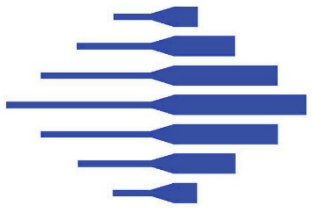


VELOCITY SOFTWARE

Automated Operations with the Velocity Performance Suite (zVPS)

Tim Kessler

VELOCITY SOFTWARE

Automated operations using:

- **zOPERATOR**
- **zAlert**

zOPERATOR

- Console and automations manager
- No charge component of zVPS
- Scrollable, searchable console display
- Messages can be:
  - Colored, highlighted, held, suppressed, message to a user, written to file, execute command, emailed or SNMP trap sent
- Log files kept for user specified days
- Can be used on OPERATOR or any other user
- Integrated with zMON
- Linux messages
  - Console, syslog

```
GRAF L0005 LOGON  AS  ZVPS     USERS = 34    FROM 192.168.5.78
GRAF L0005 LOGOFF AS  ZVPS     USERS = 33
19:35:11  * MSG FROM ZALERT  : SPOL Spool space is 72% used
LINUX001: Jan  9 21:45:17 linux001 syslog-ngÝ1334¨: STATS: dropped 0
HCPMXE6224I Event recording is pending because there are no users connected to *
MONITOR for this type of data.
HCPMXE6224I Sample recording is pending because there are no users connected to *
MONITOR for this type of data.
 DVHRLY3886I Hourly processing started; with 0 log
 DVHRLY3886I files.
 DVHRLY3886I Hourly processing started; with 0 log
 DVHRLY3886I files.
 DVHRLY3886I Hourly processing started; with 0 log
 DVHRLY3886I files.
 DVHRLY3886I Hourly processing started; with 0 log
 DVHRLY3886I files.
 ICH408I USER(TIMK    ) GROUP(DEMO    ) NAME(####################)
 LOGON/JOB INITIATION - INVALID PASSWORD ENTERED AT TERMINAL 98086472
GRAF L0003 DISCONNECT  TIMVPS   USERS = 33
GRAF L0003 RECONNECT   TIMVPS   USERS = 33   BY TIMK     FROM 152.8.100.114
 ICH408I USER(VSIMAINT) GROUP(GROUP1   ) NAME(####################)
 LOGON/JOB INITIATION - INVALID PASSWORD ENTERED AT TERMINAL 98086472

                                                    HOLDING   VSIVM4
```

