knowledge17

http://clabs.link/lab131978

WORK at LIGHTSPEED

Advanced Event Management Features: Correlation, Binding, and Impact

Benny Makovsky
Sr. Product Manager
ServiceNow

Joe Steinfeld
Advisory Solution Consultant
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

Agenda

- Event Management Overview & New Features in Jakarta
- Event Ingestion
- LAB #1 – Event rule Designer
- Alert Correlation
- LAB #2 – Rule-Based & CMDB-Based Correlation Rules
- Triage Service Outage
- LAB #3 – End to End Simulation

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



Name: Benny Makovsky

Title: Senior Product Manager

Function: ITOM Development

Company: ServiceNow

Experience: 2 years in ServiceNow as Product Manager @ ITOM, 16 years in chief architect @ CA

Expertise: DevOps, Design, architecture, Innovation, Sys engineer, Analytics…

Achievements: You're about to see some of it…+ 2 amazing kids

Current Projects: Service Mapping and Operational Intelligent vNext

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



Name: Joe Steinfeld

Title: Advisory Solution Consultant

Function: Solution Consulting – ITOM Specialty

Company: ServiceNow

Experience: 3 years at ServiceNow, 19 years consulting in ITOM & ITSM

Expertise: IT Operations, Cloud Management, Monitoring, Automation

Achievements: Helping customers drive operational efficiencies (e.g., reduce CMDB population/maintenance by 75%). Two amazing 11-year-old twins.

Current Projects: Helping customers create service-aware CMDBs & increase efficiencies via Automation.

© 2017 ServiceNow All Rights Reserved

Objectives and What You Will Learn

Objectives

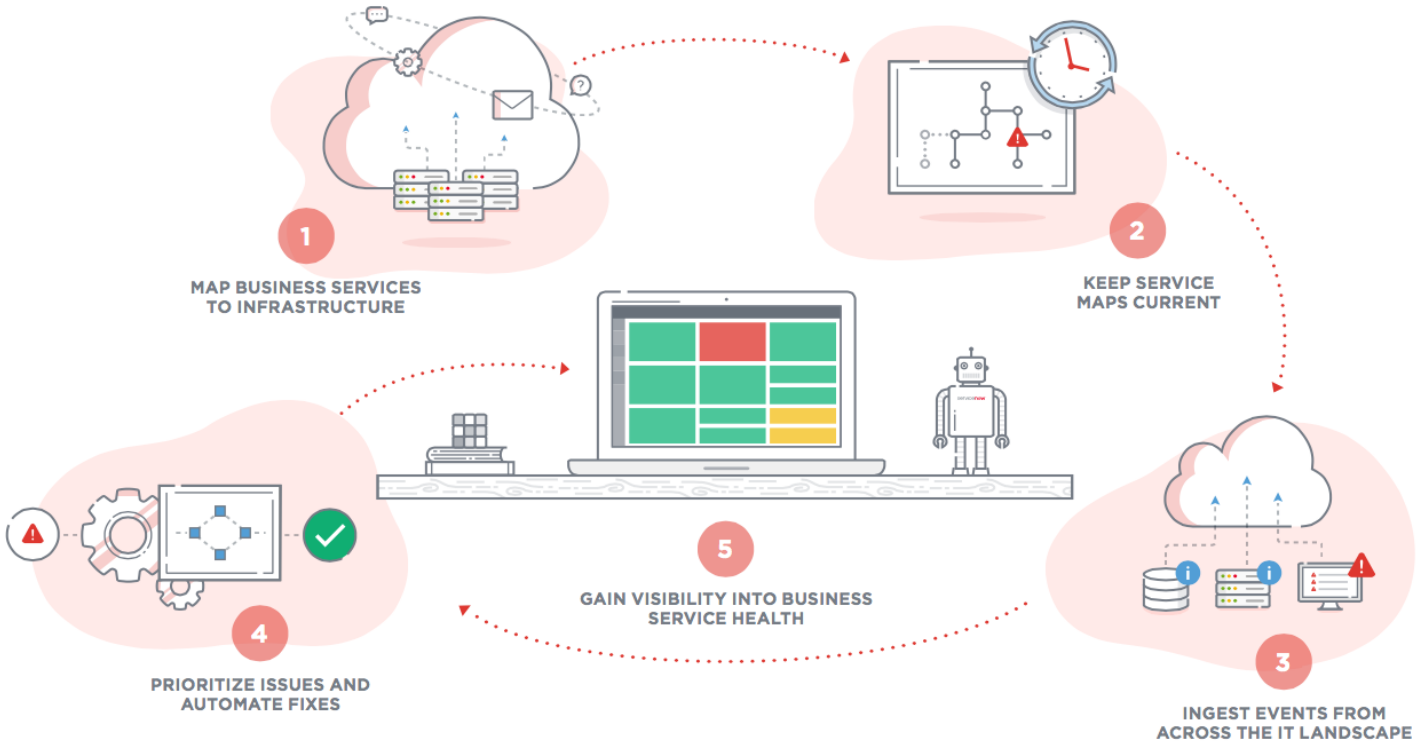
- Configure correlation rules and see how this affects Alert grouping. Configure maintenance logic to match the specific workflows and guidelines your organization uses for maintenance. Differentiate between Manual and Automatic Rules. Create event rules that allow alerts to bind to applicative CIs, and see how this affects a business service, and then configure impact rules to fine-tune the effect. Configure correlation rules and see how this affects Alert grouping. Configure maintenance logic to match the specific workflows and guidelines your organization uses for maintenance.

What you will learn

- Create event rules using new event rule designer
- Learn about alert group types
- Learn about alert correlation rules
- Discuss event management helps eliminate service outage.

© 2017 ServiceNow All Rights Reserved

Eliminate Service Outage



How to Eliminate Service Outages

1. **Map Business Services to Infrastructure**
   Discover and map relationships between business services and the IT components required to support them.

2. **Keep Service Maps Current**
   Continuously monitor IT infrastructure for changes and update service maps in real time.

3. **Ingest Events from Across the IT Landscape**
   Gain a consolidated view of service-impacting events for a rapid and effective IT response.

4. **Prioritize Issues and Automate Fixes**
   Automate IT and business processes to accelerate remediation, reduce manual tasks, and improve productivity.

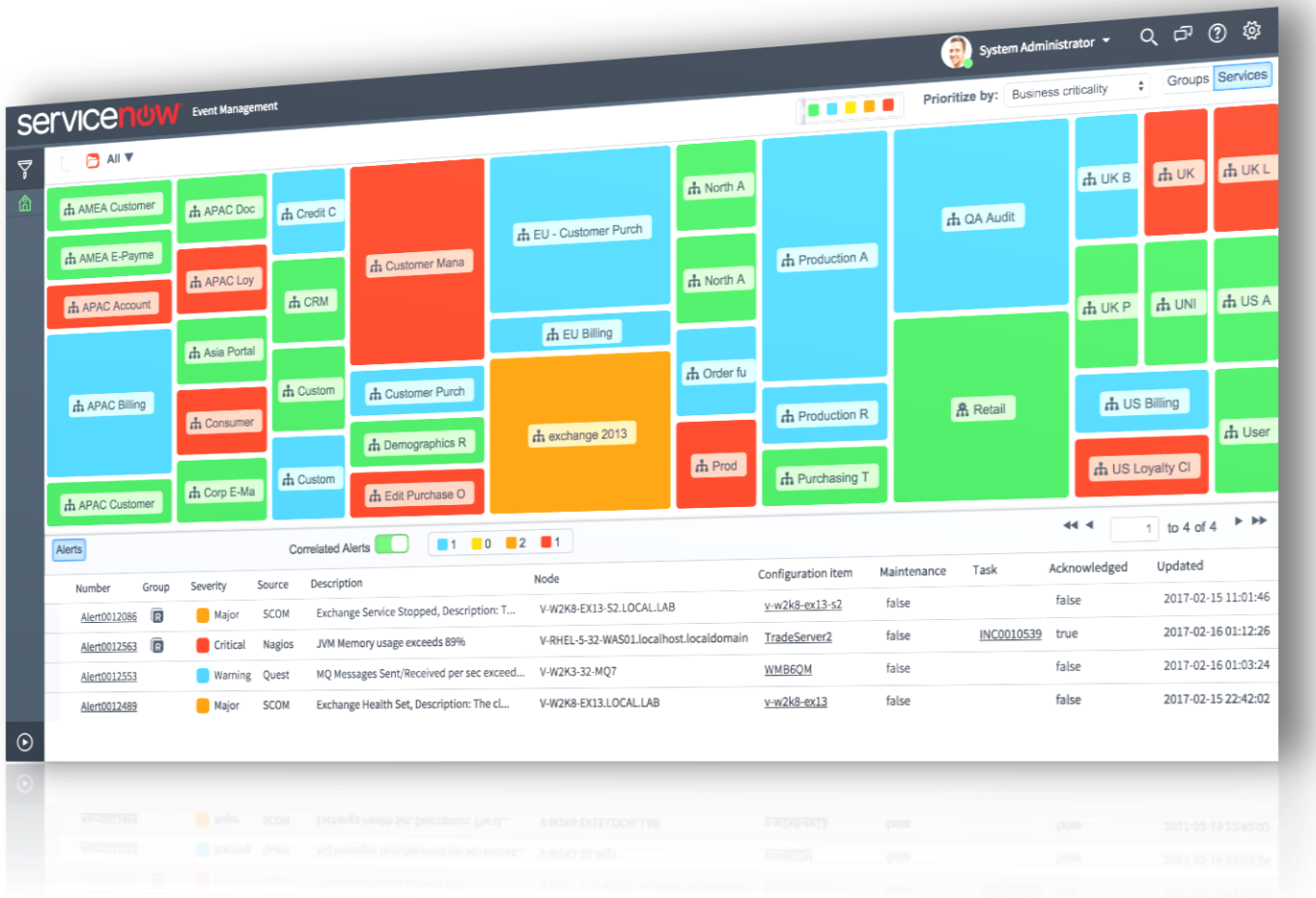
5. **Gain Visibility into Business Service Health**
   Prioritize the resolution of issues to ensure business service availability.

