Nagios and Another Layer of Indirection

John Sellens

jsellens@syonex.com

September 27, 2012

Notes PDF at http://www.syonex.com/notes/

“All problems in computer science can be solved by another level of indirection”
– David Wheeler

Notes:

- I use this idea *constantly*

Unix Philosophy:

Write programs that do one thing and do it well

– Doug McIlroy

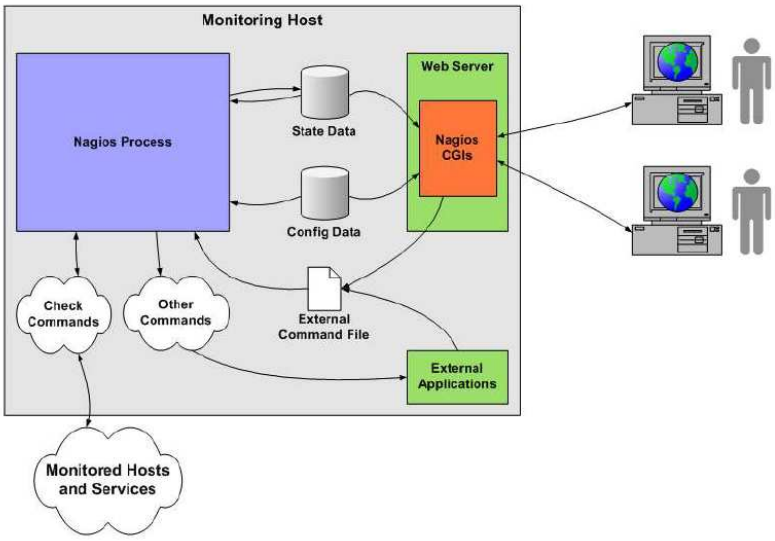
Notes:

- Doug McIlroy, inventor of the pipe, summarized his 1978 Bell System Technical Journal definition in Peter Salus' "A Quarter Century of Unix" as "This is the Unix philosophy: Write programs that do one thing and do it well. Write programs to work together. Write programs to handle text streams, because that is a universal interface."
- Or so says Wikipedia http://en.wikipedia.org/wiki/Unix_philosophy
- Or so says Eric S. Raymond in http://www.faqs.org/docs/artu/ch01s06.html "Basics of the Unix Philosophy" in "The Art of Unix Programming"

Nagios Constitution: Separation of Core and State

Notes:

- OK, so that's a bit of a stretch
- Separation of core and
  - plugins
  - addons
  - etc. . . .



Stolen from Ethan Galstad

Notes:

- Shamelessly (shamefully?) stolen from Ethan Galstad's FOSDEM 2005 presentation
  http://www.nagios.org/fosdem2005
  which is a link that no longer works
- The key here is that there are separate components and the interfaces are (very!) well documented.

Well Defined Interfaces

Notes:

- Simple interfaces between components
- Well defined and documented
- One of the keys to Nagios' success, I'll claim, is the documentation.

Where Is There Indirection?

Notes:

- Indirection already shows up in a number of places, but it might not be immediately obvious.

negate

Notes:

- negate is my favorite
  - Simple, elegant
  - Well, except for all those options . . .
- “The World Turned Upside Down” (with a tip of the lyrical hat to Leon Rosselson and the cover version by Billy Bragg)
- For example, check that a port is not open (e.g. HTTP 80, or Telnet 23)

Ways to Get There From Here

- check_by_ssh
- check_nrpe
- check_snmp

Notes:

- More wrappers around existing plugins
  - Or arbitrary commands
- In one sense or another
- Different transports

Making Pictures / Storing Data

- Apan — the original grapher
  - Wrapped the plugins, saved to RRD files, made some graphs
  - Followed by a host of others, using various techniques
- Feed a database with a plugin wrapper

Notes:

- At least I think Apan was the original graphing tool for Nagios
  - Plugin wrapper stored perfdata for certain plugins in RRD files
  - Others used the “service_perfdata_command” setting
  - Some read perfdata from the log file
  - Is there one (yet?) that uses an exent broker module?
- Now, data manipulation via event broker modules is likely the best way
  - But event broker modules don’t seem to have caught on as well as they should
  - Check out Dave Josephsen’s “Stop Being Lazy And Write An Event Broker Module Already” which is in this same time slot, track 3

How Can We Implement Indirection?

