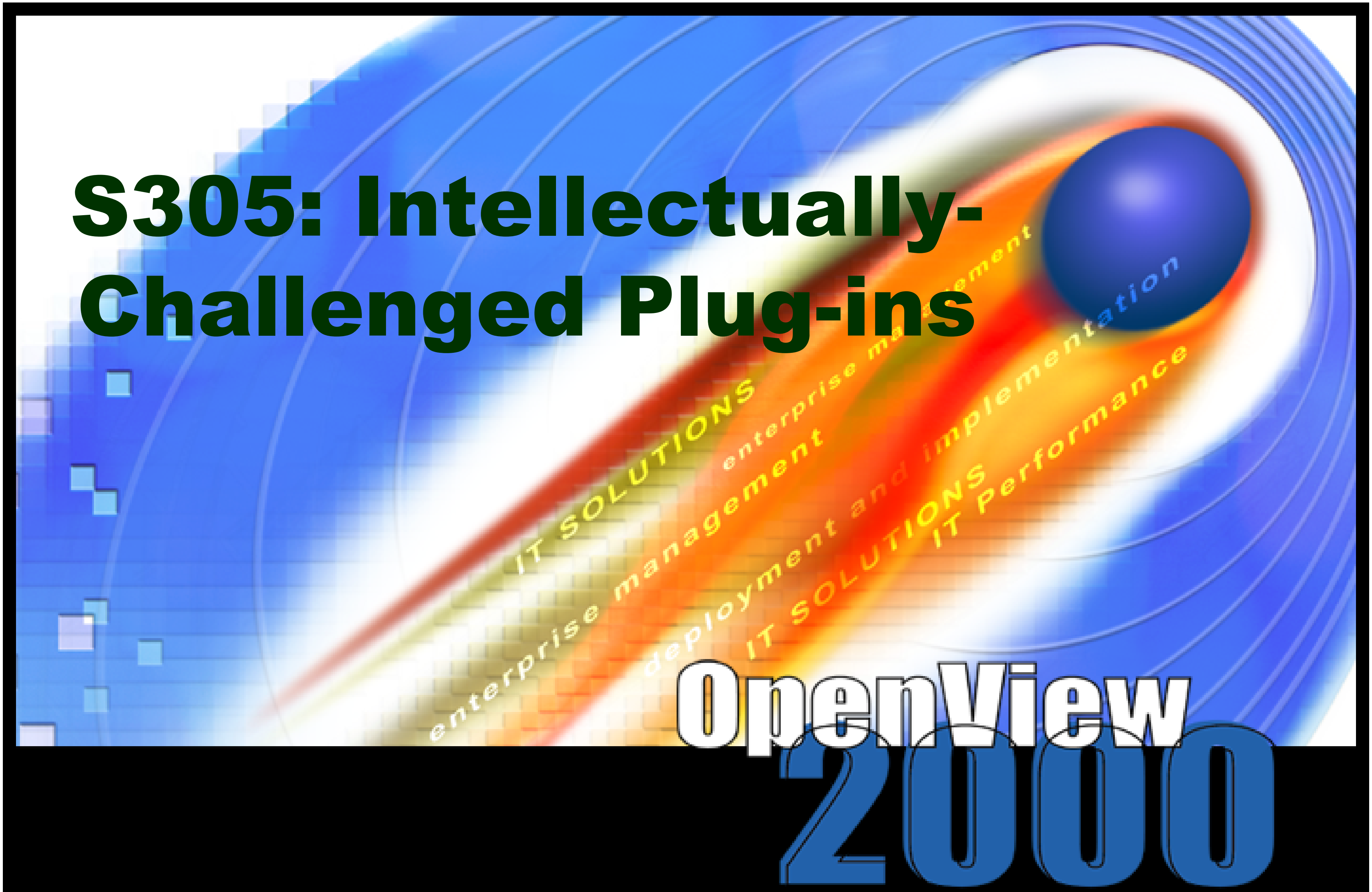
S305: Intellectually-Challenged Plug-ins



OpenView Forum International

HP OpenView

Accelerating IT Performance and Business Success

OpenView Forum International

HP OpenView

Intellectually-Challenged Plug-ins: Improving IT/Operations' Templates for UNIX System Administration

Presented by Mike Peckar

Fognet Consulting

OpenView 2000

Accelerating IT Performance and Business Success

Agenda

Intellectually-Challenged?
The Default ITO Templates
Template Admin Strategies
Improving Logfile Templates
Improving Monitor Templates
Improving Trap Templates
Some Final Notes

Intellectually-Challenged?