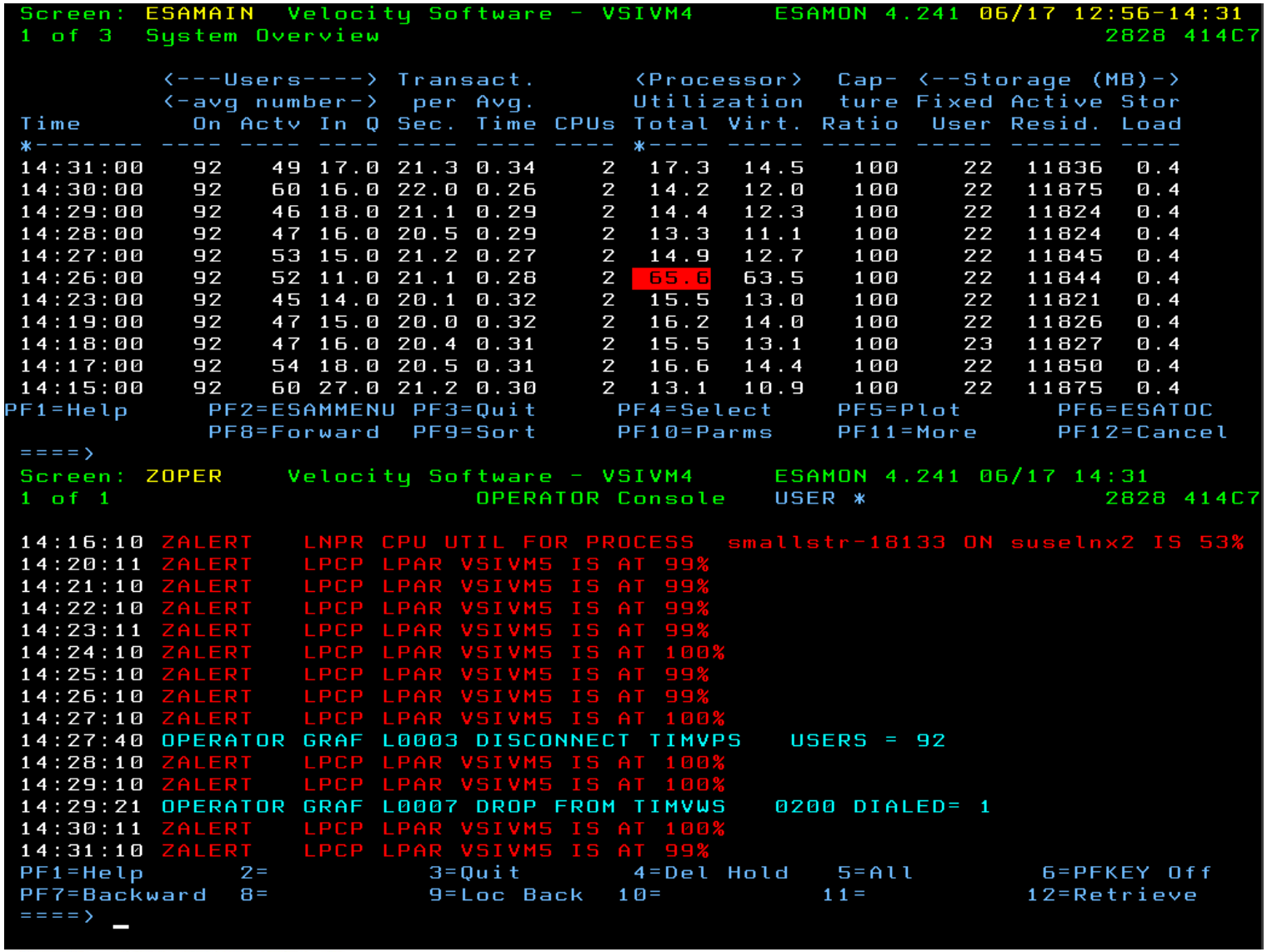
VELOCITY SOFTWARE

zOPERATOR

```
Screen: ZOPER    Velocity Software - VSIVM4     ESAMON 4.300 01/06 12:58
1 of 1                        OPERATOR Console   USER *              2828 0414C7

11:00:04 S11S2ORA -- MARK --
11:04:10 ZALERT   VMCP SLES12 RUNNING AT 23.4%
11:05:16 SUSELNX2 linux9s sshdÝ10518¨: fatal: Timeout before authentication for
                   ::ffff:116.31.116.11
11:06:10 ZALERT   LNPR CPU UTIL FOR PROCESS  smallstr-10673 ON suselnx2 IS 46%
11:06:46 SUSELNX2 linux9s sshdÝ10668¨: fatal: Timeout before authentication for
                   ::ffff:116.31.116.11
11:12:10 ZALERT   VMCP SLES12 RUNNING AT 22.3%
11:12:11 ZALERT   LNPR CPU UTIL FOR PROCESS  stresser-2795 ON sles12 IS 100%
11:12:11 ZALERT   LNPR CPU UTIL FOR PROCESS  stresser-3168 ON sles12 IS 99%
11:20:04 S11S2ORA -- MARK --
11:24:10 ZALERT   VMCP SLES12 RUNNING AT 21.4%
11:29:25 SUSELNX2 linux9s sshdÝ12589¨: fatal: Timeout before authentication for
                   ::ffff:116.31.116.11
11:36:11 ZALERT   LNPR CPU UTIL FOR PROCESS  smallstr-13245 ON suselnx2 IS 44%
11:40:04 S11S2ORA -- MARK --
11:44:06 OPERATOR GRAF L0009 LOGON  AS  TDNVSI   USERS = 92    FROM 50.193.31.1
                  29
11:44:26 OPERATOR GRAF L000A LOGON  AS  ZVPS     USERS = 93    BY TIMK     FROM
