knowledge17

WORK at LIGHTSPEED™

Operational Intelligence - Event Management vNext

BENNY MAKOVSKY
SR PRODUCT MANAGER
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

Agenda

- Operational Intelligence Overview
- What's new in Jakarta
- Key use cases

© 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, Ex-CA for 16 years as chief architect

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

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

CURRENT PROJECTS: Service Mapping and Operational Intelligent vNext

© 2017 ServiceNow All Rights Reserved

Objectives and What You Will Learn



Objectives

- What's new in Operational Intelligence (EM) in Jakarta



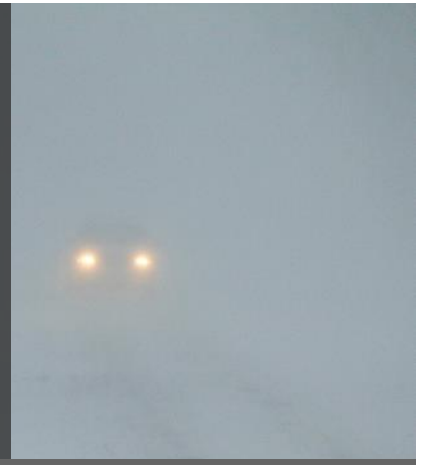
What You Will Learn

- The main challenges we try to solve with OI
- Learn about new capabilities in Event Management
- Understand how OI help elements service outage
- How can OI help in reducing MTTR and be proactive when it come to service availability

© 2017 ServiceNow All Rights Reserved

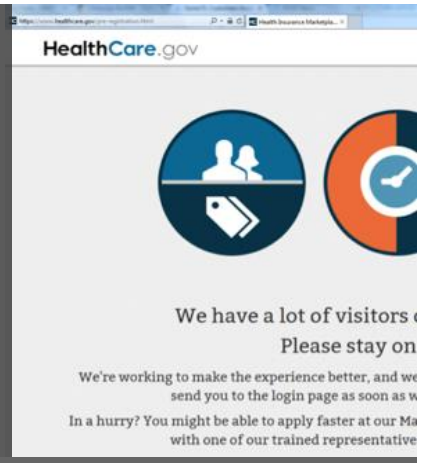
Challenges Facing IT Operations Teams

Lack of Service Visibility



I can’t tell which systems are connected to each service.

Unreliable Service Availability



If a service goes down, I can’t find the cause of the outage.

Slow Service Delivery



We need to accelerate service delivery, while maintaining quality.

© 2017 ServiceNow All Rights Reserved

Today's Challenges

"For the Fortune 1000, the average total cost of unplanned application downtime per year is $1.25 billion to $2.5 billion.

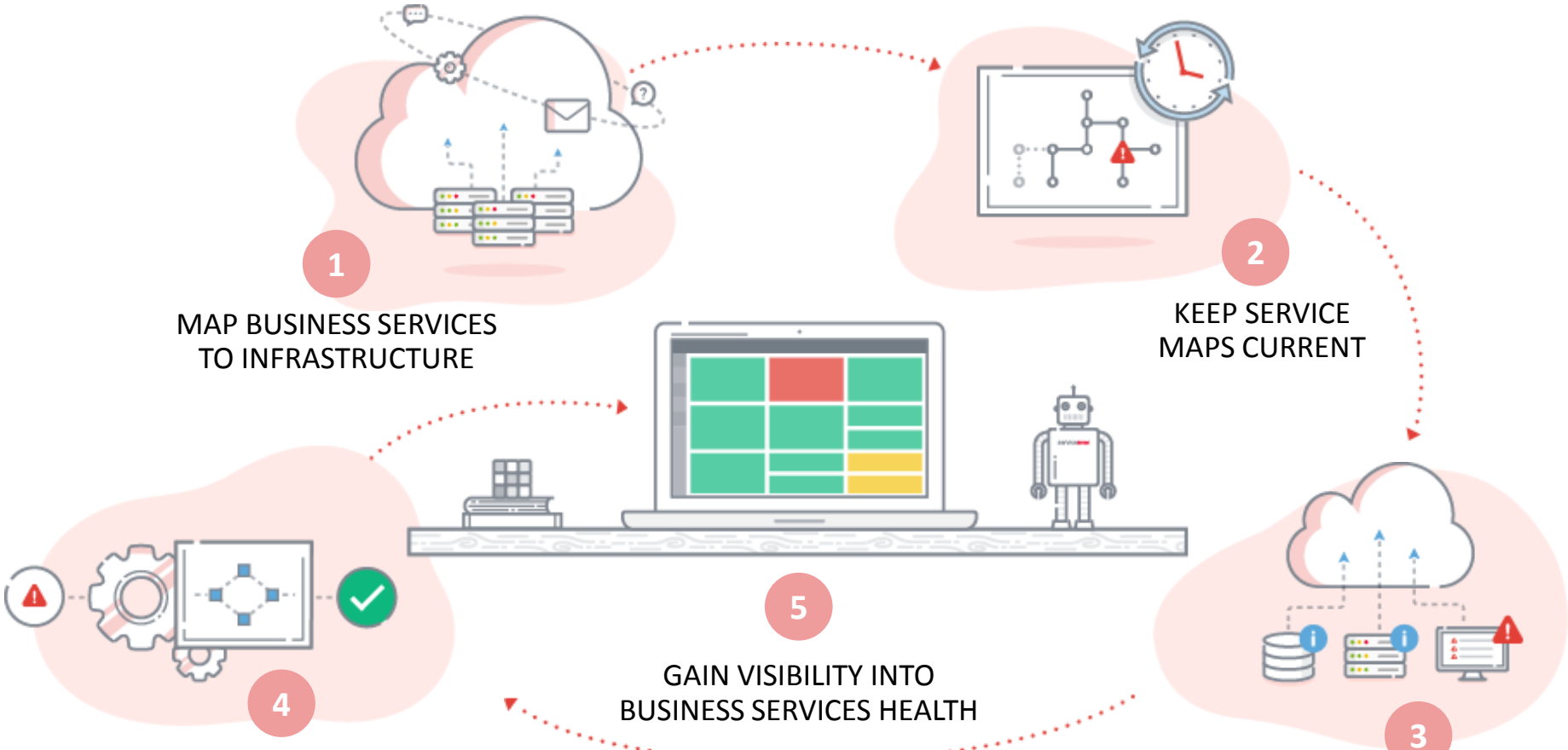
The average hourly cost of an infrastructure failure is $100,000 per hour.

The average cost of a critical application failure per hour is $500,000 to $1 million."

IDC sponsored by AppDynamics

© 2017 ServiceNow All Rights Reserved

How to Eliminate Service Outages

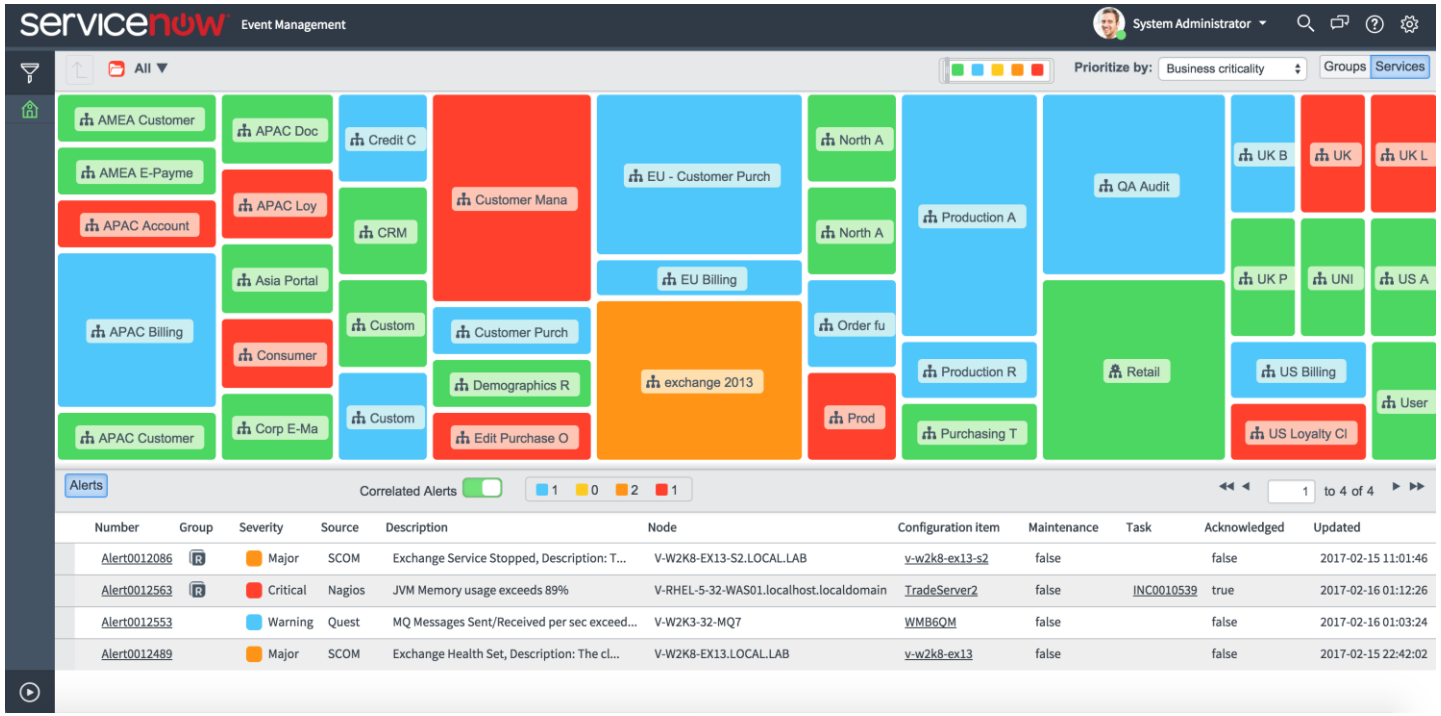


© 2017 ServiceNow All Rights Reserved

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



Key Enablers

© 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

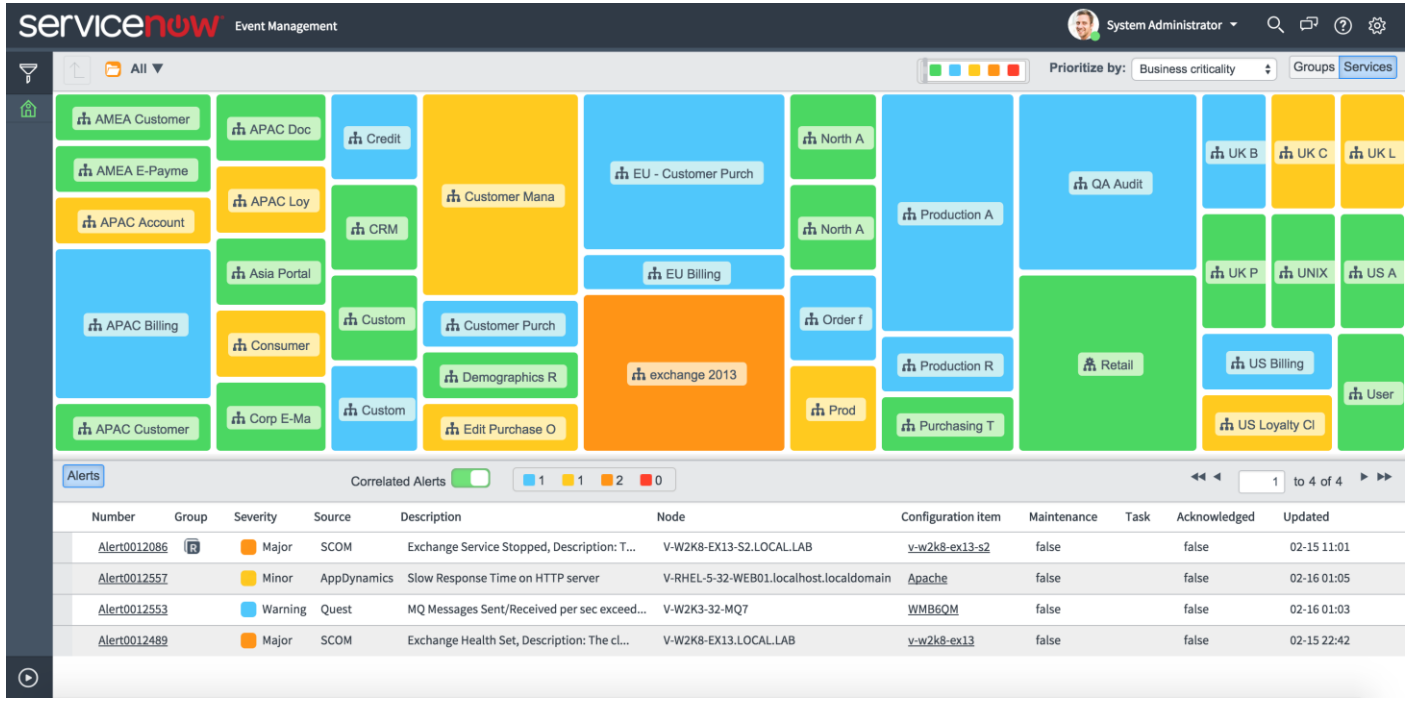
Microsoft System Center Operations Manager
solarwinds
amazon web services CloudWatch
Nagios *
bmc *
ORACLE *
splunk>
Hewlett Packard Enterprise
IBM Tivoli software Netcool
vmware
ZABBIX
Microsoft Azure *
Panopta *

OOB

REST API
SNMP

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

ServiceNow Store and 3rd party

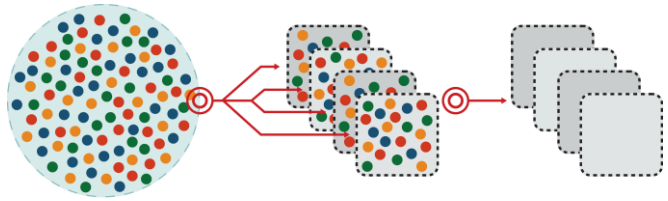


Logos are trademarks or registered trademarks of their respective owners and not ServiceNow

