SDS MAINFRAME SECURITY

Understanding Potential Savings with zIIP Offload and VitalSigns SIEM Agent for z/OS 4.3

SDS VITALSIGNS SIEM AGENT FOR z/OS

SDS

What’s new in VSA 4.3

About SDS

- Over 40 years in the mainframe industry!
- Expert development & technical support teams based in MN.
- 25+ products for mainframe and distributed platforms.
- Hundreds of organizations worldwide rely on SDS solutions.
- Focus on mainframe security and compliance.
- Long-standing global partnerships complement SDS software.
- Recognized for providing highest quality technical support.

Silver Business Partner IBM

CYBERSECURITY 500 WORLD'S HOTTEST SECURITY COMPANIES

What’s new in VSA 4.3

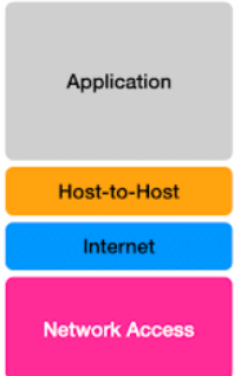
Agenda

- What’s New in VSA 4.3
  - Socket calls converted
  - Deprecated Parameters/Features
- zIIP Offload Eligibility
- zIIP Performance Figures
- Summary and Customer Feedback on VSA 4.3

What’s new in VSA 4.3

Socket calls Converted to USS Callable Services

- API use for TCP/IP communications was changed from EZASMI to USS Assembler callable (BPX) Services
- UDP datagrams or TCP segments are transmitted using BPX4AIO, the 64-bit asynchronous I/O Service



What’s new in VSA 4.3

Deprecated Parameters WtoEvents

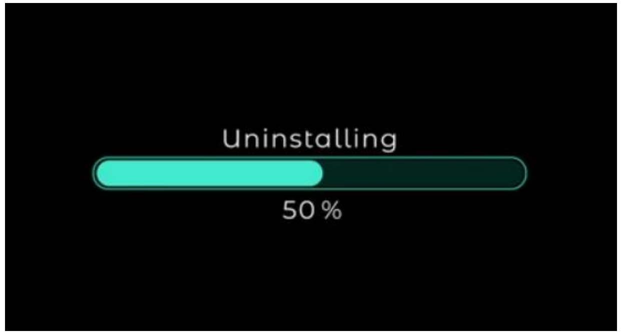
- The WtoEvents feature has been deprecated and removed
  - A new ISPF dashboard was added in VSA 4.2 to easily monitor SMF and Console event activity

SDS

What’s new in VSA 4.3

VSALOG is no longer supported

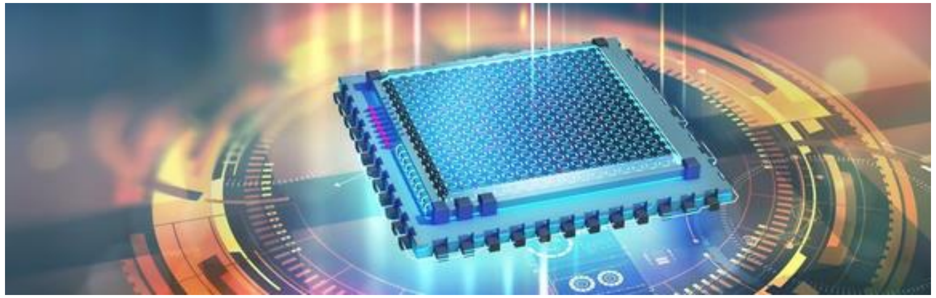
- The VSALOG DD has been removed from the shipped Agent and Batch Procs



What’s new in VSA 4.3

zIIP Offload Eligibility

- The VSA Agents event-processing tasks are converted to run in Enclave SRB mode and thus made eligible to be dispatched on zIIP processors
- VSA maintains a TCB for each enclave SRB and affinity between each TCB/SRB pair



SDS

What's new in VSA 4.3

zIIP Offload Eligibility

- Unlike many zIIP enabled program products, in normal operations there is no switching between SRB and TCB mode and no overhead is added
- In general, the longer the VSA Agent is active and processing events, the higher will be the ratio of offload-eligible to non-eligible work.

