SHARE
Technology • Connections • Results

Automating enterprise systems management: Your day (and night) just got easier

Larry Green
IBM

Thursday, March 3, 2011
Session 8234

SHARE in Anaheim 2011

Agenda

- Why automate?
- Message and Event Automation
- Message Revision
- Command Revision
- Timers
- Intrusions

Why Automate?

- Maximize availability
  - Avoid / minimize outages and incidents (and 2:00 AM phone calls)
  - Assist operators in detecting / resolving incidents
  - Identify and deal with recurring incidents
  - Improved resiliency
- Customer sat
- Improve operational efficiency and performance of IT assets and staff
  - Ensure consistent handling of incidents
  - Streamline routine tasks
  - Standardize procedures: consistent handling of complex tasks
  - Reduced potential for user error
  - Avoid / limit staff increases
  - Reduce recovery time and required operator intervention

- Key to
  - Systems / network management process implementations
  - Business processes

Report Automation Benefits

- Blow your own horn
- Automation becomes the norm …
  - And people forget about it
- Quality and availability improvements
- Valuable IT tool for improving profitability and competitiveness
- Cost savings achieved with automation, such as:
  - Incidents and outages avoided
  - Hours saved
  - Reduced human intervention
  - Whenever possible, include $$$
- Understand cost of automation vs. cost of manual process
  - Resource usage, staff, software/hardware, time to accomplish process, etc.

Report Automation Benefits

- Examples
  - Jobs cancelled to avoid an outage
  - Automated notification of abnormal situations
  - Resources recovered by automation
  - Buffers recovered to avoid an outage
  - Subsystem recoveries
  - Reduction in message traffic

