



Connectivity Security White Paper

Electronic Service Agent 4.3 for PowerLinux

February 2017

Table of Contents


I.....Introduction	2
Useful Documentation.....	2
Terms and Definitions	2
II.....Reasons for Activating ESA for PowerLinux	4
Reasons for activating ESA for PowerLinux	4
III.....Activating ESA for PowerLinux	5
IV.....ESA for PowerLinux Connectivity	6
Outbound Connectivity without Proxy Server	6
Outbound Connectivity with your Proxy Server	6
Configuring ESA to use a Proxy Server.....	7
Outbound Connectivity with ESA supplied Service and Support Proxy Server	8
Configuring the ESA supplied Service and Support Proxy Server	8
Verify Electronic Service Agent Connectivity.....	8
V.....Security Protocols and Encryption	9
Communication between ESA and IBM	9
IPv6 support	9
Communication between your browser and the ESA daemon.....	9
ESA Web User Interface Authentication	9
Communication between ESA and Serviceable Event Provider	9
VI.....Service information sent to IBM	11
Data Sent to IBM.....	11
VII.....Appendix: IP addresses and Ports for IBM Connectivity	13
Overview	13
Simplified Connectivity Options	13
Traditional Connectivity Options	14
Ports used by ESA.....	14

Introduction

This document describes the connectivity, security and service information, sent by Electronic Service Agent (ESA) for PowerLinux when ESA communicates with the IBM Service Delivery Center (SDC). The functionality that is described in this document refers to ESA version 3.4 and later.

ESA version 3.4 and later is available in the following products:

- Installation of RHEL 6.4, 6.5, 7.1, SLES 11 SP2, SP3 and later.

 Note: IBM Electronic Service Agent is not supported on any version of Ubuntu Linux operating system.

ESA supports the following systems types:

- KVM on Power Systems.
- PowerLinux installed on a standalone Power system.
- PowerLinux installed on a logical partition (no hardware problem reporting or hardware inventory reporting).
- PowerLinux installed on a Power Blade/Power ITE.
- Only if the system vendor is IBM.

Useful Documentation

A complete set of ESA documentation can be found at: <http://www-01.ibm.com/support/esa>.

Terms and Definitions

It is assumed that the reader has a basic understanding of Internet Protocol (IP) networks and protocols. The following is a list of terms and acronyms that may not be familiar to the reader.

Term	Definition
ESA	Electronic Service Agent
HTTPS	Hypertext Transfer Protocol Secure
LPAR	Logical Partition
IP	Internet Protocol
SDC	Service Delivery Center
SNAT	Source Network Address Translation

TLS	Transport Layer Security
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
FRU	Field Replaceable Unit
PAM	Pluggable Authentication Module
SRC	System Reference Code
SRN	System Reference Number
VPN	Virtual Private Network

Reasons for Activating ESA for PowerLinux

Reasons for activating ESA for PowerLinux

- Automatically report a hardware problem to IBM
- Automatically send extended error data for problem analysis by IBM
- Automatically report inventory and system configuration information to IBM
- Automatically report heartbeat and status information to IBM
- Automatically report performance information to IBM
- View reports generated using your data on the IBM Electronic Support website

Activating ESA for PowerLinux

After you install ESA, you must activate and configure it. You can activate the ESA by using the activation wizard or command activation on your PowerLinux system, PowerLinux LPAR or PowerLinux Power Blade.

For information on how to activate Electronic Service Agent, see [Electronic Service Agent for PowerLinux User's Guide](#).

While activating ESA, you must specify a port number that is used to connect to ESA through the web browsers. For example, <https://hostname:5024/esa>, where *hostname* is the fully qualified name or the IP address of the system running ESA. Port 5024 is the default port. If you have activated ESA on a different port, use that port number in the web address.

IBM Electronic Service Agent can connect to the IBM Electronic Support SDC through direct Internet (HTTPS) connection, service and support proxy, or HTTP proxy connection paths. IBM Electronic Service Agent uses these connection paths to report problems and send service information to the IBM Electronic Support SDC. IBM Electronic Service Agent uses IPv4 to connect to the IBM Electronic Support SDC.