What’s new in VSA 4.3

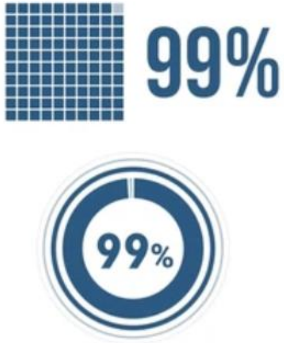
zIIP Offload Eligibility

- The overall proportion of total Agent CPU made eligible to run zIIPs will depend on many factors, including your workload.
- The greater the proportion of SMF records to console messages processed by an Agent, the larger the overall zIIP eligibility ratio will be in benchmark tests on a z16

What's new in VSA 4.3

zIIP Offload Eligibility

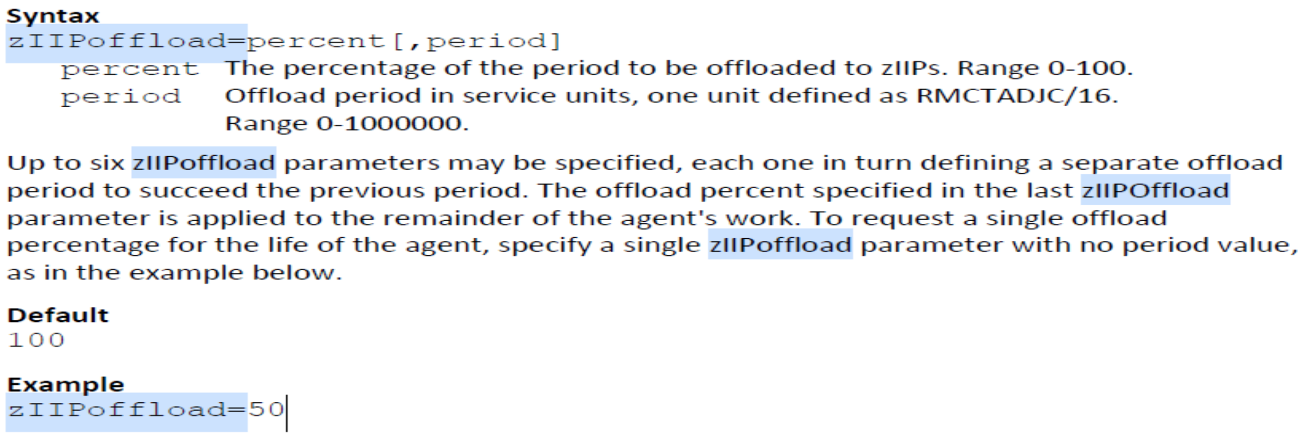
- The VSA Agent achieved more than 99% zIIP eligibility overall when processing SMF records alone and up to 60% zIIP eligibility when processing console messages alone



What’s new in VSA 4.3

zIIP Offload Eligibility

- To benefit from zIIP offload eligibility, no configuration is necessary
- To request less than 100% offload of eligible workloads, use the new zIIPoffload parameter in the VSACFG00



Syntax

```
zIIPoffload=percent[,period]
    percent   The percentage of the period to be offloaded to zIIPs. Range 0-100.
    period    Offload period in service units, one unit defined as RMCTADJC/16.
              Range 0-1000000.
```

Up to six zIIPoffload parameters may be specified, each one in turn defining a separate offload period to succeed the previous period. The offload percent specified in the last zIIPOffload parameter is applied to the remainder of the agent's work. To request a single offload percentage for the life of the agent, specify a single zIIPoffload parameter with no period value, as in the example below.

