z/OS V2.5 IBM Education Assistant

Solution Name: Predictive Failure Analysis (PFA) Enhance Recommended Actions for all checks

Solution Element(s): BCP PFA

July 2021

Agenda

- Trademarks

- Objectives

- Overview

- Usage & Invocation

- Interactions & Dependencies

- Upgrade & Coexistence Considerations

- Installation & Configuration

- Summary

- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Objectives

- Discuss enhancements to PFA to help a system operator to quickly identify anomalous systems to enable recovery and to improve decision-making regarding recovery steps so that your systems can be recovered quickly and accurately.

Overview

- Who (Audience)
  - Systems operators, systems programmers

- What (Solution)
  1. Provide recommended diagnostic actions on the PFA reports for all checks.
  2. Dump the top 2 ASIDs for PFA_COMMON_STORAGE_USAGE and PFA_PRIVATE_STORAGE_EXHAUSTION checks when DEBUG(1).
  3. Include Runtime Diagnostics output for checks in exception on all applicable checks.
  4. Provide WLM health value for applicable address spaces and checks.
  5. Provide rate of increase of storage usage for PFA_COMMON_STORAGE_USAGE and PFA_PRIVATE_STORAGE_EXHAUSTION.
  6. Provide when storage overflow occurred for PFA_COMMON_STORAGE_USAGE.
  7. Provide the capability to graph the data for exhaustion checks to show when the anomaly started.

- Wow (Benefit / Value, Need Addressed)
  - Help a system operator to more easily investigate and more quickly analyze problems before an outage occurs.

- This check's report
  1. Shows dynamic exception severity and exception message at top of report.
  2. Reminds you to look at new diagnostic actions in the "Operator Response" section of the message at the bottom of the report.
  3. Has section headings
  4. Includes Runtime Diagnostics output for two address spaces that have increased the most.
  5. Shows rate of increase and time of start of increase for each storage location and for each address space listed for locations in exception (i.e., when did the trend start to change)
  6. Shows start time of overflow.
  7. Shows ASID to address space details.
  8. Lists recommended actions in the "Operator Response" of the exception message.

- Scenario
  - Two jobs are running that get and free storage, but leak it.
  - Note that this is a contrived scenario in a test environment intended to gather the data for this report. This was not a realistic scenario.

- Note also that when an exception occurs, the 2 address spaces whose usage has increased the most recently will be dumped along with the PFA address space and the RASP address space when DEBUG(1).

1
2

```
* High Severity Exception Issued *

The common storage usage has been predicted to exceed the capacity by
10/16/2020 12:47:01.

See the 'Operator Response' section of the exception message below for
recommended actions.

                    Common Storage Usage Prediction Report

Last successful model time      :  10/16/2020 11:44:41
Next model time                 :  10/16/2020 23:44:41
Model interval                  :  720
Last successful collection time:   10/16/2020 11:44:40
Next collection time            :  10/16/2020 11:59:40
Collection interval             :  15
```

3

```
SECTION 1: COMMON STORAGE USAGE DATA


                                      Capacity When   Percentage
Storage     Current Usage  Prediction  Predicted     of Current
Location    in Kilobytes   in Kilobytes in Kilobytes  to Capacity
_____  _____  _____  _____  _____
CSA                 1180         15564          2596          45%
SQA                 2425          2425          2460          99%
*CSA+SQA            3606         17988          5056          71%
ECSA              388786       2162859        512016          76%
ESQA                8812         10290         13124          67%
ECSA+ESQA         397598       2171162        525140          76%
```

5
6

```
Additional details:

             Rate of
             Change Per
             Minute for      Start Date and
Storage      Current Trend   Time of
Location     in Kilobytes    Current Trend

_____   _____    _____
CSA                    23    10/16/2020 11:37:35
SQA                     0    10/16/2020 11:36:34
*CSA+SQA               24    10/16/2020 11:35:34
ECSA                15250    10/16/2020 11:24:27
ESQA                   -9    10/16/2020 11:30:30
ECSA+ESQA           15247    10/16/2020 11:24:27

Storage requested from SQA expanded into CSA and is being included in
CSA current usage and predictions.  Comparisons for SQA are not being
performed.  If an exception occurred in CSA, both locations were marked
as causing the exception because storage obtained from both locations
may exceed capacity. Expansion from SQA into CSA started between
10/16/2020 11:35:42 and 10/16/2020 11:36:43.

Owner gone storage:

       Storage      Current Usage
       Location     in Kilobytes

       _____   _____
       CSA                     0
       SQA                     0
       CSA+SQA                 0
       ECSA                    0
       ESQA                   13
       ECSA+ESQA              13
```

```
SECTION 2: ADDRESS SPACE DATA

Address spaces with the highest increased usage:

Job           Storage   Current Usage      Predicted Usage
Job Name ASID Location  in Kilobytes       in Kilobytes
_____ ____ _____  _____      _____
CSATST2E 0028 ECSA             375000              2153521
CSATST2S 002D *SQA               2940                17158

Additional details:

                        Rate of
                        Increase Per
                        Minute for    Start Date and
Job           Storage   Current Trend Time of
Name     ASID Location  in Kilobytes  Current Trend
_____ ____ _____  _____ _____
CSATST2E 0028 ECSA              15250 10/16/2020 11:24:27
CSATST2S 002D *SQA                124 10/16/2020 11:35:34

* = Storage locations that caused the exception.

SECTION 3: RUNTIME DIAGNOSTICS OUTPUT FOR THE TOP TWO ADDRESS SPACES

Runtime Diagnostics detected a problem in ASID:    002D
EVENT 1: HIGH:LOOP            SYSTEM: SYS1      10/16/2020 11:47:52
  ASID: 002D JOBNAME: CSATST2S TCB: 004FF1C0
  STEPNAME: STEP1   PROCSTEP:        JOBID: JOB00045
  USERID: IBMUSER JOBSTART: 2020/10/15 15:22:34
ERROR : ADDRESS SPACE MIGHT BE IN A LOOP ON SYS1.
ACTION: USE YOUR SOFTWARE MONITORS TO INVESTIGATE THE ASID.
-------------------------------------------------------------

* High Severity Exception

AIRH101E The common storage usage has been predicted to exceed the
capacity by 10/16/2020 12:47:01.
```

```
Explanation:  This check is looking to see if there is a potential for
    storage to be exhausted in the upcoming model interval. The model of
    common storage utilization for this LPAR has predicted that usage of
    common storage will exceed the threshold set by the user before the
    current model interval ends at 10/16/2020 12:47:41. The prediction
    was modeled at 10/16/2020 11:44:41.

  System Action:  Subsequent runs of this check will not produce an
    operator message until new data is available

Operator Response:

  1. Examine SECTION 1: COMMON STORAGE USAGE DATA in the report above
  and the details of the address spaces listed whose usage has grown
  the most in the modeled data. If storage has expanded from SQA to
  CSA and the exception is in CSA storage, both CSA and SQA have been
  marked as causing the exception. If storage has expanded from ESQA
  to ECSA and the exception is in ECSA storage, both ECSA and ESQA
  have been marked as causing the exception.

  2. Examine SECTION 2: ADDRESS SPACE DATA to determine which address
  spaces are most likely causing the problem. Remember that this list
  is a list of address spaces with the most increased usage, not the
  address spaces that are using the most storage. It is most often the
  case that the address spaces that have recently increased their
  storage usage are the cause of the potential exhaustion.

  3. Create the graph of the usage for the storage locations causing the
  exception. Then, create the graphs of storage usage for the storage
  locations in exception for the top five address spaces whose usage has
  increased the most. Examine the usage patterns and try to determine
  when the anomaly started and whether this is a large consumer with a
  spike, leak or creep in usage. IBM has provided Python scripts that
  can be used to graph this resource usage over time. These graphs can
  be very helpful in determining the root cause of the problem. This
  code is provided 'as-is' and can be found on the IBM GitHub page. See
  the 'Graphing Exhaustion Data' section in z/OS Problem Management for
  more details.
```

4. Determine how close the system is to exhausting common storage. The date and time of exhaustion in the exception message indicates the time of exhaustion if the rate of increase remains steady until the end of the model interval.

