The Policy Management Agent – PAGENT Inspector

The need for PAGENT Inspection is based on this simple premise:

Construction mistakes in the configuration of AT-TLS, Intrusion Detection, Policy Based Routing, IPSecurity and Quality of Service rules can degrade z/OS System Integrity!

Therefore, it should be considered true that z/OS System Integrity is enriched by any ongoing process that is constantly vigilant for such mistakes and configuration changes. PAGENT Inspection reports its findings via Image FOCUS, Health Checker and Interval Reports, optionally capturing Real-Time Backups and Changes that are easily useable as Configuration Restore Points.

Getting Started with PAGENT Inspection
A Member of the TCP/IP Family of Inspectors

Available in ICE 16.0

NewEra Software Technical Support
800-421-5035 or 408-520-7100
Or text support requests to 669-888-5061
support@newera.com

www.newera.com

Rev: 2019-07-03

1 Table of Contents

2 The PAGENT and DAEMON Inspectors

The PAGENT and DAEMON Inspectors are an integral part of the Integrity Controls Environment (ICE) family of TCP/IP Inspectors – Resolver, Profile, Data, FTP, TN3270, OMP Route and SMTP. This section will help you identify what is needed to set up the Inspectors and define to The Control Editor in order to get started quickly.

Note:

If you are licensed for the Supplemental Inspectors, you are licensed to use these Inspectors. If not, contact NewEra Technical Support support@newera.com for an Evaluation Key.

2.1 Before You Start

If you are not an Image FOCUS and a Control Editor user, you will need to contact NewEra Technical Support, support@newera.com, and arrange for download links and license keys for both. Once they are installed and operational, you are ready to proceed.

Because the PAGENT and DAEMON Inspectors enforce the same level of security you place over their configurations, you will need to have UPDATE access to their various configuration files. Using this permitted access, you will next need to define certain inspector specific controls discussed later in this document.

Finally, only TCE Administrators, may run or gain access to these Inspectors. If you are not a TCE Administrator contact the current Administrator to discuss your need to run the Inspectors and how you might gain access to them.

Note:

As used within this document, the word “File/file” should be taken to mean both MVS Datasets and UNIX Files as these Inspectors fully support both.

2.2 Setting up the Inspectors

There are a few things you need to know about your environment before you get started. First, if you want to set them up, you will need to figure out how PAGENT and the DAEMONS, if you want to set them up, are started. Once you have this information, update the additional COMMNDxx member used during a Workbench inspection with the appropriate START command. These entries would likely appear as follows:

```
COM='S DMD'
COM='S IKED'
COM='S NSSD'
COM='S PAGENT'
COM='S TN3270'
COM='S TCPIP'
```

Next, you will need to make certain that a copy of the PAGENT and the DAEMON PROCs are in PROCLIB. The standard IBM PROC used to start the PAGENT TASK appears in part as follows:

```
//PAGENT   PROC
//*
//* IBM Communications Server for z/OS
//* SMP/E distribution name: EZAPAGSP
//*
//* 5650-ZOS Copyright IBM Corp. 1998, 2013
//* Licensed Materials - Property of IBM
//* "Restricted Materials of IBM"
//* Status = CSV2R1
```

Now, scroll down in each PROC and find the first uncommented "//STDENV DD PATH=" control card. A sample from the NSSD PROC is shown below:

```
//STDENV DD PATH='/u/paul/samples/nssd.env',PATHOPTS=(ORDONLY)
```

Make a note of the fully qualified file name. You will need this name when setting up the Component Inspector to run from a "Configuration File".

If you intend to run the Component Inspector from an "Environmental File", the the configuration file points to it. The example shown below is from a PAGENT PROC.

```
PAGENT_CONFIG_FILE=/u/paul/pagent.config
PAGENT_LOG_FILE=SYSLOGD
LIBPATH=/usr/lib
TZ=EST5EDT
```

Scroll down in the configuration file and find the first uncommented "_CONFIG_FILE=" control card. Make a note of the fully qualified file name. You will need this name when setting up the Component Inspector to run from an "Environmental File".

Note:

The Component Inspector will determine which file type is used, Environmental or Configuration and automatically adjust its discovery process to accommodate either.

2.3 *Initial Operational State*

The PAGENT Inspector is included in the Integrity Controls Environment (ICE) download with an initial operational state of "OFF". In order to make it fully functional, you will need to add the following control statements to the PAGENT Configuration File as comments and then turn them "ON" as needed.

2.3.1 PAGENT Inspectors Control Statements

The following Control Statements are used to Activate/Deactivate the functions for the Inspectors. They MUST appear as "Commented Lines" in BOTH the PAGENT and DEAMON Configuration files. By default, all functions are "OFF".

```
# *NEWERA*PAGENT_INSPECT=OFF # ON|OFF - DEFAULT OFF - PAGENT INSPECTION
# *NEWERA*CHKREF_PROCESS=ON  # ON|OFF - DEFAULT ON - VALIDATE REFERENCE
# *NEWERA*SOURCE_DISPLAY=ON  # ON|OFF - DEFAULT ON - SHOW SOURCE IN REPORT
# *NEWERA*RESULT_DISPLAY=ON  # ON|OFF - DEFAULT ON - SHOW DETAIL IN REPORT
# *NEWERA*HLTCHK_PROCESS=ON  # ON|OFF - DEFAULT OFF- ENABLE AS HEALTH CHECK
# *NEWERA*NOTICE_PROCESS=OFF # ON|OFF - DEFAULT OFF- ENABLE EMAIL NOTICES
# *NEWERA*BASELN_PROCESS=ON  # ON|OFF,FIXED|MOVING - DEFAULT OFF,MOVING
```

Take Note:

The PAGENT or DAEMON JCL may point to a Configuration or to an Environmental file, which in turn points to the Configuration file. In either case, the Configuration file is the final controlling entity and therefore these Control Statements must appear in it and not the Environmental file.

2.3.2 Turning an Inspector ON

To Activate one or more of the Inspectors, add this commented line to their respective Configuration file.

```
*NEWERA*PAGENT_INSPECT=ON
```

To Activate any other function, add it to the PAGENT or DAEMON source Configuration file.

2.4 *Setting up The Control Editor*

The PAGENT and DEAMON Inspectors are tightly bound to The Control Editor in order to ensure adherence to "Best Practices" in the support of their individual configuration files.

2.4.1 The Control Category

The Control Category is the primary controlling element of The Control Editor. In order to enable the Inspectors to take full advantage of the Integrity Controls Environment (ICE), you will need to define a Category within the ICE NSECTLxx Parmlib Member that encompasses a full set of PAGENT and DAEMON Configuration files. All files for all TCP/IP Images may be defined in a single Category or Multiple Categories may be defined for each individual TCP/IP Image. Here are some Category Examples:

2.4.1 Category Examples

```
CATEGORY PAGENT.CONFIGS
PATH '/u/ice/samples'
FILE '/pagent_ImageMain.config'
PATH '/u/ice'
FILE '/samples/pagent_TTLS.conf'
PATH '/u/ice'
FILE '/samples/pagent_IDS.conf'
PATH '/u/ice'
FILE '/samples/pagent_IPSec.conf'
PATH '/u/ice'
FILE '/samples/pagent_Routing.conf'
PATH '/u/ice'
FILE '/samples/pagent_image_tcpip1.conf'
PATH '/u/ice'
FILE '/pagent_qos_tcpip1.config'
PATH '/u/ice'
FILE '/samples/pagent_image_tcpip2.conf'
PATH '/u/ice'
FILE '/pagent_qos_tcpip2.config'
CATEGORY .END

CATEGORY PAGENT.CONFIGS
DSN PAGENT.MAIN.CONFIG
DSN PAGENT.COMMON.TTLS.CONFIG
DSN PAGENT.COMMON.IDS.CONFIG
DSN PAGENT.COMMON.IPSEC.CONFIG
DSN PAGENT.COMMON.ROUTING.CONFIG
DSN PAGENT.TCPIP1.CONFIG
DSN PAGENT.TCPIP1.QOS.CONFIG
DSN PAGENT.TCPIP2.CONFIG
DSN PAGENT.TCPIP2.QOS.CONFIG
CATEGORY .END
```

3 Configuration Management

Excellence in Configuration Management is defined by adherence to "Best Practices". The bedrock of these practices is to always:

- Make a Backup BEFORE you make a change
- Test your change BEFORE you Commit it to Production
- Maintain an Inventory of Configuration Versions
- Have a Known, Accessible Restore Point
- Compare Restore Point before you Restore to Production
- Document the Authority for a Reason for your Change
- Monitor for Unauthorized Changes
- Review Configuration Reports at Regular Intervals

The integration of Image FOCUS and The Control Editor supports these "Best Practices".

3.1 Best Practice in Action

As documented in the section titled "Component Inspector", these Inspectors provide a panel access interface that will allow you to call The Control Editor controlled configuration management functions directly. The functions of this interface are presented in its Help Panel (PFK1) which is shown below.

```
PAGENT 0501      ICE 16.0 - Image Inspection Summary - TCPIP1

-Overview- ----------------------Description----------------------
           Panel shows a summary of Inspection and Change Detection
           results for named TCP/IP Image. Access them via command.
-Sources-- S - If the target DS/File is Control Editor managed, its
           content will be displayed in a TCE Edit Window.
           L - If a TCE Managed Environment command will build/show
           a worksheet of available Versions/Restore Points.
           B - Displays the current baseline DS/File in View Mode.
           Does not allow the editing of the Baseline.
-Findings- S - Shows the full Inspection of each major Statement
           and any related/defined Keywords.
           F - Presents only those major Statements that contain
           Errors, Warnings or Notices.
           C - When Baseline changes are detected, will display the
           change detail. Baseline not updated by execution.
           R - Displays report that summarizes the major elements.
 -CmmdLine-SKIP:Ends processing, shows report, returns to Menu.
           DETC:Shows the Interval Detector Primary Menu.
           PRNT:Used with 'S/B/F/C/R' to PRINT a Selection.
           COPY:Used with 'S/B/F/C/R' to COPY a selection.
           HCKR:Setup HealthChecker Notification and Audit Logging.
```

3.1.1 Configuration Access

Depending on the authority permitted to you, this function will display the select configuration file in TCE/Edit providing all of the inherent Edit Services.

3.1.2 Configuration Versions

As backups are taken and changes are made, versions of these configuration files are recorded in the TCE Control Journal. This function provides direct access to the stored versions presenting them in an interactive ISPF Worksheet.

3.1.3 Configuration Baselines

For a defined configuration file, a baseline of its content is maintained. This function will display the current baseline.

3.1.4 Inspection Reports

With each execution of the Component Inspector, a full inspection of the selected configuration file is performed. The results of the Full Inspection are summarized in the panel and can be displayed, printed or copied as a Full Inspection Report using this function.