Principle: Unix Philosophy

- Plugins/tools don't need to sing *and* dance
- Combine multiple tools
  - Add plugin timeout with timeout(1)
  - Reformat plugin input or output
  - Answer unanticipated questions

Principle: Custom Wraps

- Multi-stage plugin checks with a shell script
- Check multiple things
  - Is at least one interface up?
  - Is at least one redundant server up?
- Expect scripts for interactions
- Web form posting tools

Principle: Custom Wraps

- “Pervasive wrapper” — redefine $USER1$

  ```
  $USER1$=/usr/local/mywrapper
    /usr/local/libexec/nagios
  ```

- Custom object variables in the environment

  ```
  _web_regexp SomeRegExp
  NAGIOS__HOSTWEB_REGEXP
  ```

- Environment macros mean your plugins can know everything

Notes:

- i.e. You can make your configs suddenly very different
- enable_environment_macros=1

Principle: Simpler Configs

- Simple commands in Nagios configs
- Same config for every machine
- Set limits outside of Nagios configs
  - Manually or automatically
  - Move details/smarts outside the configs

Notes:

- Well, maybe not *every* machine, but try to avoid per-machine configs

Principle: Smarter Plugins

- Let the plugin do the work
- Smart(-er) wrappers for existing plugins
  - Time of day changes
  - Logic enhancements
  - Check only what exists
- Plugin can assume first observed state is "normal" and complain if it changes

Notes:

- For example, I recently wrote a simple plugin to make sure someone is listed as "on duty" — the plugin itself behaves different outside of what (it believes are) normal office hours
- A plugin could check what kind of RAID (or other) interface there is on a machine, and do the appropriate check
- A plugin can keep track of "normal" state and complain if state changes
  - My check_mysqlvars tells us if any MySQL settings change, assuming that the original state is "correct"

Principle: Derived Thresholds

- Let the plugin do the work (again)
- Dynamically adjust thresholds
  - Time of day
  - Trends, past experience
  - Based on other current state/activity
- Let the machines make config changes, instead of you

Notes:

- There is mathematics that will tell you if something is unusual
  - Cricket can use Holt-Winters Forecasting for aberrent behaviour detection
  - Undoubtedly other techniques (standard deviation perhaps?)(
  - I have forgotten everything I once knew about math

How Else Can We Use These Principles?

Notes:

- This is the point at which I start talking about some of the tools I've put together
- And I hope some of the ideas are new to you

Get Found: check_snmpexec

- Define exec commands in snmpd.conf
- snmpwalk the exec table, find command
- snmpget the command
- Let machine do the work of keeping track

Notes:

- e.g. check_snmpexec host snmpcomm execname
- Sadly, can’t pass arguments via SNMP
- We use it for things like checking RAID status, is the mailq empty, IPMI reports ok, etc.

Get Limits: check_allstorage

- snmpwalk hrStorageTable
- Track volumes/devices that exist
- Generate and record limits in per-host file
- No config changes required when filesystems come and go
- check_storage calls check_allstorage and check_inodes

Notes:

- An extension of check_snmp_storage
  - Author: Patrick Proy (patrick at proy.org)
  - http://www.manubulon.com/nagios/
- Similarly for NetApp volumes, inode counts/limits, etc.

Get Service: check_winservices

- check_winsvc: snmptable windows services
  - Confirms that services on cmd line are on
- check_winservices uses files to know what should be running
  - Calls check_winsvc with per-host services
  - Initializes per-host lists if missing

Notes:

- There are global FORCE and IGNORE files, used to initialize per-host lists
- Currently no way to check that a service is not running
  - My most common problem is services that stop, rather than services that show up

Where to Go: mbdivert

- Different ways to get to a remote host
  - Based on hostname, IP, domain, etc.
- Send checks through a per-location gateway
  - Firewall, relay host, etc.
- Nagios host/service configs are identical
  - Access method defined in mbdivert.cfg

Notes:

- Written to go with my MonBOX remote monitoring appliance
  - Can be used with anything
- Knows about ssh, nrpe, potentially more
- Wrap your plugins with mbdivert
  - individually in command definitions
  - by redefining $USER1$, or
  - by replacing actual plugin with a symlink to mbdivert named for the plugin (and configuring PATH to start with where the real plugins are)

mbdivert Config

```
method ssh

pluginmatch check_snmp|check_openmanage
divert mspmgt.company.com
prefix msp
# reset to match any plugin
pluginmatch

# for sfo, divert to the host itself with nrpe
method nrpe
divert -
prefix sfo

# otherwise go direct
```


Notes:

- Configuration is in `mbdivert.cfg`
- For ssh, there are config items for userid, identify file, known hosts
- For nrpe, there are config items for timeout, port

What to Say: genoa

- GEneric NOtification Author/Arranger/Artist
- Uses template files and environment variables to format notifications
- Choose a template based on hostname, problem type, notification type, custom object variables

genoa in Configs

```
define command {
    command_name host-by-email
    command_line genoa -s
}
define command {
    command_name host-by-pager
    command_line genoa -p -t
}
```


Notes:

- Isn’t that simpler than the typical printf piped into mail?
- Uses all the environment variables set by enable_environment_macros=1
- Could also of course use the env command to provide more environment variables

Sample genoa Template

```
Subject: $NOTIFICATIONTYPE$ - $HOSTNAME$/$SERVICEDESC$
is $SERVICESTATE$ - alert $NOTIFICATIONNUMBER$
To: $CONTACTEMAIL$

$NOTIFICATIONTYPE$: $SERVICEOUTPUT$

Service: $SERVICEDESC$

Host: $HOSTNAME$ / $HOSTALIAS$
State: $SERVICESTATE$ for $SERVICEDURATION$
Address: $HOSTADDRESS$

Date/Time: $SHORTDATETIME$

genoa template $GENOATEMPLATE$
```


Notes:

- Rules for template searching based on
  - HOSTNAME or HOSTADDRESS
  - _GENOACLASS custom object variable
  - For HOST or SERVICE problem
  - NOTIFICATIONTYPE - problem, acknowledgement, etc
  - Falls back on a default file
- Nagios sometimes sets variables that I didn't expect, so trying to determine whether the notification is for a HOST problem or a SERVICE problem is more convoluted than I had expected.

Sample genoa Pager Templates

tdir/pager/SERVICE_PROBLEM

```
XX $HOSTNAME$ $SERVICEDESC$ $SERVICESTATE$
$SERVICEOUTPUT$ for $SERVICEDURATION$
$SHORTDATETIME$
```

tdir/pager/SERVICE_ACKNOWLEDGEMENT

```
ACK $HOSTNAME$ $SERVICEDESC$ $SERVICEACKAUTHOR$
: $SERVICEACKCOMMENT$ : $SERVICESTATE$
$SERVICEOUTPUT$ for $SERVICEDURATION$
$SHORTDATETIME$
```


Notes:

- I was surprised how expressive I could be with just the standard environment variables
- But one could imagine running templates through, say, m4

Give Me a Call: tellitto

- Implements multiple notification methods
- Keeps trying until one succeeds
  - e.g. Try SMS service, modem, mail, etc.
- Puts phone/pager numbers in one place
- Pipe message into tellitto, or use genoa -t

Sample tellitto Config

```
# Don’t put secrets in here
# You can use different orders per contact
# for better deliverability

bob    pageuser bob
bob    smsgateway 12125551234
bob    clickatellgate 12125551234
bob    mail -s tellitto-notification
         bob@example.com

sally  clickatell 12125557890
sally  smsgateway 12125557890
sally  pageuser sally
sally  mail -s tellitto-notification
         sally@example.com
```


Notes:

- We have a command `smsgateway` which uses `curl` to send to our provider
- Ditto for `clickatellgate`
- We have a command `pageuser` which tries to use Hylfax’s `sendpage` to send via a modem

Principles:

- Unix Philosophy
- Custom Wraps
- Simpler Configs
- Smarter Plugins
- Derived Thresholds

Notes:

- Tools I've written are (or will be) available at http://www.syonex.com/software