5. Consult your performance monitor. If you are familiar with Resource Management Facility (RMF), consult RMF for details about address spaces whose resource usage is climbing the most rapidly. You can use IBM OMEGAMON which shows everyday usage and points out when something is abnormal. Assess whether the address spaces' consumption of storage was normal in the past and whether the current high rate of consumption is due to too much work and requires more compacity or if this is usage is abnormal and the sign of a storage leak.

6. Compare address space storage consumption with a peer or clone on this system or another member of the sysplex doing similar work to see if this increased storage usage is occurring elsewhere or is something abnormal only on this system.

7. If provided, example SECTION 3: RUNTIME DIAGNOSTICS OUTPUT FOR THE TOP TWO ADDRESS SPACES that have increased their usage the most in the modeled data. Perform the ACTION steps in the output. If Runtime Diagnostics output is desired for more address spaces such as address spaces that are not in the top two, invoke Runtime Diagnostics to obtain additional output using the following command:

    f hzr,analyze

8. Examine the IBM Health Checker for z/OS log for related exceptions in other checks. A list of top users of common storage can be found in the reports for the VSM_CSA_THRESHOLD check and the VSM_SQA_THRESHOLD check.

9. Examine SYSLOG, OPERLOG, and LOGREC (i.e., EREP report) around the time the anomaly started to determine whether there are problems being recovered which may be causing additional storage to be obtained in these address spaces. Look for problems reported by key components such as XCF, GRS, and Logger because problems in those components can affect components that are dependent on them. See if any SVC dumps have been taken recently for existing problems.

10. If the problem remains unknown and your local guidelines allow you to initiate a dump, take an SVC dump of the address spaces before they terminate and include the RASP address space by modifying this check's DEBUG parameter to DEBUG(1) or by taking the SVC dump manually. If the DEBUG parameter is set to 1 and this problem continues to occur, PFA will dump the top two address spaces increasing the most, the PFA address space, and the RASP address space automatically in the comparison interval when a new WTO exception is issued and then at the next comparison interval after it if the exception continues to occur. You can compare the two sets of dumps to see where the storage is continuing to increase. Change DEBUG to DEBUG(0) after the dumps have been taken.

When reviewing the dumps, investigate the control block information or the owncomm information in detail using the command 'IP VERBX VSMDATA' with the appropriate parameters. See the 'MVS Interactive Problem Control System (IPCS) Commands' book for more information on that command. If the address space causing the storage increase is a system address space, open a Case with IBM Service to determine the root cause.

To set the DEBUG parameter to 1, use the following command:

    f hzsproc,update,check(IBMPFA,PFA_COMMON_STORAGE_USAGE),
    parm('debug(1)')

11. If the address space causing the common storage growth is identified, consider the risks of quiescing the function and rerouting work around it. Determine what work is dependent on the address space consuming storage and its business importance. Follow installation restart procedures to determine whether to restart the address space.

12. To find additional recommendations, consult the z/OS Problem Management book, Predictive Failure Analysis checks chapter, PFA_COMMON_STORAGE_USAGE subsection, in the 'Best Practices' topic.

13. If the problem cannot be easily determined in a short amount of time and you want to stop all exceptions until the problem can be resolved, do one of the following:

   a. Quiesce the check so that data continues to be collected, but comparisons are not performed. Quiescing the check allows the check to resume processing with no interruption of collected data once the check is reactivated. First, ensure the check will collect and model data while deactivated by setting COLLECTINACTIVE to 1 and then deactivate the check.

```
f hzsproc,update,check(IBMPFA,PFA_COMMON_STORAGE_USAGE),
parm('collectinactive(1)')

f hzsproc,deactivate,check(IBMPFA,PFA_COMMON_STORAGE_USAGE)
```

   b. Change the severity of the exception so that all processing continues for this check, but exceptions are not issued by modifying the dynamic severity parameters for this check by setting these parameters so that all exceptions issued by this check use no severity. Use the command below or establish an IBM Health Checker for z/OS PARMLIB member to make the change persistent:

```
f hzsproc,update,check(IBMPFA,PFA_COMMON_STORAGE_USAGE),
parm('e_high(unused) e_med(unused) e_low(unused) e_none(max)')
```

14. After investigating the problem, if you have determined that the exception is normal operating behavior and you do not want to be alerted for similar data in the future, perform one or more of the following actions:

   a. Modify the THRESHOLD parameter to a higher value. This parameter defines the percentage of the capacity over 100% of the total capacity that defines the point of exhaustion. For example, if 2 is specified which is the default, the prediction must be at least 102% of the capacity for a storage location before the comparisons are performed. Setting the threshold too high might cause exhaustion problems to be undetected. Use the command below and specify your desired value in place of the X or establish an IBM Health Checker for z/OS PARMLIB member to make the change persistent:

```
f hzsproc,update,check(IBMPFA,PFA_COMMON_STORAGE_USAGE),
parm('threshold(X)')
```

   b. If the exception was for SQA, but you do not want SQA exceptions in the future, turn off checking for SQA by setting CHECKSQA to 0 using the command below or establish an IBM Health Checker for z/OS PARMLIB member to make the change persistent:

```
f hzsproc,update,check(ibmpfa,PFA_COMMON_STORAGE_USAGE),
parm('checksqa(0)')
```

   c. If the exception was for ESQA, but you don't want ESQA exceptions in the future, turn off checking for ESQA by setting CHECKESQA to 0 using the command below or establish an IBM Health Checker for z/OS PARMLIB member to make the change persistent:

```
f hzsproc,update,check(ibmpfa,PFA_COMMON_STORAGE_USAGE),
parm('checkesqa(0)')
```

   d. Modify this check's dynamic severity parameters by using the IBM Health Checker for z/OS modify command. These parameters determine the severity of the WTO issued when this check detects the potential for future exhaustion. The severity is based on the number of minutes until exhaustion would occur with a steady increase of usage such that the severity increases the closer the system is to resource exhaustion. The number of minutes is specified in the E_HIGH, E_MED, E_LOW, and E_NONE parameters. Use the command below and specify your desired values in place of X or establish an IBM Health Checker for z/OS PARMLIB member to make the change persistent:

```
f hzsproc,update,check(IBMPFA,PFA_COMMON_STORAGE_USAGE),
parm('e_high(X) e_med(X) e_low(X) e_none(X)')
```

- Enhancements
  1. Shows exception message at top of reports
  2. Reminds you to look at new diagnostic actions in the "Operator Response" section of the message at the bottom of the report.
  3. Has section headings
  4. Includes Runtime Diagnostics output
     - For address spaces causing the "too high" exception whose WLM health value is < 100 for tracked and persistent exceptions
     - For total system for other non-persistent and system exceptions
     - For exceptions indicating rates that are too low as in previous releases.
  5. Includes WLM health setting for address spaces causing exceptions.
  6. Lists recommended actions in the "Operator Response" of the exception message.

- Scenario – A job was running that was not tracked or persistent.