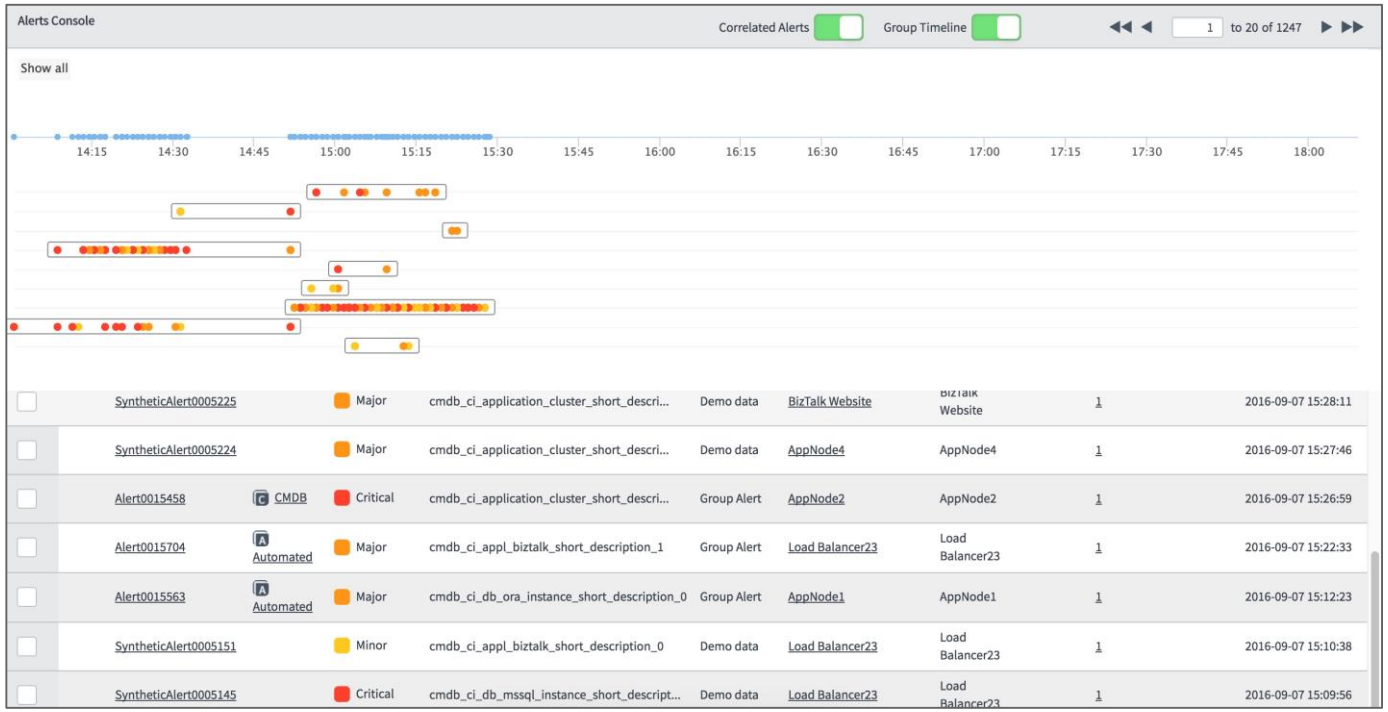
© 2017 ServiceNow All Rights Reserved

Machine Learning - Alert Correlation

Reduce noise and improve root cause analysis by service analytics



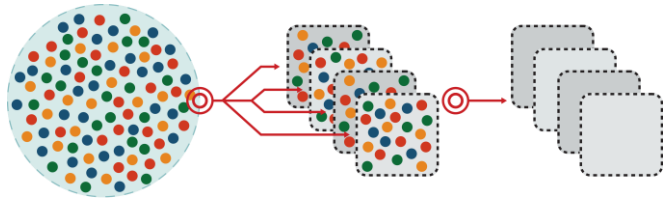
- Correlation Based on
  - Time – Organize alerts together using temporal & stochastic relationship between alerts
  - Topology – Use deterministic relationship between infrastructure components
  - Pre defined rules - Correlation rules
  - Neural Feedback – Based on human feedback on alert groups



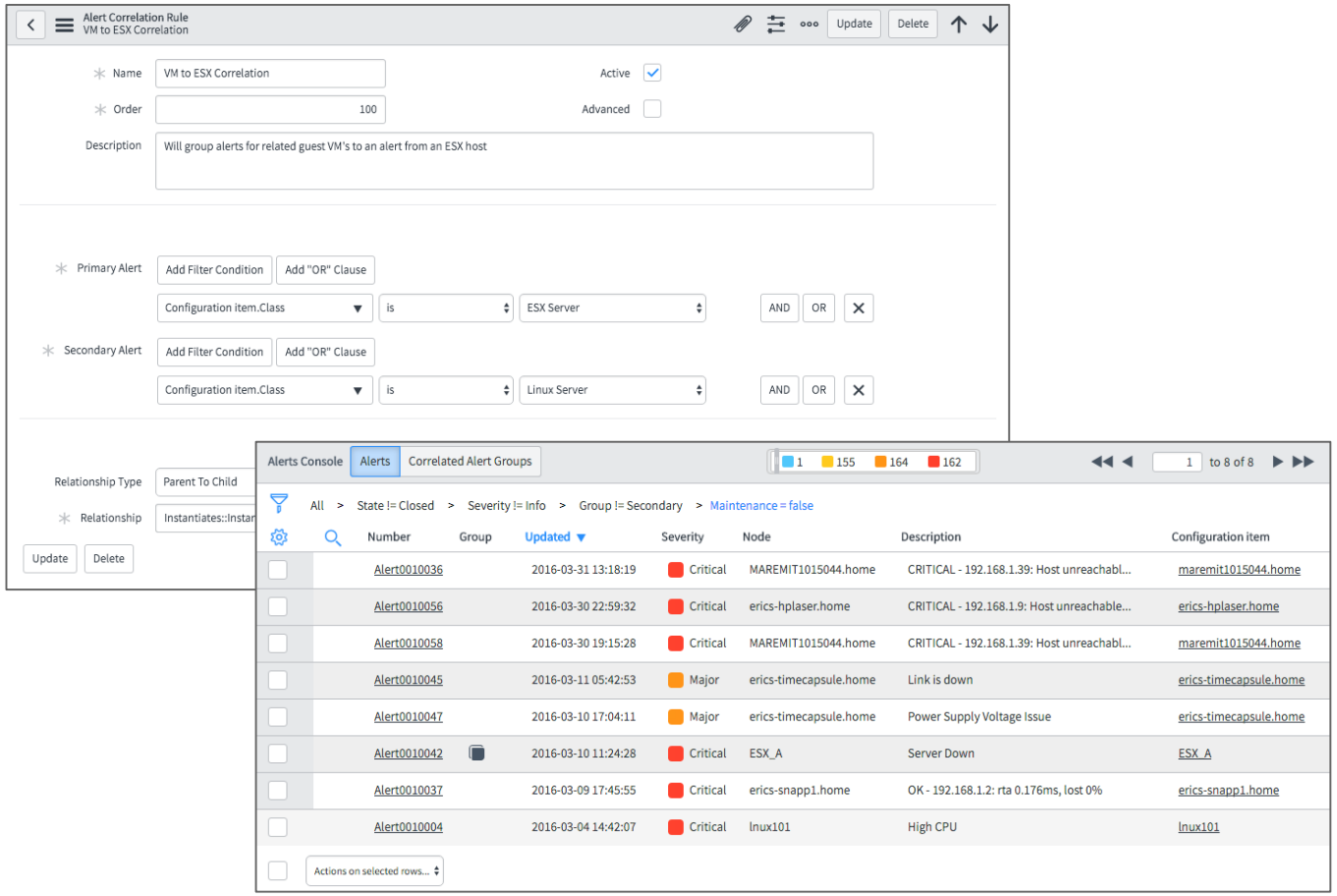
© 2017 ServiceNow All Rights Reserved

Rule Based - Alert Correlation

Reduce noise and improve root cause analysis by correlation rules



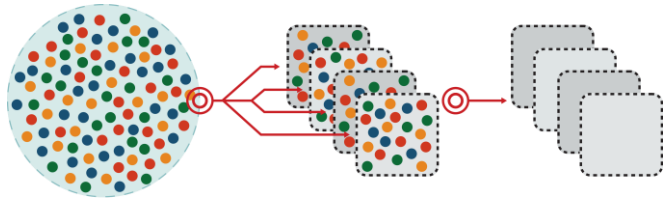
- Define rules based on notion of a Primary and Secondary alert
- Result: View ONE alert and drill into the correlated alerts
- Filters are based on alerts but can ‘dot walk’ to CI attributes
- Set the duration in which alerts should be correlated per rule
- Supports an advanced mode using script to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



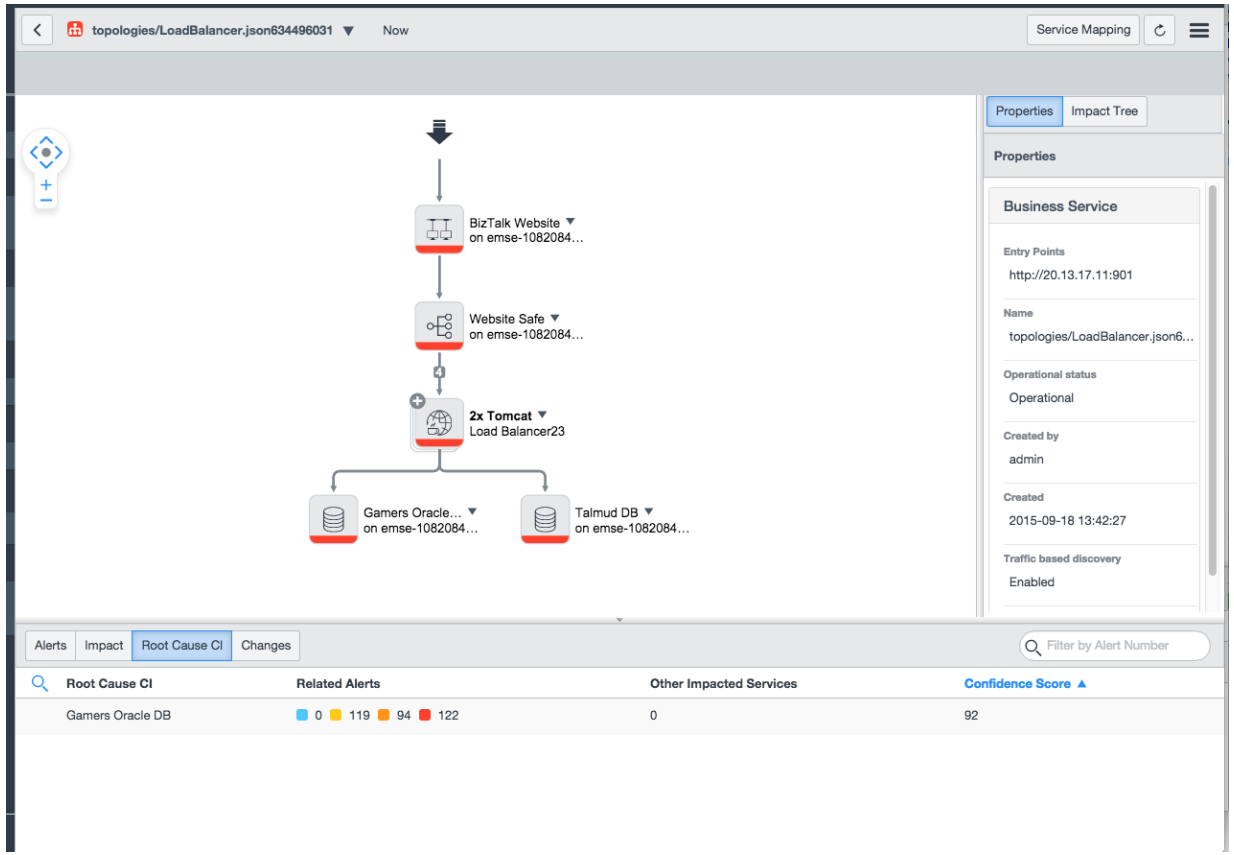
© 2017 ServiceNow All Rights Reserved

Machine Learning - Root Cause Analysis

Assign probabilities to root causes



- Assign probabilities to root causes when a significant event (alarm, failure, etc.) could have been the result of more than one upstream event
- most likely root causes can be investigated before less likely root causes
- Discover causal relationships between events unknown to the designer of the service model