Default

```
100
```

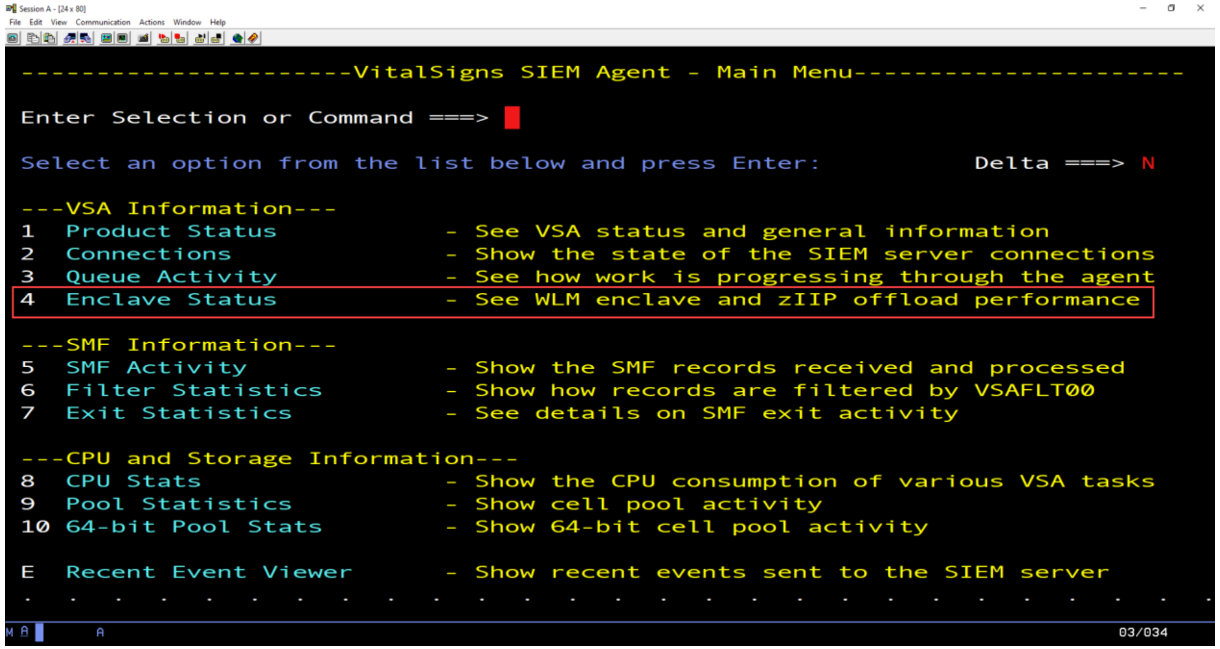
Example

```
zIIPoffload=50
```

What’s new in VSA 4.3

zIIP Offload Eligibility

- A new option 4 - Enclave Status has been added to the ISPF dialog
  - Product Status and CPU Stats Panels have also been updated

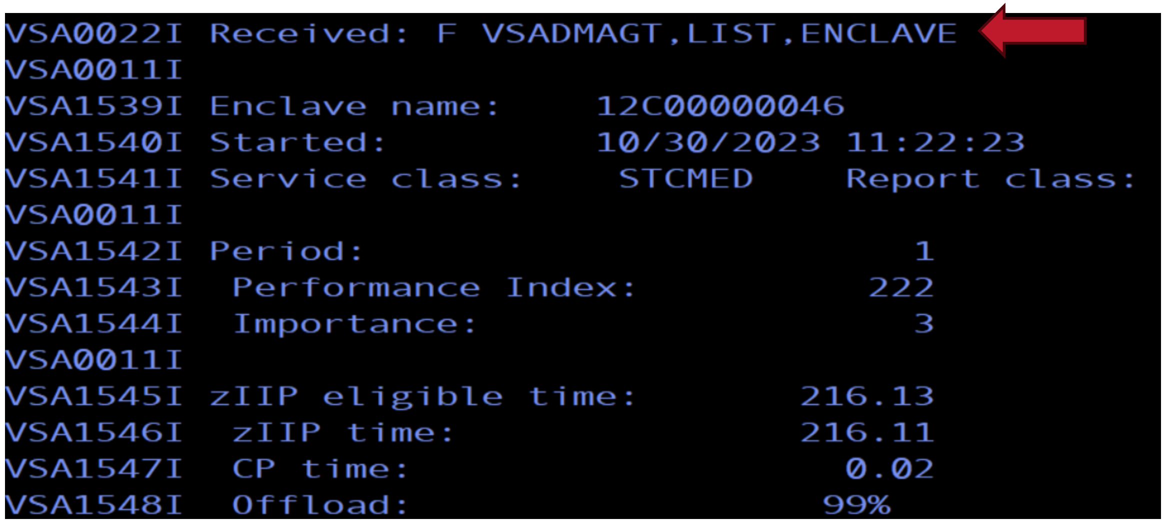


```
 ----------------------VitalSigns SIEM Agent - Main Menu----------------------

 Enter Selection or Command ===>

 Select an option from the list below and press Enter:           Delta ===> N

 ---VSA Information---
 1   Product Status              - See VSA status and general information
 2   Connections                 - Show the state of the SIEM server connections
 3   Queue Activity              - See how work is progressing through the agent
 4   Enclave Status              - See WLM enclave and zIIP offload performance

 ---SMF Information---
 5   SMF Activity                - Show the SMF records received and processed
 6   Filter Statistics           - Show how records are filtered by VSAFLT00
 7   Exit Statistics             - See details on SMF exit activity

 ---CPU and Storage Information---
 8   CPU Stats                   - Show the CPU consumption of various VSA tasks
 9   Pool Statistics             - Show cell pool activity
 10  64-bit Pool Stats           - Show 64-bit cell pool activity

 E   Recent Event Viewer         - Show recent events sent to the SIEM server
 .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
M A          A                                                          03/034
```