PFA_MESSAGE_ARRIVAL_RATE Report Changes – 2 of 3

1

```
* Exception Issued *

The total system message arrival rate is higher than expected and may
indicate a system problem.
```

2

```
See the 'Operator Response' section of the exception message below for
recommended actions.

                    Message Arrival Rate Prediction Report

Last successful model time     :  10/19/2020 16:11:14
Next model time                :  10/20/2020 04:11:14
Model interval                 :  720
Last successful collection time:  10/19/2020 16:12:14
Next collection time           :  10/19/2020 16:27:14
Collection interval            :  15
```

3

```
SECTION 1: MESSAGE ARRIVAL RATE DATA

Message arrival rate
   in last collection interval      :          43.68
Prediction based on 1 hour of data  :          18.10
Prediction based on 24 hours of data:          18.10
Prediction based on 7 days of data  :          18.10

Highest STDDEV needed to avoid this exception:  3

Top persistent users:

                                        Predicted Message
                       Message             Arrival Rate
   Job                 Arrival
   Name    ASID         Rate      1 Hour     24 Hour       7 Day
   _____ ____    _____  _____  _____  _____
   MARTST1 0028        358.82      400.00      400.00      400.00

Additional details:

                     WLM
   Job               Health
   Name    ASID      Setting

   _____ ____      _____
```

5

```
   MARTST1 0028         20
```

```
SECTION 2: RUNTIME DIAGNOSTICS OUTPUT FOR SYSTEM

EVENT 1: HIGH:SERVERHEALTH      SYSTEM: SY1      2020/10/19 16:11:15
    JOB NAME: MARTST1   ASID: 0028  CURRENT HEALTH VALUE: 20
    CURRENT LOWEST HEALTH VALUES:
              SUBSYSTEM    HEALTH                  REPORTED
    SUBSYSTEM  NAME        SETTING        REASON   DATE AND TIME
    HZR        FHBRSMAR       20          Set to 20.  2020/10/19 16:08:22
ERROR : ADDRESS SPACE SERVER CURRENT HEALTH VALUE LESS THAN 100.
ERROR : THIS VALUE MAY IMPACT YOUR SYSTEM OR SYSPLEX TRANSACTION
ERROR : PROCESSING.
ACTION: USE YOUR SOFTWARE MONITORS TO INVESTIGATE THE ASID AND TO
ACTION: DETERMINE THE IMPACT OF THE HEALTH OF THE ADDRESS SPACE TO
ACTION: OVERALL TRANSACTION PROCESSING.
----------------------------------------------------------------

* Medium Severity Exception *

AIRH152E The total system message arrival rate is higher than expected
and may indicate a system problem.

  Explanation:  This check has detected the LPAR or an address space
    could be damaged by checking for an abnormal arrival rate of WTO
    messages per amount of CPU be too high or too low when compared to
    the expected value.

    The model of the total system message arrival rate has detected that
    the arrival rate is higher than expected based on the previous
    history of this system. An unusually high message arrival rate can
    indicate a series of recurring failures on the system which can lead
    to a system hang or may be indicative of a damaged system. The
    message arrival rate is the ratio of the arrivals and the CPU used
    in the last collection interval. The next model will occur at
    10/20/2020 04:11:14. The prediction used in the comparison was
    modeled at 10/19/2020 16:11:14.
```

6 →

```
System Action:  Subsequent runs of this check will not produce an
   operator message until new data is available.

Operator Response:

  1. Examine SECTION 1: MESSAGE ARRIVAL RATE DATA in the report above
  and the details of any address spaces listed. Examine SYSLOG and
  OPERLOG for the identified address spaces to determine whether there
  are problems being recovered.

  2. If provided, examine SECTION 2: RUNTIME DIAGNOSTICS OUTPUT.
  Runtime Diagnostics was invoked for all address spaces whose WLM
  health settings were less than 100. Look for any events that show
  the address spaces are hung or looping. Events for ENQ or GRS LATCH
  could indicate waits that could be contributing to sympathy
  sickness. If there are SERVERHEALTH events, look at their details.
  Perform the ACTION steps in the output.

  3. Check IBM Health Checker for z/OS for other exceptions. See if
  any SVC dumps have been taken recently for existing problems.

  4. If the problem cannot be isolated and local guidelines allow it,
  initiate an SVC dump of the address spaces listed in the report.

  5. To find additional recommendations, consult the z/OS Problem
  Management book, Predictive Failure Analysis checks chapter,
  PFA_MESSAGE_ARRIVAL_RATE subsection, in the 'Best Practices' topic.

  6. If the problem cannot be easily determined in a short amount of
  time and you want to stop all exceptions until the problem can be
  resolved, do one of the following:

    a. Quiesce the check so that data continues to be collected, but
  comparisons are not performed. Quiescing the check allows the check
  to resume processing with no interruption of collected data once the
  check is reactivated. First, ensure the check will collect and model
  data while deactivated by setting COLLECTINACTIVE to 1 and then
  deactivate the check.

    f hzsproc,update,check(IBMPFA,PFA_MESSAGE_ARRIVAL_RATE),
    parm('collectinactive(1)')

    f hzsproc,deactivate,check(IBMPFA,PFA_MESSAGE_ARRIVAL_RATE)
```

```
  b. Change the severity of the exception so that all processing
  continues for this check, but exceptions are not issued by modifying
  the SEVERITY parameter for this check so that all exceptions issued
  by this check use no severity. Use the command below or establish an
  IBM Health Checker for z/OS PARMLIB member to make the change
  persistent:

    f hzsproc,update,check(IBMPFA,PFA_MESSAGE_ARRIVAL_RATE),
    severity(none)

  7. After investigating the problem, if you have determined that the
  exception is normal operating behavior and you do not want to be
  alerted for similar data in the future, perform one or more of the
  following actions:

    a. If this check continues to issue exceptions for address spaces
  whose rates are normal fluctuations and are not an indication of
  damage, add the address spaces to the EXCLUDED_JOBS file. The file
  is found in the pfa_directory/PFA_MESSAGE_ARRIVAL_RATE/config
  directory where 'pfa_directory' is the name of your PFA directory.
  Update the file and then restart PFA to have the changes take
  effect.

    b. Modify this check's STDDEV parameter to the value on the report
  that would have been required to avoid the exception if the value is
  not TOO HIGH or IRRELEVANT. Setting the STDDEV too high might cause
  damaged address spaces to be undetected by this check. Use the
  command below and specify your desired value in place of the X or
  establish an IBM Health Checker for z/OS PARMLIB member to make the
  change persistent:

    f hzsproc,update,check(IBMPFA,PFA_MESSAGE_ARRIVAL_RATE),
    parm('stddev(X)')

    c. If the rate causing the exception was relatively low and you
  want to avoid similar exceptions in the future, consider setting the
  EXCEPTIONMIN parameter to a higher value. For tracked jobs, this
  parameter defines the current minimum rate and the minimum predicted
  rate required to cause an exception for a rate that is too high. For
  the total system comparison, this parameter defines the current
  minimum rate that is required to cause an exception for a rate that
  is too high.

    f hzsproc,update,check(IBMPFA,PFA_MESSAGE_ARRIVAL_RATE),
    parm('exceptionmin(X)')
```

- Enhancements
    1. Shows exception message at top of reports
    2. Reminds you to look at new diagnostic actions in the "Operator Response" section of the message at the bottom of the report.
    3. Has section headings
    4. Includes Runtime Diagnostics for address spaces causing the exception if the WLM health setting < 100.
    5. Includes WLM health setting for address spaces causing exceptions.
    6. Lists recommended actions in the "Operator Response" of the exception message.

- Scenario – A job was running that changed its normal rate.

