Nagios Event Handlers

Sam Sargeant sam@onesquared.net

NZNOG 2008 Sysadmin Miniconf

Nagios

- Network and System monitoring
- Open Source
- Widespread use

States in Nagios

Working normally

OK

Seems a bit broken

WARNING

Just stopped working

CRITICAL (SOFT)

Still isn't working

CRITICAL (HARD)

Event handlers

- UNIX command
- Fires when a host or service changes state
- May include multiple ‘soft’ states
- May use a global handler for all of Nagios, or a specific handler for hosts or services

Why Event Handlers?

- Create trouble ticket
- Update status pages
- Detailed logging
- SNMP traps & 3rd party integration
- Collect diagnostics
- IDS triggered lock-down
- Auto-Restart

Event Example

- Host (www.znog.org)
- Service (HTTP)
- State (CRITICAL)
- Output (Connection refused by host)
- Type (SOFT)
- Attempt (3)

Event Handler Config

```
define command {
   command_name    host_event_command
   command_line    /etc/nagios/event-handler.py --host "$HOSTNAME$" \
        --host-state "$HOSTSTATE$" --host-address "$HOSTADDRESS$" \
        --output "$OUTPUT$" --type "$STATETYPE$" --host-attempt "$HOSTATTEMPTS$"
}

define command {
   command_name    service_event_command
   command_line    /etc/nagios/event-handler.py --host "$HOSTNAME$" \
        --host-state "$HOSTSTATE$" --host-address "$HOSTADDRESS$" \
        --type "$STATETYPE$" --service "$SERVICEDESC$" \
        --service-attempt $SERVICEATTEMPT$ --service-state "$SERVICESTATE$"
}

global_host_event_handler=host_event_command
global_service_event_handler=service_event_command
```

Auto-Fix

Are you sure you want to do this?

Press Y to continue

Auto-Fix Example (1)

- Apache isn't accepting tcp/80 connections
- Use an ssh key without a passphrase

```
ssh -i ~/.ssh/nopassphrase.key
admin@www.nznog.org sudo /etc/init.d/apache2
restart
```

Auto-Fix Example (2)

- JRUN server on Windows has died; again
- Run xvfb to provide a headless X server
- Use rdesktop to login to Windows Terminal Services and run a restart script

```
DISPLAY=:1 /usr/bin/rdesktop -u serverwrangler \
        -p fubar -s C:\\smite_jrun.bat
```

Auto-Fix Example (3)

- Network utilisation on upstream link is at 80%
- Nagios enters a warning state
- Triggers a mail to sales to bring in more cash so we can upgrade our transit

```
echo “Sell more you bastards, I want a new shiny link.” | mail -s “Urgent Requirements” sales@myorg.com
```

Dangers of Auto-Fix

- One server to rule them all
- Could interfere with troubleshooting
- Solves a symptom rather than a problem
- Makes for lazy admins
- [Your reason here]

Thanks