An IT Managers Guide To Network Process Automation

By Keith Sinclair

FirstWave

About the Author

Keith Sinclair
NMIS Founder

Keith Sinclair has a history of designing and developing software and solutions for infrastructure management and operations, having designed and built systems for NetStar, Cisco and many more. Early involvement with Open Source saw the birth of NMIS. Keith has been awarded several patents for expert systems and network management technologies. He has worked with companies all over the world on data centre architecture and design, infrastructure management systems architecture and design and network architecture and design.

An IT Managers guide to Network Process Automation

This guide is designed for IT Managers looking to implement Network Process Automation in their organisation. It discusses the best approach for change management and team buy-in, provides a methodology framework to use when considering the automation of a manual task in a network environment and the steps to take in order to identify an effective test case for your organization.

FirstWave

Automation - Embracing the 4th Industrial Revolution

The delivery of ICT services is changing, what IT people spend time on now is very different to 5, 10 or 25 years ago. Technology evolution cycles will go on, but fundamentals remain the same.
There is no better example of a technology evolution than telephony - not that long ago, every organisation would have phones on every desk, but in the modern Enterprise, people are using computer-based IP telephony (Skype, Hangouts, etc.) and mobile phones.

More and more businesses are opting to remove IP phones from the desks in their offices and there are now very few people involved in the modern enterprise working on telephony, it is just part of IT now and no longer the "other" guys.

Businesses are reliant on IT to function and IT must support the business strategies.

Organizations need to evolve and adjust resourcing to meet these changing business needs.

Business decisions like moving infrastructure into the Cloud (SaaS or public Cloud) or doing something intelligent with the data that had not previously been leveraged for the last few decades requires different resourcing and a different IT department staff skill mix.

Regardless of whether the server is in the data center or the Cloud IT technologies are still not "simple", there is still a server, users are using and they need to connect over a network to access the applications.

Wherever things are located, the business will still need people to troubleshoot problems and resolve issues, but there will be a different mix of IT people available to do this.

With continuously changing teams and increasing skills gaps, how can an IT Manager be confident that system outages are being appropriately monitored and addressed and that the IT team has the knowledge to resolve issues that arise?

> **What is needed is a focus on good operational practices and the definition of a process for troubleshooting IT problems.**
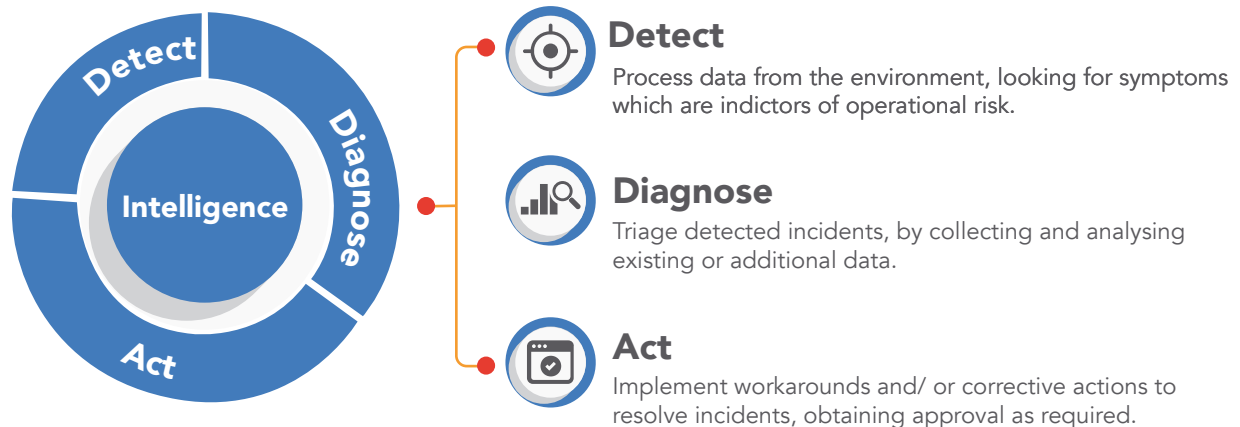
It is basic support 101 but often overlooked for various reasons.

With a defined process the business can now automate parts or a full set of tasks to facilitate end-to-end troubleshooting - from detecting a problem to diagnosing the root cause and acting to fix the problem.

Once the operational process is automated, the mix of IT skills is less critical from a troubleshooting point of view as fewer people can deliver the same result as the larger team used to.

