Solution Brief

anuta networks

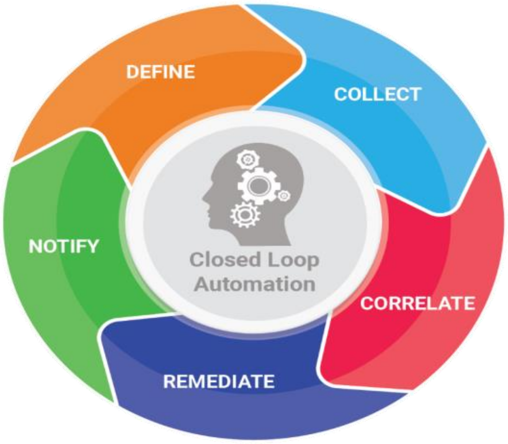
Alerting & Closed Loop Automation with ATOM

Delivers Next-generation Smart & Self-healing Networks

Key Capabilities

- Increase network visibility & awareness to build more predictable networks
- Automate troubleshooting techniques
- Build your own remediation workflows
- Offers alert routing, alert enrichment & alert correlation
- Improve MTTR in a multi-vendor network environment
- Achieve noise reduction through alert grouping & alert suppression
- Realize consistent problem resolution

Automation is a strategic consideration for most organizations today. It enables operational efficiency and rapid service delivery. With 5G use cases such as network slicing, maintaining SLAs will be a daunting task for Service Providers. Enterprises need an always-available network to offer uninterrupted services and remain in business. In this extreme competition world, organizations are also looking beyond Day-0 and have a desire to eliminate manual and time-consuming troubleshooting techniques. However, legacy automation tools tend to be open-ended and fail to ingest the required information to take remediation action.



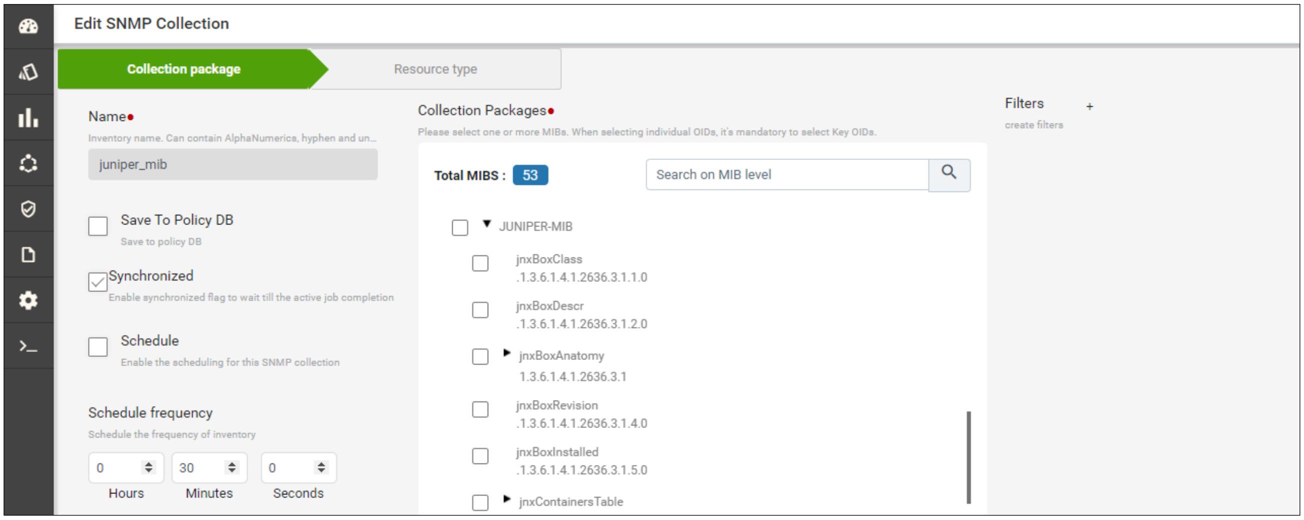
Closed Loop Automation (CLA) is the most efficient and disruptive way to automate well-known and defined troubleshooting techniques in large and complex networks. An integrated platform approach that brings together the best of automation, collection, and monitoring capabilities, positions Anuta ATOM to deliver several value-added use cases. Anuta ATOM offers organizations a framework to baseline network behavior, collect feedback, and take remediation actions to ensure the highest level of service assurance in dynamic network environments. ATOM uses data and analytics to assess network occurrences such as faults and congestion and accordingly remediates any issues. It also allows organizations to take that first step towards self-healing and autonomous networking, thus facilitating a focus on improving productivity and digital transformation.

Collect network data that matters

Anuta ATOM offers data collection capabilities for various datasets such as SNMP, Model-driven or streaming telemetry, and SNMP traps across the multi-vendor network infrastructure. ATOM's Closed-Loop Automation utilizes the data to baseline the network behavior. The performance data is processed and stored into an industry-leading time-series database that forms ATOM's performance management foundation.

SNMP Collection

ATOM supports all the industry specified MIBs and offers many of them out-of-box. Additional SNMP MIBs can be packaged and uploaded to ATOM for immediate consumption. A collection profile can be created in ATOM to trigger the SNMP collection. The profiles offer a selection of MIBs and OIDs, choice of collection frequency and schedule. The operational data collected through SNMP is stored on a Policy DB in ATOM, whereas the performance data is maintained on a Time-series DB.



Edit SNMP Collection

Collection package | Resource type

Name•
Inventory name. Can contain AlphaNumerics, hyphen and un...
juniper_mib

□ Save To Policy DB
Save to policy DB

☑ Synchronized
Enable synchronized flag to wait till the active job completion

□ Schedule
Enable the scheduling for this SNMP collection

Schedule frequency
Schedule the frequency of inventory
0 Hours | 30 Minutes | 0 Seconds

Collection Packages•
Please select one or more MIBs. When selecting individual OIDs, it's mandatory to select Key OIDs.

Total MIBS : 53
Search on MIB level

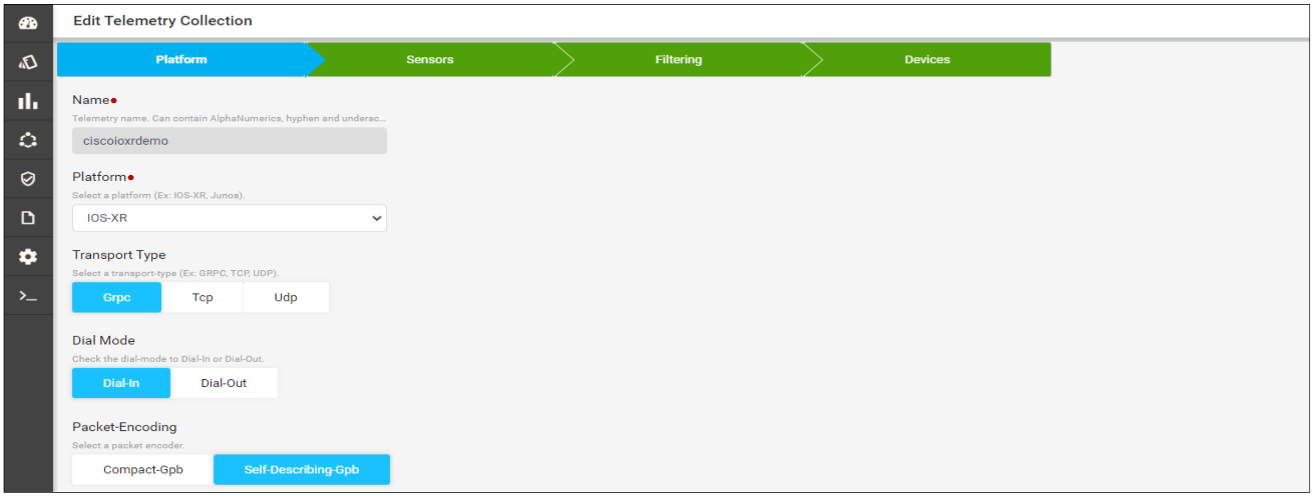
□ ▼ JUNIPER-MIB
□ jnxBoxClass .1.3.6.1.4.1.2636.3.1.1.0
□ jnxBoxDescr .1.3.6.1.4.1.2636.3.1.2.0
□ ▸ jnxBoxAnatomy 1.3.6.1.4.1.2636.3.1
□ jnxBoxRevision .1.3.6.1.4.1.2636.3.1.4.0
□ jnxBoxInstalled .1.3.6.1.4.1.2636.3.1.5.0
□ ▸ jnxContainersTable

Filters +
create filters

SNMP Collection profile

Streaming Telemetry Collection

ATOM supports streaming telemetry collection from multi-vendor devices. The collection capabilities include support for GRPC, TCP & UDP for transport, dial modes, data filtering, and packet encoding along with the choice of sensors and methods to control their collection. ATOM supports the creation of the telemetry profile on vendor devices or matches an already existing one.