3.1.5 Inspection Findings

With each execution of the Component Inspector, a full inspection of the selected configuration file is performed. The Inspection Findings – Errors, Warnings, Notices – are summarized in the panel and can be displayed, printed or copied as a Findings Report using this function.

3.1.6 Change Reports

With each execution of the Component Inspector, a comparison of the current configuration is made against its baseline; any changes discovered are summarized in the panel and can be displayed, printed or copied as a Change Report using this function.

3.2 Line Command Options

3.2.1 Interval Detectors

Enter 'DETC' on the command line and press enter to display the Inspectors Interval Detector Interface. These specific Detectors are designed to report their discovered problems and changes asynchronously from the other Image FOCUS or Control Editor reporting systems. Interval execution may be set – Daily, Weekly or Monthly – any one, or all three simultaneously, with reports delivered via Email. Use PFK1 for Help.

3.2.2 Printing

Enter 'PRNT' on the command line first and then make a selection (S,F,C,R) and press enter. These actions will display the ISPF Hardcopy Utility interface.

3.2.3 Copying

Enter 'COPY' on the command line first and then make a selection (S,F,C,R) and press enter. These actions will display the ISPF Move/Copy Utility interface.

3.2.4 Health Checks

Enter 'HCKR' and press enter to display the HealthCheck Notification Interface. These settings in the ICE NSEENSxx member are designed to work in conjunction with IPLCHECK. When IPLCHECK is active and this panel is populated, Email will be sent to a defined set of recipients. Use PFK1 for Help.

4 Running as a Workbench Inspector

Here you have two options. First, run the Inspectors inline, with all other Inspectors during an overall Image Inspection. Second, run the Inspectors as individual Inspections using the functions of the Component Inspector.

4.1 Inline Inspections

Like all Image FOCUS Inspectors, the PAGENT Inspector and its DAEMONS may be run inline with a Full Image Inspection from the Image Inspection Panel Interface. To do so requires that you access the "Define Image for Inspection" panel and do the following:

4.1.1 Requirements

First, the Additional COMMNDxx Member must have been populated with the Start Command for the PAGENT and/or IKED, NSSD, DMD and TRMD Task. The Panel line appears as follows:

```
ADD'L COMMNDxx  ==> IF           (See Image FOCUS Documentation)
```

Second, both the JES and TCPIP Inspections must be set to 'Y'. The required Panel line would appear as follows:

```
INSPECTOR NAMES     OPSYS DSRPT JESx VTAM TCPS CICS LOAD MBRS CSDS CST1 CST2
SELECTION (Y/N) ==>   Y     Y     Y    N    Y    N    N    N    N    N    N
```

4.1.2 The Index Report

When the Image Inspection completes, the Inspection Index Report will be displayed. Scroll down the report to the sections shown below:

```
LINE Member    Status       Description
CMD  Name      Code
..   -TELNET   WARNING      TELNET Profile Inspection
..   -FTP      OK           FTP Profile Inspection
..   -PAGENT   ERROR        PAGENT Inspection
..   -IKED     WARNING      IKED Inspection
..   -NSSD     WARNING      NSSD Inspection
..   -DMD      WARNING      DMD Inspection
..   -TRMD     WARNING      TRMD Inspection
```

To display the related Inspection Report, place "S" on the insertion point preceding the Inspector (Member Name) and press enter.

4.2 Component Inspection

The Component Inspector supports a number of individual z/OS and Communication Server configuration components. To set up the Component Inspector to Inspect PAGENT or one or more of its DAEMONs requires that you access the "Component Inspection Selection" panel and do the following:

4.2.1 Requirements

First, enter 'I' on any available panel insertion point (your new entry will be inserted below). Next, in the panel that appears, enter one of the following: PAGENT, IKED, NSSD, DMD or TRMD and press enter. You add Inspectors one at a time, so once you are finished setting up the first, cycle back and add others as needed.

Second, in the panel that appears, "Single Component Inspection" you will need to provide an 8 character Inspector Name within the panel line that appears as follows:

```
Inspection Name ==> yourname      =A User Assigned Name
```

Third, lower in the panel you will find this line:

```
..      STDENV    =>  ____________________________________________________  =>
```

In the space provided, enter the fully qualified name of either the Environmental or Configuration file that is pointed to by the JCL, or to any other file name that you might be using for testing or upgrading the configuration. We discussed how to located the needed file name in the sub-section titled "Setting up the Inspectors".

Fourth, once the name is entered, place "S" on the selection point preceding STDENV. If the file appears, you are ready to go. PFK3 back and press enter to begin the Inspection. If it does not appear, the entered file is not accessible by the Component Inspector.

4.2.2 Component Inspector Panel Interface

The PAGENT and DAEMON Inspector are unique in that they display inline Inspection Summary Panels that can be used to access inspection findings, detected changes and support and maintain underlying configuration files.

During a Component Inspection of PAGENT or a DAEMON, it will display an "Inline Access" panel, a sample of which is shown below:

```
        PAGENT 0501   ICE 16.0 - Image Inspection Summary - TCPIP1

-Source Datasets/Files- Cm ----------Dataset and/or File Names----------
 Policy Agent Task      .. /u/paul/samples/pagent_ImageMain.config
 TCP/IP Image Task      .. /u/paul/samples/pagent_image_tcpip1.conf
 Network IPSecurity     .. /u/paul/samples/pagent_IPSec.conf
 App Transparent TLS    .. /u/paul/samples/pagent_TTLS.conf
 Intrusion Detection    .. /u/paul/samples/pagent_IDS.conf
```

```
 Policy Based Routing   .. /u/paul/samples/pagent_Routing.conf
 Quality of Service     .. /u/paul/samples/pagent_qos_tcpip1.config

--Inspection Findings-- Cm Smnt-Refs -Err--War--Not--Inf--Unk--Ttls--Cng
 Policy Agent Task      ..   14     0    1    5    0  160    0   166    1
 TCP/IP Image Task      ..   13     0    4    0    0  186    0   190    0
 Network IPSecurity     ..  141    59    1    2    0 1859    0  1862    0
 App Transparent TLS    ..   40    48    0    0    0  604    0   604    0
 Intrusion Detection    ..   76    68    2    2    0  854    0   858    0
 Policy Based Routing   ..   17    12    0    0    0  201    0   201    0
 Quality of Service     ..    4     2    0    1    1  141    0   143    0
---------Total--------- ..  305   189    8   10    1 4005    0  4024    1

 Full Inspection Report .. IFO.TEST.$PGN.RPTS.$TCPIP1($9050413)

 Option ===>
```

The panel is interactive, listing individual configuration files, configuration baselines, full inspections, findings only and detected changes. PFK1 for HELP.

4.2.3 Multi-TCP/IP Image Inspections

When the selected Main Configuration file (Policy Agent Task) contains a multiple fully qualified (configuration file) reference on the TcpImage control statements, a multi-TCP/IP Image Inspection is performed, a sample is shown above. This is the first of two defined by TcpImage, TCP/IP Images (TCPIP1 and TCPIP2). See “SKIP” below.

4.2.4 Inspection SKIP Option

Without intervention, the inspection of TCPIP2 would commence when you select PFK3. However, if you now wish to bypass that inspection, proceed, and go directly to the final inspection report for TCPIP1, enter “SKIP” on the command line and press enter.

4.3 Configuration Access Via The Control Editor

Each file shown in the upper part of the panel may be accessed by entering “S”, but only if the file is included in an active Control Editor - Control Category. If it is, it will be displayed in ICE/ISPF Edit and inherit all of the functions of the Control Editor. They include:

4.3.1 Capture of all updates

Once a file is displayed in ICE/Edit, all changes made to it are recorded in the TCE Control Journal (a BLOCKCHAIN for z/OS Configurations). In addition to the actual updated file, they include standard ISPF Statistics: UserId, Date, Time, etc. and any related documentation provided by the user via the TCE Descriptor.

4.3.2 Edit Descriptor

The Edit Descriptor works in tandem with TCE/Edit and is called only when an actual change is detected. This intercept is a default or custom full function ISPF panel that may be designed to capture as much or as little additional information from the user as needed and may be optionally integrated into existing Change Management Systems via its API.

4.3.3 Inline ISPF Compare

All of the functions of standard ISPF Compare are available to the ICE/ISPF user.

4.3.4 Compare History Listing

Once in TCE/Edit, enter 'COMPARE HISTLIST' on the command line to display a selection list of Compare Points. Selecting a specific entry will compare its content against the current working file, displaying its findings in standard ISPF Compare.

4.3.5 Configuration Audit

Once in TCE/Edit, enter 'CONFIG AUDIT' on the command line to display a full audit of all changes related to the working file that have been captured in the TCE Control Journal, beginning with the initial backup of the file.

4.3.6 Immediate File Restore

Once in TCE/Edit, enter 'RESTORE' on the command line to display a selection list of Restore Points. Several options are offered. Selecting a specific entry will restore it. Confirmation of this action is required.

5 Running as an Interval Detector

PAGENT and DAEMON Inspections may be optionally run under the control of ICE as Interval Detectors; Daily, Weekly, Monthly or all three simultaneously. The interface necessary to configure and set up an Interval Detector is accessed via the Component Inspector.

5.1 Setting up the Detector

Once a Component Inspector is set up and operational, enter "DETC" on the command line of the Inline Inspection Summary panel and press enter; this will display the Interval Email interface panel.

5.1.1 Interval Inspection Report

```
          POLICY AGENT - PAGENT - INSPECTION - NEWERA SOFTWARE, INC.
        CONFIGURATION SCOPE - AGENT, IPSEC, ATTLS, IDS & PBR.
        UPDATE SYSTEM=ADCD23C AT=13:10:07 ON=Y19/M05/D06 BY=IFOS

 POLICY AGENT JCL PARM - /u/paul/samples/pagent_CommonEnviro.config
 POLICY AGENT TASK DSN - /u/paul/samples/pagent_CommonMain.config

           PAGENT INSPECTION SUMMARY - INSPECTION POINTS=3676
                   TCP/IP IMAGE NAME - ADCD23C

                   OVERALL SUMMARY OF FINDINGS

-----Inspections----- --Count-- --------------Results--------------
--------Names-------- Stmt-Refs  Err  War  Not  Inf  Unk  Ttls  Cng
Policy Agent Task       12    0    1    2    0  138    0   141    0
Network IPSecurity     140   56    1    1    0 1850    0  1852    3
App Transparent TLS     41   48    0    0    0  613    0   613    0
Intrusion Detection     76   68    2    2    0  854    0   858    0
Policy Based Routing    18   14    0    0    0  212    0   212    0
---------------------- ---- ---- ---- ---- ---- ---- ---- ----- ----
--------Total--------  287  186    4    5    0 3667    0  3676    3

            FULL FINDING:IFO.TEST.$PGN.RPTS.$ADCD23C($FINDING)
            FULL CHANGES:IFO.TEST.$PGN.CNGS.$ADCD23C($CHANGES)
```

5.1.2 Interval Email Control Cards

Optionally the Inspection Summary may be sent via Email when one or more of the following "Action Blocks" is coded in the ICE NSEDETxx and NSEENSxx Parmlib Member:

In the NSEDETxx Member, they would appear as follows:

```
PLCYAGNTDAY ON|OFF
PLCYAGNTDAY CYCLE(DAILY) TIME('DH':'DM') INTERVAL('DI')
PLCYAGNTWKS ON|OFF
PLCYAGNTWKS CYCLE(WEEKLY('WI')) TIME('WH':'WM')
PLCYAGNTMTH ON|OFF
PLCYAGNTMTH CYCLE(MONTHLY('MI')) TIME('MH':'MM')
```

```
IKEDAEMNDAY ON|OFF
IKEDAEMNWKS ON|OFF
IKEDAEMNMTH ON|OFF

NSSDAEMNDAY ON|OFF
NSSDAEMNWKS ON|OFF
NSSDAEMNMTH ON|OFF

DEFMANGRDAY ON|OFF
DEFMANGRWKS ON|OFF
DEFMANGRMTH ON|OFF

TRMDAEMNDAY ON|OFF
TRMDAEMNWKS ON|OFF
TRMDAEMNMTH ON|OFF
```

These NSEDETxx "Action Blocks" support, simultaneously, the multiple intervals; day, week and month at any specified (24hr) time of the day, day of the week and/or month.