© 2017 ServiceNow All Rights Reserved

ServiceNow Operational Intelligence (Event Management)

Improve Availability by combining event management and service maps to maximize service health

- Consolidate events from different sources
- Filter incoming events to reduce noise and generate qualified alerts
- Map events to CMDB CIs
- Suppress alerts due to planned maintenance
- Service impact analysis
- Service availability dashboard for understanding service health
- Spawn any ServiceNow task from an alert
- Alert remediation: automated or manual
- Troubleshooting capabilities utilizing events and performance data



© 2017 ServiceNow All Rights Reserved

Jakarta Marquee Features

- Event Rule
  - **New** Event Rules designer
- Event Ingestion
  - **New** event listener at the MID level (alongside to the instance)
  - **New** event “free format” listener at the MID level and the instance
  - **New** content - OOTB ,Store and vendors (23 connectors in total) : Azure , Nagios, HP OMi, BMC TrueSight, Oracle EM, AppDynamics, New Relic, CA UIM, CA APM, Dynatrace, CA Specrtum, Datadog, Panopta
- NOC View
  - **Updated** alert console – platform compliant and reusable
  - **New** composite business service list view
- Metric
  - **New** Service Metrics – Operational Metrics in context of business service
  - **New** Anomaly alerts promotion – Use analytics for dynamic threshold
  - Performance improvements – **Updated** SCOM metric collection
  - **New** Time Series DB (clotho) – better scale and performance
- Service Analytics
  - **New** predictive alerts

© 2017 ServiceNow All Rights Reserved

Event Ingestion

© 2017 ServiceNow All Rights Reserved

Connect to Multiple Monitoring Tools

Collect, filter, and normalize events from multiple monitoring tools to rapidly understand impact to service

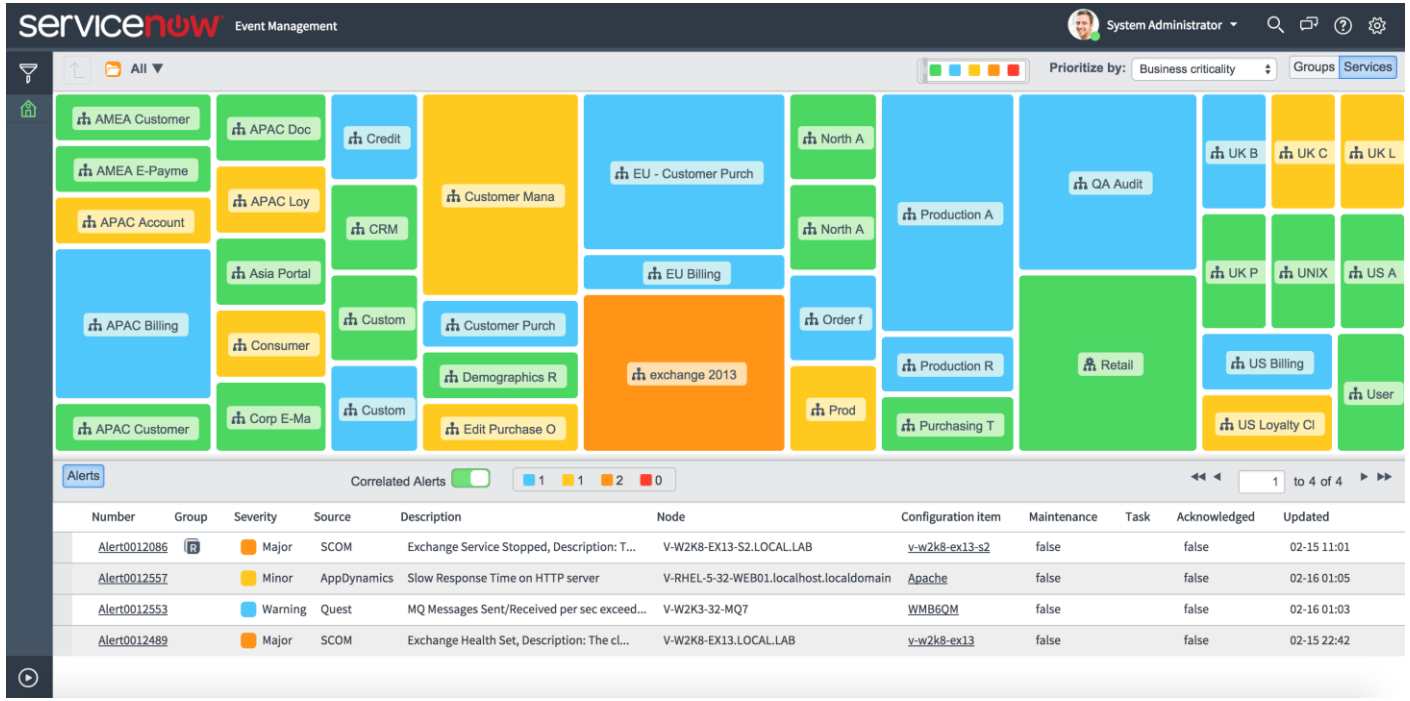
Microsoft System Center Operations Manager
solarwinds
amazon web services CloudWatch
Nagios *
bmc *
ORACLE *
splunk>
Hewlett Packard Enterprise
IBM Tivoli software Netcool
vmware
ZABBIX
Microsoft Azure *
Panopta *

OOB

REST API
SNMP

zenoss
sumologic
APPDYNAMICS
ThousandEyes
keynote
DATADOG
ca technologies *
New Relic. *

ServiceNow Store and 3rd party



© 2017 ServiceNow All Rights Reserved

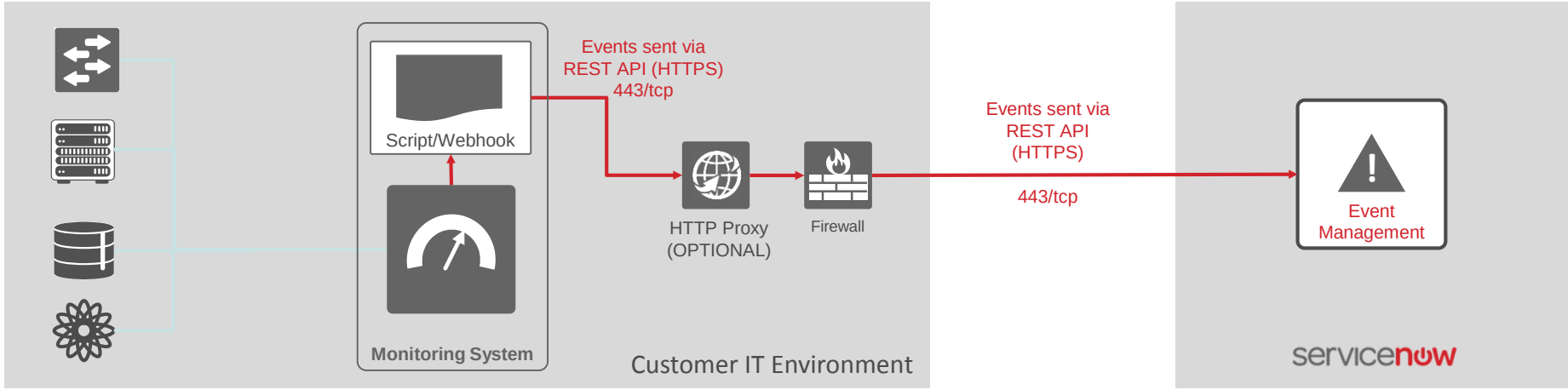
New Push and Transform API

- **Description of Feature:** Client can send bulk of events directly to the MID and the instance API in a “free format”.
- **Differentiation Assessment:** Simplified integrations both in cases where the payload is dictated by the event source (Cloud, etc.), and cases where security considerations mandate that event sources communicate only with endpoints within the corporate network.

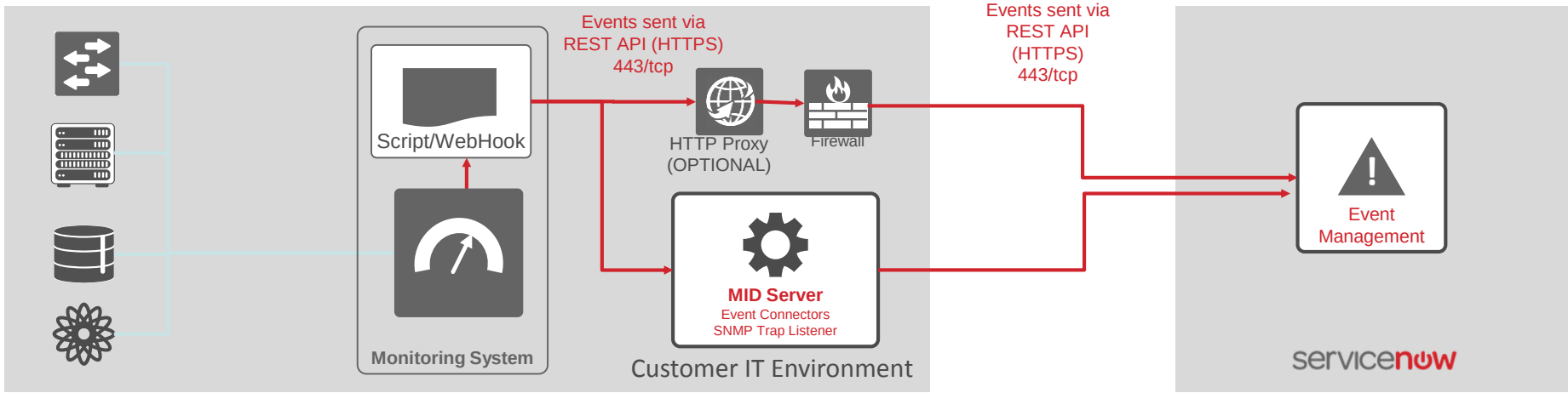
© 2017 ServiceNow All Rights Reserved

Integrating Events using the REST API

Istanbul



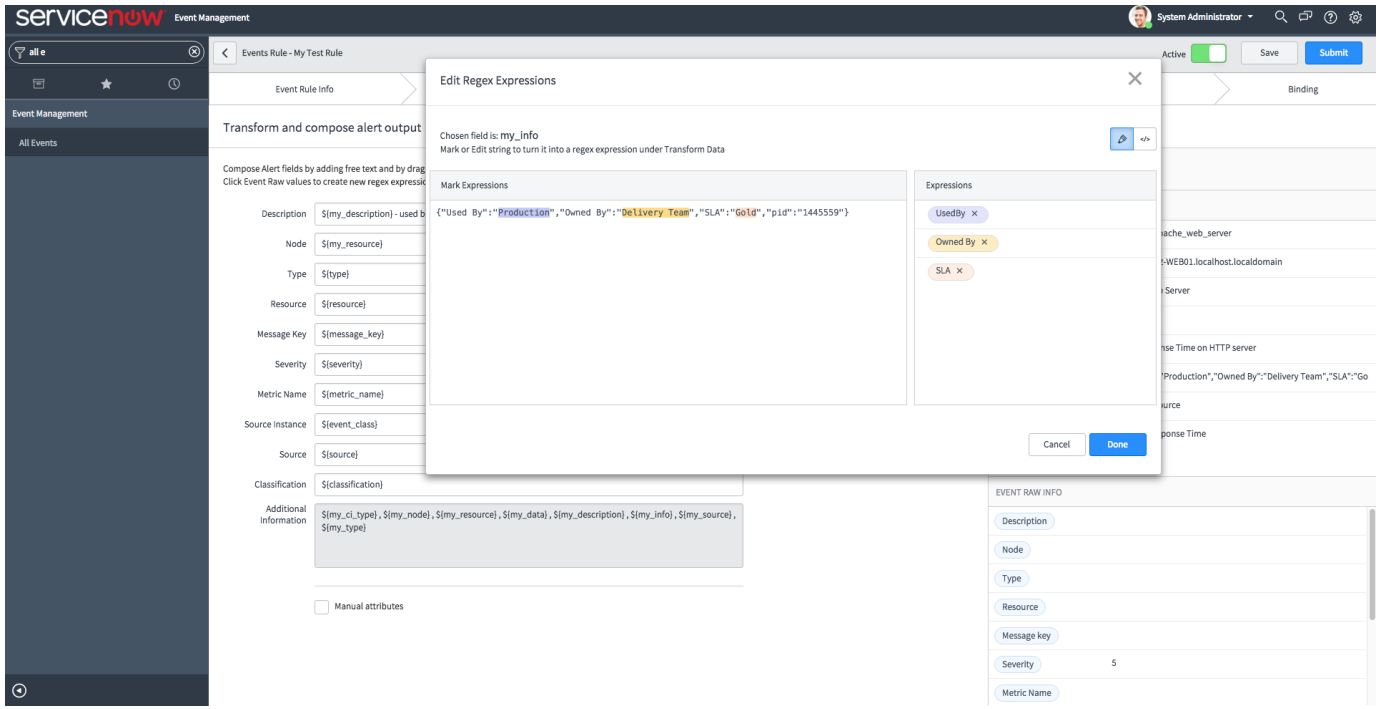
NEW in Jakarta



© 2017 ServiceNow All Rights Reserved

Event Rules Designer

- **Description of Feature:** EM admins can create event rules using an intuitive and process-driven approach.
- **Differentiation Assessment:** Codeless, step by step approach which reduces complexity and provides a simple method for transforming events into alerts in a few basic steps.



