opEvents Think-Through

Thought process

opEvents ships with a lot of features but what it ships with is not all that it can do. Opmantek's various modules are meant to be tinkered with to give you a product that works specifically for you. With a little thought and planning you and your team can make opEvents and other Opmantek modules act as if they were made custom for your organization.

So opEvents is set up and running and you are able to see every event that is occurring. You are happy knowing any time an event pops up you can clearly see it as well as dig into the event details however, there is still work to be done once the event occurs. You notice one event in particular keeps displaying in the event list. Every time this event shows up you keep having to run the same few commands to troubleshoot and resolve the issue. Ask yourself, "How can I bridge the gap from where our process is now to leveraging the tools I have to get to where I want to be?". You remember that opConfig can run commands automatically and you begin brainstorming on how you can get these modules to do the work so you or your team don't have to.

Basic event automation

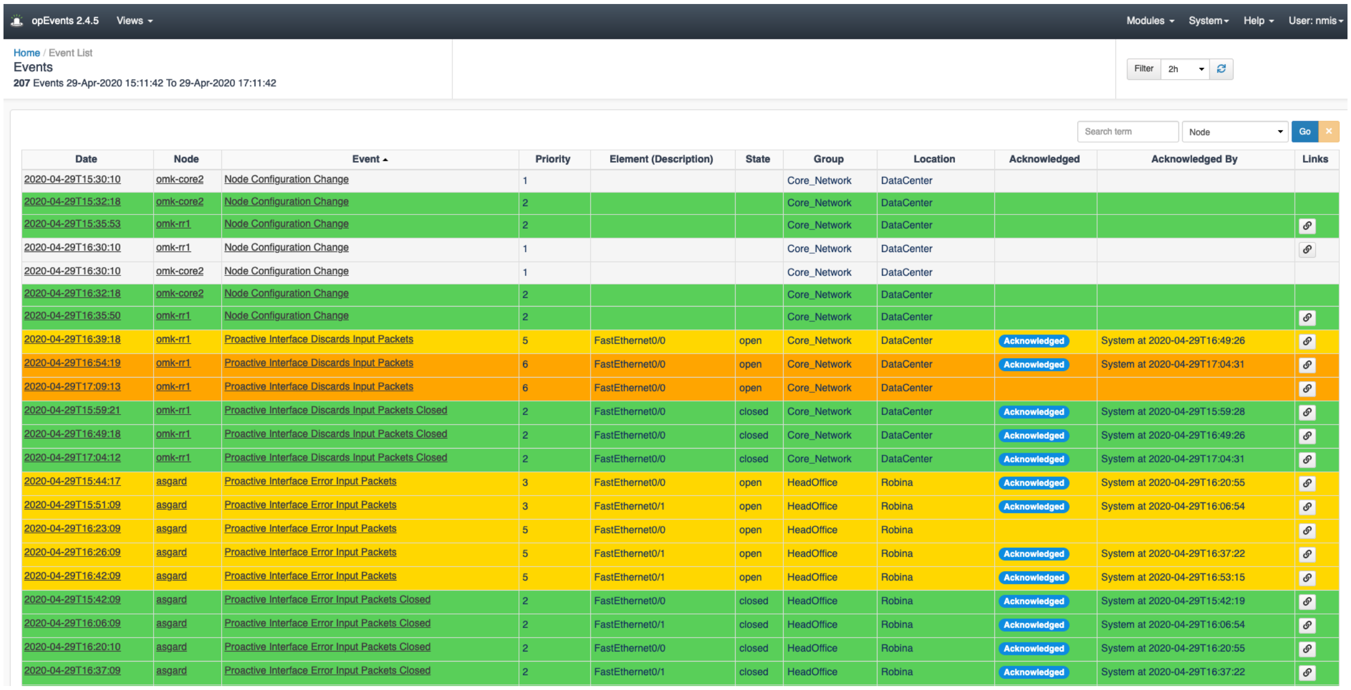
Event automation can be completed in four steps:

1. Identify the top network events you respond to frequently (daily, weekly, etc.)
2. List the steps you take to troubleshoot and remediate when the issue occurs.
3. Identify how these steps can be automated.
4. Create an action to respond to the event.

Step 1: Identify top network events you respond to frequently.

Gather up a group of your architects, NOC engineers, customer service representatives, etc. and list the top 3-4 issues that each group deals with commonly.

