VPO, SNMP, and Crawfish Etouffee

Integrated SNMP Management with
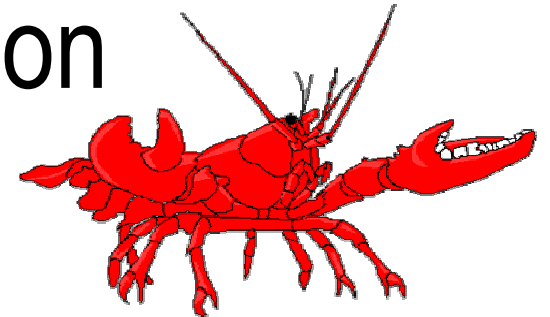## HP OpenView
VantagePoint Operations and Network Node Manager

Presented by: Mike Peckar

Principal, Fognet Consulting

What you will learn in this session

In this session, you will learn…

- Why network mgmt & system mgmt are hard to integrate
- The differences between SNMP events & VPO Messages
- Details of the NNM event and VPO message architectures
- How to integrate SNMP events via NNM into VPO
- Pitfalls and best practices in integrating SNMP into VPO
- Some alternative approaches to integration
- Everything I know about good Cajun cooking

Agenda

VPO, SNMP, and Crawfish Etouffee

- Why INSM is like Jambalaya
- VPO & NNM Roux
- Combine Ingredients
- Cook, Simmer and Spice
- Recipes

Why INSM is like Jambalaya?

- They Both are combinations of unlikely ingredients
- No two batches/implementations are ever alike
- Cooks will argue incessantly over recipes
- Good things sometimes come from strange mixtures
- Severe indigestion can inflict the uninitiated
- Religion and politics are inextricably linked to each

Why INSM is like Jambalaya?

What is Jambalaya?

- Derived from the Spanish jamón for ham, Creole balayez: to mix.
- Similar to Paella, but with local ingredients. First appeared late 1700's. Made with anything: ham, chicken, sausage, fresh pork, shrimp, oysters.
- An ideal dish for outdoor cooking over hardwood fire. Big black cast iron pots made preparation easy and economical for use for churches, political rallies, weddings, family reunions, etc.
- Gonzales, LA is the Jambalaya Capital of The World. The Jambalaya Festival and World Champion Jambalaya Cooking contest is held annually there and attracts area cooks who have spent years perfecting the art of cooking and seasoning this Creole delicacy.

Why INSM is like Jambalaya

What is INSM?

- Integrated Network and Systems Management
- A still somewhat unpalatable mix of IT Mgmt disciplines
- Network mgmt centered on status, topology, troubleshooting
- Systems mgmt centered on client-server, service orientation
- Today's INSM solutions are heavily laden with legacy code
- INSM Standards (OSI, DMTF, etc) have failed in market
- For platform vendors integration means "add to suite"
- Vendors too busy catching up w/ latest technology to integrate

6

VPO & NNM Roux

What is Roux?
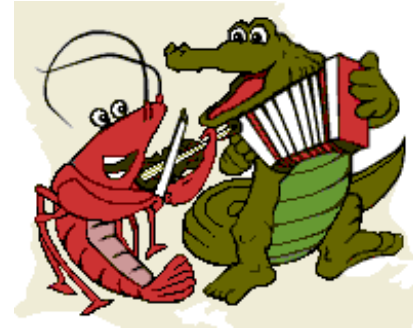
- A cooked mixture of flour and fat (oil or butter or both)

- A fundamental building block of cajun/creole/french cooking

- Requires a lot of attention to make properly – easy to burn

- Dangerous – must be constantly stirred over high heat

- Called "cajun napalm" because splatters cause bad burns

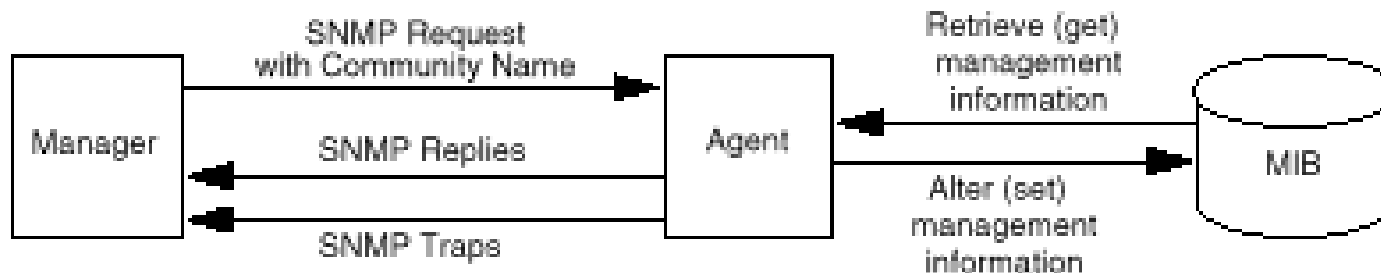Inattention to implementation means you'll get burned

VPO & NNM Roux

What is VPO?

- VPO formerly ITO, OpC - Built on NNM API's

- Enterprise-class distributed systems management tool

- Completely separate infrastructure/arch from NNM

  – Different model/method for events/messaging

  – Different back-end databases and event infrastructures

- NNM is completely embedded in VPO

  – VPO launch launches NNM with NNM events suppressed

VPO & NNM Roux

- SNMP Traps – "the oil"

    – Simple Network Management Protocol – agent truly simple

    – Complex management and development.

    – MIB - Logical repository for data

    – Data represented as numbers on agent translated by manager

    – iso.org.dod.internet.mgmt.mib-2.system.sysObjectID

    – 1 . 3 . 6 . 1 . 2 . 1 . 1 . 2

Manager — SNMP Request with Community Name → Agent — Retrieve (get) management information ← MIB

Manager ← SNMP Replies — Agent

Agent — Alter (set) management information → MIB

Manager ← SNMP Traps

VPO & NNM Roux

Why are SNMP events so hard to mix with VPO?