3 and 4

1

2

3

5

```
* Exception Issued *

The enqueue request rate for one or more tracked, persistent address
spaces is lower than expected and may indicate a system problem.

See the 'Operator Response' section of the exception message below for
recommended actions.

                    Enqueue Request Rate Prediction Report

Last successful model time     :  10/20/2020 13:42:47
Next model time                :  10/21/2020 01:42:47
Model interval                 :  720
Last successful collection time:  10/20/2020 13:44:59
Next collection time           :  10/20/2020 13:45:59
Collection interval            :  1

SECTION 1: ENQUEUE REQUEST RATE DATA

Highest STDDEVLOW needed to avoid this exception:  IRRELEVANT

Persistent address spaces with low rates:

                                        Predicted Enqueue
                   Enqueue                 Request Rate
  Job              Request
  Name    ASID       Rate       1 Hour      24 Hour       7 Day
  _____  ____  _____  _____  _____  _____

  ENRTST1 0028        0.00       18.90        18.90       18.90

Additional details:

                   WLM
  Job              Health
  Name    ASID     Setting
  _____  ____  _____

  ENRTST1 0028       20
```

```
SECTION 2: RUNTIME DIAGNOSTICS OUTPUT FOR TOP PERSISTENT ADDRESS SPACES

Runtime Diagnostics detected a problem in ASID:   0028
EVENT 1: HIGH:SERVERHEALTH      SYSTEM: SY1      2020/10/20 13:45:01
   JOB NAME: ENRTST1   ASID: 0028  CURRENT HEALTH VALUE: 20
   CURRENT LOWEST HEALTH VALUES:
                     SUBSYSTEM    HEALTH                    REPORTED
   SUBSYSTEM   NAME          SETTING          REASON   DATE AND TIME
   HZR         FHBRSENR        20          Set to 20.  2020/10/20 13:16:24
ERROR : ADDRESS SPACE SERVER CURRENT HEALTH VALUE LESS THAN 100.
ERROR : THIS VALUE MAY IMPACT YOUR SYSTEM OR SYSPLEX TRANSACTION
ERROR : PROCESSING.
ACTION: USE YOUR SOFTWARE MONITORS TO INVESTIGATE THE ASID AND TO
ACTION: DETERMINE THE IMPACT OF THE HEALTH OF THE ADDRESS SPACE TO
ACTION: OVERALL TRANSACTION PROCESSING.
-----------------------------------------------------------------

* Medium Severity Exception *

AIRH190E The enqueue request rate for one or more tracked, persistent
address spaces is lower than expected and may indicate a system
problem.

  Explanation:  This check has detected that the LPAR or an address
    space could be damaged by checking for an abnormal number of enqueue
    requests per amount of CPU used. The model of the tracked,
    persistent address spaces when compared to the request rate for each
    is lower than expected based on the previous history of each tracked
    address space. An unusually low enqueue request rate can indicate an
    impending system hang. The enqueue request rate is the ratio of the
    requests and the CPU used in the last collection interval. The next
    model will occur at 10/21/2020 01:42:47. The prediction used in the
    comparison was modeled at 10/20/2020 13:42:47.
```

When PFA detects that the enqueue request rate is lower than expected, PFA calls Runtime Diagnostics to detect if an address space seems hung or otherwise damaged. At least one event must be issued to cause an enqueue request rate too low exception. By detecting these conditions early, you can correct the problem before it causes the system to hang or crash.

System Action: Subsequent runs of this check will not produce an operator message until new data is available.

6

Operator Response:

1. Examine SECTION 1: ENQUEUE REQUEST RATE DATA in the report above and the details of any address spaces listed.

2. If provided, examine SECTION 2: RUNTIME DIAGNOSTICS OUTPUT. Runtime Diagnostics was invoked for all address spaces whose rates were too low. Look for any events that show the address spaces are hung or looping. Events for ENQ or GRS LATCH could indicate waits that could be contributing to sympathy sickness. If there are SERVERHEALTH events, look at their details. Perform the ACTION steps in the output.

3. Investigate the address spaces shown in the EREP report. Consult a performance monitor such as Resource Management Facility (RMF) to look for clues to the problem based on CPU, I/O, CF (internal, external) and storage delays and to seek clues of underlying problems such as additional resource being used for error recovery. Examine specific errors within the context of the delays as they may point out problems related to the identified address spaces. Look for problems reported by key components, like XCF, GRS, Logger, etc., as problems in those areas can affect components that are dependent on them. In addition, examine the joblog of the identified jobs to determine what may be contributing to the problem.

4. If the problem cannot be isolated and local guidelines allow it, initiate an SVC dump of the address spaces listed in the report.

5. To find additional recommendations, consult the z/OS Problem Management book, Predictive Failure Analysis checks chapter, PFA_ENQUEUE_REQUEST_RATE subsection, in the 'Best Practices' topic.

6. If the problem cannot be easily determined in a short amount of time and you want to stop all exceptions until the problem can be resolved, do one of the following:

   a. Quiesce the check so that data continues to be collected, but comparisons are not performed. Quiescing the check allows the check to resume processing with no interruption of collected data once the check is reactivated. First, ensure the check will collect and model data while deactivated by setting COLLECTINACTIVE to 1 and then deactivate the check.

   ```
   f hzsproc,update,check(IBMPFA,PFA_ENQUEUE_REQUEST_RATE),
   parm('collectinactive(1)')
   ```

   ```
   f hzsproc,deactivate,check(IBMPFA,PFA_ENQUEUE_REQUEST_RATE)
   ```

   b. Change the severity of the exception so that all processing continues for this check, but exceptions are not issued by modifying the SEVERITY parameter for this check so that all exceptions issued by this check use no severity. Use the command below or establish an IBM Health Checker for z/OS PARMLIB member to make the change persistent:

   ```
   f hzsproc,update,check(IBMPFA,PFA_ENQUEUE_REQUEST_RATE),
   severity(none)
   ```

   c. Turn off checking for too low until the problem is resolved by issuing the following command. Checking for rates that are too high will continue.

   ```
   f hzsproc,update,check(IBMPFA,PFA_ENQUEUE_REQUEST_RATE),
   parm('checklow(0)')
   ```

```
7. After investigating the problem, if you have determined that the
   exception is normal operating behavior and you do not want to be
   alerted for similar data in the future, perform one or more of the
   following actions:

   a. If this check continues to issue exceptions for address spaces
   whose rates are normal fluctuations and are not an indication of
   damage, add the address spaces to the EXCLUDED_JOBS file. The file
   is found in the pfa_directory/PFA_ENQUEUE_REQUEST_RATE/config
   directory where 'pfa_directory' is the name of your PFA directory.
   Update the file and then restart PFA to have the changes take
   effect.

   b. Modify this check's STDDEVLOW parameter to the value on the
   report that would have been required to avoid the exception if the
   value is not TOO HIGH or IRRELEVANT. Setting the STDDEVLOW too high
   might cause damaged address spaces to be undetected by this check.
   Use the command below and specify your desired value in place of the
   X or establish an IBM Health Checker for z/OS PARMLIB  member to
   make the change persistent:

   f hzsproc,update,check(IBMPFA,PFA_ENQUEUE_REQUEST_RATE),
   parm('stddevlow(X)')

   c. If the rate causing the exception was relatively high and you
   want to avoid similar exceptions in the future, consider setting the
   LIMITLOW parameter to a lower value. This parameter defines the
   maximum rate that is allowed when issuing an exception for an
   unexpectedly low rate. For example, with LIMITLOW(3), the rate must
   be 3 or less in order for an exception for a rate that is too low to
   occur.

   f hzsproc,update,check(IBMPFA,PFA_ENQUEUE_REQUEST_RATE),
   parm('limitlow(X)')
```

- Enhancements
  1. Shows exception message at top of reports
  2. Reminds you to look at new diagnostic actions in the "Operator Response" section of the message at the bottom of the report.
  3. Has section headings
  4. Includes Runtime Diagnostics for address spaces causing the exception if the WLM health setting < 100.
  5. Includes WLM health setting for address spaces causing exceptions.
  6. Lists recommended actions in the "Operator Response" of the exception message.

- Scenario – A problem in a persistent address space.

