SDS

Software Diversified Services

FAQ

VitalSigns SIEM Agent™ for z/OS

Contents

08.16.23

Introduction

SDS VitalSigns SIEM Agent™ for z/OS (VSA) monitors the mainframe running on z/OS to detect intrusions and insider threats, then delivers critical events in real time to the enterprise SIEM (security incident and event management system).

VSA acquires messages from the z/OS system console and SMF (system management facility). Using powerful, field-level SMF filters, the agent determines which SMF events are critical. VSA reformats the data as syslog, CEF, or LEEF events and forwards them, as well as messages from RACF, ACF2, Top Secret, DB2, CICS, IMS, and FTP, to one or two SIEMs. VSA is agnostic and integrates with Splunk, LogRhythm, QRadar, AlienVault, ArcSight, and many other SIEMs.

Installation

Is VSA dynamically installed?

Yes; you have only to APF-authorize the library containing the executables, and the product is ready to run. The agent dynamically installs its own SMF exits and dynamically creates its own EMCS console.

How long does it take to install and set up VSA?

The VSA agent may be uploaded and dynamically installed within a few minutes. With some minor configuration updates, it can then be up and running with default filters in a few minutes more. All program executables are available in binary format and uploaded to z/OS along with supporting z/OS JCL and installation instructions. The installation automatically activates filters commonly used by customers, allowing you to immediately see event notifications on the SIEM before defining and customizing the filters.

How long does VSA migration take going from one LPAR to another?

Assuming shared DASD, you can use the same libraries. Just APF authorize the load library on the additional LPARs and start the VSA agent. If changes are required, VSA allows for suffixing of configuration members such that each LPAR can have its own configuration and filters while operating out of the same VSA configuration library. For example, for LPAR14 and LPAR31, VSA could be started with VSACFG14 configuration members on LPAR 14 and VSACFG31 configuration members on LPAR31.

Operation

Does VSA run on zIIPs?

Yes. Event processing is performed on WLM Enclave SRBs and is made 100% zIIP-eligible without additional configuration. In benchmark tests, the VSA agent achieved more than 99% zIIP eligibility overall when processing SMF records alone, and up to 60% zIIP eligibility when processing console messages alone.

How much common storage does VSA use?

VSA loads its SMF exits into ECSA at agent startup. This program storage uses approximately 14 Kbytes of ECSA. During operation, SMF records are buffered, fixed cell pools residing in above-the-

bar common storage (HVCOMMON) for transmission to the agent. This storage is configurable, defaulting to 128 Mbytes.

Is VSA compatible with the latest z/OS?

VSA is compatible with any version of z/OS that is currently supported by IBM.

Which security products are supported?

VSA can be run on systems that use RACF, ACF2, and Top Secret.

Do I need additional hardware? Are there any product dependencies?

The z/OS agent is a stand-alone, software-only solution that uses common IBM z/OS functions to operate. There are no other z/OS software product dependencies.

Note that to achieve zIIP offload, one or more zIIPs must be online to the LPAR with available capacity to process the new workloads.

Can VSA push data in real time from a running z/OS?

Yes. When originally released as SMA_RT, it was the first z/OS SIEM agent to offer real-time mainframe intrusion detection and log event processing.

Can log data be pushed in batch?

Yes. The z/OS agent can read archived SMF logs, and can push the data into the real-time running task and out to the SIEM software.

Can the VSA agent be automatically managed?

Yes. The z/OS agent produces WTO messages that are displayed at all important junctures for any automation software package, such as at startup of the z/OS agent, open for business, and processing, and different shutdown phases, similar in design to CICS, DB2, IMS, and other z/OS software. The WTO messages can be used to automatically initiate and manage operations.

If a SIEM server becomes backlogged and the TCP connection stalls, the VSA agent issues a message to the system console. The Reload command can be used to automatically redirect messages to the other, healthy server. The format for subsequent messages can be changed using the Srv*n*Format command at the same time.

Configuration updates can be invoked in real time via a Modify command to the VSA agent.

How do I change the configuration? Can configuration be shared among LPARs?

VSA is configured via a set of partitioned dataset members. All configuration members can be shared by VSA agents running on different LPARS, updated using ISPF edit, and refreshed dynamically while the agent is running.

Does VSA support DNS names for SIEMs?

Yes, customers can specify an IP address or DNS name in the VSA configuration member.

Can VSA capture z/OS system log messages?

Yes. The customer defines the messages to be processed when setting up the filters. The z/OS agent can filter using up to the first 16 positions of the system log message. The filter process allows all messages (*), generically defined messages (ICH*), or specific messages (ICH408I*) to be included for processing. Refer to the section in this document about Filtering Data.

Can VSA capture logon failures and access failures?

Yes. Records can be configured to detect these events.

Can VSA capture access to sensitive resources?

Yes, even if the user security definitions have authority for the resource.

Does VSA support Unix systems running on z/OS?

Yes. The z/OS agent supports Unix System Services (USS). USS generates SMF records on specific events passed as SMF type 92 records to the VSA SMF exits for processing.

Can alerts be routed to multiple locations?

Yes, the z/OS agent can deliver alerts simultaneously to more than one location. VSA can send event alerts concurrently to multiple IP addresses or products such as ArcSight or Splunk via UDP or TCP.

The VSA agent can send alerts to one or two SIEM products that accept syslog, CEF, or LEEF format, as well as send to log consolidation products. Some customers may have an active log collector software product and an active SIEM product within the same environment. Other customers may want to send alerts to production and disaster recovery SIEM software simultaneously. The z/OS agent is able to satisfy both of these requirements.

