We will send you the recording.

Submit your questions anytime. We’ll do Q&A throughout.

Please complete the Exit survey.
Topics for Today

It happens all the time, an engineer shifts a setting for troubleshooting and forgets to put it back when he's done. Another configures a device from memory, rather than the checklist, and a device gets deployed with a default password still in effect. Across town an employee brings a wireless router into work and plugs it into his cubical port so he can have access around the office. Join us for this 30-minute session while we learn -

• How to configure opConfig to collect device configurations and raise alerts to NMIS
• How and when to take action on reported configurations changes
• How to leverage opConfig's setting push capability in response to an event
IT Service Management Maturity Model

Level 0
- Chaotic
  - Ad Hoc
  - Undocumented
  - Unpredictable
  - Multiple help desks
  - Minimal IT operations
  - User call notification

Level 1
- Reactive
  - Fight fires
  - Inventory
  - Desktop software distribution
  - Initiate problem management process
  - Alert and event management
  - Measure component availability (up/down)

Level 2
- Proactive
  - Analyze trends
  - Set thresholds
  - Predict problems
  - Measure application availability
  - Automate
  - Mature problem configuration, change, asset and performance mgmt. processes

Level 3
- Services
  - IT as a service provider
  - Define services, classes, pricing
  - Understand costs
  - Guarantee SLAs
  - Measure and report service availability
  - Integrate processes
  - Capacity Mgmt.

Level 4
- Value
  - IT as a strategic business partner
  - IT and business metric linkage
  - IT/business collaboration improves business process
  - Real-time infrastructure
  - Business planning
  - Manage IT as a Business

Increasing Performance & Value to Organization

Tool Leverage

Operational Process Engineering

Service Delivery Process Engineering

Service & Account Management
Architecting a Solution

**Open-Source**
NMIS: Core performance and fault monitoring

**Commercial Solutions**
opConfig: Capture, track and push configuration changes
opEvents: Advanced event management and response
Useful References

Where can I go when I have questions?

• opConfig Wiki – https://community.opmantek.com/display/opconfig/Home
  • Automating Configuration Changes - https://community.opmantek.com/x/JQH6
• opEvents Wiki – https://community.opmantek.com/display/opEvents/Home
  • Setup Email Notifications and Other Actions - https://community.opmantek.com/x/oYh4AQ
  • Actions and Escalation - https://community.opmantek.com/display/opEvents/Event+Actions+and+Escalation

• Community Questions Board - https://community.opmantek.com/questions
• Support Issues – support@opmantek.com
• Sales – usa@opmantek.com
References

You should bookmark these...

UC Berkley Secure Device Configuration Guideline
https://security.berkeley.edu/secure-device-configuration-guideline

Center for Internet Security
https://www.cisecurity.org/controls/
https://benchmarks.cisecurity.org/en-us/?route=downloads.benchmarks

National Security Agency Security Configuration Guidelines (now hosted at IAD)
MONITORING FOR CONFIGURATION CHANGES WITH opCONFIG
Configuration Change Detection

Focused Goals

• Configuration changes on covered devices should be logged automatically or via established change management processes
• Resource custodians should be alerted when configuration changes are made on covered devices to allow for identification of malicious activities on covered devices

opConfig can capture, track, push and rollback configuration changes for any network connected device or cloud application.

Configuration Change Criteria

When and How are device configurations collected?

- **Device Commands**
  - Command Collection (which commands are run, and how) are defined in `command_sets.nmis`
  - How opConfig talks to a device is defined in cli phrasebooks
  - These can (and should) be customized for your environment

- **Scheduled Collection**
  - Daily/Hourly scheduled through CRON job
  - Commands are defined as to when they should run (i.e. Daily/Hourly/Troubleshooting)

- **On Demand**
  - opConfig includes a robust API that can run from the CLI or called via script
  - opEvents can use the opConfig API for command collection for a specified device
  - Can call one command or a group of commands (i.e. Troubleshooting)

https://community.opmantek.com/display/opconfig/Home
opConfig Collection and Alerting

Queued by CRON job (usually command collection)

Cron Job Runs
opConfig Executes Command Collection
opConfig compares results of Collection
opConfig Generates Change Event
NMIS Receives Change Event
opConfig Links Results to Event
Common Workflow for Configuration Change Detection

This is a starting point for internal discussion

**Identify**
- Device
- Event/Element
- Priority

**Investigate**
- Revisions
- Change Control

**Remediate**
- Add Comments
- Acknowledge

**Close Event**
- After Action
- Actions
- Correlations
ESCALATING THE NODE CONFIGURATION CHANGE
NMIS8 Escalation Policy

What Actions to Take at Each Escalation Period

- System -> System Configuration -> Escalation Policy
- Also: Setup -> Emails, Notifications and Escalations

- Six Built-In Notification Methods
  - Syslog, json, email, ccopy, pager and netsend
  - These can be expanded on
**opEvents**

Advanced Fault Management and Operational Automation

**WHY** – Expands on efforts already done through NMIS, and scientifically improves automated response thereby decreasing workload and improving operational efficiency

- Enhances and builds-on NMIS’ Thresholding, Escalation and Notification systems
- Support whitelisting and blacklisting of events
- Handles event correlation, deduplication, event storms, and event flap
- Allows application of event Actions, or responses to events
- Supports flexible escalation and notification
- Supports custom email templates per contact
Event Processing Flow

These are all background processes...

- Apply Archive List
- Apply Blacklist
- Apply Whitelist
- Correlate Events into Outages
- Deduplicate Events
- Determine Priority
- Conduct Actions
- Start Escalations
Event Actions

All Event Actions are defined in: EventActions.nmis

• Actions are stored in the Script section of EventActions.nmis
• Actions can be called from any section, i.e. Policy, Escalate as script.<i>scriptname()</i>
• Actions can do anything, from troubleshooting to remediative in nature

https://community.opmantek.com/display/opEvents/Event+Actions+and+Escalation
Pushing Configuration Changes

Leveraging opConfig’s Push Capability via opEvents’ Actions

From EventActions.nmis –

Example Policy
'40' => {
    IF => 'node.roleType eq "core" and node.type eq "router" and event.event eq "Node Configuration Change"',
    THEN => 'script.reset_routerconfig()',
    BREAK => 'false'
},

Example Script
'reset_routerconfig' => {
    arguments => 'act=push_configset name=routerconfig at=now+1minute nodes=event.node',
    exec => '/usr/local/omk/bin/opconfig-cli.exe',
    output => 'save'
},

opconfig-cli.pl act=push_configset name='set name' [info=0/1][node=nodeX][nodes=nodeA,nodeB...][at='time spec']
Commercial enquiries:

**Tom Wiri**
Account Executive
+1 (512) 430-4450
usa@opmantek.com

Technical enquiries:

**Mark Henry**
Senior Engineer
+1 (207) 951-2428
markh@opmantek.com