                   64.128.170.6
11:48:44 OPERATOR GRAF L0007 RECONNECT  ZADMIN   USERS = 93    BY TDNVSI   FROM
                   50.193.31.129
12:00:00 OPERATOR HCPMXE6224I Event recording is pending because there are no u
                  sers connected to *MONITOR for this type of data.
12:00:00 OPERATOR HCPMXE6224I Sample recording is pending because there are no
                  users connected to *MONITOR for this type of data.
12:00:04 S11S2ORA -- MARK --
12:06:10 ZALERT   LNPR CPU UTIL FOR PROCESS  smallstr-15807 ON suselnx2 IS 44%
12:16:10 ZALERT   LPCP LPAR VSIVM4 CPU Utilization is 94%
12:20:04 S11S2ORA -- MARK --
12:36:11 ZALERT   LNPR CPU UTIL FOR PROCESS  smallstr-18410 ON suselnx2 IS 47%
12:38:11 ZALERT   LNPR CPU UTIL FOR PROCESS  stresser-2795 ON sles12 IS 699%
12:38:11 ZALERT   LNPR CPU UTIL FOR PROCESS  stresser-3168 ON sles12 IS 680%
12:38:11 ZALERT   LNPR CPU UTIL FOR PROCESS  stresser-3502 ON sles12 IS 28%
12:40:05 S11S2ORA -- MARK --
12:53:42 OPERATOR GRAF L0003 DIALED TO OPERATOR 0100 DIALED= 2     FROM 192.168
                  .5.75
PF1=Help      2=          3=Quit       4=Del Hold   5=All        6=PFKEY Off
PF7=Backward  8=          9=Loc Back  10=          11=          12=Retrieve
====>
```