FirstWave

Introducing
Network Process Automation

Detect
Process data from the environment, looking for symptoms which are indictors of operational risk.

Diagnose
Triage detected incidents, by collecting and analysing existing or additional data.

Act
Implement workarounds and/ or corrective actions to resolve incidents, obtaining approval as required.

The Automation process can be summarized by three major steps, Detect, Diagnose and Act. Each of these steps is enhanced with Intelligence, which can be provided by humans or with emerging machine learning technologies.

The high-level process is helpful, but with the additional details of how this would be applied the process becomes more applicable. This detailed process or flow is a methodology for diagnosis and troubleshooting or incidents.

Diagnosis and Troubleshooting Methodology

Once we have a robust methodology for troubleshooting, we can look at automating as many steps as possible so that we can scale how this is carried out in our live IT environment.

FirstWave

Finding the right tasks to support operational decision making

The first step is in detecting issues and presenting them to the operations team in a way which assists them in making decisions; this is a Decision Support System and was one of the motivators behind **NMIS.**

With detection well taken care of by NMIS, we need to look at how people diagnose problems. The concept is based on scientific principles of observation and developing a theory of the cause, once you have a theory of the cause, you can now prove or reject the theory with analysis of data. once you have a theory of the cause, you can now prove or reject the theory with analysis of data.

Creating consistency in the approach to solving common problems

Consistent 'best practice' handling of common issues through automation reduces risk and time to resolution as you will see in the following example of troubleshooting a high CPU load on a Linux server.

The engineer responding to the event may theorise which process was causing the CPU load and would then confirm that theory by running a command like "top" and reviewing the command output. From this they would learn which process was using the CPU - it might have been a different one than they suspected, and they could now decide what is an appropriate corrective action to reduce that CPU load.

However, given there are several different operations people they may all have different theories based on their experiences, and if they have just joined the operations team, maybe those experiences are limited. So wouldn't it be better to have an automatic process look for which process is causing the high CPU load?

Then depending on which process it was, it might be as simple as restarting the process or daemon.

FirstWave

Mapping out processes

In addressing the high CPU load issue, the flow chart for the best practice diagnosis might look like this:

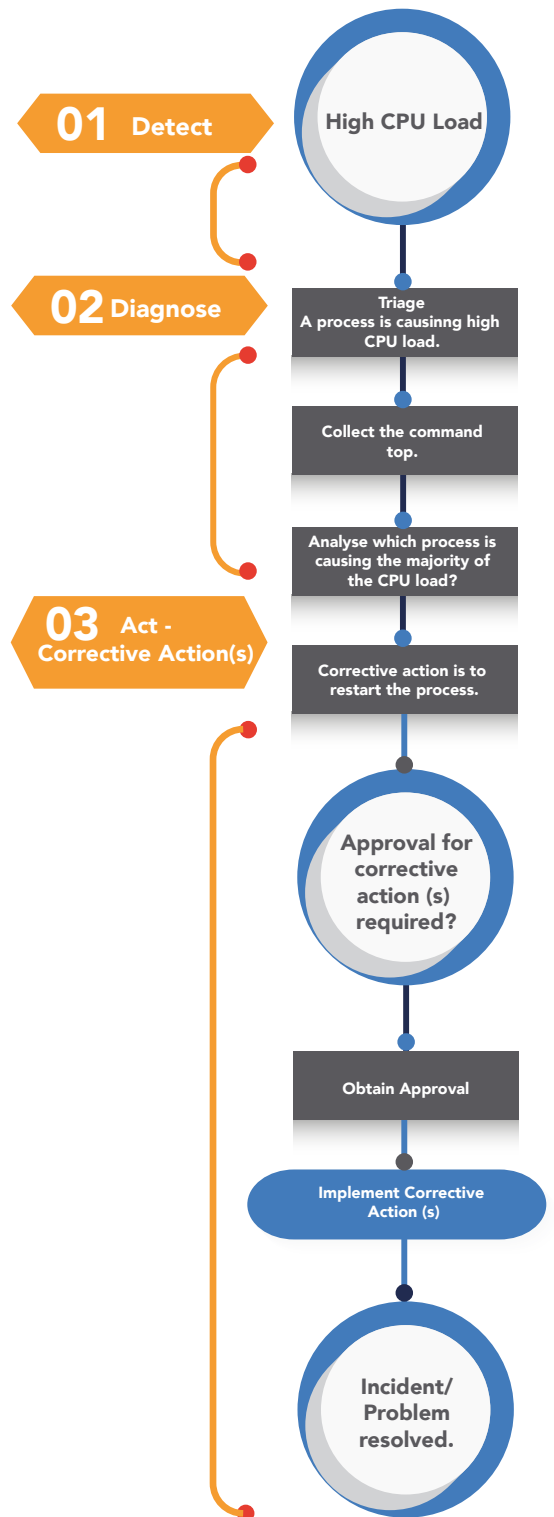This process could be carried out by a human or a computer running FirstWave software.