Edit Telemetry Collection

Platform | Sensors | Filtering | Devices

Name•
Telemetry name. Can contain AlphaNumerics, hyphen and undersc...
ciscoioxrdemo

Platform•
Select a platform (Ex: IOS-XR, Junos).
IOS-XR

Transport Type
Select a transport-type (Ex: GRPC, TCP, UDP).
Grpc | Tcp | Udp

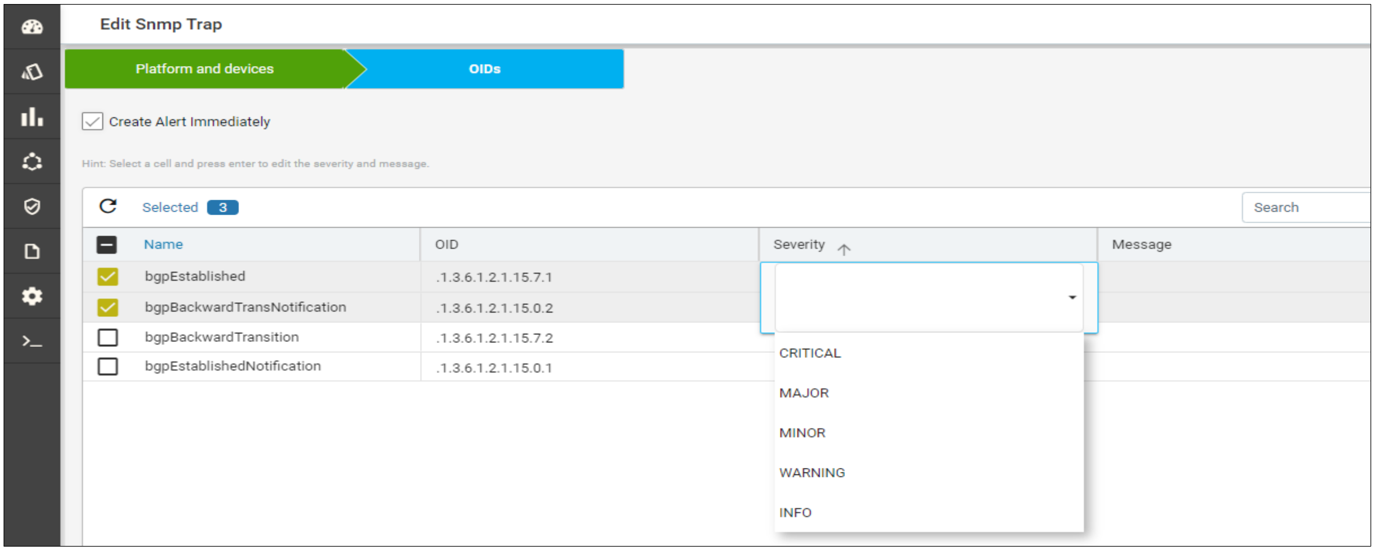
Dial Mode
Check the dial-mode to Dial-In or Dial-Out.
Dial-In | Dial-Out

Packet-Encoding
Select a packet encoder.
Compact-Gpb | Self-Describing-Gpb

Streaming Telemetry Settings

SNMP Traps Collection

To track any emergency alerts, ATOM supports SNMP traps. The SNMP MIBs available in ATOM aids in the SNMP traps collection. In addition to the choice of OIDs, an alert can be generated immediately to the global ATOM alert window when an SNMP trap surfaces. An appropriate severity and a corresponding alert message can be applied to the newly generated alert.



☑ Create Alert Immediately

Hint: Select a cell and press enter to edit the severity and message.

	Name	OID	Severity	Message
☑	bgpEstablished	.1.3.6.1.2.1.15.7.1		
☑	bgpBackwardTransNotification	.1.3.6.1.2.1.15.0.2		
□	bgpBackwardTransition	.1.3.6.1.2.1.15.7.2		
□	bgpEstablishedNotification	.1.3.6.1.2.1.15.0.1		

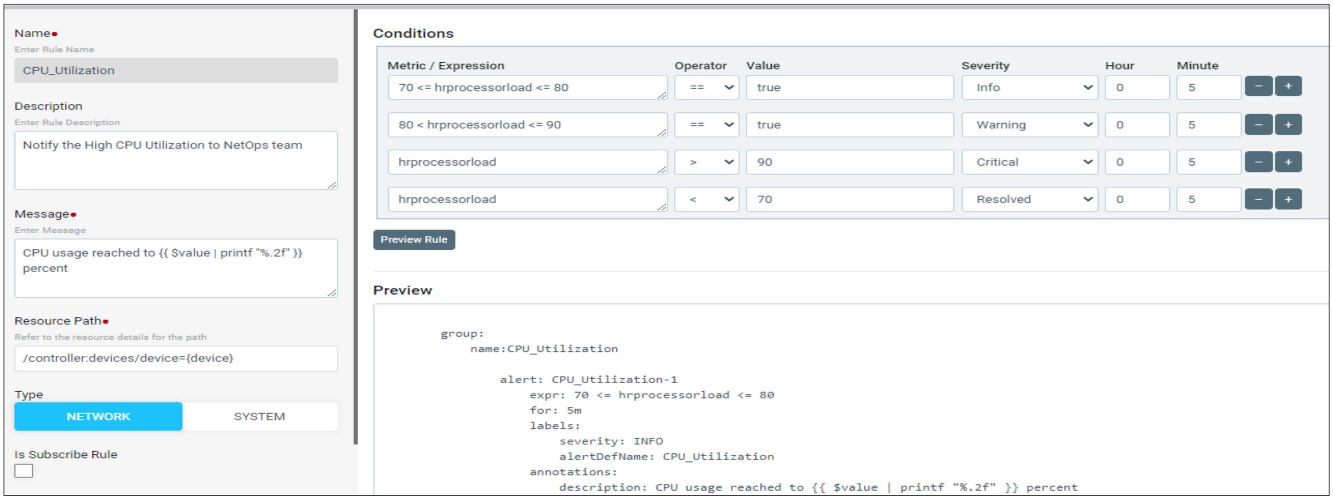
SNMP Traps Profile

Define the KPI thresholds for the network

ATOM provides a flexible framework for network architects to customize thresholds, triggers, and notifications. The condition can be expressed in the form of a query against ATOM's time-series DB utilizing SNMP or Streaming telemetry data. Mathematical operators aid in defining a threshold to the condition. In addition to the severity assignment to the impending alert, alert condition helps setting an urgency to the alert generation. The alert generation can be instantaneous or based on monitoring over time. The preview gives a detailed view of the alerting rules that define the KPI thresholds for the organization.

Alerts have two different categories in ATOM. The system alerts are ATOM specific alerts where ATOM components, licensing, infrastructure components, etc. are monitored and reported on the breach. The network alerts are specific to the network ATOM is keeping an eye on. Few examples of alert definition in ATOM is shown below.

In the screenshot below, a multi-level condition is defined to track the network's CPU utilization.



Name
Enter Rule Name
CPU_Utilization

Description
Enter Rule Description
Notify the High CPU Utilization to NetOps team

Message
Enter Message
CPU usage reached to {{ $value | printf "%.2f" }} percent

Resource Path
Refer to the resource details for the path
/controller:devices/device={device}

Type

Is Subscribe Rule
□

Conditions

Metric / Expression	Operator	Value	Severity	Hour	Minute
70 <= hrprocessorload <= 80	==	true	Info	0	5
80 < hrprocessorload <= 90	==	true	Warning	0	5
hrprocessorload	>	90	Critical	0	5
hrprocessorload	<	70	Resolved	0	5

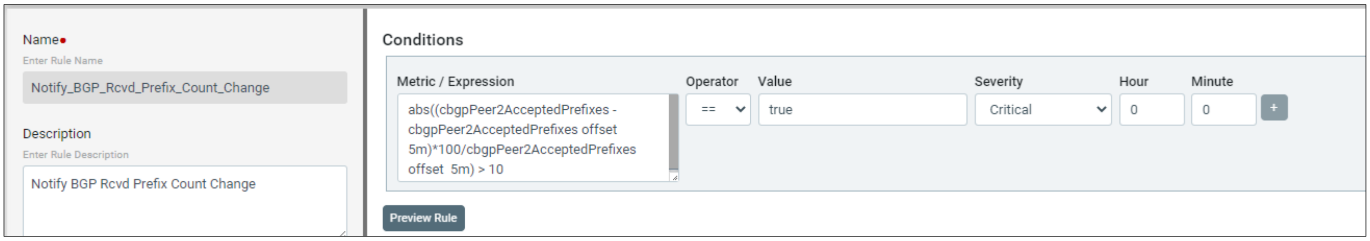
Preview

```
group:
    name:CPU_Utilization

        alert: CPU_Utilization-1
            expr: 70 <= hrprocessorload <= 80
            for: 5m
            labels:
                severity: INFO
                alertDefName: CPU_Utilization
            annotations:
                description: CPU usage reached to {{ $value | printf "%.2f" }} percent
```

Alert Definition

The alert definition below monitors the variation in the number of BGP prefixes over 5 minutes.



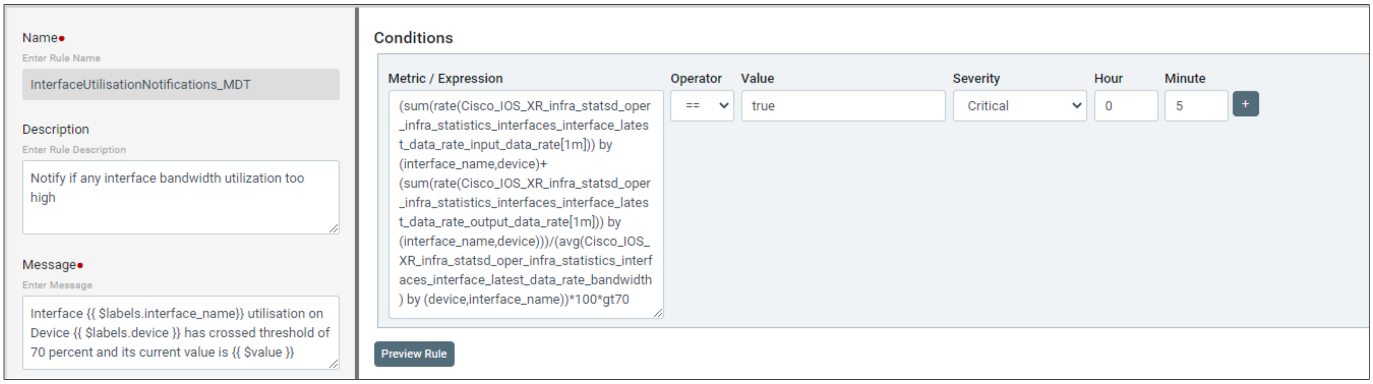
Name●
Enter Rule Name
Notify_BGP_Rcvd_Prefix_Count_Change
Description
Enter Rule Description
Notify BGP Rcvd Prefix Count Change

Conditions

Metric / Expression	Operator	Value	Severity	Hour	Minute
abs((cbgpPeer2AcceptedPrefixes - cbgpPeer2AcceptedPrefixes offset 5m)*100/cbgpPeer2AcceptedPrefixes offset 5m) > 10	==	true	Critical	0	0

Alert Definition using SNMP

An alert definition using streaming telemetry sensors to track interface utilization is shown below.