3 and 4

1

2

3

```
* Exception Issued *

The SMF arrival rate for one or more persistent address spaces is higher
 than expected and may indicate a system problem.

See the 'Operator Response' section of the exception message below for
recommended actions.

                    SMF Arrival Rate Prediction Report

Last successful model time     :  10/16/2020 16:24:04
Next model time                :  10/17/2020 04:24:04
Model interval                 :  720
Last successful collection time:  10/16/2020 16:26:05
Next collection time           :  10/16/2020 16:41:05
Collection interval            :  15

SECTION 1: SMF ARRIVAL RATE DATA

Other persistent jobs group:
SMF arrival rate
   in last collection interval     :          253.70
Prediction based on 1 hour of data  :           61.89
Prediction based on 24 hours of data:           61.89
Prediction based on 7 days of data  :           61.89

Highest STDDEV needed to avoid this exception:  58

Persistent address spaces with high rates:

                        SMF   WLM
  Job               Arrival  Health
  Name     ASID        Rate  Setting
 _____ ____  _____  _____
  OMVS     000F      3425.00      70
```

```
SECTION 2: RUNTIME DIAGNOSTICS OUTPUT FOR JOBS
            WITH WLM HEALTH LESS THAN 100

Runtime Diagnostics detected a problem in ASID:   000F
EVENT 1: HIGH:SERVERHEALTH     SYSTEM: SY1      2020/10/16 16:26:06
  JOB NAME: OMVS      ASID: 000F  CURRENT HEALTH VALUE: 70
  CURRENT LOWEST HEALTH VALUES:
             SUBSYSTEM   HEALTH                    REPORTED
  SUBSYSTEM  NAME        SETTING          REASON   DATE AND TIME
  HZR        FHBRSSAR        70         Set to 50.  2020/10/16 16:24:30
ERROR : ADDRESS SPACE SERVER CURRENT HEALTH VALUE LESS THAN 100.
ERROR : THIS VALUE MAY IMPACT YOUR SYSTEM OR SYSPLEX TRANSACTION
ERROR : PROCESSING.
ACTION: USE YOUR SOFTWARE MONITORS TO INVESTIGATE THE ASID AND TO
ACTION: DETERMINE THE IMPACT OF THE HEALTH OF THE ADDRESS SPACE TO
ACTION: OVERALL TRANSACTION PROCESSING.
-----------------------------------------------------------------------

* Medium Severity Exception *

AIRH188E The SMF arrival rate for one or more persistent address
spaces is higher than expected and may indicate a system problem.

  Explanation:  This check has detected the LPAR or an address space
    could be damaged by checking for an abnormal SMF arrival rate per
    amount of CPU used in the last collection interval. PFA examines
    only the SMF record types you set to generate in the SMFPRMxx
    PARMLIB member. When the number of SMF records written per amount of
    CPU used is unusually high or low, PFA can provide an early
    indication of a problem and potentially prevent damage to an LPAR.

    For the persistent address spaces that are not being tracked
    individually, the model of the persistent address spaces when
    compared to the average arrival rate for the group is higher than
    expected. An unusually high SMF arrival rate can indicate a series
    of recurring failures for the address space which can lead to a
    system hang or may be indicative of a damaged system. The SMF
    arrival rate is the ratio of the arrivals and the CPU used in the
    last collection interval. The next model will occur at 10/17/2020
    04:24:04. The predictions used in the comparison were modeled at
    10/16/2020 16:24:04.
```

When an unexpectedly high number of SMF records is detected, the best practice is to review the SMF records being sent by the address spaces identified on the report and examine the system log to determine what is causing the increase in SMF activity.

System Action: Subsequent runs of this check will not produce an operator message until new data is available.

6 →

Operator Response:

1. Examine SECTION 1:SMF ARRIVAL RATE DATA in the report above and the details of any address spaces listed.

2. Consult a performance monitor such as Resource Management Facility (RMF) to look for clues to the problem based on CPU, I/O, CF (internal, external) and storage delays and to seek clues of underlying problems such as additional resource being used for error recovery. Examine specific errors within the context of the delays as they may point out problems related to the identified address spaces. Look for jobs using a very significant amount of I/O and CPU resource.

3. If provided, examine SECTION 2: RUNTIME DIAGNOSTICS OUTPUT. Runtime Diagnostics was invoked for all address spaces whose WLM health settings were less than 100. Look for any events that show the address spaces are hung or looping. Events for ENQ or GRS LATCH could indicate waits that could be contributing to sympathy sickness. If there are SERVERHEALTH events, look at their details. Perform the ACTION steps in the output.

4. If the problem cannot be isolated and local guidelines allow it, initiate an SVC dump of the address spaces listed in the report.

5. To find additional recommendations, consult the z/OS Problem Management book, Predictive Failure Analysis checks chapter, PFA_SMF_ARRIVAL_RATE subsection, in the 'Best Practices' topic.

6. If the problem cannot be easily determined in a short amount of time and you want to stop all exceptions until the problem can be resolved, do one of the following:

   a. Quiesce the check so that data continues to be collected, but comparisons are not performed. Quiescing the check allows the check to resume processing with no interruption of collected data once the check is reactivated. First, ensure the check will collect and model data while deactivated by setting COLLECTINACTIVE to 1 and then deactivate the check.

   f hzsproc,update,check(IBMPFA,PFA_SMF_ARRIVAL_RATE), parm('collectinactive(1)')

   f hzsproc,deactivate,check(IBMPFA,PFA_SMF_ARRIVAL_RATE)

   b. Change the severity of the exception so that all processing continues for this check, but exceptions are not issued by modifying the SEVERITY parameter for this check so that all exceptions issued by this check use no severity. Use the command below or establish an IBM Health Checker for z/OS PARMLIB member to make the change persistent:

   f hzsproc,update,check(IBMPFA,PFA_SMF_ARRIVAL_RATE), severity(none)

7. After investigating the problem, if you have determined that the exception is normal operating behavior and you do not want to be alerted for similar data in the future, perform one or more of the following actions:

   a. If this check continues to issue exceptions for address spaces whose rates are normal fluctuations and are not an indication of damage, add the address spaces to the EXCLUDED_JOBS file. The file is found in the pfa_directory/PFA_SMF_ARRIVAL_RATE/config directory where 'pfa_directory' is the name of your PFA directory. Update the file and then restart PFA to have the changes take effect.

```
    b. Modify this check's STDDEV parameter to the value on the report
that would have been required to avoid the exception if the value is
not TOO HIGH or IRRELEVANT. Setting the STDDEV too high might cause
damaged address spaces to be undetected by this check. Use the
command below and specify your desired value in place of the X or
establish an IBM Health Checker for z/OS PARMLIB member to make the
change persistent:

    f hzsproc,update,check(IBMPFA,PFA_SMF_ARRIVAL_RATE),
    parm('stddev(X)')

    c. If the rate causing the exception was relatively low and you
want to avoid similar exceptions in the future, consider setting the
EXCEPTIONMIN parameter to a higher value. For tracked jobs, this
parameter defines the current minimum rate and the minimum predicted
rate required to cause an exception for a rate that is too high. For
the total system comparison, this parameter defines the current
minimum rate that is required to cause an exception for a rate that
is too high.

    f hzsproc,update,check(IBMPFA,PFA_SMF_ARRIVAL_RATE),
    parm('exceptionmin(X)')
```

- Enhancements
    1. Shows exception message at top of reports
    2. Reminds you to look at new diagnostic actions in the "Operator Response" section of the message at the bottom of the report.
    3. Has section headings
    4. Includes Runtime Diagnostics for address spaces causing the exception if the WLM health setting < 100.
    5. Includes WLM health setting for address spaces causing exceptions.
    6. Lists recommended actions in the "Operator Response" of the exception message.

- Scenario – A job was running that abnormally increased its usage of track groups.