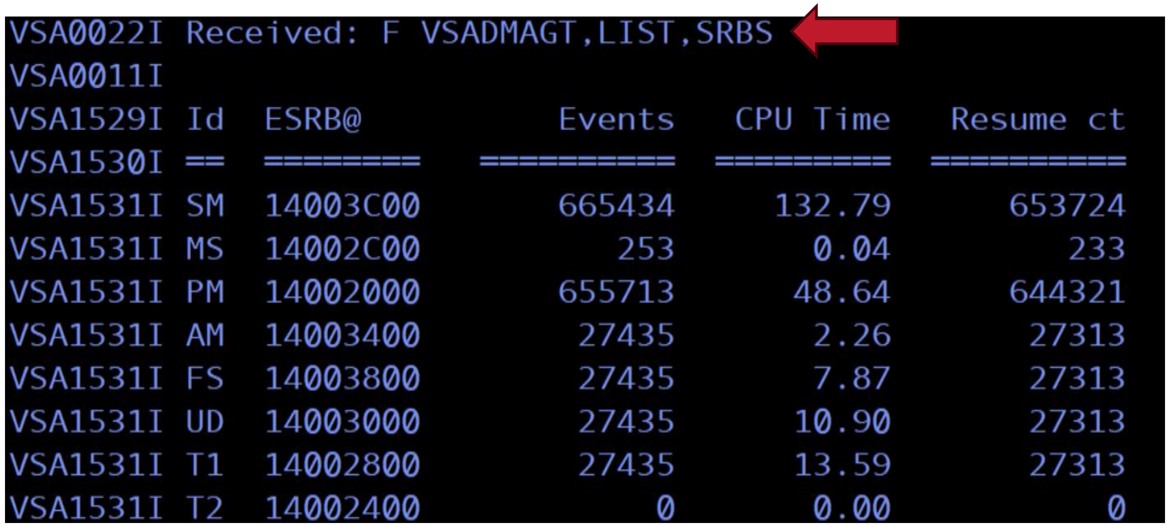
What's new in VSA 4.3

zIIP Offload Eligibility

- There is a new Agent command
  - LIST,ENCLAVE
  - LIST,SRBS



```
VSA0022I Received: F VSADMAGT,LIST,ENCLAVE
VSA0011I
VSA1539I Enclave name:     12C00000046
VSA1540I Started:          10/30/2023 11:22:23
VSA1541I Service class:     STCMED      Report class:
VSA0011I
VSA1542I Period:                              1
VSA1543I  Performance Index:                222
VSA1544I  Importance:                         3
VSA0011I
VSA1545I zIIP eligible time:             216.13
VSA1546I  zIIP time:                     216.11
VSA1547I  CP time:                         0.02
VSA1548I  Offload:                        99%
```



```
VSA0022I Received: F VSADMAGT,LIST,SRBS
VSA0011I
VSA1529I Id  ESRB@         Events   CPU Time   Resume ct
VSA1530I ==  ========  ==========  =========  ==========
VSA1531I SM  14003C00      665434     132.79      653724
VSA1531I MS  14002C00         253       0.04         233
VSA1531I PM  14002000      655713      48.64      644321
VSA1531I AM  14003400       27435       2.26       27313
VSA1531I FS  14003800       27435       7.87       27313
VSA1531I UD  14003000       27435      10.90       27313
VSA1531I T1  14002800       27435      13.59       27313
VSA1531I T2  14002400           0       0.00           0
```

VSA 4.3 Benchmark Tests - Environment

- Benchmark Hardware Environment
  - Tests were run on a z16 -IBM3931 Model A01 running on z/OS 2.5
    - 1 CP
    - 1 zIIP

VSA 4.3 Benchmark Tests - Environment

- Test 1 (3 separate batch runs were run consecutively)
    - Performance while processing SMF events was tested using the VSA batch utility to queue a mixed workload of SMF records to the Agent
    - SMF exits and the EMCS console were disabled to reduce the number of variables

VSA 4.3 Benchmark Tests - Environment

- Test 2 (WTO messages)
  - Performance while processing console messages was tested using a REXX exec to generate WTO messages.
