

VELOCITY
S O F T W A R E

*Automated Operations with the Velocity
Performance Suite (zVPS)*

Tim Kessler

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-ng[1334]: 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

```

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 sshdY10518": 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 sshdY10668": 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 sshdY12589": 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  TDNVTI  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 TDNVTI  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
=====

```

zOPERATOR

```

Screen: ESAMAIN  Velocity Software - VSIVM4  ESAMON 4.241 06/17 12:56-14:31
1 of 3  System Overview  2828 414C7

      <---Users----> Transact.      <Processor>  Cap- <--Storage (MB)-->
      <-avg number-> per Avg.      Utilization  ture  Fixed  Active  Stor
Time   On  Actv In Q  Sec. Time  CPUs  Total Virt. Ratio  User  Resid. Load
*-----
14:31:00  92   49 17.0 21.3 0.34   2   17.3 14.5  100   22  11836  0.4
14:30:00  92   60 16.0 22.0 0.26   2   14.2 12.0  100   22  11875  0.4
14:29:00  92   46 18.0 21.1 0.29   2   14.4 12.3  100   22  11824  0.4
14:28:00  92   47 16.0 20.5 0.29   2   13.3 11.1  100   22  11824  0.4
14:27:00  92   53 15.0 21.2 0.27   2   14.9 12.7  100   22  11845  0.4
14:26:00  92   52 11.0 21.1 0.28   2   65.6 63.5  100   22  11844  0.4
14:23:00  92   45 14.0 20.1 0.32   2   15.5 13.0  100   22  11821  0.4
14:19:00  92   47 15.0 20.0 0.32   2   16.2 14.0  100   22  11826  0.4
14:18:00  92   47 16.0 20.4 0.31   2   15.5 13.1  100   23  11827  0.4
14:17:00  92   54 18.0 20.5 0.31   2   16.6 14.4  100   22  11850  0.4
14:15:00  92   60 27.0 21.2 0.30   2   13.1 10.9  100   22  11875  0.4
PF1=Help      PF2=ESAMMENU PF3=Quit      PF4=Select    PF5=Plot      PF6=ESATOC
              PF8=Forward  PF9=Sort      PF10=Parms    PF11=More     PF12=Cancel
====>
Screen: ZOPER  Velocity Software - VSIVM4  ESAMON 4.241 06/17 14:31
1 of 1  OPERATOR Console  USER *  2828 414C7

14:16:10 ZALERT  LNPR CPU UTIL FOR PROCESS  smallstr-18133 ON suselnx2 IS 53%
14:20:11 ZALERT  LPCP LPAR VSIVM5 IS AT 99%
14:21:10 ZALERT  LPCP LPAR VSIVM5 IS AT 99%
14:22:10 ZALERT  LPCP LPAR VSIVM5 IS AT 99%
14:23:11 ZALERT  LPCP LPAR VSIVM5 IS AT 99%
14:24:10 ZALERT  LPCP LPAR VSIVM5 IS AT 100%
14:25:10 ZALERT  LPCP LPAR VSIVM5 IS AT 99%
14:26:10 ZALERT  LPCP LPAR VSIVM5 IS AT 99%
14:27:10 ZALERT  LPCP LPAR VSIVM5 IS AT 100%
14:27:40 OPERATOR  GRAF L0003 DISCONNECT TIMVPS  USERS = 92
14:28:10 ZALERT  LPCP LPAR VSIVM5 IS AT 100%
14:29:10 ZALERT  LPCP LPAR VSIVM5 IS AT 100%
14:29:21 OPERATOR  GRAF L0007 DROP FROM TIMVWS  0200 DIALED= 1
14:30:11 ZALERT  LPCP LPAR VSIVM5 IS AT 100%
14:31:10 ZALERT  LPCP LPAR VSIVM5 IS AT 99%
PF1=Help      2=          3=Quit      4=Del Hold  5=All      6=PFKEY Off
PF7=Backward  8=          9=Loc Back 10=         11=         12=Retrieve
====>
  