You may already have an idea of what network events you and your team respond to frequently but should you need a little help you can take a look at the Events view in opEvents.



Home / Event List

Events

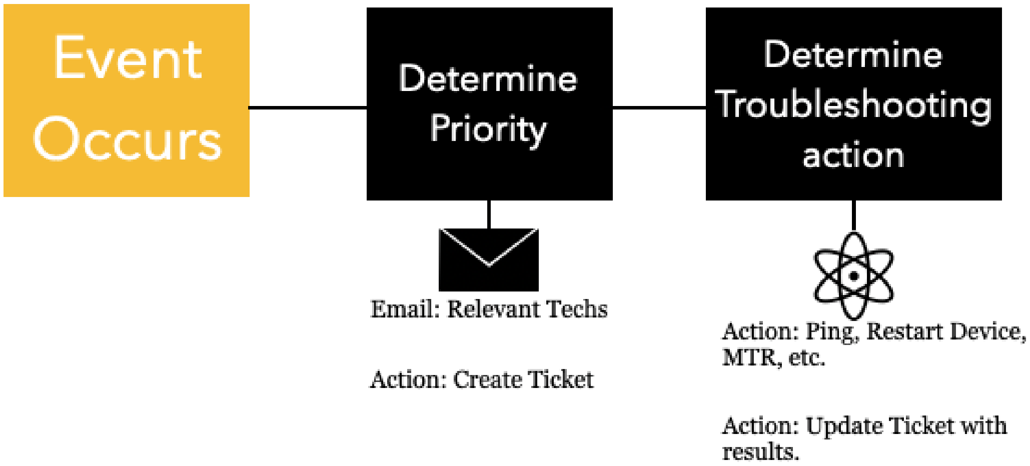
207 Events 29-Apr-2020 15:11:42 To 29-Apr-2020 17:11:42

Date	Node	Event ▲	Priority	Element (Description)	State	Group	Location	Acknowledged	Acknowledged By	Links
2020-04-29T15:30:10	omk-core2	Node Configuration Change	1			Core_Network	DataCenter			
2020-04-29T15:32:18	omk-core2	Node Configuration Change	2			Core_Network	DataCenter			
2020-04-29T15:35:53	omk-rr1	Node Configuration Change	2			Core_Network	DataCenter			🔗
2020-04-29T16:30:10	omk-rr1	Node Configuration Change	1			Core_Network	DataCenter			🔗
2020-04-29T16:30:10	omk-core2	Node Configuration Change	1			Core_Network	DataCenter			
2020-04-29T16:32:18	omk-core2	Node Configuration Change	2			Core_Network	DataCenter			
2020-04-29T16:35:50	omk-rr1	Node Configuration Change	2			Core_Network	DataCenter			🔗
2020-04-29T16:39:18	omk-rr1	Proactive Interface Discards Input Packets	5	FastEthernet0/0	open	Core_Network	DataCenter	Acknowledged	System at 2020-04-29T16:49:26	🔗
2020-04-29T16:54:19	omk-rr1	Proactive Interface Discards Input Packets	6	FastEthernet0/0	open	Core_Network	DataCenter	Acknowledged	System at 2020-04-29T17:04:31	🔗
2020-04-29T17:09:13	omk-rr1	Proactive Interface Discards Input Packets	6	FastEthernet0/0	open	Core_Network	DataCenter			🔗
2020-04-29T15:59:21	omk-rr1	Proactive Interface Discards Input Packets Closed	2	FastEthernet0/0	closed	Core_Network	DataCenter	Acknowledged	System at 2020-04-29T15:59:28	🔗
2020-04-29T16:49:18	omk-rr1	Proactive Interface Discards Input Packets Closed	2	FastEthernet0/0	closed	Core_Network	DataCenter	Acknowledged	System at 2020-04-29T16:49:26	🔗
2020-04-29T17:04:12	omk-rr1	Proactive Interface Discards Input Packets Closed	2	FastEthernet0/0	closed	Core_Network	DataCenter	Acknowledged	System at 2020-04-29T17:04:31	🔗
2020-04-29T15:44:17	asgard	Proactive Interface Error Input Packets	3	FastEthernet0/0	open	HeadOffice	Robina	Acknowledged	System at 2020-04-29T16:20:55	🔗
2020-04-29T15:51:09	asgard	Proactive Interface Error Input Packets	3	FastEthernet0/1	open	HeadOffice	Robina	Acknowledged	System at 2020-04-29T16:06:54	🔗
2020-04-29T16:23:09	asgard	Proactive Interface Error Input Packets	5	FastEthernet0/0	open	HeadOffice	Robina			🔗
2020-04-29T16:26:09	asgard	Proactive Interface Error Input Packets	5	FastEthernet0/1	open	HeadOffice	Robina	Acknowledged	System at 2020-04-29T16:37:22	🔗
2020-04-29T16:42:09	asgard	Proactive Interface Error Input Packets	5	FastEthernet0/1	open	HeadOffice	Robina	Acknowledged	System at 2020-04-29T16:53:15	🔗
2020-04-29T15:42:09	asgard	Proactive Interface Error Input Packets Closed	2	FastEthernet0/0	closed	HeadOffice	Robina	Acknowledged	System at 2020-04-29T15:42:19	🔗
2020-04-29T16:06:09	asgard	Proactive Interface Error Input Packets Closed	2	FastEthernet0/1	closed	HeadOffice	Robina	Acknowledged	System at 2020-04-29T16:06:54	🔗
2020-04-29T16:20:10	asgard	Proactive Interface Error Input Packets Closed	2	FastEthernet0/0	closed	HeadOffice	Robina	Acknowledged	System at 2020-04-29T16:20:55	🔗
2020-04-29T16:37:09	asgard	Proactive Interface Error Input Packets Closed	2	FastEthernet0/1	closed	HeadOffice	Robina	Acknowledged	System at 2020-04-29T16:37:22	🔗