  - All messages generated by the execs were selected for processing, formatted, and sent to the server. Incidental console messages received during the test period were not selected.

What's new in VSA 4.3

VSA 4.3 Benchmark Tests - SMF Event Processing

- A mixed workload of 2,589,597 SMF records was queued to the Agent
- Three separate batch runs were submitted in sequence. Each test consisted of:
  - Sending 863,199 records
  - Rate of approximately 70,000 records per minute
  - All SMF records were formatted into event messages in the CEF format
  - SMF Events were transmitted to a single TCP server

What's new in VSA 4.3

VSA 4.3 Benchmark Tests - SMF Event Processing

- Agent completed receiving records and formatting SIEM messages in 22 minutes 19 seconds
- All events messages were fully processed and transmitted to the Server within 24 minutes and 17 seconds
- CPU time was recorded at run time by each component's TCB and SRB using TIMEUSED
- Actual zIIP offload data was retrieved from z/OS Workload Manager (WLM) using IWMEQTME

What's new in VSA 4.3

VSA 4.3 Benchmark Tests - Summary

- Agent recorded zIIP eligibility (i.e., the percent of CPU time run on enclave SRBs) between 99.77% and 99.97% during and immediately following the test
- Actual zIIP offload during the test was consistently recorded at 92% to 93%

SDS

What’s new in VSA 4.3

VSA 4.3 Benchmark Tests - Mix of records for SMF Event Test

Record Type	SMF Record Description	Received from Batch
SMF 14	Input Dataset Activity	37572
SMF15	Output Dataset activity	6888
SMF17	Scratch Dataset Status (Expand)	669
SMF18	Rename Non-VSAM Dataset	3
SMF30	Job or task initiation / termination	85485
SMF32	TSO User work	318
SMF42	DFSMD Statistics and Configuration	4389
SMF62	VSAM open or cluster opened	1956
SMF80	RACF and PKI processing	55923
SMF92	z/OS UNIX file system activity	2380092
SMF119	TCP/IP Statistics	16302
	Total	**2589597**

What’s new in VSA 4.3

VSA 4.3 Benchmark Tests - SMF Event Processing

- ▶ Several CPU snapshots were taken during the test as per the next 3 slides for Test 1 (SMF Event Testing)