- With SNMP Traps, variable bindings are *variable*

- SNMP traps have no default severities that can be mapped to Icon Status on maps or message priorities – formats unfixed

- NNM Events – they're not SNMP traps, not VPO Messages…

- NNM encapsulates SNMP Traps into an "ovevent", adding severity, logging behavior, actions, and uses TCP transport.

- Most SNMP events come from NNM itself. Results of status polling such as "Node Down" are Defined SNMP events under the OpenView enterprise and are generated by NNM

10

VPO & NNM Roux

NNM Event Infrastructure – ingredients:

- *ovtrapd:* trap receptor/informer/buffer listens on UDP port 162
- pmd: Postmaster Daemon brokers events to/from SNMP API-registered services
- *trapd.log*: ASCII event log deprecated in NNM 5.0+
- BES: Binary Event Store for NNM, a.k.a eventdb
- *xnmevents* & *ovalarm*: NNM Native Event Display GUI for X, JAVA
- *trapd.conf*: SNMP trap configuration file (ASCII)
  - Provides SNMP manager trap translation for SNMP agent traps
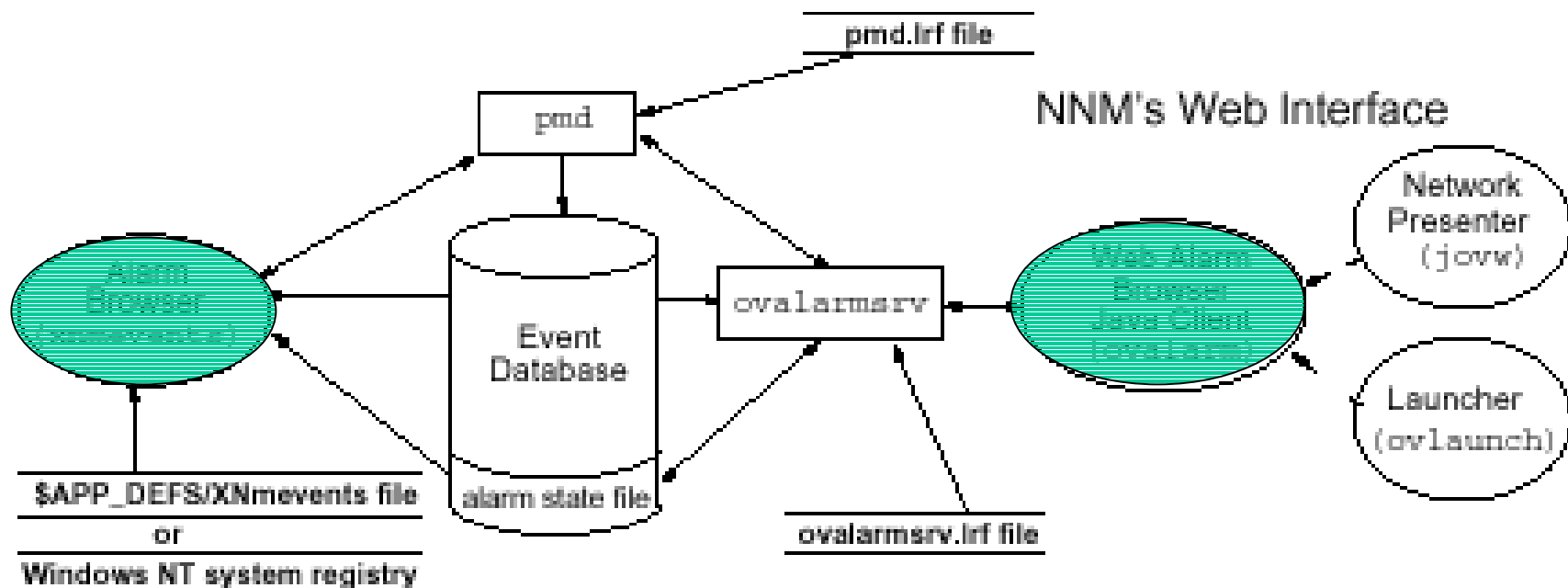 - Provides NNM-Specific event mappings for severity, logging, actions…

