Service Agent configurations, such as a monitored machine that is located in a different location than the gateway, you must run the Configuration Manager on the monitored machine.

The Service Agent configuration contains the following information:

- System Status: Reports the current status of Service Agent and allows you to start and stop it
- Company: Contains information about your company
- Contact: Contains information about the person responsible for this system
- Location: Describes where this system is located
- Communications: Contains information about the network setup
- Advanced: Helps you define who can view the data
- History: Provides historical details about significant system events
- General: Shows system details, “about” information, and legal notices

Figure 11-7 shows the Windows location of Service Agent Manager (esaManager).

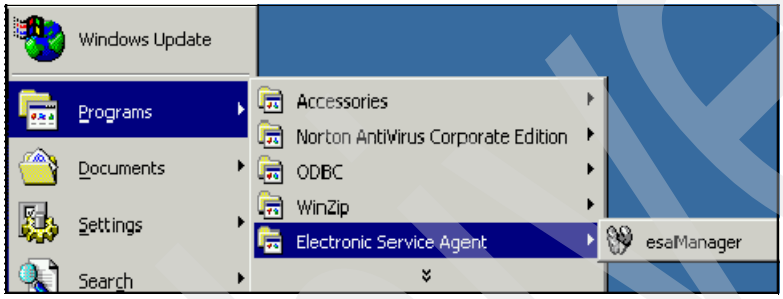


Figure 11-7 Windows location of Service Agent Manager main menu

Figure 11-8 shows the main menu view of Service Agent Manager. There are four major sections with multiple tabs in each section.

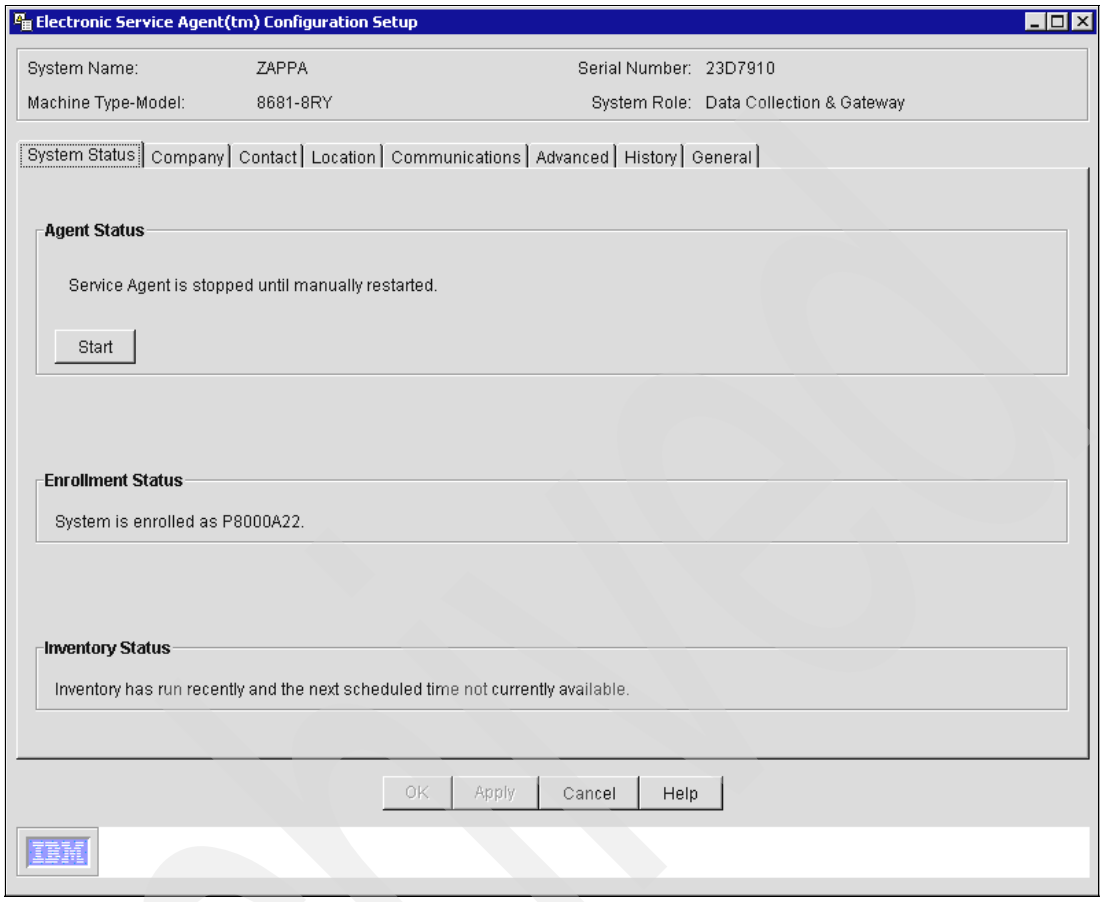


Figure 11-8 Service Agent Manager main menu

On the Advanced tab (shown in Figure 11-9 on page 153), you can register two IBM IDs to view the Service Agent inventory information and to use that information during Premium Search queries.

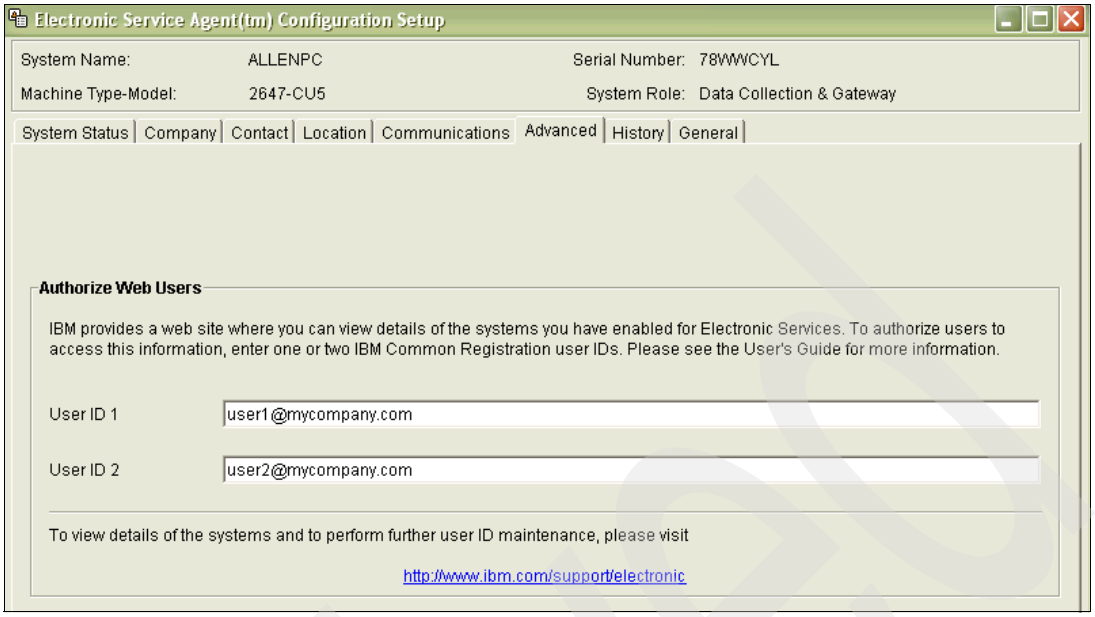


Figure 11-9 Electronic Service Agent for System x: Advanced tab

The History tab (shown in Figure 11-10) provides historical details about significant system events, such as enrollment history, inventory history, and Problem Management Report (PMR) history.

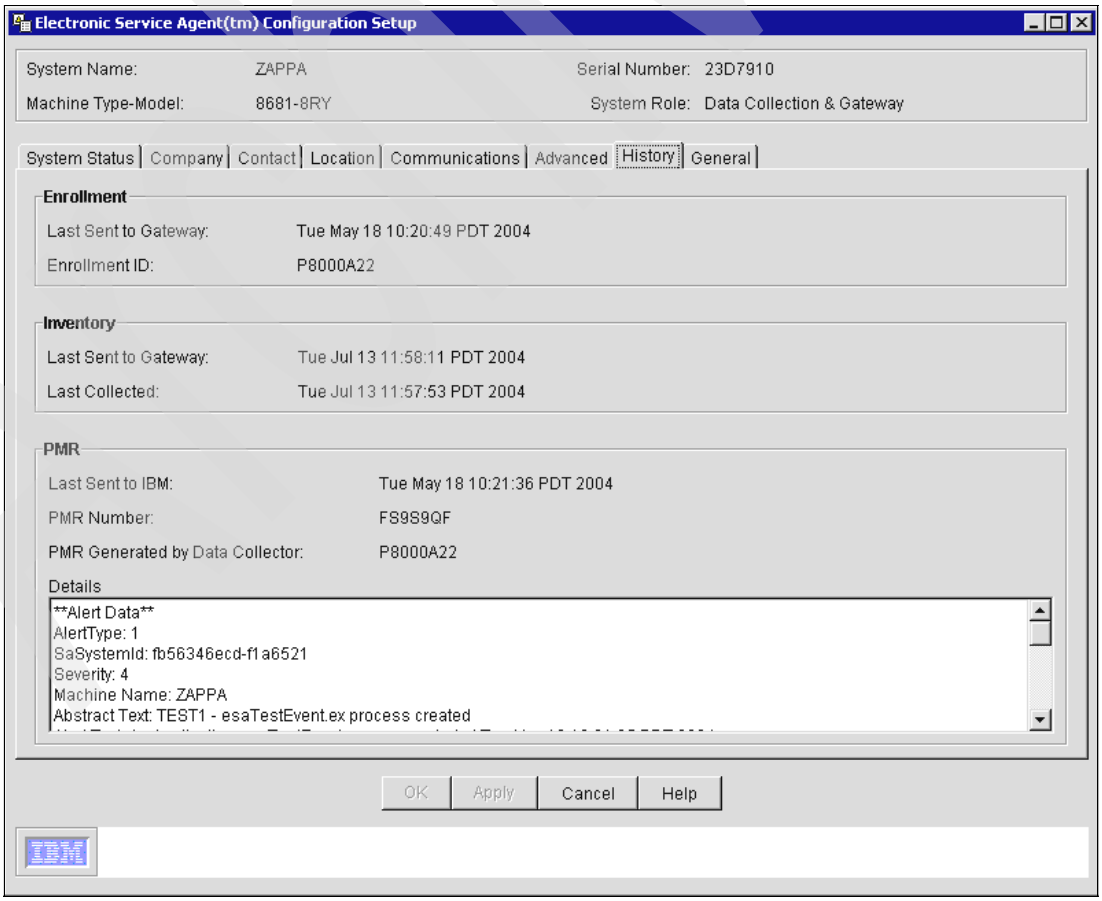


Figure 11-10 Service Agent menu: History tab

The items on the History tab include:

- Enrollment:
  - Last Sent to gateway is the locale-sensitive time stamp of when the enrollment status was sent to the *Service Data Receiver (SDR)*, the facility on the IBM server that receives messages from Service Agent.
  - Enrollment ID is the ID with which Service Agent is enrolled with IBM.
- Inventory:
  - Last Sent to gateway is the locale-sensitive time stamp of when the inventory status was last sent to IBM.
  - Last Collected is the locale-sensitive time stamp of when the inventory was collected.
- PMR:
  - Last Sent to IBM is the locale-sensitive time stamp of when a PMR was last sent to IBM.
  - PMR Number is an identifying number from IBM for the last submitted PMR. Give this number to the IBM Support Representative when you call IBM about a problem.
  - PMR Generated by Data Collector is the number of the system that generated the PMR. In most cases, the number is the same as the number that appears in the message `System is enrolled as nnnnnnnn` when you enroll a machine with the SDR. However, if a system is generating PMRs on behalf of another system, this number can differ from the number of the system you are using.
  - Details of the last submitted PMR are only available on the gateway User Interface and are not translated.