More information on opEvents and its features can be found HERE

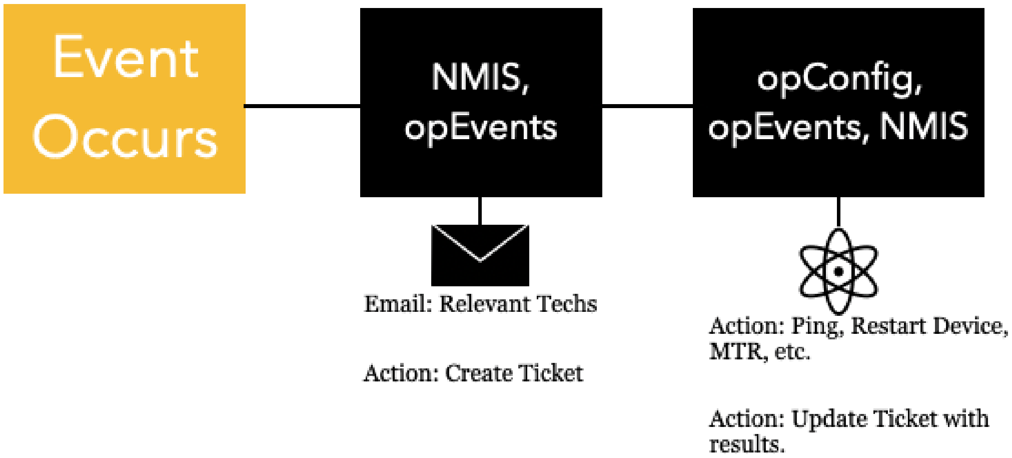
Step 2: List the steps taken to troubleshoot and remediate issues.

From the list of top network events gathered in step 1 figure out what are the steps and processes your team typically takes to troubleshoot and remediate these events. Gather examples of each issue from your team members and come up with a plan.


Event Occurs
Determine Priority
Determine Troubleshooting action
Email: Relevant Techs
Action: Create Ticket
Action: Ping, Restart Device, MTR, etc.
Action: Update Ticket with results.