NNM event flow
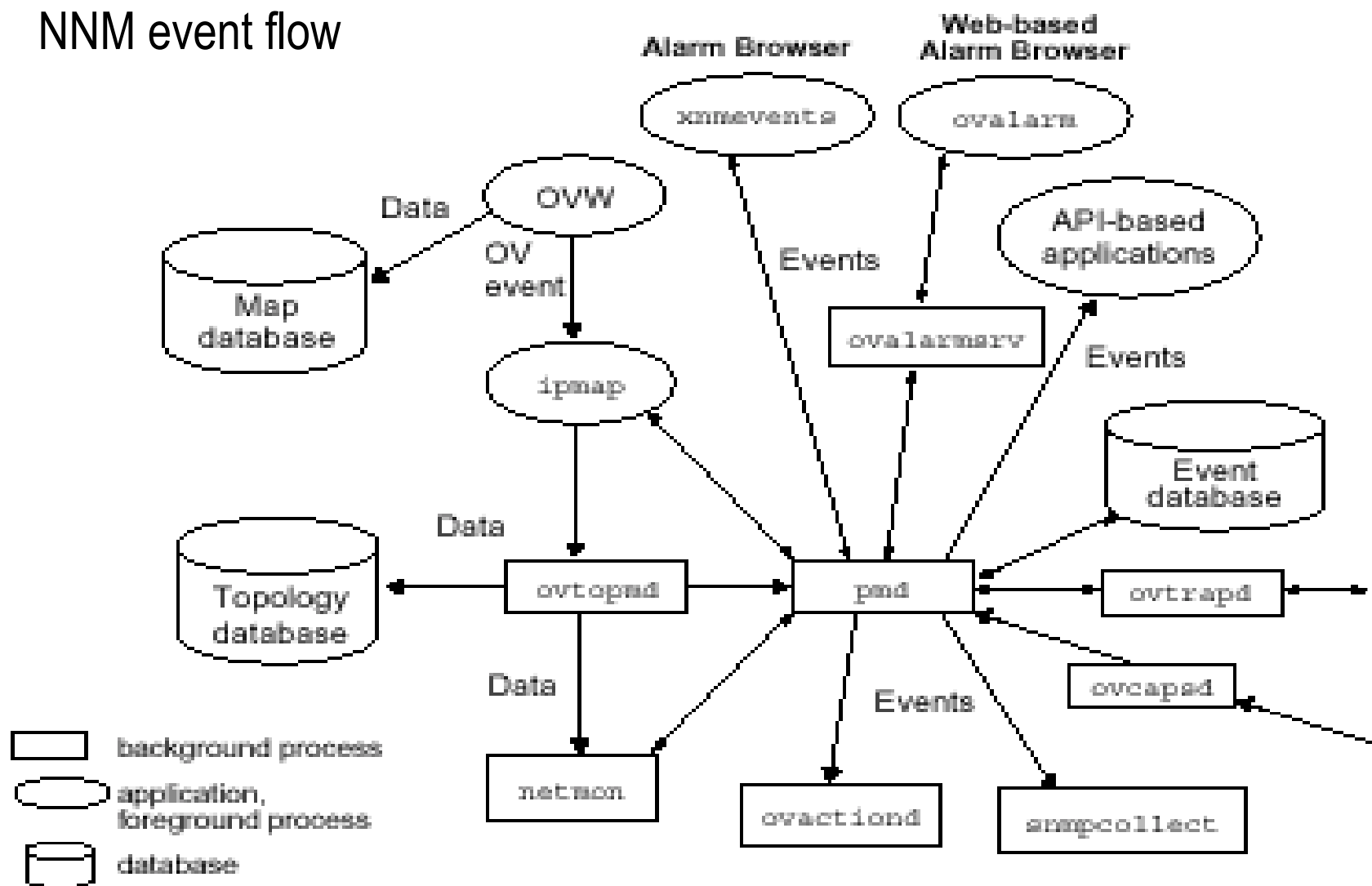
VPO & NNM Roux

NNM Event logging and Browsers

- Suppressed in VPO GUI
  - NNM eventdb settings same defaults as for NNM standalone

VPO & NNM Roux

- VPO message – "the flour"
  - Message types
    - Log file, Monitor, opcmsg, console
  - Message formats
    - Fixed set of attributes, some with default settings, such as severity, message group, node source, application, unique Msg ID, etc.
  - Message transports
    - RPC-based - reliable, buffered, layers of security available
  - Message Storage
    - Message attributes map to multiple keys and tables in oracle DB

OPENVIEW
2001:
OPENVIEW USER'S CONFERENCE

OPENVIEW
FORUM
INTERNATIONAL

hp

VPO & NNM Roux

- VPO Message Infrastructure – Ingredients:

VPO management server daemons:

opcctlm	- Control manager	*opcactm*	- Action manager
opcmsgm	- Message manager	*opcecm*	- ECS manager
opcdistm	- Distribution manager	*opctss*	- Dist mgr subprocesses
opcmsgr	- Message receiver	*opcmsgrd*	- DCE/NCS msg receiver
opcttnsm	- Notification manager	*ovoareqsdr*	- Request Sender
ovoareqhdlr	- Request handler	*opcforwm*	- Mgr to mgr forwarder
opcdispm	- Display manager	*opcuiadm*	- VPO Admin GUI
opcuiopadm	- VPO AdminOp GUI	*opcuiop*	- VPO operator GUI
opcuitadm	- VPO Template adm	*opcuiwww*	- VPO JAVA GUI [15]

OPENVIEW
2001:
OPENVIEW USER'S CONFERENCE

OPENVIEW
FORUM
INTERNATIONAL

hp

VPO & NNM Roux

· VPO Message Infrastructure – Ingredients:

VPO agent processes:

opcctla - Control agent   *opcacta* - Action agent

opcmsga - Message agent   *opcmsgi* - Message interceptor

opceca - ECS agent   *opconsi* - Console agent (MPX only)