© 2017 ServiceNow All Rights Reserved

Send Custom Event

Send Custom Event

POST | http://10.196.33.50:7676/api/mid/em/inbound_event | Params | Send | Save

Authorization ● | Headers (3) | Body ● | Pre-request Script | Tests | Code

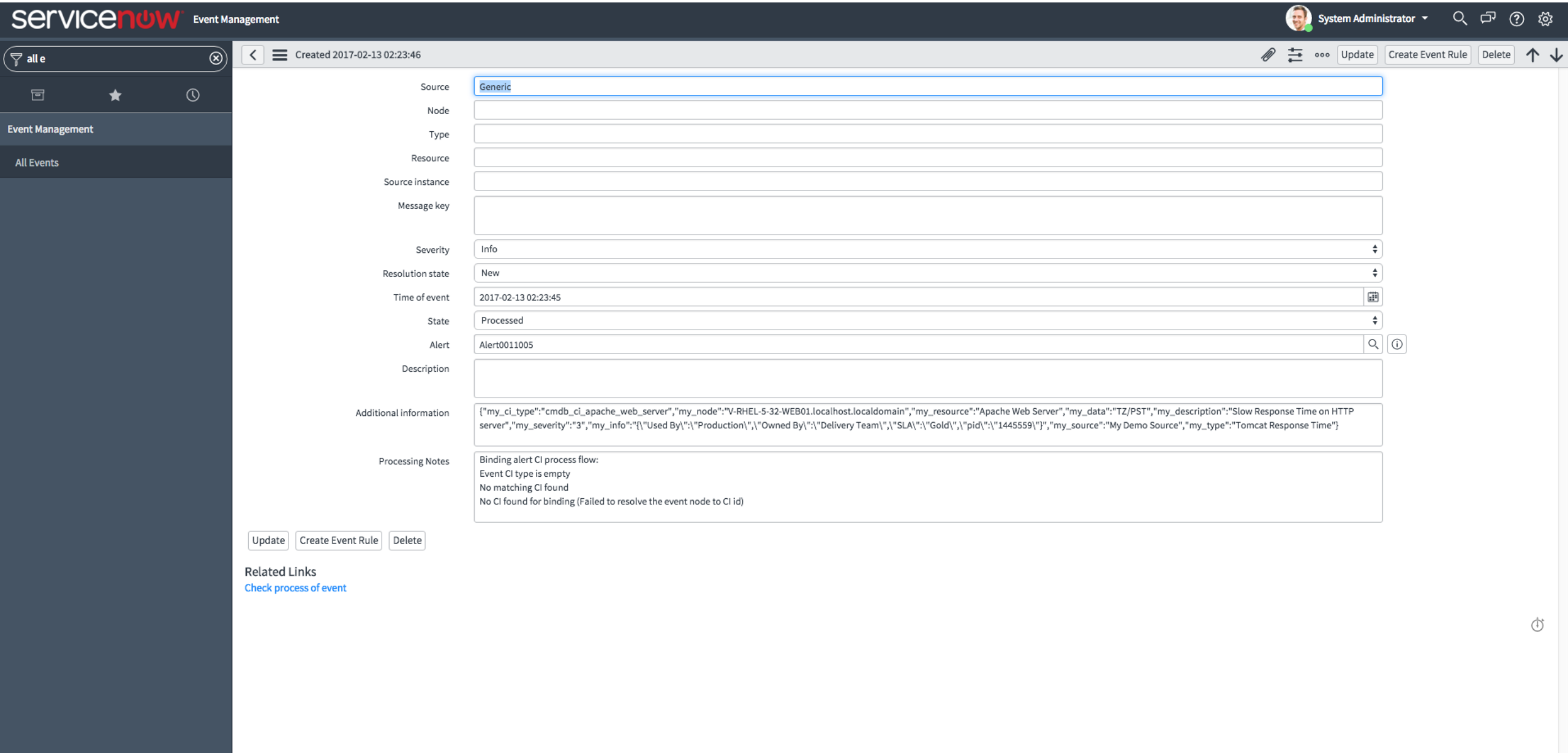
form-data | x-www-form-urlencoded | raw | binary | JSON (application/json)

```
{
    "my_source" : "My Demo Source",
    "my_node" : "V-RHEL-5-32-WEB01.localhost.localdomain" ,
    "my_type" : "Tomcat Response Time",
    "my_resource" : "Apache Web Server",
    "my_severity" : "3",
    "my_description" : "Slow Response Time on HTTP server",
    "my_ci_type" : "cmdb_ci_apache_web_server",
    "my_info" : "{Used By:Production,Owned By:Delivery Team,SLA:Gold,pid:1445559}",
    "my_data" : "TZ/PST"

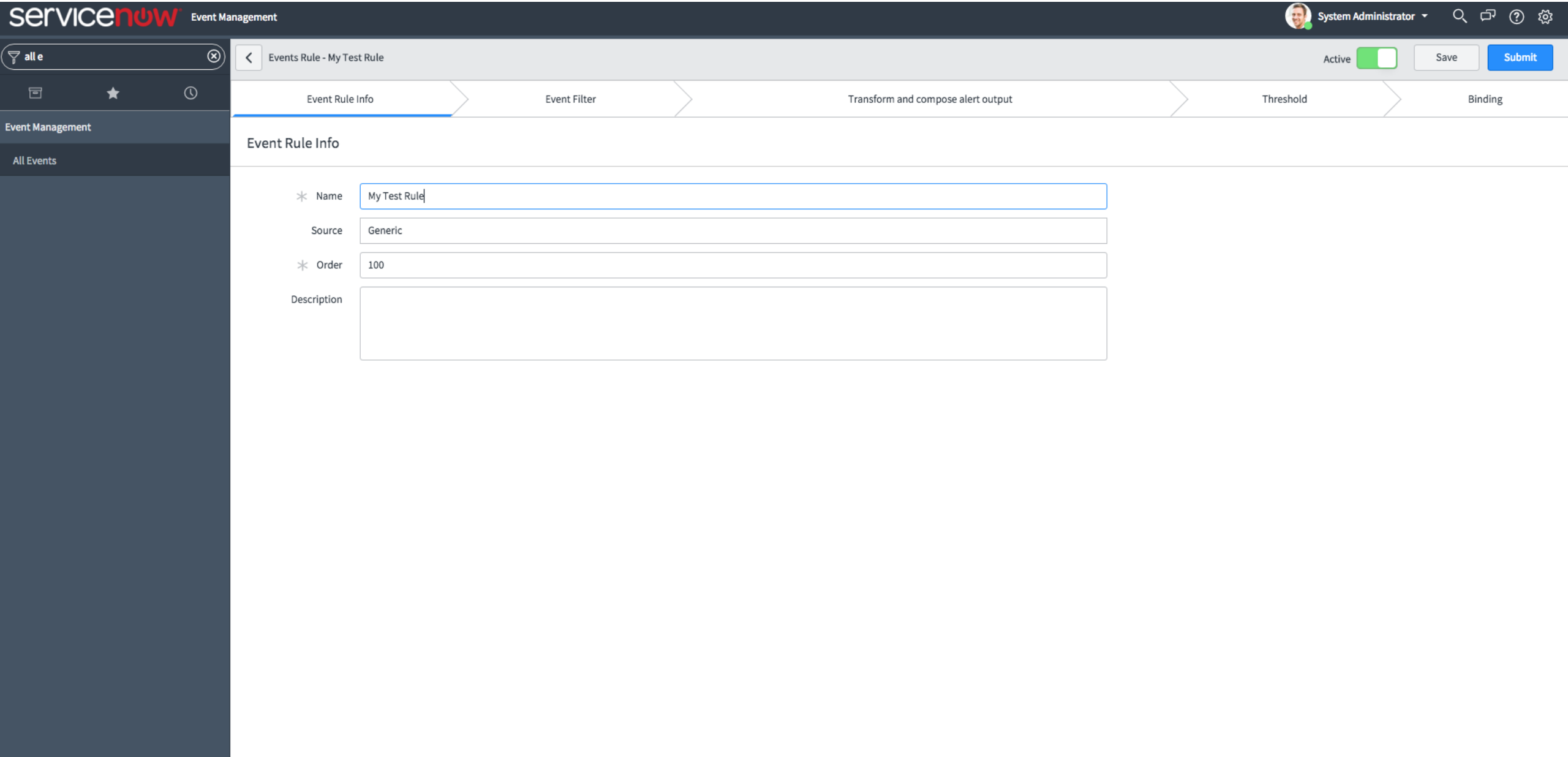
}
```