In the NSEENSxx Member they would appear as follows:

```
ACTION DETECTOR(PLCYAGNTDAY) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END
ACTION DETECTOR(PLCYAGNTWKS) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END
ACTION DETECTOR(PLCYAGNTMTH) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END

ACTION DETECTOR(IKEDAEMNDAY) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END
ACTION DETECTOR(IKEDAEMNWKS) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END
ACTION DETECTOR(IKEDAEMNMTH) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END

ACTION DETECTOR(NSSDAEMNDAY) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END
ACTION DETECTOR(NSSDAEMNWKS) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END
ACTION DETECTOR(NSSDAEMNMTH) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END

ACTION DETECTOR(DEFMANGRDAY) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END
ACTION DETECTOR(DEFMANGRWKS) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END
ACTION DETECTOR(DEFMANGRMTH) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END

ACTION DETECTOR(TRMDAEMNDAY) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END
ACTION DETECTOR(TRMDAEMNWKS) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END
ACTION DETECTOR(TRMDAEMNMTH) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END
```

These NSEENSxx "Action Blocks" support the full NSEENSxx Control Card Standards, i.e. TO, FROM, COPY, SUBJECT, Etc.

5.1.1 Interval Detector Email Interface

The "Action Blocks" and Control Cards described above may be (with appropriate permits) added, deleted or modified directly using TSO/ISPF. The same may be accomplished using a direct programmatic panel interface that combines access to NSEENSxx and NSEDETxx. Both methods may be used without concern for either interfering with the other. The panel interface is shown below:

```
       NSIMLDX 0501   ICE 16.0 - IKE Daemon Event Monitor - IKED

/. IKEDAEMONTR IKE Daemon Event Monitors  .. Update .. Changes .. Finding

  <> Select Report Scope - Day, Wks, Mth - Set 24hr Time and Interval <>

 /. Day - Set Time 10 : 37 and Interval 12 Specify Hourly Interval
          24 Hours hh : mm       Values 1|2|3|4|6|8|12|24:Use Blank
 .. Wks - Set Time 16 : 09 and Interval FRI_____________________
          24 Hours hh : mm       Values SUN,MON,TUE,WED,THR,FRI,SAT
 .. Mth - Set Time 16 : 10 and Interval 29_____________________
          24 Hours hh : mm       Values 1,2,3,10,15,20,25,30 or EOM

/. EMAILREPORT Subject IKED_Interval_____________________________________

  /. 1-To PRR@NEWERA.COM_____________________________________________
  /. 2-To PAT@NEWERA.COM_____________________________________________
  .. 3-To ___________________________________________________________
  /. From SUPPORT@NEWERA.COM_________________________________________

.. AltHLQ IFO.TEST_____________ /. JrlPost Ok /. CngOnly Ok /. ErrOnly Ok
.. PROC Name TESTDTA_ .. Email Method Yes .. Email Note On_ .. Retain _10

Option ===>_____________________________________________________________
```

To reach the panel, you will need to set up a Component Inspector for the targeted Inspector that you wish to run as an Interval Detector. Once you reach the target's Inspection Summary panel, enter "DETC" on the command line and press enter. This displays the Interval Event Notification Via Email setup panel.

If an "Action Block" already exists in NSEENSxx or NSEDETxx, its values will be displayed. Follow the outline of the panel to add or delete Email Addresses or to Change Settings, PFK1 for Help. If there is no existing "Action Block", follow the outline of the panel. Be certain to activate each entry by placing a check '/' on the insertion point shown before it, PFK1 for Help.

When you exit (PFK3) the panel, it will automatically check for updates/changes. If they are discovered, the settings in NSEENSxx and NSEDETxx are automatically updated and the ICE Primary Control Task, IFOM, is cycled and activated.

When the NSEENSxx and NSEDETxx members are updated in this manner, the following notation will appear immediately prior to the updated/new Action Block:

```
* ACTION UPDATE BY TCE/NSIMLDX - USER:USER01 DATE:2019/05/01 TIME:10:23:
```

All prior "* ACTION UPDATE" notations are automatically removed.

The Help Panel that supports the Email Notification functions is shown below:

```
                ICE 16.0 - Policy Agent Event Monitor - IKED

Overview ------------------------Description----------------------
         This panel displays controls that are used to configure
         settings that manage the ICE Detector task. To activate
         a Task and its configuration elements check '/' the
         command area .. that precedes the Report Name and its
         related configuration options, providing a specific Time
         and Interval setting for report production. When settings
         are as desired select Update to force an update/change.
         A message will confirm when update action has completed.
Displays Reports display list of available Reports with findings.
         Use Update to reset/update the Interval Settings.
         Select Denials to display a list of recorded Violations.
MailAddr Reports may be sent by email to named recipients. To act-
         ivate Email Notification, '/' before 'EMAILREPORT', pro-
         vide a subject, one/more recipient addresses & a sender.
         Each recipient and Sender address must be activated.
Settings Field Checking is automatically provided. When problems
         are encountered descriptive messages are displayed. Rep-
         orts can be programmed & sent only if new violations are
         discovered. Number retained by default is 10, in/decrease
         as needed. Post permanent copies to Journal if needed.
```

6 Running as a Health Check

PAGENT Inspections may be optionally run under the control of the IBM Health Checker for z/OS.

The Default setting for Health Check Processing is 'OFF'.

When the Health Check setting is 'ON', the check may be activated by issuing the following command from the system console:

```
/S IPLCHECK
```

The resulting Inspection Summary posted to the Health Checker queue may be viewed and/or rerun by using either the SDSF CK option or CA SysView. A sample Health Check is shown below:

6.1.1 Health Check Report

```
CHECK(NEWERA,NEZ_PAGENT_INSPECTION)
SYSPLEX:    ADCDPL    SYSTEM: ADCD23C
START TIME: 05/04/2019 07:53:41.348951
CHECK DATE: 20190429  CHECK SEVERITY: HIGH

INSPECTION SUMMARY Report

Message  Text
-------- ------------------------------------------------------------
ICE0000N   POLICY AGENT - PAGENT - HEALTH CHECK - NEWERA SOFTWARE, INC.
ICE0000N    CONFIGURATION SCOPE - AGENT, IPSEC, ATTLS, IDS & PBR.
ICE0000N    UPDATE SYSTEM=ADCD23C AT=07:54 ON=Y19/M05/D04 BY=IFOS
ICE0000N
ICE0000N      PAGENT HEALTH CHECK SUMMARY - INSPECTION POINTS=3875
ICE0000N
ICE0000N      POLICY AGENT JCL PARM - /u/pat/pagnt.txt
ICE0000N      POLICY AGENT TASK DSN - /u/paul/pagent.config
ICE0000N
ICE0000N                 OVERALL PAGENT INSPECTION SUMMARY
ICE0000N                    TCP/IP IMAGE TASK - TCPIP1
ICE0000N              /u/paul/samples/pagent_image_tcpip1.conf
ICE0000N
ICE0000N -----Inspections----- --Count-- --------------Results-------------
ICE0000N --------Names-------- Stmt-Refs  Err  War  Not  Inf  Unk  Ttls Cng
ICE0000N Policy Agent Task       14    0    1    6    0  156    0   163   0
ICE0000N TCP/IP Image Task       12    0    4    0    0  180    0   184   2
ICE0000N Network IPSecurity     141   59    1    4    0 1859    0  1864   0
ICE0000N App Transparent TLS     40   48    0    0    0  604    0   604   0
ICE0000N Intrusion Detection     76   68    2    2    0  854    0   858   0
ICE0000N Policy Based Routing    17   12    0    0    0  201    0   201   0
ICE0000N Quality of Service       0    0    0    0    1    0    0     1   0
ICE0000N -------------------- ---- ---- ---- ---- ---- ---- ---- ----- ---
ICE0000E --------Total--------  300  187    8   12    1 3854    0  3875   2
ICE0000N
ICE0000N        FULL FINDING:IFO.TEST.$PGN.CHKS.$TCPIP1($HLCKALL)
ICE0000N        FULL CHANGES:IFO.TEST.$PGN.CNGS.$TCPIP1($CHANGES)
ICE0000N
ICE0000N        Email Alerts:IFO.TEST.$PGN.MCHK.$TCPIP1
ICE0000N
ICE0000N        Email Success: RC=0 DETECTOR=PAGENTCHECK

* High Severity Exception *

NEZH051E The NEZ_PAGENT_INSPECTION check has found one or
```

```
more potential errors in IPL integrity on this system.
```

6.1.2 A view of NewEra Health Checks

Sample of the Health Checker queue as shown using SDSF CK function:

```
NEZ_DMD_INSPECTION               NEWERA          ACTIVE(ENABLED)    EXCEPTION
NEZ_DYNAMIC_CHANGE_INSPECTION    NEWERA          ACTIVE(ENABLED)    SUCCEESS
NEZ_IKED_INSPECTION              NEWERA          ACTIVE(ENABLED)    EXCEPTION
NEZ_JES2_INSPECTION              NEWERA          ACTIVE(ENABLED)    EXCEPTION
NEZ_JES3_INSPECTION              NEWERA          ACTIVE(DISABLED)   ENV NOT
NEZ_NSSD_INSPECTION              NEWERA          ACTIVE(ENABLED)    EXCEPTION
NEZ_OPSYS_INSPECTION             NEWERA          ACTIVE(ENABLED)    EXCEPTION
NEZ_PAGENT_INSPECTION            NEWERA          ACTIVE(ENABLED)    EXCEPTION
```

6.1.3 Health Check Email Control Cards

Optionally the Health Check Summary may be sent via Email when one or more of the following "Action Blocks" appear in the ICE NSEENSxx Parmlib Member:

```
ACTION DETECTOR(PAGENTCHECK) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END

ACTION DETECTOR(IKEDMNCHECK) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END

ACTION DETECTOR(NSSDMNCHECK) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END

ACTION DETECTOR(TRMDMNCHECK) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END

ACTION DETECTOR(DMGDMNCHECK) METHOD(EMAIL) SCOPE(REPORT)
ACTION .END
```

These NSEENSxx "Action Blocks" support the full NSEENSxx Control Card Standards, i.e. TO, FROM, COPY, SUBJECT, Etc. In addition, it supports Control Cards that are specific to PAGENT Inspection Health Check Emails. They are:

```
HCDELTAONLY (YES/NO)
```

When this Control Card is specified with a value of 'YES', Email will only be sent when a change in Inspection Finding and/or Configuration Settings is discovered. This means that if the prior report has the same content as the current report, Email will not be sent. A new Email will only be sent when a "New" finding or a "New" change to the configuration has been detected. When the value is set to "NO", or not present in the "Action Block", the default case, Email will be sent with each Health Check interval.

```
HCAUDITLOG (YES/NO)
```

When this Control Card is specified with a value of 'YES', a summary record of the Health Check interval report is written to the IPLCHECK SysOut. This AuditLog therefore contains a record of each Health Check interval and its findings.