opcdista - Distribution agent   *opctaa* - Dist agent subprocesses

opcle - Logfile encapsulator   *opcmona* - Monitor agent

                          opctrapi - Trap interceptor

16

VPO & NNM Roux: VPO Message Infrastructure
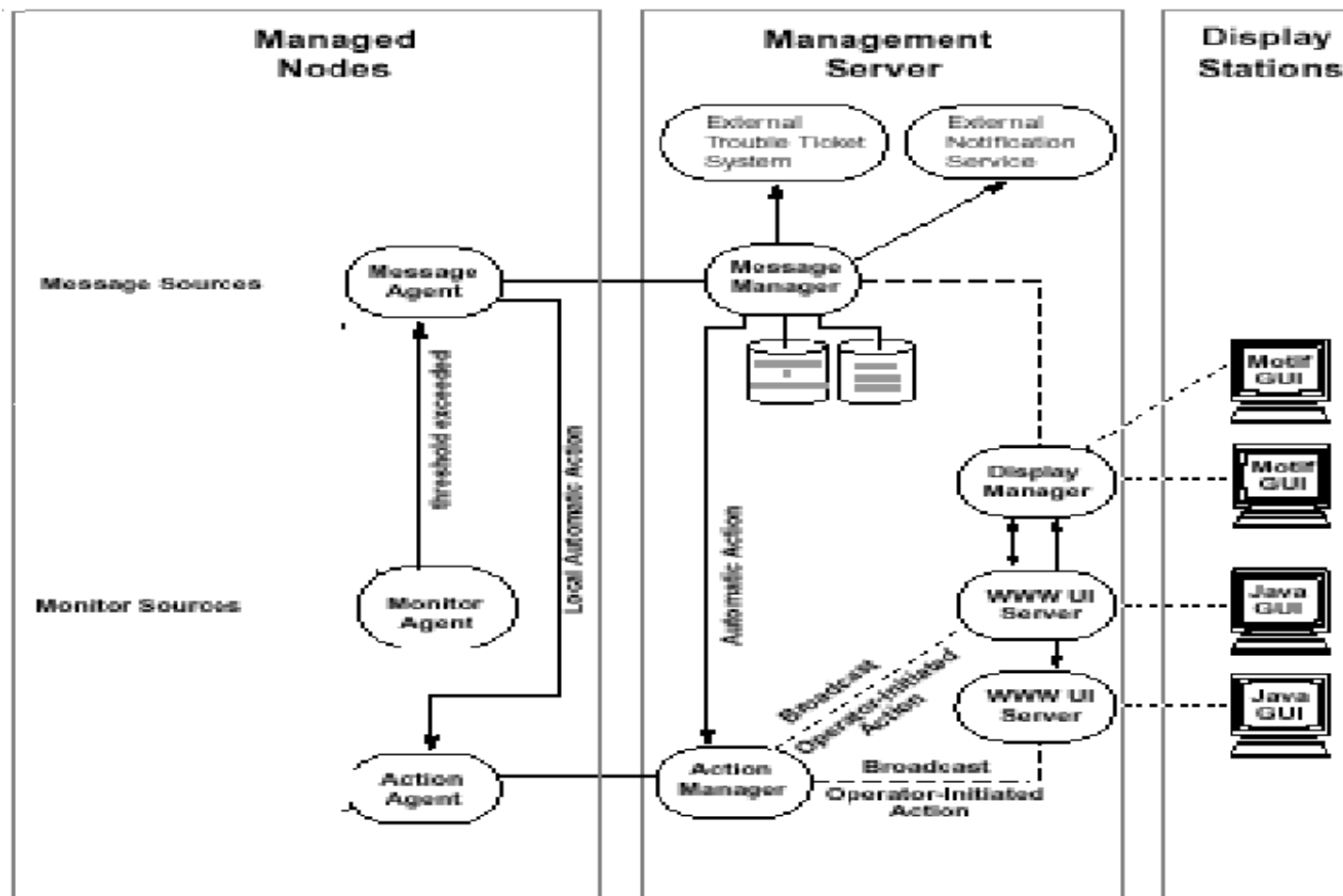
VPO & NNM Roux: VPO Infrastructure: Agent details
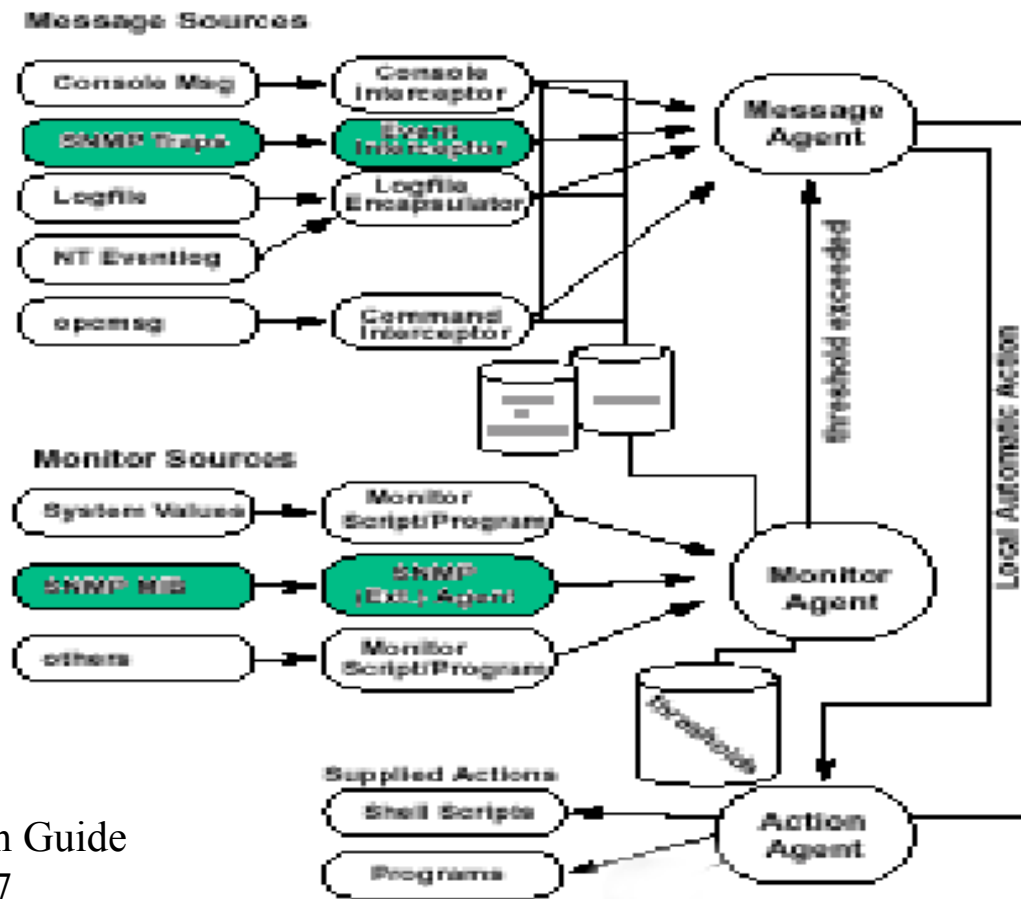
From VPO Admin Guide
Vol 1 p 217

Combine Ingredients

- Integrated SNMP Message flow:
  - SNMP messages still logged to NNM event store
  - *xnmevents* GUI suppressed in VPO
  - VPO sub-agent *opctrapi* registers with NNM's *pmd* to receive traps based on VPO SNMP trap template(s)
  - Default VPO trap template reflects default NNM *trapd.conf* event configurations as shipped
  - *ovtrap2opc* command-line tool provided to upload customized NNM event configurations.
    - Wrapper for *opccfgupld* template upload command

19

Combine Ingredients

- VPO Agent Trap Interceptor, *opctrapi*:

    - Intercepts standard SNMP traps or NNM events (default)

    - Supported agent platforms (VPO 6.0):