Name●
Enter Rule Name
InterfaceUtilisationNotifications_MDT
Description
Enter Rule Description
Notify if any interface bandwidth utilization too high
Message●
Enter Message
Interface {{ $labels.interface_name}} utilisation on Device {{ $labels.device }} has crossed threshold of 70 percent and its current value is {{ $value }}

Conditions

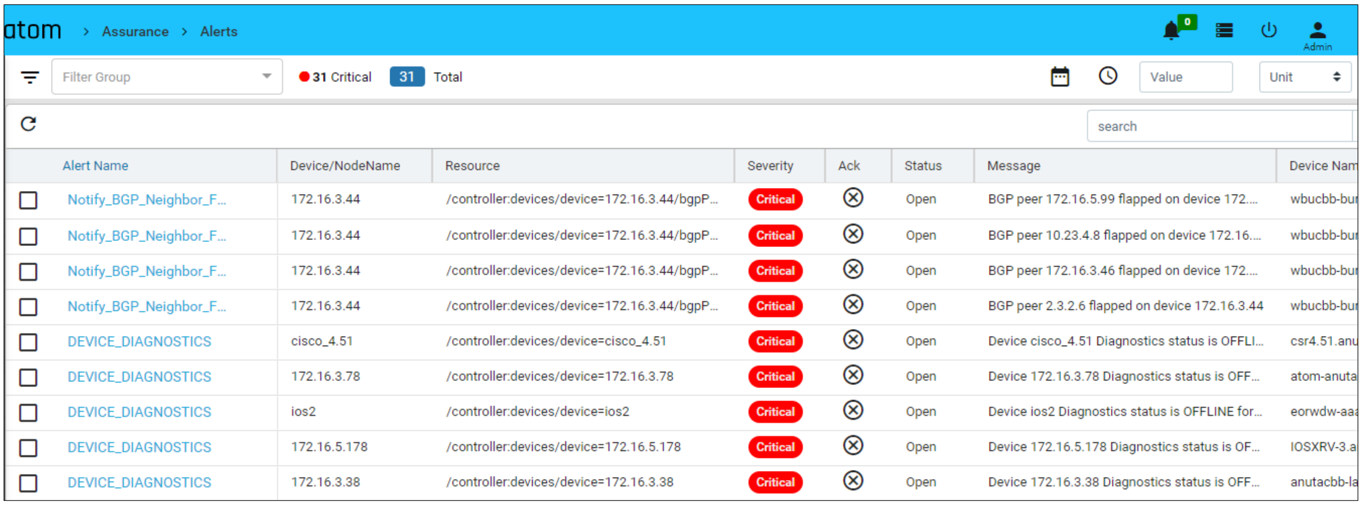
Metric / Expression	Operator	Value	Severity	Hour	Minute
(sum(rate(Cisco_IOS_XR_infra_statsd_oper_infra_statistics_interfaces_interface_latest_data_rate_input_data_rate[1m])) by (interface_name,device)+ (sum(rate(Cisco_IOS_XR_infra_statsd_oper_infra_statistics_interfaces_interface_latest_data_rate_output_data_rate[1m])) by (interface_name,device)))/(avg(Cisco_IOS_XR_infra_statsd_oper_infra_statistics_interfaces_interface_latest_data_rate_bandwidth) by (device,interface_name))*100*gt70	==	true	Critical	0	5

Alert Definition using Streaming Telemtry

It is also essential to display the alerts appropriately with meaningful information. ATOM offers custom messaging of alerts to offer additional value during a triage. How ATOM can enrich an existing alert is discussed in the upcoming sections.

Alert Generation

ATOM uses the data collected from SNMP, Streaming telemetry, and SNMP traps for alert generation. The collection frequency of each of these datasets forms a vital trigger for alerts. The data received is compared to the alert definition metrics to determine the alert generation. The network alerts are available at the device level and in the global alerts view.



● 31 Critical 31 Total

	Alert Name	Device/NodeName	Resource	Severity	Ack	Status	Message	Device Nam
□	Notify_BGP_Neighbor_F...	172.16.3.44	/controller:devices/device=172.16.3.44/bgpP...	Critical	⊗	Open	BGP peer 172.16.5.99 flapped on device 172....	wbucbb-bu
□	Notify_BGP_Neighbor_F...	172.16.3.44	/controller:devices/device=172.16.3.44/bgpP...	Critical	⊗	Open	BGP peer 10.23.4.8 flapped on device 172.16....	wbucbb-bu
□	Notify_BGP_Neighbor_F...	172.16.3.44	/controller:devices/device=172.16.3.44/bgpP...	Critical	⊗	Open	BGP peer 172.16.3.46 flapped on device 172....	wbucbb-bu
□	Notify_BGP_Neighbor_F...	172.16.3.44	/controller:devices/device=172.16.3.44/bgpP...	Critical	⊗	Open	BGP peer 2.3.2.6 flapped on device 172.16.3.44	wbucbb-bu
□	DEVICE_DIAGNOSTICS	cisco_4.51	/controller:devices/device=cisco_4.51	Critical	⊗	Open	Device cisco_4.51 Diagnostics status is OFFLI...	csr4.51.anu
□	DEVICE_DIAGNOSTICS	172.16.3.78	/controller:devices/device=172.16.3.78	Critical	⊗	Open	Device 172.16.3.78 Diagnostics status is OFF...	atom-anuta
□	DEVICE_DIAGNOSTICS	ios2	/controller:devices/device=ios2	Critical	⊗	Open	Device ios2 Diagnostics status is OFFLINE for...	eorwdw-aa
□	DEVICE_DIAGNOSTICS	172.16.5.178	/controller:devices/device=172.16.5.178	Critical	⊗	Open	Device 172.16.5.178 Diagnostics status is OF...	IOSXRV-3.a
□	DEVICE_DIAGNOSTICS	172.16.3.38	/controller:devices/device=172.16.3.38	Critical	⊗	Open	Device 172.16.3.38 Diagnostics status is OFF...	anutacbb-la

Global Alerts view

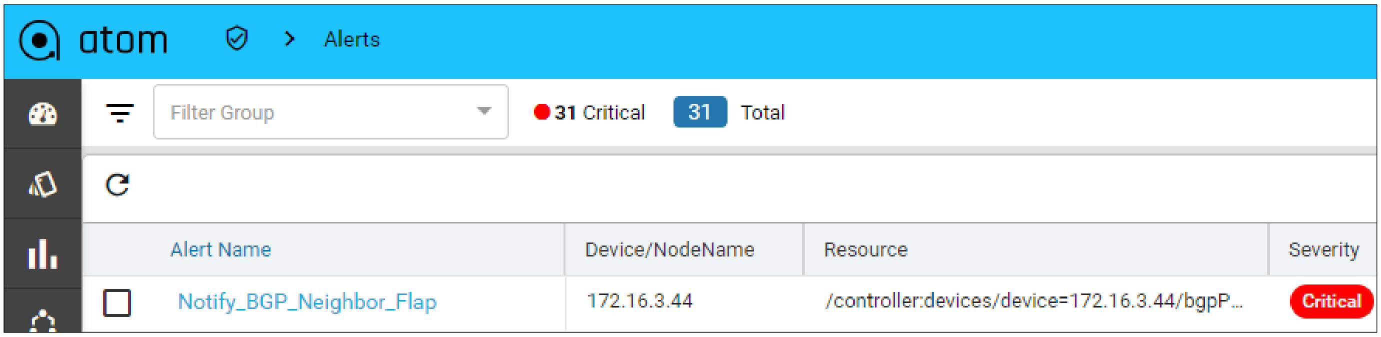
ATOM’s Alerting Framework

One of the main reason organizations resort to monitoring is “Alerting”. There is no point in monitoring tons of metrics if the system cannot alert any network discrepancies. But alerting can turn unpleasant if not done in the right way. An alert should not become a constant set of interruptions to the network teams.

After careful deliberation, Anuta ATOM has been modeled, keeping in mind the operational challenges of service providers and enterprises.

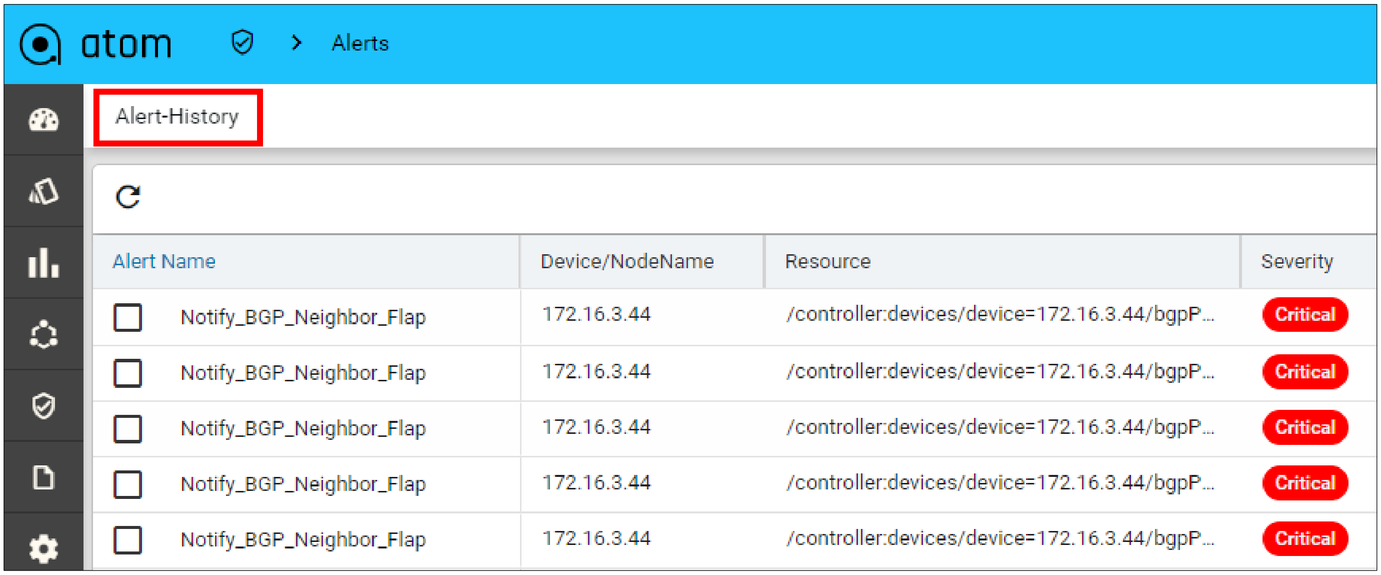
Alert Grouping

Alert grouping in ATOM categorizes alerts of similar nature into a single alert. Alert grouping is essential when many devices/resources are affected, causing a sudden burst of alerts simultaneously. For example, a BGP neighbor flap may generate several instances of the alert. ATOM's alert manager performs grouping of such similar alerts and furnishes a single and latest instance of the alert showing the exact service instance or resource affected. A click on the newest alert will show all the occurrences of the specific alert.