6.1.4 Health Check Email Interface

The "Action Blocks" and Control Cards described above may be (with appropriate permits) added, deleted or modified directly using TSO/ISPF or the same accomplished using a direct programmatic panel interface to NSEENSxx. Both methods may be used without concern for either interfering with the other. The panel interface is shown below:

```
     NSIMLDX 0501   ICE 16.0 - HealthChecker Notification Via Email

/. IKEDMNCHECK IKED HealthChecker Notice Last Run: Tuesday 05D/04M/19Y

/. EMAILREPORT Subject: IKED CHECK FINDINGS_____________________________

  /. 01-To PRR@NEWERA.COM_____________________________________________
  /. 02-To PAT@NEWERA.COM_____________________________________________
  .. 03-To ___________________________________________________________
  .. 04-To ___________________________________________________________
  .. 05-To ___________________________________________________________
  .. 06-To ___________________________________________________________
  .. 07-To ___________________________________________________________
  .. 08-To ___________________________________________________________
  .. 09-To ___________________________________________________________
  .. 10-To ___________________________________________________________
  .. 11-To ___________________________________________________________
  .. 12-To ___________________________________________________________

  /. From: SUPPORT@NEWERA.COM_________________________________________

           .. Email Method Act .. Changes Only No  .. Write Audit Log No

Option ===>_____________________________________________________________
```

To reach the panel, you will need to set up a Component Inspector for the targeted Inspector that you wish to run as a Health Check. Once you reach the target's Inspection Summary panel, enter "HCKR" on the command line and press enter. This displays the Health Checker Notification Via Email setup panel.

If an "Action Block" already exists in NSEENSxx, its values will be displayed. Follow the outline of the panel to add or delete Email Addresses or to Change Settings, PFK1 for Help. If there is no existing "Action Block" follow the outline of the panel. Be certain to activate each entry by placing a check '/' on the insertion point shown before it, PFK1 for Help.

When you exit (PFK3) the panel, it will automatically check for updates/changes. If they are discovered, the settings in NSEENSxx are automatically updated and the ICE Primary Control Task, IFOM, is cycled and activated.

When the NSEENSxx member is updated in this manner, the following notation will appear immediately prior to the updated/new Action Block:

```
* ACTION UPDATE BY TCE/NSIMLDX - USER:USER01 DATE:2019/05/01 TIME:10:23:
```

All prior "* ACTION UPDATE" notations are automatically removed.

The Help Panel that supports the Email Notification functions is shown below:

```
           ICE 16.0 - HealthChecker Notification Via Email

Overview ------------------------Description----------------------
         When running the selected Inspector as a Health Check you
         may elect to send Email Notification containing Inspect-
         ion findings and/or configuration changes. These Emails
         are sent continuously or only when findings/changes are
         found to have changes from the prior Email Notification.
Required Check '/' both the Inspectors Action Block Name & 'EMAIL-
         REPORT. Failing to do so will turn off the Email Service.
         Subject - Enter an Email Subject.
         Enter and Check '/' one or more Email Addresses. Failing
         to check an Email Address will remove it from the system.
         Enter and Check '/' the From Email Address. Failing to
         check the From Address will remove it from the system.
Result   If you fail to provide the required information you will
         be prompted to do so and cycled back to the panel until
         you do so or uncheck the Inspectors Action Block Name.
Method   Select 'S' to show the NSEENSxx Email Method Block.
Changes  Select 'S' to toggle shown value 'Yes/No'.
AuditLog Select 'S' to toggle shown value 'Yes/No'. The AuditLog
         is optionally maintained in IPLCHECK SYSTSPRT.
Last Run Cursor under, press enter to show last Summary Report.
```

If you wish to ABORT your update, type “ABORT” on the panel command line and press enter. This action will return you to the Component Inspector.

7 Starting Up of the Inspectors

The Policy Management Agent (PAGENT), a component of IBM Communication Server (CS) for z/OS TCP/IP, is configured by policy definitions stored in either a Lightweight Directory Access Protocol (LDAP) server or more likely in local configuration flat UNIX files or MVS Datasets. Without regard for their source, these stored policies control network security and traffic prioritization to and from the z/OS environment. Upon initialization, PAGENT reads these configuration files, parses out their policies, and stores them in the TCP/IP stack where they are used for ongoing policy enforcement.

The PAGENT Inspector automatically discovers the JCL that will be used to start the PAGENT task. Parsing it determines the nature of the configuration pointed to by the DD Statements imbedded therein – UNIX File Vs. MVS Dataset and Environmental Source Vs. Configuration Source. It validates each configuration source to identify the starting points for the inspection of TcpImage, AT-TLS, Intrusion Detection, Policy Based Routing, IPSecurity and Quality of Service. Source configurations that cannot be opened or located are reported as inspection "Errors". A sample of both a successful and failed source validation are shown below.

If successful:

```
PAG1008I LINE 00080 BGINS * BEGIN POLICYLOAD INSPECTION
PAG3108I LINE 00080 DSNAM >..IFO.TEST.PAGEMT
PAG3208I LINE 00080 VALID >...SUCCESS - 1066 RECORDS FOUND
PAG3008I LINE 00080 ENINS * END POLICYLOAD INSPECTION
```

If failure:

```
PAG1008I LINE 00085 BGINS * BEGIN POLICYLOAD INSPECTION
PAG3108I LINE 00085 FILES >../u/user1/pagent.remote.ttls
PAG3208E LINE 00085 ERROR >...FAILURE - NOT FOUND - RC=4
PAG3008I LINE 00085 ENINS * END POLICYLOAD INSPECTION
```

7.1 UNIX Actions Imbedded in the Initialization JCL

If PAGENT is started with its configuration defined using UNIX Files, the Inspection process will report on two possible imbedded UNIX Commands:

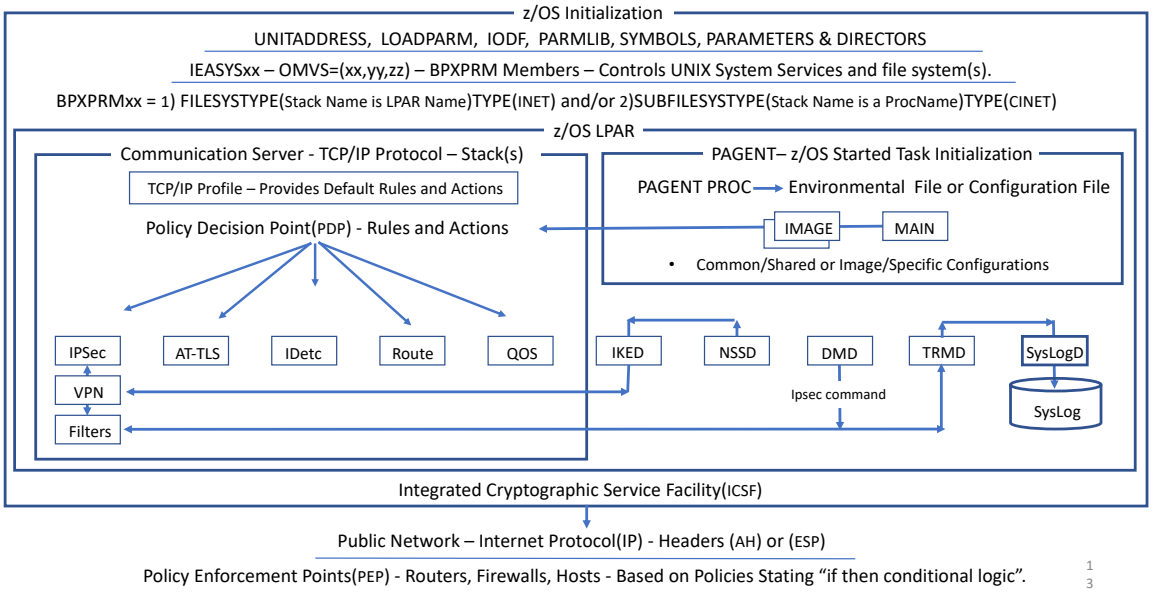
(-C/-c), If this command is found, the Inspector will start up using the PAGENT Configuration File as opposed to its Environmental File. If an Environmental File is used, the Inspector will parse it or the source name of the Configuration File.

(-I/-I), If this command is found, the Inspector will report it as a Notice that updates to any PAGENT configuration and will immediately be acted on and initialized. If the PAGENT configuration is based on MVS Datasets, such immediate action is not available and, therefore, only becomes effective when the PAGENT main task is restarted. A sample of this reporting is shown below:

```
PAG9610I <> PAGENT SETTINGS DEFINED IN STARTUP JCL.
|
PAG9620I (-C/-c) PAGENT INITIALIZED USING A CONFIGURATION FILE.
PAG9630N DYNAMIC MONITORING OF UNIX FILE UPDATES IS OFF
```

7.2 PAGENT Inspection Elements

Once the PAGENT configuration files/datasets – TcpImage, IPSecurity, AT-TLS, Intrusion Detection, Policy Based Routing - are validated, each is read and processed in that order. Other files referenced in the TcpImage Configuration file – The TCP/IP Image and the Image Quality of Service (QoS) – if found are validated and processed within the TCP/IP Image Inspection, Image by Image. The diagram below shows the primary actions taken by the Inspectors as they identify PAGENT and DAEMON configurations for inspection.



The Inspection Report is divided into six or eight sections, one each for the five inspectable configuration files and an overall PAGENT Inspection Summary, and if configured, one or more TCP/IP Images and their related QoS configurations.