        - .AIX 4.2 and 4.3 (direct port access mode)
        - .HP-UX 10.x and 11.x
        - .Novell NetWare 4.1, 4.11, 5.0, 5.1 with NMA 2.1
        - .Solaris 2.5.1 and above
        - .Windows NT 4.0 and Windows 2000

    - Agent environment variable to toggle ovevent/raw SNMP:
        - SNMP_SESSION_MODE NO_TRAPD

Combine Ingredients: Integrated SNMP
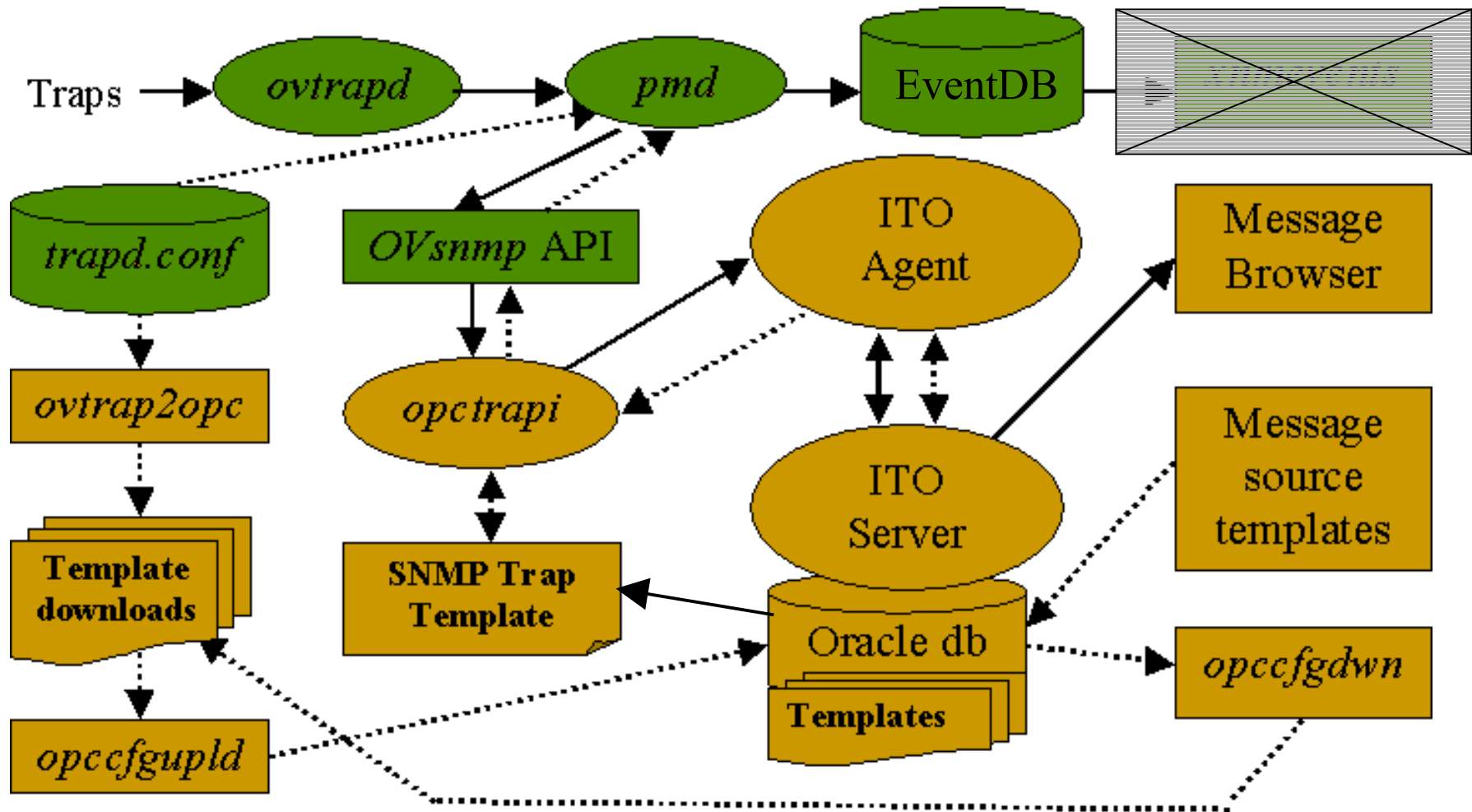
Combine Ingredients

- ## Basic VPO/SNMP Integration

  - SNMP template must be distributed to VPO Server's agent

  - SNMP traps will be received only for default set of node sources – nodes in Node Bank.

  - Additional sources can be added to Node Bank or administrator can "*add node for external events*" and use IP address or wildcards: <*>.<*>.<*>.<*>

  - Node Group for SNMP sources is *net_devices,* for netop operator

  - SNMP traps received not limited to NNM-managed nodes – This is true in Native NNM as well!

22

Combine Ingredients

Some SNMP event Integration choices:

- Default SNMP trap handling scheme
  - Use xnmevents for network management, VPO browser for systems. SNMP Traps only received for VPO agent nodes

- All SNMP traps into ITO for all nodes:
  - Easy set-up, Issues with message storms, Use to integrate quickly but take steps to address issues first. No need to use xnmevents

- Selected SNMP traps from important selected nodes:
  - Set up Trap template for traps of interest and configure Node Bank entries for only devices of interest. – typically network devices – use VPO mostly, but may have occasional need for xnmevents

Combine Ingredients

Some cooking tips:

- Most systems' default SNMP agents are dysfunctional

- Most network devices are quiet too, unless traps turned up

- NNM generates lots of traps from status events, but…

    – NNM events have polled node set as source, not NNM server

- Check SNMP devices have only one SNMP destination, particularly NNM Collection Stations:

    – /etc/SnmpAgent.d/snmpd.conf: **trap_dest:<nodename>**

- Suppress duplicate messages for whole SNMP template

24

Combine Ingredients

SNMP and VPO message formats don't mix well

- NNM adds status, logging, actions to raw SNMP traps

- NNM "Log-only" events map to "Put directly in history" in VPO.