	Alert Name	Device/NodeName	Resource	Severity
□	Notify_BGP_Neighbor_Flap	172.16.3.44	/controller:devices/device=172.16.3.44/bgpP...	Critical

Grouped Alert



	Alert Name	Device/NodeName	Resource	Severity
□	Notify_BGP_Neighbor_Flap	172.16.3.44	/controller:devices/device=172.16.3.44/bgpP...	Critical
□	Notify_BGP_Neighbor_Flap	172.16.3.44	/controller:devices/device=172.16.3.44/bgpP...	Critical
□	Notify_BGP_Neighbor_Flap	172.16.3.44	/controller:devices/device=172.16.3.44/bgpP...	Critical
□	Notify_BGP_Neighbor_Flap	172.16.3.44	/controller:devices/device=172.16.3.44/bgpP...	Critical
□	Notify_BGP_Neighbor_Flap	172.16.3.44	/controller:devices/device=172.16.3.44/bgpP...	Critical

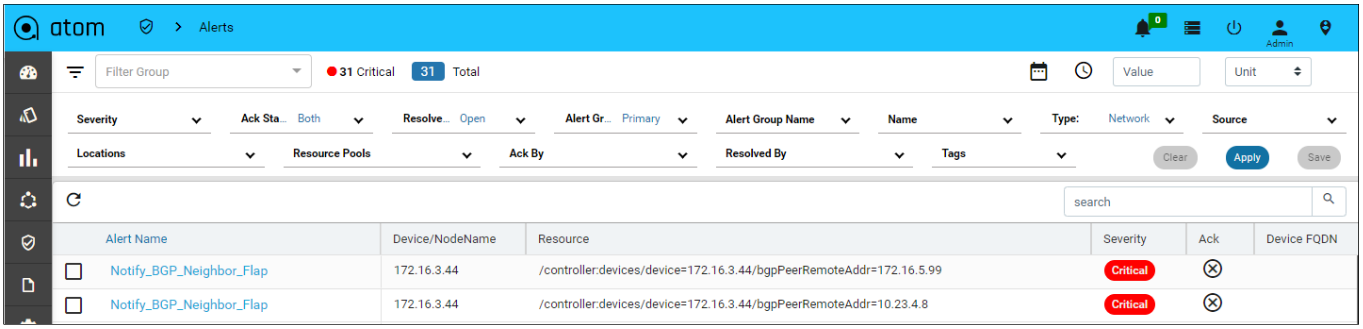
Alert History

Alert Suppression during maintenance windows

ATOM offers alert suppression for a given time. Alert suppression is an essential feature for network teams to avoid a storm of alerts due to planned activities. For example, if a maintenance activity is scheduled on a particular device, incoming alerts from the device can be suppressed based on ATOM's silence criteria.

Alert filtering

ATOM offers alert filtering to narrow down the displayed alerts based on customer criteria. The filtering options offered include a mix of severity, alert status, location, alert definition, etc. A choice of single criteria or a combination of query filter categories displays the matching alerts. The filters can also be saved and reserved for future use in scenarios such as resolution.



31 Critical 31 Total

Severity | Ack Sta... Both | Resolve... Open | Alert Gr... Primary | Alert Group Name | Name | Type: Network | Source

Locations | Resource Pools | Ack By | Resolved By | Tags

	Alert Name	Device/NodeName	Resource	Severity	Ack	Device FQDN
□	Notify_BGP_Neighbor_Flap	172.16.3.44	/controller:devices/device=172.16.3.44/bgpPeerRemoteAddr=172.16.5.99	Critical	⊗	
□	Notify_BGP_Neighbor_Flap	172.16.3.44	/controller:devices/device=172.16.3.44/bgpPeerRemoteAddr=10.23.4.8	Critical	⊗	

Alert Filtering

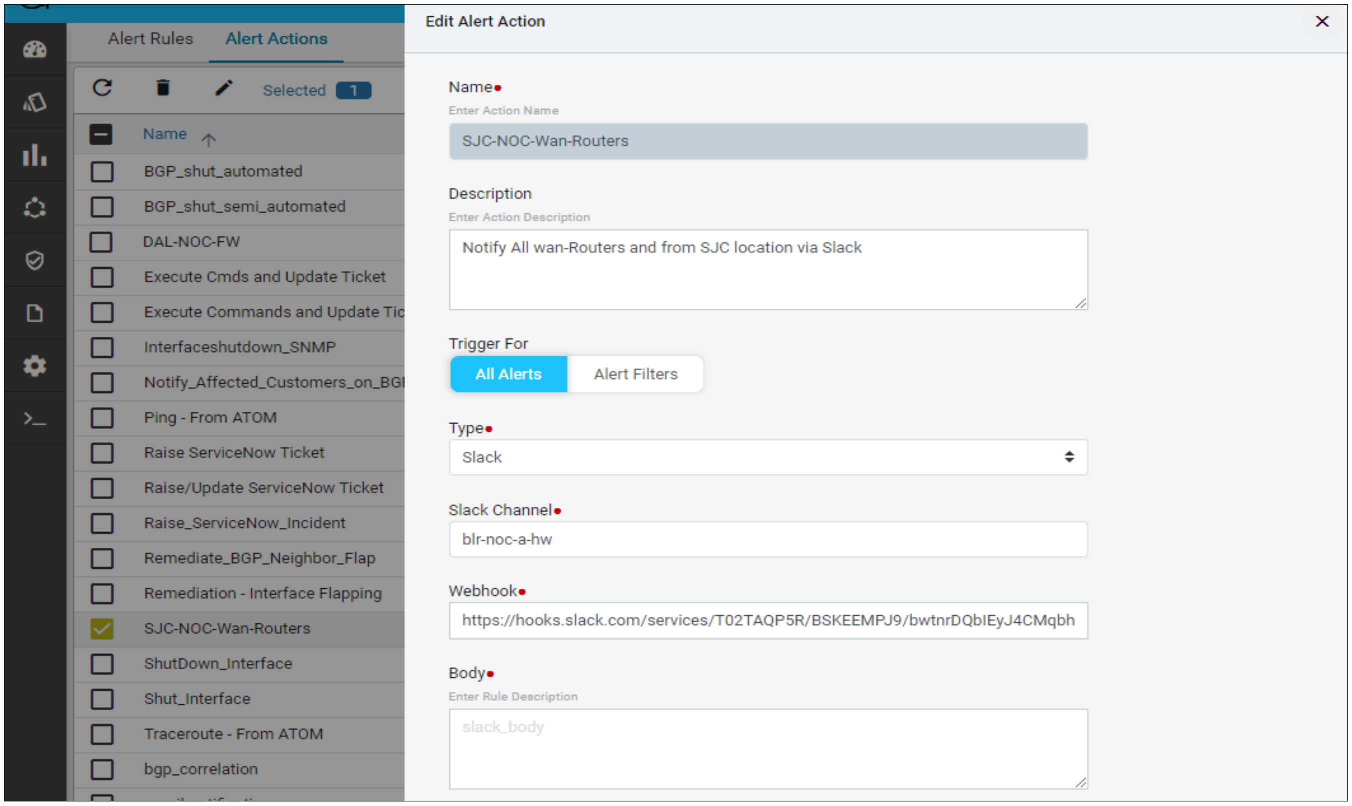
Notify & Remediate with Alert Actions

Mean-time-to-repair (MTTR) or reducing incident resolution time is a crucial metric for Network teams. ATOM offers alert actions that can speed up troubleshooting and resolution, thus offering significant improvements to MTTR. Offering additional information in the generated alerts, logging tickets at the click of a button, leveraging self-help actions, resolving issues, and much more. ATOM understands the network faults and offers the right solution to handle the daily issues.

As part of ATOM's alert actions, alert routing, and workflows help organizations achieve desired outcomes.

Alert Routing

Alerts must reach the teams responsible for those alerts. But alert notifications are not just through emails. Organizations use collaboration tools such as Slack for their daily interactions. There is an expectation of tying the network operations into the existing business processes to keep a tab on network events. ATOM realizes this need by offering out-of-box slack integration as part of its Alert routing feature in addition to the Email support. In the upcoming versions of ATOM, integrations with other collaboration tools via webhooks are planned.