3 and 4

1

2

3

5

```
* Exception Issued *

The change in JES spool usage by one or more persistent address spaces
is higher than expected.

See the 'Operator Response' section of the exception message below for
recommended actions.

                    JES Spool Usage Prediction Report

Last successful model time      :  10/19/2020 11:18:48
Next model time                 :  10/19/2020 23:18:48
Model interval                  :  720
Last successful collection time:  10/19/2020 11:20:50
Next collection time            :  10/19/2020 11:25:50
Collection interval             :  5


Highest STDDEV needed to avoid this exception:  12

SECTION 1: JES SPOOL USAGE DATA

Address spaces causing exception:

                  Current Change in   Expected Change in         Current
  Job               Number of Track     Number of Track    Number of Track
  Name     ASID        Groups Used          Groups Used        Groups Used
 _____  ____    _____     _____    _____
  JESPOLE  002A                 12                   1                 53

Additional details:

                  WLM
  Job            Health
  Name     ASID  Setting

 _____  ____  _____
  JESPOLE  002A       70
```

```
SECTION 2: RUNTIME DIAGNOSTICS OUTPUT FOR JOBS
            WITH WLM HEALTH LESS THAN 100

Runtime Diagnostics detected a problem in ASID:    002A
EVENT 1: HIGH:SERVERHEALTH     SYSTEM: SY1     2020/10/19 11:18:49
   JOB NAME: JESPOLE   ASID: 002A  CURRENT HEALTH VALUE: 70
   CURRENT LOWEST HEALTH VALUES:
              SUBSYSTEM   HEALTH                 REPORTED
   SUBSYSTEM  NAME        SETTING        REASON  DATE AND TIME
   HZR        FHBRSSAR        70         Set to 70.  2020/10/19 10:44:55
ERROR : ADDRESS SPACE SERVER CURRENT HEALTH VALUE LESS THAN 100.
ERROR : THIS VALUE MAY IMPACT YOUR SYSTEM OR SYSPLEX TRANSACTION
ERROR : PROCESSING.
ACTION: USE YOUR SOFTWARE MONITORS TO INVESTIGATE THE ASID AND TO
ACTION: DETERMINE THE IMPACT OF THE HEALTH OF THE ADDRESS SPACE TO
ACTION: OVERALL TRANSACTION PROCESSING.
---------------------------------------------------------------------

* Medium Severity Exception *

AIRH198E The change in JES spool usage by one or more persistent
address spaces is higher than expected.

  Explanation:  PFA uses the metric of the amount of JES spool usage
    (i.e., track groups) to determine if an address space is behaving
    abnormally based on the previous behavior for the address space. If
    a job's spool usage is higher than expected, this can indicate a
    damaged address space. The change in JES spool usage is higher than
    expected when compared to the model of the expected change in JES
    spool usage for one or more persistent address spaces. The next
    model will occur at 10/19/2020 23:18:48. The expected change used in
    the comparison was modeled at 10/19/2020 11:18:48.

  System Action:  Subsequent runs of this check will not produce an
    operator message until new data is available.
```

6

```
Operator Response:

  1. Examine the address spaces in SECTION 1: JES SPOOL USAGE DATA and
  investigate if they are behaving abnormally. The best practice is to
  inspect the job log and other files written to the JES spool. To fix
  the problem, recycle the job.

  2. If provided, examine SECTION 2: RUNTIME DIAGNOSTICS OUTPUT FOR
  WLM HEALTH SETTINGS < 100. Runtime Diagnostics was invoked for all
  address spaces causing the exception whose WLM health settings were
  less than 100. Look at the details for those events and perform the
  ACTION steps in the output.

  3. For other address spaces, if desired, invoke Runtime Diagnostics
  using F HZR,ANALYZE and examine the output for contention issues and
  other anomaly contributors that may result in increasing JES2 spool
  usage.

  4. To find additional recommendations, consult the z/OS Problem
  Management book, Predictive Failure Analysis checks chapter,
  PFA_JES_SPOOL_USAGE subsection, in the 'Best Practices' topic.

  5. If the problem cannot be easily determined in a short amount of
  time and you want to stop all exceptions until the problem can be
  resolved, do one of the following:

    a. Quiesce the check so that data continues to be collected, but
  comparisons are not performed. Quiescing the check allows the check
  to resume processing with no interruption of collected data once the
  check is reactivated. First, ensure the check will collect and model
  data while deactivated by setting COLLECTINACTIVE to 1 and then
  deactivate the check.

    f hzsproc,update,check(IBMPFA,PFA_JES_SPOOL_USAGE),
    parm('collectinactive(1)')

    f hzsproc,deactivate,check(IBMPFA,PFA_JES_SPOOL_USAGE)

    b. Change the severity of the exception so that all processing
  continues for this check, but exceptions are not issued by modifying
  the SEVERITY parameter for this check so that all exceptions issued
  by this check use no severity. Use the command below or establish an
  IBM Health Checker for z/OS PARMLIB member to make the change
  persistent:

    f hzsproc,update,check(IBMPFA,PFA_JES_SPOOL_USAGE),
    severity(none)
```

```
  6. After investigating the problem, if you have determined that the
  exception is normal operating behavior and you do not want to be
  alerted for similar data in the future, perform one or more of the
  following actions:

    a. If you have a CICS workload and the CICS jobs are causing the
  exception, consider adding CICS* or your job prefix if using a
  different prefix to the JES spool usage EXCLUDED_JOBS file. The file
  is found in the pfa_directory/PFA_JES_SPOOL_USAGE/config directory
  where 'pfa_directory' is the name of your PFA directory. Update the
  file and then force PFA to read the file by issuing the following
  command:

    f pfa,update,check(PFA_JES_SPOOL_USAGE),EXCLUDED_JOBS

    b. If this check continues to issue exceptions for address spaces
  whose usage of track groups is normal and not an indication of
  damage, add the address spaces to the EXCLUDED_JOBS file and force
  PFA to read the file as described in the previous step.

    c. Modify this check's STDDEV parameter to the value on the report
  that would have been required to avoid the exception if the value is
  not TOO HIGH or IRRELEVANT. Setting the STDDEV too high might cause
  damaged address spaces to be undetected by this check. Use the
  command below and specify your desired value in place of the X or
  establish an IBM Health Checker for z/OS PARMLIB member to make the
  change persistent:

    f hzsproc,update,check(IBMPFA,PFA_JES_SPOOL_USAGE),
    parm('stddev(X)')


    d. If the amount of spool usage was relatively small, consider
  setting the EXCEPTIONMIN to a higher value. This parameter defines
  the minimum number of track groups required by an address space to
  cause an exception.

    f hzsproc,update,check(IBMPFA,PFA_JES_SPOOL_USAGE),
    parm('exceptionmin(X)')
```

- Enhancements
  1. Shows exception message at top of reports
  2. Reminds you to look at new diagnostic actions in the "Operator Response" section of the message at the bottom of the report.
  3. Has section headings
  4. Includes Runtime Diagnostics for address spaces having logrecs in the last collection interval if the WLM health setting < 100.
  5. Includes WLM health setting for address spaces causing exceptions.
  6. Lists recommended actions in the "Operator Response" of the exception message.

- Scenario – A job was running that increased its rate.

1

2

3

```
* Exception Issued *

The LOGREC entry arrival rate is higher than expected and may indicate a
system problem.

See the 'Operator Response' section of the exception message below for
recommended actions.

                    LOGREC Arrival Rate Prediction Report

Last successful model time     :  10/23/2020 10:41:22
Next model time                :  10/23/2020 22:41:22
Model interval                 :  720
Last successful collection time:  10/23/2020 10:47:04
Next collection time           :  10/23/2020 11:47:04
Collection interval            :  60

SECTION 1: LOGREC ARRIVAL RATE DATA

                          Key 0        Key 1-7       Key 8-15
                       _____   _____   _____
Arrivals in last
   collection interval:     57            0             0
Predicted rates based on...
     1 hour of data:         5            0             0
    24 hours of data:        0            0             0
     7 days of data:         0            0             0
    30 days of data:         0            0             0

Highest STDDEV needed to avoid this exception:  12

Jobs having LOGREC arrivals in last collection interval:

                            WLM
                            Health
   Job Name  ASID  Arrivals  Setting
   _____  ____  _____  _____
   LOGREC00  002E       57      100
```

5

6

```
* Medium Severity Exception *

AIRH110E The LOGREC entry arrival rate is higher than expected
and may indicate a system problem.

  Explanation:  This check is looking at the arrival frequency of
     selected software LOGREC entries. The model of the LOGREC entry
     arrival rate has detected that the arrival rate is higher than
     expected based on the previous history of this system. An unusually
     high LOGREC entry rate can indicate a series of recurring failures
     on the system which can lead to a system hang or may be indicative
     of a damaged system. The next model will occur at 10/23/2020
     22:41:22. The prediction used in the comparison was modeled at
     10/23/2020 10:41:22. Note: When this check triggers an exception,
     it's very likely that you have an underlying problem.

  System Action:  Subsequent runs of this check will not produce an
     operator message until new data is available.

Operator Response:

   1. Examine the address spaces in SECTION 1: LOGREC ARRIVAL RATE DATA
   and investigate if they are behaving abnormally. Look for problems
   recorded in EREP by using the EREP summary report. If you find
   suspicious records, run an EREP detail report for the shorter time
   range.

   2. Investigate the address spaces shown in the EREP report. Consult
   a performance monitor such as Resource Management Facility (RMF) to
   look for clues to the problem based on CPU, I/O, CF (internal,
   external) and storage delays and to seek clues of underlying
   problems such as additional resource being used for error recovery.
   Examine specific errors within the context of the delays as they may
   point out problems related to the identified address spaces.

   3. If the problem cannot be isolated and local guidelines allow it,
   initiate an SVC dump of the address spaces listed in the report.
```

4. If provided, examine SECTION 2: RUNTIME DIAGNOSTICS OUTPUT FOR WLM HEALTH SETTINGS < 100. Runtime Diagnostics was invoked for all address spaces that had LOGREC entries in the last collection interval whose WLM health settings were less than 100. Look at the details for those events and perform the ACTION steps in the output.