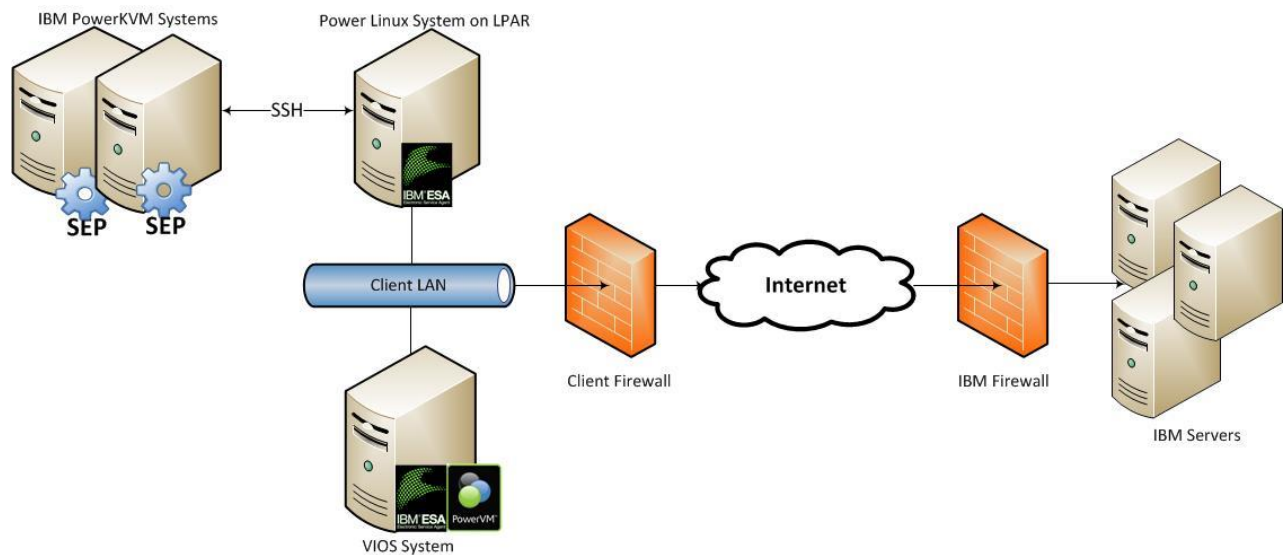
If you use only a default direct Internet connection, no additional configuration is needed. However, if a direct connection is not always available, you can configure IBM Electronic Service Agent to communicate with IBM using a proxy server. You can specify up to three proxy servers. IBM Electronic Service Agent uses the connections in the order they appear, so if one service connection is not configured, busy, or unavailable, the next service connection is used.

ESA for PowerLinux Connectivity

ESA on PowerLinux only supports outbound Internet connectivity.

Outbound Connectivity without Proxy Server

The following diagram shows the default setup of ESA on PowerLinux that is connected to IBM without a proxy server.



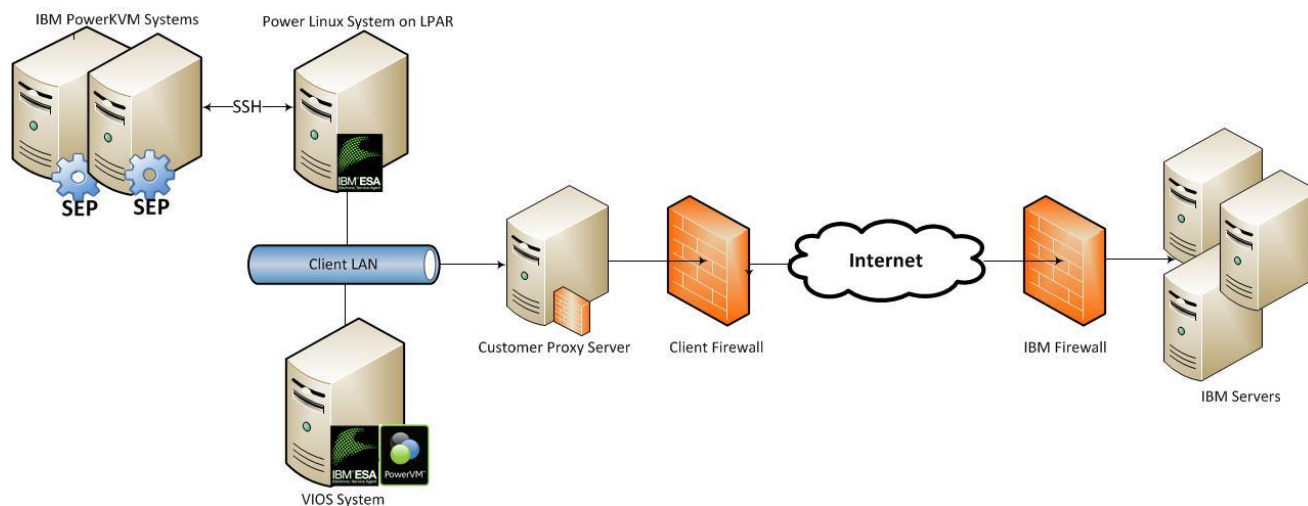
In this setup, ESA connects through your internet connection by the default route. For this type of configuration, you can optionally use a second network card to physically separate the local system network from the internet enabled network.