```

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 & | ↵

```

Screen: ZOPER      Velocity Software – VSIVM4      ESAMON 4.300 01/10 08:26
1 of 1 REDISPLAY 01/10/17      OPERATOR Console      USER *                2828 0414C7

08:16:44 SUSELNX2 linux9s last message repeated 2 times
08:16:44 SUSELNX2 linux9s sshdY5050": error: PAM: Authentication failure
08:17:02 SUSELNX2 linux9s last message repeated 2 times
08:17:02 SUSELNX2 linux9s sshdY5119": error: PAM: Authentication failure
08:17:13 SUSELNX2 linux9s last message repeated 2 times
08:17:13 SUSELNX2 linux9s sshdY5126": error: PAM: Authentication failure
08:17:47 SUSELNX2 linux9s last message repeated 2 times
08:17:47 SUSELNX2 linux9s sshdY5133": error: PAM: Authentication failure
08:17:58 SUSELNX2 linux9s last message repeated 2 times
08:17:58 SUSELNX2 linux9s sshdY5202": error: PAM: Authentication failure
08:18:10 ZALERT  VMCP SLES12 RUNNING AT 22.8%
08:18:15 SUSELNX2 linux9s last message repeated 2 times
08:18:15 SUSELNX2 linux9s sshdY5209": error: PAM: Authentication failure
08:18:29 SUSELNX2 linux9s last message repeated 2 times
08:18:29 SUSELNX2 linux9s sshdY5214": error: PAM: Authentication failure
08:18:44 SUSELNX2 linux9s sshdY5218": error: PAM: Authentication failure
08:19:14 SUSELNX2 linux9s last message repeated 2 times
08:19:14 SUSELNX2 linux9s sshdY5289": error: PAM: Authentication failure
08:19:42 SUSELNX2 linux9s last message repeated 2 times
08:19:42 SUSELNX2 linux9s sshdY5296": error: PAM: Authentication failure
08:19:56 SUSELNX2 linux9s last message repeated 2 times
08:19:56 SUSELNX2 linux9s sshdY5365": error: PAM: Authentication failure
08:20:03 S11S2ORA -- MARK --
08:20:11 SUSELNX2 linux9s last message repeated 2 times
08:20:11 SUSELNX2 linux9s sshdY5370": error: PAM: Authentication failure
08:20:24 SUSELNX2 linux9s last message repeated 2 times
08:20:24 *SUSELNX2 linux9s sshdY5214": fatal: Timeout before authentication for
:ffff:116.31.116.18
08:20:46 SUSELNX2 linux9s sshdY5377": error: PAM: Authentication failure
08:21:18 SUSELNX2 linux9s last message repeated 2 times
08:21:25 SUSELNX2 linux9s sshdY5450": error: PAM: Authentication failure
08:21:44 SUSELNX2 linux9s last message repeated 2 times
08:21:44 SUSELNX2 linux9s sshdY5455": error: PAM: Authentication failure
08:21:49 OPERATOR GRAF L0007 DIALED TO OPERATOR 0100 DIALED= 2      FROM 192.168
.5.77
08:21:49 OPERATOR EXEC HACKER
08:21:50 OPERATOR ZOPCZ0109I Erasing file CONSOLE 20161008 B1
PF1=Help      2=          3=Return     4=          5=All      6=PFKEY Off
PF7=Backward  8=Forward   9=Loc Back  10=Loc Fwd  11=       12=Retrieve
==> /timeout

```


zOPERATOR

Screen: ZOPER Velocity Software - VSIVM4 ESAMON 4.300 01/10 08:24
1 of 1 REDISPLAY 10/28/16 OPERATOR Console USER * 2828 0414C7