© 2017 ServiceNow All Rights Reserved

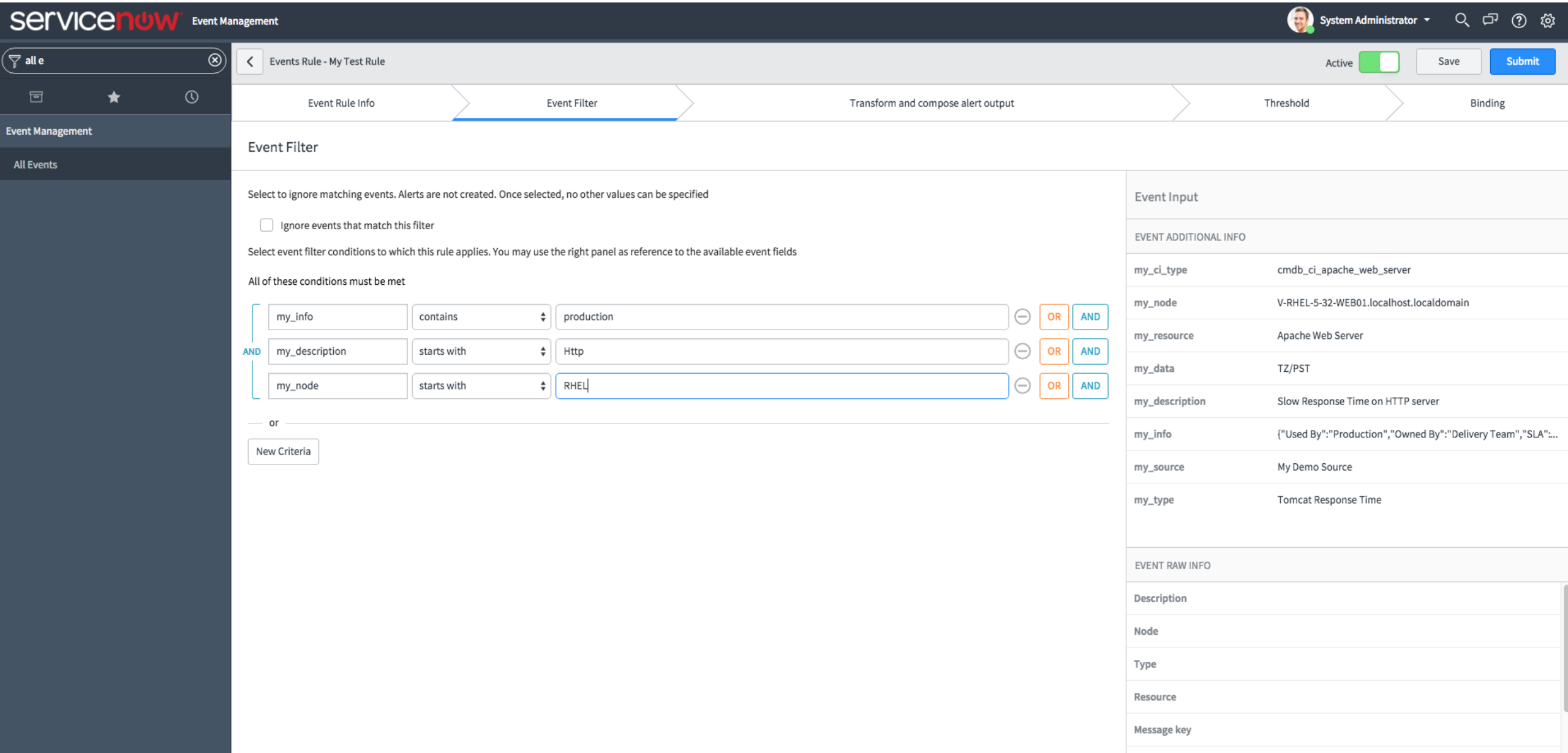
Custom Event Can Be Easily Captured and Transformed



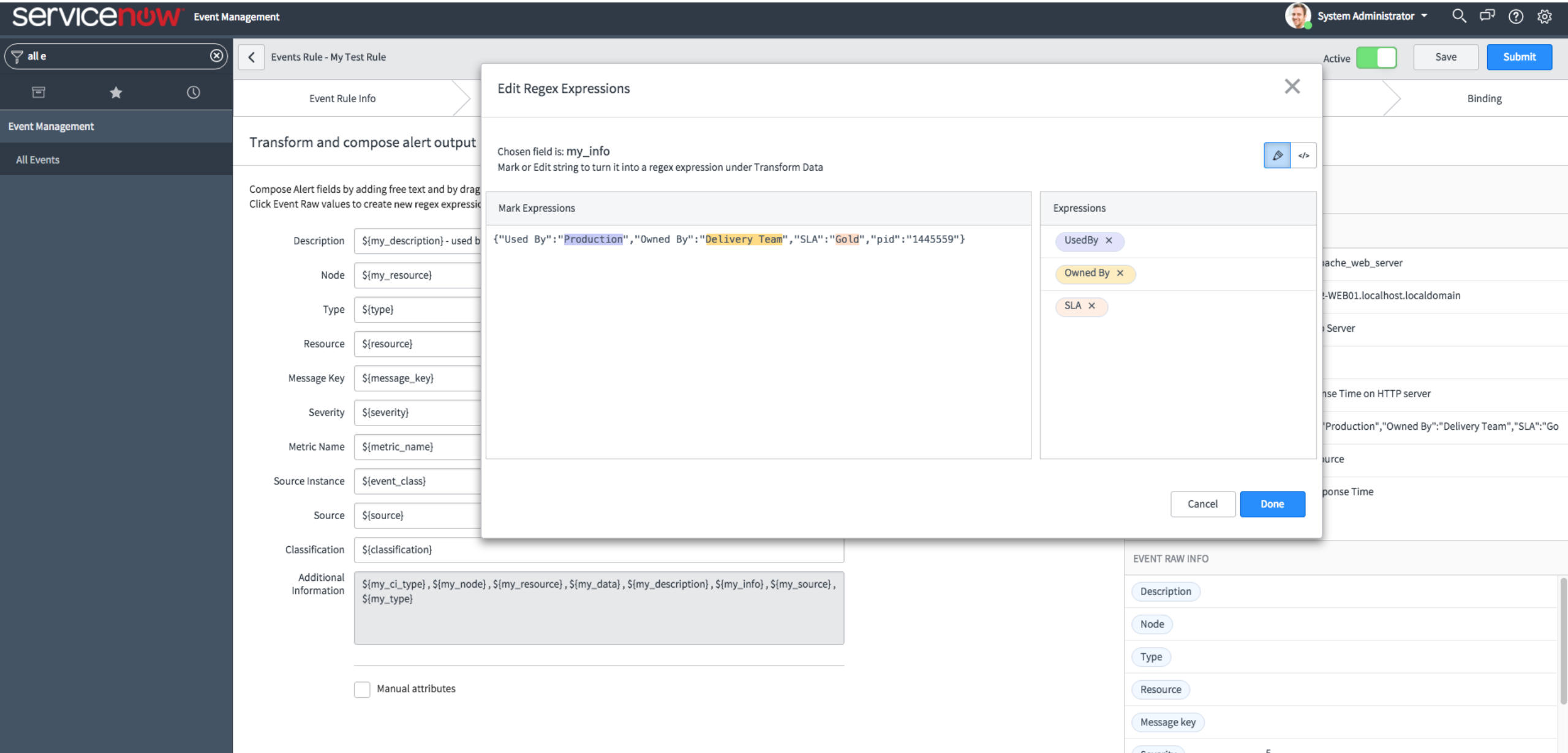
Use the Event Rule Designer to Compose New Alert



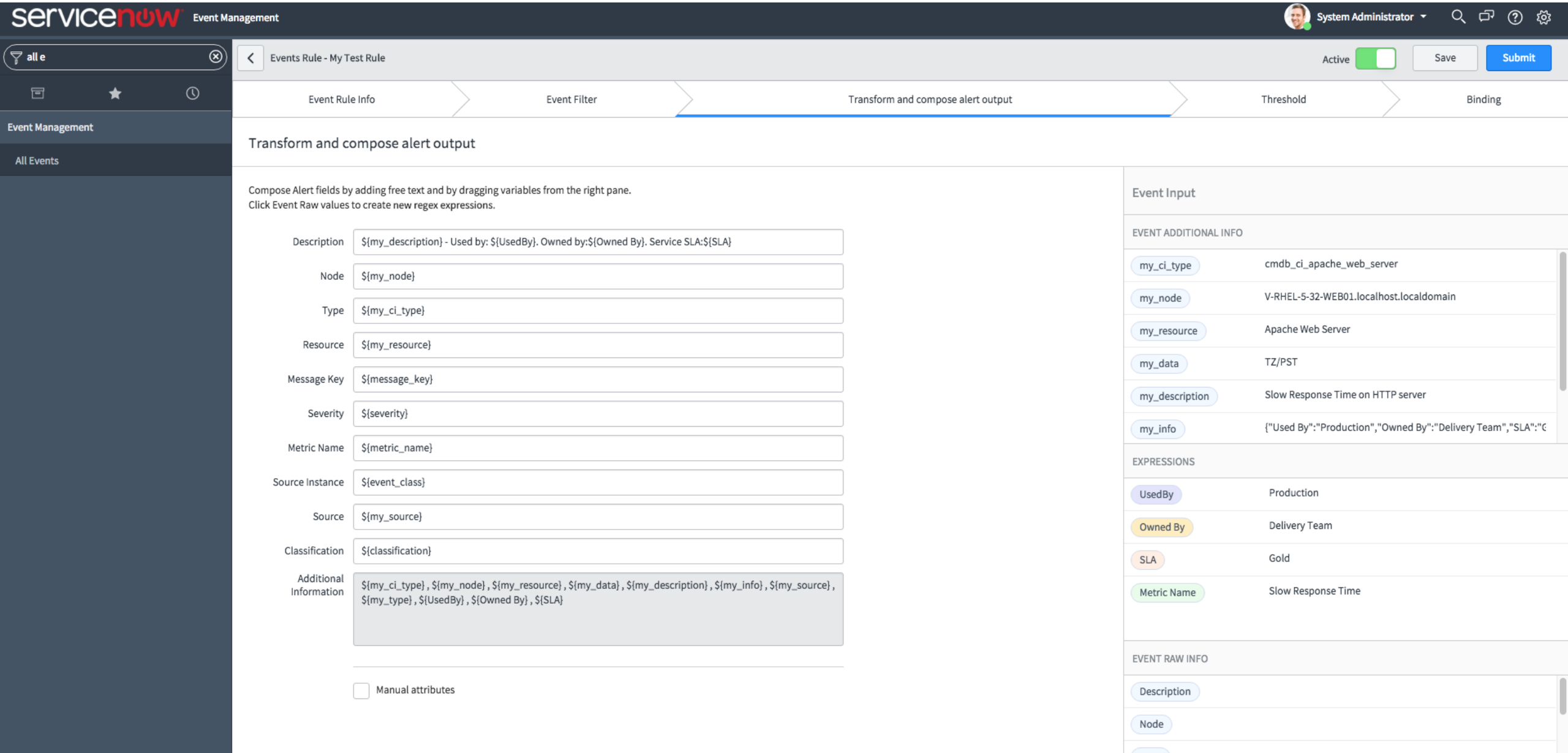
Use the Event Rule Designer to Compose New Alert - Filter