VSA Task	No of Events	Total TCB time	Enclave SRB time	CPU per event	zIIP Eligibility
SCI		0.01248			
SCR		0.01144			
SCD		0.00249			
SCT		0.00108			
DI		0.00651			
NR		0.00039			
XM		0.00010			
MC		0.00080			
SM	**422174**	0.04208	43.06	0.00010	99.90%
MS		0.00004	0.00		62.55%
PM	422154	0.00005	0.22		99.97%
AM	422154	0.00003	0.35		99.98%
FS	116795	0.00004	3.67	0.00003	99.99%
UD		0.00011	0.00		52.96%
T1		0.00008	0.00		61.64%
T2	**116797**	0.00009	0.49	0.00000	99.97%
Total		0.07788	**47.80**		**99.83%**

- Test 1 SMF (1st run) - After 422,174 records had been received and 116,797 SIEM event messages had been transmitted, the Agent had used 47.80 CPU seconds with a zIIP eligibility rate of 99.83%

VSA Task	No of Events	Total TCB time	Enclave SRB time	CPU per event	zIIP Eligibility
SCI		0.01248			
SCR		0.03443			
SCD		0.01125			
SCT		0.01687			
DI		0.00708			
NR		0.00039			
XM		0.00010			
MC		0.00080			
SM	2317946	0.04208	458.67	0.00019	99.99%
MS		0.00004	0.00		62.55%
PM	2317942	0.00005	1.60		99.99%
AM	2317942	0.00003	2.00		99.99%
FS	1925430	0.00004	108.13	0.00005	99.99%
UD		0.00011	0.00		52.96%
T1		0.00008	0.00		61.64%
T2	1925432	0.00009	9.47	0.00000	99.99%
Total		0.12599	579.89		99.97%

- Test 1 SMF (2nd run) - After 2,317,946 records had been received and 1,925,432 SIEM event messages had been transmitted, the Agent had used 579.89 CPU seconds with a zIIP eligibility rate of 99.97%

VSA Task	No of Events	Total TCB time	Enclave SRB time	CPU per event	zIIP Eligibility
SCI		0.01248			
SCR		0.03443			
SCD		0.01125			
SCT		0.01687			
DI		0.00708			
NR		0.00039			
XM		0.00010			
MC		0.00080			
SM	2589603	0.04208	565.26	0.00021	99.99%
MS		0.00004	0.00		62.55%
PM	2589600	0.00005	2.07		99.99%
AM	2589600	0.00003	2.23		99.99%
FS	1925430	0.00004	108.13	0.00005	99.99%
UD		0.00011	0.00		52.96%
T1		0.00008	0.00		52.96%
T2	2589597	0.00009	12.69	0.00000	99.99%
Total					**99.97%**

- Test I SMF (3rd run) - After all SMF records had been received, formatted and transmitted to the TCP destination, 747.27 CPU seconds had been used with a reported 99.97% zIIP eligibility

VSA Task	No of Events	Total TCB time	Enclave SRB time	CPU per event	zIIP Eligibility
SCI		0.01248			
SCR		0.03443			
SCD		0.01125			
SCT		0.01687			
DI		0.00708			
NR		0.00039			
XM		0.00010			
MC		0.00080			
SM	**2589603**	0.04208	565.26	0.00021	99.99%
MS		0.00004	0.00		62.55%
PM	2589600	0.00005	2.07		99.99%
AM	2589600	0.00003	2.23		99.99%
FS	1925430	0.00004	108.13	0.00005	99.99%
UD		0.00011	0.00		52.96%
T1		0.00008	0.00		52.96%
T2	**2589597**	0.00009	12.69	0.00000	99.99%
Total					**99.97%**

- Test 1 SMF (notes) - Each batch run included a pair of marker records that were counted by the Agent as received but were not formatted or transmitted. This accounts for the difference between the events count shown by the SM (receiver) task and the T2 (TCP Server) task.

What's new in VSA 4.3

VSA 4.3 Benchmark Test 1 - Notes

- By the end of the test, the continued high event arrival rate drove cell pool contraction processing in the DI (Director) task, which increased the total TCB time and consequently slightly reduced the overall zIIP eligibility calculation.