ITO Default Templates

- *Same basic elements as Smart Plug-Ins*
- *Intended to provide generic system and application management hooks*
- *Intended to serve as examples or starting points from which more intelligent management could be built*

The power of ITO lies in the extensibility and flexibility of the ITO Client/Server infrastructure and NOT in the off-the-shelf instrumentation

Intellectually-Challenged?

ITO Default Templates

- *The Danger of blindly deploying default templates:*
  - *Unimportant messages*
  - *Message floods*
  - *False sense of security (Disk Utilization)*
  - *Hidden pitfalls*

ITO is commonly purchased and deployed with just the default templates -- Often only a little extra effort is required to greatly improve the scope and intelligence of the ITO management framework.

The Default ITO Templates

Overview

- *Generalities*
- *Default Logfile Templates*
- *Default Monitor Templates*
- *Other Templates*

The Default ITO Templates

Generalities

- *Dumb*
- *Few changes in last 3 versions*
  - *Changes reflect platform version support*
- *Widely variable:*
  - *May or may not have instructions*
  - *May or may not have associated actions*
  - *Sometimes weird polling intervals*
- *Auto actions: simple examples only*
- *Few demonstrations of new features*

The Default ITO Templates

Default Logfile Templates

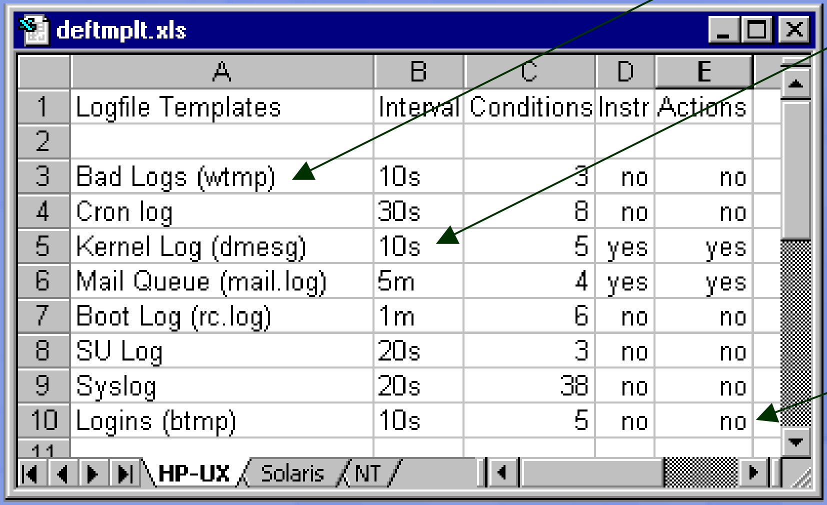
notes for:

Screen shot:

add logfile template

The Default ITO Templates

Default Logfile Templates



	A	B	C	D	E
1	Logfile Templates	Interval	Conditions	Instr	Actions
2					
3	Bad Logs (wtmp)	10s	3	no	no
4	Cron log	30s	8	no	no
5	Kernel Log (dmesg)	10s	5	yes	yes
6	Mail Queue (mail.log)	5m	4	yes	yes
7	Boot Log (rc.log)	1m	6	no	no
8	SU Log	20s	3	no	no
9	Syslog	20s	38	no	no
10	Logins (btmp)	10s	5	no	no
11					

Bad logs - Example of binary command to execute (opcfwtmp)