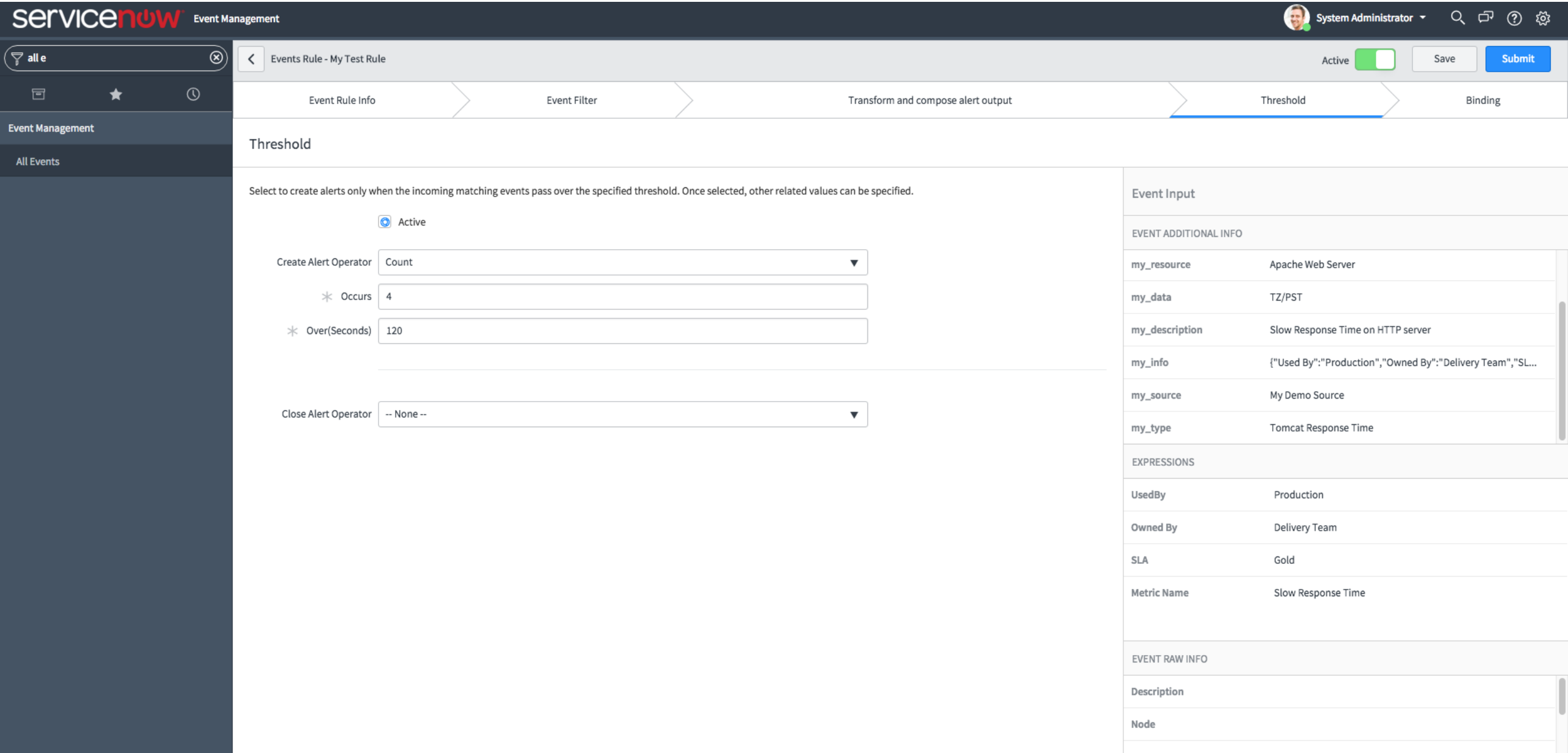
Use the Event Rule Designer to Compose New Alert - Transform



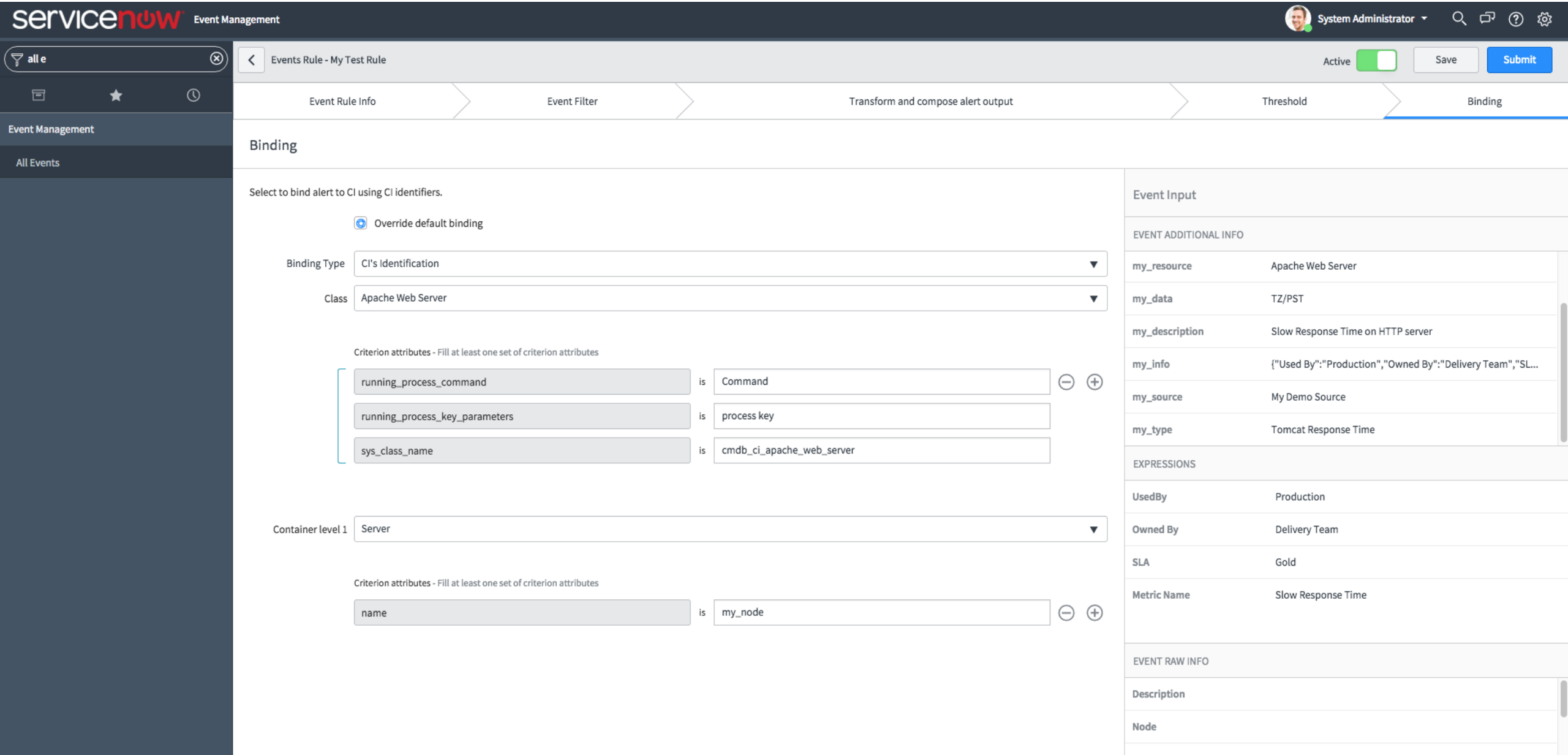
Use the Event Rule Designer to Compose New Alert - Transform



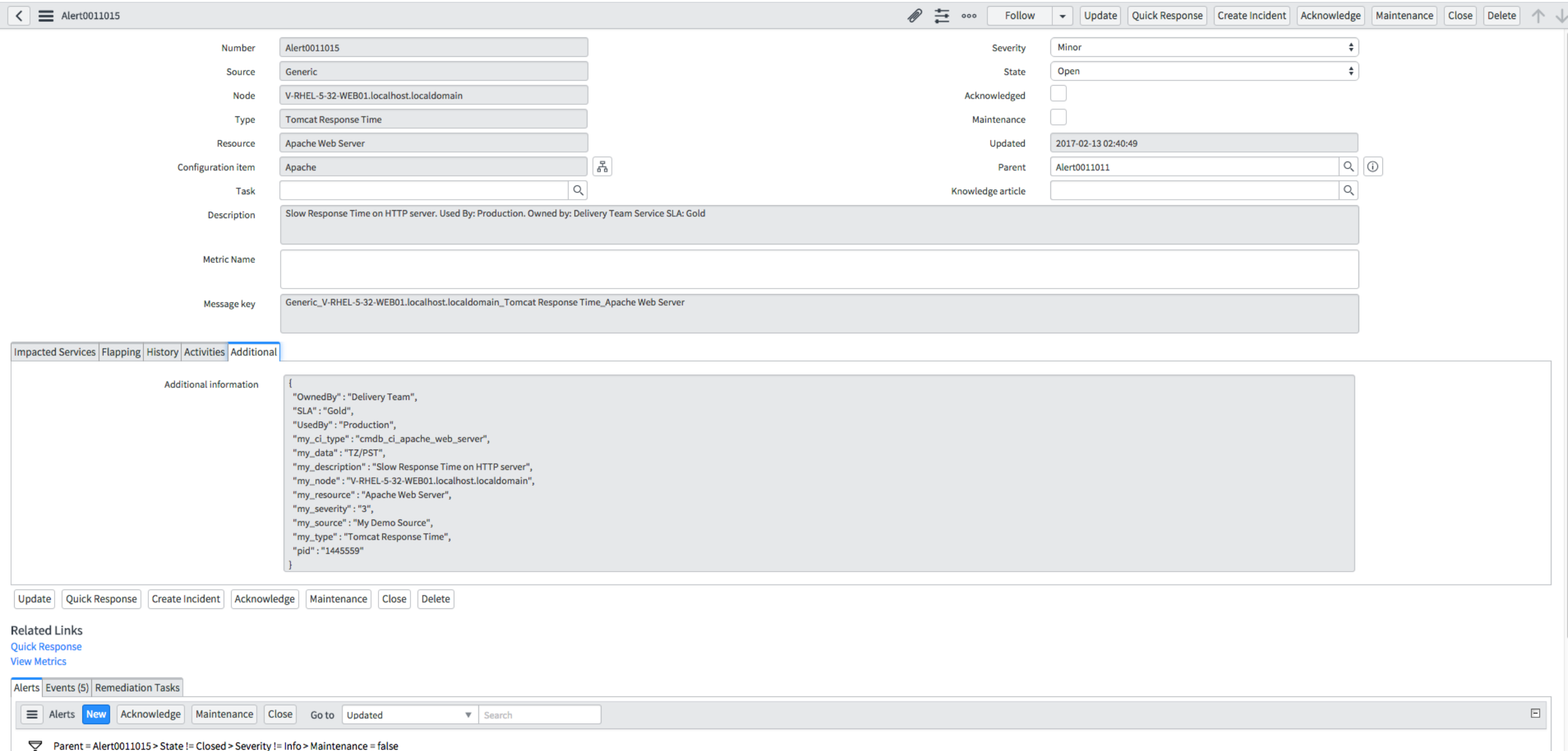
Use the Event Rule Designer to Compose New Alert - Threshold



Use the Event Rule Designer to Compose New Alert - Binding



Resend New Event and Capture its Transformation



Lab #1
Event Rule Designer

© 2017 ServiceNow All Rights Reserved

Lab Scenarios

- Send “free format” event to instance (use event free format JSON)
- Use Event Rule designer to reformat the raw event into a meaningful alert
- Use Event Rule designer to reformat the raw event into a meaningful alert using thresholds
- Use Event Rule designer to reformat the raw event into a meaningful alert using classic binding

© 2017 ServiceNow All Rights Reserved

Addendum

Lab 1.0: Event Rules Designer

Section: Send Event Using Event Management API Format

Step 2. Import Postman collection by doing the following:

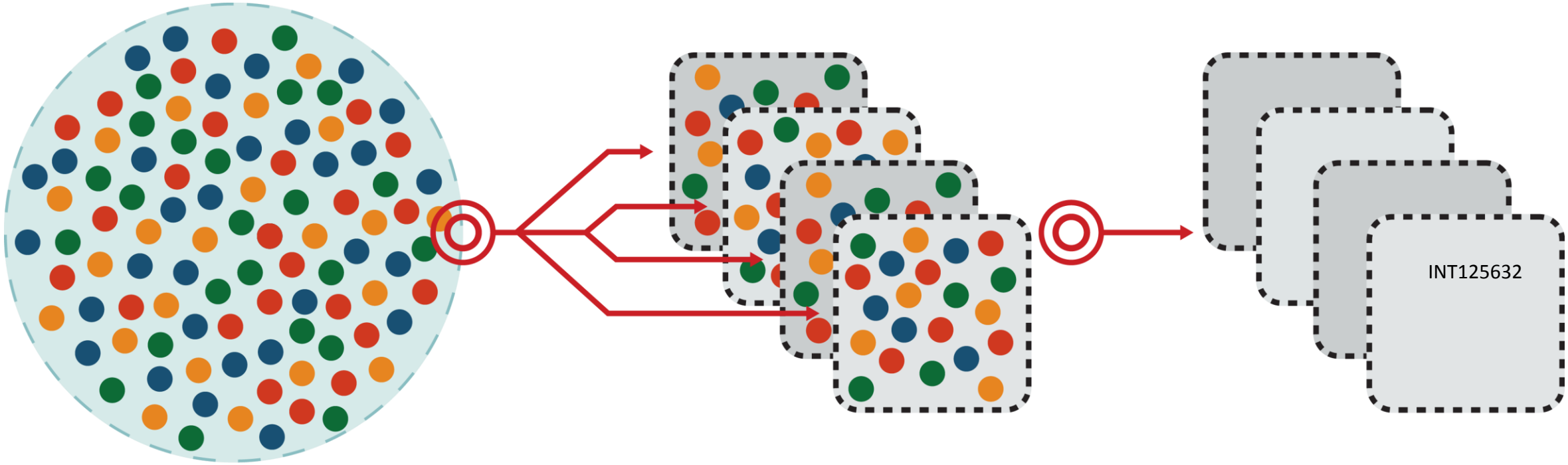
- Go to **Knowledge > Published** and search for **Short Description = *Postman** and click on article.
- On the **Manage Attachments** section in the top of the screen click on the **K17.postman_collection** to download the Postman collection.

© 2017 ServiceNow All Rights Reserved

Alert Correlation

© 2017 ServiceNow All Rights Reserved

Alert Correlation/Aggregation



IT Alerts

Alert Correlation

Incidents

© 2017 ServiceNow All Rights Reserved

What is Alert Correlation



Alert Correlation is a method of problem solving that organizes alerts based on temporal correlation and structural feature

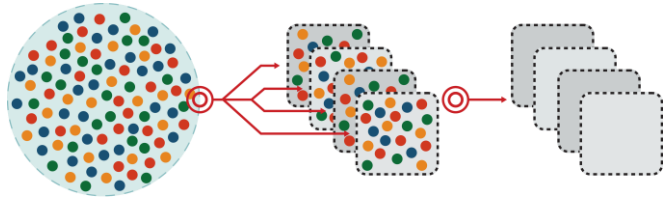
Its **objective** is to reveal significant relationships between alerts so that:

- Alerts can be combined and treated as a **single phenomenon**
- **Reveal key relationships** between alerts.
- **Eliminate noise** by only displaying alerts that are related

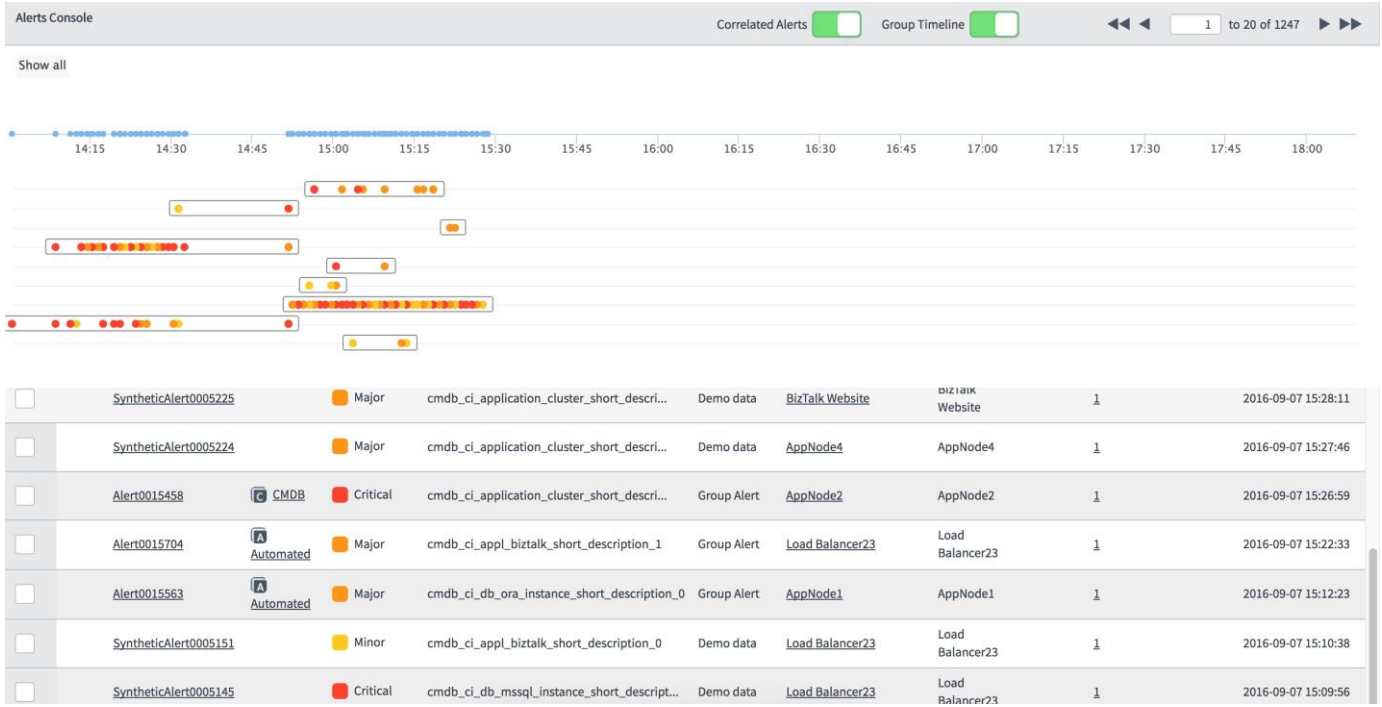
© 2017 ServiceNow All Rights Reserved

Machine Learning - Alert Correlation

Reduce noise and improve root cause analysis by service analytics

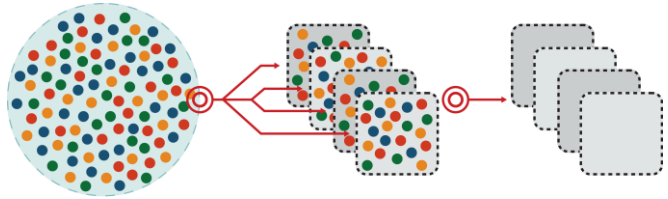


- Correlation Based on:
  - Time – Organize alerts together using temporal & stochastic relationship between alerts
  - Topology – Use deterministic relationship between infrastructure components
  - Pre-defined rules – Correlation rules
  - Neural Feedback – Based on human feedback on alert groups



