Cisco Automated Fault Management

Reduce OpEx and free up your IT staff to create more value for the business

Network automation speeds reaction time

As companies make the move to digital, the demands on their IT environment will continue to grow. Network automation is one of the only solutions to ride this wave of digital disruption, giving businesses, regardless of size, the tools to keep pace with the competition.

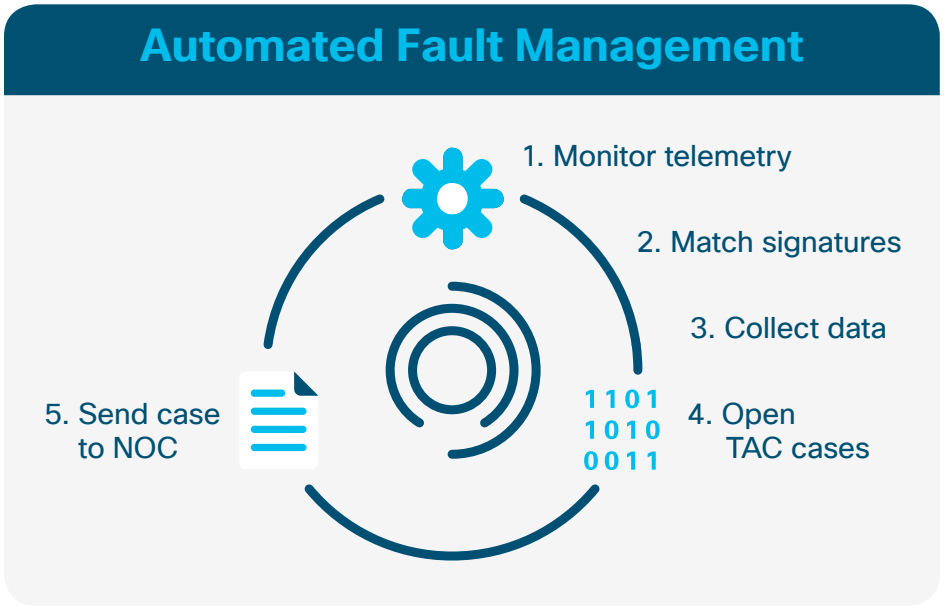
Intelligent automation tools, such as Cisco® Automated Fault Management, have the ability to automatically analyze situations and proactively correct errors in a way that is similar to, yet much faster and more accurate than if performed manually. As an example, when a fault occurs in your IT environment what if you could speed your reaction from hours to minutes, to before it even happens?

Benefits

- Increase speed of event detection and resolution
- Save countless hours of troubleshooting and case management through automation
- Enhance network agility and reliability
- Boost overall subscriber satisfaction – increased uptime provides a better overall customer experience

Automated Fault Management responds to network issues on its own

The data pouring through your network includes millions of syslog messages every day. Among these messages there are warning patterns. If you could spot them, it could save you countless hours of troubleshooting and downtime. That's exactly what Automated Fault Management does. It combines automation and machine learning to work behind the scenes and recognize potential network problems and resolve them.



Powered by Cisco intellectual capital and our industry-leading database of millions of devices worldwide, we collect vast amounts of data. We use that data to identify conditions that indicate urgent network problems that need immediate attention. From there, machine learning is applied to find patterns and trends so our engineers can create an ever-growing global database of signatures.

These signatures are programmed as "triggers" in our fault management service so when one appears during a routine daily report, it automatically activates a sequence of predefined responses, including:

- Generating an email identifying the issue and directing it to the appropriate source
- Opening a case with the Cisco Technical Assistance Center (TAC)
- System self-diagnosis without any human interaction and an automatic list of remediation steps to use to solve the problem

Customized for your IT environment

Every network is different with distinct priorities and vulnerabilities. Automated Fault Management is customized to match your business requirements. You tell us which devices are critical to your operation or if you want TAC case notifications to stay internal. We set up the service to match your preferences.

To start, our engineers collect up to a year's worth of data from your network—virtually billions of device syslog messages. We identify all the faults that have occurred and then pinpoint the sequences that preceded them. We correlate that data with our intellectual capital to create rules, or signatures, specifically for your IT environment. Moving forward, when a pattern appears or an event occurs, our automated fault management service sees it, recognizes it, and responds.

Since deploying Automated Fault Management, a large service provider estimated savings of approximately $8 million annually with a 50% drop in its historic Time-To-Resolution (TTR).

Continuous updates...automatically

Most network signatures have a shelf life. So when you upgrade your network software, configurations, and hardware, the initial signatures may no longer be valid. Getting to know your network is what makes the service even more effective. Machine learning enables us to keep discovering the patterns specific to your IT environment so our ability to identify warning patterns keeps improving. And, we keep getting better at alerting you to faults before they occur. That means we can help free up your IT talent to focus on more strategic activities while increasing the agility and reliability of the IT environment.

Before	After
Historically when a fault occurs, your IT team has to: • Spend countless time and effort to manually pinpoint what happened • Open a ticket • Wait for a response requesting specific information • Locate information, input it, and send back to the TAC • A TAC engineer identifies appropriate steps to take • Your IT team performs recommended remediation activities prescribed by the TAC engineer	• Director runs in the client environment • Leverages library of global and customer signatures • Performs real-time syslog monitoring • Detects an event • Connects to the device to collect information on event detection • Matches data against our global database • Opens a TAC case via an API • Sends a notification to the customer's NOC • Instructs a TAC engineer with the remediation plan

Next steps

For more information, contact your Cisco Services representative or Cisco partner to start the conversation, and learn more.

C45-741224-00 08/18