Kernel Logs - Example of command used in lieu of executable:
`/sbin/dmesg - > <PATH>/dmesg.out`
and command in automatic action:
`"echo \"Current diskspace\” && echo && bdf <filesys>”`

Logins - also uses opcfwtmp

The Default ITO Templates

Default Monitor Templates

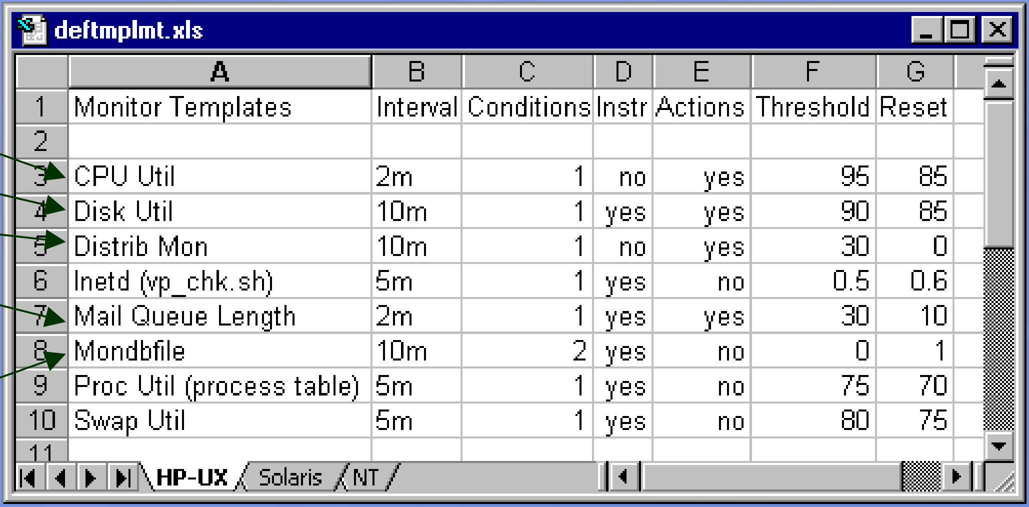
Screen shot- add monitor

The Default ITO Templates

Default Monitor Templates

CPU Util action: ps -ef
Disk Util action: bdf
Dist_mon action: del
MQ length action: ls Q

Mondbfile: example of multiple object monitor:
TS: Space in tablespace
DS: Space on disk



	A	B	C	D	E	F	G
1	Monitor Templates	Interval	Conditions	Instr	Actions	Threshold	Reset
2							
3	CPU Util	2m	1	no	yes	95	85
4	Disk Util	10m	1	yes	yes	90	85
5	Distrib Mon	10m	1	no	yes	30	0
6	Inetd (vp_chk.sh)	5m	1	yes	no	0.5	0.6
7	Mail Queue Length	2m	1	yes	yes	30	10
8	Mondbfile	10m	2	yes	no	0	1
9	Proc Util (process table)	5m	1	yes	no	75	70
10	Swap Util	5m	1	yes	no	80	75
11							

The Default ITO Templates

Other Templates

- *SNMP Trap Template*
  - *NNM 6.0 traps: 837 conditions!*
  - *Intended to mirror image trapd.conf*
- *ECS Circuits*
  - *Bad SU*
    - *Suppress when followed by good SU*
  - *IF Down*
    - *Suppress when followed by IF Up*
  - *Node Down*
    - *Suppress when followed by Node Up*

Template Admin Strategies

Overview

- *Getting Going*
- *GUI Issues*
- *Managing Templates*
- *Simplifying Templates and Template Groups*

Template Admin Strategies

Getting Going

- ***ITO 5.3 Concepts Guide very good***
- ***Familiarize with script repository structure***
  - ***See ITO Admin Guide Volume 2***
  - ***Set up environment variables to often used directories.***
  - ***Note ov.envvars.sh used for NNM directories and overwritten by upgrades***
  - ***Example:***

```
OPCHPC=/var/opt/OV/share/databases/OpC/mgd_node/\
customer/hp/pa-risc/hp-ux11 ; export OPCHPC
```