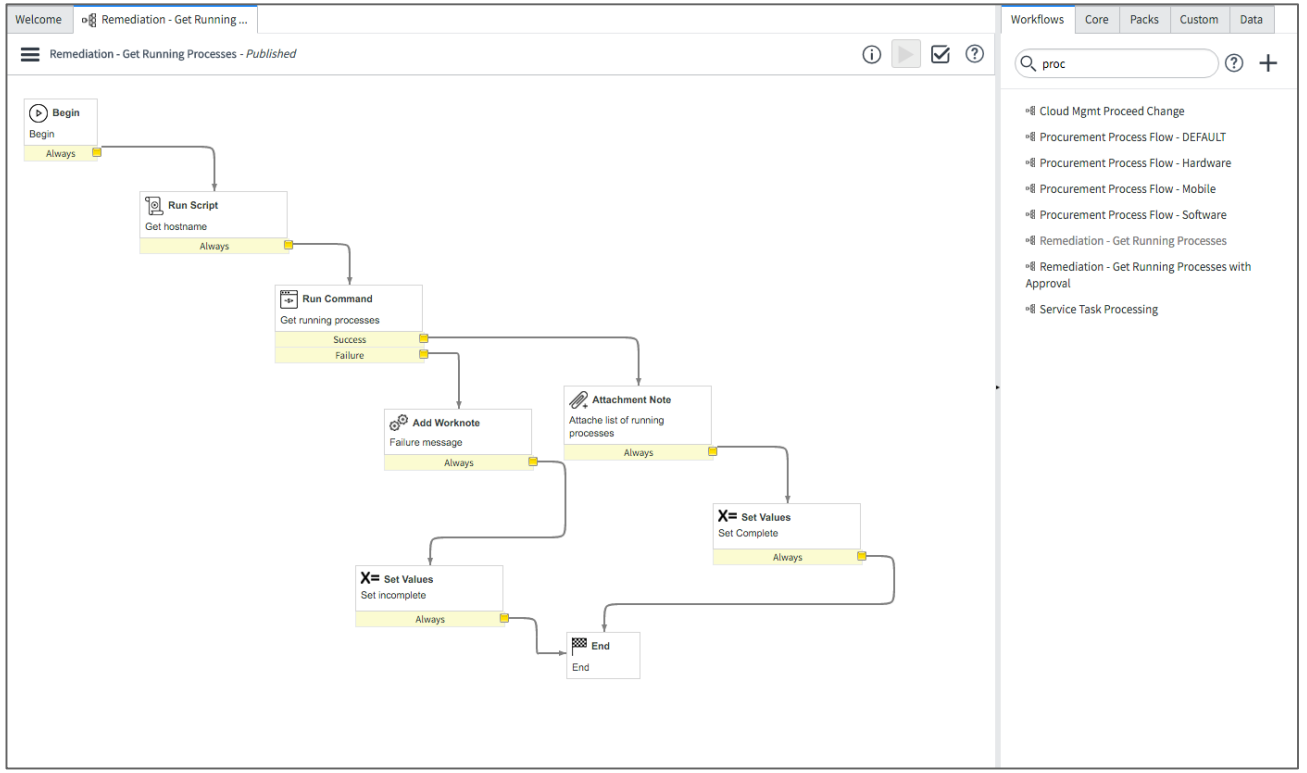


© 2017 ServiceNow All Rights Reserved

Automated Remediation

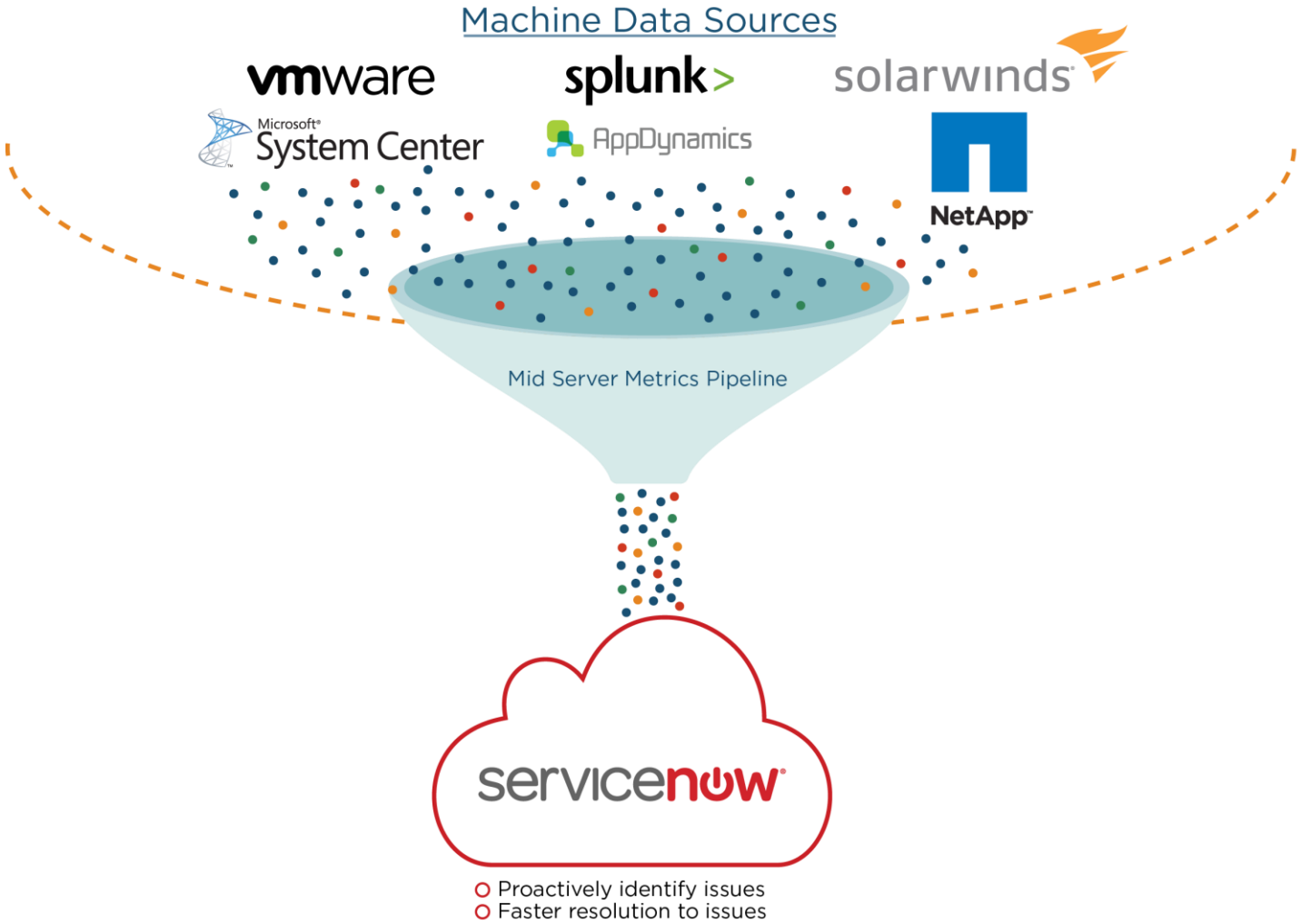
Perform remediation by automatically (or manually) triggering Orchestration workflows

- Fully automated remediation
  - E.g: Reboot server, Restart service, Increase capacity
  - Can also be used for automated reconnaissance
- Leverage Orchestration Workflow capabilities:
  - Point-and-click workflow authoring
  - SSH, PowerShell, REST, SOAP
  - Extensible
- Fall back on human fulfillment if needed

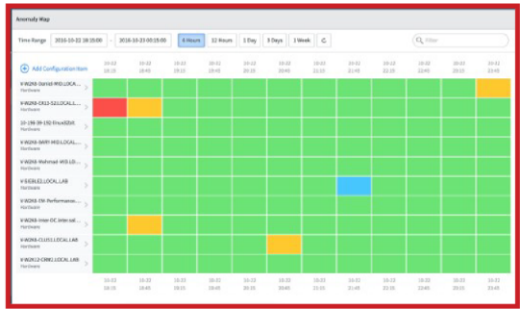


© 2017 ServiceNow All Rights Reserved

Operational Metrics



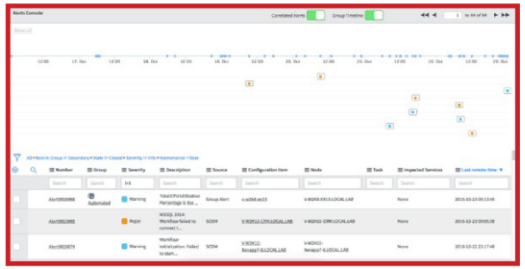
Anomaly Heat Map



Metrics Explorer



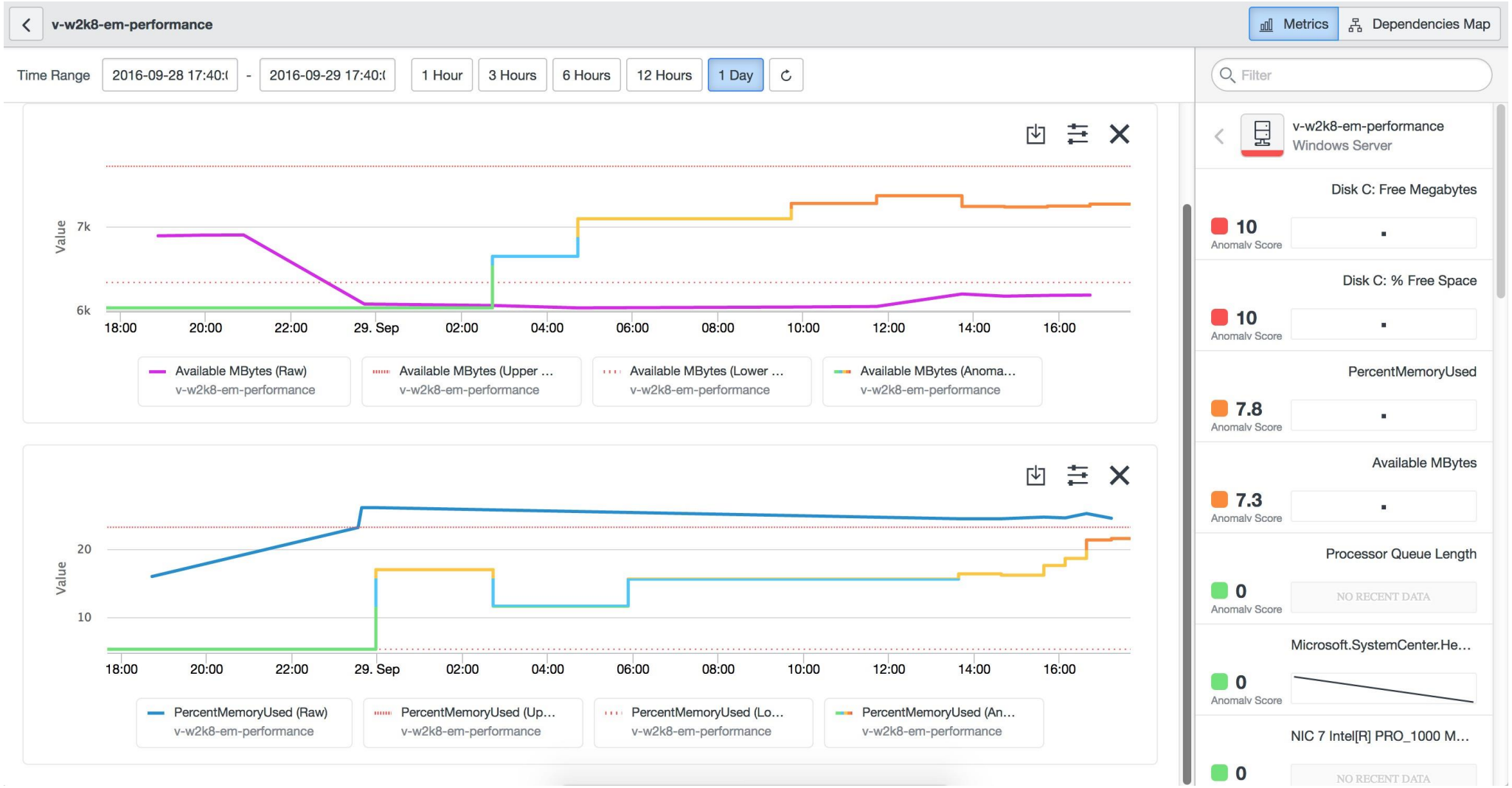
Anomaly Alerts



Logos are trademarks or registered trademarks of their respective owners and not ServiceNow

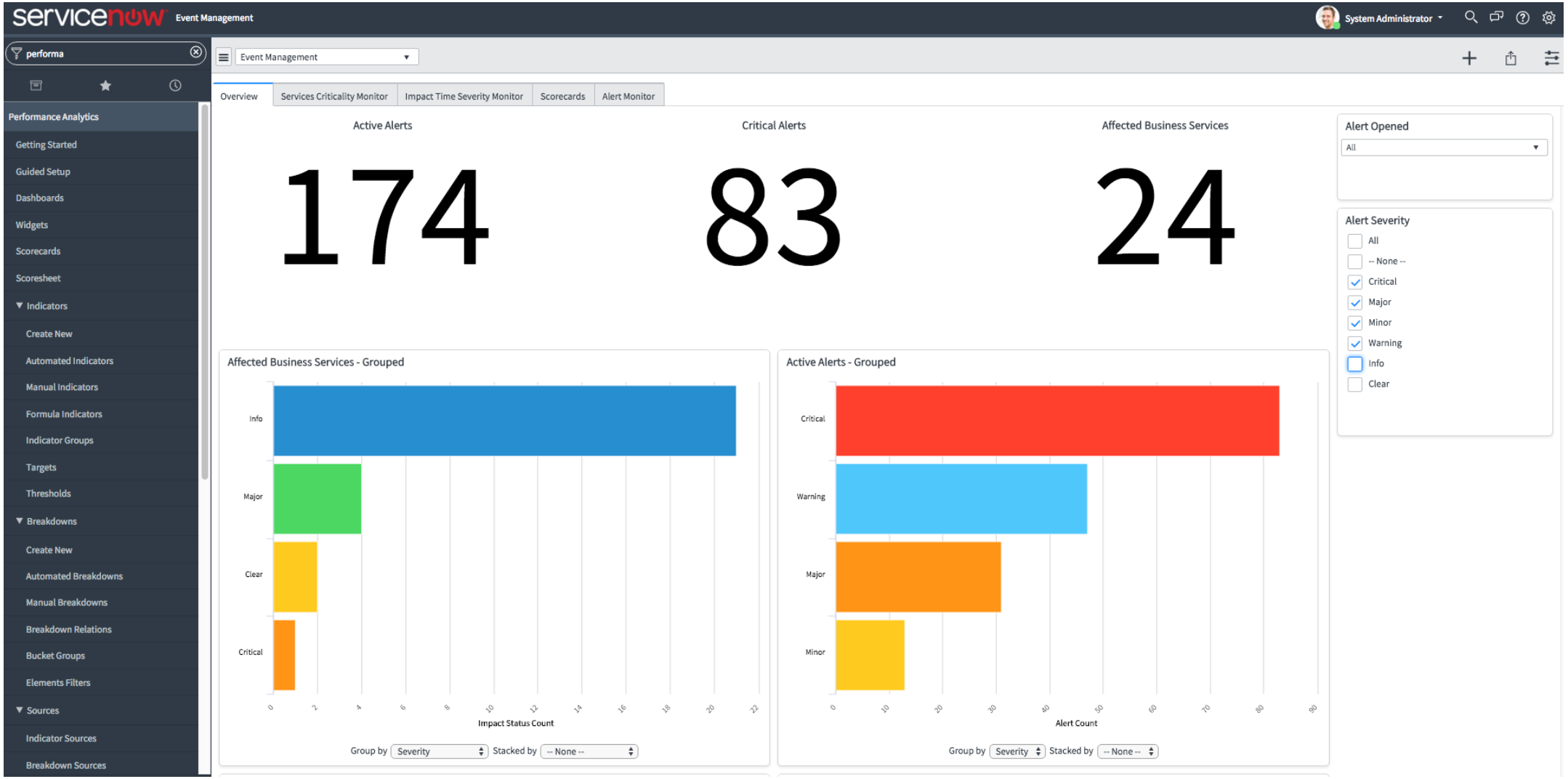
© 2017 ServiceNow All Rights Reserved

Anomaly Metrics – Istanbul+



© 2017 ServiceNow All Rights Reserved

Performance Analytics Dashboard



© 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
- 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
  - Performance improvements – Updated SCOM metric collection
  - New Time Series DB (clotho) – better scale and performance
- Service Analytics
  - New predictive alerts
  - Updated RCA logic