5. To find additional recommendations, consult the z/OS Problem Management book, Predictive Failure Analysis checks chapter, PFA_LOGREC_ARRIVAL_RATE subsection, in the 'Best Practices' topic.

6. If the problem cannot be easily determined in a short amount of time and you want to stop all exceptions until the problem can be resolved, do one of the following:

  a. Quiesce the check so that data continues to be collected, but comparisons are not performed. Quiescing the check allows the check to resume processing with no interruption of collected data once the check is reactivated. First, ensure the check will collect and model data while deactivated by setting COLLECTINACTIVE to 1 and then deactivate the check.

```
f hzsproc,update,check(IBMPFA,PFA_LOGREC_ARRIVAL_RATE),
parm('collectinactive(1)')

f hzsproc,deactivate,check(IBMPFA,PFA_LOGREC_ARRIVAL_RATE)
```

  b. Change the severity of the exception so that all processing continues for this check, but exceptions are not issued by modifying the SEVERITY parameter for this check so that all exceptions issued by this check use no severity. Use the command below or establish an IBM Health Checker for z/OS PARMLIB member to make the change persistent:

```
f hzsproc,update,check(IBMPFA,PFA_LOGREC_ARRIVAL_RATE),
severity(none)
```

7. After investigating the problem, if you have determined that the exception is normal operating behavior and you do not want to be alerted for similar data in the future, perform one or more of the following actions:

  a. If this check continues to issue exceptions for address spaces that intermittently issue LOGREC entries and is not an indication of damage, add the address spaces to the EXCLUDED_JOBS file. The file is found in the pfa_directory/PFA_LOGREC_ARRIVAL_RATE/config directory where 'pfa_directory' is the name of your PFA directory. Update the file and then force PFA to read the file by issuing the following command:

```
f pfa,update,check(PFA_LOGREC_ARRIVAL_RATE),EXCLUDED_JOBS
```

  b. Modify this check's STDDEV parameter to the value on the report that would have been required to avoid the exception if the value is not TOO HIGH or IRRELEVANT. Setting the STDDEV too high might cause damaged address spaces to be undetected by this check. Use the command below and specify your desired value in place of the X or establish an IBM Health Checker for z/OS PARMLIB member to make the change persistent:

```
f hzsproc,update,check(IBMPFA,PFA_LOGREC_ARRIVAL_RATE),
parm('stddev(X)')
```

  c. If the number of LOGREC entries was relatively small, consider setting the EXCEPTIONMIN to a higher value. This parameter defines the minimum LOGREC arrival rate and the minimum predicted LOGREC arrival rate required to cause an exception.

```
f hzsproc,update,check(IBMPFA,PFA_LOGREC_ARRIVAL_RATE),
parm('exceptionmin(X)')
```

Other checks' reports

- Reports with the enhancements are shown and described in other T3 presentations for the following checks and aren't duplicated here:
  - PFA_JES2_RESOURCE_EXHAUSTION
    - IEAV2R5 PFA JES2 Resource Exhaustion.pptx
  - PFA_PRIVATE_STORAGE_EXHAUSTION
    - IEAV2R5 PFA Private Storage Exhaustion Above Bar.pptx
  - PFA_WLM_ADDR_SPACE_VELOCITY
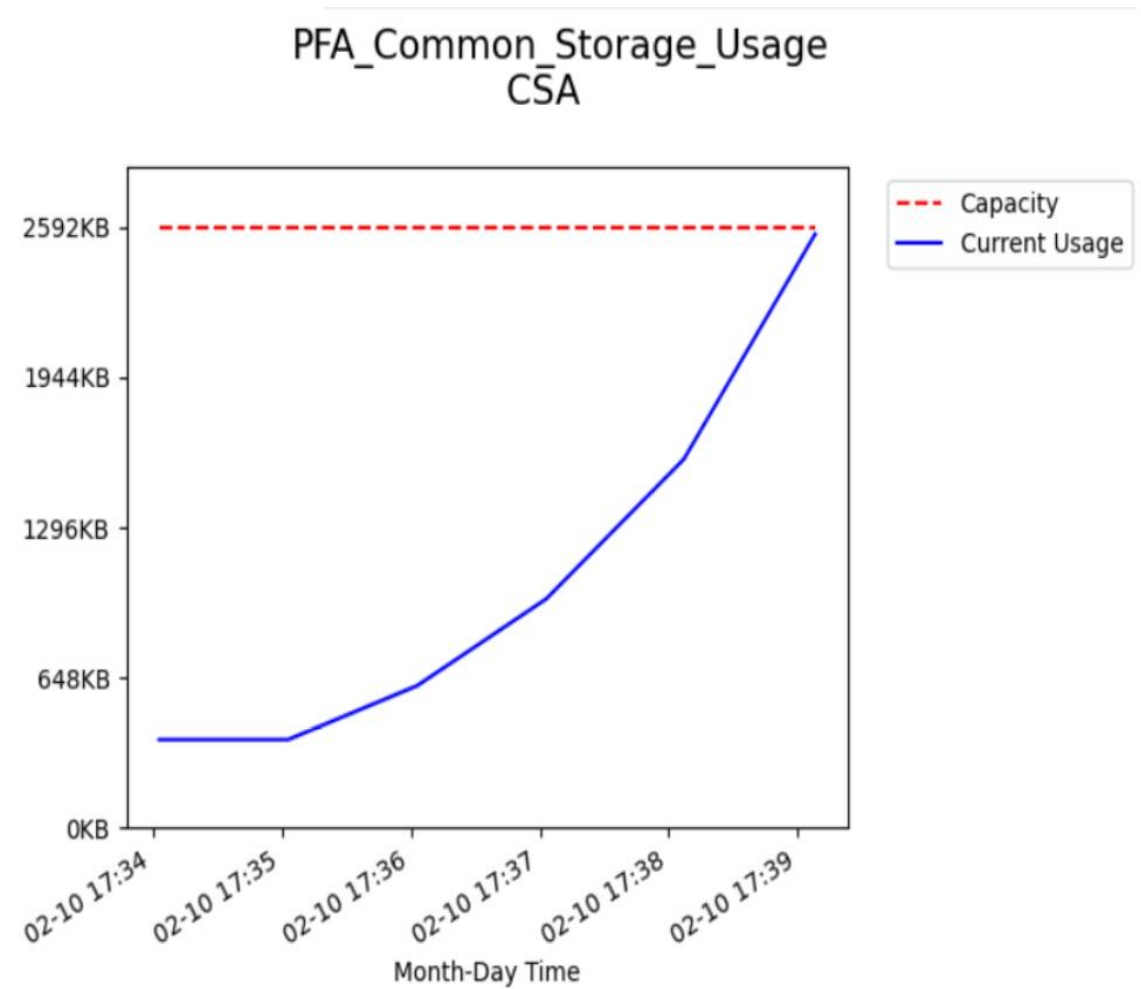   - IEAV2R5 PFA WLM Addr Space Velocity.pptx

- PFA stores collected data in USS files.