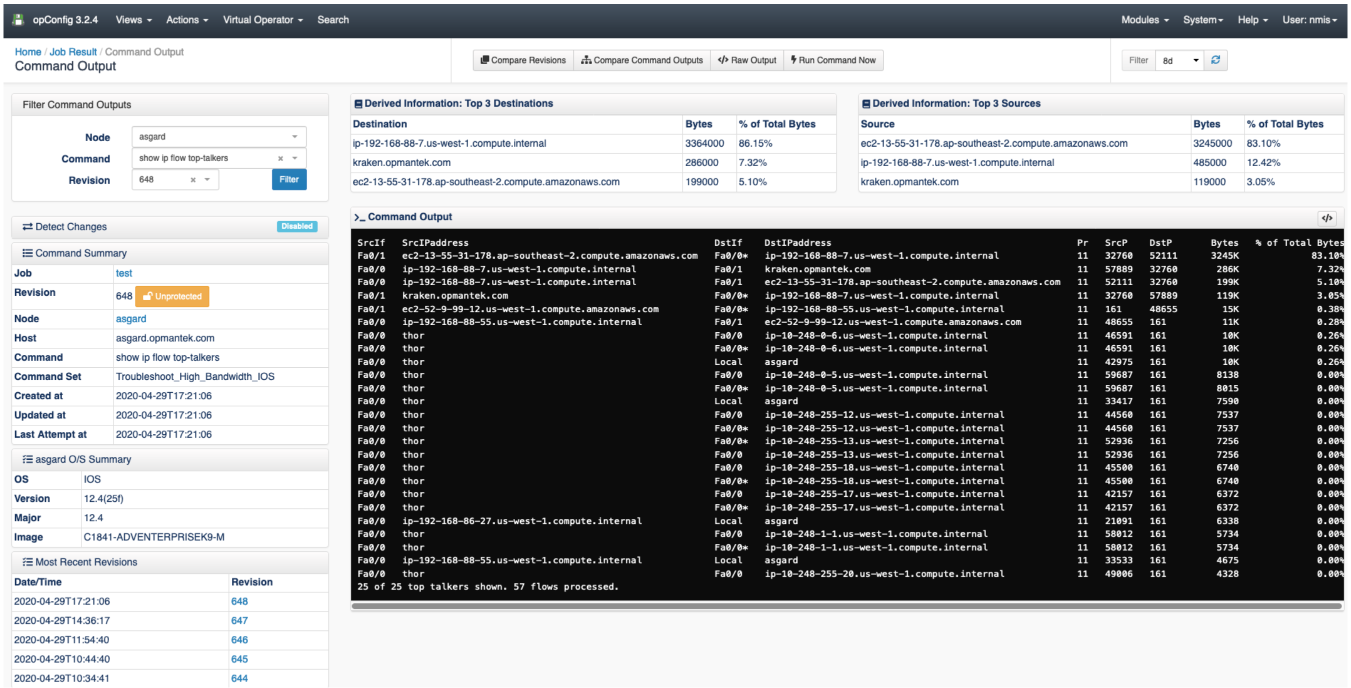
Step 3: Identify how these steps can be automated.

With the information from step 1 and step 2 you can then figure out how to automate these actions by leveraging the tools you have in your Opmantek arsenal.



Step 4: Create an action to respond to the event.

You and your team decide to use the Virtual Operator feature in opConfig to simplify and automate troubleshooting. Any time one of these common events comes in you have a plan for immediate troubleshooting and remediation.



Command Output

Filter Command Outputs

Node: asgard
Command: show ip flow top-talkers
Revision: 648
Filter: 8d

Derived Information: Top 3 Destinations

Destination	Bytes	% of Total Bytes
ip-192-168-88-7.us-west-1.compute.internal	3364000	86.15%
kraken.opmantek.com	286000	7.32%
ec2-13-55-31-178.ap-southeast-2.compute.amazonaws.com	199000	5.10%

Derived Information: Top 3 Sources

Source	Bytes	% of Total Bytes
ec2-13-55-31-178.ap-southeast-2.compute.amazonaws.com	3245000	83.10%
ip-192-168-88-7.us-west-1.compute.internal	485000	12.42%
kraken.opmantek.com	119000	3.05%

Command Summary

Job	test
Revision	648
Node	asgard
Host	asgard.opmantek.com
Command	show ip flow top-talkers
Command Set	Troubleshoot_High_Bandwidth_IOS
Created at	2020-04-29T17:21:06
Updated at	2020-04-29T17:21:06
Last Attempt at	2020-04-29T17:21:06

asgard O/S Summary

OS	IOS
Version	12.4(25f)
Major	12.4
Image	C1841-ADVENTERPRISEK9-M

Most Recent Revisions

Date/Time	Revision
2020-04-29T17:21:06	648
2020-04-29T14:36:17	647
2020-04-29T11:54:40	646
2020-04-29T10:44:40	645
2020-04-29T10:34:41	644

