FirstWave

Automated Remediation & Getting A Good Nights Sleep

E-Book By

Product Engineer
Nick Day

E-BOOK

Automating Your Remediation

A major PaaS provider offering a non-stop compute platform needed to automate theirway around recurring issues to continue guaranteeing their millisecond data loss and recovery SLAs, giving them time to diagnose and remove the underlying problems.

I assisted one of the engineers from a major PaaS provider the other week so he could get back to having a good nights sleep.

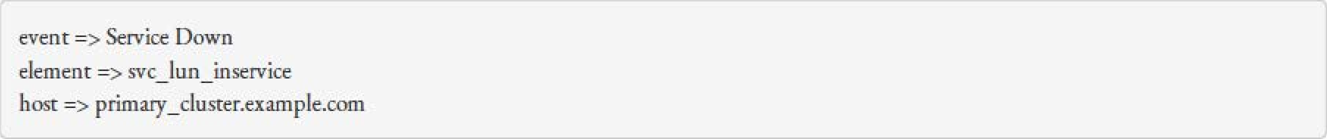
The company he works for offer a non-stop IBM Power PC compute platform and he needed to automate activities his engineers were doing so his platform could be relied on to continue guaranteeing the millisecond data loss and recovery SLAs it was designed for. They knew they needed time to diagnose and remove the underlying problems and so needed a fast and reliable way to fix the issues as they occurred in the meantime.

This E-book describes what was done in this specialist environment but provides a great example of applying remediation automation in any environment. This service provider happens to offer an IBM PowerPC Platform as a Service to banks, utilities, telcos and the like making use of two clusters in two data centres, cross site replication provides High Availability and zero dataloss failover.

The engineers use NMIS, opEvents and opConfig for managing the whole environment. NMIS is used to collect statistics, state and events from the IBM Power PC Cluster instances, NMIS also collects data from the member servers, the Fibre Channel and Ethernet switching and the SAN. Having NMIS meant visibility across the entire environment and all the way down to OS health particularly the underlying daemons, services etc on the Power PC cluster. In this case making use of NMIS's Service management and plugin capabilities to monitor the IBM systems.

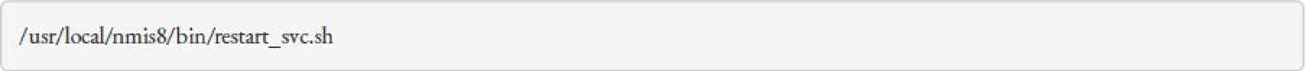
The team were making use of NMIS's server management functions to collect state and performance data from several Nagios plugins for the PowerPC servers. NMIS and opEvents were successfully alerting the team to the fact that SVC replication was failing occasionally by sending notifications via SMS and Email to the right teams. The team were responding to these by following a process to restart the SVC service on the machines, of course this was usually in the middle of the night! They needed a way to automate this remediation task quickly so here is what they did in about 20 minutes to complete the work and without spending money.

Next they looked at the SVC replication events in opEvents by looking at the details tab for one of the previous events. It was decided they only wanted this triggered if the alert was "Service Down" rather than "Service Degraded" and they only wanted it to happen if the service was down on the Primary site not if it was down on the Secondary site. In the details tab of the event they noted the following event attributes:



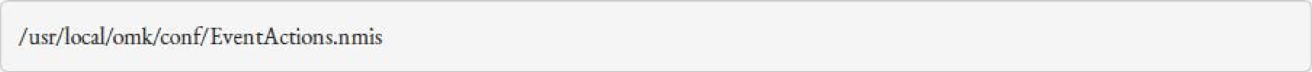
```
event => Service Down
element => svc_lun_inservice
host => primary_cluster.example.com
```

Next they tested a shell script they had used for restarting the svc service remotely, this was simply three remote ssh commands they had been issuing by hand, they placed it on the NMIS server in:



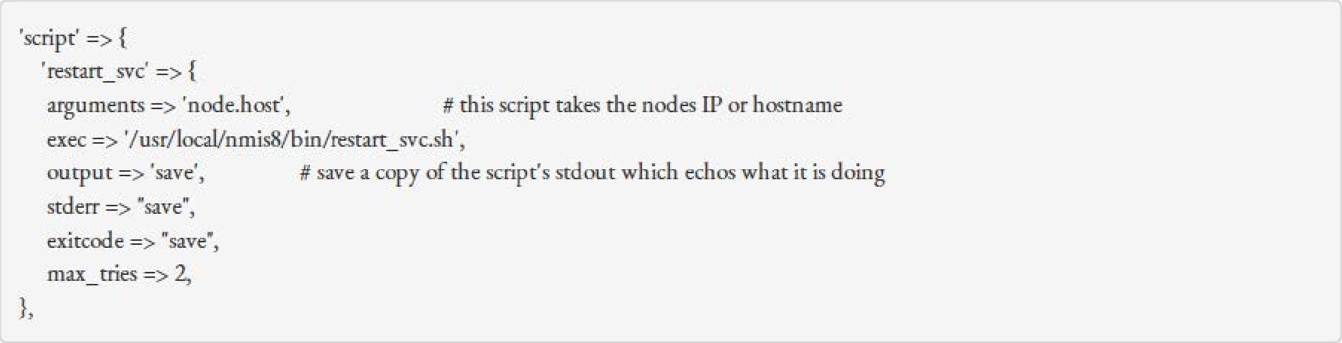
```
/usr/local/nmis8/bin/restart_svc.sh
```

Final piece of the puzzle was to call the script when the event details matched.
So editing the EventActions.nmis file



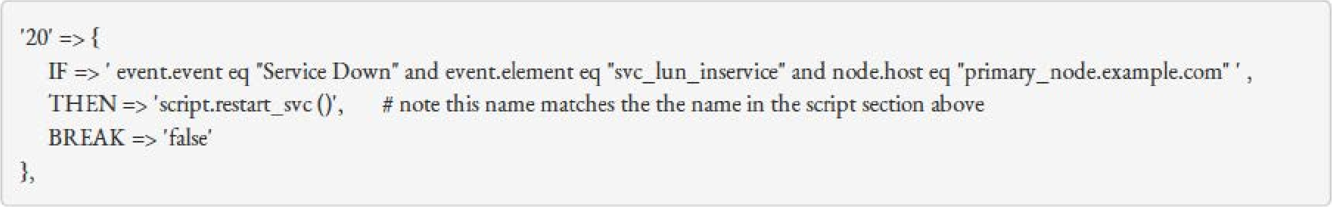
```
/usr/local/omk/conf/EventActions.nmis
```

The following was added:
1. A script action – added to the 'script' section of EventActions.nmis (copying one of the example scripts as an example) they created the follwing:



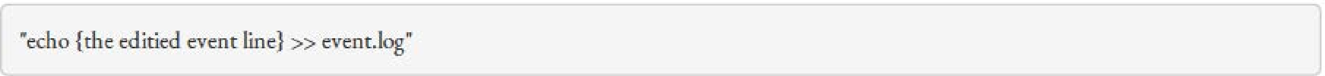
```
'script' => {
  'restart_svc' => {
   arguments => 'node.host',                  # this script takes the nodes IP or hostname
   exec => '/usr/local/nmis8/bin/restart_svc.sh',
   output => 'save',            # save a copy of the script's stdout which echos what it is doing
   stderr => "save",
   exitcode => "save",
   max_tries => 2,
},
```

2. A matching rule – added near the top of EventActions.nmis in the appropriate location (again the easiest was copying and editing one of the existing entries).



```
'20' => {
    IF => ' event.event eq "Service Down" and event.element eq "svc_lun_inservice" and node.host eq "primary_node.example.com" ' ,
    THEN => 'script.restart_svc ()',      # note this name matches the the name in the script section above
    BREAK => 'false'
},
```

Finally they needed a way to test it without actually doing anything or breaking anything. So they first edited the restart script slightly so it only echoed the key commands it would issue on the server. They then found a copy of the service down event in /usr/local/nmis/logs/event.log copied it to the clipboard changed the datestamp(epoch) to now and appended it back to the log



```
"echo {the editied event line} >> event.log"
```

and watched opEvents for the event to appear.

They then looked at the actions section of the event in the GUI and were able to see the script had fired and were able to see everything the script had done, from it's output to it's exit code to it's stderr messages. Finally they changed the script so it actually ran the commands and went home.

That night the svc replication failed – they didn't get emailed or smsed about this time though as the system repaired itself immediately and before the 5 minute escalation time had passed. Job done.

In the meantime after a month of further diagnostics with the network carrier, the data-centre provider the SAN vendor and a team of others they found the underlying issue for the LUN replication, a timeout problem related to cross site Fibre Channel and the additional backup loads happening at night. Couple of timers changed and all good.

FirstWave

Get Your Virtual Machine

Experince the power of FirstWave solutions in one easy-to-install Virtual Machine. This package s curated by FirstWave and is the easiest way to install our apps, including NMIS and Open-AudIT, without the hassel of setting up a server.

Book a demo

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.

firstwavecloud.com | +61 2 9409 7000 | connect@firstwavecloud.com