Alert Rules | Alert Actions

Selected 1

	Name
□	BGP_shut_automated
□	BGP_shut_semi_automated
□	DAL-NOC-FW
□	Execute Cmds and Update Ticket
□	Execute Commands and Update Tic
□	Interfaceshutdown_SNMP
□	Notify_Affected_Customers_on_BGI
□	Ping - From ATOM
□	Raise ServiceNow Ticket
□	Raise/Update ServiceNow Ticket
□	Raise_ServiceNow_Incident
□	Remediate_BGP_Neighbor_Flap
□	Remediation - Interface Flapping
☑	SJC-NOC-Wan-Routers
□	ShutDown_Interface
□	Shut_Interface
□	Traceroute - From ATOM
□	bgp_correlation

Edit Alert Action

Name●
Enter Action Name
SJC-NOC-Wan-Routers

Description
Enter Action Description
Notify All wan-Routers and from SJC location via Slack

Trigger For
[✓ All Alerts] Alert Filters

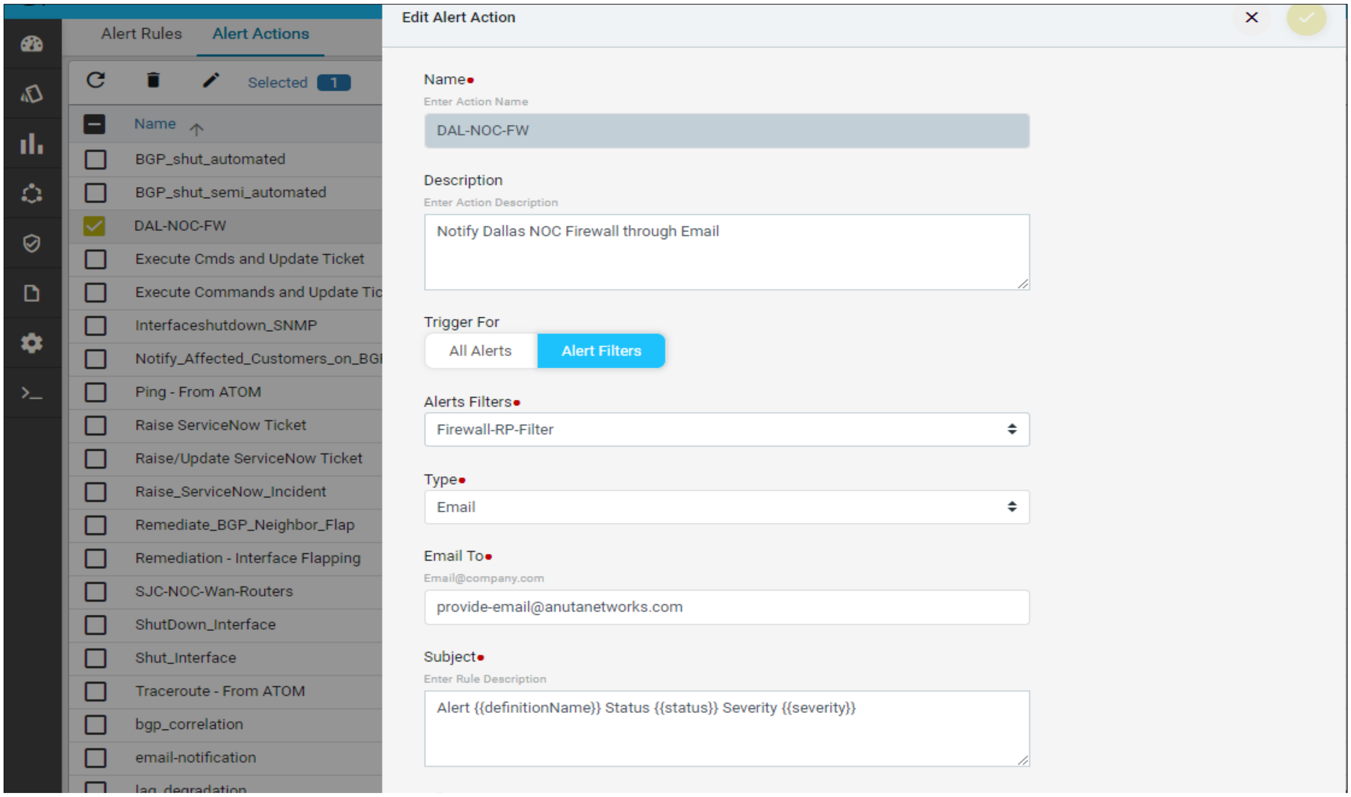
Type●
Slack

Slack Channel●
blr-noc-a-hw

Webhook●
https://hooks.slack.com/services/T02TAQP5R/BSKEEMPJ9/bwtnrDQbIEyJ4CMqbh

Body●
Enter Rule Description
slack_body

Alert Routing via Slack



Alert Rules | Alert Actions

Selected 1

	Name
□	BGP_shut_automated
□	BGP_shut_semi_automated
☑	DAL-NOC-FW
□	Execute Cmds and Update Ticket
□	Execute Commands and Update Tic
□	Interfaceshutdown_SNMP
□	Notify_Affected_Customers_on_BGI
□	Ping - From ATOM
□	Raise ServiceNow Ticket
□	Raise/Update ServiceNow Ticket
□	Raise_ServiceNow_Incident
□	Remediate_BGP_Neighbor_Flap
□	Remediation - Interface Flapping
□	SJC-NOC-Wan-Routers
□	ShutDown_Interface
□	Shut_Interface
□	Traceroute - From ATOM
□	bgp_correlation
□	email-notification
□	lag_degradation

Edit Alert Action

Name●
Enter Action Name
DAL-NOC-FW

Description
Enter Action Description
Notify Dallas NOC Firewall through Email

Trigger For
All Alerts [✓ Alert Filters]

Alerts Filters●
Firewall-RP-Filter

Type●
Email

Email To●
Email@company.com
provide-email@anutanetworks.com

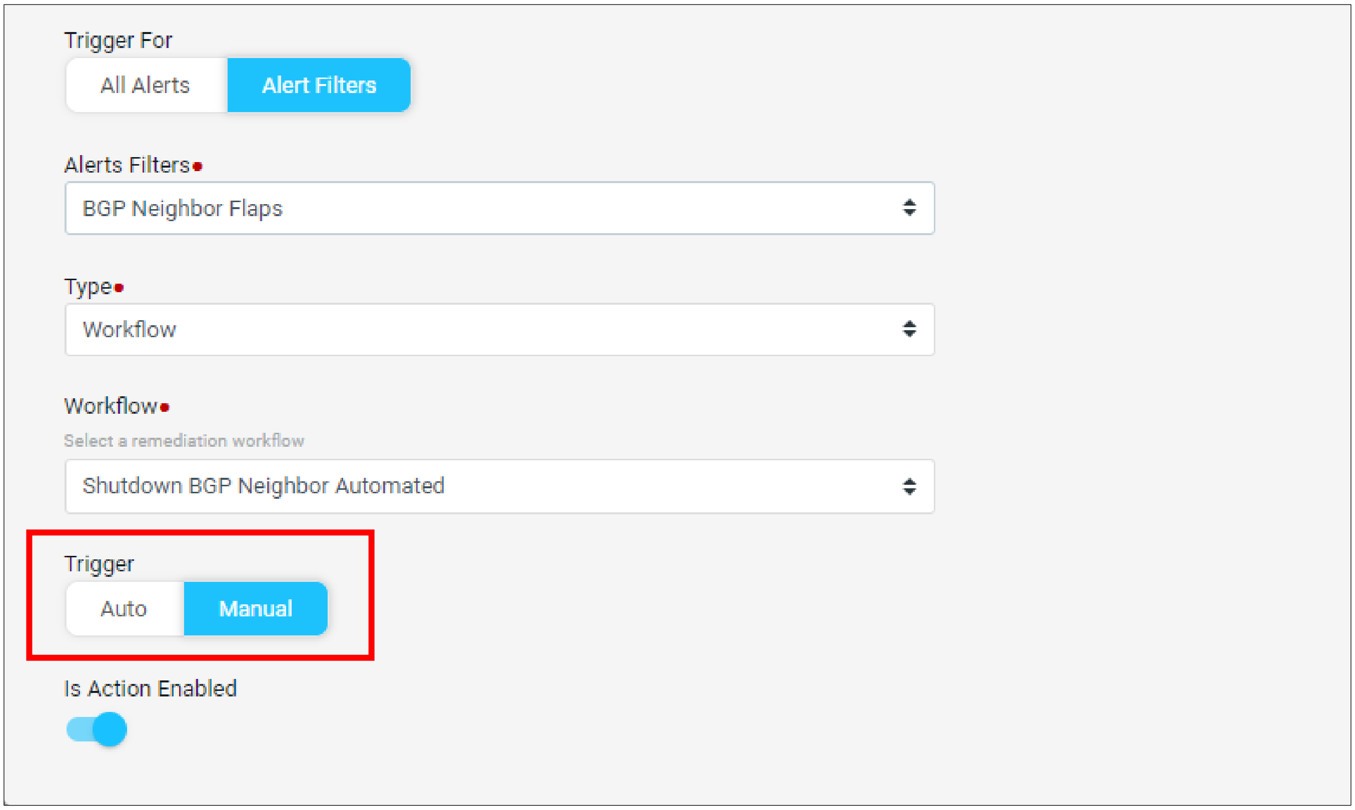
Subject●
Enter Rule Description
Alert {{definitionName}} Status {{status}} Severity {{severity}}

Alert Routing via Email

Workflows for troubleshooting & remediation

Closed-Loop Automation has gathered a lot of interest from service providers and enterprises, keeping in mind the automation of existing troubleshooting techniques and remediation flows. This move towards self-reliant and self-driving networks helps network teams eliminate the paraphernalia involved in network operations. ATOM allows NetOps to get rid of their exhaustive method-of-procedures (MOPs) and countless hours of validating issues. A diagnostic or remediation workflow set as the action collects all relevant command outputs, performs pre-checks, raises a service ticket, and applies a remediation step after approval.

The trigger can be fully automated, where ATOM directly takes a suggested action. It can also be manual, where the operator is expected to act as part of analyzing the alert.



Trigger For

All Alerts [✓ Alert Filters]

Alerts Filters•

BGP Neighbor Flaps

Type•

Workflow

Workflow•

Select a remediation workflow

Shutdown BGP Neighbor Automated

Trigger

Auto [✓ Manual]

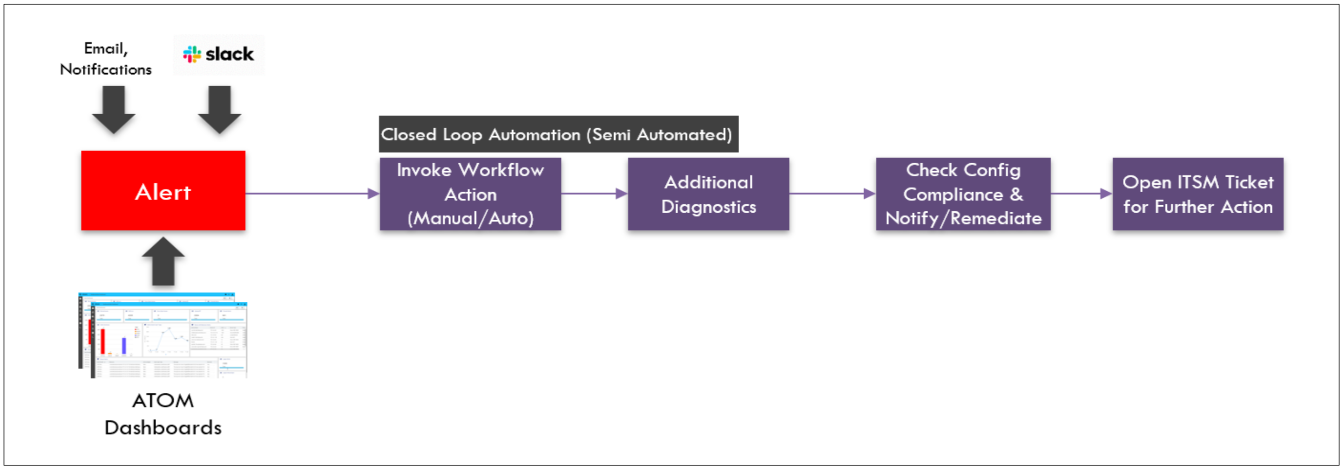
Is Action Enabled

Auto & Manual Trigger

Anuta ATOM offers troubleshooting capabilities to NOC teams. Based on the KPI breach against the alert definition in ATOM, an alert is generated. The alerts can be filtered and pinned to the ATOM alert dashboard that offers different widgets to view instantaneous and trend data in various formats. Based on the alert action, the NOC teams can be notified on Slack, Email, or ServiceNow with alert information. As a first step to the troubleshooting, the ATOM dashboard gives them a high-level view of the network.