Template Admin Strategies

GUI Issues

- ***Problem: Template development requires many open windows (up to XX)***
- ***screen shot***

Template Admin Strategies

GUI Issues

- *What about Template Administrator?*
  - *Problem: can’t assign/distribute for testing*
- *What to do*
  - *Use separate window panes*
  - *Consider separate platform just for template development.*
    - *Other long-term benefits include test bed for upgrades and hot standby*
    - *Or, for ramp-up, can use 60-Day eval*

Template Admin Strategies

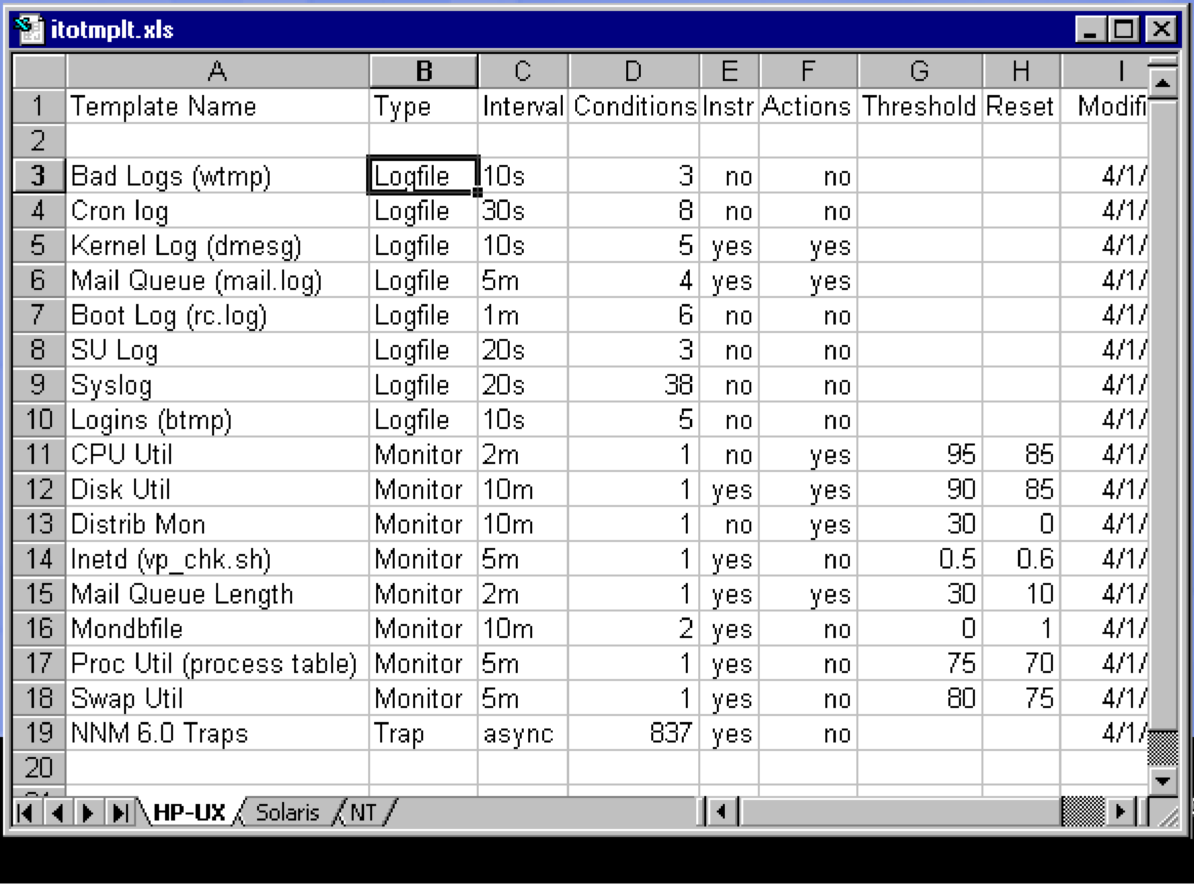
Managing Templates

- *Problems:*
  - *What is being managed on my agent nodes?*
  - *Are most current templates deployed to all?*
- *What to do*
  - *Use new opc_adm audit logs? - Yuck.*
  - *Track templates/changes in spreadsheets*
  - *Track node assignments in speadsheets*