- NNM generates many more log-only events than logged ones!

  – Can fill up Oracle tables without VPO operator knowledge.

  – Solution: Purge unwanted traps from VPO SNMP Trap Template

  – Suppressing them by condition not recommended (performance)

  – See procedure (next slide)

Combine Ingredients

Procedure for pairing down trap template in VPO:

- Copy SNMP trap template in mgmt server template group.
- Delete original template from management server template group.
- Delete *log-only* conditions under Openview Enterprise
- Log to a severity those log-only conditions you do want
- Delete unused default enterprise traps (DMI, etc)
- Important: Modify template; suppress unmatched conditions!
- Distribute VPO Server's agent, force update
- Download template to back it up – you don't want to repeat this!

Combine Ingredients

Trap template customization in VPO:

- Example OpenView enterprise log-only NNM events
  - Delete: OV_Station_Critical   OV_Network_Major

                  OV_Station_ Marginal   OV_Network_Critical

                  OV_Station_ Warning   OV_Segment_Major

                  OV_Station_ Major   OV_Segment_Critical
  - Log: Node_Up   Interface_Down (for selected nodes)

                                             Interface_Up (for selected nodes)

- Other log-only events you may want to log

                      Authentication_fail

Combine Ingredients

What about my vendor trapdefs?

- Many (most) vendors provide embedded macros in their MIBS
- These macros update *trapd.conf* with vendor's trap definitions
- *ovtrap2opc* integration utility supplied with VPO to upload trapd.conf to reflect changes in VPO trap template. This utility has several issues, mostly due to message format differences
- Solution:
  - Use procedures on next slide for integrating many new traps
  - Update trap template manually – enter a new condition for every trap
  - Use ovtrap2opc if not planning to customize VPO trap template

28

Combine Ingredients

Procedures for loading trap updates in VPO:

Case 1)

 You have file containing trapdefs that conform to trapd.conf format as supplied by by vendor with instructions to run *xnmloadmib*:

1. Follow vendor instructions to update NNM's *trapd.conf*, then…

2. add the text: "VERSION 3" on first line at very top of file supplied

3. $OV_BIN/OpC/utils/ovtrap2opc $OV_CONF/C/trapd.opc "MY SNMP 6.0 Traps" mytraps; answer "no" when asked to upload

4. opccfgupld -subentity -add mytraps

5. Assign/distribute new trap template to SNMP source agent

Combine Ingredients

Procedures for loading trap updates in VPO:

Case 2)

Use when new trap definitions already loaded into *trapd.conf*, or loaded automatically from install of 3rd-party product such as CiscoWorks

1. Backup *trapd.conf*; add new trapdefs per instructions from vendor

2. diff -e trapd.conf.orig trapd.conf > trapd.opc or separate in editor.

3. strip ed controls (a,c,d); add "VERSION 3" at top of file.

4. $OV_BIN/OpC/utils/ovtrap2opc $OV_CONF/C/trapd.opc "MY SNMP 6.0 Traps" mytraps; answer "no" when asked to upload.

5. opccfgupld -subentity -add mytraps.

6. Assign/distribute new trap template to SNMP source agent

Combine Ingredients

Procedures for loading trap updates in VPO:

Notes on this method:

- Creates additional trap templates
  - Nice for organizing
  - Assign template related to a set of devices to own Msg Groups
    - For example, Omniback traps can go into Backup Msg Group
  - Be sure to always set "Suppress unmatched" for template

Combine Ingredients

ovtrap2opc issues

- No realistic way to do a "*opc2ovtrap*"
  - VPO trap template customizations cannot be written back to *trapd.conf* – re-invocation of *ovtrap2opc* creates template that is "unaware" of any customizations and will overwrite on upload.
- Message format incompatibilities:
  - Action's node sources are translated to event source, which for NNM status events is not the "real" source – the NNM server
  - Defined node sources for NNM-customized events
    - NNM sources space separated, VPO pipe (or) separated
    - VPO doesn't support external list of node sources
  - Trap forwarding can only be done in *trapd.conf*

Combine Ingredients

What to do about *ovtrap2opc* issues:

– Pick One:

1. Keep all trap customizations in trapd.conf, use ovtrap2opc, and understand impacts of VPO customizations to update process.

2. Maintain all traps in VPO - use procedures here or manually update VPO trap template. Turn off/ignore NNM event system.

3. Same as above, but maintain NNM events and *trapd.conf* for trap forwarding, multiple node source customizations, eventdb reporting. Use *xnmevents* on occasion, like for "drill-down".