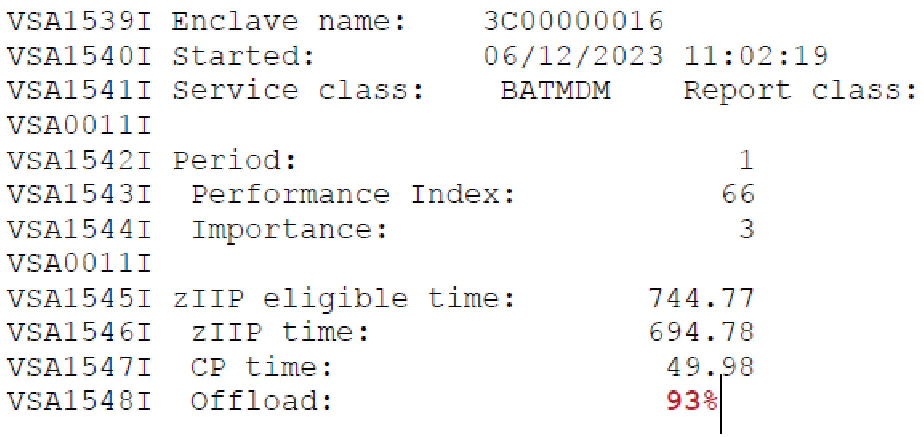
What's new in VSA 4.3

VSA 4.3 Benchmark Test I - Notes

- SMF exit processing time, which is counted and reported separately by the Agent, is not shown here, since all records were queued directly from batch.
- The SMF exits and the batch utility use the same technique to queue records to the agent.

VSA 4.3 Benchmark Test 1 - Notes

- Six times during and immediately following the test, WLM was queried for actual zIIP time vs. CP time within the enclave.
- One query reported actual zIIP offload of 92% and five reported 93%



```
VSA1539I Enclave name:     3C00000016
VSA1540I Started:          06/12/2023 11:02:19
VSA1541I Service class:     BATMDM    Report class:
VSA0011I
VSA1542I Period:                          1
VSA1543I  Performance Index:             66
VSA1544I  Importance:                     3
VSA0011I
VSA1545I zIIP eligible time:        744.77
VSA1546I  zIIP time:                694.78
VSA1547I  CP time:                   49.98
VSA1548I  Offload:                   93%
```

SDS

What’s new in VSA 4.3

VSA 4.3 Benchmark Test 2 - Console Message Event Processing

- A REXX exec was used to issue 6,000 WTO (Write to Operator) calls.
- All messages sent by the REXX exec were formatted into event messages in the CEF format and transmitted to a single TCP server.

```
stringReplace = string
value = float(value) tempValue = str(
Format = 14 #Replace string by value's Q4 temp
tempString = tempString.replace("czDataTyp
value*pow(10,14-tmpFormat)))) tempString = temp
typeOfFID == "BUFFER"): s = value dataCal =
tempString.replace("czFieldID",str(key)) tempStri
typeOfFID == "ASCII_STRING"): s = value dataC
tempString = tempString.replace("czData
Name value=" in line and flagCheckRicnam
</Message>" in line: myEvent = "RT_CHA
onlyFilename+"\n" if typeOfFile == "RT":
os.path.exists(path): os.makedirs(path)
InputARTAVTEST/"): shutil.rmtree(
searchObj = re.search(
Filename
```

What's new in VSA 4.3

VSA 4.3 Benchmark Test 2 - Console Message Event Processing

- In addition to the 6,000 messages issued by the exec, the agent received 37 "naturally occurring" messages from the console during the test.
- None of these messages were formatted or transmitted.

```
stringReplace = string
value = float(value) tempValue = str(
tmpFormat = 14 #Replace string by value's Q4 temp
tempString = tempString.replace("czDataTy
(value*pow(10,14-tmpFormat)))) tempString = temp
typeOfFID == "BUFFER"): s = value dataCal =
tempString.replace("czFieldID",str(key)) tempStri
typeOfFID == "ASCII_STRING"): s = value dataC
tempString = tempString.replace("czData
"Name value=" in line and flagCheckRicnam
if "</Message>" in line: myEvent = "RT_CHA
onlyFilename+"\n" if typeOfFile == "RT": b
os.path.exists(path): os.makedirs(path)
"InputRTAVTEST/"): shutil.rmtree(
searchObj = re.search(
filename
```