The Policy Agent Task configuration file/dataset contains base configuration settings as well as points to - TcpImage, IPSecurity, AT-TLS, Intrusion Detection, Policy Based Routing and Quality of Service - configuration files, the major components of these sections.

7.2.1 The PAGENT Base Configuration

```
PAG9850I /*********************************************************/
PAG9850I /*   Policy Agent Configuration Inspection is Beginning   */
PAG9850I /*********************************************************/
|
PAG1000I PAGENT INSPECTOR STARTED: 15.0 - 05.01.19 - z/OS 2.3
PAG1001I  INSPECTION DATE SATURDAY, 4 MAY 2019.
PAG1002I  INSPECTOR PROCESSING PAGENT FOR z/OS V2R3.
PAG1003I  INSPECTION RULES SET FOR TARGET z/OS V2R3.
|
PAG1003I  SOURCE TYPE EQUALS CONFIGURATION.
PAG1004I   SOURCE FILE IS /u/paul/pagent.config.
PAG1005I     136 CONFIGURATION RECORDS WERE FOUND.
|
<> CONFIGURATION SOURCE AND INSPECTION LINES ARE INSERTED BY INSPECTOR HERE <>
|
PAG4099I PAGENT STATEMENT PARSING COMPLETE.
|
PAG3006I INSPECTION REPORT SUMMARY:
PAG3007I  8 MAIN CONFIGURATION STATEMENTS PROCESSED.
|
PAG3010I     1 ERRORS.
PAG3011I     0 WARNINGS.
PAG3012I     0 NOTICES.
PAG3013I   151 INFORMATION.
PAG3014I     0 UNINSPECTED.
|
PAG6099I PAGENT INSPECTOR ENDED.
```

7.2.2 Individual Images when Multiple are Defined

```
IMA9850I /*********************************************************/
IMA9850I /*   TCP/IP Image Configuration Inspection is Starting    */
IMA9850I /*********************************************************/

IMA1000I TCP/IP Image INSPECTOR - 15.0 - 05.01.19 - z/OS 2.4
IMA1001I  INSPECTION DATE SATURDAY, 4 MAY 2019.
IMA1002I  INSPECTOR PROCESSING PAGENT FOR z/OS V2R3.
IMA1003I  INSPECTION RULES SET FOR TARGET z/OS V2R3.
|
IMA1004I TCP/IP IMAGE STACK NAME - TCPIP1 - IS RUNNING.
IMA1005I  IMAGE CONFIGURATION SOURCE - IMAGE CONFIGURATION:
IMA1006I   SOURCE FILE IS:
IMA1008I    UNIX - /u/paul/samples/pagent_image_tcpip1.conf.
IMA1007I     115 CONFIGURATION RECORDS WERE FOUND.
|
<> CONFIGURATION SOURCE AND INSPECTION LINES ARE INSERTED BY INSPECTOR HERE <>
|
IMA4099I TCPIP1 STATEMENT PARSING COMPLETE.
|
IMA3006I IMAGE CONFIGURATION SOURCE - INSPECTION SUMMARY:
IMA3007I  12 IMAGE CONFIGURATION STATEMENTS PROCESSED.
|
IMA3010I     4 ERRORS.
IMA3011I     0 WARNINGS.
IMA3012I     0 NOTICES.
IMA3013I   180 INFORMATION.
IMA3014I     0 UNINSPECTED.
|
IMA6099I PAGENT IMAGE INSPECTOR ENDED.
```

7.2.3 Network IPSecurity

```
IPS9850I /*********************************************************/
IPS9850I /*  Policy Agent IPSEC Configuration Inspection Beginning */
IPS9850I /*********************************************************/
|
IPS1000I IPSEC INSPECTOR STARTED: 15.0 - 05.01.19 - z/OS 2.3
IPS1001I  INSPECTION DATE SATURDAY, 4 MAY 2019.
IPS1002I  INSPECTOR PROCESSING PAGENT FOR z/OS V2R3.
IPS1003I  INSPECTION RULES SET FOR TARGET z/OS V2R3.
|
IPS1003I  SOURCE TYPE EQUALS CONFIGURATION.
IPS1004I   SOURCE FILE IS /u/paul/samples/pagent_CommonIPSec.conf.
IPS1005I     1000 CONFIGURATION RECORDS WERE FOUND.
|
<> CONFIGURATION SOURCE AND INSPECTION LINES ARE INSERTED BY INSPECTOR HERE <>
|
IPS4099I IPSEC STATEMENT PARSING COMPLETE.
|
IPS3006I INSPECTION REPORT SUMMARY:
IPS3007I  140 IPSEC CONFIGURATION STATEMENTS PROCESSED.
|
IPS3010I     1 ERRORS.
IPS3011I     1 WARNINGS.
IPS3012I     0 NOTICES.
IPS3013I  1836 INFORMATION.
IPS3014I     0 UNINSPECTED.
|
IPS6099I IPSEC INSPECTOR ENDED.
```

7.2.4 Application Transparent TLS

```
TLS9850I /*********************************************************/
TLS9850I /* Policy Agent AT-TLS Configuration Inspection Beginning */
TLS9850I /*********************************************************/
|
TLS1000I AT-TLS INSPECTOR STARTED: 15.0 - 05.01.19 - z/OS 2.3
TLS1001I  INSPECTION DATE SATURDAY, 4 MAY 2019.
TLS1002I  INSPECTOR PROCESSING PAGENT FOR z/OS V2R3.
TLS1003I  INSPECTION RULES SET FOR TARGET z/OS V2R3.
|
TLS1003I  SOURCE TYPE EQUALS CONFIGURATION.
TLS1004I   SOURCE FILE IS /u/paul/samples/pagent_TTLS.conf.
TLS1005I     371 CONFIGURATION RECORDS WERE FOUND.
|
<> CONFIGURATION SOURCE AND INSPECTION LINES ARE INSERTED BY INSPECTOR HERE <>
|
TLS4099I AT-TLS STATEMENT PARSING COMPLETE.
|
TLS3006I INSPECTION REPORT SUMMARY:
TLS3007I  40 AT-TLS CONFIGURATION STATEMENTS PROCESSED.
|
TLS3011I     0 WARNINGS.
TLS3012I     0 NOTICES.
TLS3013I   492 INFORMATION.
TLS3014I     0 UNINSPECTED.
|
TLS6099I AT-TLS INSPECTOR ENDED.
```

7.2.5 Intrusion Detection

```
IDS9850I /*******************************************************/
IDS9850I /*  Policy Agent IDS Configuration Inspection Beginning   */
IDS9850I /*******************************************************/
|
IDS1000I IDS INSPECTOR STARTED: 15.0 - 05.01.19 - z/OS 2.3
IDS1001I  INSPECTION DATE SATURDAY, 4 MAY 2019.
IDS1002I  INSPECTOR PROCESSING PAGENT FOR z/OS V2R3.
IDS1003I  INSPECTION RULES SET FOR TARGET z/OS V2R3.
|
IDS1003I  SOURCE TYPE EQUALS CONFIGURATION.
IDS1004I   SOURCE FILE IS /u/paul/samples/pagent_IDS.conf.
IDS1005I     528 CONFIGURATION RECORDS WERE FOUND.
|
<> CONFIGURATION SOURCE AND INSPECTION LINES ARE INSERTED BY INSPECTOR HERE <>
|
IDS4099I INTDETC STATEMENT PARSING COMPLETE.
|
IDS3006I INSPECTION REPORT SUMMARY:
IDS3007I  66 INTRUSION DETECTION STATEMENTS PROCESSED.
|
IDS3010I     0 ERRORS.
IDS3011I     1 WARNINGS.
IDS3012I     0 NOTICES.
IDS3013I   825 INFORMATION.
IDS3014I     0 UNINSPECTED.
|
IDS6099I INTDETC INSPECTOR ENDED.
```

7.2.6 Policy Based Routing

```
PBR9800I /*******************************************************/
PBR9800I /*   Prevailing, Active & Resolved ROUTING Configuration  */
PBR9800I /*******************************************************/
|
PBR9811N ------DISPLAY OF ROUTING CONFIGURATION RECORDS IS OFF------
|
PBR9850I /*******************************************************/
PBR9850I /* Policy Based Routing Configuration Inspection Beginning*/
PBR9850I /*******************************************************/
|
PBR1000I ROUTEING INSPECTOR STARTED: 15.0 - 05.01.19 - z/OS 2.3
PBR1001I  INSPECTION DATE SATURDAY, 4 MAY 2019.
PBR1002I  INSPECTOR PROCESSING PAGENT FOR z/OS V2R3.
PBR1003I  INSPECTION RULES SET FOR TARGET z/OS V2R3.
|
PBR1003I  SOURCE TYPE EQUALS CONFIGURATION.
PBR1004I   SOURCE FILE IS /u/paul/samples/pagent_Routing.conf.
PBR1005I     118 CONFIGURATION RECORDS WERE FOUND.
|
<> CONFIGURATION SOURCE AND INSPECTION LINES ARE INSERTED BY INSPECTOR HERE <>
|
PBR4099I ROUTING STATEMENT PARSING COMPLETE.
PBR3007I  18 POLICY BASED ROUTING STATEMENTS PROCESSED.
|
PBR3010I     0 ERRORS.
PBR3011I     0 WARNINGS.
PBR3012I     0 NOTICES.
PBR3013I   210 INFORMATION.
PBR3014I     0 UNINSPECTED.
|
PBR6099I ROUTING INSPECTOR ENDED.
```

```
QOS9850I /*********************************************************/
QOS9850I /* Quality of Service Configuration Inspection Beginning  */
QOS9850I /*********************************************************/
|
QOS1000I QUALITY OF SERVICE INSPECTOR - 15.0 - 05.01.19 - z/OS 2.3
QOS1001I  INSPECTION DATE SATURDAY, 4 MAY 2019.
QOS1002I  INSPECTOR PROCESSING PAGENT FOR z/OS V2R3.
QOS1003I  INSPECTION RULES SET FOR TARGET z/OS V2R3.
|
QOS1004I SOURCE TYPE EQUALS CONFIGURATION.
QOS1005I  SOURCE FILE IS /u/paul/samples/pagent_qos_tcpip1.config.
QOS1006I   72 CONFIGURATION RECORDS WERE FOUND.
|
<> CONFIGURATION SOURCE AND INSPECTION LINES ARE INSERTED BY INSPECTOR HERE <>
|
QOS4099I TCPIP1 QoS STATEMENT PARSING COMPLETE.
|
QOS3006I INSPECTION REPORT SUMMARY:
QOS3007I  4 QUALITY OF SERVICE STATEMENTS PROCESSED.
|
QOS3010I     0 ERRORS.
QOS3011I     1 WARNINGS.
QOS3012I     1 NOTICES.
QOS3013I   141 INFORMATION.
QOS3014I     0 UNINSPECTED.
|
QOS6099I QoS INSPECTOR ENDED.
```