>_ Command Output

```
SrcIf    SrcIPaddress                                           DstIf    DstIPaddress                                           Pr   SrcP    DstP     Bytes   % of Total Bytes
Fa0/1    ec2-13-55-31-178.ap-southeast-2.compute.amazonaws.com  Fa0/0*   ip-192-168-88-7.us-west-1.compute.internal             11   32760   52111    3245K             83.10%
Fa0/0    ip-192-168-88-7.us-west-1.compute.internal             Fa0/1    kraken.opmantek.com                                    11   57889   32760     286K              7.32%
Fa0/0    ip-192-168-88-7.us-west-1.compute.internal             Fa0/1    ec2-13-55-31-178.ap-southeast-2.compute.amazonaws.com  11   52111   32760     199K              5.10%
Fa0/1    kraken.opmantek.com                                    Fa0/0*   ip-192-168-88-7.us-west-1.compute.internal             11   32760   57889     119K              3.05%
Fa0/1    ec2-52-9-99-12.us-west-1.compute.amazonaws.com         Fa0/0*   ip-192-168-88-55.us-west-1.compute.internal            11   161     48655      15K              0.38%
Fa0/0    ip-192-168-88-55.us-west-1.compute.internal            Fa0/1    ec2-52-9-99-12.us-west-1.compute.amazonaws.com         11   48655   161        11K              0.28%
Fa0/0    thor                                                   Fa0/0    ip-10-248-0-6.us-west-1.compute.internal               11   46591   161        10K              0.26%
Fa0/0    thor                                                   Fa0/0*   ip-10-248-0-6.us-west-1.compute.internal               11   46591   161        10K              0.26%
Fa0/0    thor                                                   Local    asgard                                                 11   42975   161        10K              0.26%
Fa0/0    thor                                                   Fa0/0    ip-10-248-0-5.us-west-1.compute.internal               11   59687   161       8138              0.00%
Fa0/0    thor                                                   Fa0/0*   ip-10-248-0-5.us-west-1.compute.internal               11   59687   161       8015              0.00%
Fa0/0    thor                                                   Local    asgard                                                 11   33417   161       7590              0.00%
Fa0/0    thor                                                   Fa0/0    ip-10-248-255-12.us-west-1.compute.internal            11   44560   161       7537              0.00%
Fa0/0    thor                                                   Fa0/0*   ip-10-248-255-12.us-west-1.compute.internal            11   44560   161       7537              0.00%
Fa0/0    thor                                                   Fa0/0*   ip-10-248-255-13.us-west-1.compute.internal            11   52936   161       7256              0.00%
Fa0/0    thor                                                   Fa0/0    ip-10-248-255-13.us-west-1.compute.internal            11   52936   161       7256              0.00%
Fa0/0    thor                                                   Fa0/0    ip-10-248-255-18.us-west-1.compute.internal            11   45500   161       6740              0.00%
Fa0/0    thor                                                   Fa0/0*   ip-10-248-255-18.us-west-1.compute.internal            11   45500   161       6740              0.00%
Fa0/0    thor                                                   Fa0/0    ip-10-248-255-17.us-west-1.compute.internal            11   42157   161       6372              0.00%
Fa0/0    thor                                                   Fa0/0*   ip-10-248-255-17.us-west-1.compute.internal            11   42157   161       6372              0.00%
Fa0/0    ip-192-168-86-27.us-west-1.compute.internal            Local    asgard                                                 11   21091   161       6338              0.00%
Fa0/0    thor                                                   Fa0/0    ip-10-248-1-1.us-west-1.compute.internal               11   58012   161       5734              0.00%
Fa0/0    thor                                                   Fa0/0*   ip-10-248-1-1.us-west-1.compute.internal               11   58012   161       5734              0.00%
Fa0/0    ip-192-168-88-55.us-west-1.compute.internal            Local    asgard                                                 11   33533   161       4675              0.00%
Fa0/0    thor                                                   Fa0/0    ip-10-248-255-20.us-west-1.compute.internal            11   49006   161       4328              0.00%
25 of 25 top talkers shown. 57 flows processed.
```

Where to go from here?

You now have your top events automatically troubleshooted, tickets automatically created, relevant employees alerted and remediation completed. Next, you may want to gather up that same group of NOC engineers, customer service representatives, etc. and again discuss the next batch of top network events. Now that these common issues are taken care of what are the next top network events we can follow this same process with to automatic event resolution. Eventually by following and repeating this same process you could have an almost fully autonomous network.