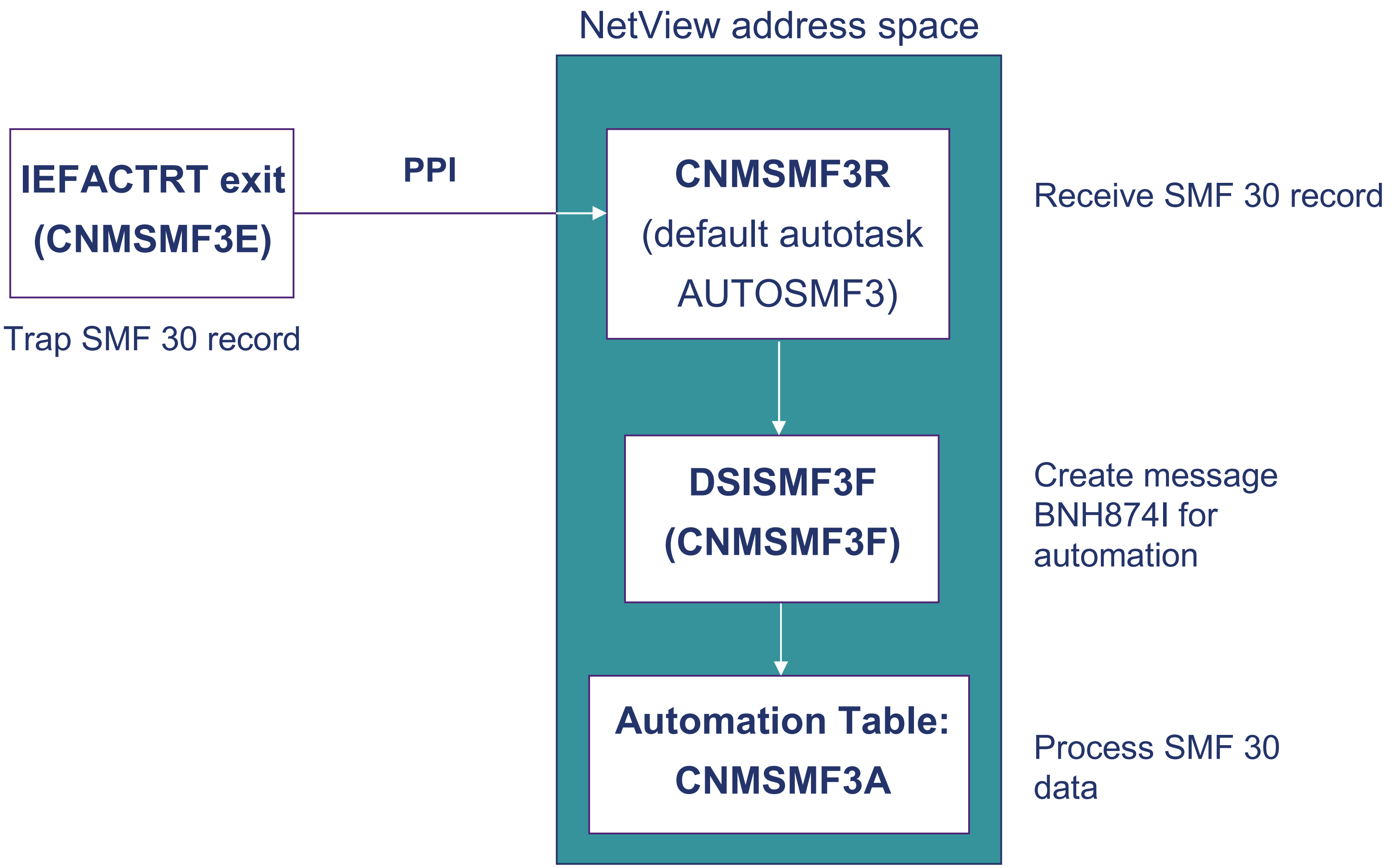
Agenda

- Why automate?
- Message and Event Automation
  - Job / job step termination
  - Job execution problems
  - Traps
- Message Revision
- Command Revision
- Timers
- Intrusions

Job / job step termination

- Automated response to job and job step termination
- Faster, more consistent handling, whether normal termination or abend
- Automation enablement for SMF type 30 records

Automation Flow



NetView address space

IEFACTRT exit (CNMSMF3E)

Trap SMF 30 record

PPI

CNMSMF3R (default autotask AUTOSMF3)

Receive SMF 30 record

DSISMF3F (CNMSMF3F)

Create message BNH874I for automation

Automation Table: CNMSMF3A

Process SMF 30 data

Message BNH874I

BNH847I SMF RECORD RECEIVED: data

- Two-line message created by CNMSMF3R when an SMF30 record is received.
- Intended for automation
- First line includes
  - Record type
  - Record subtype
  - Work type indicator (e.g., STC, TSO)
  - Date/time when record was moved to SMF buffer
  - Address space ID of source
  - Subtype identification (e.g., step total, job ended)
  - Subsystem name
  - Program name
  - Step name
  - Step completion code
  - Termination indicator
  - Abend code
  - (more)
- Second line
  - SMF 30 record itself
  - Available to automation
  - Not logged or displayed
  - Truncated at 32000 characters

Agenda

- Why automate?
- Message and Event Automation
  - Job / job step termination
  - Job execution problems
  - Traps
- Message Revision
- Command Revision
- Timers
- Intrusions

Job execution problems

- Tivoli Workload Scheduler
  - Plan / execute jobs, track execution
  - Generate alerts to NetView when problems are detected in production workload, such as:
    - An operation ends in error
    - A batch job has been queued by JES for a long time
    - A batch job or started task has been running longer than expected
    - Processing is getting late and deadlines are in jeopardy
    - A Tivoli Workload Scheduler for z/OS subtask fails
    - A defined threshold has been reached on the Tivoli Workload Scheduler for z/OS queue
    - Jobs above a certain priority are late
    - A workstation that has been unavailable/failed for more than xx minutes becomes available

Job execution problems

- Leverage NetView automation facilities
  - Automation Table
    - Trap TWS messages
    - Trigger responses
    - Issue commands
  - Send a one-line e-mail (EZLESMTP)
  - Send e-mail (EZLEMAIL)
  - Generate an immediate action based on policy. Specify person or group to contact, optionally specify message text (INFORM)

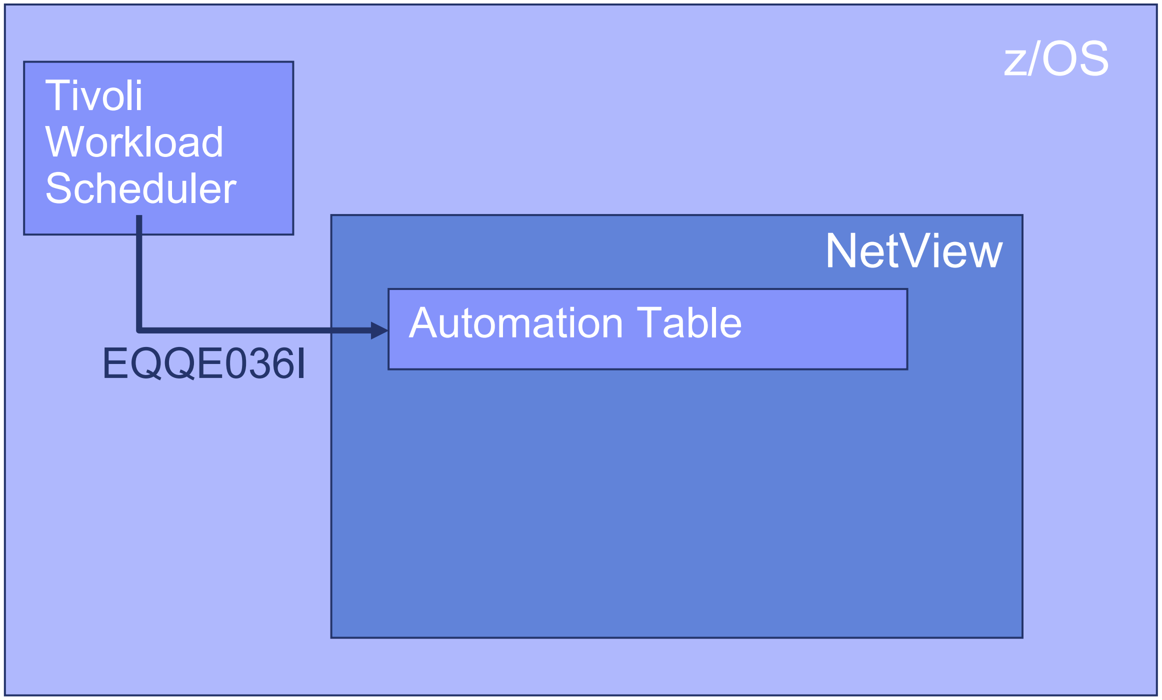
Example: operation ended in error status