Template Admin Strategies

Managing Templates

- *Example template management spreadsheet*

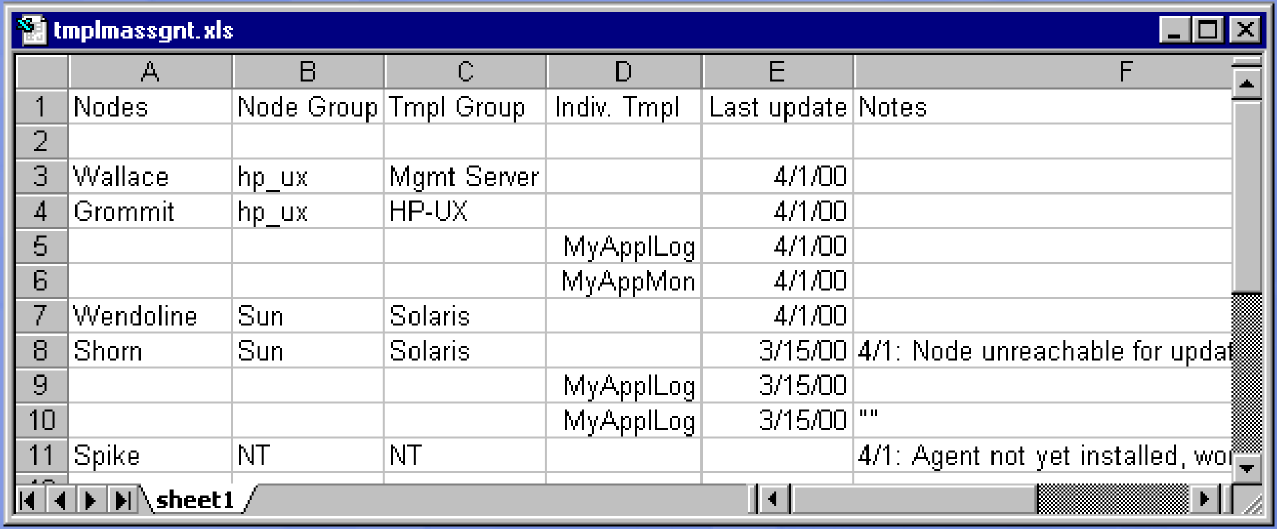


	A	B	C	D	E	F	G	H	I
1	Template Name	Type	Interval	Conditions	Instr	Actions	Threshold	Reset	Modifi
2									
3	Bad Logs (wtmp)	Logfile	10s	3	no	no			4/1/
4	Cron log	Logfile	30s	8	no	no			4/1/
5	Kernel Log (dmesg)	Logfile	10s	5	yes	yes			4/1/
6	Mail Queue (mail.log)	Logfile	5m	4	yes	yes			4/1/
7	Boot Log (rc.log)	Logfile	1m	6	no	no			4/1/
8	SU Log	Logfile	20s	3	no	no			4/1/
9	Syslog	Logfile	20s	38	no	no			4/1/
10	Logins (btmp)	Logfile	10s	5	no	no			4/1/
11	CPU Util	Monitor	2m	1	no	yes	95	85	4/1/
12	Disk Util	Monitor	10m	1	yes	yes	90	85	4/1/
13	Distrib Mon	Monitor	10m	1	no	yes	30	0	4/1/
14	Inetd (vp_chk.sh)	Monitor	5m	1	yes	no	0.5	0.6	4/1/
15	Mail Queue Length	Monitor	2m	1	yes	yes	30	10	4/1/
16	Mondbfile	Monitor	10m	2	yes	no	0	1	4/1/
17	Proc Util (process table)	Monitor	5m	1	yes	no	75	70	4/1/
18	Swap Util	Monitor	5m	1	yes	no	80	75	4/1/
19	NNM 6.0 Traps	Trap	async	837	yes	no			4/1/
20									