VELOCITY SOFTWARE

zOPERATOR

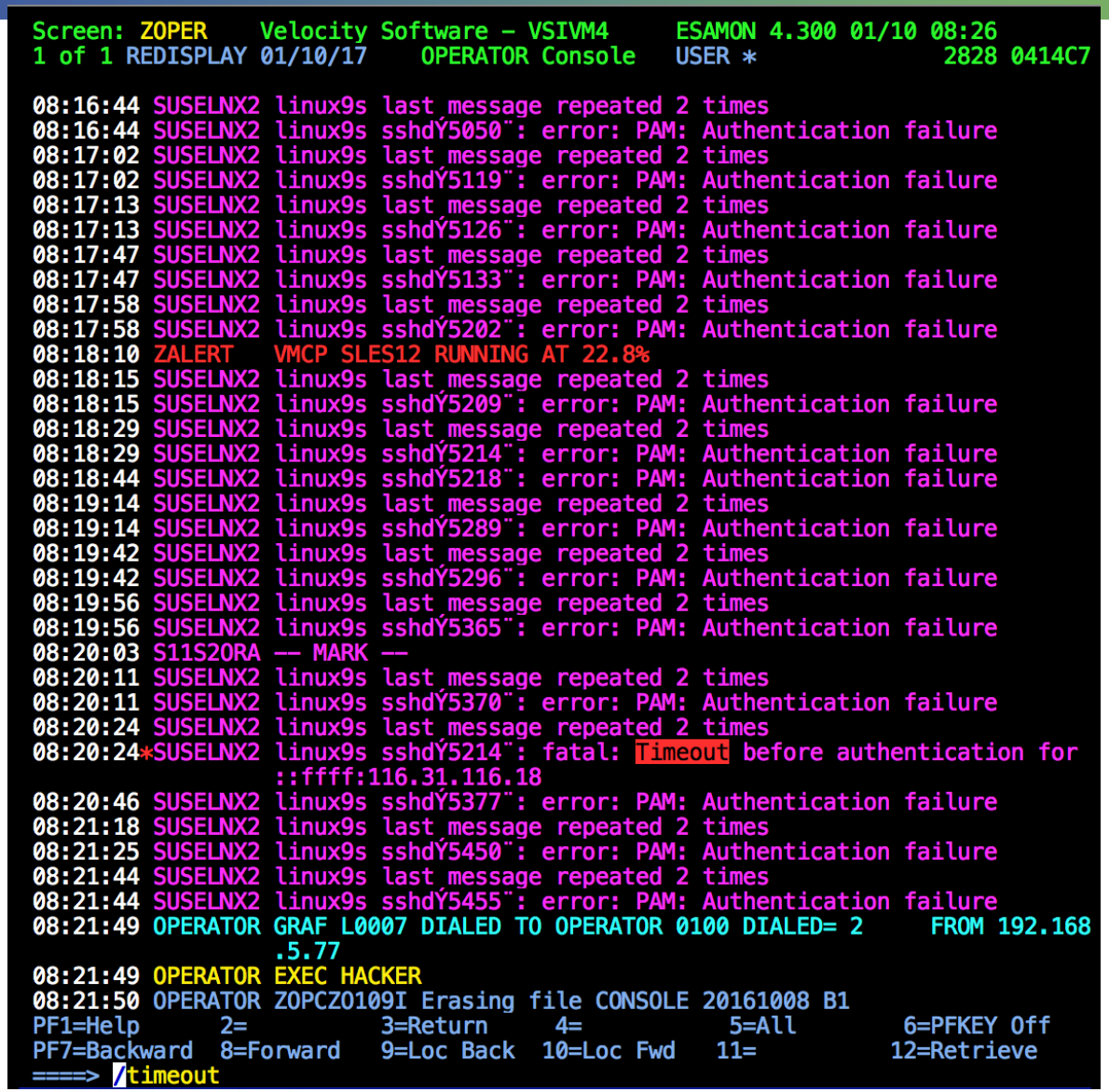


VELOCITY SOFTWARE

Redisplay and searching

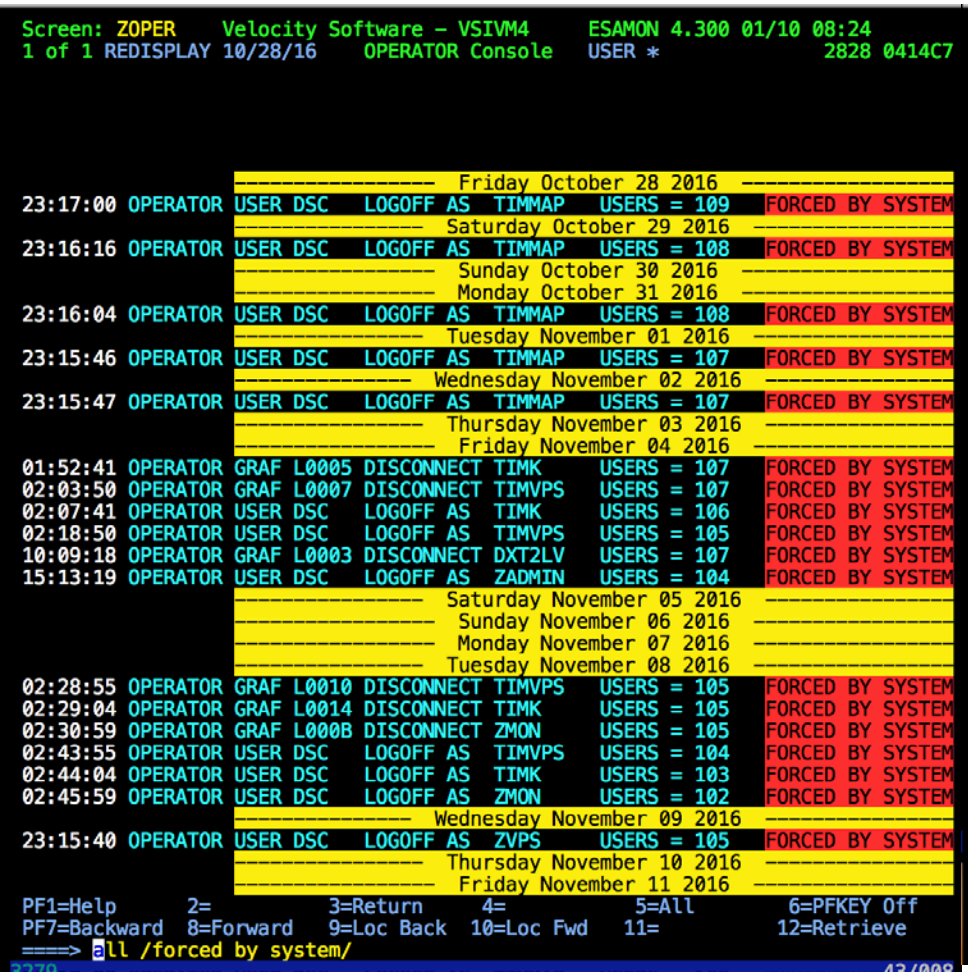
- Page or search forward or backward
- Date and/or time
- Literals
  - Similar to XEDIT: */literal/*
  - Search backwards unless in redisplay mode will continue in same direction
- ALL command
- Multiple targets with & | ¬