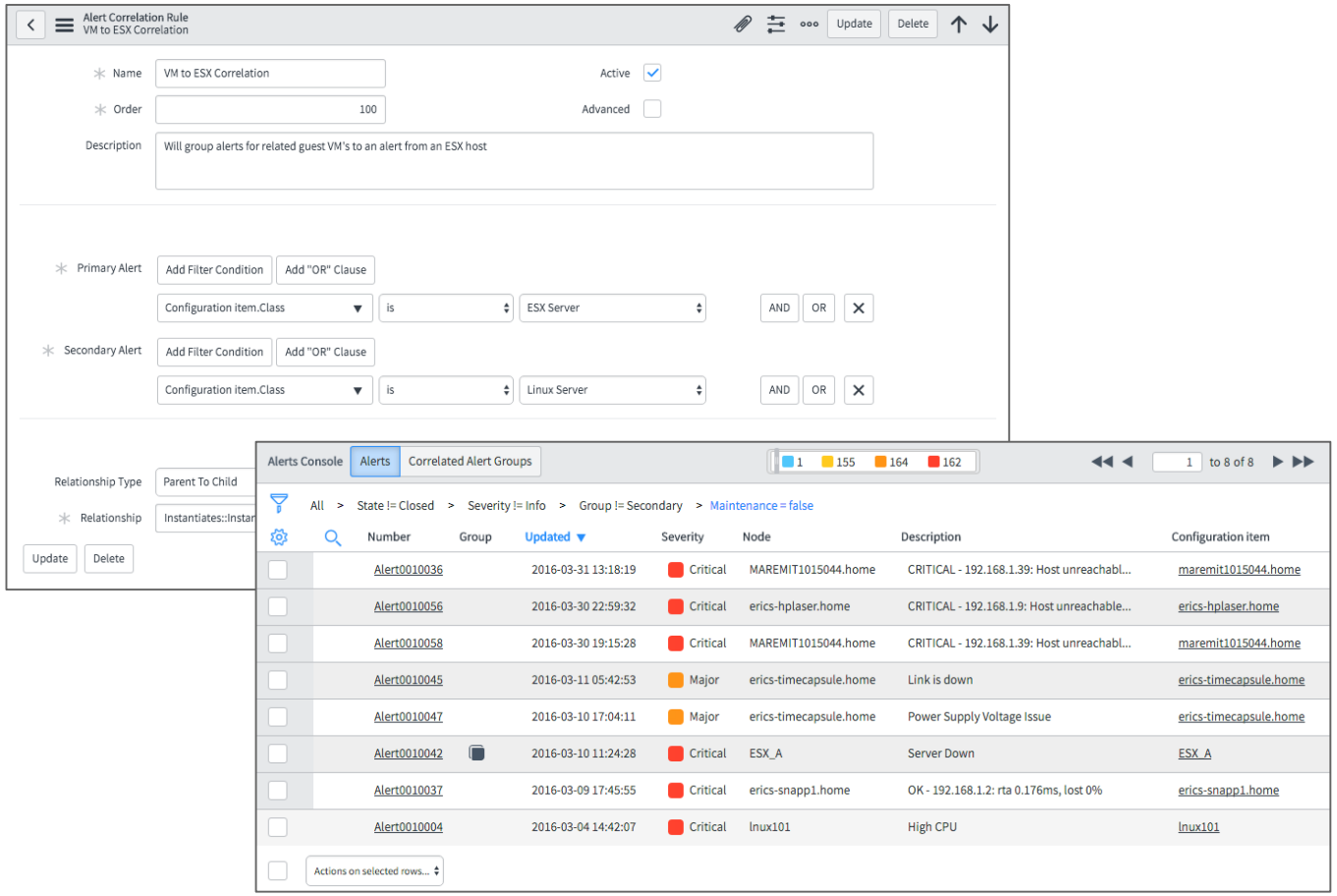
© 2017 ServiceNow All Rights Reserved

Rule-Based – Alert Correlation



Reduce noise and improve root cause analysis by correlation rules

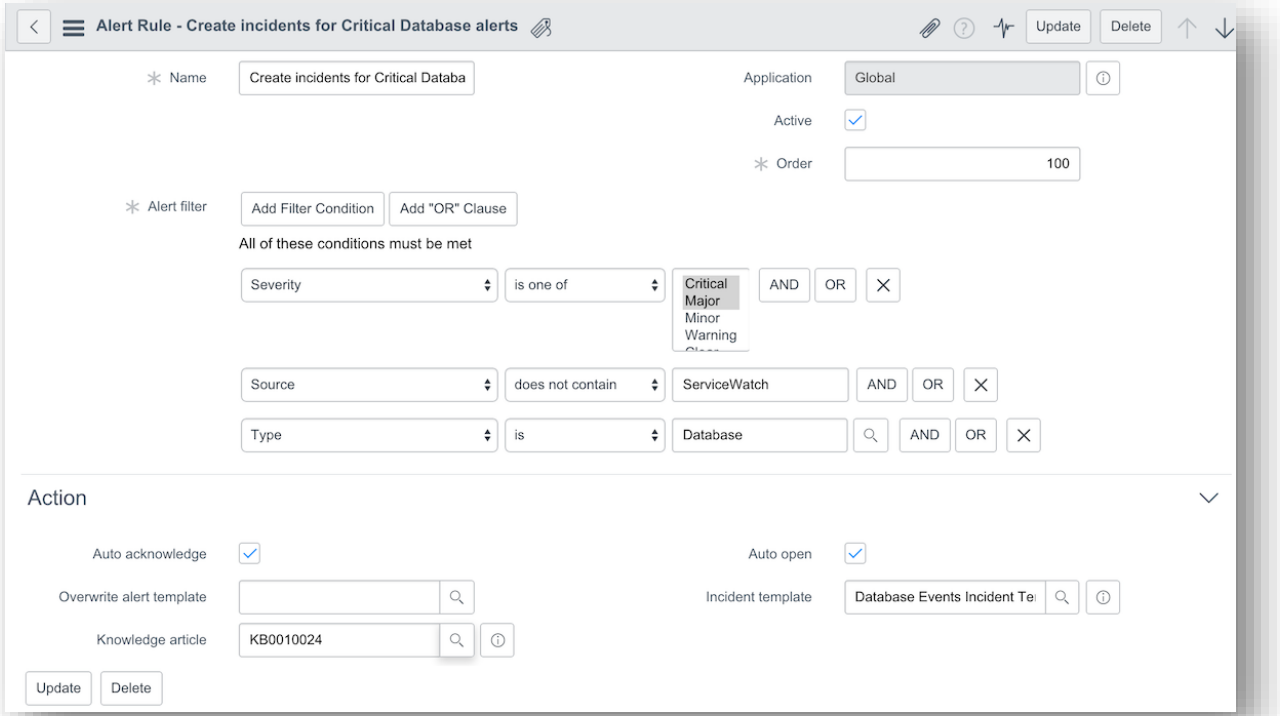
- Define rules based on notion of a Primary and Secondary alert
- Result: View ONE alert and drill into the correlated alerts
- Filters are based on alerts but can ‘dot walk’ to CI attributes
- Set the duration in which alerts should be correlated per rule
- Supports an advanced mode using script to define more complex use cases



© 2017 ServiceNow All Rights Reserved

Alert Action Rules – Automate Actions

(formerly – Alert Rules)



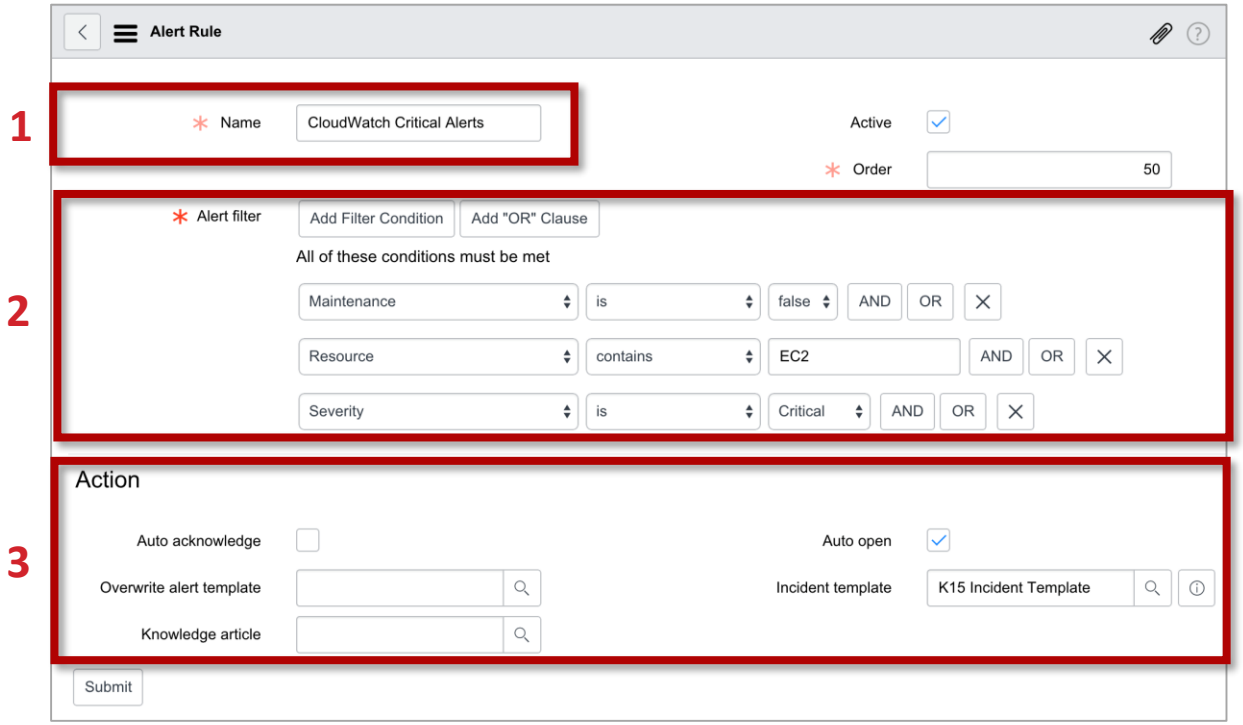
- Create Incidents
- Associate Knowledge
- Auto-acknowledge / Auto-open

- Alert enrichment via Overwrite alert templates
- Trigger remediation workflow (orchestration)
- Combine multiple steps in a single Alert rule

© 2017 ServiceNow All Rights Reserved

Components of an Alert Rule

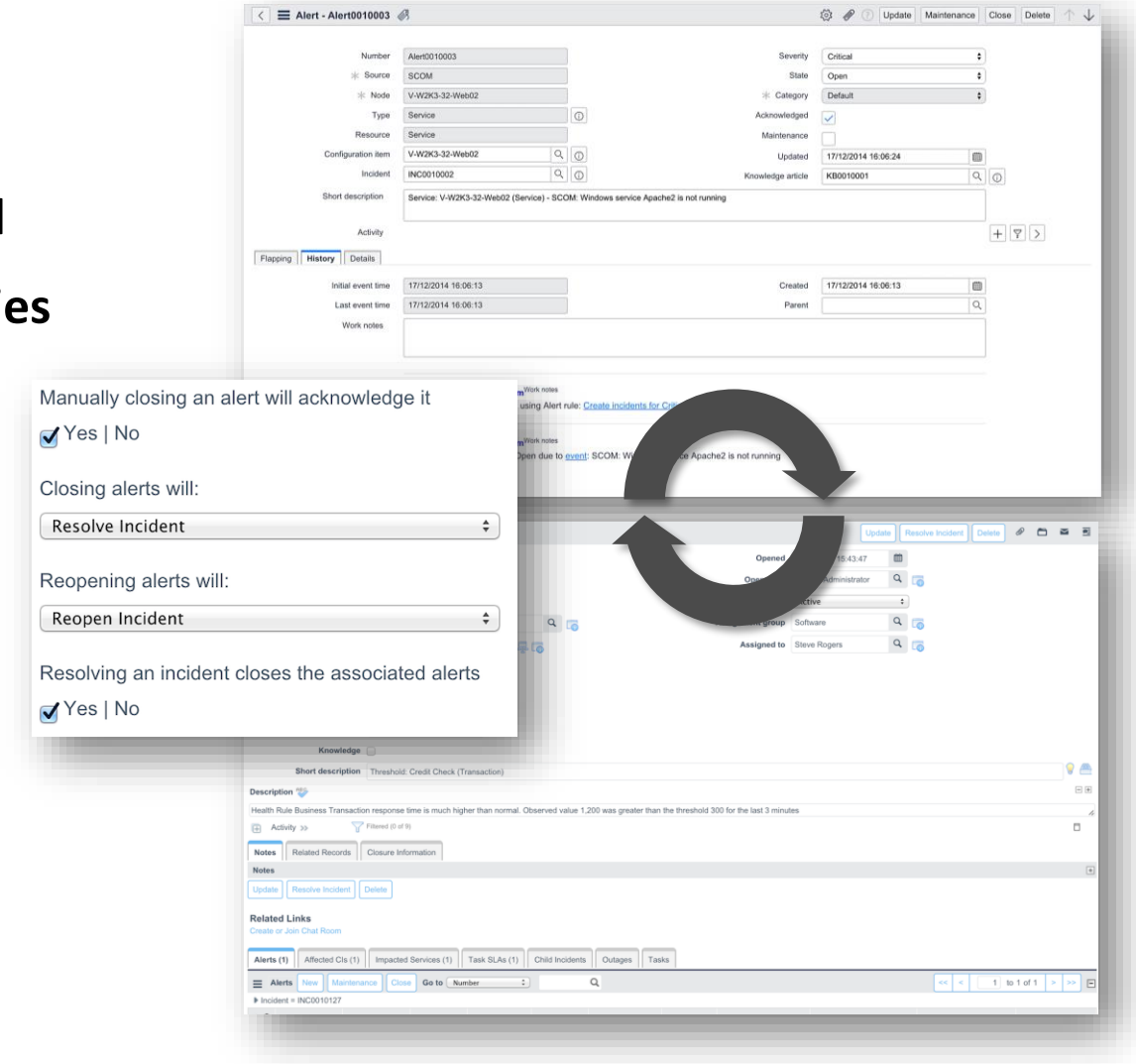
1. Name, e.g.: **CloudWatch Critical Alerts**.
2. Alert filter: configure a condition using fields
   e.g.:
   - **Maintenance** **is** **false**
   - **Resource** **contains** **EC2**
   - **Severity** **is** **Critical**
3. Action: automate responses to alerts meeting the condition.