4. Do not integrate traps to VPO at all. Use NNM's native event browser, *xnmevents.* De-assign VPO SNMP templates
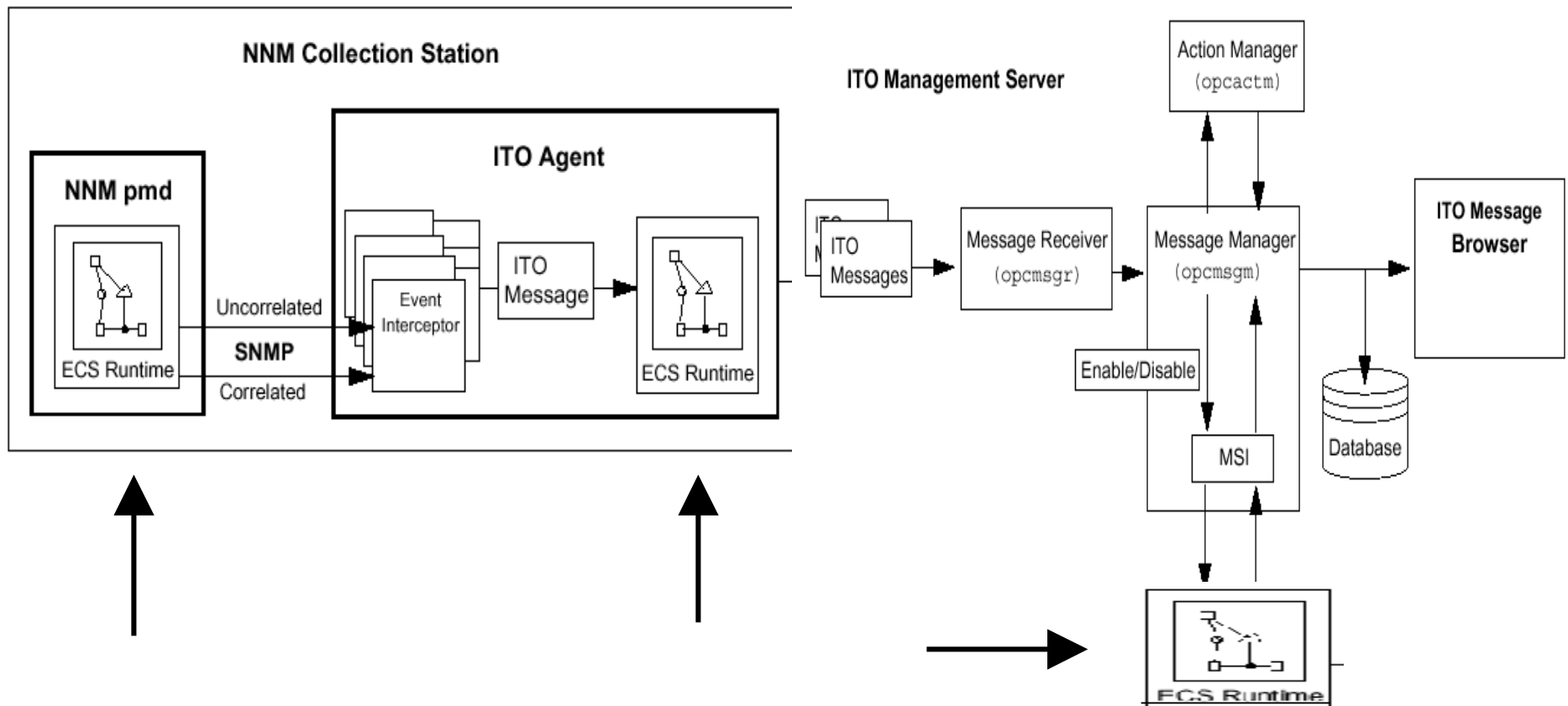
Cook, Simmer, Spice
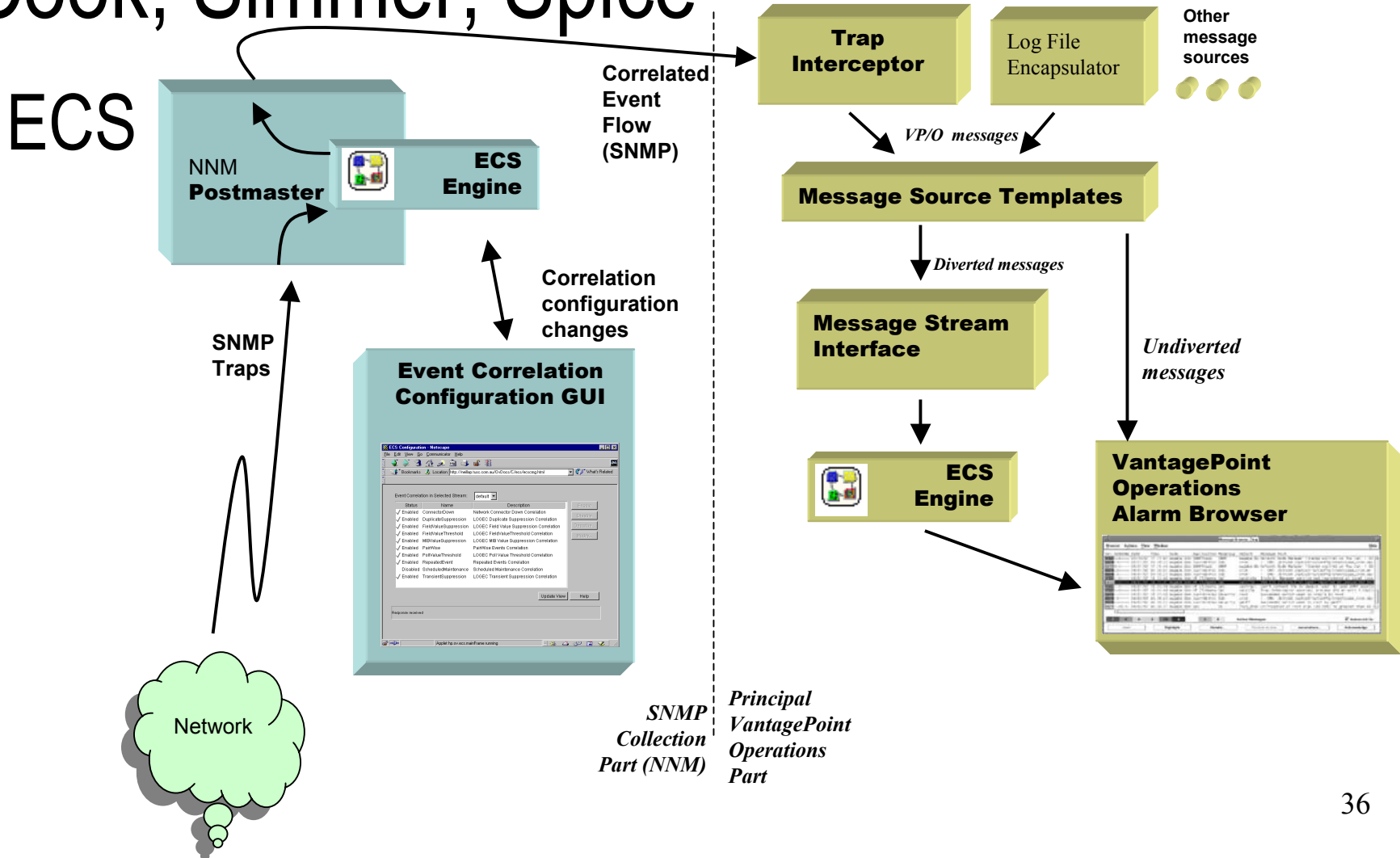
VPO MIB object monitors vs. NNM's *snmpCollect*