The setting

Job TWSEXTCP ended with error 0012

TWS issues message EQQE036I:

```
EQQE036I JOB TWSEXTCP(JOB04259), OPERATION(0020), ENDED IN ERROR 0012
PRTY=9, APPL = DAILYPLAN, WORK STATION = CPU1, IA = 0501180700
```



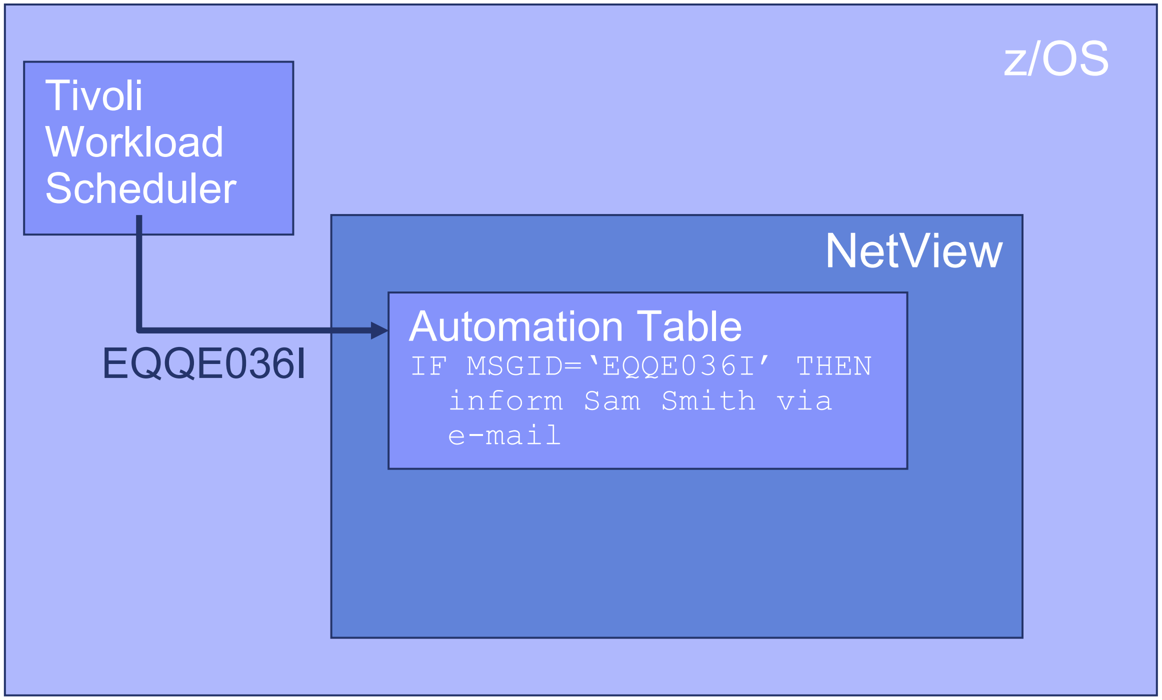
Example: operation ended in error status

The setting

Job TWSEXTCP ended with error 0012

TWS issues message EQQE036I:

```
EQQE036I JOB TWSEXTCP(JOB04259), OPERATION(0020), ENDED IN ERROR 0012
PRTY=9, APPL = DAILYPLAN, WORK STATION = CPU1, IA = 0501180700
```



```
IF MSGID='EQQE036I' THEN
  inform Sam Smith via
  e-mail
```