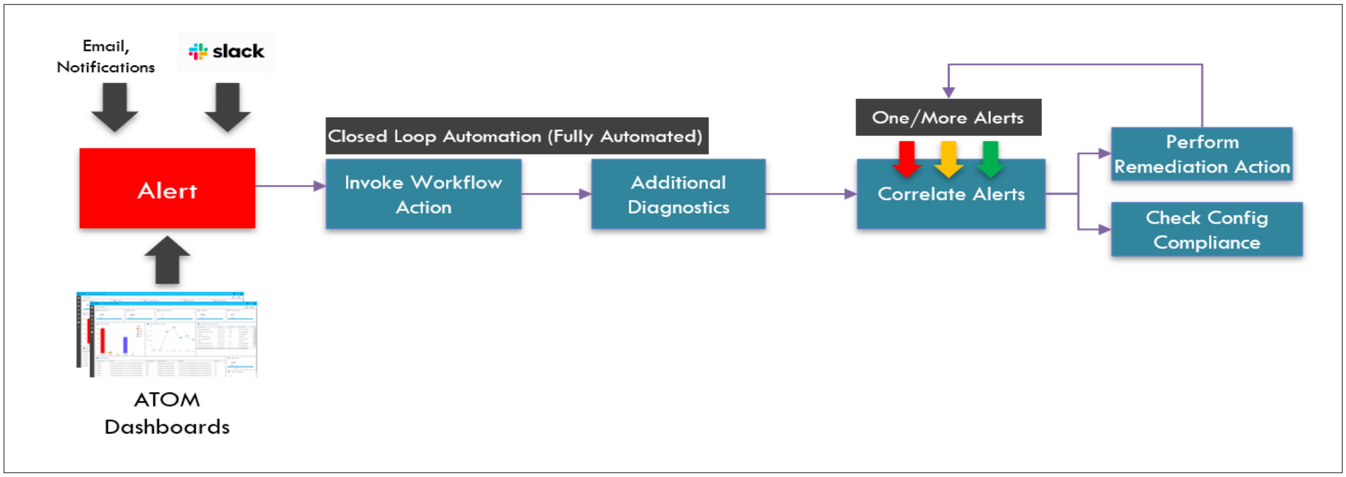
In contrast, a drill-down will showcase a detailed view of the alert, its source, resource affected, time of the alert, alert history, actions taken, and ticket information, if any. Some of the quick troubleshooting utilities include Ping and Traceroute to expedite the triage. For a detailed analysis, one of the below mentioned approaches can be followed.

1. In the semi-automated approach, a manual action triggered from ATOM's alert window triggers a diagnosis workflow. The workflow performs compliance audits to ensure configuration compliance, performs validations in the form of exec commands such as "show" commands to capture information relevant to the alert from all the affected devices, and submits a ServiceNow ticket with all the gathered output. The user does not have to log in to ATOM or the devices to troubleshoot the issue. All the information is presented in the Service ticket for the next set of manual remediation actions from the user.


Email,
Notifications
slack
Alert
ATOM
Dashboards
Closed Loop Automation (Semi Automated)
Invoke Workflow Action (Manual/Auto)
Additional Diagnostics
Check Config Compliance & Notify/Remediate
Open ITSM Ticket for Further Action

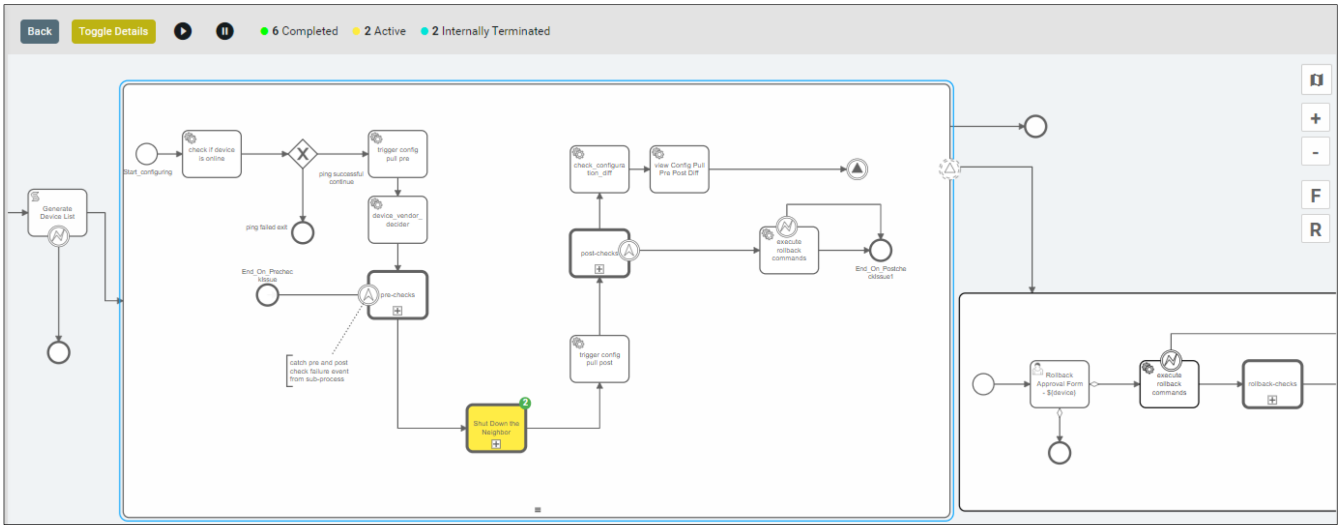
Semi-automated Troubleshooting

2. In the fully automated approach, the alert action automatically gets triggered after alert generation in the form of a remediation workflow. The workflow performs compliance checks, validates exec command output relevant to the alert, and, based on which the remediation commands are pushed to the network to resolve the alerts. Optionally, an approval request is to view the exec command output and remediation commands before application.

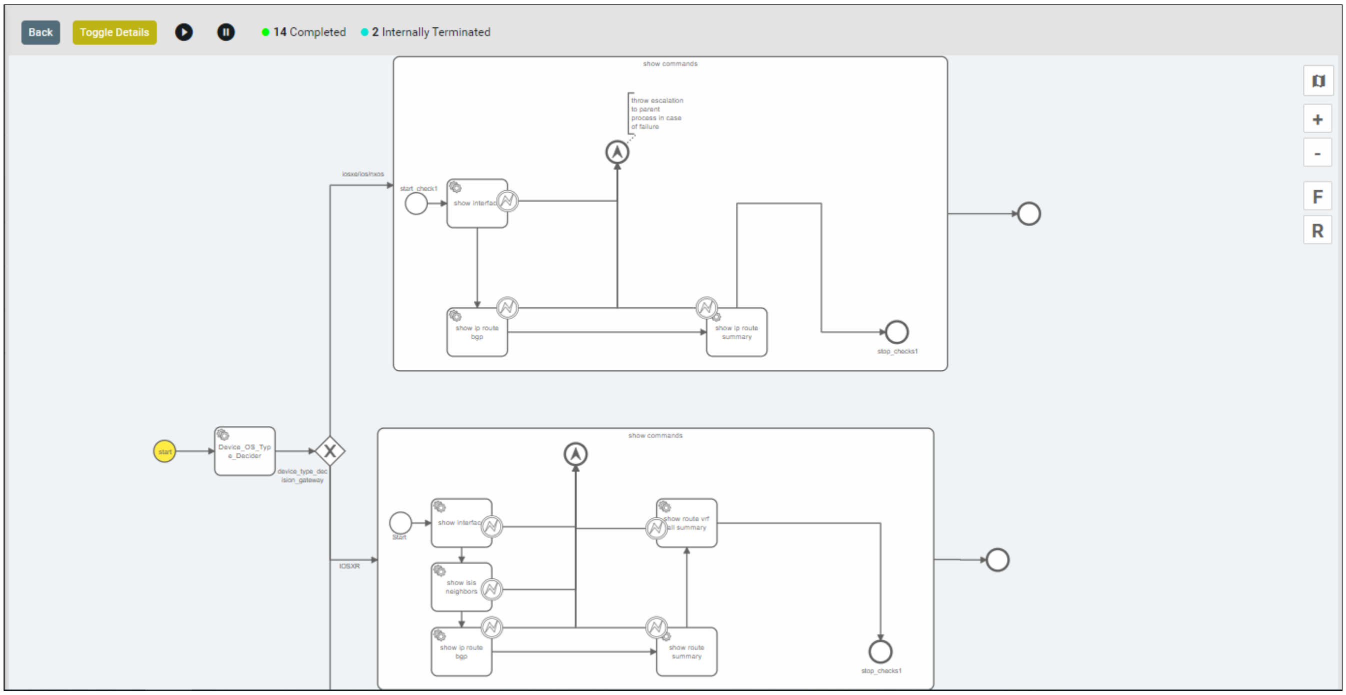


Full Automated Troubleshooting & Remediation

An example of a remediation workflow shown below handles BGP neighbor flaps. The workflow performs validations through ATOM's pre-check library, performs remediation action, completes post-checks, and pre-post validation to complete the remediation flow. If the post-check validation fails, a rollback of commands is triggered immediately. However, if the issue is fixed, on-demand rollback is made available to the operator through approval to de-provision the commands.