11.2.5 Uninstall process

Before you uninstall Service Agent, be sure that your machine is not a gateway that is used by one or more Data Collectors. Uninstalling the program disables Service Agent on those machines.

To uninstall Service Agent, use the Windows Add/Remove programs function:

1. From your Windows desktop, select **Start** → **Control Panel**.
2. In the Control Panel window, select **Add/Remove Programs**.
3. In the Add/Remove Programs window, select **IBM Director Agent** and click **Remove**. You must remove this program first.
4. In the same window, select **IBM Electronic Service Agent** and click **Remove**.

11.3 Director Extension: Planning, installation, and activation

Figure 11-11 shows the activation process for the Service Agent in the Director Extension environment.

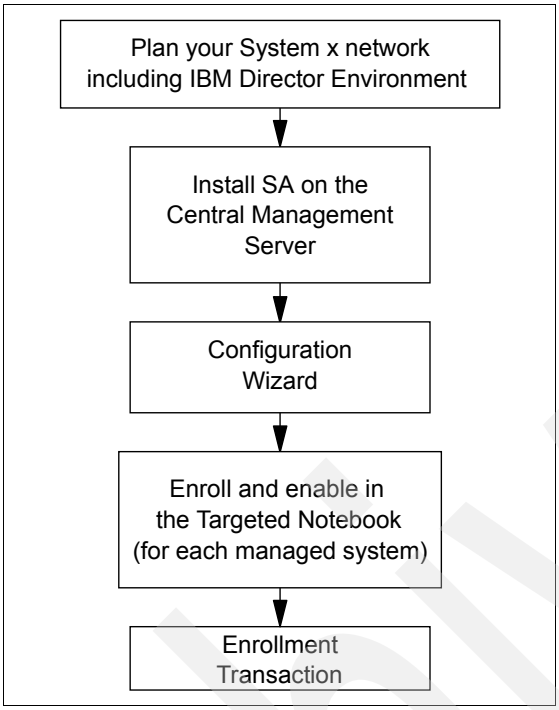


Figure 11-11 System x Director Extension activation flow

11.3.1 Planning for the Service Agent application setup

Early planning can help save you valuable time and can help prevent errors later. Understanding how to set up the Service Agent application to best cover your IT environment helps make the use of Service Agent much more effective.

Consider these items when you make your decisions:

- You need to verify that your systems are supported.
- You must have a SupportLine contract (or similar contract) for IBM Director and Service Agent support.
- You need to ensure that the latest drivers are installed on the hardware.

11.3.2 Installation, configuration, and activation

To install Service Agent on your IBM Director server, follow these steps:

1. Double-click your *setup.exe* file to run the setup program to begin the installation process.
2. In the Language Option window, select the language option that you want to use. Click **OK**.
3. In the Electronic Service Agent Setup window, click **Next** to continue.
4. In the next window, if you accept the terms and conditions of the License Agreement, click **Yes**.

5. In the following window, if you accept the terms and conditions of the Communications Charges Agreement, click **Yes**.
6. In the Question window, click **Yes** to view the readme file and then click **Next**.
7. In the Setup Complete window, select **Yes** to restart your system now.
8. Click **Finish** to complete the installation.

After you install Service Agent, you must configure several settings before you can use Service Agent to monitor your managed systems and perform any other administrative tasks. The Configuration Wizard leads you step-by-step through the configuration process.

To launch the Configuration Wizard, follow these steps:

1. Start IBM Director.
2. In the Tasks list (shown in Figure 11-12), double-click **Electronic Service**.

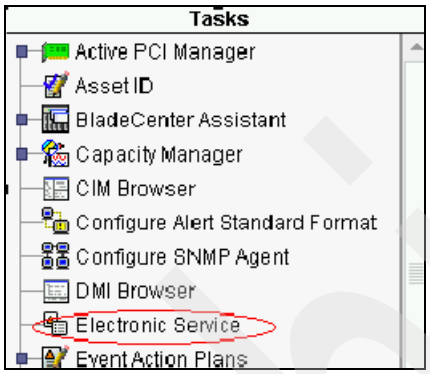


Figure 11-12 IBM Director Task menu

3. The Electronic Service Agent Setup Wizard opens as shown in Figure 11-13. Click **Next**.

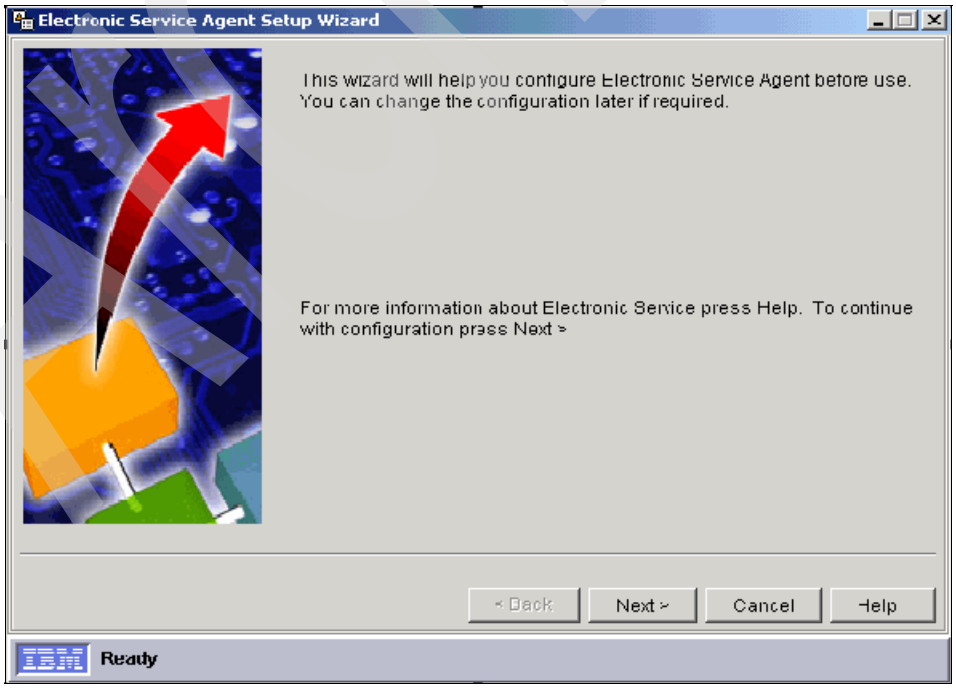


Figure 11-13 Electronic Service Agent Setup Wizard for configuration

4. Select the country (region) where the Director server is located. Click **Next**.
5. Select either Modem or Internet connection. Then, click **Next**.
6. Depending on your communication selection, the next windows configure the modem or the Internet connections. Click **Next** when you are finished.
7. Complete your company information fields of name, phone, and e-mail. Click **Next**.
8. Complete the company contact information fields of name, phone, and e-mail. Click **Next**.
9. Complete the machine location information fields of building, floor, office, city, postal code, state, or province. Click **Next**.
10. *Automatic Upgrade* selection configures Service Agent to download and apply program updates automatically when they are available. This check box is enabled by default. Clear the check box if you do not want this feature. Click **Next**.
11. When you complete the wizard, you see the window stating that you have completed the required configuration for Electronic Service Agent (shown in Figure 11-14). Click **Finish**.

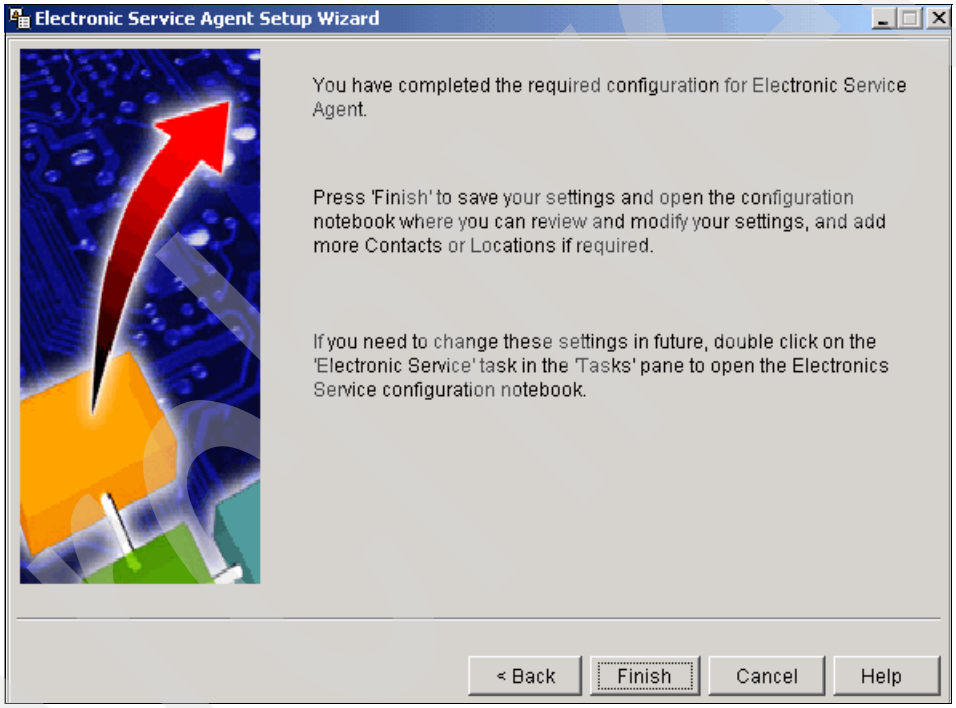


Figure 11-14 Wizard completion panel

The untargeted Service Agent Configuration Notebook automatically appears. Service Agent is now ready for you to perform administrative tasks.

After you properly install and configure Service Agent, you must enable and enroll each of your managed systems for Service Agent before Service Agent can perform information-gathering operations and send Service Requests to IBM.

To enable one or more managed systems for Service Agent, follow these steps:

1. Open the targeted Electronic Service Agent Configuration Notebook. Launch the **Electronic Service Task** that is targeted at an individual managed system, group of managed systems, or multiple selected managed systems.
2. Open the **System** page.
3. Select **Enable for Electronic Service**. Click **Apply** or click **OK** to close the System page.

To enroll a managed system for Service Agent and complete an enrollment transaction, follow these steps:

1. Open the single targeted Electronic Service Agent Configuration Notebook. Launch the **Electronic Service Task** that is targeted at a single managed system.
2. Open the **Test** page.
3. Click **Enroll System**.
4. Wait for the Enroll System Test window to confirm that the transaction has been successful or follow the instructions on the window. Click **OK** to close the Test page.