- When an exception occurs, PFA copies the files required by PFA development to deeply analyze the exception into */pfadir*/PFA_*checkname*/EXC_*timestamp*

- Some of the files copied can be graphed to help pinpoint when the exception started.

- The graph at the right shows a common storage usage example.

- Notice the storage location- CSA. Other valid locations are SQA, ESQA, and ECSA.

- Combinations of CSA+SQA and ECSA+ESQA are also allowed.

PFA_Common_Storage_Usage
CSA

- The graph at the right shows a private storage exhaustion example.

- Notice the Jobname (WATSON), the ASID (1914), and the storage key (ABOVE – meaning "above the line").

PFA Private Storage Exhaustion Check
WATSON/1914 ABOVE
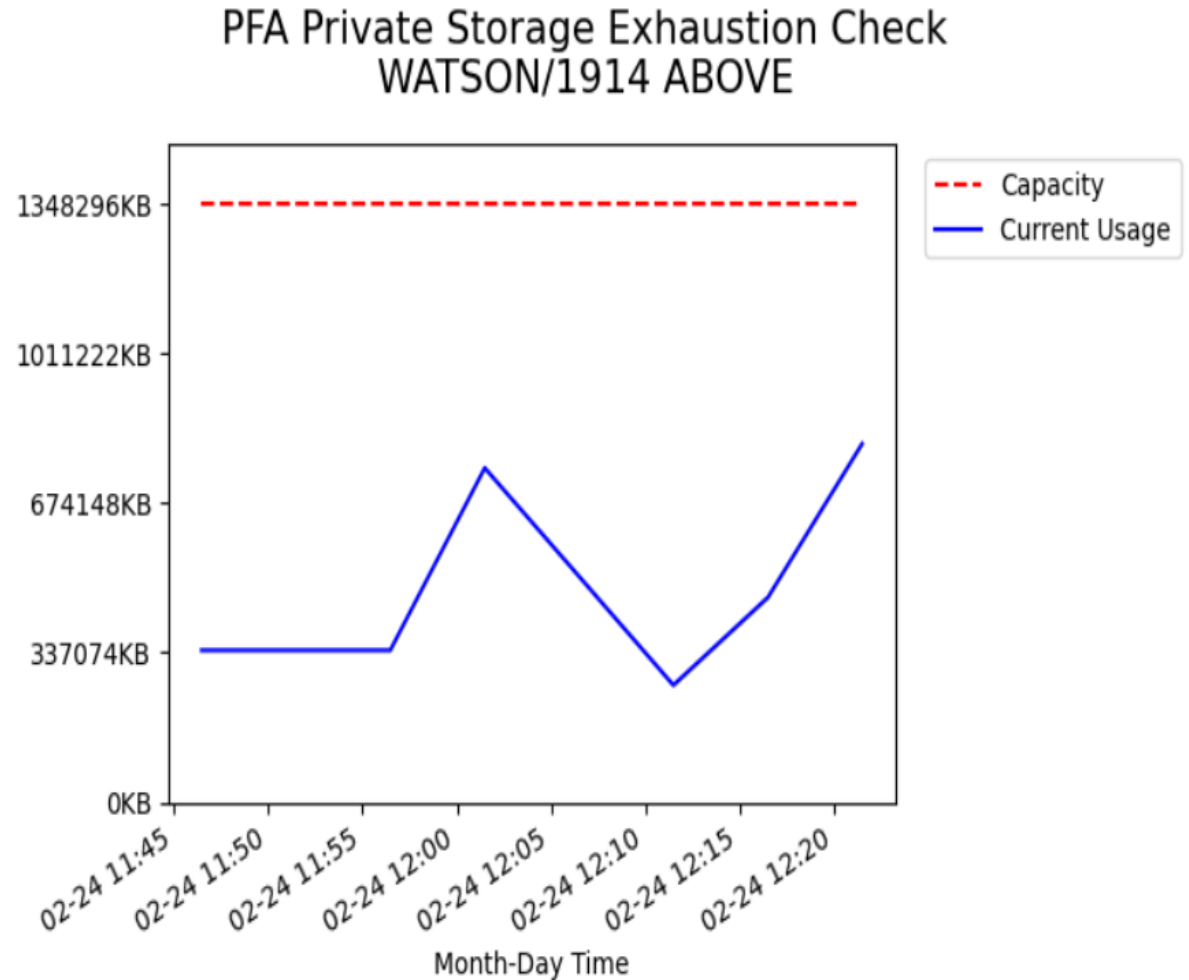
Graphing the PFA Exhaustion Checks – 4 of 6

- Five python scripts for graphing data
  - PFA_PRIVATE_STORAGE_EXHAUSTION: One for address space data
  - PFA_COMMON_STORAGE_USAGE: One for system-wide data and one for address space data
  - PFA_JES2_RESOURCE_EXHAUSTION: One for JES2 system-wide data and one for address space data
- All scripts will be invoked from the command line with command line arguments
- Each script will also have the following options:
  - The –h or help option will explain how to invoke the program for the specific check and the valid key entries that are required.
    - python *script_name.py* -h
  - The –v or verbose option will print additional data to the screen to help verify the results you see in the graph or to debug any problems you may experience.
    - Add –v to the end of any script invocation

- PFA_PRIVATE_STORAGE_EXHAUSTION
  - Uses the *systemName*.data file
  - Script name: Graph_PSE_Data.py
  - Syntax: python Graph_PSE_Data.py *systemName*.data *jobname asid key*
    - Where *jobname* and *asid* are a job and ASID found on the prediction report and *key* is the storage location as shown on the prediction report
- PFA_COMMON_STORAGE_USAGE
  - System-wide storage:
    - Uses the *systemName.*5day.data file and the *systemName.*capacity file
    - Script name: Graph_CSU_Data.py
    - Syntax: python Graph_CSU_Data.py *systemName.*5day.data *systemName.*capacity *key*
      - Where *key* is the storage location as shown on the prediction report
  - Address spaces with the highest increased usage:
    - Uses the *systemName.*5day.All.data file and the *systemName.*capacity file
    - Script name: Graph_CSU_Asid.py
    - Syntax: python Graph_CSU_Asid.py *systemName.*5day.data *systemName.*capacity *jobname asid key*
      - Where *jobname* and *asid* are a job and ASID found on the prediction report and *key* is the storage location as shown on the prediction report

- PFA_JES2_RESOURCE_EXHAUSTION
  - System-wide storage:
    - Uses the *systemName.*5day.data file and the *systemName.*capacity file
    - Script name: Graph_JRE_Data.py
    - Syntax: python Graph_JRE_Data.py *systemName.*5day.data *systemName.*capacity *key*
      - Where *key* is JES2 resource as shown on the prediction report
  - Address spaces with the highest increased usage:
    - Uses the *systemName.*5day.All.data file and the *systemName.*capacity file
    - Script name: Graph_JRE_Job.py
    - Syntax: python Graph_JRE_Job.py *systemName.*5day.All.data *systemName.*capacity *jobname asid key*
    - Where *jobname* and *asid* are a job and ASID found on the prediction report and *key* is the JES2 resource as shown on the prediction report

Interactions & Dependencies

- Software Dependencies
  - None

- Hardware Dependencies
  - None

- Exploiters
  - None

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Sysplex must be at the new z/OS level: No

- List any toleration/coexistence APARs/PTFs: None

Installation & Configuration

- Nothing new.
  - All checks are automatically added to IBM Health Checker for z/OS when PFA starts.
  - If you have not previously used PFA, see the chapter entitled *Predictive Failure Analysis overview and installation* in *z/OS Problem Management* (also listed in the Appendix of this presentation).

Summary

- Predictive Failure Analysis (PFA) has enhanced all checks to provide assistance in quickly identifying anomalous behavior to enable recovery and to improve decision-making regarding recovery steps so that your systems can be recovered quickly and accurately.

Appendix

- *z/OS Problem Management* SC23-6844