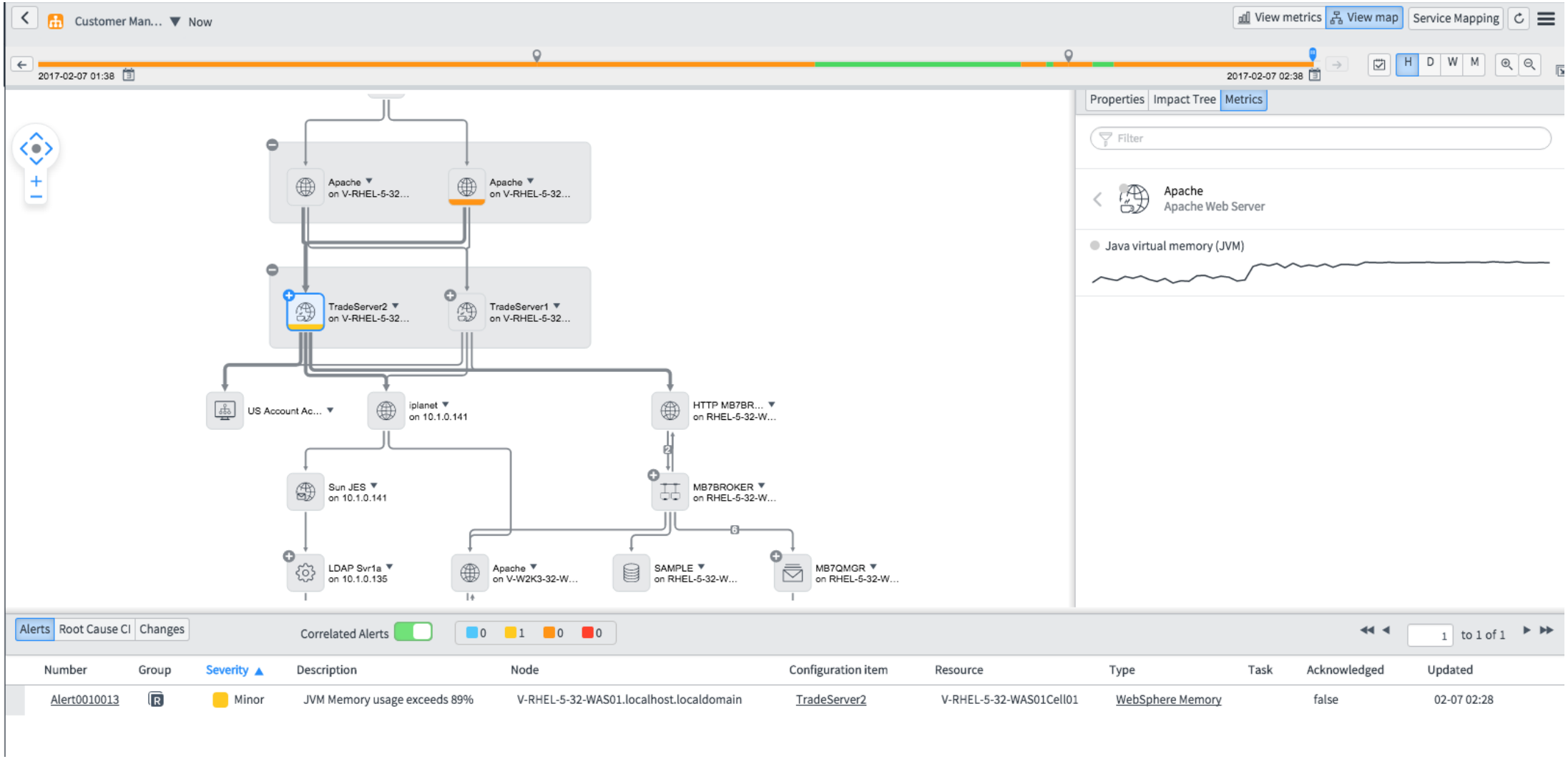
© 2017 ServiceNow All Rights Reserved

Jakarta New Feature Overview

- Product: Event Management
- User Persona(e): EM Admin, EM Operator
- Feature/Capability: Business Service Metrics
- Description of Feature: Operational metrics data (anomalies and performance charts) are embedded into business service maps
- Differentiation Assessment: Better service health triage by adding performance data into the service context.

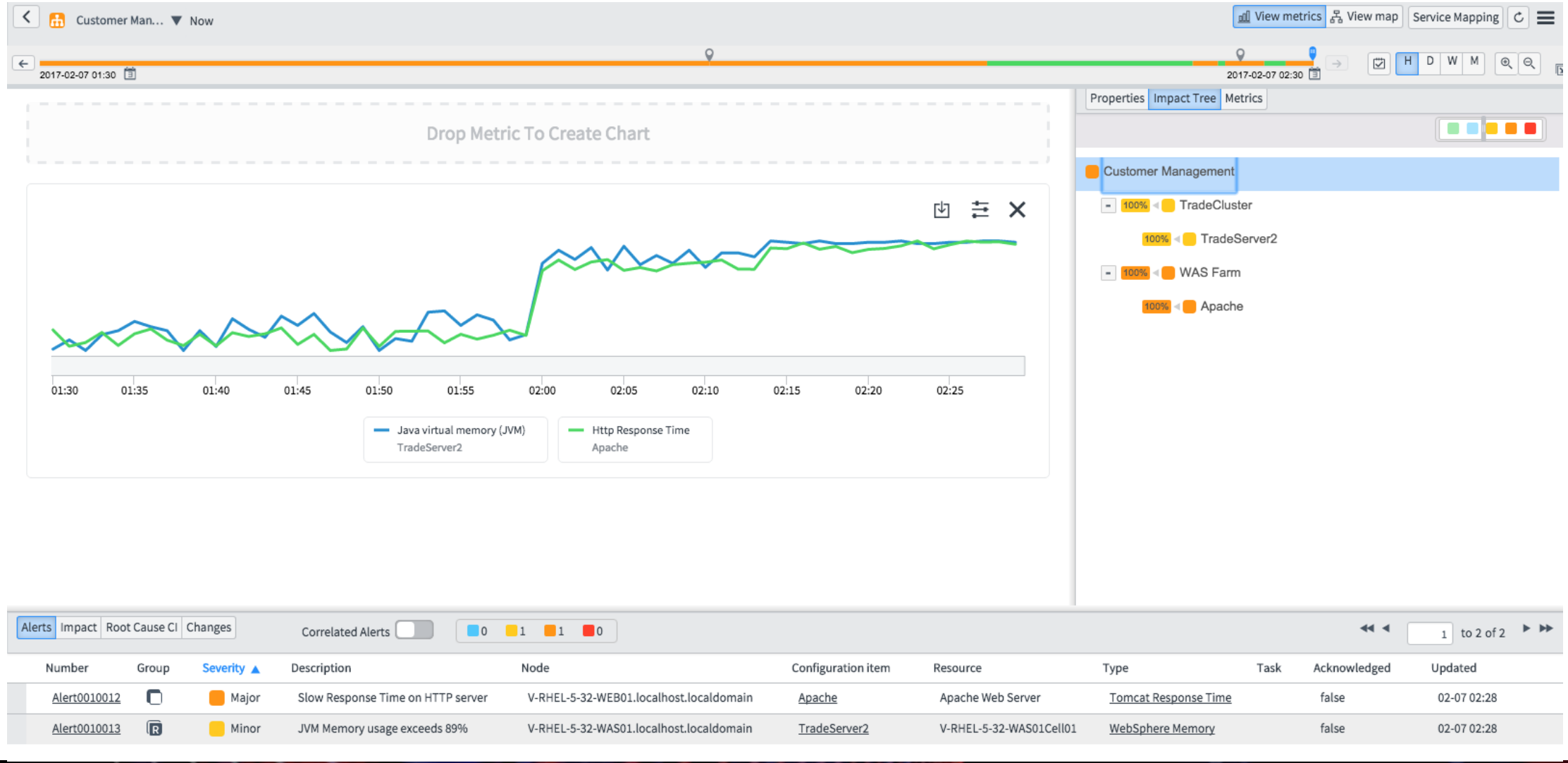
© 2017 ServiceNow All Rights Reserved

Business Service Metric



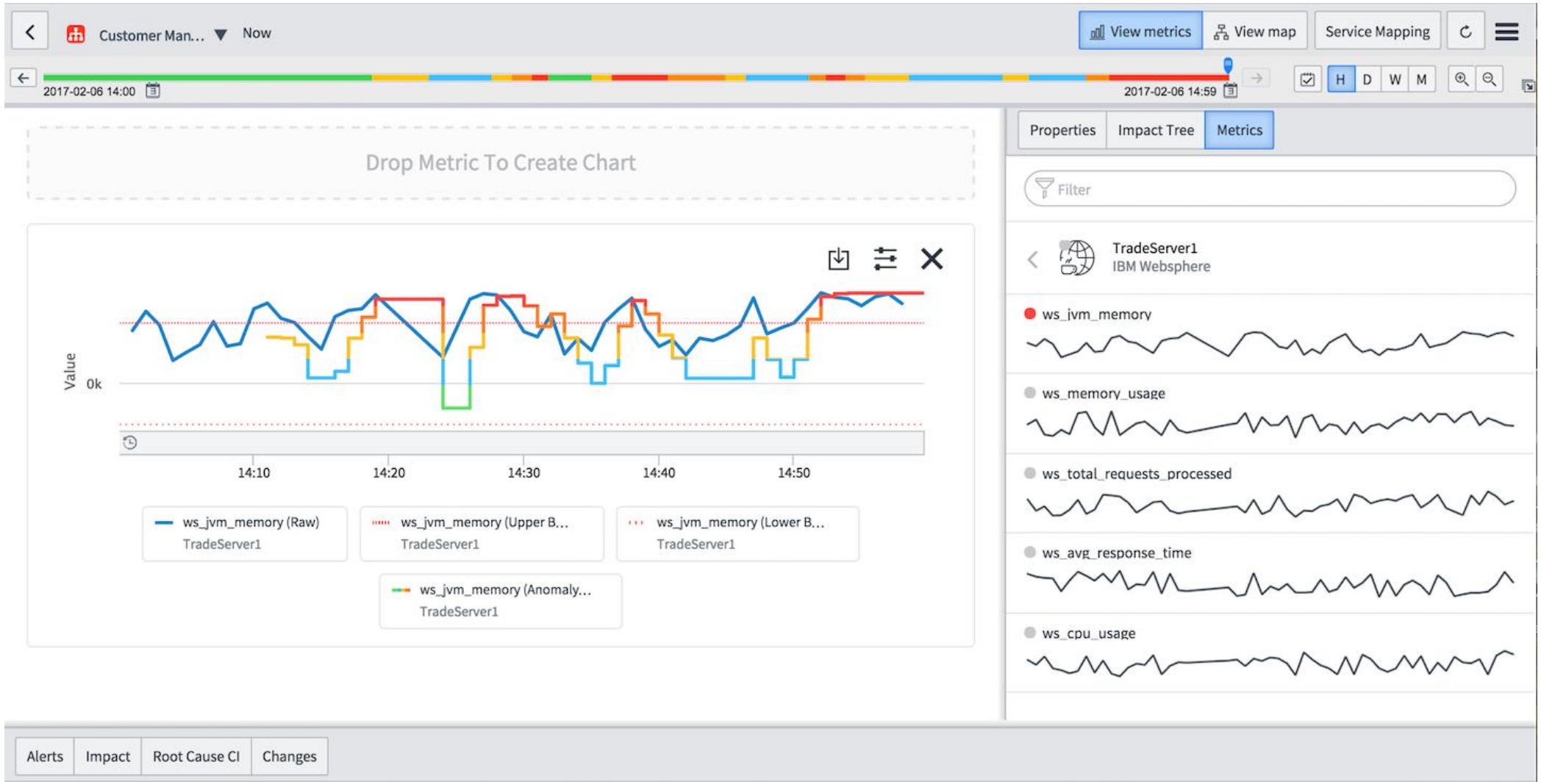
© 2017 ServiceNow All Rights Reserved

Business Service Metric



© 2017 ServiceNow All Rights Reserved

Business Service Metric



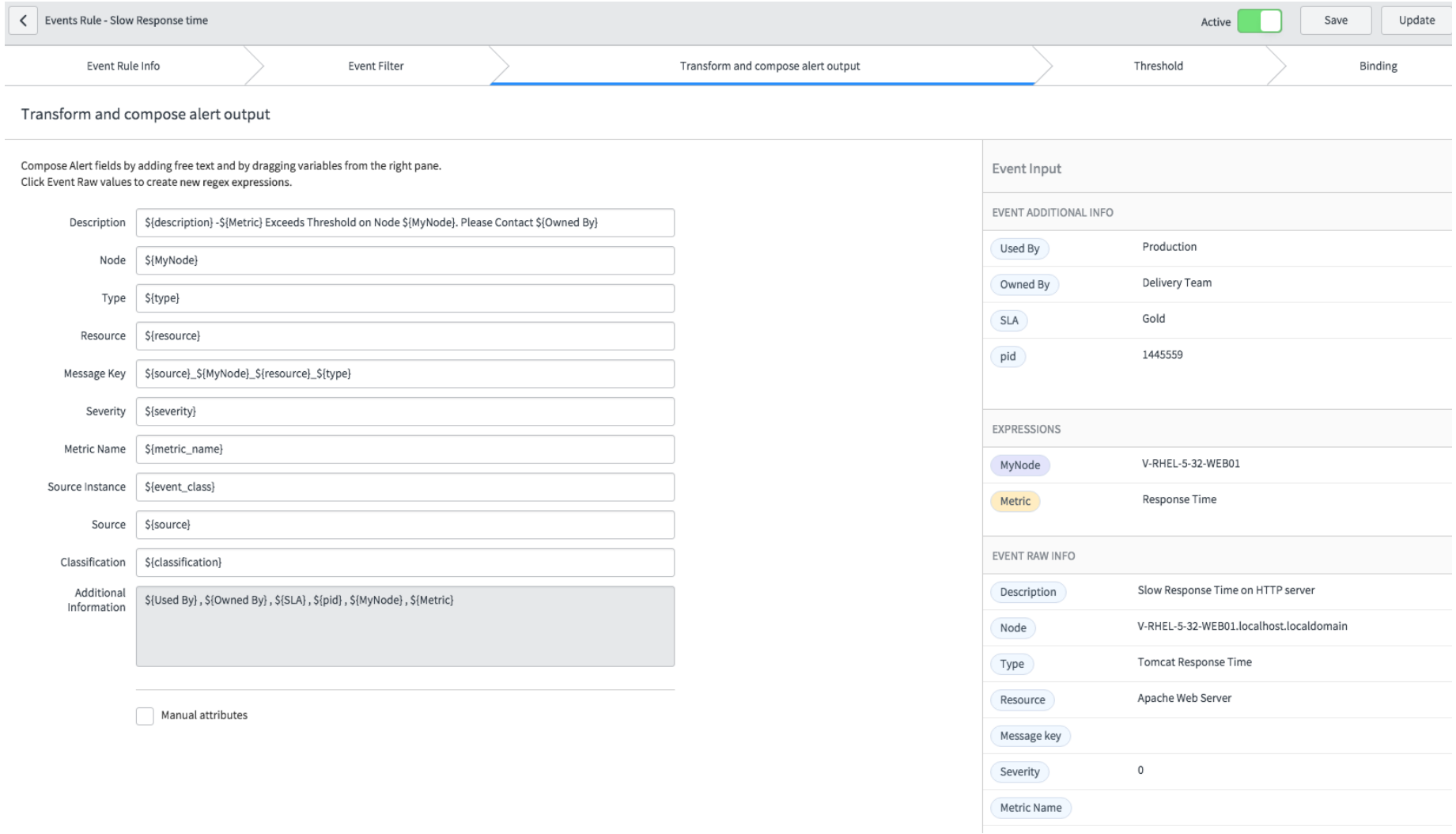
© 2017 ServiceNow All Rights Reserved

Jakarta New Feature Overview

- Product: Event Management
- User Persona(e): EM Admin, EM Operator
- Feature/Capability: 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

Event Rules Designer



© 2017 ServiceNow All Rights Reserved

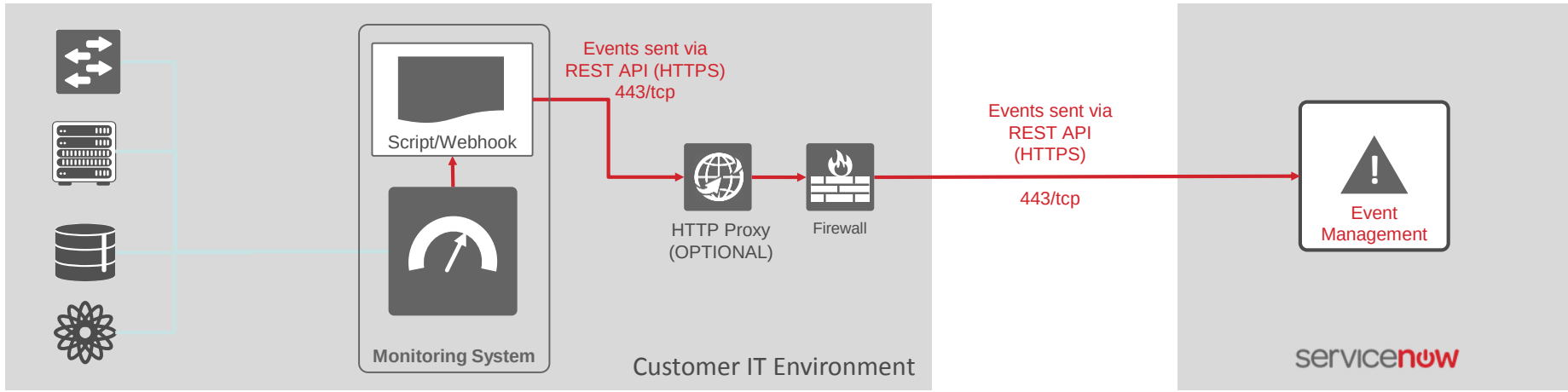
Jakarta New Feature Overview

- Product: Event Management
- User Persona(e): EM Admin, EM Operator
- Feature/Capability: New push and transform API to integrate event sources both on the Instance and in the MID. OOB support for Cloud (AWS/Azure)
- 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.