11.3.3 Maintenance

You can access the Service Agent main menu under two possible locations, the untargeted notebook or the targeted notebook, in the Director Extension environment. The untargeted and targeted notebooks are launched from the IBM Director Console. Refer to your IBM Director online help for more information about using the IBM Director Console.

The Untargeted Notebook Service Agent menu (shown in Figure 11-15) shows several tabs.

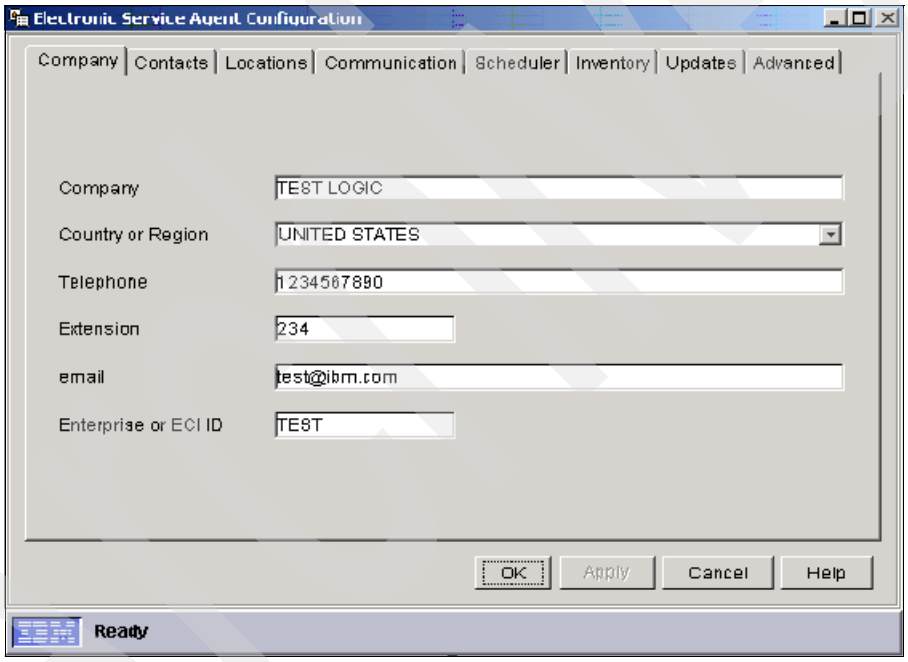


Figure 11-15 Untargeted Service Agent main menu

For example, on the untargeted menu, under the Advanced tab (shown in Figure 11-16), you can register IBM IDs to view the Service Agent information and use in Premium Search queries.

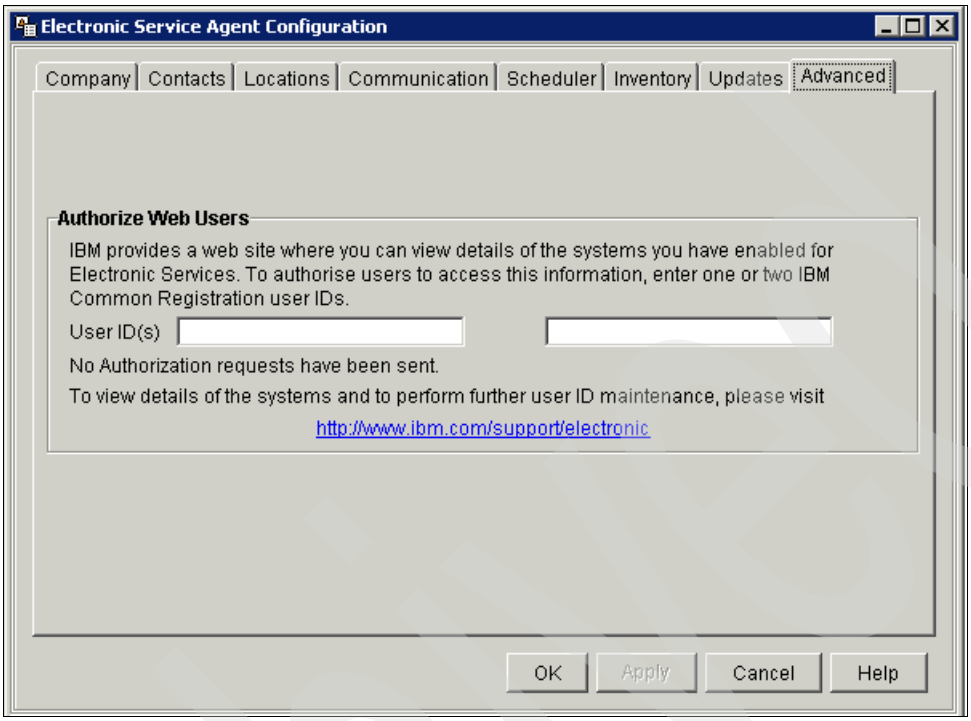


Figure 11-16 Director Extension Service Agent menu: Advanced tab

You can display the targeted menu for these configurations:

- Single-targeted mode: Select a single managed system.
- Multi-targeted mode: Select two or more managed systems.
- Group-targeted mode: Select a group of managed systems.

The Targeted Notebook menu (shown in Figure 11-17) has tabs for System, Services, Contact/Location, History, and Test (for use in single-targeted mode only).

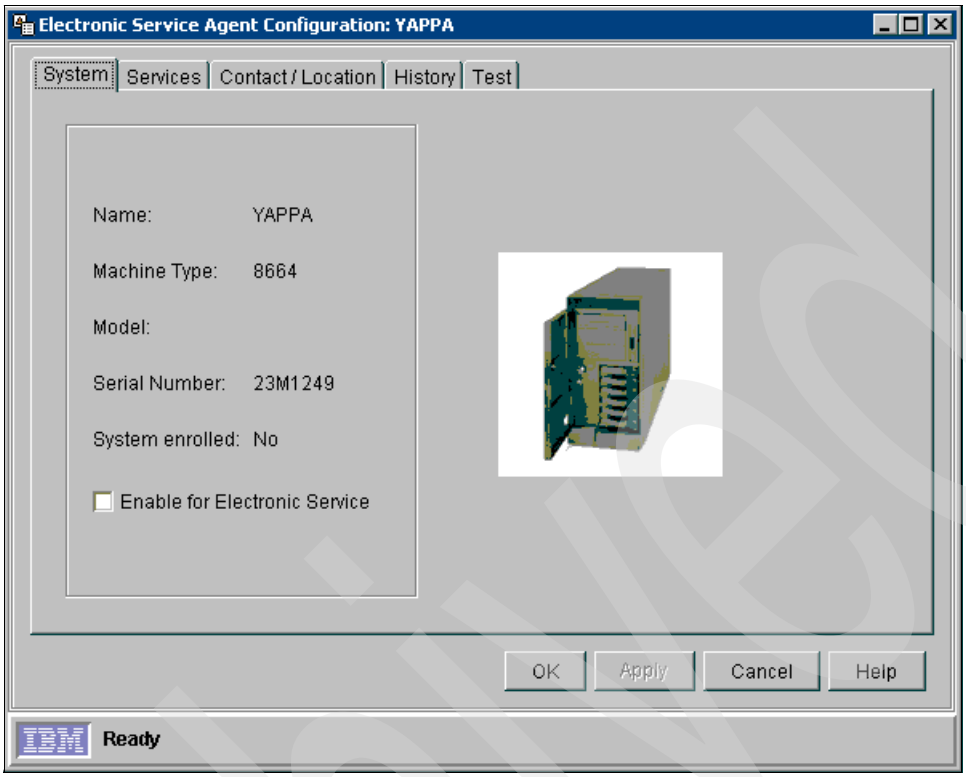


Figure 11-17 Targeted Service Agent main menu

11.3.4 Uninstall process

To permanently remove Service Agent from your server, use your administrator console:

1. From the Windows desktop, click **Start** → **Control Panel**.
2. In the Control Panel window, select **Add/Remove Programs**.
3. In the Add or Remove Programs window, select **Electronic Service Agent for xSeries®.** Click **Add/Remove**.
4. In the Language Selection window, select the language of your choice from the pull-down list, and click **OK**.
5. In the Add or Remove Programs window, select **Electronic Service Agent for xSeries - Director Extension**. Click **Add/Remove**.
6. In the Language Selection window, select the language of your choice from the pull-down list, and click **OK**.
7. In the Question window, click **Yes** to restart your computer now or **No** to restart your computer later. Then, click **OK**.
8. On the Setup window, click **Finish**.

You have removed Service Agent from your server.

12

IBM Electronic Service Agent for System z

The IBM Electronic Service Agent for System z is a “no charge” System Modification Program Extended (SMP/E) installable z/OS product. You can order the product number 5655-F17 through the normal z/OS product ordering channel. It is designed to monitor events and transmit system inventory information to IBM.

This chapter is intended for System z software administrators and support staff who are responsible for the installation, configuration, and activation of Electronic Service Agent for System z.

12.1 Electronic Service Agent for System z

Electronic Service Agent has two functions: automatic hardware problem reporting of connected I/Os and system inventory collection for monitored systems. With these functions, Electronic Service Agent for System z can monitor, track, and capture system inventory and hardware errors.

Electronic Service Agent for System z (zSA) is designed to reduce the downtime of IBM input/output (I/O) devices when a hardware problem occurs or is predicted to occur. Detected I/O hardware failures are sent immediately to the IBM Support Center. When system problem descriptions and inventory information are available to IBM Service or Support Center representatives, the representatives can better assist you in diagnosing problems. With the early knowledge about potential problems that is provided by the Electronic Service Agent, IBM can proactively respond to clients and assist in maintaining higher availability and performance.

Service Agent is also designed to transmit, on a scheduled basis, performance and service inventories to IBM. This information allows IBM support or authorized client representatives to obtain and view necessary information. Service Agent for System z is designed to work with z/OS Version 1.4 and higher.

Electronic Service Agent for System z has been enhanced with several new features, including secure data transmission, direct communication mode with IBM, and additional data collection capabilities.

Several of these features require the Hardware Management Console (HMC) Version 2.9 or higher, which is available with the IBM System z9.

Figure 12-1 shows a sample environment.