Does VSA have a dashboard facility?

VSA provides an ISPF dialog that reports on various internal statistics, including events received, SMF types processed, queue depths, TCP/IP connection status, memory usage, CPU utilization, and zIIP offload performance. The ISPF dashboard also provides a window into recent event messages formatted and transmitted by the agent.

Data Sources

What are the data sources for VSA?

The z/OS agent receives its information from four different areas. The two primary data feeds are the SMF Exits and the EMCS console. A third data feed is from batch application programs communicating directly with the z/OS agent by using the batch API. A fourth data feed is from online applications running inside of CICS, IMS, or DB2, communicating directly with the z/OS agent by using the online API.

Filtering Data

How does VSA filter data?

VSA gathers data from SMF records and the EMCS console in real time. The raw z/OS data is filtered as specified in configuration members that are maintained in a partitioned dataset allocated to the agent. SMF records and EMCS console messages are each processed by multi-level selection and filtering options.

The available complex SMF filters enable SMF records to be filtered down to the field level, which provides unprecedented control over whether to escalate or disregard a record. This multi-step

filtering ensures that all user-defined critical information is forwarded and also minimizes the flood of messages at the server. VSA can help cut costs by reducing non-critical traffic and false alarms.

- **Filtering SMF Messages**

First-level selection and filtering of SMF records is performed at the point of capture in the SMF exits. Records filtered at this level are not forwarded to the agent for processing. This is the most efficient way to filter out events.

Second-level selection and filtering of SMF records is performed within the agent, after records are received from the exits. These filters provide powerful, field-level escalation or rejection of SMF records. Records selected for escalation will bypass third-level filtering and will be automatically escalated to the SIEM server. Records rejected by a second-level filter are immediately dropped.

Third-level filtering of SMF records is also performed within the agent. SMF records that match any of the configured rules are escalated to the SIEM server. Remaining records that do not match are rejected.

- **Fast-Path Filters**

Certain VSA filters during the first and second levels of filtering operate as “fast-path” filters for SMF records. Records that match any of these filters are formatted and transmitted to the SIEM server immediately.

- **Filtering Console Messages**

Console messages are filtered in two levels. During the first level, messages that match a configured rule are escalated to the second level. Remaining records are immediately dropped.

The second level of filtering uses an exclusion filter. Records that match the second filter are rejected. Remaining messages that have passed both first- and second-level filtering are escalated to the SIEM server.

Using generic characters, the interaction of first-level and second-level message processing allows you to easily define and qualify groups of messages to be escalated. For example, the first-level filter can capture all RACF IRR messages using the message rule IRR*, then the second-level exclusion filter can eliminate the high-volume message IRR0101.

Can SMF records be filtered based on any field?

VSA contains a comprehensive data dictionary of over 900 individual fields and Boolean values. Complex SMF filters can be configured based on any combination of these fields for unprecedented granularity.

What skills are required to create and maintain filters?

A security administrator with an intermediate z/OS skill set and a basic knowledge of SMF records can create and maintain filters.

Monitoring DB2

Does VSA collect DB2 records?

SMF 100 records are DB2 statistical records. SMF 101 records are DB2 accounting records. SMF 102 records carry DB2 performance, audit, and monitor data.

VSA can be configured for the collection of SMF 102 records only, and can filter by the different audit classes within the SMF 102 records.

SMF 100 records are collected internally by the software on a very limited basis, depending on the SMF 102 audit class(es) configured by the customer. They are used to cross-reference audit data found within the SMF 102 records. This saves on related overhead associated with unnecessarily and continuously collecting SMF 100 records. It also provides an additional level of filtering and makes VSA DB2 syslog event data more meaningful to the SIEM when it arrives.

Monitoring IMS

Does VSA collect IMS records?

VSA can be configured to collect IMS log records (IMS record subtypes 10, 16, and 22) from batch or using the IMS LOGWRT user exit. These records are packaged as SMF records and presented to the VSA agent for filtering, event formatting, and forwarding. The SMF record type number for IMS records can be defined by the operator.

Availability

Can VSA be run with 24x7 high availability?

Yes. The z/OS agent has designed safeguards within the VSA SMF exits to ensure high availability and recoverability. The VSA exits are automatically disabled when the agent is not active and the agent releases all related CSA storage at termination. VSA, in combination with z/OS recovery, provides the highest level of availability on a z/OS system.

The z/OS agent has been processing millions of possible security events 24x7 across multiple data centers in the U.S., Europe, and Australia since 2002 and has never caused a system outage.

Maintenance

Are new versions included in the license fee?

Yes, new versions and all new features are included with the license fee to customers with active maintenance and support agreements.

How often are new versions released?

SDS is dedicated to product improvements. Although there isn't a predetermined, set schedule, new releases are driven by the development roadmap, enhancement requests, and PTF requirements.

How are fixes supplied to customers?

Software executables are sent via TSO XMIT on the z/OS system running VSA, downloaded in binary format from z/OS to a workstation, and the new file is emailed to the customer.

The customer allocates a new loadlib on z/OS and uploads the new set of executables, in binary format, from a workstation to z/OS. The customer issues a TSO RECEIVE into the new solution loadlib and changes the solution configuration file parameter to the new executable library name. The z/OS agent solution is then restarted.

Do software upgrades or system updates require system outages?

No. VSA uses an MCS console that is dynamically activated during VSA agent initialization, or it can be activated with an operator command while the agent is running. The SMF exits are dynamically loaded into ECSA, and dynamically defined and added using the system CSVDYNEX facility.