Screen: ZOPER Velocity Software - VSIVM4 ESAMON 4.300 01/10 08:25
1 of 1 REDISPLAY 10/28/16 OPERATOR Console USER * 2828 0414C7

```
----- Friday October 28 2016 -----
23:17:00 OPERATOR USER DSC LOGOFF AS TIMMAP USERS = 109 FORCED BY SYSTEM
----- Saturday October 29 2016 -----
23:16:16 OPERATOR USER DSC LOGOFF AS TIMMAP USERS = 108 FORCED BY SYSTEM
----- Sunday October 30 2016 -----
----- Monday October 31 2016 -----
23:16:04 OPERATOR USER DSC LOGOFF AS TIMMAP USERS = 108 FORCED BY SYSTEM
----- Tuesday November 01 2016 -----
23:15:46 OPERATOR USER DSC LOGOFF AS TIMMAP USERS = 107 FORCED BY SYSTEM
----- Wednesday November 02 2016 -----
23:15:47 OPERATOR USER DSC LOGOFF AS TIMMAP USERS = 107 FORCED BY SYSTEM
----- Thursday November 03 2016 -----
----- Friday November 04 2016 -----
01:52:41 OPERATOR GRAF L0005 DISCONNECT TIMK USERS = 107 FORCED BY SYSTEM
02:03:50 OPERATOR GRAF L0007 DISCONNECT TIMVPS USERS = 107 FORCED BY SYSTEM
02:07:41 OPERATOR USER DSC LOGOFF AS TIMK USERS = 106 FORCED BY SYSTEM
02:18:50 OPERATOR USER DSC LOGOFF AS TIMVPS USERS = 105 FORCED BY SYSTEM
10:09:18 OPERATOR GRAF L0003 DISCONNECT DXT2LV USERS = 107 FORCED BY SYSTEM
15:13:19 OPERATOR USER DSC LOGOFF AS ZADMIN USERS = 104 FORCED BY SYSTEM
----- Saturday November 05 2016 -----
----- Sunday November 06 2016 -----
----- Monday November 07 2016 -----
----- Tuesday November 08 2016 -----
02:28:55 OPERATOR GRAF L0010 DISCONNECT TIMVPS USERS = 105 FORCED BY SYSTEM
02:29:04 OPERATOR GRAF L0014 DISCONNECT TIMK USERS = 105 FORCED BY SYSTEM
02:30:59 OPERATOR GRAF L000B DISCONNECT ZMON USERS = 105 FORCED BY SYSTEM
02:43:55 OPERATOR USER DSC LOGOFF AS TIMVPS USERS = 104 FORCED BY SYSTEM
02:44:04 OPERATOR USER DSC LOGOFF AS TIMK USERS = 103 FORCED BY SYSTEM
02:45:59 OPERATOR USER DSC LOGOFF AS ZMON USERS = 102 FORCED BY SYSTEM
----- Wednesday November 09 2016 -----
23:15:40 OPERATOR USER DSC LOGOFF AS ZVPS USERS = 105 FORCED BY SYSTEM
----- Thursday November 10 2016 -----
----- Friday November 11 2016 -----
```

PF1=Help 2= 3=Return 4= 5=All 6=PFKEY Off
PF7=Backward 8=Forward 9=Loc Back 10=Loc Fwd 11= 12=Retrieve
====> All /forced by system/

```
----- Friday October 28 2016 -----
23:17:00 OPERATOR USER DSC LOGOFF AS TIMMAP USERS = 109 FORCED BY SYSTEM
----- Saturday October 29 2016 -----
23:16:16 OPERATOR USER DSC LOGOFF AS TIMMAP USERS = 108 FORCED BY SYSTEM
----- Sunday October 30 2016 -----
----- Monday October 31 2016 -----
23:16:04 OPERATOR USER DSC LOGOFF AS TIMMAP USERS = 108 FORCED BY SYSTEM
----- Tuesday November 01 2016 -----
23:15:46 OPERATOR USER DSC LOGOFF AS TIMMAP USERS = 107 FORCED BY SYSTEM
----- Wednesday November 02 2016 -----
23:15:47 OPERATOR USER DSC LOGOFF AS TIMMAP USERS = 107 FORCED BY SYSTEM
----- Thursday November 03 2016 -----
----- Friday November 04 2016 -----
02:07:41 OPERATOR USER DSC LOGOFF AS TIMK USERS = 106 FORCED BY SYSTEM
02:18:50 OPERATOR USER DSC LOGOFF AS TIMVPS USERS = 105 FORCED BY SYSTEM
15:13:19 OPERATOR USER DSC LOGOFF AS ZADMIN USERS = 104 FORCED BY SYSTEM
----- Saturday November 05 2016 -----
----- Sunday November 06 2016 -----
----- Monday November 07 2016 -----
----- Tuesday November 08 2016 -----
02:43:55 OPERATOR USER DSC LOGOFF AS TIMVPS USERS = 104 FORCED BY SYSTEM
02:44:04 OPERATOR USER DSC LOGOFF AS TIMK USERS = 103 FORCED BY SYSTEM
02:45:59 OPERATOR USER DSC LOGOFF AS ZMON USERS = 102 FORCED BY SYSTEM
----- Wednesday November 09 2016 -----
23:15:40 OPERATOR USER DSC LOGOFF AS ZVPS USERS = 105 FORCED BY SYSTEM
----- Thursday November 10 2016 -----
----- Friday November 11 2016 -----
```