Template Admin Strategies

Managing Templates

– *Example node assignments spreadsheet*



	A	B	C	D	E	F
1	Nodes	Node Group	Tmpl Group	Indiv. Tmpl	Last update	Notes
2						
3	Wallace	hp_ux	Mgmt Server		4/1/00	
4	Grommit	hp_ux	HP-UX		4/1/00	
5				MyApplLog	4/1/00	
6				MyAppMon	4/1/00	
7	Wendoline	Sun	Solaris		4/1/00	
8	Shorn	Sun	Solaris		3/15/00	4/1: Node unreachable for updat
9				MyApplLog	3/15/00	
10				MyApplLog	3/15/00	""
11	Spike	NT	NT			4/1: Agent not yet installed, wo

Template Admin Strategies

Simplifying Templates and Template Groups

- ***Templates***
  - ***Delete templates for unwanted platforms***
  - ***Delete uneeded templates***
  - ***Move unwanted stuff from repositories***
- ***Template Groups***
  - ***Consolidate where appropriate***
  - ***Delete unwanted template groups***
  - ***Delete***

Always “config download” before deleting templates!

Improving Logfile Templates

Overview

- *Exception Management Process*
- *Improving Automatic Actions*
- *Operator-Initiated Actions*

Improving Logfile Templates

Exception Management Process

– ***Screen shot - ito msg browser with unmatched*** **syslog file entries**

Improving Logfile Templates

Exception Management Process

- *Exception management: opening the floodgates*
- *Process for unmatched message handling:*
  - *Choose to filter in or suppress*
  - *If filtering in, consider corrective actions*
  - *If you don't understand the meaning of an unmatched message - find out!*

Improving Logfile Templates

Exception Management Process

- *Solicit for input on un-matched messages*
  - *"What did you do to solve this problem?"*
  - *What is appropriate severity; potential corrective actions; instructions?*
- *Could be a condition matching unmatched that calls a TCL/TK script to prompt input*
  - *Not "=" (suppress unmatched not matching pattern in condition)*
- *Employ a process for entering data as annotations*
- *Smaller shops: Do not acknowledge unmatched until a condition is defined for it*

Improving Logfile Templates

Improving Automatic Actions

- *Take a close look at default actions*
- *List repetitive tasks that could be automated*
- *Script actions verbosely to help in debugging and retracing problems/solutions*
- *Consider automated actions to:*
  - *React to security issues*
  - *Build exception reports*
  - *Proactively troubleshoot*
- *Do not use automatic actions for notifications*

Improving Logfile Templates

Improving Automatic Actions

- *Examples:*
  - *Automated action for bad logins*
    - *lastb -a | head*
  - *Automated action for syslog: file system full*
    - *find /<filesys> -size +5000000c -xdev -exec ls -la {} \; (note: supress dups)*

Improving Logfile Templates

Operator-Initiated Actions

- *"No Harm" in replicating automatic actions*
  - *Use to poll/compare current situation*
  - *Use to document state changes*
  - *Good justification for acknowledgement*

May prefer new restart autoaction feature

or

Autoaction restart only on failed actions

- *Consider use for testing more complex actions*

Improving Monitor Templates

Overview

- *Monitor generalities*
- *Multiple-object monitors*
- *Improving default monitors*
- *Process monitoring alternatives*

Improving Monitor Templates

Monitor Generalities

- *Monitors run programs that pass variable data to ITO to compare against thresholds.*
- *Monitors are sometimes useful when looking at non-variable data*
- *Monitors can poll certain SNMP MIB Variables to compare against thresholds:*
  - *From ITO agent nodes only (systems)*
  - *Useful when using cross-platform agents (CMU, Empire, CIA, etc)*
  - *Data not intended to be stored by NNM's SnmpCollect database*
  - *Very useful in ITO & NNM DIM shops*