VSA Task	No of Events	Total TCB time	Enclave SRB time	CPU per event	zIIP Eligibility
SCI		0.01161			
SCR		0.01428			
SCD		0.00311			
SCT		0.00498			
DI		0.00632			
NR		0.00033			
XM		0.00010			
MC	6037	0.14257		0.00002	
SM		0.00027	0.00		17.58%
MS	6000	0.00004	0.05	0.00000	99.92%
PM	6000	0.00003	0.07	0.00001	99.95%
AM	6000	0.00005	0.01	0.00000	99.50%
FS	6000	0.00005	0.15	0.00002	99.96%
UD		0.00009	0.00		57.61%
T1		0.00008	0.00		63.14%
T2	6000	0.00008	0.07	0.00001	99.87%
Total		0.18404	0.37		67.01%

- SMF Console Messages (Test 2) - During the test, the Agent used 0.55 seconds and measured 67.01% zIIP eligibility

What's new in VSA 4.3

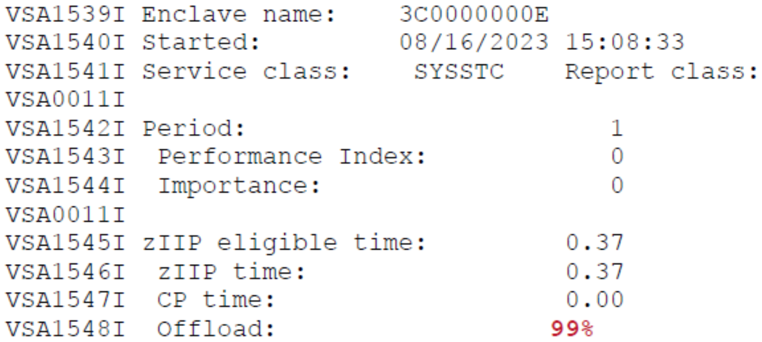
VSA 4.3 Benchmark Tests - Notes

- Since EMCS console services must be called in task mode, console messages are received and primary filtering done on the MC task's TCB, which is not zIIP eligible.
- Any messages selected for further processing are queued to the MS task enclave SRB.
- Processing from that point was generally 100% zIIP eligible.

What’s new in VSA 4.3

VSA 4.3 Benchmark Tests - Notes

- The higher the proportion of selected to excluded messages, then, the greater the total CPU consumption, but the higher would be the zIIP eligibility ratio.
- After conclusion of the test, WLM was queried for actual zIIP time vs. CP time within the enclave. The query reported 99% zIIP offload of eligible CPU:



```
VSA1539I Enclave name:    3C0000000E
VSA1540I Started:         08/16/2023 15:08:33
VSA1541I Service class:    SYSSTC    Report class:
VSA0011I
VSA1542I Period:                        1
VSA1543I  Performance Index:            0
VSA1544I  Importance:                   0
VSA0011I
VSA1545I zIIP eligible time:         0.37
VSA1546I  zIIP time:                 0.37
VSA1547I  CP time:                   0.00
VSA1548I  Offload:                  99%
```

What's new in VSA 4.3

Customer Feedback on VSA 4.3

- Favorable feedback from VSA customers
  - Some customers are seeing as much as 92% eligibility/offload to their zIIP
  - Comments from customers:
    - "Easy to install"
    - "Immediate Results"
    - "It just works"

What’s new in VSA 4.3

Summary

- VSA 4.3 has significant performance improvements
- If you have zIIP hardware, it’s a “no brainer” upgrading to VSA 4.3
- No configuration is required on VSA to exploit the zIIP
- Contact the SDS Support team if you want to download VSA 4.3.
  - Open a support ticket: https://support.sdsusa.com/issues/
  - Email: support@sdsusa.com

Would you like additional information?

763-571-9000

SDS

info@sdsusa.com

(800) 443-6183
(763) 571-9000

www.sdsusa.com