PF1=Help 2= 3=Return 4= 5=All 6=PFKEY Off
PF7=Backward 8=Forward 9=Loc Back 10=Loc Fwd 11= 12=Retrieve
====> All /forced by system/ & ^/disconnect/



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 CMSGOUT  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

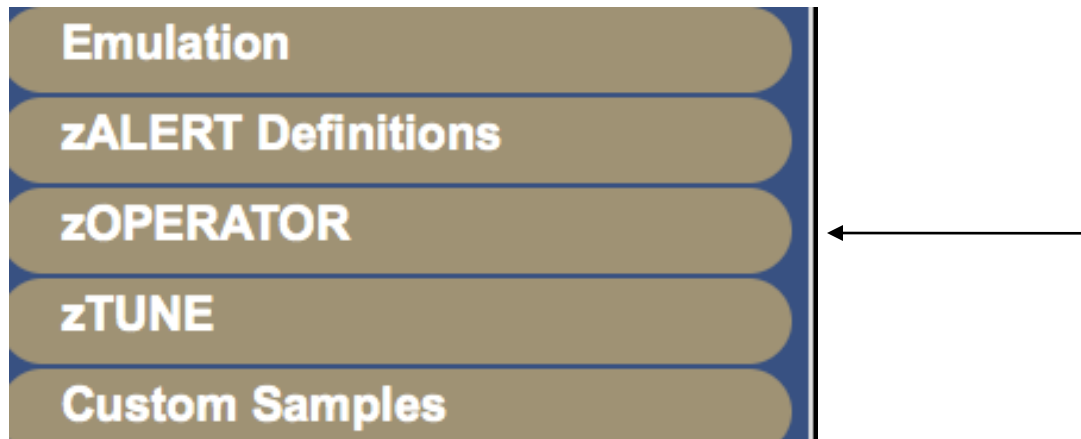
- Equal/Not equal

- 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
 - Params 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	<input type="text" value="17/01/11"/>
Start Time	<input type="text" value="12:00"/>
End Date	<input type="text" value="17/01/11"/>
End Time	<input type="text" value="13:52"/>
Node name	<input type="text"/>
User ID	<input type="text" value="suselnx2"/>
Click to build direct URL	<input type="button" value="Build URL"/>

- 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 ZOPRULES Configuration

ZOPER PROD4210

Match: Msg type SECUSR User ID _____ Comment Linux authentication error
Start col 29 End col 55 = Target PAM: Authentication failure
Start col 2 End col 2 Target _____
Action: Color RED Ext highlight _____ Suppress _____ Hold _____ Stop _____
Send to _____ Send type _____ Send zSERVE _____
Cmd _____ File _____
EMAIL address _____ SNMP trap YES









OPERATOR Console ESAMON 4.300 01/11 14:11
USER * 2828 0414C7

Looking for
'PAM: Authentication failure'

```
14:01:07 LINUX001 sshdY4729 : error: PAM: Authentication failure for root from
192.168.5.77
14:01:07 LINUX001 sshdY4729 : error: PAM: Authentication failure for root from
192.168.5.77
14:02:17 LINUX001 sshdY4729 : error: PAM: Authentication failure for root from
192.168.5.77
14:02:17 LINUX001 sshdY4729 : 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 sshdY4733 : pam_unix2(sshd:auth): conversation failed
14:03:04 LINUX001 sshdY4733 : error: ssh_msg_send: write
14:03:04 LINUX001 sshdY4733 : 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 sshdY4734 : error: PAM: Authentication failure for root from
192.168.5.77
14:06:22 LINUX001 sshdY4734 : 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 sshdY4734 : error: PAM: Authentication failure for root from
192.168.5.77
14:07:12 LINUX001 sshdY4734 : 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 sshdY4738 : pam_unix2(sshd:auth): conversation failed
14:08:19 LINUX001 sshdY4738 : error: ssh_msg_send: write
14:08:19 LINUX001 sshdY4738 : 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
====>
```

- Result of sending the trap

247

Normal  Jan 11, 2017 2:08:03 PM  192.168.5.48  uei.opennms.org/generic/traps/EnterpriseDefault   [Edit notifications for event](#)