Improving Monitor Templates

Monitor Generalities

- *add monitor screen shot, showing object/MIB selection screen*

Improving Monitor Templates

Monitor Generalities

- *Non-variable or “binary” Monitors are dumb*
  - *An ITO monitor program that returns a dummy value or just values 0 or 1*
  - *Used in the past to launch scripts:*
    - *Poll for states then send opcmsgs*
    - *Process monitors: 0 = up, 1 = down*
  - *Scheduled Actions (ITO v4+) can take over for these Templates in many cases*

Improving Monitor Templates

Process Monitoring Alternatives

- *Old way: One “binary” monitor template for each process monitored (vp_chk.sh)*
- *Scheduled action for group of processes*
  - *Easier to deploy, set-up*
  - *Better error handling*
  - *More resource efficient - better scaling*
- *Multiple Object Monitor*
  - *Message post-processing is available (actions, notifications/tt, ecs, etc)*
  - *Control msg attribs through ITO admin GUI*
  - *Changes subject to audit*

Improving Monitor Templates

Process Monitoring Alternatives

- ***Scheduled action for group of processes***
  - ***Related to a service, machine type, etc***
  - ***Use fixed opcmsg attributes or set opcmsg attributes as first set of arguments***
  - ***Example: Msg Group as variable attrib.***
  - ***Send process names as subsequent args***
  - ***Can add args for other attributes:***
    - ***Severity, Application, Object, etc***

```
ProcMon CAIngres iidbms dmfrcp dmfacp iigcn
```

Improving Monitor Templates

Process Monitoring Alternatives

- *Scheduled action script*

```
#!/bin/sh
COUNT=0 ; ME=basename(0) ; OPCMSG=/opt/OV/bin/OpC/opcmsg
for PRC in $* ; do
   if [ $COUNT -eq 0 ] ; then
      MSGRP=${PRC}
   fi
   ps -ef | grep ${PRC} | grep -v grep |grep -v $ME
   if [ $? -eq 1 ] ; then
      $OPCMSG sev=Major appl=ProcMon obj=${PRC} msg_text=\
      “Process ${PRC} detected not running” msg_gr=$MSGRP
   fi
   COUNT = `expr $COUNT + 1`
done
```

Improving Monitor Templates

Process Monitoring Alternatives

- ***Multiple Object Process Monitor***
  - ***Build single monolithic template with conditions for all processes (related or not)***
  - ***One-to-one relationship between process, monitored object, and message condition***
  - ***Pass processes to monitor as arguments to monitor program, see example***
  - ***Alternative: Local config file. Provides ability to make on-the-fly adds/deletes***

```
moprcmon sendmail inetd portmap xntpd httpd
```

CHECK if objects not sent result in errs for objects defined in template!

Improving Monitor Templates

Process Monitoring Alternatives

- *Mutiple Object Process Monitor Script*

```
#!/bin/sh
ME=basname(0)
OPCMON=/opt/OV/bin/OpC/opcmon
for PRC in $* ; do
#for PRC in `cat /etc/procnames` ; do
ps -ef | grep ${PRC} | grep -v grep |grep -v $ME
   if [ $? -eq 1 ] ; then
      $OPCMON moprcmon=1 object=${PRC}
   else
      $OPCMON moprcmon=0 object=${PRC}
   fi
done
```

Improving Trap Templates

In General:

- *Download trap template only as backup*
- *Delete unwanted log-only trap conditions*
  - *Could suppress, but loose instructions*
- *Set wanted log-only to log as a status*
  - *If down, Node up, AuthFail (suppress dups)*
- *Delete unwanted logged traps*
- *Set template to not log unmatched messages*
- *Set up SOLID DB for event reporting - see doc:*
  - *Reporting & Data Analysis w/ HP OV NNM*
- *See 1999 OVForum S304: ITO/NNM integration*

Final Notes

- Windows-NT
- opcmsg
  - *opc_int_msg_flt true*
  - *perfview.managex,opcmsg*
- dedup using supress duplic and open poll ints

Header

- Aljslajfldk
  - *aslakjdf*
    - *alskjdfa;l*
      - *laksdfoe*

Accelerating IT Performance and Business Success

OpenView 2000