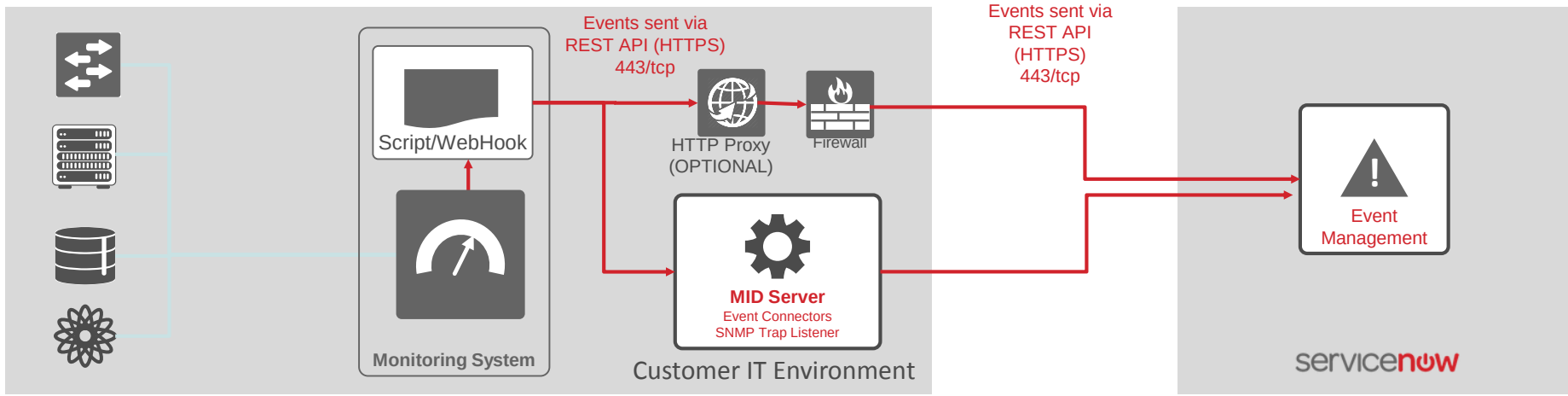
© 2017 ServiceNow All Rights Reserved

Integrating Events Using the REST API

Istanbul



NEW in Jakarta



© 2017 ServiceNow All Rights Reserved

Demo Use Cases

- Business service dashboard
  - View business service status
  - Impact analysis
  - Automatic action (open INT)
  - Remediation (open a change request and resolve problem)
- Noise Reduction
  - Receive alerts from multiple sources
  - Use alert grouping and alert correlation to identify key alerts
  - Define automation action on primary alerts
- Integrate with 3rd party source
  - Receive event from any 3rd party source
  - Use Event Rule designer to compose
- Triage service outage using service metrics
  - Use operational metrics data to triage alerts
  - Correlate metric to better understand probable cause
  - Identify probable cause using history and change view

© 2017 ServiceNow All Rights Reserved



Business Service Dashboard

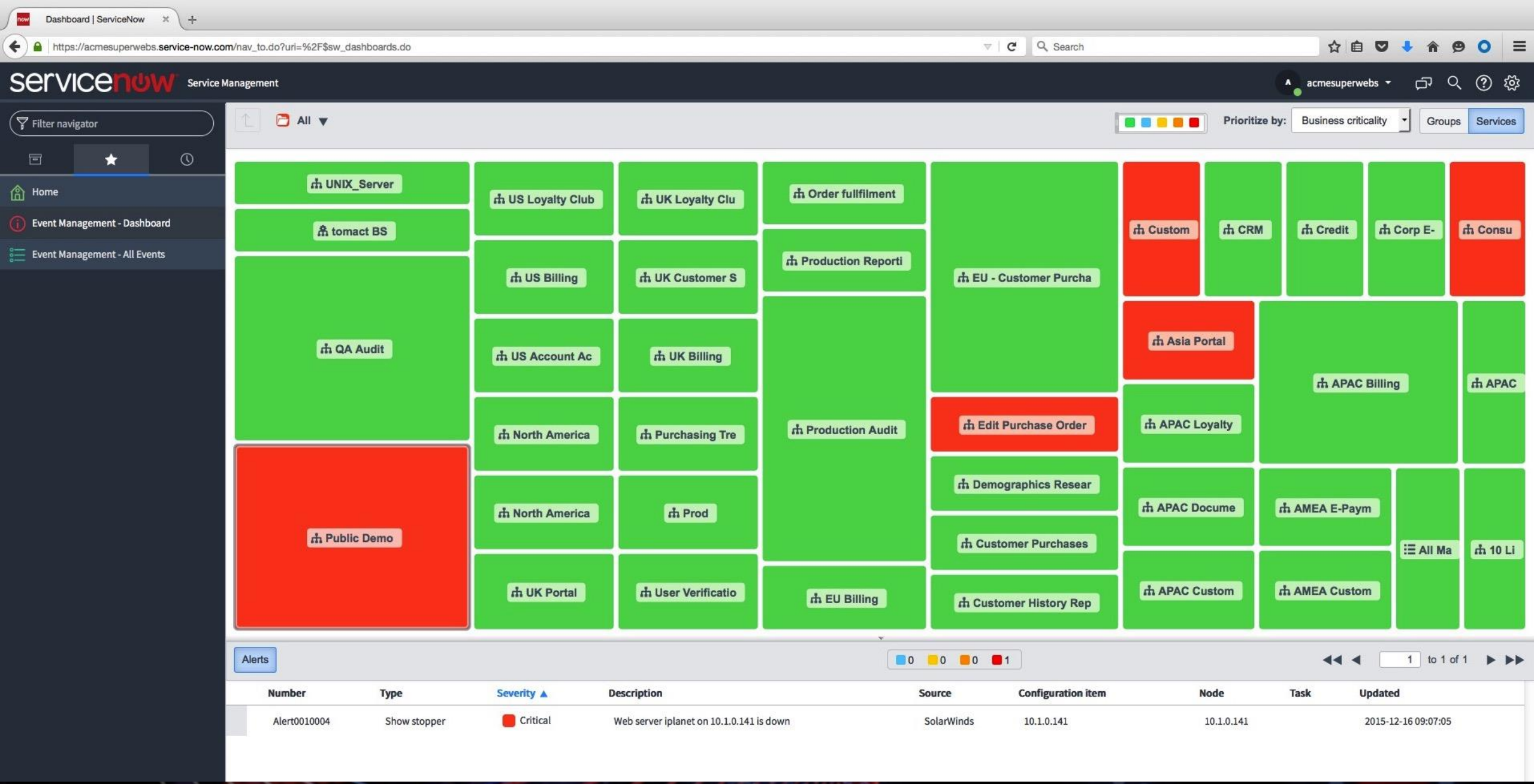
View business service status

Impact analysis

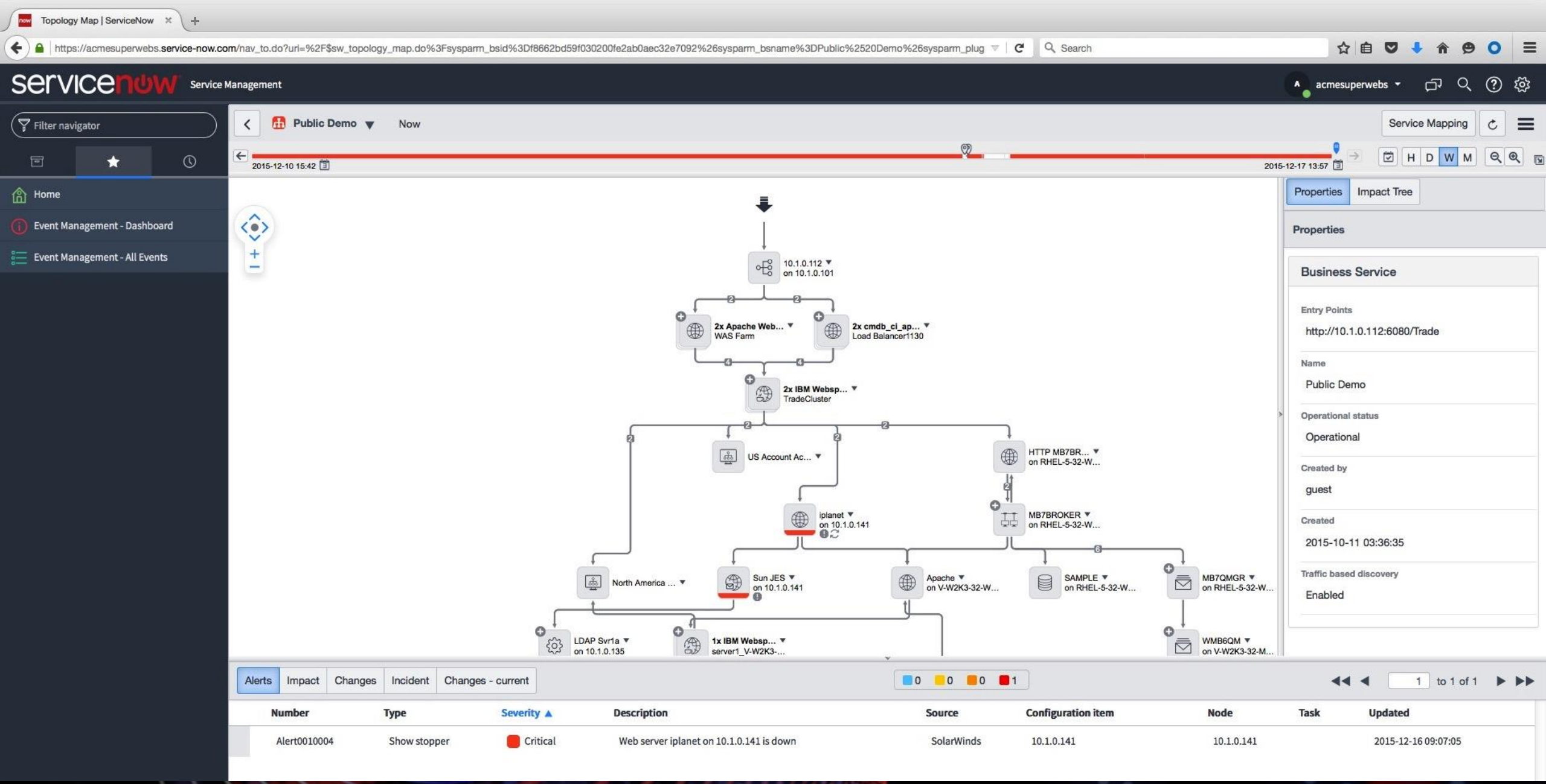
Automatic action (open INT)

Remediation (open a change request and resolve problem)