Trap from 192.168.5.48

Type: 0

Message: LINUX001 sshd[4734]: error: PAM: Authentication failure for root from 192.168.5.77

- 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

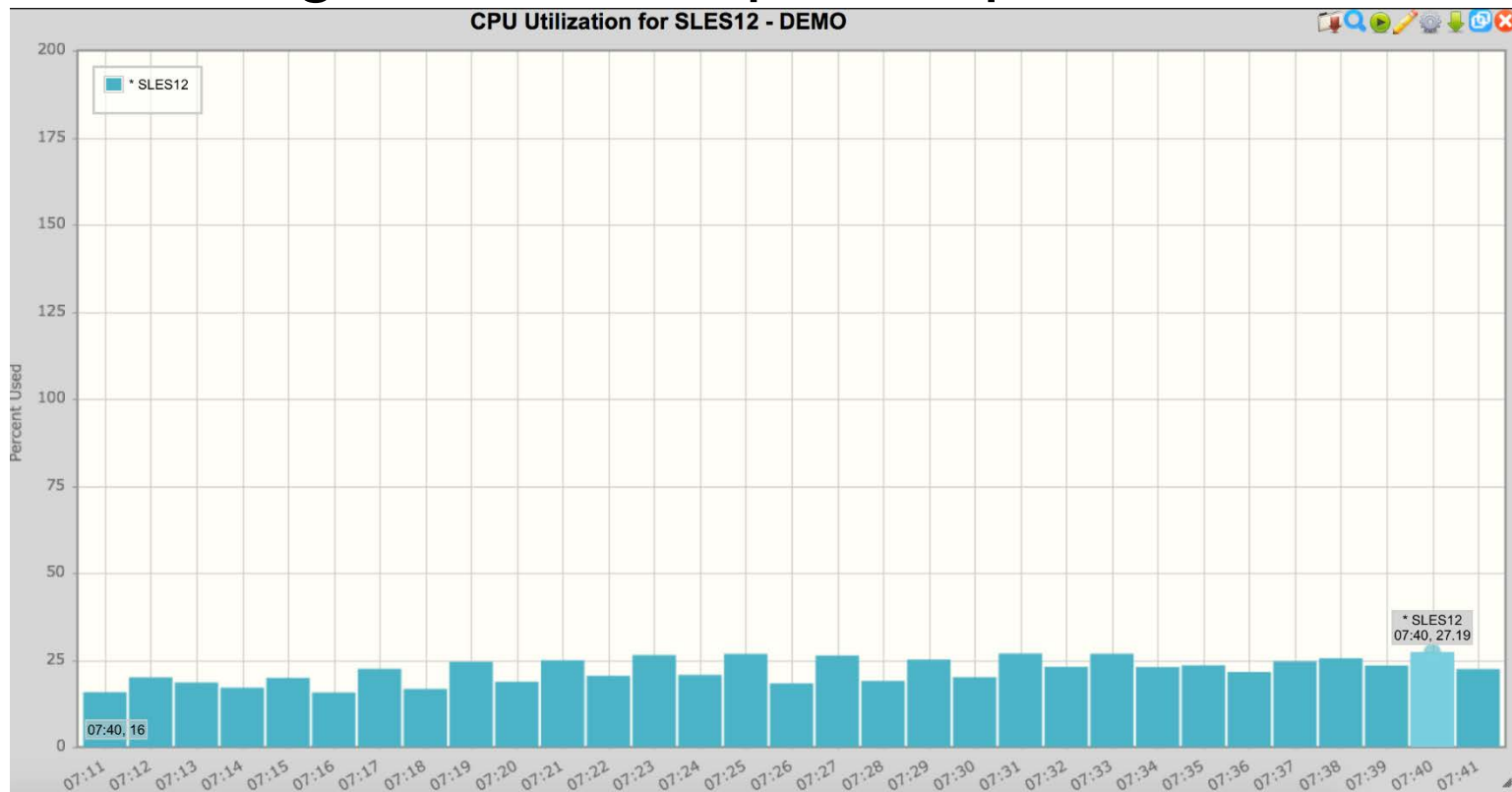
```
CLICKTHRU VMCP GRAPH=USERCPU USER=W1
```

- 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

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



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



Tim Kessler
Velocity Software, Inc
timk@velocitysoftware.com