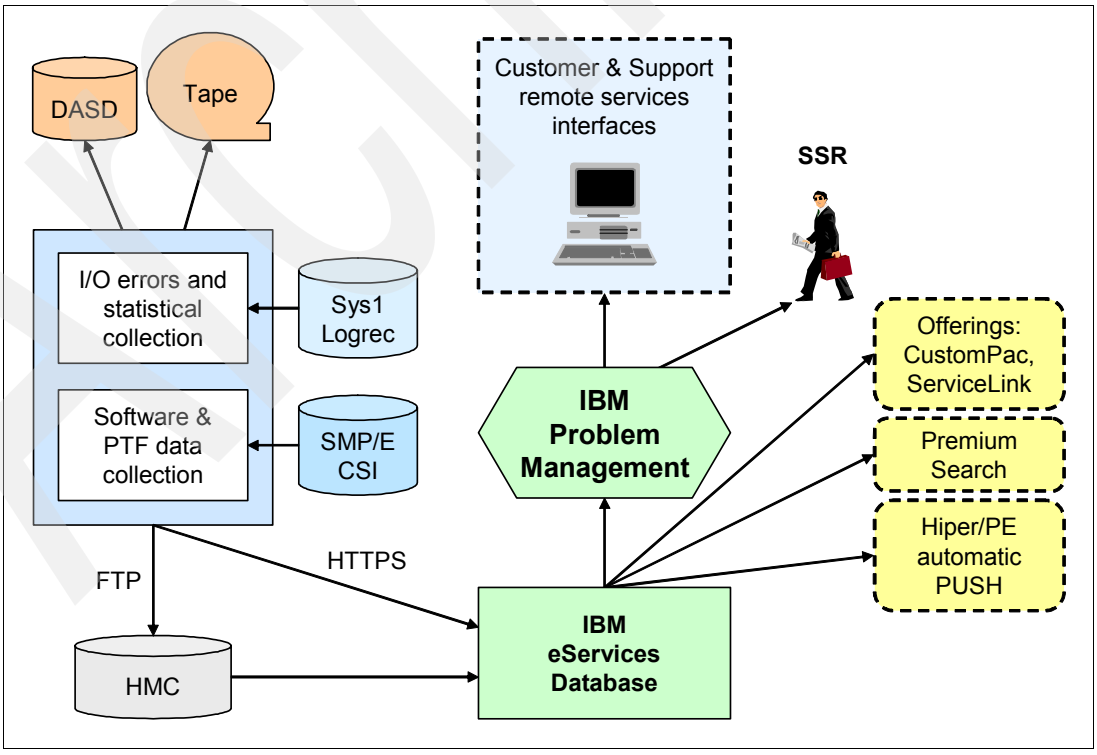


Figure 12-1 Service Agent for System z overview

12.2 Features and functions

The Service Agent for System z includes the following features:

- Secure Internet access to IBM through Hypertext Transfer Protocol Secure (HTTPS)
- 24x7 access to IBM technical support
- Two modes of communication to IBM:
  - HMC communication mode
  - Direct communication mode using an existing Internet connection
- zSA utilizes the enhanced security features of z9 HMC
- Electronic Service Agent access to IBM through an authenticating proxy
- Easy HMC configuration
- Hardware problems and direct access storage device (DASD) and tape error data reported
- Problems routed to the correct IBM Support Center queue with the required information
- Required system information automatically gathered and reported, reducing data entry errors or misreading of system information

  You must include an IBM ID with the activation in order to view and use this information.
- Media Maintenance reports for the IBM Support community to review
- Ability to view Service Agent information by both IBM and the client
- Inventory collections:
  - Hardware I/O errors
  - Installed software and program temporary fixes (PTFs)
  - Automatic PUSH of HIPERs and PTFs fixing program errors reporting
  - Client configuration data using IBM Customer Configuration Collection (CCC) tool
- Periodic “heartbeat” to IBM

The hardware events that are captured include DASD errors, ESCON® Director errors, tape errors, and tape volume errors. The automatic problem reporting helps prevent hard crashes and extended downtime in the installation. Media maintenance recommendations are produced when Service Agent examines tape media and tape drives to determine if the media or drives are experiencing problems.

The Service Agent uses historical data and proprietary algorithms to determine if media need to be replaced. Media that is recommended for replacement is highlighted on the Media Maintenance display that is visible to the IBM Support community. Replacing this media can prevent a hard failure and loss of device production time.

The service information collection function of Service Agent for System z uses your specified System Modification Program Extended (SMP/E) Consolidated Software Inventory (CSI) inventories to collect the information. IBM support staff can view your software inventory on an internal site. Your authorized users can view it at the Electronic Services Web site, My Systems selection, using the IBM ID as authentication:

`https://www.ibm.com/support/electronic`

The following System z documents provide more detailed information:

- *SMP/E V3R4.0 Messages, Codes and Diagnosis,* GA22-7770
- *SMP/E V3R4.0 Reference*, SA22-7772

- *SMP/E for z/OS and OS/390: User's Guide*, SA22-7773
- *Electronic Service Agent for zSeries and S/390 V1R2 LPS,* GA38-0956
- *Electronic Service Agent for System z User Guide*, SC38-7104
- *Program Directory for Electronic Service Agent for zSeries and S/390 V1R2*, GI11-2492
- *IBM Electronic Service Agent for IBM zSeries and IBM S/390 Messages Guide*, SC38-7108
- *Hardware Management Console Operations Guide, Version 2.9.0, IBM, S*C28-6821
- The z/OS Internet Library at this Web site:

  http://www.ibm.com/servers/eserver/zseries/zos/bkserv/

12.3 Planning

Early planning can help save you valuable time and prevent aggravation later. Understanding your information technology (IT) environment and planning the installation and activation of the Service Agent application is the best way to make your configuration and activation tasks more efficient and effective.

The user guide recommends that you enable and activate Service Agent in a phased approach. The user guide includes specific steps that enable a smooth transition. The information in this section summarizes that information.

You must consider these data types for inventory collection:

- Hardware data needs to be collected for each instance of a LOGREC data set.
- Software inventory and service (PTFs) data can be collected from any system that has addressability to the SMP/E CSI that contains information about the installed products and service on the system.

  HIPER/PE reporting can be requested for reporting the SMP/E CSI target zones.
- External data collection for sending configuration data is collected by the IBM CCC tool.

Personnel responsible for installing and configuring the Service Agent for hardware data collection and reporting must be familiar with or have a working knowledge of:

- System z architectures
- MVS™ system commands
- SMP/E installation skills
- SMP/E CSI structure
- UNIX® System Services environment
- Program Directory and listed prerequisites

The System z environment is complex. Ensure that you consider all of the items in the following list in the planning process for Service Agent activation:

- The systems programmer must have the correct authority to place Service Agent on the images.
- Plan the Service Agent elements that you are going to activate: hardware and software.
- Plan the Service agent communication mode that you want to use:
  - HMC communication mode:
    - Ensure that there is a local area network (LAN) connection between the HMC and System z image. The focal point HMC needs to be LAN accessible from all z/OS

system images where Service Agent is installed to perform information collection and transmission.

- Ensure that the focal point HMC has the correct communications for contacting IBM.
- Ensure that the HMC is at the latest level.

– Direct communication mode using the existing Internet connection:

- Ensure that there is a LAN connection between the system where zSA will be installed and activated and your Internet Service Provider (ISP).

- Ensure that your System z platform is at least on z/OS V1.4 or higher with the current maintenance installed.
- Ensure that the Java product level is IBM Developer Kit for z/OS, Java 2 Technology Edition V1.3 or higher with the current maintenance installed: the 32-bit mode only at this time. The 64-bit mode is expected in the future.
- Order the correct media for your operating system level. You order Service Agent for System z code as a stand-alone program product or with one of the following package offerings in one of four media (6250 tape, 3480 cartridge, 3590 cartridge, or 4mm cartridge):
  - 5751-CS3 MVS Custom-Built PDO (CBPDO)
  - 5751-CS4 IBM SystemPac/MVS
  - 5751-CS5 IBM ProductPac/MVS
  - 5751-CS9 ServerPac
- Ensure that there is a minimum of 256 MB of memory for Service Agent on the z/OS platform:
  - HESEVEM Task: Requires 64 MB of memory
  - HESSCAN Task: Requires a minimum of 256 MB of memory
  - HESRDLOG or HESHWRDL Task: Requires 64 MB of memory
- DFSORT™ or other equipment manufacturer (OEM) equivalent is required only if you enable performance data collection.

Table 12-1 on page 166 provides a comprehensive list of components that are related to the Service Agent activation that is required for HMC communication mode.

Table 12-1 Component list required for HMC connection mode

Various components related to Service Agent	Hardware reporting prerequisites	Software inventory collection prerequisites
OS: z/OS 1.4 or higher	X	X
LAN connection between HMC and host through TCP/IP	X	X
Activation of xSA HMC component	X	X
HMC Console: ► HMC Driver 26+ MCL or >= Driver 38 ► HMC 2.9.*x* level	X	X
Installation of Service Agent on host system using SMP/E	X	X
TCP/IP with File Transfer Protocol (FTP) enabled; Security Server or equivalent ISV product	X	X
IBM SDK for z/OS, Java 2 Technology Edition 1.3.*x* or higher (31-bit only)	N/A	X
Unix System Services enabled and activated		X
ISPF/PDF: Invoke Service Agent Main Dialog to customize and activate collections	N/A	X

Table 12-2 provides a comprehensive list of components that are related to the Service Agent activation required for direct communication mode.

Table 12-2 Component list required for direct connection mode

Various components related to Service Agent	Hardware reporting prerequisites	Software inventory collection prerequisites
OS: z/OS 1.4 or higher	X	X
LAN connection between HMC and host through TCP/IP	X	X
Activation of zSA HMC component	X	X
HMC Console: ► HMC Driver 26+ MCL or >= Driver 38 ► HMC 2.9.*x* level	X	X
Installation of Service Agent on host system using SMP/E	X	X
TCP/IP with File Transfer Protocol (FTP) enabled; Security Server or equivalent ISV product	X	X
IBM SDK for z/OS, Java 2 Technology Edition 1.3.*x* or higher (31-bit only)	N/A	X
Unix System Services enabled and activated	N/A	X
ISPF/PDF: Invoke Service Agent Main Dialog to customize and activate collections	N/A	X

12.4 Connection modes

Electronic Service Agent for System z now provides two connection modes for sending data to IBM. Both connection modes (HMC and Direct) are designed to help provide a secure means of transmitting data to IBM:

- HMC connection mode, which is the traditional connection mode. Data is forwarded by the Service Agent client (using the FTP protocol) to the HMC Service Agent and then to IBM.

  With zSA HMC Version 2.9, you also have the choice of Internet or modem connection to IBM for inventory and automatic hardware problem reporting from your z/OS systems.

- Direct connection mode (APAR PK15210) is supported using an existing Internet connection at your client site. Data is forwarded directly to IBM from the z/OS Service Agent client using a secure connection, which is implemented using HTTPS. This implementation removes the requirement for the HMC to have a separate LAN connection for Service Agent use. All Service Agent's components are enhanced to use this feature: software, hardware, and external components.

12.4.1 Enhanced security for data transmissions

IBM takes ongoing steps to provide security-enhanced transmissions for Service Agent transactions. HMC Version 2.9.*x* and PTF UK13197 (December 2005) have added a number of functions to assist in the security of your data transmissions:

- Outbound transmission only: The Service Agent client initiates outbound communications only; it does not accept inbound connections.
- Public key encryption: Service Agent uses Secure Socket Layer (SSL) and a 128-bit public key encryption mechanism to help maintain the integrity and authenticity of the data exchanged between your network and IBM.
- Enrollment: On activation, Service Agent's first communication to IBM is to request a unique ID and password for each System z9 it will monitor. IBM uses this ID and password to authenticate each subsequent communication with your server.
- Processor information only: Service Agent sends only processor or error-related information to IBM. It transmits no other information about the servers that it monitors.

Table 12-3 on page 168 summarizes the differences between the transmissions methods.