For ESA to communicate successfully, your external firewall must allow outbound packets to flow freely on port 80 and port 443. You can use Source Network Address Translation (SNAT) and masquerading rules to hide the ESA system's source IP address.

On your firewall, you may choose to limit the specific IP addresses to which the ESA system can connect. Section [IBM Server Address List](#) contains the list of IP addresses and ports of the IBM servers.

Outbound Connectivity with your Proxy Server

The following diagram shows the ESA for PowerLinux that is connected to IBM using a proxy server supplied by you. This is not the default setup and you must configure ESA to use your proxy.



To forward ESA packets, the proxy server must support the basic proxy header functions (as described in RFC #2616) and the CONNECT method. Optionally, basic proxy authentication (RFC #2617) may be configured so that the ESA authenticates before attempting to forward packets through your proxy server.

Configuring ESA to use a Proxy Server

Connecting IBM Electronic Service Agent through the IBM Service and Support proxy or your HTTP proxy can be fast and easy from your business network, and minimizes the number of systems that are directly connected to the Internet.

You can use the ESA web user interface to configure your service connection. You can also use the **esacli connectionSettings** command to configure your service connection. For information on how to configure service connection, see [Electronic Service Agent for PowerLinux User's Guide](#).

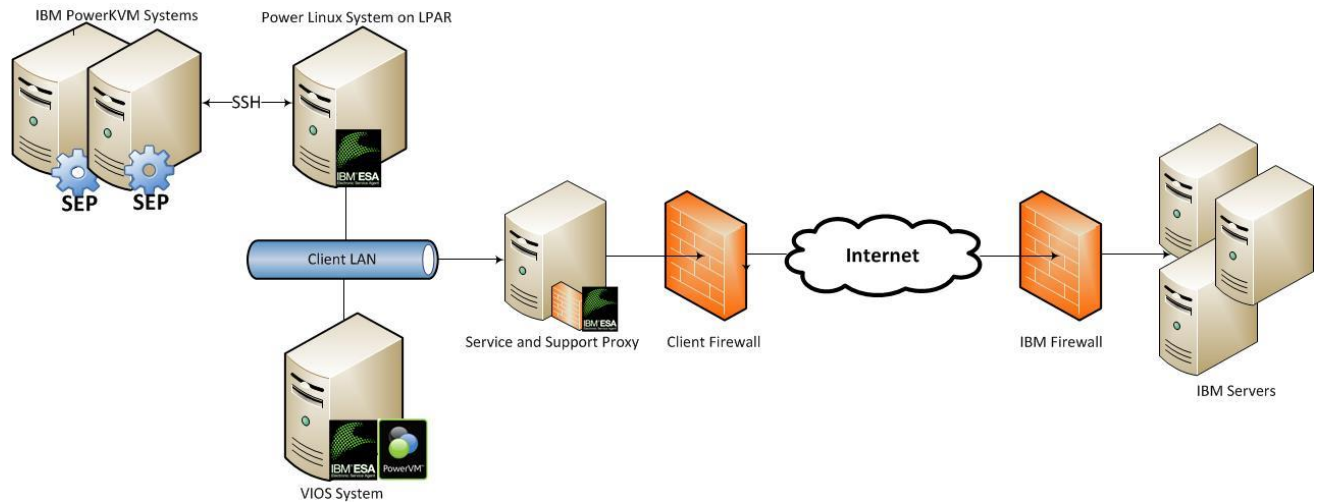
If you select the proxy path to send your information, then the following process applies:

1. At the scheduled time, IBM Electronic Service Agent collects the information to be transmitted and queues it for transmission.
2. Using the TLS connection between the system and the IBM Electronic Support SDC, IBM Electronic Service Agent establishes a TLS Internet connection between the proxy and the IBM Electronic Support SDC. This connection is authenticated using the system ID and password that is previously created.
3. IBM Electronic Service Agent sends the collected information through the proxy to the IBM Electronic Support SDC.
4. After the information arrives at the IBM Electronic Support SDC, the information is transferred to the appropriate IBM database.

Outbound Connectivity with ESA supplied Service and Support Proxy Server

ESA supplies a Service and Support Proxy Server. This proxy server can be deployed in your environment to aggregate connectivity to IBM through a single Internet-enabled system. This proxy only supports the destinations listed in section [IBM Server Address List](#) and as such cannot be used in your environment to serve as a general purpose proxy server.