- Poll **certain** SNMP MIB Variables to compare against thresholds:
  - From ITO agent nodes running *opcmon* (systems)
  - Useful for cross-platform agents (Empire, CIA, CMU)
  - Data not stored by NNM's *SnmpCollect* database
  - Useful for distributed ITO & NNM for automating fail-overs

- NNM's *snmpCollect*
  - Many functional enhancements to *snmpCollect* in NNM 6.2
  - Better scaling, performance, control.
  - Robust SNMP data grapher, *xnmgraph*

Cook, Simmer, Spice
VPO, SNMP, and ECS

Cook, Simmer, Spice ECS

Trap Interceptor

Log File Encapsulator

Other message sources

VP/O messages

Message Source Templates

Diverted messages

Message Stream Interface

Undiverted messages

Correlated Event Flow (SNMP)

NNM **Postmaster**

ECS Engine

Correlation configuration changes

Event Correlation Configuration GUI

SNMP Traps

ECS Engine

VantagePoint Operations Alarm Browser

Network

SNMP Collection Part (NNM)

Principal VantagePoint Operations Part

36

Cook, Simmer, Spice

ECS Event Correlation

– NNM-based correlation

- Turned on by default for "connector down" built-in circuit

- This ECS circuit suppresses Status Polling event storms

– VPO Agent-based correlation

- Turned on when "suppress duplicate messages" set

– VPO Server-based correlation

- Use to suppress duplicates from multiple NNM collectors

Cook, Simmer, Spice
ECS Event Correlation at VPO Agent

- *opctrapi* registers with pmd for correlated event flow

- Change how *opctrapi* registers in opcinfo:

  - SNMP_EVENT_FLOW [ALL|RAW|CORR]

- *opctrapi* connects to default ECS stream of pmd.

- Specify an alternate ECS stream in the opcinfo file:

  - SNMP_STREAM_NAME <stream_name>

Cook, Simmer, Spice

Final words:

- Its easy to cook, but hard to cook well
- Crawfish look horrible, but taste really really good
  - VPO/SNMP integration looks bad, but results can be good
- If you can't take the heat, get out of the kitchen
  - Some third-party tools may help a lot:
    - Micromuse Netcool
    - Edge Technologies EnPortal

Crawfish facts

Ecrevisse in French

Mudbugs in the deep south

Crawdads in the appalachians

Crayfish up north

The Japanese word for crawfish translates as "cockroach-in-water"

There are about 250 species of crawfish found in the U.S.

90% of all crawfish consumed are either the red swamp or white river species

US annual production of crawfish is around 50,000 tons

Sweden imports about 2,500 tons of crawfish from U.S. per year

China exports of processed red swamp crawfish tail to the US are increasing

40

Recipes

Jambalaya

2 lb chopped white onion	3 lb smoked hot sausage, cut bite size
2 bunches green onion tops	2 cans blackeyed peas
1 large bell pepper	3 lb uncooked rice
5 cloves garlic chopped	1 cup chopped parsley
3 lb salt meat, boiled, bite size	12 cups water
1 tsp. black pepper	1 tsp. red pepper

Saute onions, pepper, garlic, and parsley. Cook until limp. Add salt meat, sausage, blackeye peas with liquid and rice. Add seasoning. Add 12 cups water. Bring to boil; mix well and cover tightly. Cook on lowest heat for 45 minutes. *DO NOT* remove the cover during this time. Remove cover for 10 minutes before serving. (serves 20)

Recipes

Crawfish Étouffée (from Perry Mark Glorioso, of Laplace, LA)

1 pound crawfish tails, with fat
8 tablespoons (1 stick) butter
1 medium - large onion, chopped
2 cloves garlic
2 tablespoons bell pepper, minced
1/2 stalk celery, minced
Green onion tops

2 teaspoons tomato paste
Cayenne pepper
Freshly ground black pepper
Salt
2 tablespoons flour
1 - 2 cups water
Fresh parsley

Melt butter in pot, add flour and stir like hell. Add onions, bell pepper, celery and garlic. Cook until tender, and keep stirring. Add crawfish fat, if possible, and cook down 10-15 minutes. Add tails and tomato paste, then add water. Cook down for 20 minutes or so, but be careful not to overdo it. Add salt and peppers to taste. Cook a little more, then add chopped green onion tops and parsley and cook till ready. Note: Some directions and amounts are intentionally vague ... use the challenge.

Yield: Meal for 4 men or 6 pansies.

Recipes

Étouffée d'écrevisses au maire Joubert -- (from Curtis Joubert, former mayor of the City of Eunice, Louisiana)
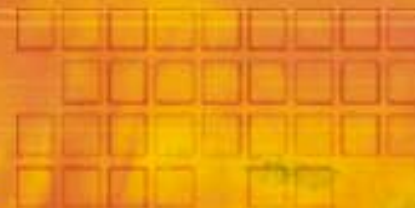
 1 pound crawfish tails
Salt
Black pepper
Onion powder
Garlic powder
4 tablespoons butter

1 medium yellow onion, chopped
2 cloves garlic, minced
1/2 cup finely chopped bell peppers
1/2 cup water or fish stock
1 bunch green onions, chopped, green part only
1 bunch parsley, minced (use Italian parsley)

Season crawfish tails in a bowl with salt, pepper, onion powder and garlic powder. Melt the butter and add the onions, garlic, and bell pepper, stirring constantly, and cook until wilted. Add the water or stock and bring the mixture to a boil. Reduce heat and simmer for 15-20 minutes. Add the crawfish and simmer another 15-20 minutes. Add onion tops and parsley and simmer 5 minutes more. Ladle over hot, long-grain white rice. Serves four.

The End

(Thank you)