7.3 *PAGENT Inspection Summary – Single TCP/IP Stack*

At the conclusion of the inspection, a summary of the five configurations – Policy Agent Task, IPSecurity, AT-TLS, Intrusion Detection, Policy Based Routing – is presented, as shown below:

```
ALL2000I                  OVERALL SUMMARY OF FINDINGS
|
|        -----Inspections----- --Count-- --------------Results--------------
ALL2010I --------Names-------- Stmt-Refs  Err  War  Not  Inf  Unk  Ttls  Cng
ALL2020I Policy Agent Task        12    0    1    3    0  137    0   141    0
ALL2030I Network IPSecurity      140   56    1    1    0 1850    0  1852    0
ALL2040I App Transparent TLS      41   48    0    0    0  613    0   613    0
ALL2050I Intrusion Detection      76   68    2    2    0  854    0   858    0
ALL2060I Policy Based Routing     18   14    0    0    0  212    0   212    0
ALL2070I -------------------- ---- ---- ---- ---- ---- ---- ---- ----- ----
ALL2080E --------Total--------  287  186    4    6    0 3666    0  3676    0
|
ALL0000I         FULL FINDING:IFO.TEST.$PGN.RPTS.$ADCD23C($9050411)
|
IFO0746I PAGENT PROCESS COMPLETED WITH ERRORS.
IFO0783I PAGENT PROCESSING ENDED.

IFO1002I END OF REPORT.
```

Within the summary, the fully qualified name of the Inspection Report Dataset and Member are shown. The dynamic member name is assigned using the format $YMMDDHH, where Y = the last digit of the current year, MM = digits representing the current month, DD = digits representing the current day of the current month, and HH = digits representing the current hour of the current day.

7.4 PAGENT Inspection Summary – Multi-TCP/IP Stacks

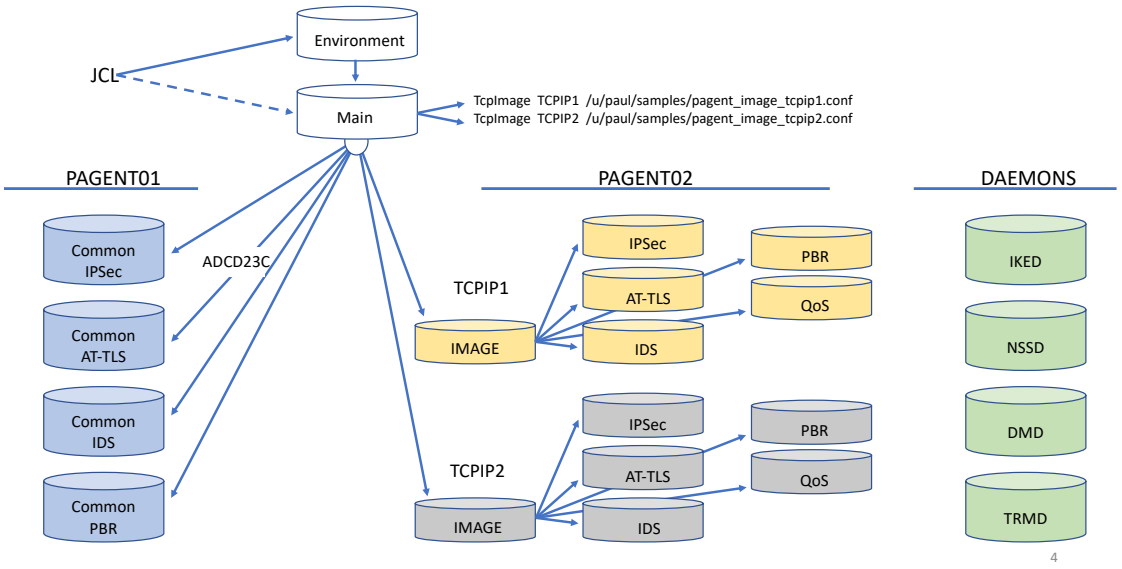
```
ALL2000I           TCP/IP IMAGE TCPIP1 OVERALL SUMMARY OF FINDINGS
|
|        -----Inspections----- --Count-- --------------Results--------------
ALL2010I --------Names-------- Stmt-Refs  Err  War  Not  Inf  Unk  Ttls  Cng
ALL2020I Policy Agent Task       14     0    1    5    0  160    0   166    1
ALL2030I TCP/IP Image Task       13     0    4    0    0  186    0   190    0
ALL2040I Network IPSecurity     141    59    1    2    0 1859    0  1862    0
ALL2050I App Transparent TLS     40    48    0    0    0  604    0   604    0
ALL2060I Intrusion Detection     76    68    2    2    0  854    0   858    0
ALL2070I Policy Based Routing    17    12    0    0    0  201    0   201    0
ALL2080I Quality of Service       4     2    0    1    1  141    0   143    0
ALL2090I ---------------------- ---- ---- ---- ---- ---- ---- ---- ----- ----
ALL2100E --------Total--------  305  189    8   10    1 4005    0  4024    1
|
ALL0000I         FULL FINDING:IFO.TEST.$PGN.RPTS.$TCPIP1($9050411)
ALL0000I         CHNG DETAILS:IFO.TEST.$PGN.CNGS.$TCPIP1($CHANGES)
|
ALL9999I TCP/IP IMAGE CONFIGURATION INSPECTIONS HAVE ENDED.
|
IFO0746I PAGENT PROCESS COMPLETED WITH ERRORS.


ALL2000I           TCP/IP IMAGE TCPIP2 OVERALL SUMMARY OF FINDINGS
|
|        -----Inspections----- --Count-- --------------Results--------------
ALL2010I --------Names-------- Stmt-Refs  Err  War  Not  Inf  Unk  Ttls  Cng
ALL2020I Policy Agent Task       14     0    1    5    0  160    0   166    0
ALL2030I TCP/IP Image Task       10     0    1    0    0   51    0    52    0
ALL2040I Network IPSecurity     141    59    1    2    0 1859    0  1862    0
ALL2050I App Transparent TLS     40    48    0    0    0  604    0   604    2
ALL2060I Intrusion Detection     76    68    2    2    0  854    0   858    0
ALL2070I Policy Based Routing    17    12    0    0    0  201    0   201    0
ALL2080I Quality of Service       4     0    1    0    0   22    0    23    0
ALL2090I ---------------------- ---- ---- ---- ---- ---- ---- ---- ----- ----
ALL2100E --------Total--------  302  187    6    9    0 3751    0  3766    2
|
ALL0000I         FULL FINDING:IFO.TEST.$PGN.RPTS.$TCPIP2($9050411)
ALL0000I         CHNG DETAILS:IFO.TEST.$PGN.CNGS.$TCPIP2($CHANGES)
|
ALL9999I TCP/IP IMAGE CONFIGURATION INSPECTIONS HAVE ENDED.
|
IFO0746I PAGENT PROCESS COMPLETED WITH ERRORS.
```

8 The Scope of Inspection

PAGENT and its DAEMONs may be configured in a number of unique ways. In certain z/OS TCP/IP installations, there may be only one TCP/IP Image, as illustrated in the diagram below, by "PAGENT01" supporting Image ADCD23C, while in others there may be multiple Stacks within the same LPAR or in remote host as illustrated by "PAGENT02" supporting Images TCPIP1 and TCPIP2. Each illustration, including the "DAEMONS", shows all possible configuration elements. Not all are needed and not all will likely be configured in support of your specific Network Security needs.

Further, in certain cases PAGENT may be configured as a "Server" supporting remote PAGENT "Clients". Whatever the configuration, the PAGENT Inspector will support them.

PAGENT Inspector Demo Configuration – Image FOCUS Component Inspection



8.1 Processing Options

PAGENT Inspection is an integral part of the overall, optional, inspection of TCP/IP for z/OS – Profile, Resolver, Data, FTP, Telnet – within the ICE application Image FOCUS. By default, PAGENT Inspection is 'ON'. Alternatively, along with its various options, it can be turned 'OFF' by entering the following KEYWORD Values as comments in the PAGENT Configuration File/Dataset:

To control PAGENT Inspection:

```
# *NEWERA*PAGENT_INSPECT=ON  # ON|OFF - DEFAULT OFF - PAGENT INSPECTION
```

To control PAGENT Inspection Options:

```
# *NEWERA*CHKREF_PROCESS=ON  # ON|OFF - DEFAULT ON - VALIDATE REFERENCE
# *NEWERA*SOURCE_DISPLAY=ON  # ON|OFF - DEFAULT ON - SHOW SOURCE IN REPORT
# *NEWERA*RESULT_DISPLAY=ON  # ON|OFF - DEFAULT ON - SHOW DETAIL IN REPORT
# *NEWERA*HLTCHK_PROCESS=ON  # ON|OFF - DEFAULT OFF- ENABLE AS HEALTH CHECK
# *NEWERA*NOTICE_PROCESS=ON  # ON|OFF - DEFAULT OFF- ENABLE EMAIL NOTICES
# *NEWERA*BASELN_PROCESS=ON  # ON|OFF,FIXED|MOVING - DEFAULT OFF/FIXED,MOVING
```

Whether they appear as comments in the configuration or not, the settings of these options are reported early on in the PAGENT Inspection Report, as follows:

```
PAG9760I PAGENT INSPECTION APPLICATION CONFIGURATION SETTINGS.
PAG9761I  *NEWERA*PAGENT_INSPECT=ON.
PAG9761I  *NEWERA*CHKREF_PROCESS=ON.
PAG9761I  *NEWERA*SOURCE_DISPLAY=ON.
PAG9762I  *NEWERA*RESULT_DISPLAY=ON.
PAG9762I  *NEWERA*NOTICE_PROCESS=ON.
PAG9763I  *NEWERA*HTLCHK_PROCESS=ON.
PAG9764I  *NEWERA*BASELN_PROCESS=ON,MOVING.
```

Each of these options is explained in the text that follows:

8.2 *RACF, its Database and SERVAUTH Class Standing*

The TCP/IP Image is a vital z/OS resource defining and enforcing the controls and policies that are used to protect the host, transactions and their endpoints. The good standing of RACF, its Database and the SERVAUTH Class are critical to the overall inspection results presented by the PAGENT and DAEMON Inspectors. In this evaluation the Inspectors do the following:

First, the External Security Manager (ESM) must be RACF. If it is not, this inspection step is skipped.

Second, if the ESM is RACF, a check is made of its Database to determine if a profile exists to protect it and if it does, what is the UACC. If no profile exists, or if the UACC is not set to “NONE”, a warning is issued.

Third, the ZEB.INITSTACK and ZEB.PAGENT are examined to determine if they have existing SERVAUTH profiles, if each of the profiles is enforced in the appropriate Class assignment and finally the standing of each profiles assigned UACC. If no profile exists, if an existing profile in not assigned to the following classes – Audit, Active, RacList, Generic – or if the profile’s UACC is not equal to “NONE”, a warning is issued.