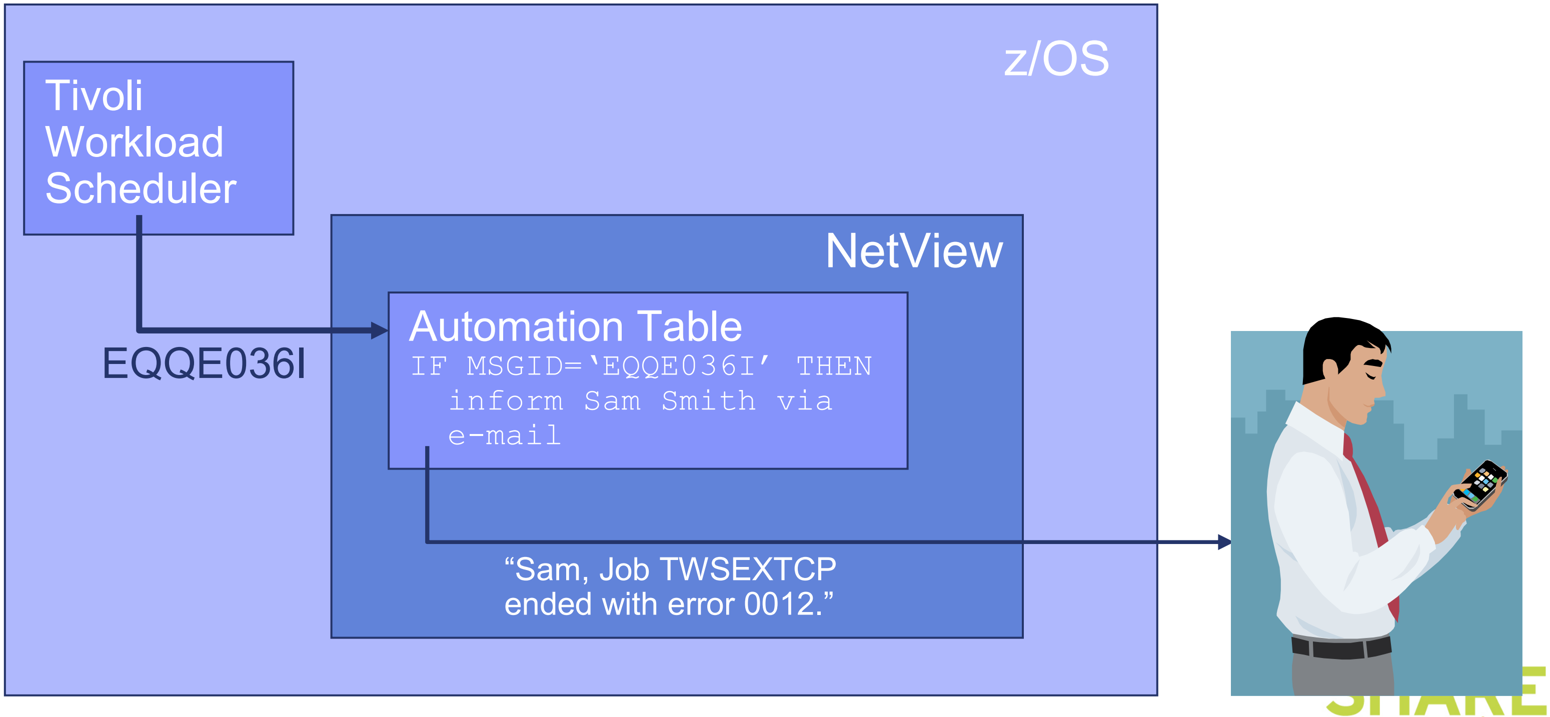
Example: operation ended in error status

The setting

Job TWSEXTCP ended with error 0012

TWS issues message EQQE036I:

```
EQQE036I JOB TWSEXTCP(JOB04259), OPERATION(0020), ENDED IN ERROR 0012
PRTY=9, APPL = DAILYPLAN, WORK STATION = CPU1, IA = 0501180700
```



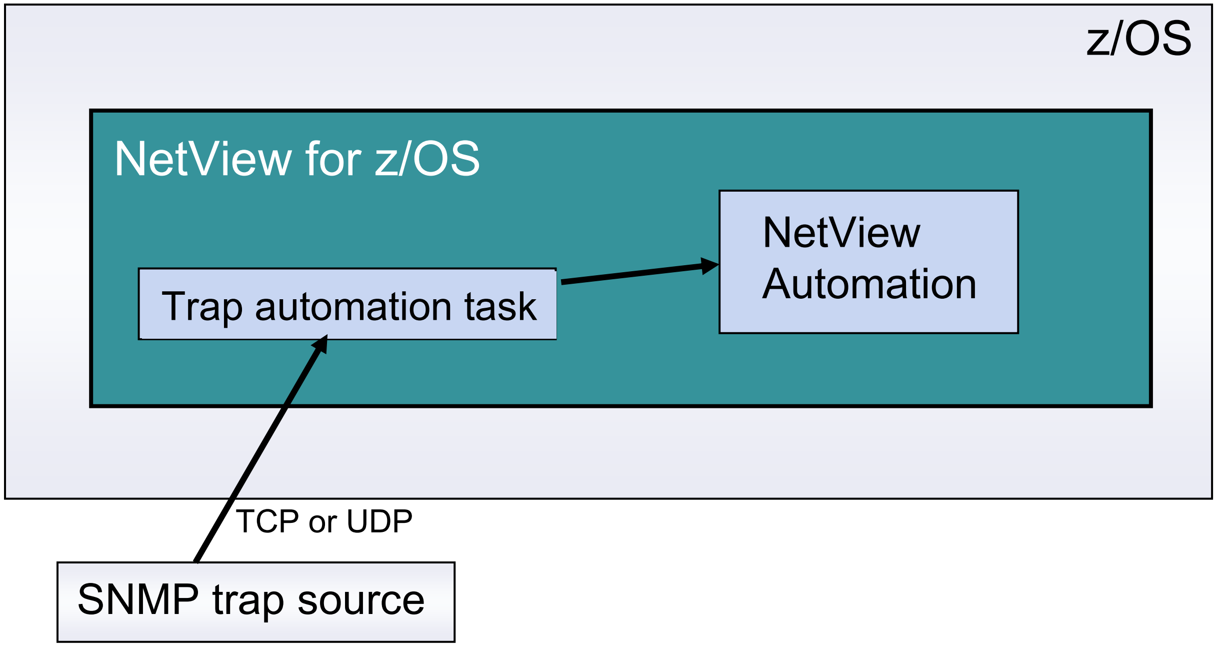
```
IF MSGID='EQQE036I' THEN
  inform Sam Smith via
  e-mail
```