Table 12-3 zSA communication mode differences

HMC connection mode	Direct connection mode
Service Agent uses the HMC modem to access IBM Service. This telephone-based connection allows communication only with IBM Remote Support Facility (RSF) servers.	Service Agent uses HTTPS, which uses SSL 128-bit encryption, and TCP/IP protocols to access IBM Service.
A security-rich service authenticates Service Agent data transmission to IBM Service. Each HMC has a unique account with IBM. Authentication data is system-generated, non-viewable, and non-modifiable.	A security-rich service authenticates Service Agent data transmission to IBM Service. Each Service Agent has a unique account with IBM.
After the HMC modem has dialed into the phone-based connection, access is restricted through a fenced Internet connection. Here, the target addresses are limited to the small set required to access IBM Service.	Service Agent initiates HTTPS communications and sends collected data, but does not allow any inbound connections.
Service Agent uses HTTPS, which uses SSL 128-bit encryption, and TCP/IP protocols to access IBM Service.	You can configure Service Agent to work with firewalls and proxies.
Service Agent does not accept incoming calls from the modem.	The ISP relationship and connection is your responsibility.

We describe the security and the privacy of all Electronic Service Agent transmissions in detail in Chapter 5, “IBM Electronic Service Agent and the Hardware Management Console security” on page 51.

12.4.2 HMC connectivity

If you have more than one Hardware Management Console, choose one that you want to use for working with the Service Agent program. This HMC is called your *focal point Hardware Management Console*.

The focal point Hardware Management Console needs to be attached to the the client local area network (LAN). The focal point Hardware Management Console’s IP address needs to be accessible to every operating system where the client wants to install and run Service Agent, using one of these methods:

- Connect the Hardware Management Console to the client’s LAN through a bridge or otherwise.
- Connect the Hardware Management Console to the client’s LAN using a second LAN adapter. This method allows the host MVS systems to FTP the data to the HMC through the client’s LAN but does not expose the HMC functions to the client’s LAN. The HMC uses a private network on the other LAN adapter to communicate with its managed systems.
- Install a separate Hardware Management Console on the client’s LAN. This Hardware Management Console needs to have its own phone line and is not a part of the processor complex.

OS/2-based HMC

Verify or obtain the IP address of the focal point Hardware Management Console by performing these steps:

1. Log on as *ACSADMIN*.
2. Select **Console Actions**.
3. Select **Hardware Management Console settings**.
4. The IP address is displayed in this panel. Record this IP address. You will need it to configure the other Service Agent components.

To configure the other Service Agent components:

1. Under Console Actions, select **Enable Hardware Management Console Services**. We recommend that you enable this focal point Hardware Maintenance Console as a Phone Server if there is a phone line connected to it.
2. Under Console Actions**,** select **Enable Electronic Agent for zSeries**.

   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 that it was enabled. If you do not agree to the terms in the panel, you can select Cancel or Discontinue and Service Agent is not enabled.
3. Select **I Agree.** A second panel is displayed.

   Verify that the information in the fields on the lower part of the window is complete and accurate, especially the voice phone number. For automatic dispatching of an IBM service support representative (SSR), this phone number must be the same as the phone number registered with IBM Service. This information is used by IBM Service to contact you if you have a failure on IBM maintained hardware.
4. Select **Continue**.

   The next panel has two check boxes. You can allow Service Agent to process I/O error data, or Software (Software and Service (PTFs) data as configured on the 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**. Record this password for later use. You will need it during configuration of the Service Agent collection attributes.
5. Select a time when you want Service Agent to send accumulated I/O statistical data to IBM. Service Agent must send data to IBM at least one time a day. When you are done, select **Finish**.

   If Service Agent was disabled prior to this action, a Service Agent call is sent to IBM to confirm registration of this focal point Hardware Management Console. Service Agent is disabled using this same icon.
6. 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.

HMC 2.9 only

Enabling the Service Agent task allows the HMC Service Agent to send your data directly over the Internet to the IBM Service Support System. The HMC Internet connection is new with HMC 2.9.*x*. You can configure HMC 2.9.*x* to attempt connections through the Internet,

through the local modem, or both. The other direct communication option is using the Service Agent z/OS client to communicate over the Internet with IBM, therefore, bypassing the HMC. The following list provides an overview of the Service Agent security features that are now available with HMC 2.9.*x:*

- HMC Internal Firewall. Through its internal firewall, HMC Version 2.9.*x* limits TCP/IP access to the HMC-related functions. HMC Version 2.9.*x* operates as a closed platform. It does not allow other programs to access the underlying HMC operating environment or to run under the HMC operating environment. All communication between the HMC and IBM Service Support System is encrypted using HTTPS protocol.
- Optional high-speed Internet-based *call home* support. HMC Version 2.9.*x* can access the IBM Service Support System over the Internet using SSL encryption. Only your HMC can initiate this connection; the IBM Service Support System cannot initiate a connection to your HMC. To use this call home support, your HMC requires a LAN adapter configured with a default gateway for accessing the Internet.
- Other security enhancements in HMC Version 2.9.*x* include:
  - Limiting FTP access to a particular directory; there is no root access through FTP.
  - Providing you the option of limiting HMC FTP access to only those z/OS systems that run Service Agent.
  - Authenticating your data transmissions (performed by the IBM Service Support System through an authentication service).

Verify or obtain the IP address of the focal point Hardware Management Console:

1. Log on as *ACSADMIN*
2. Select **Console Actions** → **Hardware Management Console settings** → **Customize Network Settings** → **LAN Adapters**.

   If there are two LAN adapters, two IP addresses display. You might need to verify with your network support personnel which IP address is connected to the LAN. Record this IP address.

Next, you need the IP address to configure the other Service Agent components:

1. Under Console Actions, select **Enable System z 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 that it was enabled. If you do not agree to the terms in the panel, you can select Cancel or Discontinue and Service Agent is not enabled.
2. Select **I Agree.** A second panel called the Data Selection Panel is displayed. The Data Selection panel is comprised of four sections:
   a. Data Types: This has two check boxes, which specify the data types that zSA HMC Service Agent can process. Check the applicable boxes that you want:
      - IBM I/O Device Error data. This indicates that Service Agent is to process hardware error data from LOGREC.
      - IBM Software Inventory and PTF levels. This indicates that Service Agent is to process Software data: Software and Service (PTFs) data. Select this check box if you plan to send Hiper/PE report requests or external transaction data.

   b. FTP Password: Service Agent sends data to the HMC using FTP. Note that the user ID is set as *esa390* and is not changeable. 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 want Service Agent to send accumulated I/O statistical data to IBM. Service Agent must send data to IBM at least one time a day.

d. FTP Access: You have an option to create an FTP access table to specify the IP addresses of z/OS systems that will transfer data (FTP) to this HMC. This allows IP access only from the listed client z/OS systems. When you are done, select **OK**. If Service Agent was disabled prior to this action, a Service Agent call is sent to IBM to confirm registration of this focal point Hardware Management Console.

Figure 12-2 shows the client panel for selecting FTP access.

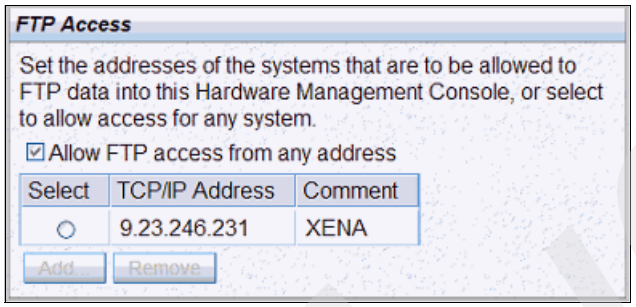


Figure 12-2 SA client panel to select FTP access

Tip: 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.

The z/OS systems running the Service Agent client need TCP/IP access to the HMC, if you are running in HMC connection mode. Here, we recommend that you isolate the Service Agent traffic from your network traffic. To do so, define and use the secondary HMC Ethernet interface card to provide TCP/IP access to these systems.

For more information about these functions, refer to the *Hardware Management Console Operations Guide, Version 2.9.0, IBM*, SC28-6821.

12.4.3 Direct connectivity

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

Certain clients might prefer the direct mode at their installations, because the direct mode saves you from having to configure a separate LAN connection to the HMC for the Service Agent's use, as well as direct mode removes the dependency on the HMC. Proxy Server authentication is also supported in Direct Connection mode with PTF UK20450 installed.

Using direct mode requires that your z/OS host system satisfies the following product prerequisites. After the prerequisites have been satisfied, specify the enablement of Service Agent to transmit data to IBM over the internet by using the Service Agent ISPF Dialog and using one of these options:

- Operating system z/OS or z/OS.e V1R5 or higher
- TCP/IP

- IBM Security Server or an equivalent product
- The z/OS UNIX System Services enabled and activated
- IBM Developer Kit for S/390, Java 2 Technology Edition (5655-D35) SDK1.3.1 with Java JSSE, or higher.

To ensure successful communication between Service Agent and IBM, we recommend that you apply the latest TCP/IP and Java service levels that are applicable to your systems.

Clarification: You do not need to install Java products if you only plan to use hardware data collection and the HMC communication mode.

Figure 12-3 illustrates how direct mode is set for the Service Agent z/OS client. In Figure 12-3, you use the Service Agent ISPF Dialog to set the Direct Connection option to `Y`. If you set this field to `N`, the Service Agent z/OS client uses the HMC as the data transmission vehicle to IBM. For the complete set of steps, refer to the *Electronic Service Agent for System z User Guide,* SC38-7104.

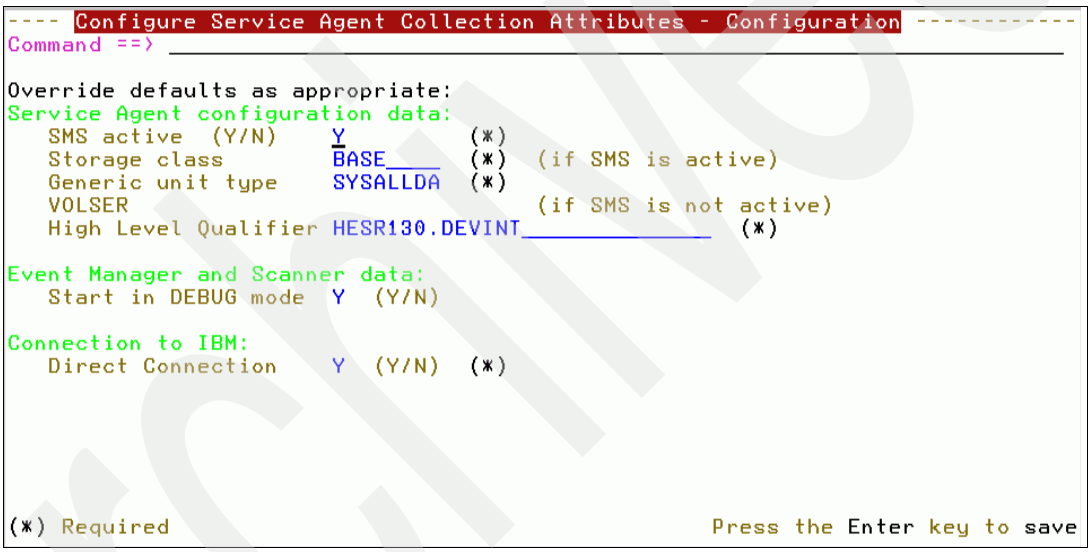


Figure 12-3 Configure Service Agent Collection Attributes - Configuration panel

12.5 Applying the Service Agent code to all images

A system programmer from your organization or a similarly authorized representative applies the Service Agent code to all images where Service Agent is to be activated. Refer to your planning documentation for which image to activate for hardware problem submission or software inventory collection.