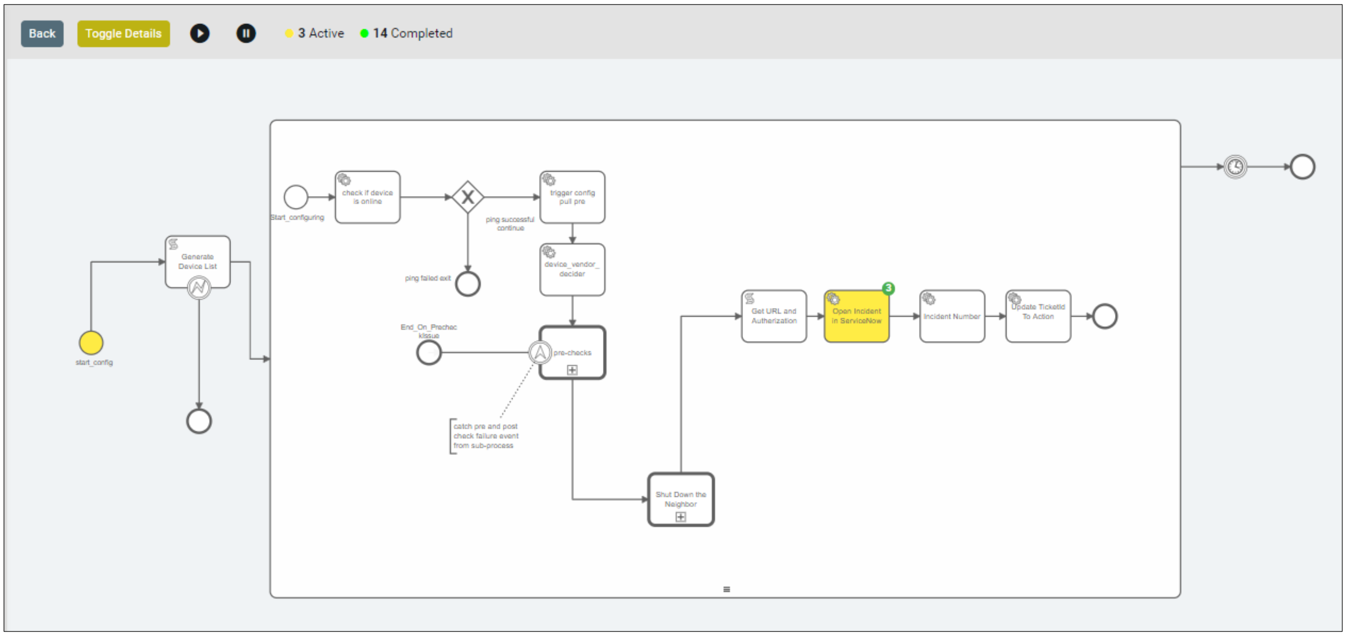


Fully Automated Troubleshooting & Remediation



Pre & Post Validations as Sub-process

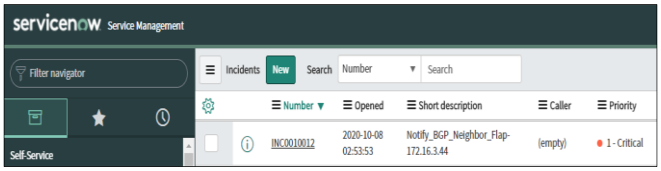
An example of a diagnostic workflow below works similarly to the remediation flow, barring the remediation part. The workflow creates an incident ticket on ServiceNow with all the command outputs and suggested remediation commands for the admin's action.



Semi-automated Troubleshooting with Incident Reporting

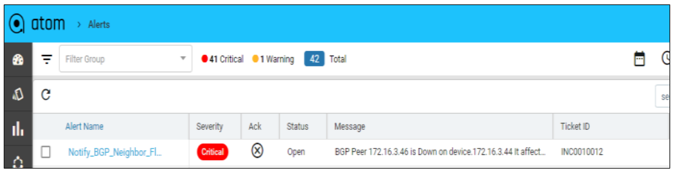
ATOM Integration with ServiceNow

ATOM offers out-of-box integration to ServiceNow ticketing. ATOM supports various types of tickets ServiceNow can handle, such as Incident Management and Change Management relevant to network teams. ATOM can raise service tickets, change requests, or approval requests as part of a workflow. In the context of alerting and closed-loop automation, a diagnostic or remediation workflow that validates an issue can include a task that triggers the requests to ServiceNow and waits for a response to take the workflow forward. The incident tickets are updated against the relevant alerts in the global alerts window.



Number	Opened	Short description	Caller	Priority
INC0010012	2020-10-08 02:53:53	Notify_BGP_Neighbor_Flap-172.16.3.44	(empty)	● 1 - Critical

Incident Ticket raised from ATOM on ServiceNow

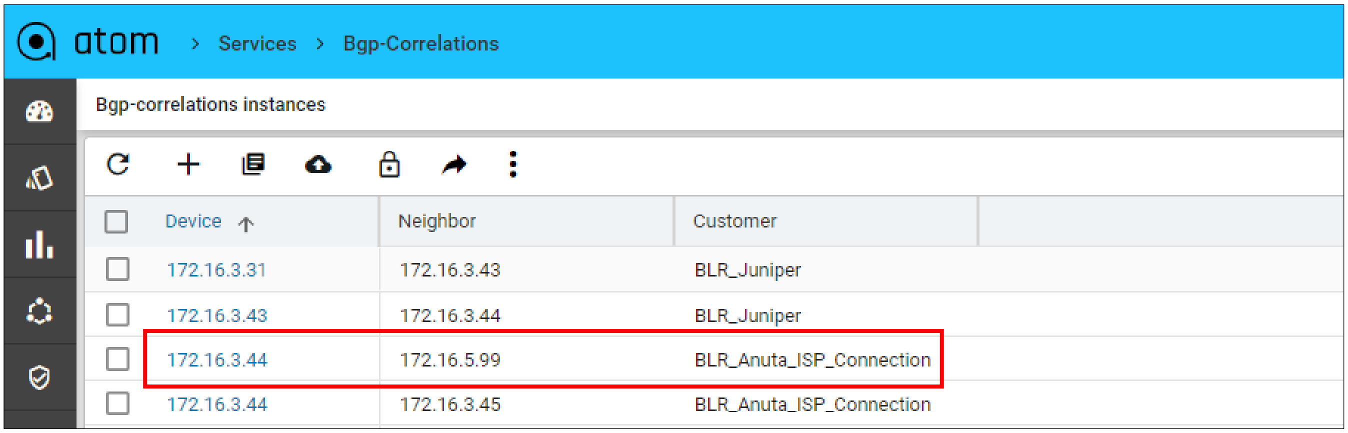


Alert Name	Severity	Ack	Status	Message	Ticket ID
Notify_BGP_Neighbor_Fl...	Critical	⊗	Open	BGP Peer 172.16.3.46 is Down on device.172.16.3.44 It affect...	INC0010012

Incident Ticket ID updated in ATOM

Alert Enrichment

An alert message should be actionable. While ATOM offers custom messaging in alert definitions, alert enrichment adds contextual information to alerts so that incidents can be intelligently correlated and understood. ATOM offers alert enrichment by feeding the raw alert from its monitoring and alerting system to a workflow. In this context, the workflow performs a lookup to ATOM's resource YANG model or an external DB where additional information for the alert is populated and extracts the relevant information. The extracted information undergoes a composition phase, where the existing alert message is enriched with the additional information.



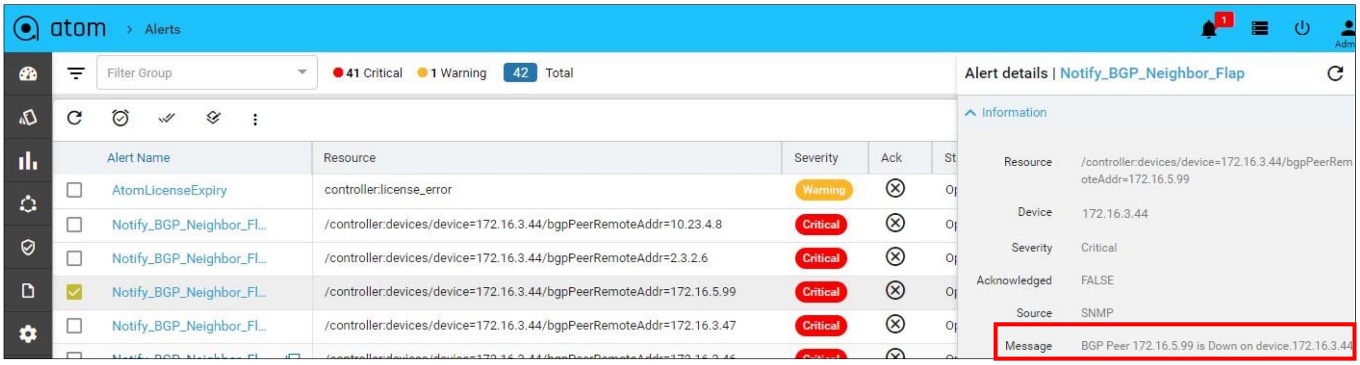
atom > Services > Bgp-Correlations

Bgp-correlations instances

☐	Device ↑	Neighbor	Customer
☐	172.16.3.31	172.16.3.43	BLR_Juniper
☐	172.16.3.43	172.16.3.44	BLR_Juniper
☐	172.16.3.44	172.16.5.99	BLR_Anuta_ISP_Connection
☐	172.16.3.44	172.16.3.45	BLR_Anuta_ISP_Connection

Resource Model in ATOM

As shown below, in a BGP neighbor flap scenario, the original message contains information on the affected device and its corresponding neighbor. It misses the vital information on the affected customers. ATOM's resource model is the data mapping table that contains additional information on customers. ATOM's alert enrichment workflow performs the lookup and enriches the alert to offer additional value. In the example below, the initial alert only suggests the affected device and neighbor, where as in the enriched alert after resource model lookup has the customer name appended to the primary alert.