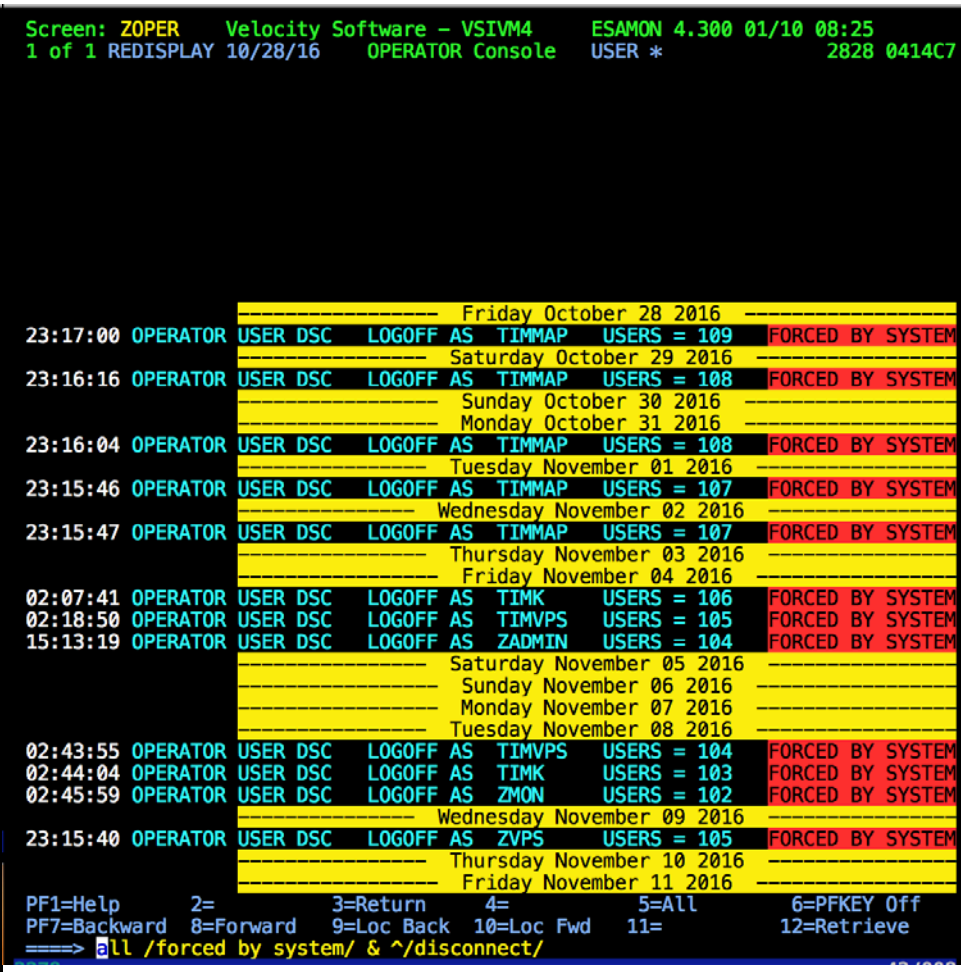
zOPERATOR



VELOCITY SOFTWARE

zOPERATOR





VELOCITY SOFTWARE

Other display options

- Split screen
  - Performance display in one and OPERATOR log in other
- SCALE
  - Useful when creating rules
- ZONE
  - Limit search to specific columns
- PFKEY
  - Control display of PF Keys on screen
- SUPPRESS (redisplay mode)
  - Control display of suppressed messages
- USER
  - ON, OFF, *, ALL, userid1 userid2 … or userid*
- TIME
  - Timestamp display, ON, OFF
- WRAP
  - Control display of long messages

- Customizable PFKEYs
  - zOPERATOR commands
  - Commands with data inserted from command line
- CLEAR key to clear current display

Remote access

- DIAL terminals
  - Option to restrict commands
  - One terminal buffer
  - Terminal size must be less than or equal to original size
- View from another CMS user
- zVIEW web page
  - Automatically updates every 30 seconds
  - Select date and time range
  - Select user(s)
  - zALERT click through

Message rules processing

- Easy online configuration
- Fast and efficient processing
- Unique or common to each zOPERATOR instance

```
                    ZOPER ZOPRULES Configuration

                          zOPERATOR Action Rules
Match:  Msg type CMSOUT User ID ________ Comment zOPERATOR error
        Start col 10    End col 12  = Target ZOP
      & Start col2 19  End col2 19  = Target E
Action: Color RED       Ext highlight REVERSE   Suppress ___ Hold YES Stop ___
        Send to ____________________    Send type ______       Send zSERVE ___
        Cmd ____________________________________ File ____________________
        EMAIL address ____________________________________ SNMP trap ___

Match:  Msg type CPOUT  User ID ________ Comment Log ons
        Start col 30    End col 34  = Target LOGON
      _ Start col2 ___ End col2 ___ _ Target ____________________________
Action: Color GREEN     Ext highlight _________ Suppress YES Hold ___ Stop YES
        Send to ____________________    Send type ______       Send zSERVE ___
        Cmd ____________________________________ File ____________________
        EMAIL address ____________________________________ SNMP trap ___

Match:  Msg type *      User ID ________ Comment DIRMAINT hour process start
        Start col 10    End col *   = Target DVHRLY3886I
      _ Start col2 ___ End col2 ___ _ Target ____________________________
Action: Color GREEN     Ext highlight _________ Suppress YES Hold ___ Stop YES
        Send to ____________________    Send type ______       Send zSERVE ___
        Cmd ____________________________________ File ____________________
        EMAIL address ____________________________________ SNMP trap ___
```

- Match conditions
  - Message Type
    - *, CMD, CMS, CP, MSG, EMSG, IMSG, SMSG, WNG or SECUSR
  - User ID
  - Comment
  - Start column
  - End column
  - Condition
    - Equal/Not equal

- Match conditions
  - Target
  - Optional second condition
    - Connected with & or |

- Actions
  - Color
  - Extended highlighting
  - Suppress
  - Hold
  - Stop
    - Don’t check any additional rules
  - Send to User
    - Send type MSG, SMSG, MSGNOH

- Actions
  - Cmd
    - Invoke command or EXEC
    - Parms passed &1 through &n
      - Word number in message
      - Or &ALL, entire message
  - File
  - Email
    - Email address or @filename.filetype to use a list
  - SNMP trap
- Condense rules view with F9

- zView integration
  - zOperator messages can be viewed via the web
  - Use the zOperator selection under the zMon tab