12.5.1 Hardware configuration

You can set up hardware data to collect hardware I/O errors data by using one of the following programs or tasks:

- HESRDLOG collects and sends data to the HMC on regular intervals. HESRDLOG does not support direct connection to IBM over the Internet.
- HESHWRDL is a new module, which supports direct connection and requires you to install APAR PK15210. HESHWRDL's sole responsibility is collecting data. It notifies the

HESEVEM and HESSCAN Service Agent tasks to format the data and send the data to IBM.

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). State information is written to this dataset, hlq.HESSTATE. When critical data has been read, the HESTEMP file is renamed to EREPDATA and a new HESTEMP file is allocated.

If you use the HESRDLOG task, all of the data in the EREPDATA dataset is sent to the focal point Hardware Management Console for analysis and processing, and then sent from the HMC to IBM Electronic Services.

If you use the HESHWRDL and Direct Connection, Service Agent bypasses the HMC step and transmits the data directly to IBM using the HESSCAN task. With APAR PK15210 installed, HESHWRDL relies on the Service Agent sending components HESEVEM and HESSCAN to transmit data to IBM either through the HMC or directly. As a result, no specific sending parameters, such as HMC IP address, user ID, or password, are required. The EREPDATA file is removed from the system after it has been successfully transmitted.

Write To Operator (WTO) messages are utilized to inform the operator of critical error conditions. Job status information can be located in the spooled output ddname HESPRINT.

12.5.2 Hardware activation

We summarize the steps to configure and activate the Hardware Function of Service Agent after the completion of the SMP/E installation of Service Agent:

1. Allocate data sets required by the Hardware Data Collection and Reporting function of Service Agent by modifying and running the sample HESALCHW job provided in dataset hlq.SHESJCL.
2. APF-authorize the Service Agent load library dataset (hlq.SHESLMOD).
3. Update and add Service Agent procedures to SYS1.PROCLIB.
4. Add a step in the EREP JCL job to run and capture Service Agent data.
5. 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.
6. Start the hardware collection by starting the HESRDLOG/HESHWRDL procedure in the SYS1.PROCLIB dataset.

Where LOGREC is a LOGSTREAM: In a sysplex where the LOGREC is a LOGSTREAM, only one instance of the HESRDLOG task must 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.

For LOGSTREAM in a sysplex, remember that the person who performs the installation is responsible for ensuring that 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 presented to the IBM SSR.

12.5.3 Software collection configuration

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, is formatted and sent to IBM.

Hiper data is collected from either a subset of the SMP/E CSIs 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. External data is collected by systems that are outside of Service Agent, and it is transmitted by Service Agent at the same time as software data is collected and transmitted.

Collected data is formatted in XML and the file is sent using FTP to the focal point Hardware Management Console or directly to IBM using HTTPS. The transaction file is sent by the zSA HMC function, which regularly checks for any information to send to IBM. A response XML file is generated that describes 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. You can locate job status information in the spooled output ddname SYSPRINT.

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

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

1. Allocate data sets required by the Software Data Collection and Reporting function of the Service Agent by modifying and running the sample HESALCSW job provided in data set hlq.SHESJCL.
2. APF-authorize the Service Agent load library using sample provided in data set hlq.SHESSAMP(HESAPF).
3. Authorize Service Agent programs for Service Agent Dialog usage by modifying the IKJTSO*xx* member in SYS1.PARMLIB. The sample is provided in the data set hlq.SHESSAMP(HESTSO).
4. APF-authorize Java dynamic link libraries (DLLs) used by the Service Agent. The sample job is provided in data set hlq.SHESSAMP(HESJAVA).
5. 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).
6. 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.
7. Verify that the 31-bit Java JDK™ level 1.3.*x* or higher is available to be used with the Service Agent. The 64-bit JDK level is not currently supported.
8. Verify and update, if necessary, the environment variables in the ../usr/lpp/esa/esa1.2/envvars file:
   - CLASSPATH and LIBPATH for the Java JDK level 1.3.*x* and higher
   - Time zone
   - Service Agent System call variables

9. Customize the Service Agent Dialog ISPF interface.
10. Configure Service Agent using the Service Agent Dialog.
11. Start the Verify transaction to verify connection to IBM.
12. Enable scheduled collection for the data types of your choice:
    - Software data collection and reporting
    - Hiper/PE collection and reporting if you are eligible for this function
    - Hardware collection if you activated the HESHWRDL hardware collection task

12.5.4 Collection and transmission activation

This section discusses:

- Enabling Service Agent to automatically collect and transmit data
- Enabling Hiper/PE Reporting
- Enabling external data collection

Enabling Service Agent to automatically collect and transmit data

You can enable Service Agent to perform data collection and to report automatically on a predetermined schedule for the software data type. You also can enable Service Agent to transmit the LOGREC data that is collected by the Hardware Data Collector to IBM. When enabled for automatic data collection and reporting, the Service Agent initiates data collection and reporting at a user-specified or default time each day for the software data type.

You need to set the *Enable Service Agent scheduled collection* parameter to `Y` (Yes) to enable automatic data collection and reporting on a scheduled basis.

After you enable the Service Agent scheduled collection function, the software data type automatic data collection and reporting is enabled by default. You can also individually disable or enable data collection types.

Figure 12-4 on page 176 shows the SA panel for schedule selection.

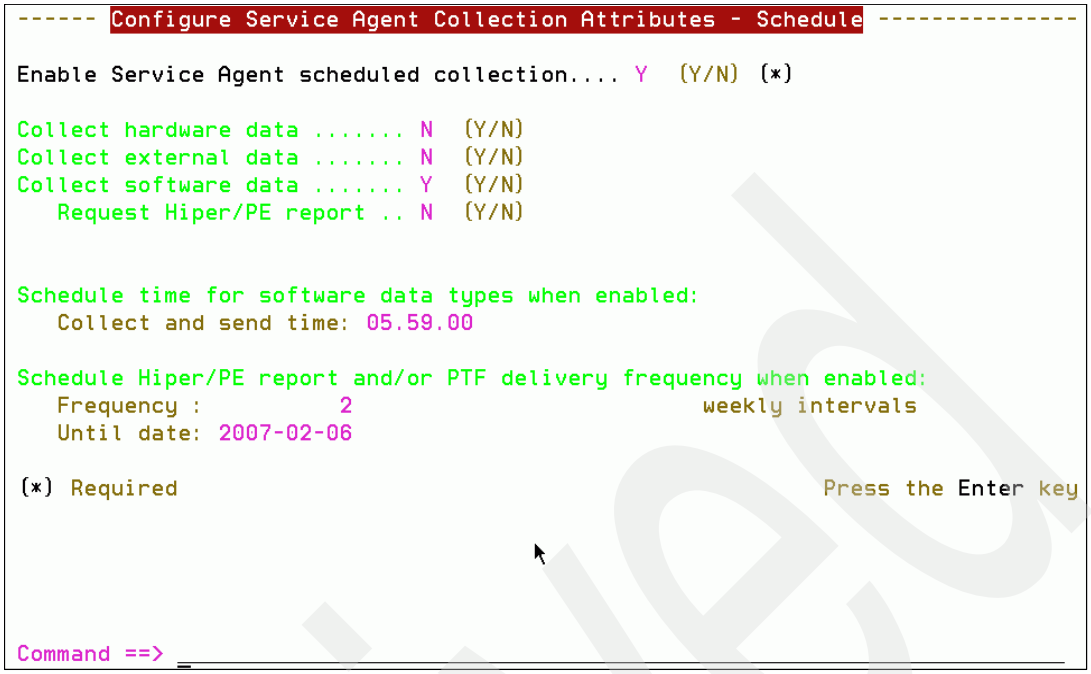


Figure 12-4 Configure Service Agent Collection Attributes - Schedule panel

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 Figure 12-4.

   After you do this, Collect time, Send time, and Day of week are set to the default values. Service Agent uses these values to determine when to initiate automatic daily data collection and transmission. If you want to send hardware collected data to IBM, you must set the collect hardware data field to Y, which indicates data that was previously collected by the HESHWRDL task. 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.
4. The Request Hiper/PE report field is set to N (No) by default. This parameter is visible only if SMP/E target zones were previously selected for automatic hiper alerts (AHAs); otherwise, this field is disabled. Change the Request Hiper/PE report to Y, allowing the AHA frequency fields to display (under Schedule Hiper/PE report or PTF delivery frequency):

   a. *Until date* (after the frequency field has been populated) indicates the time at which AHA reporting will stop. The date is limited to 2 years.

   b. *Frequency* specifies the interval in weeks of the next scheduled report.
5. Here are several parameters that you might want to reset at this time:

   – The *Collect software data* parameter is set to Y (Yes) by default. This parameter is visible only if you previously enabled Enable Service Agent scheduled collection and SMP/E zones are selected; otherwise, this option is disabled. *If the parameter Collect software data is set to N, the Service Agent will not automatically collect and transmit software data.*

– The *Collect External Data* parameter is set to N (No) by default. Setting this parameter to Y indicates that an external routine is collecting data that Service Agent will report at the Schedule send time for software data. If this is the only collection-enabled software, system enrollment is initiated.

6. Press Enter to save the data.
7. Press PF3 to return.

   If Service Agent tasks have been activated and if the Hiper schedule has been specified, then pressing PF3 automatically causes Service Agent to initiate a Hiper entitlement transaction to verify if you are entitled to receive Hiper reports and PTF delivery. If a positive response is received, Hiper reporting and PTF delivery will be scheduled according to the frequency interval that you specified.

Enabling Hiper/PE Reporting

PTF UQ94890 introduced new functionality to Service Agent to support HIPER/PE reporting. Service Agent can now electronically notify clients of critical software fixes (HIPER APARS) and PTFs in Error (PEs). It also provides the ability to electronically download the fixes for these problems.

This Automatic Hiper Alert report and PTF delivery feature is available to clients who have purchased certain software contracts: ETS in Europe or Swxcel Enterprise Edition in the United States. You use the Service Agent ISPF Dialog to enable Service Agent for HIPER/PE reporting and electronic delivery of PTFs. The steps are:

1. Select the SMP/E zones for HIPER/PE reporting and delivery of PTFs as shown in Figure 12-5.

   Prerequisites: Software Inventory collection must be enabled and SMP/E target zones must be selected for Inventory collection prior to enabling these zones for HIPER/PE reporting.

```
--- Configure Service Agent Collection Attributes - Automatic  Row 1 to 3 of 3
Command ==> _                                                  Scroll ==> PAGE

PRIM Cmds:(SET L F N P SORT CANcel SELect DESelect)
LINE Cmds:<Deselect Report PTFs>

Select the Consolidated System Inventory (CSI) target Zones for which Hiper/PE
checking report will be done.  Select or Deselect zones as appropriate.

S ZoneName Report PTFs Data Set Name
- -------- ------ ---- ----------------------------------------
_ TARGET     Y     Y   SMPESA.VEN.CSI
_ MT1VE6     Y     N   SMPVE6.GLOBALA.CSI
```

Figure 12-5 Selecting target zones for HIPER/PE reporting

2. Enable HIPER/PE and its frequency interval. We recommend these settings:
   – Collect software data: Y
   – Request HIPER/PE report: Y
   – Frequency: Specifies how often this should be done (defaults to every 2 weeks)
   – Until Date: Specifies the last date to report on HIPER/PE fixes or delivery of fixes

Enabling external data collection

Users of external applications, such as the IBM CCC tool, can use the software transmission facilities of zSA to send their collected data to IBM on a regular basis.