The following diagram shows the ESA for PowerLinux that is connected to IBM using the Service and Support proxy server supplied by ESA.



Configuring the ESA supplied Service and Support Proxy Server

You can use the ESA web user interface to create the IBM Service and Support proxy server. You can also use the `esacli supportProxySettings` command to create the IBM service and support proxy. For information on how to configure ESA supplied service and support proxy server, see [Electronic Service Agent for PowerLinux User's Guide](#).

Verify Electronic Service Agent Connectivity

IBM Electronic Service Agent communicates with several IBM servers, and all connections with IBM are backed up by redundant sites. So if a primary connect point is unavailable, a connection is attempted to a backup server.

When you have completed configuration of your connectivity settings, test for connectivity to IBM. For information on how to test connectivity to IBM, see [Electronic Service Agent for PowerLinux User's Guide](#).

Security Protocols and Encryption

Communication between ESA and IBM

ESA uses the HTTPS protocol for transmission of data between your site and the IBM Service Delivery Center. The HTTP protocol serves as a backup path for initiating the download of a new configuration information when an appropriate HTTPS path cannot be established. Your data is never uploaded using the HTTP protocol.

HTTPS is achieved by encapsulating the HTTP application protocol with the Transport Layer Security (TLSv1) cryptographic protocol.

IPv6 support

Call home does not fully support the IPv6 protocol at this time.

Communication between your browser and the ESA daemon

The ESA web user interface (default port is 5024) uses the HTTPS protocol for securing administrative requests between your browser and the ESA subsystem (daemon) running within PowerLinux.

HTTPS is achieved by encapsulating the HTTP application protocol with the Transport Layer Security (TLSv1) cryptographic protocol.

ESA Web User Interface Authentication

The ESA Web User interface uses the Pluggable Authentication Module (PAM) to authenticate users. ESA uses the PAM login service definition found in the `/etc/pam.conf` file.

Communication between ESA and Serviceable Event Provider

Electronic Service Agent communicates with the Serviceable Event Provider on the PowerKVM host system and listens for the SNMP traps on the default `5028` port and *public* community.

ESA creates an ESA specific user ID on the KVM host – **esaadmin**. ESA uses **esaadmin** for any further communication with remote KVM host without requiring any password, but with a private key that is generated on ESA system.

 The `esaadmin` user ID has limited admin privileges, which can run all the commands needed by ESA.

ESA generates public-private key pairs that are stored on ESA and uses to communicate to this user on KVM hosts. The private key is stored on the system on which ESA runs. Public key is copied to each of the KVM hosts. These keys are configured on KVM hosts, such that only ESA system can log in without a password. Hence the root credentials for any KVM

host system are not stored / saved.

The **esaadmin** can do sudo executions on the system to collect additional problem data like SEP commands, sosreport, opal-log commands, but not any other generic admin commands.

When the SNMP traps are received, ESA processes them and sends to IBM support, if it is a call home problem.

Service information sent to IBM

This section outlines what Service information is sent to IBM.

Data Sent to IBM

This is a list of the data that may be sent to IBM, the command or component used to collect the information and brief descriptions of the contents.

Table 1: Data sent to IBM from PowerLinux

Reason	Command/Component	Description
Problem reporting	PowerLinux diagnostics	The SRC/SRN and FRU information are collected using the PowerLinux diagnostics package.
Extended error data	Snap	The “snap -g” data is collected and sent as the result of a hardware problem being reported to IBM.
System configuration	Snap	Automated system configuration is collected and sent weekly by default and uses the “snap -g” command. Manual (on demand) system configuration uses the “snap -a” command.
Hardware service Information	CISA	Common Inventory Sub-Agent (component bundled with ESA) hardware service information is collected and sent daily by default.
Software service Information	CISA	Automated Common Inventory Sub-Agent software service (component bundled with ESA) information is collected and sent daily by default.
Performance information	pmcfg	ESA uses “pmcfg -s” command to collect Performance information. ESA sends the performance information daily when available.
Contact information	ESA User Interface	Contact information is reported to IBM, securely stored at IBM, and used only by designated IBM service personnel for contacting you about problems with your system.
ESA supplemental service information	uname, lsmcode, hostname, lsattr Files look at:	Includes ESA version, PowerLinux version, firmware level, machine type and model, processor type, and hostname.