ZOPER - zOPERATOR Console - DEMO

```
08:18:10 ZALERT   VMCP SLES12 RUNNING AT 22.8%
08:20:03 S11S2ORA -- MARK --
08:20:24 SUSELNX2 linux9s sshd[5214]: fatal: Timeout before authentication for ::ffff:116.31.116.18
08:21:49 OPERATOR GRAF L0007 DIALED TO OPERATOR 0100 DIALED= 2     FROM 192.168.5.77
08:21:50 OPERATOR ZOPCZO109I Erasing file CONSOLE 20161008 B1
08:21:50 OPERATOR ZOPCZO109I Erasing file CONSOLE 20161009 B1
08:21:50 OPERATOR ZOPCZO109I Erasing file CONSOLE 20161010 B1
08:21:50 OPERATOR ZOPCZO109I Erasing file CONSOLE 20161011 B1
08:21:51 OPERATOR GLOBALV SELECT ZOPER PURGE
08:21:57 OPERATOR GLOBALV SELECT ZOPER PURGE
08:21:59 OPERATOR GLOBALV SELECT ZOPER PURGE
08:22:03 OPERATOR GLOBALV SELECT ZOPER PURGE
08:24:10 ZALERT   VMCP SLES12 RUNNING AT 21.3%
08:39:10 ZALERT   VMCP SLES12 RUNNING AT 22.4%
08:40:03 S11S2ORA -- MARK --
08:43:15 SUSELNX2 linux9s last
08:43:15 SUSELNX2  message repeated 2 times
08:44:15 OPERATOR GRAF L0007 DROP FROM OPERATOR 0100 DIALED= 1
08:44:26 OPERATOR GRAF L0004 DIALED TO OPERATOR 0100 DIALED= 2     FROM 192.168.5.77
08:45:10 ZALERT   VMCP SLES12 RUNNING AT 23.1%
08:46:10 ZALERT   LPCP LPAR VSIVM4 CPU Utilization is 94%
08:56:11 ZALERT   LNPR CPU UTIL FOR PROCESS  smallstr-8369 ON suselnx2 IS 46%
08:57:42 SUSELNX2 linux9s sshd[8415]: fatal: Timeout before authentication for ::ffff:116.31.116.18
09:00:00 OPERATOR HCPMXE6224I Event recording is pending because there are no users connected to *MONITOR for this type of data.
09:00:00 OPERATOR HCPMXE6224I Sample recording is pending because there are no users connected to *MONITOR for this type of data.
09:00:03 S11S2ORA -- MARK --
09:06:11 ZALERT   LNPR CPU UTIL FOR PROCESS  smallstr-9250 ON suselnx2 IS 45%
09:06:27 SUSELNX2 linux9s sshd[9173]: fatal: Timeout before authentication for ::ffff:116.31.116.18
09:16:11 ZALERT   LNPR CPU UTIL FOR PROCESS  smallstr-10122 ON suselnx2 IS 42%
09:19:21 OPERATOR GRAF L0007 LOGON  AS  RKSDEV   USERS = 94    FROM 192.168.5.77
09:20:03 S11S2ORA -- MARK --
09:24:33 OPERATOR GRAF L0007 LOGOFF AS  RKSDEV   USERS = 93
09:25:02 OPERATOR GRAF L0007 LOGON  AS  RKSDEV   USERS = 94    FROM 192.168.5.77
09:28:20 SUSELNX2 linux9s sshd[11153]: fatal: Timeout before authentication for ::ffff:116.31.116.18
09:35:11 ZALERT   LNPR CPU UTIL FOR PROCESS  stresser-28 ON rksctnr1 IS 21%
09:36:10 ZALERT   LNPR CPU UTIL FOR PROCESS  smallstr-11912 ON suselnx2 IS 46%
09:37:15 SUSELNX2 linux9s sshd[11928]: fatal: Timeout before authentication for ::ffff:116.31.116.18
09:37:29 SUSELNX2 linux9s sshd[11944]: fatal: Timeout before authentication for ::ffff:116.31.116.18
09:40:04 S11S2ORA -- MARK --
09:40:57 SUSELNX2 linux9s sshd[12290]: fatal: Timeout before authentication for ::ffff:116.31.116.18
09:46:10 ZALERT   LNPR CPU UTIL FOR PROCESS  smallstr-12788 ON suselnx2 IS 45%
09:55:11 SUSELNX2 linux9s sshd[13495]: fatal: Timeout before authentication for ::ffff:116.31.116.18
09:56:10 ZALERT   LNPR CPU UTIL FOR PROCESS  smallstr-13662 ON suselnx2 IS 47%
10:00:00 OPERATOR HCPMXE6224I Event recording is pending because there are no users connected to *MONITOR for this type of data.
10:00:00 OPERATOR HCPMXE6224I Sample recording is pending because there are no users connected to *MONITOR for this type of data.
10:00:04 S11S2ORA -- MARK --
```

- Filtering by user and/or time

ZOPER - zOPERATOR Console - DEMO

12:40:39 SUSELNX2 linux9s sshd[24463]: error: PAM: User not known to the underlying authentication module
12:40:53 SUSELNX2 linux9s sshd[24463]: error: PAM: User not known to the underlying authentication module

Parameters

ZOPER Parameters

Start Date	17/01/11
Start Time	12:00
End Date	17/01/11
End Time	13:52
Node name	
User ID	suselnx2
Click to build direct URL	Build URL

Submit Reset Restart

VELOCITY SOFTWARE

- SNMP Trap Configuration
- Create/Modify SNMP TRAPDEST on the CONFIG disk

```
* following is default 1.3.6.1.4.1.15601
192.168.5.182 velocity 2B06010401F971 ;
```