The following actions are required to enable external reporting:

1. Ensure that the externally collected data file is written to shared DASD that is accessible by both the external data collector and the HESSCAN sending component.
2. When started, the HESSCAN task looks for files that contain the name, hlq.C*.S*.D*.T*, where *hlq* is the high level qualifier that is defined by the envvars environment variable ibmhes.sysconf.dataset.prefix. HESSCAN transmits any of these files it locates. Be sure that HESSCAN has authorization to rename and delete each file.
3. If you want HESSCAN to delete each file after the file's successful transmission, set the envvars environment variable ibmhes.sysconf.dataset.cleanup to `Y`. If you do not define this environment variable or if you set it to N, HESSCAN renames the file hlq.C*.S*.D*.T* to hlq.C*.S*.D*.X* after each successful transmission.

Where the envvars environment variable ibmhes.sysconf.dataset.cleanup is set to `N`, HESSCAN deletes any file that has the same name as its rename target, which means that you must avoid using duplicate .T* file names.

Optional advanced configuration option: Authorize Web Users

The Configure Service Agent Collection Attributes - Advanced panel (shown in Figure 12-6 on page 179) allows you to authorize users to access the Electronic Services Web site to view or use the Software Inventory data for the system that is enrolled by this Service Agent.

The *User ID (s)* field (on this panel) can accept two IBM IDs. After you enter the IBM IDs, IBM remotely validates the IDs. If either of the fields is deemed invalid, a message is sent to your TSO logon ID with a reason code:

- Code 9970: `Length of given user ID is invalid.`
- Code 9972L `Illegal character within given user ID.`

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

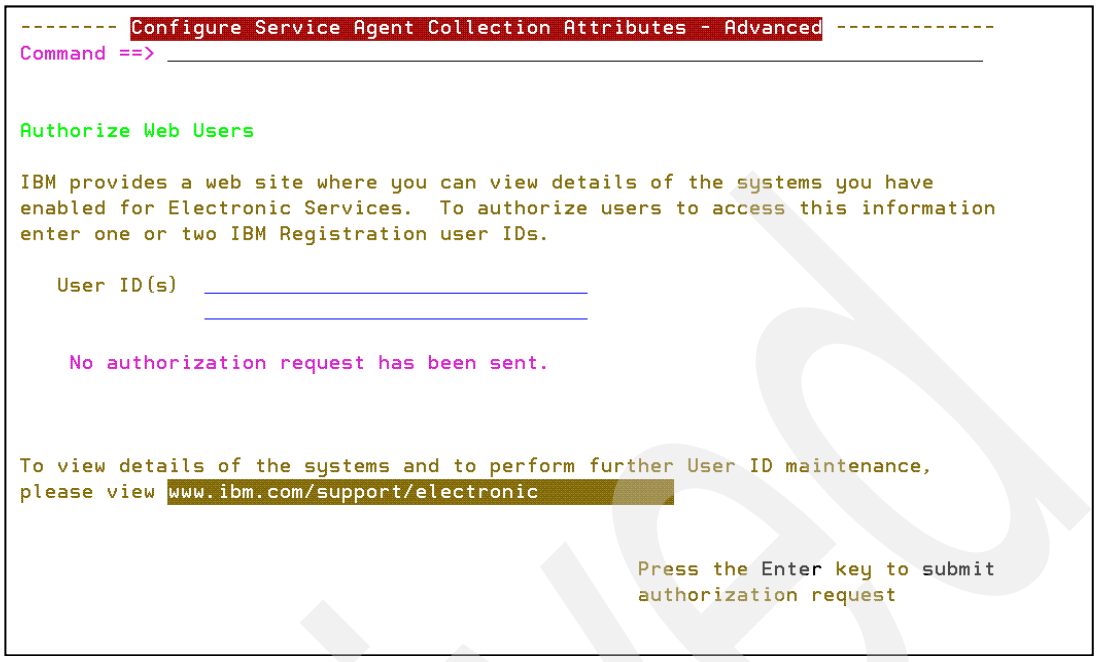


Figure 12-6 Configure Service Agent Collection Attributes - Advanced: IBM ID field

12.5.5 Activating Service Agent tasks

After you configure Service Agent software collection, the next step is to activate the Service Agent started tasks. If the Service Agent tasks are not activated, automatic data collection is not initiated. The Service Agent tasks remain active only if you enabled Service Agent for automatic collection and reporting of data.

You can start the Service Agent tasks in one of the following ways:

- On the Electronic Service Agent Main Menu, shown in Figure 12-7 on page 180, select option **1 Start Service Agent** to start the Service Agent tasks.
- Using the MVS console, enter the MVS command:

  `START HESMAIN,ESAPARM=START or S HESMAIN,ESAPARM=START`
- From the command line on the Electronic Service Agent Main Menu, type the command:

  `STARTSA`

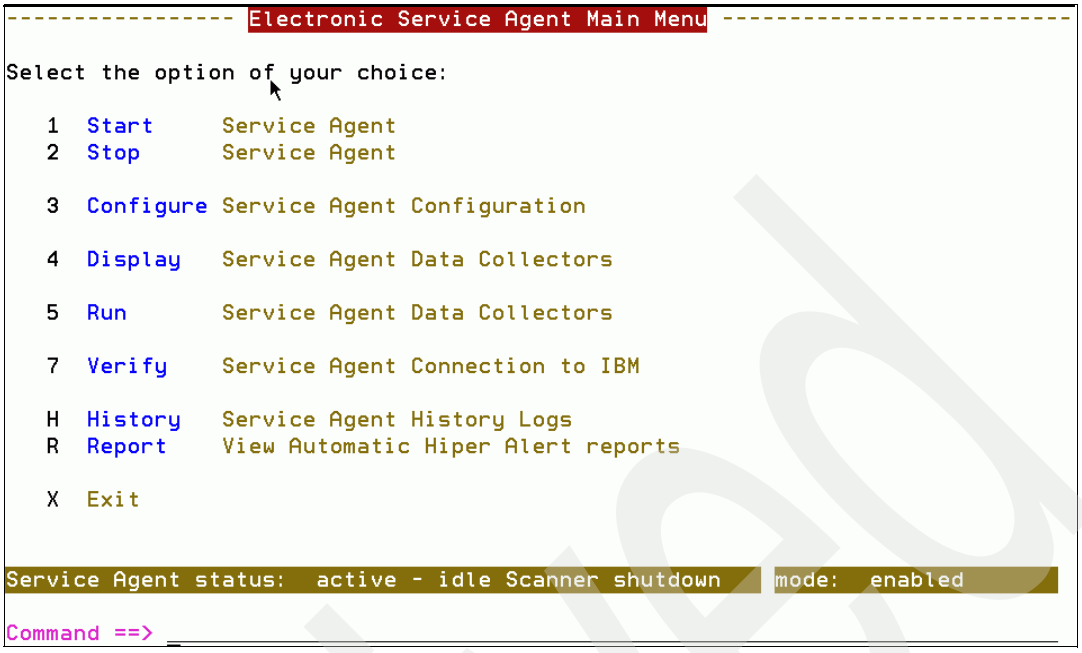


Figure 12-7 Electronic Service Agent Main Menu

12.6 Maintenance

The Electronic Service Agent Main Menu, shown in Figure 12-7, manages the software actions, and in direct mode, hardware actions. The Electronic Service Agent Main Menu displays a status of the running tasks at the bottom of the view.

Use option **H History Service Agent History Logs** to view history logs of all of the saved Service Agent transactions.

For hardware problem submission, use the System z ISPF menu.

12.7 Uninstall process

Service Agent is installed under the SMP/E umbrella, and you use this same process to uninstall it.

You can start and shut down Service Agent manually. Or, you can use an automatic procedure for the Electronic Service Agent software component in an automated operations environment. For more information about these steps, refer to the *Electronic Service Agent for System z User Guide,* SC38-7104.

12.8 HMC activation

Tip: The following steps are for Service Agent processes. They do not have any relationship to the focal point HMC reporting errors on processors.

To activate the HMC Service Agent, follow these steps:

1. Log on as *ASCADMIN*.
2. The HMC menu (shown in Figure 12-8) opens. In the upper pane, select **Console Actions**.
3. Now the HMC menu displays options in the Console Actions Work Area (bottom area in Figure 12-8). Select **Hardware Management Console Settings**.

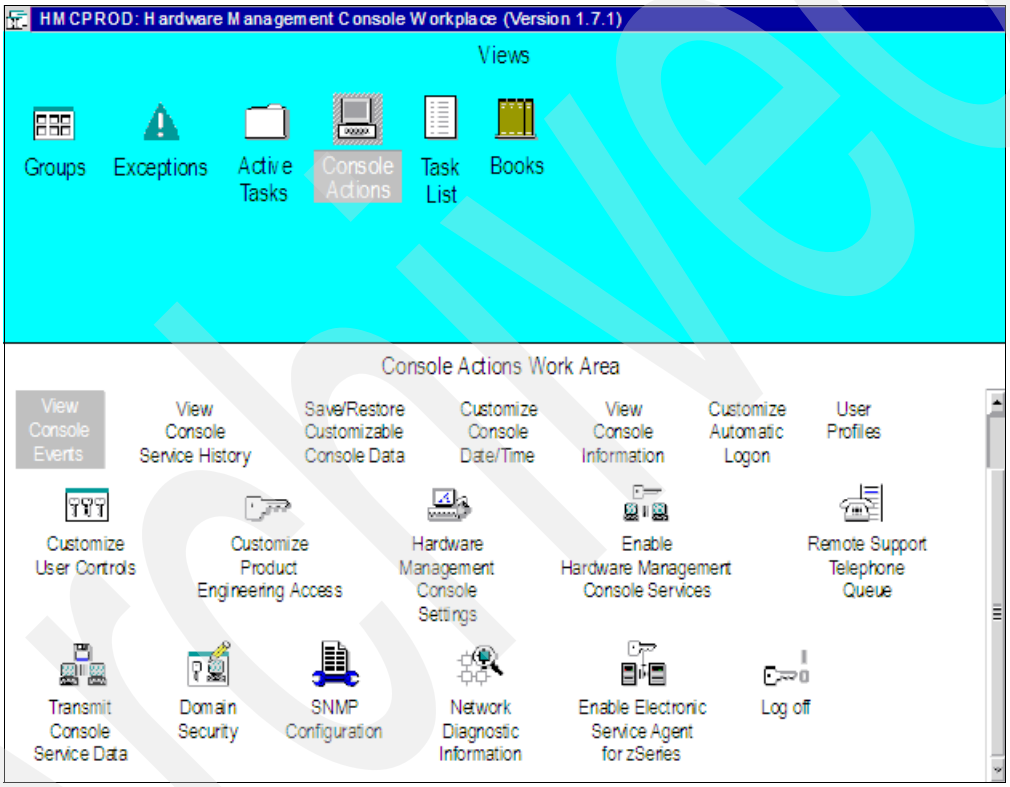


Figure 12-8 HMC menu

4. A pop-up window opens on the HMC menu and displays an IP address. Record the address. You need this address to complete a field in the Service Agent collection attributes. Then, click the icon in upper left corner and select **Close** to close this pop-up window.
5. In the Console Actions Work Area (shown in the lower pane in Figure 12-8), select **Enable Electronic Service Agent for zSeries**.
6. The Service Agent License Agreement window (shown in Figure 12-9 on page 182) opens. To continue with the Service Agent activation process, page through the agreement and select **I AGREE**.