Example of the The RACF, SERVAUTH Inspection:

```
PAG9640I MAIN CONFIGURATION SOURCE - EXTERNAL SECURITY:
PAG9641I  EXTERNAL SECURITY MANAGER IS IBM/RACF - RELEASE:7791.
PAG9642I   ACTIVE RACF DATABASE:SYS1.RACFDS                              .
PAG9643W    RESOURCE PROFILE:RACF DATASET HAS NO PROFILE.
PAG9644I     PROFILE UACC:RACF PROFILE HAS NO UACC.
|
```

```
PAG9650I /*********************************************************/
PAG9650I /* The SERVAUTH Class is use to protect TCP/IP features,  */
PAG9650I /* functions and products. Failure to activate this RACF  */
PAG9650I /* class will result in unprotected resources. This may   */
PAG9650I /* threaten the integrity of the operating system & data. */
PAG9650I /*********************************************************/
|
PAG9660I +----------+-----------+-----------+-----------+-----------+
PAG9660I |  Class   |   Audit   |   Active  |  Raclist  |  Generic  |
PAG9660I +----------+-----------+-----------+-----------+-----------+
PAG9660W | SERVAUTH |    ---    |    YES    |    YES    |    YES    |
PAG9660I +----------+-----------+-----------+-----------+-----------+
PAG9660I |   Selected Profiles  |   UACC    |  Discrete |  Generic  |
PAG9660I +----------------+-Ttl-+-Read+Othr-+-Read+Othr-+-Read+Othr-+
PAG9660I | EZB.INITSTACK  |   3 |   0 |   3 |   0 |   1 |   9 |   2 |
PAG9660I | EZB.PAGENT     |   3 |   0 |   3 |   1 |   0 |   1 |   1 |
PAG9660I +----------------+-----+-----+-----+-----+-----+-----+-----+
|
PAG9660I EZB.INITSTACK PROFILES - RESTRICT ACCESS DURING INITIALIZATION.
|
PAG9660I EZB.INITSTACK.ADCD223.TCPIP.DISCRETE              UACC:NONE
PAG9660I EZB.INITSTACK.*.TCPIP                             UACC:NONE
PAG9660I EZB.INITSTACK.**                                  UACC:NONE
|
PAG9660I EZB.PAGENT PROFILES - RESTRICT ACCESS TO "PASEARCH" COMMAND.
|
PAG9660I EZB.PAGENT.ADCD223.TCPIP.GENERIC                  UACC:NONE
PAG9660I EZB.PAGENT.**.TCPIP.GENERIC                       UACC:NONE
PAG9660I EZB.PAGENT.**                                     UACC:NONE
```

8.3 *PAGENT/DAEMON Inspection*

The default setting for PAGENT/DAEMON Inspection is ‘ON”.

Inspection of a PAGENT configuration (after filtering out all comments) includes an examination of a file/dataset for valid statements and keywords, the construction of the file/dataset for matching braces ‘{}’, the positioning of each statement and keyword on a separate line, the unique naming of statements, the appropriate assignment of values, ranges, and ranges and/or values to a keyword.

If unmatched braces:

```
IPS1006I <> CONFIGURATION HAS UNBALANCED OPENING/CLOSING BRACE(S):
|
IPS1007E LINE 00018 SNAME >.IpServiceGroup              FTPServer
```

If a keyword value is not valid:

```
IPS1020I LINE 00149 BGINS * BEGIN IPSERVICE INSPECTION
IPS2020I LINE 00149 SNAME >.IpService IS A VALID STATEMENT.
IPS2020I LINE 00149 VALUE >..SecureWeb
IPS2020I LINE 00151 POS01 >...SourcePortRange
IPS2020E LINE 00151 VALUE >....443000 (Should be 0 or between 1 and 65535)
IPS2020I LINE 00152 POS02 >...Protocol
IPS2020I LINE 00152 VALUE >....tcp
IPS2020I LINE 00153 POS03 >...Direction
IPS2020I LINE 00153 VALUE >....bidirectional
IPS2020I LINE 00154 POS04 >...Routing
IPS2020I LINE 00154 VALUE >....local
IPS2020I LINE 00155 POS05 >...SecurityClass
IPS2020I LINE 00155 VALUE >....0
IPS3020I LINE 00155 ENINS * END IPSERVICE INSPECTION
```

Invalid statements (and related keywords) and keywords (and their related values) are ignored at PAGENT initialization and reported in the inspection as follows.

If statement unknown:

```
IPS0906I <> IPSEC CONFIGURATION CONTAINS UNKNOWN STATEMENT. BRACE(S):
|
IPS0907E IpServiceGroPU               SecureFTPServer
```

If keyword unknown:

```
IPS1002I LINE 00025 BGINS * BEGIN IPSERVICEGROUP INSPECTION
IPS2002I LINE 00025 SNAME >.IpServiceGroup IS A VALID STATEMENT.
IPS2002I LINE 00025 VALUE >..SecureFTPServer
IPS2002E LINE 00027 UNKNW >..IpServiceRfe               Secure-FTPServer-Control
IPS2002I LINE 00028 POS02 >...IpServiceRef
IPS2002I LINE 00028 VALUE >....Secure-FTPServer-Data
IPS2002I LINE 00029 POS03 >...IpServiceRef
IPS2002I LINE 00029 VALUE >....Secure-FTPServer-Data-Passive
IPS3002I LINE 00029 ENINS * END IPSERVICEGROUP INSPECTION
```

8.4 *Statement Reference Processing*

The default setting for Reference Processing in 'ON'.

Each PAGENT Statement is (generally) assigned a unique statement name (NAMEVALUE) as a statement is configured. That name may be specifically called (Referenced) by a 'Keyword Reference'; all such keywords end with 'Ref'. When such a keyword reference does not match with a statement name, it is ignored and will result in a loss of an expected rule/monitoring/control. When such a mismatched or orphan statement is detected, it is reported as follows:

```
IDS9754I <> IDS REFERENCES THAT ARE NOT RESOLVEABLE TO NAMEVALUE:
|
IDS9755E LINE 00097 IDSActionRef                Attack-action-dallas
```

8.5 *Source Display*

The Default setting for Source Display is 'ON'.

Once the source files/datasets are validated, they are stripped of all comments and optionally displayed inline within the Inspection Report.

When Source Display is 'ON':

```
IDS9751I INCLUDED COMMONIDSCONFIG AS A UNIX FILE.
IDS9752I  /u/paul/samples/pagent_IDS.conf
IDS9753I   FROM IT IFO EXTRACTED 528 CONFIGURATION RECORDS.
|
IDS9800I /*********************************************************/
IDS9800I /*     Prevailing, Active & Resolved IDS Configuration    */
IDS9800I /*********************************************************/
|
IDS9811I ---------ACTIVE/RESOLVED IDS CONFIGURATION RECORDS---------
|
```

```
IDS9811I 00023 IDSRule                    AttackMalformed-rule
IDS9811I 00024 {
IDS9811I 00025   ConditionType            Attack
IDS9811I 00026   Priority                 2
IDS9811I 00027   IDSAttackCondition
IDS9811I 00028   {
IDS9811I 00029     AttackType             MALFORMED_PACKET
IDS9811I 00030   }
IDS9811I 00031   IDSActionRef             Attack-action
IDS9811I 00032 }
```

When Source Display is 'OFF':

```
TLS9750I INCLUDED COMMONTTLSCONFIG AS A UNIX FILE.
TLS9750I  /u/paul/samples/pagent_TTLS.conf
TLS9751I   FROM IT IFO EXTRACTED 371 CONFIGURATION RECORDS.
|
TLS9800I /*********************************************************/
TLS9800I /*   Prevailing, Active & Resolved AT-TLS Configuration   */
TLS9800I /*********************************************************/
|
TLS9811N -------DISPLAY OF AT-TLS CONFIGURATION RECORDS IS OFF-------
```

8.6 *Result Display*

The Default setting for Results Display is 'ON'.

When the Results Display setting is 'ON', all inspection steps and detail are shown in the Inspection Report as shown below:

```
PAG9850I /*********************************************************/
PAG9850I /*   Policy Agent Configuration Inspection is Beginning   */
PAG9850I /*********************************************************/
|
PAG1000I PAGENT INSPECTOR STARTED: 15.0 - 12.16.18 - z/OS 2.3  Support - Beta
PAG1001I  INSPECTION DATE TUESDAY, 18 DEC 2018.
PAG1002I  INSPECTOR PROCESSING PAGENT FOR z/OS V2R3.
PAG1003I  INSPECTION RULES SET FOR TARGET z/OS V2R3 - Beta.
|
PAG1003I  SOURCE TYPE EQUALS CONFIGURATION.
PAG1004I   SOURCE FILE IS /u/paul/pagent.config.
PAG1005I     136 CONFIGURATION RECORDS WERE FOUND.
|
PAG1001I LINE 00012 BGINS * BEGIN AUTOMONITORAPPS INSPECTION
PAG2001I LINE 00012 SNAME >.AutoMonitorApps IS A VALID STATEMENT.
PAG3001I LINE 00014 POS01 >..AppName IS A VALID KEYWORD.
PAG3101I LINE 00014 POS01 >...IKED IS VALID APPLICATION NAME.
PAG3001I LINE 00016 POS02 >...Procname IS A VALID KEYWORD.
PAG3101I LINE 00016 POS02 >....POLPROC IS VALID PROCEDURE NAME.
PAG3001I LINE 00018 POS03 >..AppName IS A VALID KEYWORD.
PAG3101I LINE 00018 POS03 >...TRMD IS VALID APPLICATION NAME.
PAG3001I LINE 00020 POS04 >..TcpImageName IS A VALID KEYWORD.
PAG3101I LINE 00020 POS04 >....TCPIP1 IS VALID SYSTEM/IMAGE NAME.
PAG3001I LINE 00022 POS05 >...Procname IS A VALID KEYWORD.
PAG3101I LINE 00022 POS05 >....POLPROC IS VALID PROCEDURE NAME.
PAG3001I LINE 00023 POS06 >...Jobname IS A VALID KEYWORD.
PAG3101I LINE 00023 POS06 >....TRMD1 IS VALID JOB/TASK NAME.
PAG3001I LINE 00025 POS07 >..TcpImageName IS A VALID KEYWORD.
PAG3101I LINE 00025 POS07 >....TCPIP3 IS VALID SYSTEM/IMAGE NAME.
PAG3001I LINE 00027 POS08 >...Procname IS A VALID KEYWORD.
PAG3101I LINE 00027 POS08 >....POLPROC IS VALID PROCEDURE NAME.
PAG3001I LINE 00028 POS09 >...Jobname IS A VALID KEYWORD.
PAG3101I LINE 00028 POS09 >....TRMD3 IS VALID JOB/TASK NAME.
PAG3001I LINE 00028 ENINS * END AUTOMONITORAPPS INSPECTION
|
PAG1008I LINE 00053 BGINS * BEGIN COMMONIDSCONFIG INSPECTION
PAG3108I LINE 00053 FILES >../u/paul/samples/pagent_IDS.conf
```

```
PAG3208I LINE 00053 VALID >...SUCCESS - 636 RECORDS FOUND
PAG3008I LINE 00053 ENINS * END COMMONIDSCONFIG INSPECTION
|
PAG1008I LINE 00059 BGINS * BEGIN COMMONIPSECCONFIG INSPECTION
PAG3108I LINE 00059 FILES >../u/paul/samples/pagent_CommonIPSec.conf
PAG3208I LINE 00059 VALID >...SUCCESS - 1212 RECORDS FOUND
PAG3008I LINE 00059 ENINS * END COMMONIPSECCONFIG INSPECTION
|
PAG1008I LINE 00085 BGINS * BEGIN POLICYLOAD INSPECTION
PAG3108I LINE 00085 FILES >../u/user1/pagent.remote.ttls
PAG3208E LINE 00085 ERROR >...FAILURE - NOT FOUND - RC=4
PAG3008I LINE 00085 ENINS * END POLICYLOAD INSPECTION
|
PAG4099I PAGENT STATEMENT PARSING COMPLETE.
```