- Make sure OPERATOR is authorized in zTCP
  - In ESATCP PARMS

```
authuser = 'ZALERT'
authuser = 'OPERATOR'
```

zOPERATOR

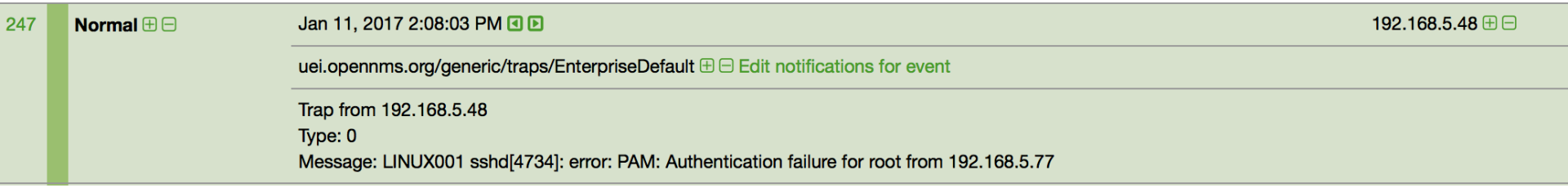
```
ZOPRULES                    Velocity Software Inc.              ZOPER PROD4210
                          ZOPER ZOPRULES Configuration

Match:  Msg type SECUSR User ID _______ Comment Linux authentication error
        Start col 29    End col 55  = Target PAM: Authentication failure
      _ Start col2 ___ End col2 ____ _ Target ____________________________
Action: Color RED       Ext highlight ________ Suppress ___ Hold ___ Stop ___
        Send to ____________________   Send type _____      Send zSERVE ___
        Cmd ____________________________________________ File ______________
        EMAIL address ____________________________________ SNMP trap YES
```

Looking for
'PAM: Authentication failure'

```
                                                    ESAMON 4.300 01/11 14:11
                                OPERATOR Console    USER *              2828 0414C7
14:01:07 LINUX001 sshdÝ4729¨: error: PAM: Authentication failure for root from
                  192.168.5.77
14:01:07 LINUX001 sshdÝ4729¨: error: PAM: Authentication failure for root from
                  192.168.5.77
14:02:17 LINUX001 sshdÝ4729¨: error: PAM: Authentication failure for root from
                  192.168.5.77
14:02:17 LINUX001 sshdÝ4729¨: error: PAM: Authentication failure for root from
                  192.168.5.77
14:02:17 ZTCP     14:02:17 Unauthorized command request from: OPERATOR requesti
                  ng:ALERT LINUX001 s
14:02:17 ZTCP     14:02:17 Unauthorized command request from: OPERATOR requesti
                  ng:ALERT LINUX001 s
14:03:04 LINUX001 sshdÝ4733¨: pam_unix2(sshd:auth): conversation failed
14:03:04 LINUX001 sshdÝ4733¨: error: ssh_msg_send: write
14:03:04 LINUX001 sshdÝ4733¨: error: ssh_msg_send: write
14:05:34 OPERATOR USER DSC   LOGOFF AS  ZTCP     USERS = 33
14:05:40 OPERATOR AUTO LOGON  ***       ZTCP     USERS = 34    BY ZVPS
14:06:22 LINUX001 sshdÝ4734¨: error: PAM: Authentication failure for root from
                  192.168.5.77
14:06:22 LINUX001 sshdÝ4734¨: error: PAM: Authentication failure for root from
                  192.168.5.77
14:07:00 OPERATOR GRAF L0005 RECONNECT  ZTCP     USERS = 34    FROM 192.168.5.7
                  7
14:07:12 LINUX001 sshdÝ4734¨: error: PAM: Authentication failure for root from
                  192.168.5.77
14:07:12 LINUX001 sshdÝ4734¨: error: PAM: Authentication failure for root from
                  192.168.5.77
14:08:10 ZALERT   VMPG Page rate for OPERATOR is 16.1/sec (above 5 for 3)
14:08:10 ZALERT   VMPG Page rate for SMTP is 10.8/sec (above 5 for 3)
14:08:10 ZALERT   VMPG Page rate for ZALERT is 7.2/sec (above 5 for 3)
14:08:19 LINUX001 sshdÝ4738¨: pam_unix2(sshd:auth): conversation failed
14:08:19 LINUX001 sshdÝ4738¨: error: ssh_msg_send: write
14:08:19 LINUX001 sshdÝ4738¨: error: ssh_msg_send: write
14:09:10 ZALERT   VMPG Page rate for SMTP has recovered, now 2.5
14:09:33 OPERATOR GRAF L0005 DISCONNECT ZTCP     USERS = 34
14:11:10 ZALERT   VMPG Page rate for OPERATOR has recovered, now 4.2
14:11:10 ZALERT   VMPG Page rate for ZALERT has recovered, now 3.6
PF1=Help      2=          3=Quit      4=Del Hold   5=All        6=PFKEY Off
PF7=Backward  8=          9=Loc Back  10=          11=          12=Retrieve
====>
```

VELOCITY SOFTWARE

- Result of sending the trap



- zAlert click through
  - Alert messages can be routed to OPERATOR

```
alert cpuutil vmcp
limit 5 1 | &userid
level 20 yellow rev action cp msg op &code &userid running at &cpuutil%
level 40 red
text User &userid CPU Utilization is &cpuutil%
```