atom > Alerts

Filter Group ● 41 Critical ● 1 Warning 42 Total

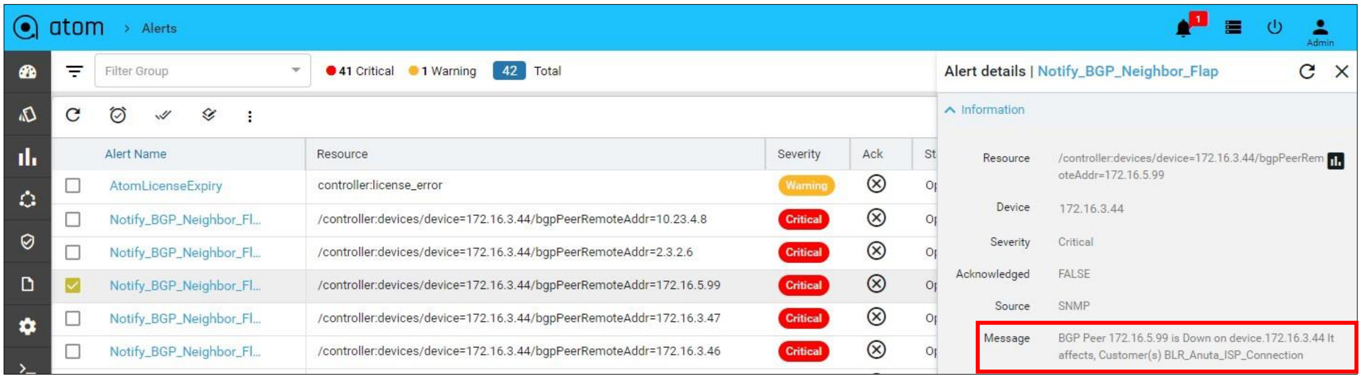
	Alert Name	Resource	Severity	Ack	St
☐	AtomLicenseExpiry	controller:license_error	Warning	⊗	Op
☐	Notify_BGP_Neighbor_Fl...	/controller:devices/device=172.16.3.44/bgpPeerRemoteAddr=10.23.4.8	Critical	⊗	Op
☐	Notify_BGP_Neighbor_Fl...	/controller:devices/device=172.16.3.44/bgpPeerRemoteAddr=2.3.2.6	Critical	⊗	Op
☑	Notify_BGP_Neighbor_Fl...	/controller:devices/device=172.16.3.44/bgpPeerRemoteAddr=172.16.5.99	Critical	⊗	Op
☐	Notify_BGP_Neighbor_Fl...	/controller:devices/device=172.16.3.44/bgpPeerRemoteAddr=172.16.3.47	Critical	⊗	Op

Alert details | Notify_BGP_Neighbor_Flap

Information

Resource	/controller:devices/device=172.16.3.44/bgpPeerRemoteAddr=172.16.5.99
Device	172.16.3.44
Severity	Critical
Acknowledged	FALSE
Source	SNMP
Message	BGP Peer 172.16.5.99 is Down on device.172.16.3.44

Alert before Enrichment



atom > Alerts

Filter Group ● 41 Critical ● 1 Warning 42 Total

	Alert Name	Resource	Severity	Ack	St
☐	AtomLicenseExpiry	controller:license_error	Warning	⊗	Op
☐	Notify_BGP_Neighbor_Fl...	/controller:devices/device=172.16.3.44/bgpPeerRemoteAddr=10.23.4.8	Critical	⊗	Op
☐	Notify_BGP_Neighbor_Fl...	/controller:devices/device=172.16.3.44/bgpPeerRemoteAddr=2.3.2.6	Critical	⊗	Op
☑	Notify_BGP_Neighbor_Fl...	/controller:devices/device=172.16.3.44/bgpPeerRemoteAddr=172.16.5.99	Critical	⊗	Op
☐	Notify_BGP_Neighbor_Fl...	/controller:devices/device=172.16.3.44/bgpPeerRemoteAddr=172.16.3.47	Critical	⊗	Op
☐	Notify_BGP_Neighbor_Fl...	/controller:devices/device=172.16.3.44/bgpPeerRemoteAddr=172.16.3.46	Critical	⊗	Op

Alert details | Notify_BGP_Neighbor_Flap

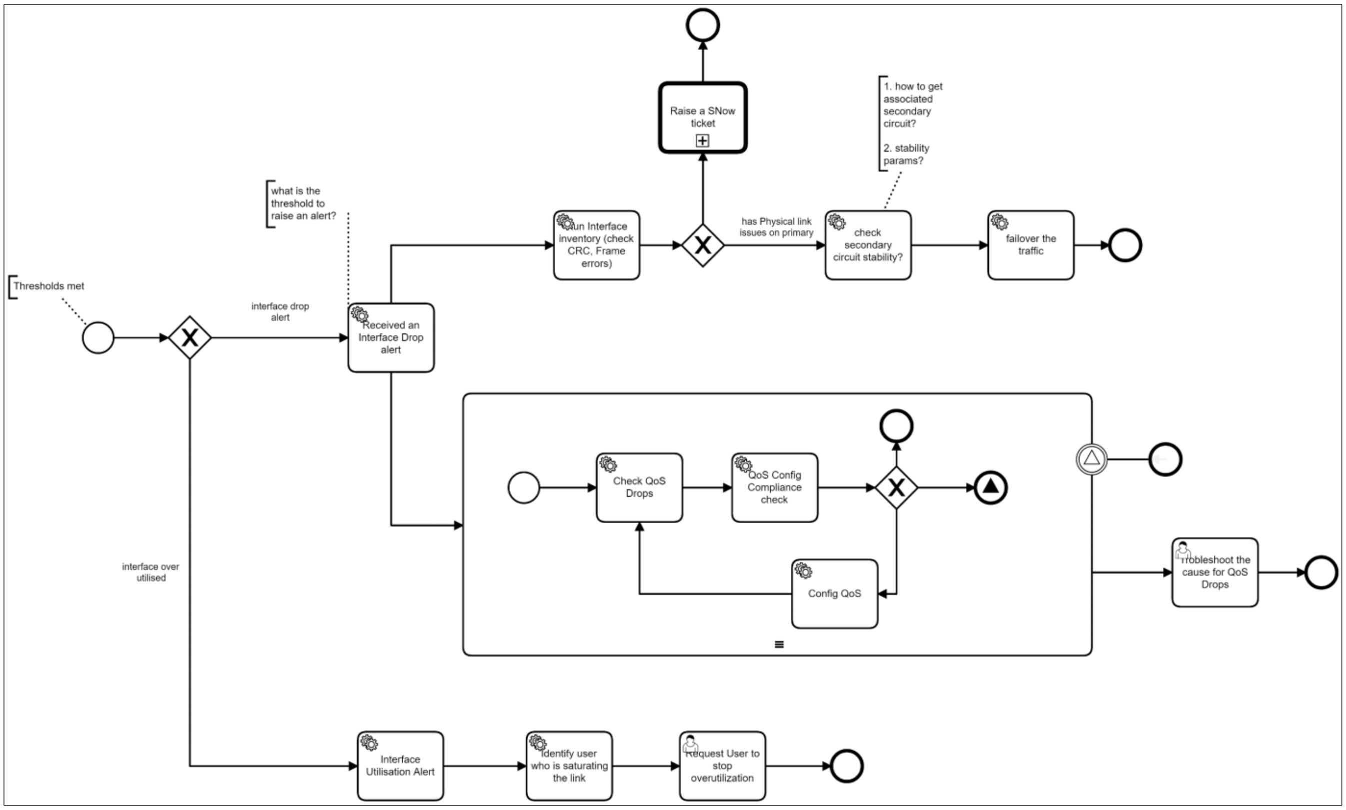
Information

Resource	/controller:devices/device=172.16.3.44/bgpPeerRemoteAddr=172.16.5.99
Device	172.16.3.44
Severity	Critical
Acknowledged	FALSE
Source	SNMP
Message	BGP Peer 172.16.5.99 is Down on device.172.16.3.44 It affects, Customer(s) BLR_Anuta_ISP_Connection

Alert after Enrichment

Alert Correlation

A particular fault could be a result of one or more related failures in the network. It also means there could be multiple alerts pointing to the same problem. Multiple secondary alerts can be correlated, checked for anomalies, and perform individual remediation to address the primary alert. An example below shows how an alert on interface packet drops is correlated to three different network events with each section of the workflow pointing to a remediation/notification action.


Raise a SNow ticket
1. how to get associated secondary circuit?
2. stability params?
what is the threshold to raise an alert?
Run Interface inventory (check CRC, Frame errors)
has Physical link issues on primary
check secondary circuit stability?
failover the traffic
Thresholds met
interface drop alert
Received an Interface Drop alert
Check QoS Drops
QoS Config Compliance check
Config QoS
Trobleshoot the cause for QoS Drops
interface over utilised
Interface Utilisation Alert
Identify user who is saturating the link
Request User to stop overutilization

Alert Correlation

Closed-Loop Automation at Scale

Anuta ATOM has a microservices-based horizontally scalable platform. It supports remote collection capabilities to address latency issues and has been scale tested to meet large Service providers and enterprises' requirements. ATOM’s scalable time-series DB supports the handling of millions of metrics through SNMP and Streaming telemetry with millisecond latency and forms the foundation of ATOM’s alerting framework. Thousands of simultaneous remediation and diagnostic workflows can be executed with ease to ensure a healthy network. ATOM also supports integration into its Apache Kafka message bus to support additional use cases.

With the advent of 5G and IoT, networks are set to rise to another inflection point. However, with scale comes a deluge of notifications and anomalies in any given network that must be managed. The ATOM platform can automate everyday use cases such as congestion management, DDoS mitigation services, and other service assurance use cases while enhancing QoE with ATOM's comprehensive closed-loop automation capabilities.

Additional Resources

Video-on-demand on ATOM Alerting & Closed-Loop Automation

To learn how Anuta Network's ATOM Alerting & Closed-Loop Automation contact us at https://www.anutanetworks.com