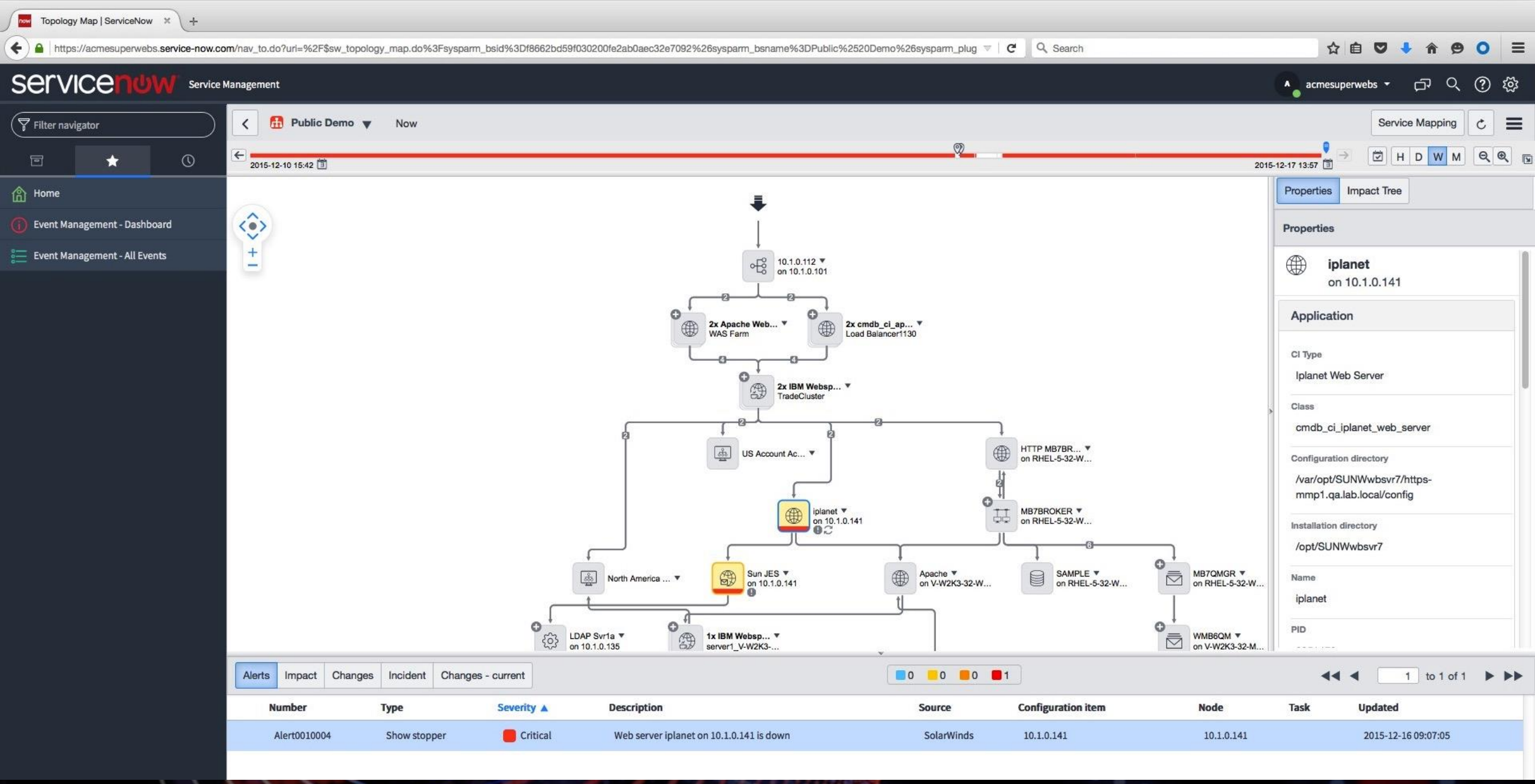
© 2017 ServiceNow All Rights Reserved



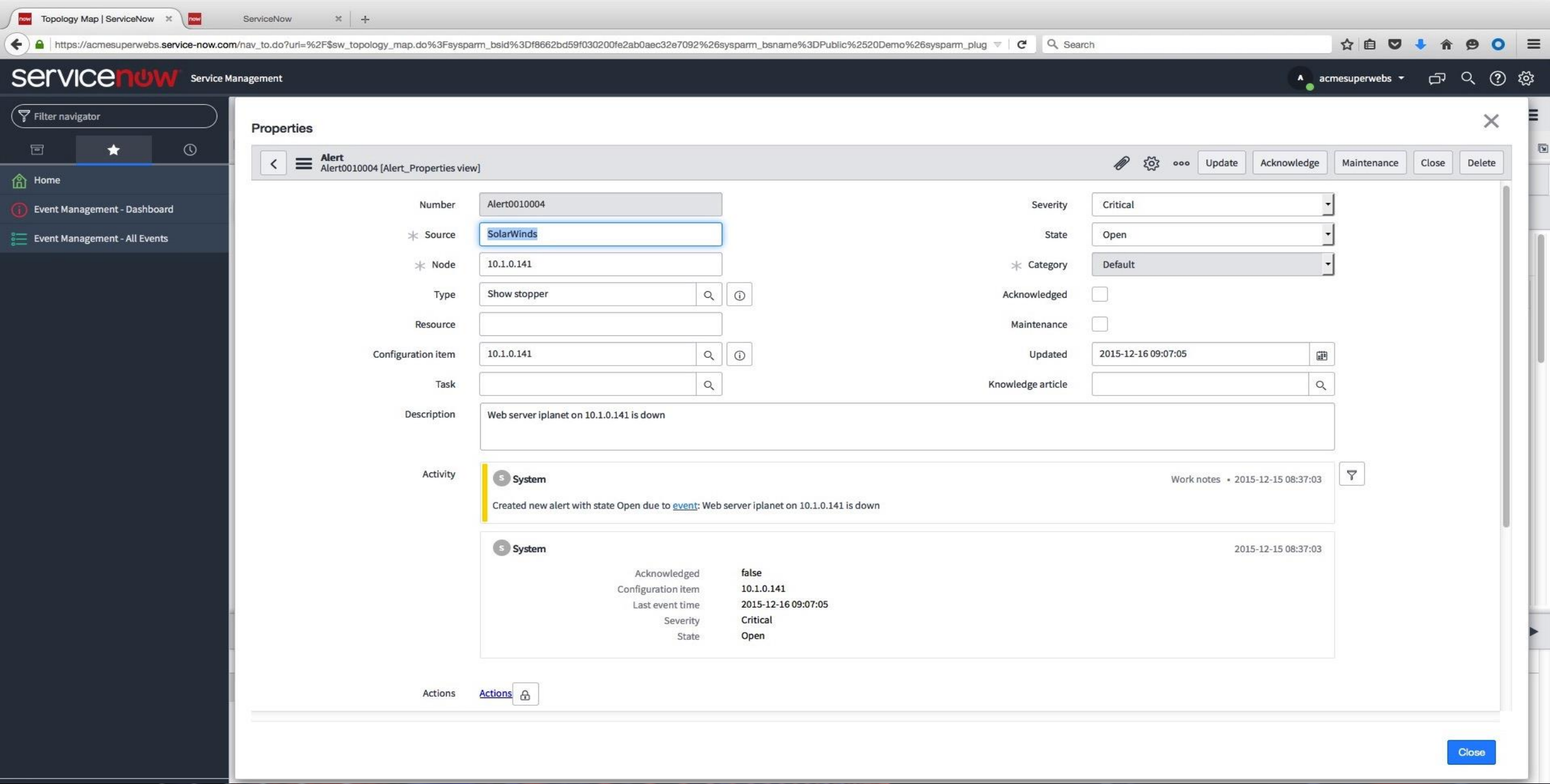
© 2017 ServiceNow All Rights Reserved



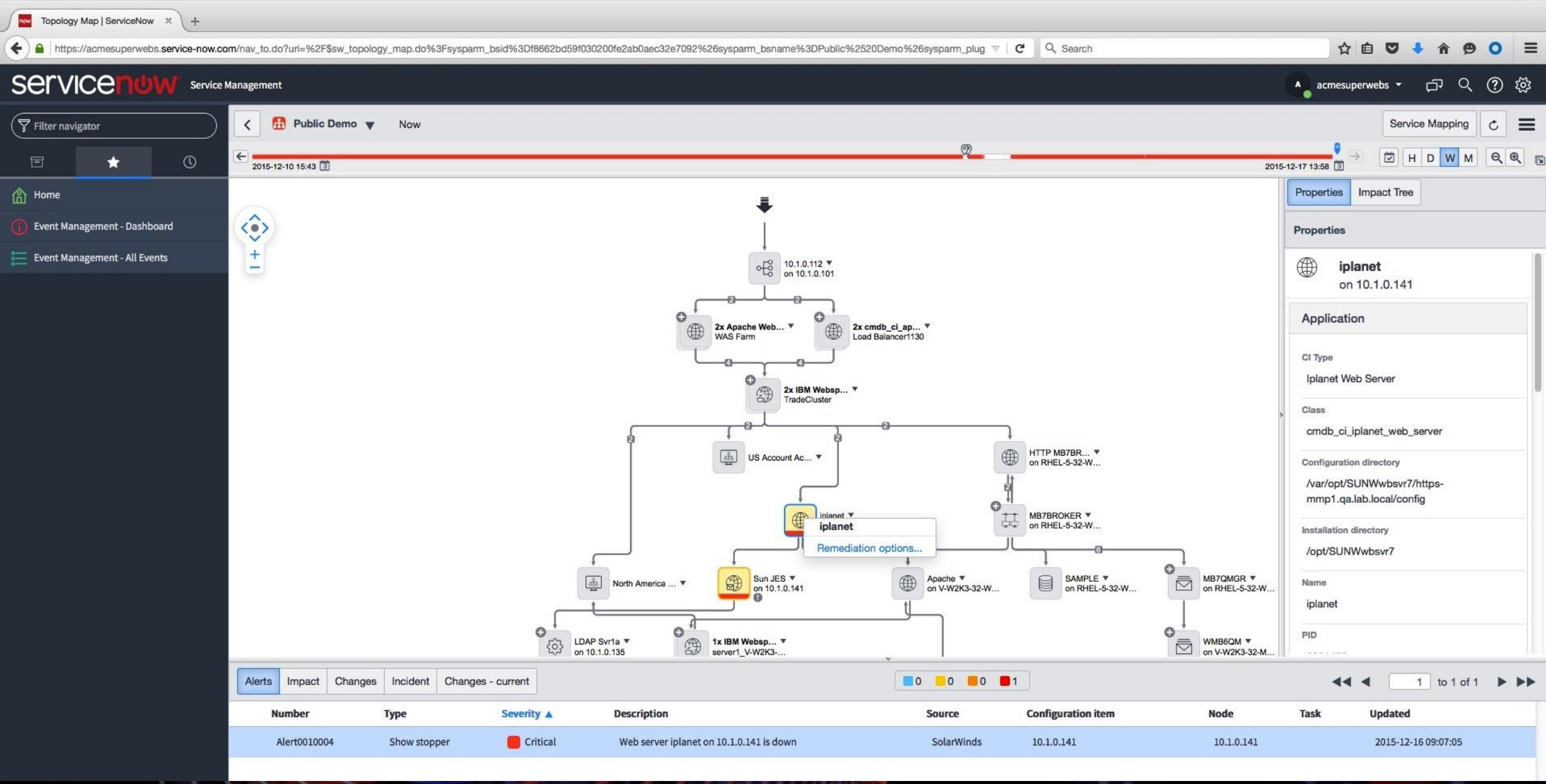
© 2017 ServiceNow All Rights Reserved



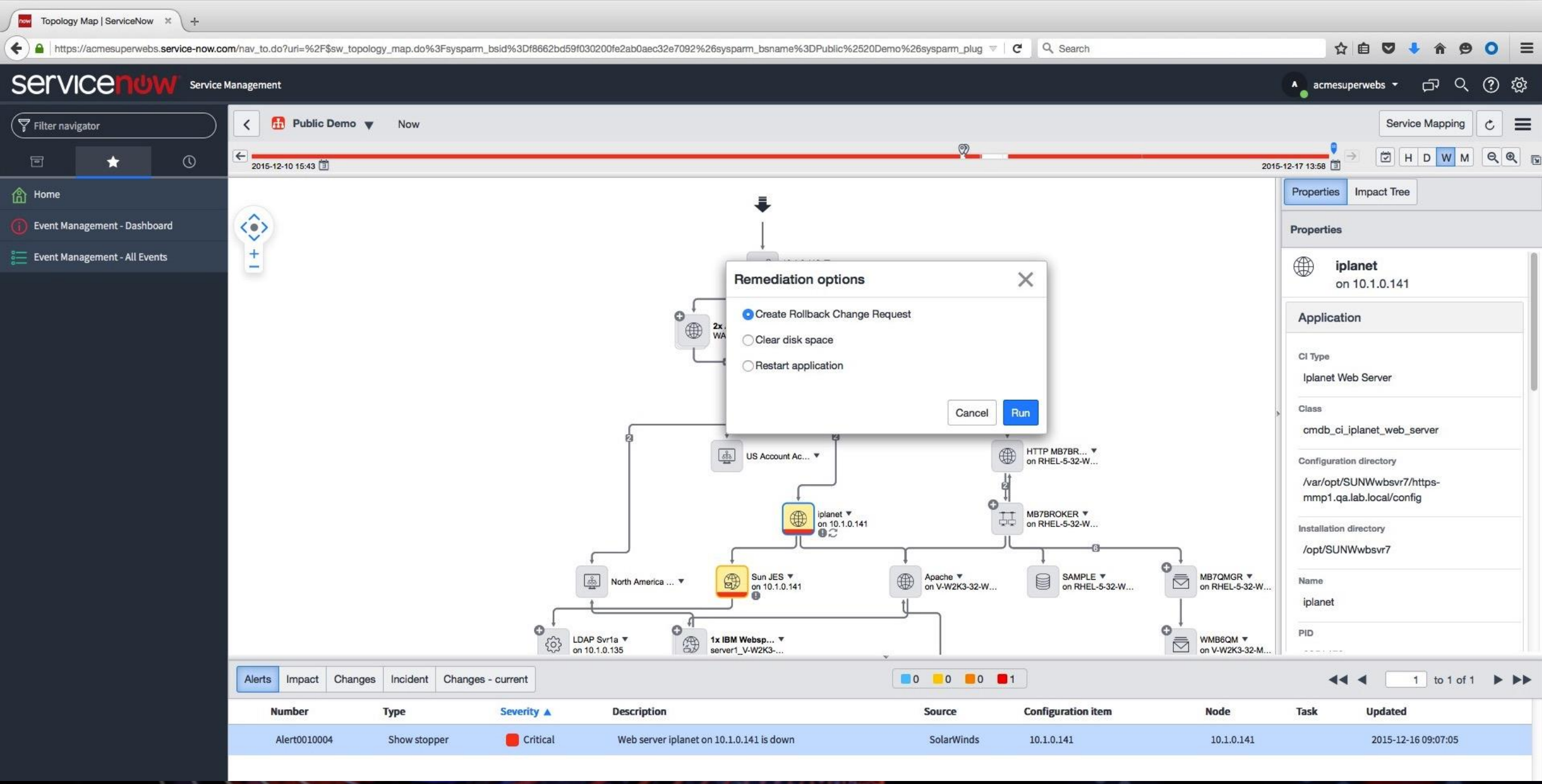
© 2017 ServiceNow All Rights Reserved



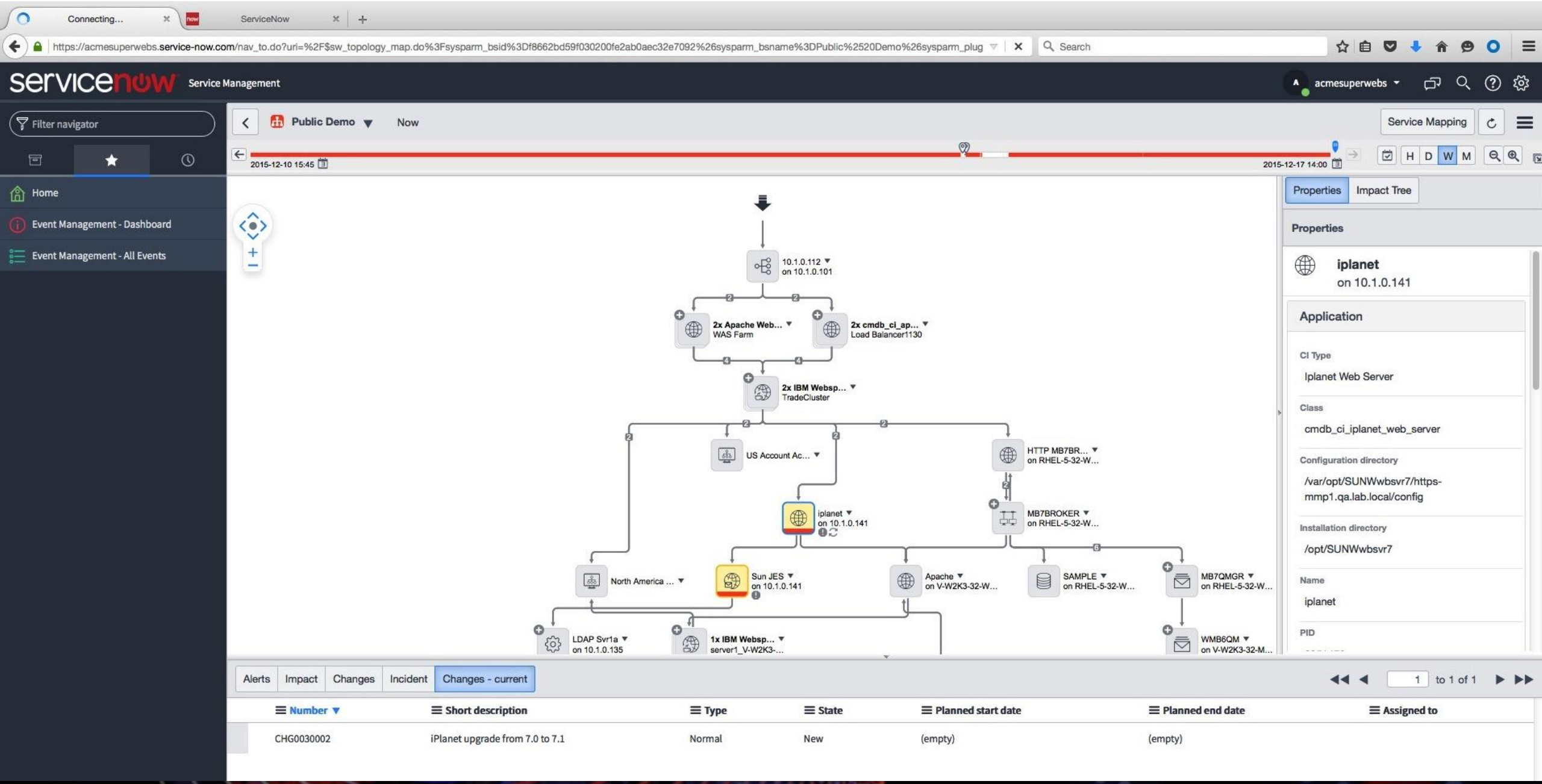
© 2017 ServiceNow All Rights Reserved



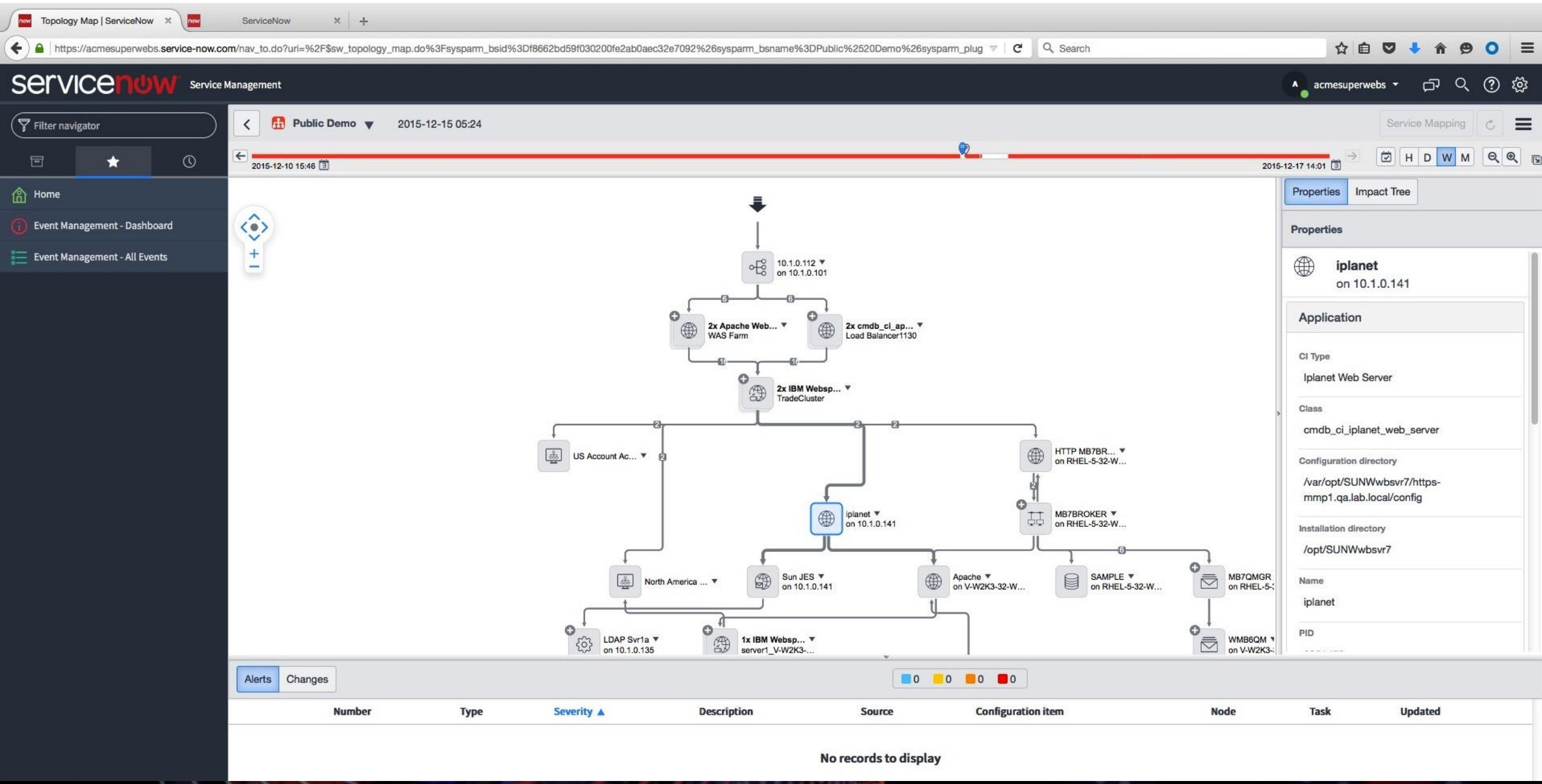
© 2017 ServiceNow All Rights Reserved



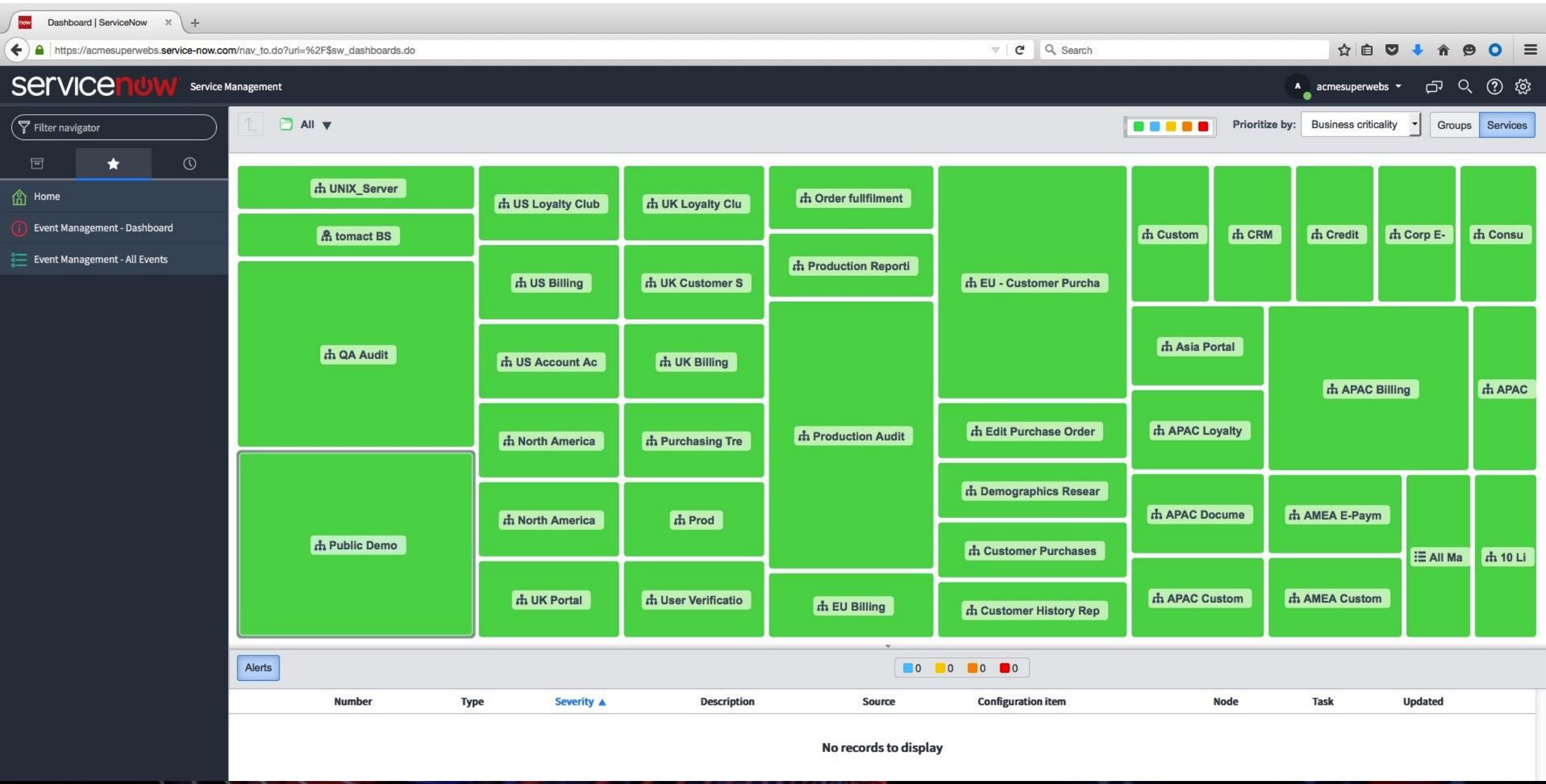
© 2017 ServiceNow All Rights Reserved



© 2017 ServiceNow All Rights Reserved



© 2017 ServiceNow All Rights Reserved



© 2017 ServiceNow All Rights Reserved



Noise Reduction

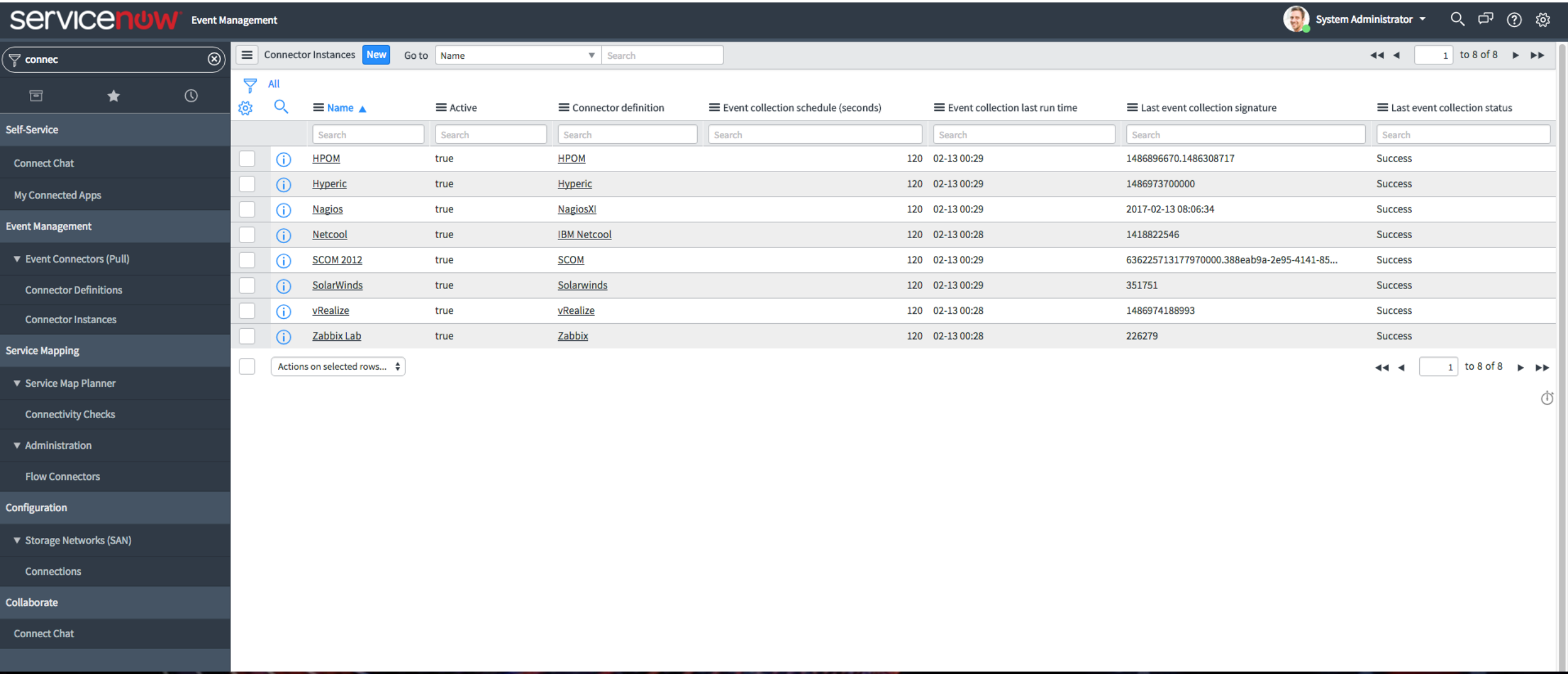
Receive alerts from multiple sources

Use alert grouping and alert correlation to identify key alerts

Define automation action on primary alerts

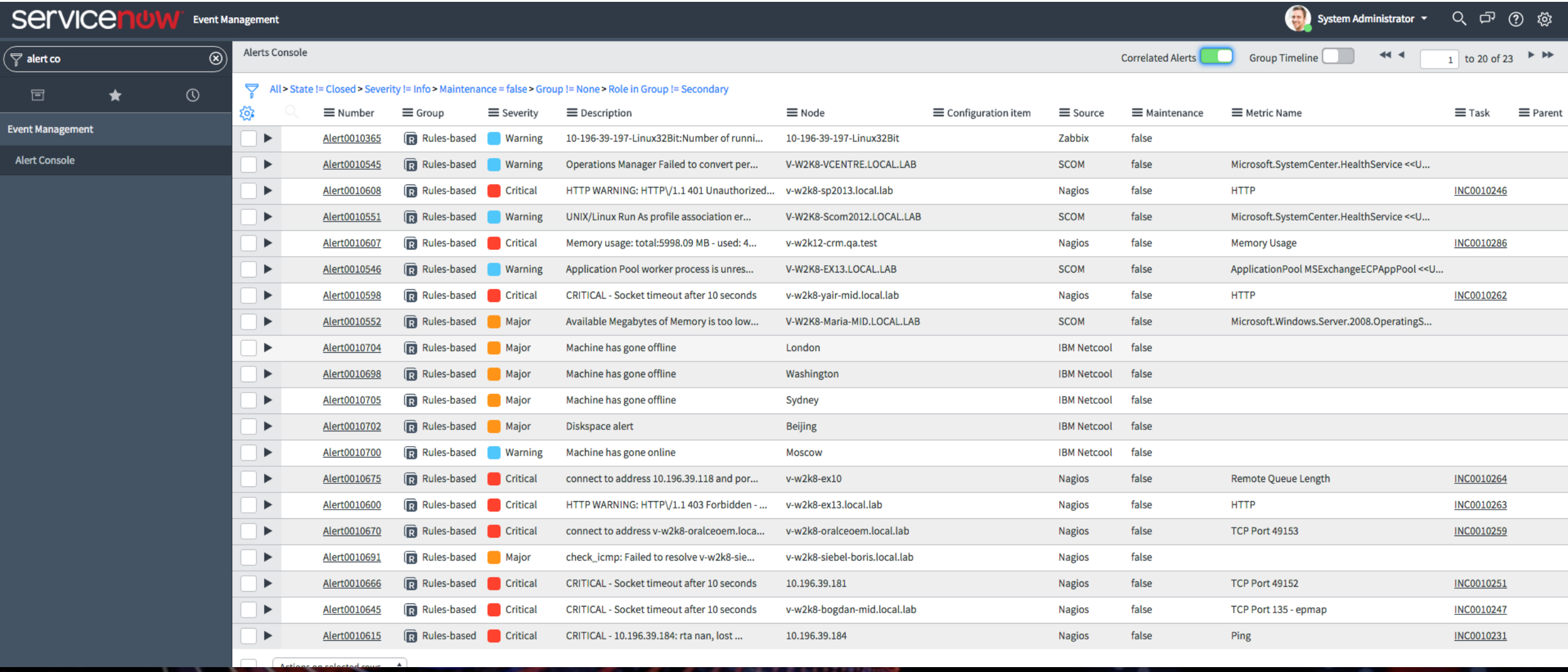
© 2017 ServiceNow All Rights Reserved

Define Multiple Sources



© 2017 ServiceNow All Rights Reserved

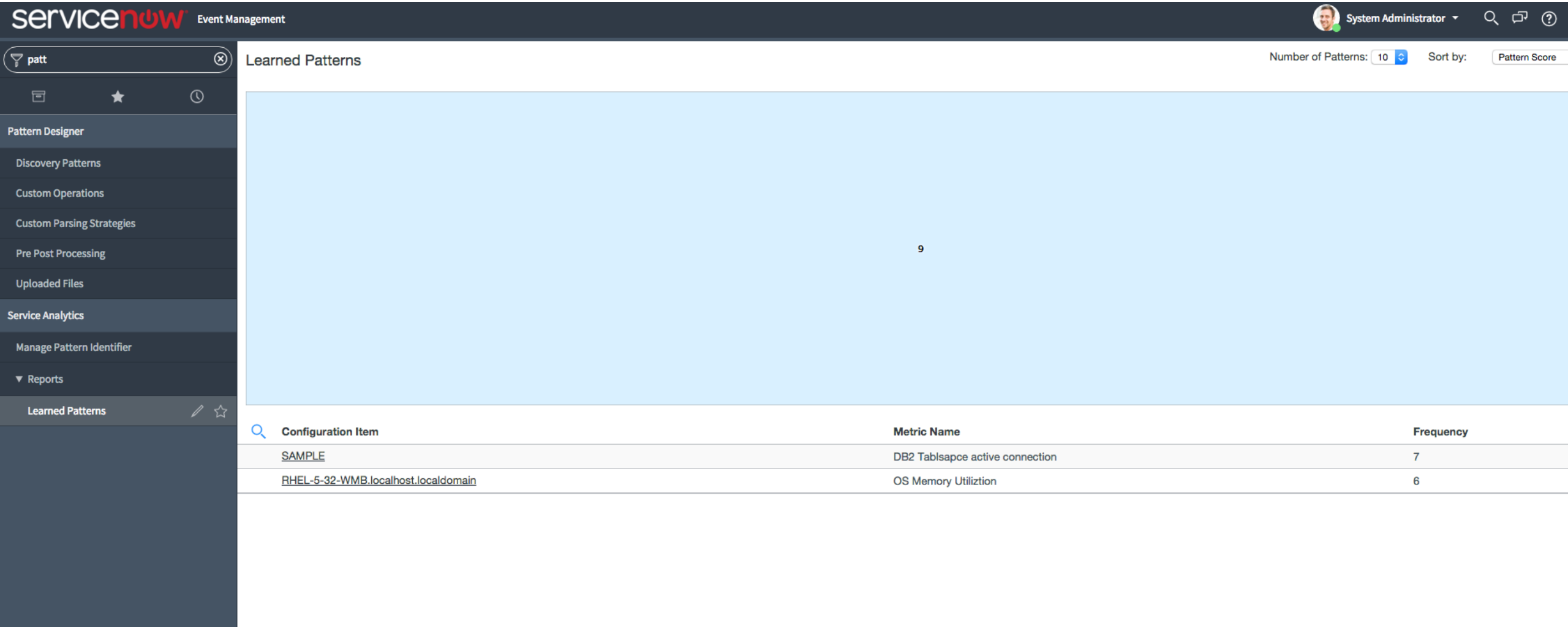
Receive Alerts from Multiple Sources



Number	Group	Severity	Description	Node	Configuration item	Source	Maintenance	Metric Name	Task	Parent
Alert0010365	Rules-based	Warning	10-196-39-197-Linux32Bit:Number of runni...	10-196-39-197-Linux32Bit		Zabbix	false			