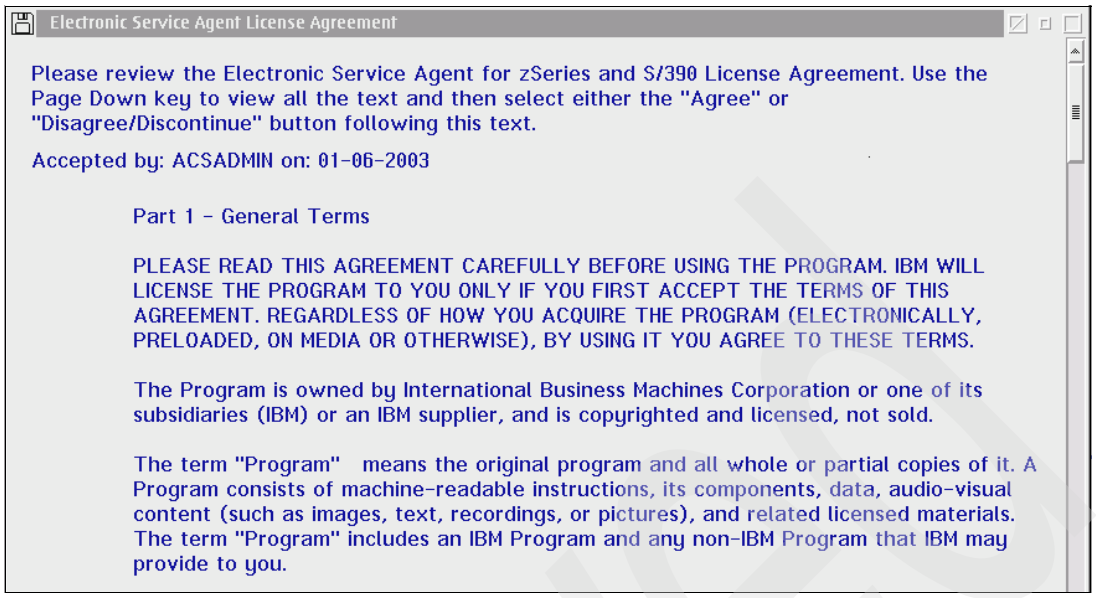


Figure 12-9 Service Agent for System z: License Agreement window

7. Next, client contact information (shown in Figure 12-10) is used to register this HMC with Service Agent and IBM. IBM uses this information to communicate regarding service requests. Change or correct any of the client information as necessary. Click **Continue**.

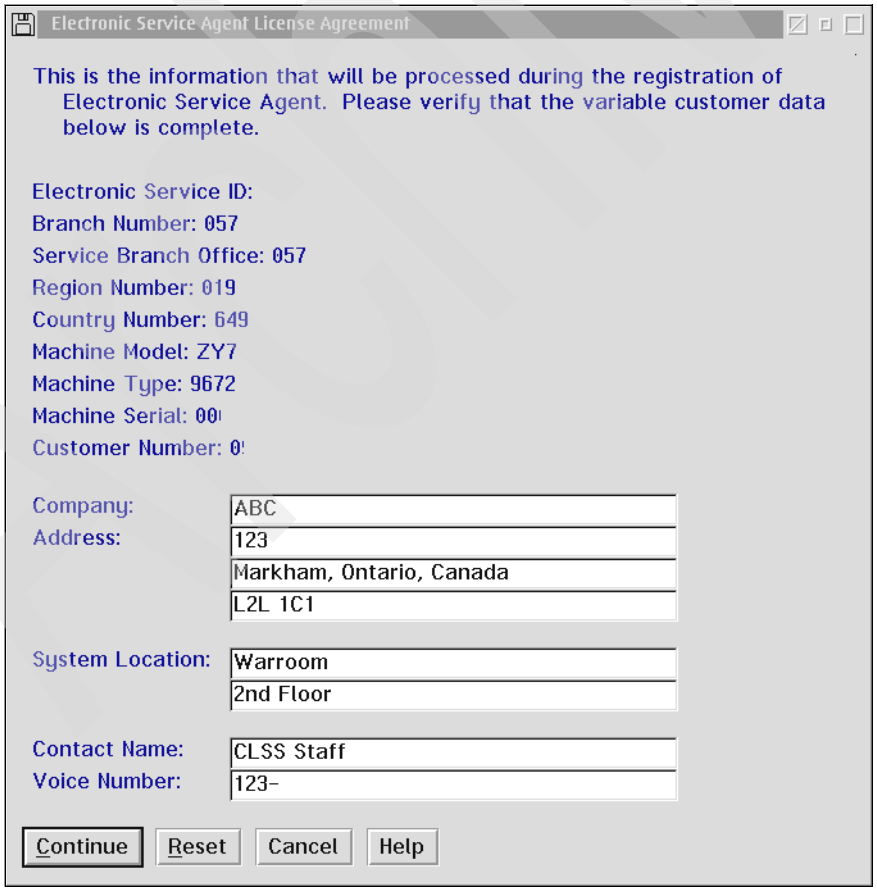


Figure 12-10 Service Agent for System z: Updating client information

8. The Electronic Service Agent License Agreement window (shown in Figure 12-11) allows you to enable or disable subsections of the Service Agent and set the FTP password used by the z/OS software to send information to the HMC. Select the boxes that you want to enable. Enter an FTP password that must also be entered into the z/OS software. Click **Continue** when you finish.

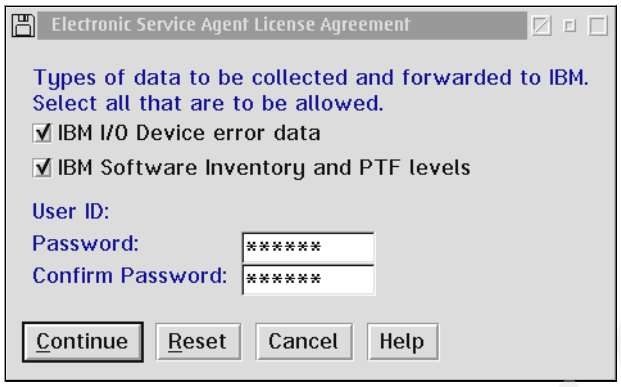


Figure 12-11 Service Agent for System z: Enabling or disabling the types of data to send to IBM

9. In the next window, select the time of day for the daily transmission of the inventory information that is sent to IBM. Click **Finish** to complete the configuration process and store the data within the HMC.

   The HMC sends the automatic registration transaction to IBM. This transaction must be completed before IBM can accept any problem or inventory transactions.

10. Add a step in the EREP JCL job to run and capture Service Agent data.
11. Create started task IDs and started task entries in the STARTED RACF class for HESRDLOG using the supplied sample job.
12. Configure Service Agent by editing dataset hlq.HESPARMS. Change the HMC IP address and HMC FTP password to match that of your installation.
13. Start the hardware collection. Start the HESRDLOG procedure in the SYS1.PROCLIB dataset.
14. Enable a scheduled collection for the data types of your choice.
15. Enable collection and reporting for software data, performance data, or both.

You have activated Service Agent for System z.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this bookbook.

IBM Redbooks publications

For information about ordering these publications, see “How to get IBM Redbooks publications” on page 186. Note that some of the documents referenced here might be available in softcopy only:

- *A Systems Management Guide to Performance Management for i5 and p5 Systems*, SG24-7122
- *IBM eServer iSeries Universal Connection for Electronic Support and Service*, SC24-6224
- *Effective System Management Using the IBM Hardware Management Console for pSeries*, SG24-7038
- *Performance Management Services for AIX in a Partitioned Environment*, REDP-0223
- *Difference Between Two Backup Tasks: Backup Critical Console Data and Save Upgrade Data (HMC for pSeries)*, TIPS0156
- *What is a Hardware Management Console (HMC)?*, TIPS0280

Other publications

These publications are also relevant as further information sources:

- *Electronic Service Agent for System p User Guide*, SC38-7105 at:

  http://www.ibm.com/support/electronic
- *Electronic Service Agent for System p Hardware Management Console (HMC)*, SC38-7107 at:

  http://www.ibm.com/support/electronic
- *SMP/E V3R4.0 Messages, Codes and Diagnosis*, GA22-7770
- *SMP/E V3R4.0 Reference*, SA22-7772
- *SMP/E V3R4.0 for z/OS: User's Guide,* SA22-7773
- *Electronic Service Agent for zSeries and S/390 V1R2 LPS*, GA38-0956
- *Electronic Service Agent for System z User Guide*, SC38-7104 at:

  http://www.ibm.com/support/electronic
- *Program Directory for Electronic Service Agent for zSeries and S/390 V1R2*, GI11-2492
- *IBM Electronic Service Agent for IBM zSeries and IBM S/390 Messages Guide*, SC38-7108
- *Hardware Management Console Operations Guide, Version 2.9.0, IBM*, SC28-6821
- *Electronic Service Agent for System p - Linux User Guide*, SC38-7109 at:

  http://www.ibm.com/support/electronic

- *System Manager Use*, SC41-5321, at this Web site:

  http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/books/sc415321.pdf

Online resources

These Web sites are also relevant as further information sources:

- Electronic Services Web site

  http://www.ibm.com/support/electronic

- z/OS Internet Library

  http://www.ibm.com/servers/eserver/zseries/zos/bkserv/

- System i Information Center

  http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/rzaji/service_agent.htm

- System p Information Center

  http://publib16.boulder.ibm.com/pseries/index.htm

How to get IBM Redbooks publications

You can search for, view, or download IBM Redbooks publications, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy IBM Redbooks publications, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

IBM Electronic Services: Support using Automation and Web Tools

IBM Electronic Services

Support using Automation and Web Tools

Redbooks

Simplify and enable faster support for your IT environment

Electronic Service Agents run on all IBM systems

Worldwide access and utilization

What is IBM Electronic Services? Why do I need it? Where do you get it? When and how do you use it? How will this help your electronic support relationship with IBM? Find the answers to these questions and more details about IBM Electronic Services in this IBM Redbooks publication.

The goal of IBM Electronic Services is to simplify your support relationship to make it easier and faster to do business with IBM. Through automation and Internet access, Electronic Services integrates the IBM Support community with your company staff and your IT environment. The two major components are IBM Electronic Service Agent (Service Agent) and the IBM Electronic Services Web site.

IBM Electronic Services reaches across all IBM systems in all countries or regions where IBM does business. Electronic Services can provide the electronic support relationship for a single machine environment or a multinational complex of many servers.

This book is intended for IT management, system operators, and others who work for and with IBM clients. Prior to reading this book, you need to have a thorough understanding of your computer system and networking environment.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-6323-01 ISBN 0738488852