"Sam, Job TWSEXTCP ended with error 0012."

Agenda

- Why automate?
- Message and Event Automation
    - Job / job step termination
    - Job execution problems
    - Traps
- Message Revision
- Command Revision
- Timers
- Intrusions

Trap Automation



v1, v2c or v3 trap

Agenda

- Why automate?
- Message and Event Automation
- Message Revision
- Command Revision
- Timers
- Intrusions

Why revise a message?

- Attract attention: change color
- Append text
- Customize response according to originating system
- Suppress the message
- Override MPF

Change message color

- Operators sometimes overlook an important message
- Call attention to it:

```
UPON (MSGID = 'IEA404A'   ! SEVERE WTO BUFFER SHORTAGE - 100% FULL
| MSGID = 'IRA200E')      ! AUXILIARY STORAGE SHORTAGE
      REVISE ("cr hr" color)    ! Change color to red with
                                ! reverse video
      …
```

```
IEA404A SEVERE WTO BUFFER SHORTAGE - 100% FULL
```

becomes

```
IEA404A SEVERE WTO BUFFER SHORTAGE - 100% FULL
```

Append text

- Continuing with previous messages …

```
UPON (MSGID = 'IEA404A'     ! SEVERE WTO BUFFER SHORTAGE - 100% FULL
| MSGID = 'IRA200E')        ! AUXILIARY STORAGE SHORTAGE
      REVISE ("cr hr" color)      ! Change color to red with
                                  ! reverse video
      REVISE('11xx0xxx' FLGRTCD1 ! send to Rt Cd 1,2 but not 4 ...
      1.* 1 “Call me @ 555-1234") ! and add my phone number to text
      ...
```

IEA404A SEVERE WTO BUFFER SHORTAGE - 100% FULL Call me @ 555-1234

Customize response, depending on source

```
UPON (MSGID=‘abc123e’)
  SELECT
      WHEN (SYSNAME=‘xyz’)
      …
      OTHERWISE
      …
  END
UPON (PREFIX=‘IEE’)
  SELECT
      WHEN (SYSNAME=‘xyz’)
      …
      OTHERWISE
      …
  END
```

Suppress a broadcast message

- An operator has broadcast a message to everyone:

```
    Hey guys. I just found the MSG ALL command. It’s cool!
```

- Intercept, suppress

```
    UPON (OTHERMSG)
      SELECT
        WHEN (broadcast YESNO = ‘Yes’)
         NETVONLY                          ! Send message to NetView, but
                                           ! suppress from display, logging &
                                           ! sysplex routing.
        WHEN …
      END
```

- Tell him/her “Don’t do that!”
  - From NetView Automation Table:
    - Issue WTO back to operator: “`Don’t broadcast messages to everyone.`”

Override Message Processing Facility (MPF)

- MPF says `AUTO(NO)` for message ABC123I
- But you’ve decided you do need to automate

```
UPON (MSGID=“ABC123I”)
     REVISE (‘Y’ AUTOMATE)
     …
```