Alert0010545	Rules-based	Warning	Operations Manager Failed to convert per...	V-W2K8-VCENTRE.LOCAL.LAB		SCOM	false	Microsoft.SystemCenter.HealthService <<U...		
Alert0010608	Rules-based	Critical	HTTP WARNING: HTTP\/1.1 401 Unauthorized...	v-w2k8-sp2013.local.lab		Nagios	false	HTTP	INC0010246	
Alert0010551	Rules-based	Warning	UNIX/Linux Run As profile association er...	V-W2K8-Scom2012.LOCAL.LAB		SCOM	false	Microsoft.SystemCenter.HealthService <<U...		
Alert0010607	Rules-based	Critical	Memory usage: total:5998.09 MB - used: 4...	v-w2k12-crm.qa.test		Nagios	false	Memory Usage	INC0010286	
Alert0010546	Rules-based	Warning	Application Pool worker process is unres...	V-W2K8-EX13.LOCAL.LAB		SCOM	false	ApplicationPool MSExchangeECPAppPool <<U...		
Alert0010598	Rules-based	Critical	CRITICAL - Socket timeout after 10 seconds	v-w2k8-yair-mid.local.lab		Nagios	false	HTTP	INC0010262	
Alert0010552	Rules-based	Major	Available Megabytes of Memory is too low...	V-W2K8-Maria-MID.LOCAL.LAB		SCOM	false	Microsoft.Windows.Server.2008.OperatingS...		
Alert0010704	Rules-based	Major	Machine has gone offline	London		IBM Netcool	false			
Alert0010698	Rules-based	Major	Machine has gone offline	Washington		IBM Netcool	false			
Alert0010705	Rules-based	Major	Machine has gone offline	Sydney		IBM Netcool	false			
Alert0010702	Rules-based	Major	Diskspace alert	Beijing		IBM Netcool	false			