© 2017 ServiceNow All Rights Reserved

Alert Action Rule Use Case – Create Incident

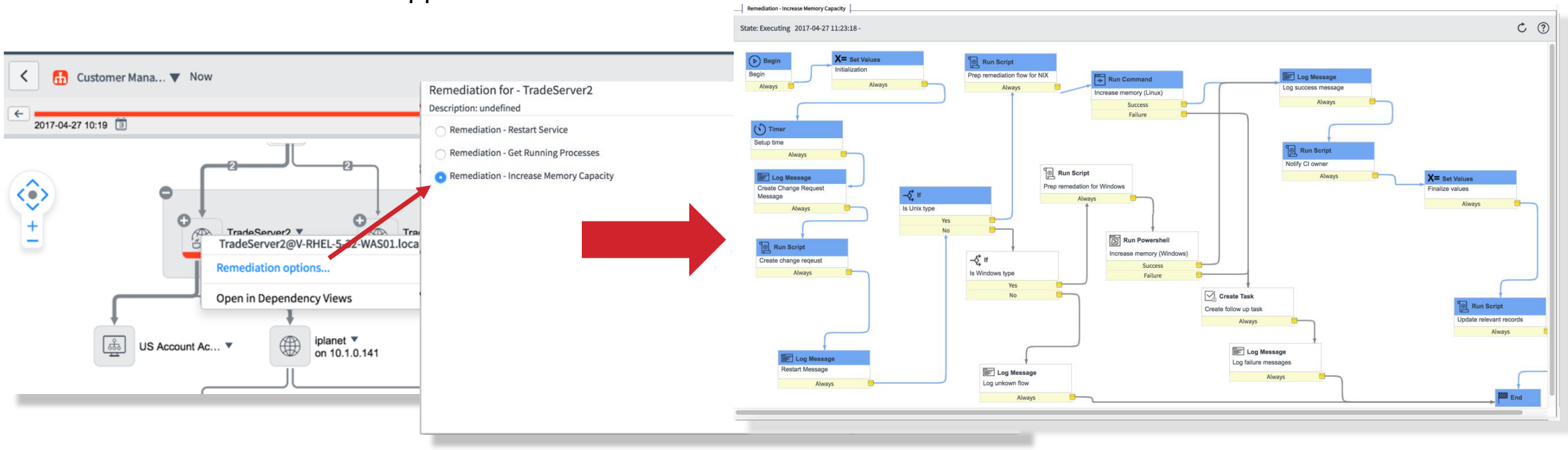
- Automatically create Incident states
- Resolve/Close an Incident and the related Alert is closed
- Close an Alert and the related Incident is resolved/closed
- Behaviour configurable in **Event Management > Properties**



© 2017 ServiceNow All Rights Reserved

Alert Action Use Case - Remediation

- Geneva Event Management introduced the ability to perform remediation for Alerts and CIs
- Remediation is based on orchestration workflows and a method of applying the workflow
- Remediation is available for two scenarios
  - Alert-based remediation – applied via an Alert Rule
  - CI-based remediation – applied via a CI Remediation definition



© 2017 ServiceNow All Rights Reserved

Lab #2: Correlation Rules & Actions

#Know17 | http://clabs.link/lab131978

© 2017 ServiceNow All Rights Reserved

Lab 2 Scenarios

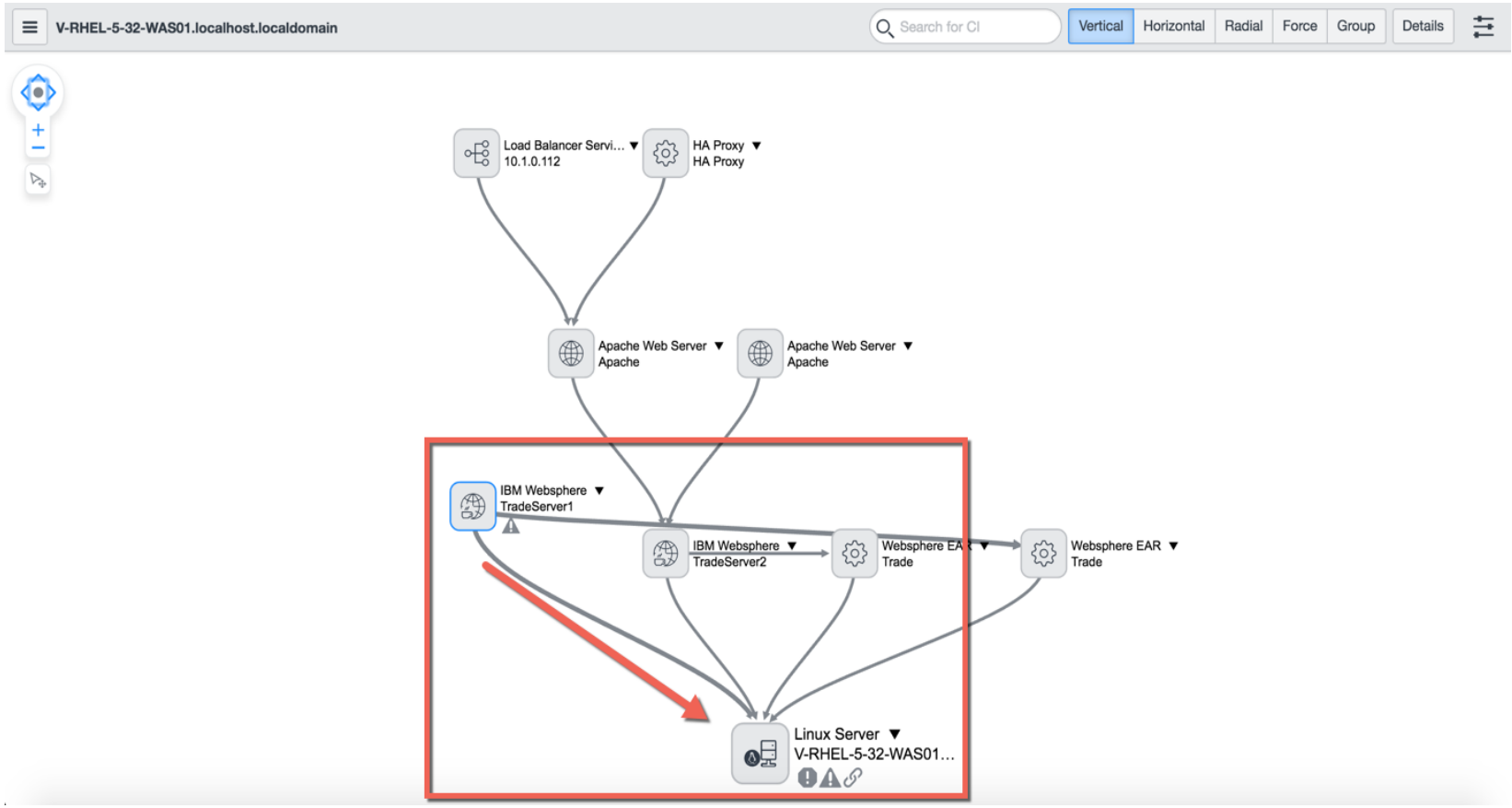
- Lab 2.0: CMDB Correlation - Send Alerts from CIs that have CMDB relationship and explore CMDB event correlation
- Lab 2.1: Manual Correlation – Build a manual correlation between CIs and explore effect on events.
- Lab 2.2: Alert Action Rule – Create an an incident automatically when Critical Event is received from a Windows Server and automatically assign the ticket.

© 2017 ServiceNow All Rights Reserved

Addendum

Lab 2.0: CMDB Correlation

Step 6 - Notice that **TradeServer1 WebSphere Server** has a …..



© 2017 ServiceNow All Rights Reserved

Triage Service Outage

#Know17 | http://clabs.link/lab131978

© 2017 ServiceNow All Rights Reserved

Demo – Triage Service Outage

- Detect/Sense
- Analyze
- Response

© 2017 ServiceNow All Rights Reserved

Lab #3
End to End Simulation

© 2017 ServiceNow All Rights Reserved

Lab 3 Scenarios

- Detect and Prioritize – Receive events and see impact on of events on the business to prioritize what gets worked on.
- Analyze – Drill into issues affecting a critical business application to explore impact and probable root cause of the issue
- Respond – Create an Emergency Change from the Incident record to take corrective actions to fix the issue.

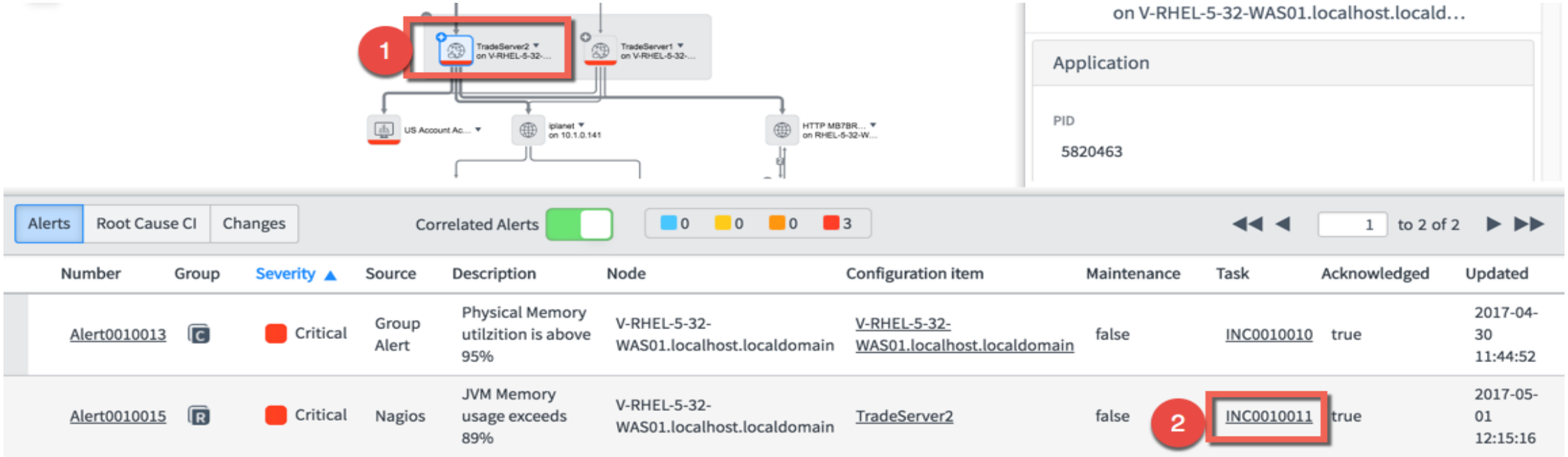
© 2017 ServiceNow All Rights Reserved

Addendum

Section: **Respond**

Create an Emergency Change against this issue to roll back the change.

Step 1: Return to **Dashboard View** and click on **Tradeserver2** to filter Alerts associated with this CI and then click on the **incident** associated with the rule based alert.



© 2017 ServiceNow All Rights Reserved

Top Takeaways

1

Reduce noise by automatic filtering and aggregating raw events into actionable alerts

2

Increase Service Availability by utilizing Service Mapping with Event Management

3

Take Automatic Corrective Actions to reduce MTTR

© 2017 ServiceNow All Rights Reserved

Thank You

Lab Sponsored by Amazon Web Services



Benny Makovsky
Sr. Product Manager
ServiceNow

Joe Steinfeld
Advisory Solution Consultant
ServiceNow

#Know17 | http://clabs.link/lab131978

© 2017 ServiceNow All Rights Reserved