	/etc/SuSE-release	
	/etc/redhat-release	
	/proc/device-tree/system-id	
	/proc/device-tree/model	
IBM ID	ESA User Interface	Your IBM ID is sent to IBM and used to provide secure access to IBM reports generated on your behalf and made available on the web.
Operational Test	Internally generated by ESA	While ESA is active on your system, it will perform a daily operational test (aka. heartbeat) with IBM.
SOS Report	Extended error data	Extended error data is collected for every serviceable event that is sent to IBM (call home events) from the KVM host. Whenever a hardware problem is identified, ESA collects all system logs, configuration, and diagnostic information that can be used for debugging.

Appendix: IP addresses and Ports for IBM Connectivity

Overview

This appendix identifies the IP addresses and ports that are used by Power Linux ESA when it is configured to use internet connectivity.

If your PowerLinux ESA supports the simplified connectivity path, view the section [Simplified Connectivity Options](#), else view section [Traditional Connectivity Options](#) to configure the IP addresses and ports.

Simplified Connectivity Options

From ESA version 3.3 for Power Linux, a new Call Home server environment has been deployed that provides a front-end proxy to the current Call Home infrastructure. This environment simplifies the IT for Call Home customers by reducing the number of customer facing IBM servers, enabling IPv6 connectivity, and providing enhanced security by supporting NIST 800-131A. Customers will have fewer IBM addresses to open on their firewall. All Call Home internet traffic will flow through the Call Home proxy and then fan out to various internal IBM service providers.

This list applies to all pre-defined ports and addresses used by ESA, but not to those ESA functions which allows the entry of a target address / port.

Table 2: Addresses and ports are used by ESA

Host Name	IP Address(es)	Port(s)	Protocol	Additional detail
esupport.ibm.com	129.42.56.189	443, 80	HTTPS (to IBM), HTTP (from IBM)	IPV4, Recommendation is that customers open the address range of 129.42.0.0 / 18 to minimize churn in the future if additional addresses are added.
	129.42.60.189			
	129.42.54.189			
	2620:0:6c0:200:129:42:56:189	443, 80	HTTPS (to IBM), HTTP (from IBM)	IPV6, Recommendation is that customers open 2620:0:6c0: /45 to minimize churn in the future if additional addresses are added.
	2620:0:6c2:200:129:42:60:189			
	2620:0:6c4:200:129:42:54:189			

Traditional Connectivity Options

This section of the appendix covers configuration for older versions of the Power Linux ESA.

IP address	Port	Host name	Purpose
207.25.252.197	443	eccgw01.boulder.ibm.com	Service information reporting
129.42.160.51	443	eccgw02.rochester.ibm.com	Service information reporting
129.42.26.224	443	www-945.ibm.com	Problem reporting
129.42.50.224	443	www-945.ibm.com	Problem reporting
129.42.42.224	443	www-945.ibm.com	Problem reporting
170.225.15.41	443	www6.software.ibm.com	Extended error data and system configuration reporting
192.109.81.20	443	www.ecurep.ibm.com	Extended error data and system configuration reporting
204.146.30.17	80,443	www-03.ibm.com	Configuration updates

Ports used by ESA

Table 3: Default ports used by ESA

Port	Description
5024	Port number at which the Electronic Service Agent graphical user interface is accessible through the HTTPS protocol.
5026 (Optional)	Port number at which the Service Proxy is configured as an ECC service proxy.
5028	Port number at which the firewall must be opened for UDP traffic to receive SNMP Traps.

© IBM Corporation 2015

IBM Corporation

Marketing Communications

Systems and Technology Group

Route 100

Somers, New York 10589

Produced in the United States of America

July 2015.

All Rights Reserved

This document was developed for products and/ or services offered in the United States. IBM may not offer the products, features, or services discussed in this document in other countries.

The information may be subject to change without notice. Consult your local IBM business contact for information on the products, features and services available in your area.

All statements regarding IBM future directions and intent are subject to change or withdrawal without notice and represent goals and objectives only.

IBM, the IBM logo, POWER, System I, System p, i5/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both. A full list of U.S. trademarks owned by IBM may be found at <http://www.ibm.com/legal/copytrade.shtml>.

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

IBM hardware products are manufactured from new parts, or new and used parts. Regardless, our warranty terms apply.

This equipment is subject to FCC rules. It will comply with the appropriate FCC rules before final delivery to the buyer.

Information concerning non-IBM products was obtained from the suppliers of these products.

Questions on the capabilities of the non-IBM products should be addressed with the suppliers.

The IBM home page on the Internet can be found at <http://www.ibm.com>.

PSW03007-USEN-00