What is important is that for a given symptom detected, there is a known way to diagnose that issue. This has been determined as the best way to diagnose this problem and when done by an automated process it will be done every time the same way.

This produces consistent, repeatable results.

Another feature of this process is the "Obtain Approval" step, so if this carried out by a human or FirstWave Software there is a step which allows for "Change Management".

When known combinations of symptoms and corrective actions have been proven, this process could be fully automated and no longer require the approval step.

A computer system would learn from this approval step and over time would make recommendations on which processes could be automated.

01 Detect

02 Diagnose

03 Act - Corrective Action(s)

High CPU Load

Triage
A process is causinng high CPU load.

Collect the command top.

Analyse which process is causing the majority of the CPU load?

Corrective action is to restart the process.

Approval for corrective action (s) required?

Obtain Approval

Implement Corrective Action (s)

Incident/ Problem resolved.

High CPU Example

FirstWave

Complementing Existing Technologies

Another example would be where routing protocols do not correct for performance or error related issues; OSPF does not have consideration for interfaces which are dropping packets. As a result, packets are forwarded over interfaces causing applications to be impacted.

NMIS detects when interfaces have errors or are discarding packets and using **opConfig** we can change the router configuration on the fly to increase the cost of the interface in real time. Now OSPF can make better decisions about the true cost of a path and dynamically route around the problem.

The same could be done with interface utilization in near real time with the OSPF cost being updated to reflect the current interface usage.

This would ensure that traffic is following the right path.

Improving Operations to Reduce Cost

With Operations teams using process automation, the efficiency will be increased along with consistently resolving issues regardless of the individual's experiences; this allows the operations team to better meet the needs of the organization (their customers) and deliver high-quality services with higher levels of satisfaction, while reducing the cost of delivery.

Getting Started Checklist

To get started with automation, here is a simple checklist that you can complete with your IT team to get the first process underway:

- Talk to staff to identify a 3-5 step troubleshooting task they regularly do that takes up time and they don't like.

- Ask each staff member to map out the steps that they generally take to diagnose the problem and to resolve it.

- Determine best practice based on the different approaches put forward by the team.

- Have a human follow the process to diagnose the issue next time it is detected to test the process. Time the process.

- Implement software to complete the tested process.

- Record the time saving between the human and computerized process as a measurement of effectiveness.

FirstWave

Learn More

If you would like to learn more about Network process automation and the sorts of processes that can be automated within a modern enterprise IT team, contact our engineering team for a free network assessment.

Book a demo

FirstWave

'*Our game* is always about improving IT operations through intelligent software that is *lower-cost*, more *flexible* and easier **to use**.'

FirstWave

Our passion is to create intelligent software that our service provider partners and customers love.

Get Expert
Solutions

Book a demo

FirstWave is a publicly-listed, global technology company formed in 2004 in Sydney, Australia. FirstWave's globally unique CyberCision platform provides best-in-class cybersecurity technologies, enabling FirstWave's Partners, including some of the world's largest telcos and managed service providers (MSPs), to protect their customers from cyber-attacks, while rapidly growing cybersecurity services revenues at scale.

In January 2022, FirstWave acquired Opmantek Limited (FirstWave), a leading provider of enterprise-grade network management, automation and IT audit software, with 150,000 organisations using their software across 178 countries and enterprise clients including Microsoft, Telmex, Claro, NextLink and NASA.

Integrating CyberCision with FirstWave's flagship Network Management Information System (NMIS) and Open-AudIT product enables FirstWave to provide a comprehensive end-to-end solution for network discovery, management and cybersecurity for its Partners globally.

With over 150,000 organisations now using FirstWave technology, we are well positioned to be a leader of transformational change in the IT Operations and Cybersecurity world.

firstwave.com | connect@firstwave.com