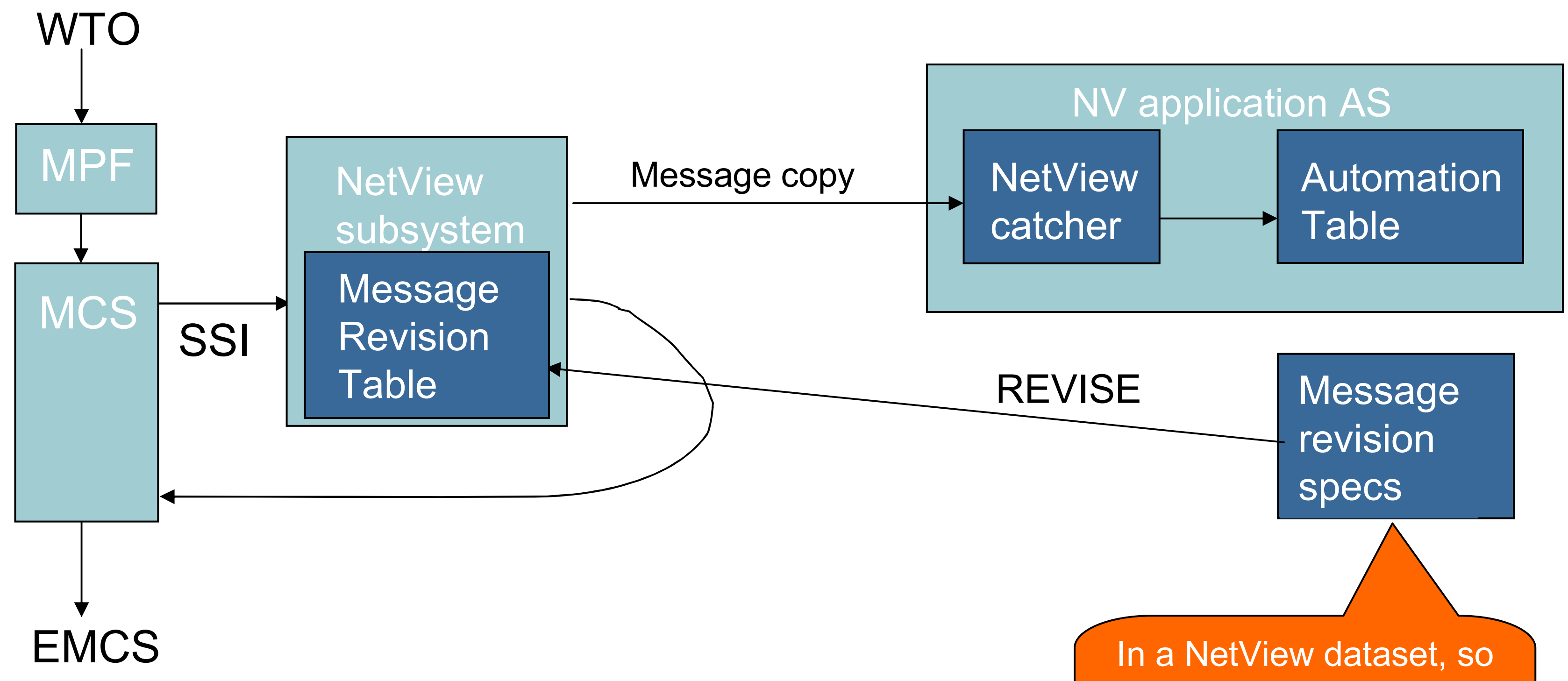
What else can I do?

- Change
  - Text
  - Text case (upper, lower)
  - Color
  - Console
  - Route codes
  - Descriptor codes
  - Broadcast
  - Display
  - Syslog
  - AMRF
  - Data type: C2D, C2B, C2X, D2C, D2X, X2C
  - more
- Handle messages from other LPARs
- Get usage reports
  - Statistics and usage information about active revision table
  - How many messages processed?
  - How many hits in each category?
  - How many deletions?
  - more

What else can I check for?

- All WQE bits
- Locate within a message (right, left, substring, skipto, up to, next, etc.)
- Address space ID
- Domain
- Time
- Character positions

Message Revision: Where It Happens



In a NetView dataset, so you don't have to ask for update to SYS1.PARMLIB

Agenda

- Why automate?
- Message and Event Automation
- Message Revision
- Command Revision
- Timers
- Intrusions

Why revise a command?

- Automatically revise command text in-line before execution
- For all MVS commands: change, reject, or transfer to NetView
- Suppress a broadcast
- Suppress a sensitive command
- Require confirmation

Suppress a broadcast command

An operator has broadcast a command to all systems.

```
UPON (ALLCMD)                              ! This applies even to console ROOT
  SELECT
    WHEN (CMDVERB ¬= 'SEND')
```

* The above means that the following is only for the SEND command.

```
    WHEN (SKIPTO /USER=/ 1 FOUND ¬= 'Yes') ! default = "ALL"
      WTO(“XYZ447E Please do not broadcast to all.")
      REVISE('Y' DELETE)                   ! disallow default
    OTHERWISE
   END
```

Suppress a sensitive command

A sensitive command has been entered.

Only consoles having Master authority are allowed to execute that command.

```
UPON (CMDVERB = 'SENSITIVE')     ! Sensitive command
  SELECT
    WHEN (CONSAUTH ¬= ‘M’)        ! Not Master authority
      REVISE('Y' DELETE)          ! Delete command
    OTHERWISE
  END
```

Suppress a sensitive command

The business day has ended.

A sensitive command has been entered from console ABC03.