- Click through directive in CONFIG ZALERT

```
CLICKTHRU VMCP GRAPH=USERCPU  USER=W1
```

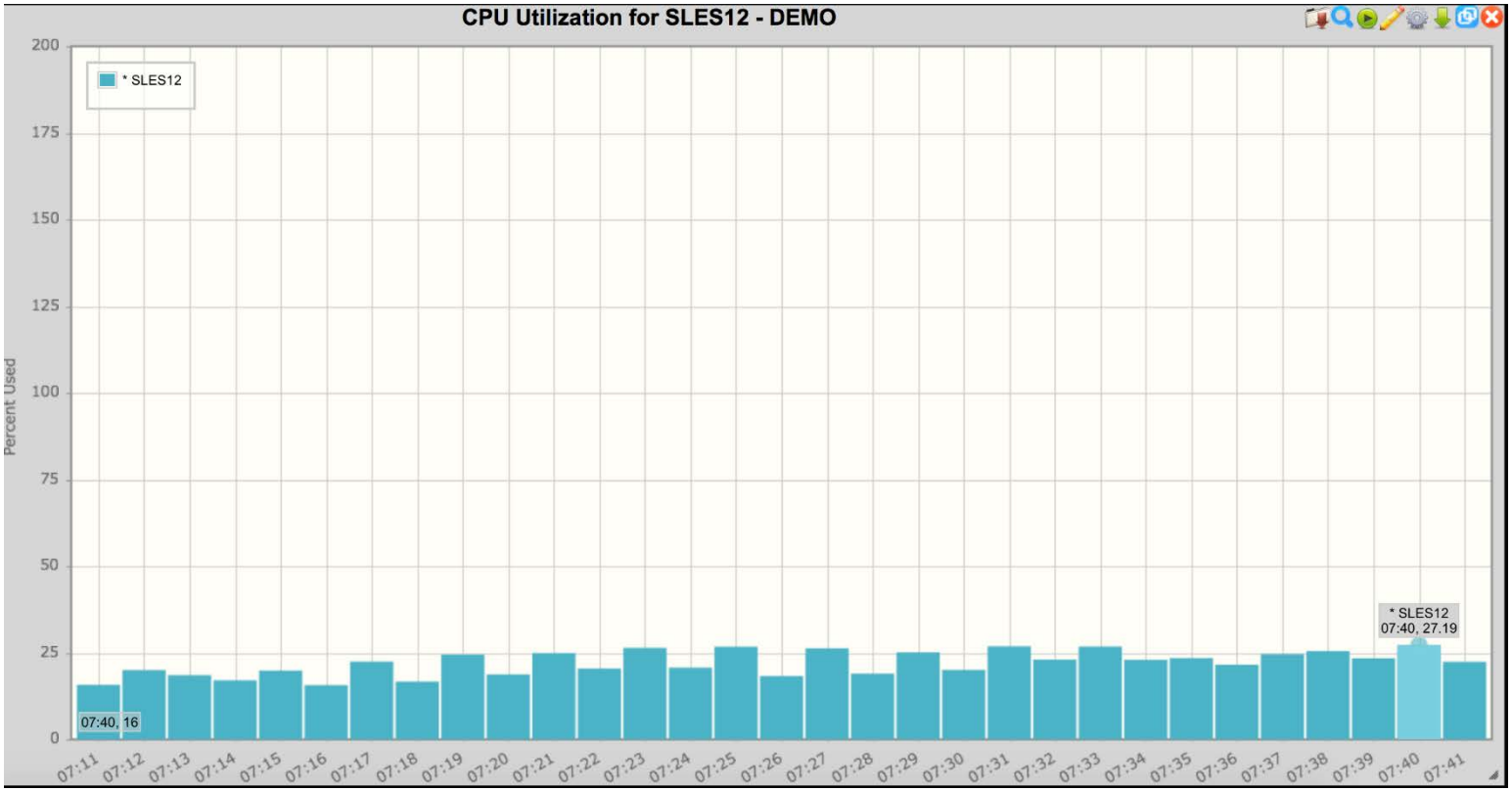
- Points to a specific display element in zView
  - Passes an optional parameter

```
07:34:10 ZALERT    VMCP SLES12 RUNNING AT 23.0%
07:40:04 S11S2ORA -- MARK --
07:40:10 ZALERT    VMCP SLES12 RUNNING AT 27.2%
```

Alerts configured for click through are underlined

VELOCITY SOFTWARE

- Clicking on an alert code brings up the configured report, graph or view
  - Targeted to the optional parameter



VELOCITY SOFTWARE

Events to automate

- TCP/IP or other server crashes
- SFS file space problems
- Security violations
- Linux issues
- Messages routed from zALERT
- Block hackers and denial of service attacks
- Monitor web servers using ZVWS user

Questions

?

Tim Kessler
Velocity Software, Inc
timk@velocitysoftware.com

VELOCITY SOFTWARE