When the Results Display setting is 'OFF', only Errors and Warnings are displayed in the Inspection Report as shown below:

When Files and/or Datasets cannot be found or located:

```
PAG1008I LINE 00085 BGINS * BEGIN POLICYLOAD INSPECTION
PAG3108I LINE 00085 FILES >../u/user1/pagent.remote.ttls
PAG3208E LINE 00085 ERROR >...FAILURE - NOT FOUND - RC=4
PAG3008I LINE 00085 ENINS * END POLICYLOAD INSPECTION
```

When Statement Referenced by NameValue cannot be resolved:

```
IDS9754I <> IDS REFERENCES THAT ARE NOT RESOLVEABLE TO NAMEVALUE:
|
IDS9755E LINE 00097 IDSActionRef                Attack-action-PAUL
IDS9755E LINE 00211 IDSActionRef                ScanEventLow-action
```

When a configuration contains unknown statements:

```
IDS0906I <> IDETC CONFIGURATION CONTAINS UNKNOWN STATEMENT.
|
IDS0907E IDSActi0n                  ScanEventLow-action
```

When Keywords are unknown:

```
IDS2023E LINE 00285 UNKNW >..IDSActi0n                  ScanEventLow-action
IDS2023E LINE 00287 UNKNW >..ActionTypes                ScanEvent count
```

8.7 *Notice Processing*

The Default setting for Notice Processing is 'OFF'.

When the Notice Processing setting is 'ON', and the Inspection ends with the discovery of Errors or Warnings, only then will an Email or SMS Text be sent in the format shown below:

```
|        -----Inspections----- Statement --------------Results--------------
ALL2010I --------Names-------- --Count--  Err  War  Not  Inf  Unk  Ttls  Cng
ALL2020I Policy Agent Task          8       1    0    0  151    0   210  n/a
ALL2030I Network IPSecurity       140       1    1    0 1836    0  1838  n/a
ALL2040I App Transparent TLS       40       0    0    0  492    0   492  n/a
ALL2050I Intrusion Detection       66       0    1    0  825    0   826  n/a
ALL2060I Policy Based Routing      18       0    0    0  210    0   210  n/a
ALL2070I ---------------------  -------  ---- ---- ---- ---- ---- ----- ----
ALL2080E --------Total--------    272       2    2    0 3514    0  3518  n/a
|
ALL0000I         Full Finding:IFO.TEST.$PGN.RPTS.$ADCD23C($8121812)
```

To activate Notice Processing, the additional step of defining a notification Action Block in the ICE Parmlib Member NSEENSxx is necessary. A sample is shown below:

```
ACTION DETECTOR(PAGENTCHECK) METHOD(EMAIL) SCOPE(REPORT)
TO PRR@NEWERA.COM
TO PAT@NEWERA.COM
FROM SUPPORT@NEWERA.COM
SUBJECT 'PAGENT FINDINGS'
ACTION .END
```

In addition, this Action Block must be paired with an NSEENSxx Method Block. If you have questions about activating notification, NewEra Technical Support will assist in setting up the needed controls components.

8.8 Baseline Processing

The PAGENT Inspector may also be used to maintain a Baseline of the Policy Agent configuration definitions, comparing them with the configuration discovered during - background, batch, or full foreground - inspections in order to detect configuration changes. The default setting for Baseline Processing is 'ON'.

When Baseline Processing is 'ON', a baseline PDSE Dataset is allocated using the following naming convention:

```
ice_hlq.$PGN($IKD,$NSS,$DMD,$TRM).BASE.$image_name
```

The members in the Baseline Dataset may represent both static (FIXED) members and dynamic (MOVING) members that will be used for detecting configuration changes. The single fixed member is named $BSELINE. Dynamic member names are assigned using the format $YMMDDHH, where Y = the last digit of the current year, MM = digits representing the current month, DD = digits representing the current day of the current month, and HH = digits representing the current hour of the current day.

8.8.1 The Baseline File

Each Baseline File is identified by System, Time, Date, and Update UserId as shown in the sample below:

```
PAGENT CONFIGURATION BASELINE:
LAST UPDATE ON SYSTEM=ADCD23C AT=12:26:58 ON=Y18/M12/D06 BY=PROBI1

-------ATTLS CONFIGURATION STATEMENTS, NAMES, KEYWORDS & VALUES-------
ATT.+.TTLSGroupAction               grp_Production
ATT.|..TTLSEnabled                   On
ATT.|..Trace                         2
ATT.+.TTLSGroupAction               grp_StartUp
ATT.|..TTLSEnabled                   On
ATT.|..Trace                         6
ATT.+.TTLSGroupAction               grp_Diagnostic
ATT.|..TTLSEnabled                   On
ATT.|..Trace                         30
ATT.+.TTLSEnvironmentAction         Generic_Server_Env
ATT.|..HandshakeRole                 Server
ATT.|..TTLSKeyRingParms              <No_Parm>
```

```
ATT.|..Keyring                        Server_Ring
ATT.+.TTLSRule                       Secure_Ftp_client
ATT.|..LocalPortRange                 21
ATT.|..Direction                      Outbound
ATT.|..TTLSGroupActionRef             grp_Production
ATT.|..TTLSEnvironmentActionRef       Secure_Ftp_Client_Env
ATT.+.TTLSRule                       Secure_Ftpd
```

When Baseline Processing is 'OFF', no baseline file is created. However, if baselines exist when processing is turned off, they will persist in the Baseline Dataset.

8.8.2 The Baseline Change Report

The following is a sample Change Report:

```
PAGENT CONFIGURATION CHANGES:
THIS UPDATE ON SYSTEM=ADCD23C AT=12:26:58 ON=Y18/M12/D06 BY=PROBI1

CONFIGURATION CHANGES WERE DETECTED AFTER:
LAST UPDATE ON SYSTEM=ADCD23C AT=12:24:37 ON=Y18/M12/D06 BY=PROBI1

----------CHANGES DETECTED BETWEEN BASELINE DATES SHOW ABOVE----------

<> PRIME CONFIGURATION STATEMENTS, NAMES, KEYWORDS & VALUES.

STATEMENTS ADDED:
NO STATEMENTS ADDED.

STATEMENTS DELETED:
NO STATEMENTS DELETED.

STATEMENTS CHANGED:
+.AutoMonitorApps
Del|..AppName                        IKED-dallas
Add|..AppName                        IKED

<> IPSEC CONFIGURATION STATEMENTS, NAMES, KEYWORDS & VALUES.

STATEMENTS ADDED:
+.KeyExchangePolicy
|..KeyExchangeRuleRef           Admin KeyExRule1
|..KeyExchangeRuleRef           ZoneA KeyExRule1
|..KeyExchangeRuleRef           ZoneB KeyExRule1
|..KeyExchangeRuleRef           ZoneC KeyExRule1
|..KeyExchangeRuleRef           ZoneN KeyExRule1

STATEMENTS DELETED:
NO STATEMENTS DELETED.

STATEMENTS CHANGED:
+.IpFilterPolicy
Add|..FilterLogging                  on
Add|..AllowOnDemand                  no
Add|..IpFilterGroupRef               Admin
Add|..IpFilterGroupRef               ZoneA

<> ATTLS CONFIGURATION STATEMENTS, NAMES, KEYWORDS & VALUES.

NO STATEMENT, KEYWORD OR VALUE CHANGES DETECTED.

<> IDETC CONFIGURATION STATEMENTS, NAMES, KEYWORDS & VALUES.

NO STATEMENT, KEYWORD OR VALUE CHANGES DETECTED.

<> ROUTE CONFIGURATION STATEMENTS, NAMES, KEYWORDS & VALUES.

NO STATEMENT, KEYWORD OR VALUE CHANGES DETECTED.
```

9 Reporting Problems

Any problem, real or suspected, should be immediately reported to NewEra Technical Support, support@newera.com. In doing so, consider what your support team might need to move things along quickly.

9.1 What Support May Need

- A copy of the full Inspection Report if any was produced.
- A screen of any offending Panel or displayed message.
- A copy of the related configuration file, if possible.
- If a Health Check issue, a copy of the IPLCHECK SYSTSPRT.
- If a Workbench issue, a copy of the IFO Started TASK.

The PAGENT and DAEMON Inspectors are configured as ReXX applications designed to run specifically in the NewEra Integrity Controls Environment (ICE). As such, as problems are reported and resolved, you will have the option to receive an update that may be installed immediately, not having to wait for the next formal patch.

9.2 Immediate Updates

If you do elect to receive an immediate update, it will come as a TEXT file Email Attachment. To install the update, take control of the file by saving it to your desktop, then allocate at least a two meg sequential dataset – your_userid.inspector_name.

Inspector_names include:

- `XIPAGNT`
- `XIIKED`
- `XINSSD`
- `XIDMD`
- `XITRMD`

Next, move (FTP) the file to your mainframe host in BINARY using the newly allocated file as the target. Finally, rename the file from your_userid.inspector_name to simply the inspector_name and then copy the renamed, uploaded file to hlq.SISPCLIB.

Please Email or TEXT support of your post-update findings.

10 Technical Support Contact Information

NewEra Software, Inc.

Mailing Address:

18625 Sutter Boulevard, Suite 950
Morgan Hill, CA 95037

Phone:

(408) 520-7100
(800) 421-5035

Text:
669-888-5061

FAX:

(888) 939-7099

Email Address:

support@newera.com

Web Site:

https://www.newera.com

Technical Support:

24 hours a day, 7 days a week
1-800-421-5035
support@newera.com