At this time of day, no one should be using that console.

```
UPON (CMDVERB = 'SENSITIVE')   ! Sensitive command
  SELECT
    WHEN (RVAR(afterhours) yesno 1 CONSNAME left 5 N =
  ‘YesABC03’)
       REVISE('Y' DELETE)
    OTHERWISE
  END
```

Require confirmation

- Operators occasionally shut down a process before it completes creation of a checkpoint.
- Intercept the shutdown command
- Transfer command to NetView Automation Table
  - Issue WTOR to console where the command was issued:
    ```
    Has the checkpoint been created?
    ```
  - If Yes: re-issue command
  - If No: suppress command; tell operator checkpoint must be created.

Command Revision

- Issue message when
  - A command is revised, showing original & revised
  - Unauthorized command revision is attempted
- Test mode
  - Issues a message showing changes that would have been made.

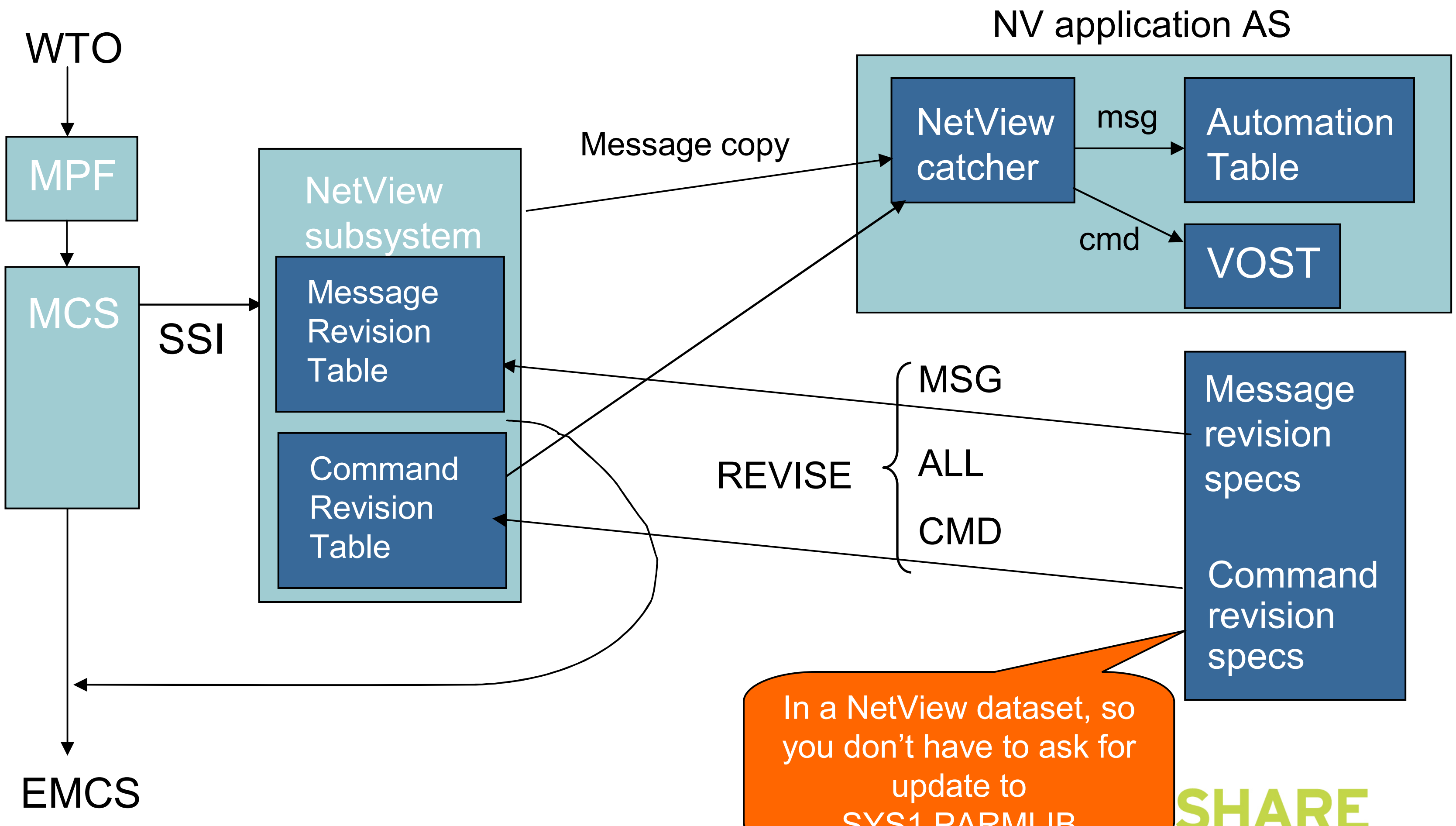
- Sample CNMSCRT1

What else can I check for?

- Name of console issuing command
- Authority of console issuing command
- SAF user identity and/or group name
- Value of first token
- Substrings of the command
- ASID
- Job type (how the address space was started)
- JOBNAME of command originator
- SYSNAME that command originated from
- Locate within a message (right, left, substring, next, etc.)

- Trap all commands
- Trap all other commands

Command Revision: Where It Happens



In a NetView dataset, so you don't have to ask for update to SYS1.PARMLIB

Agenda

SHARE
Technology • Connections • Results

- Why automate?
- Message and Event Automation
- Message Revision
- Command Revision
- Timers
- Intrusions

SHARE in Anaheim 2011

Why timers?

Some actions need to occur at a specified time or at regular intervals:

- At a certain time
- Repeatedly at specified intervals
- After a specified delay
- Complex combinations

At a specified time

```
AT 12/24 18:00:00,ID=EVESAVE,SAVE,STOPSYS
```

schedules the `STOPSYS` command list to shut down the system at 6:00 p.m. on December 24 and saves the command in the Save/Restore database

Repeatedly at specified intervals

```
EVERY 01:00:00,ID=CHEKST,CHEKSTAT AUTOVTAM
```

schedules the `CHEKSTAT` command list to run every hour, starting one hour after the timer command is run

After a specified delay

```
AFTER 00:05:00,ID=DISPSTAT,MVS D A,L
```

schedules the “MVS D A,L” command to be issued after 5 minutes to solicit status information about system elements

Complex combinations of factors

```
CHRON AT=(08:00:00) EVERY=(INTERVAL=(01:00:00
  OFF=17:00:00) REMOVE=(12/31/11 00:00:00)
  DAYSWEEK=(WEEKDAY) CALENDAR=(NOT HOLIDAY))
  COMMAND=LOGTSTAT ROUTE=PPT
```

issues the `LOGTSTAT` command once every hour from 8:00 a.m. until 5:00 p.m. on all weekdays except holidays, from now until the last day of the year 2011. The `LOGTSTAT` command runs on the PPT task. If this CHRON is entered between 8:00 A.M. and 5:00 P.M., `LOGTSTAT` runs at the next hour. This enables you to specify a shift for following days and have a partial shift run today.

How to use timers

Use timers

- Directly
- In other automation
- In command lists
- In command processors

Agenda

- Why automate?
- Message and Event Automation
- Message Revision
- Command Revision
- Timers
- Intrusions

TCP/IP Intrusions

- What is an intrusion?
  - Information gathering (scan)
    - Network and system information
    - Data locations
    - Map target of an attack
  - Eavesdropping, impersonation, or theft
    - On the network, on the host
    - Base for further attacks on others
  - Denial of Service
    - Attack on availability
- Intrusions can occur from Internet or Intranet
  - Firewall can provide some level of protection from Internet
  - Perimeter security strategy *alone* may not be enough
  - Within a firewall, systems can be vulnerable to attack or misuse, whether accidental or malicious.

TCP/IP Intrusions

- z/OS Communications Server Intrusion Detection Service (IDS) detects:
  - Scans
    - Fast
    - Slow
    - ICMP, TCP UDP
  - Attacks
    - Malformed packets
    - IP option restrictions
    - ICMP redirect restrictions
    - Outbound raw socket restrictions
    - And more …
  - Floods

Intrusion Event

- IDS issues message(s) to system console or USS syslog for IDS events

system console

```
EZZ8761I IDS EVENT DETECTED
EZZ8762I IDS EVENT TYPE: SUSPICIOUS PACKET RECEIVED
EZZ8763I CORRELATOR 4 – PROBEID 04030001
EZZ8764I SOURCE IP ADDRESS 10.10.11.199 – PORT 0
EZZ8765I DESTINATION IP ADDRESS 197.11.106.1 – PORT 0
EZZ8766I IDS RULE prIDS-FRG1
EZZ8767I IDS ACTION paIDS-FRG1
```

syslog

```
EZZ8648I TRMD ATTACK packet was discarded:09/21/2004 09:30:19.66,
sipaddr=10.10.11.199, dipaddr=197.11.106.1, sport=0, dport=0, type=malformed,
proto=TCP, correlator=4, probeid=04030001
```

This tells us what we need to know:

- ProbeID (the type of intrusion – this one is an Attack Detection event).
- Source IP address (address of intruder)
- Destination IP address (address of target stack)

Intrusion Event

- A NetView clist listens for syslog updates, and issues an internal message for automation.

```
BNH180I INTRUSION DETECTION MESSAGE RECEIVED Sep 21 09:30:20.22
MVS118/USER1  USER16  TRMD.TCPCS[27M: EZZ8648I TRMD ATTACK packet
was discarded:09/21/2007 09:30:19.66, sipaddr=10.10.11.199, dipaddr=197.11.106.1,
sport=0, dport=0, type=malformed, proto=TCP, correlator=4, probeid=04030001
```

Automated Actions

- Notify
  - e-mail to designated recipient (e.g., security administrator)
  - Alert to NetView (default)
  - Message to designated NetView operators (default)
- Issue UNIX, z/OS, or NetView commands
  - Gather more data
  - Take action, such as close the port
- Update statistics kept on basis of probe ID
- Collect additional statistics
  - Generate *trmdstat* reports and e-mail to security administrators

Thank You!