Alert0010700	Rules-based	Warning	Machine has gone online	Moscow		IBM Netcool	false			
Alert0010675	Rules-based	Critical	connect to address 10.196.39.118 and por...	v-w2k8-ex10		Nagios	false	Remote Queue Length	INC0010264	
Alert0010600	Rules-based	Critical	HTTP WARNING: HTTP\/1.1 403 Forbidden - ...	v-w2k8-ex13.local.lab		Nagios	false	HTTP	INC0010263	
Alert0010670	Rules-based	Critical	connect to address v-w2k8-oralceoem.loca...	v-w2k8-oralceoem.local.lab		Nagios	false	TCP Port 49153	INC0010259	
Alert0010691	Rules-based	Major	check_icmp: Failed to resolve v-w2k8-sie...	v-w2k8-siebel-boris.local.lab		Nagios	false			
Alert0010666	Rules-based	Critical	CRITICAL - Socket timeout after 10 seconds	10.196.39.181		Nagios	false	TCP Port 49152	INC0010251	
Alert0010645	Rules-based	Critical	CRITICAL - Socket timeout after 10 seconds	v-w2k8-bogdan-mid.local.lab		Nagios	false	TCP Port 135 - epmap	INC0010247	
Alert0010615	Rules-based	Critical	CRITICAL - 10.196.39.184: rta nan, lost ...	10.196.39.184		Nagios	false	Ping	INC0010231	

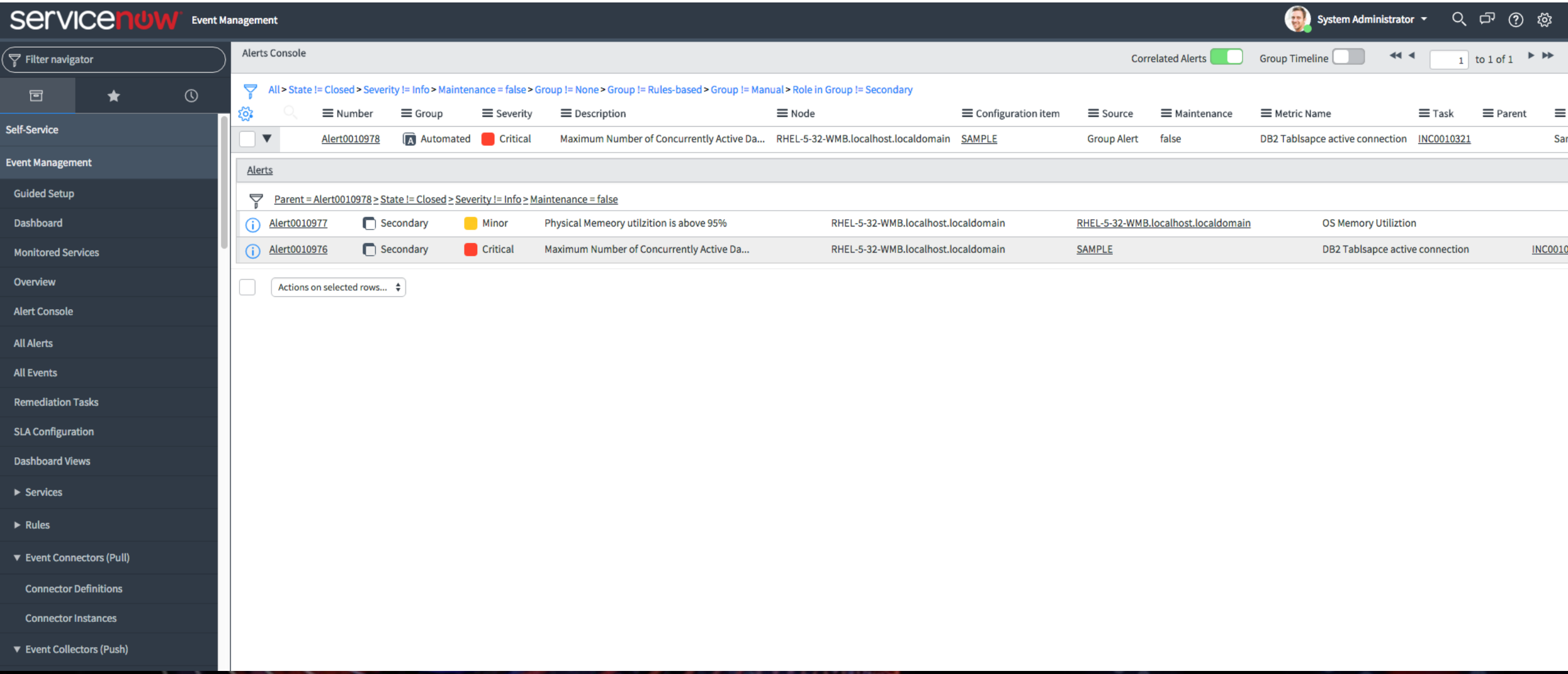
© 2017 ServiceNow All Rights Reserved

Automatic Alert Grouping – Machine Learning patterns



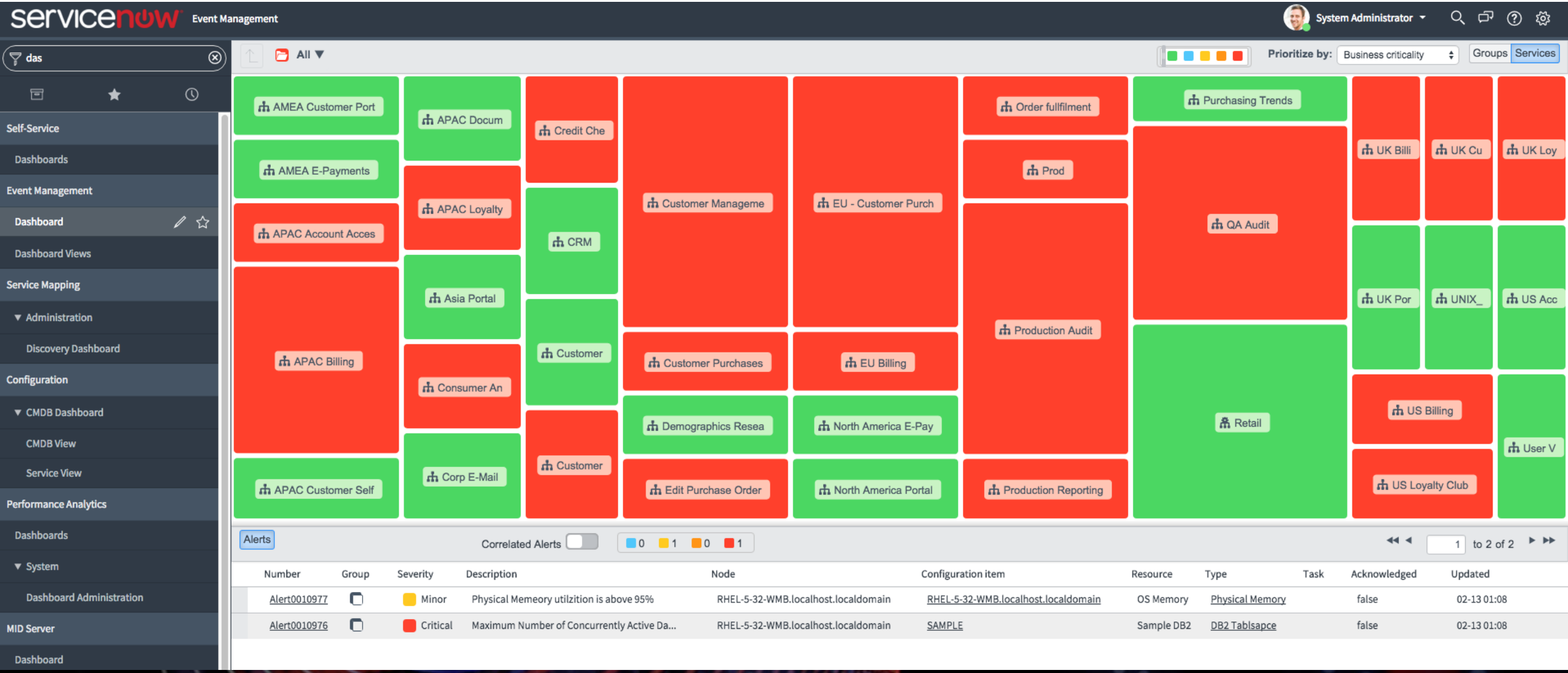
© 2017 ServiceNow All Rights Reserved

[Alert Console] Automatic Alert Grouping – Machine Learning



© 2017 ServiceNow All Rights Reserved

[Dashboard] Automatic Alert Grouping – Machine Learning



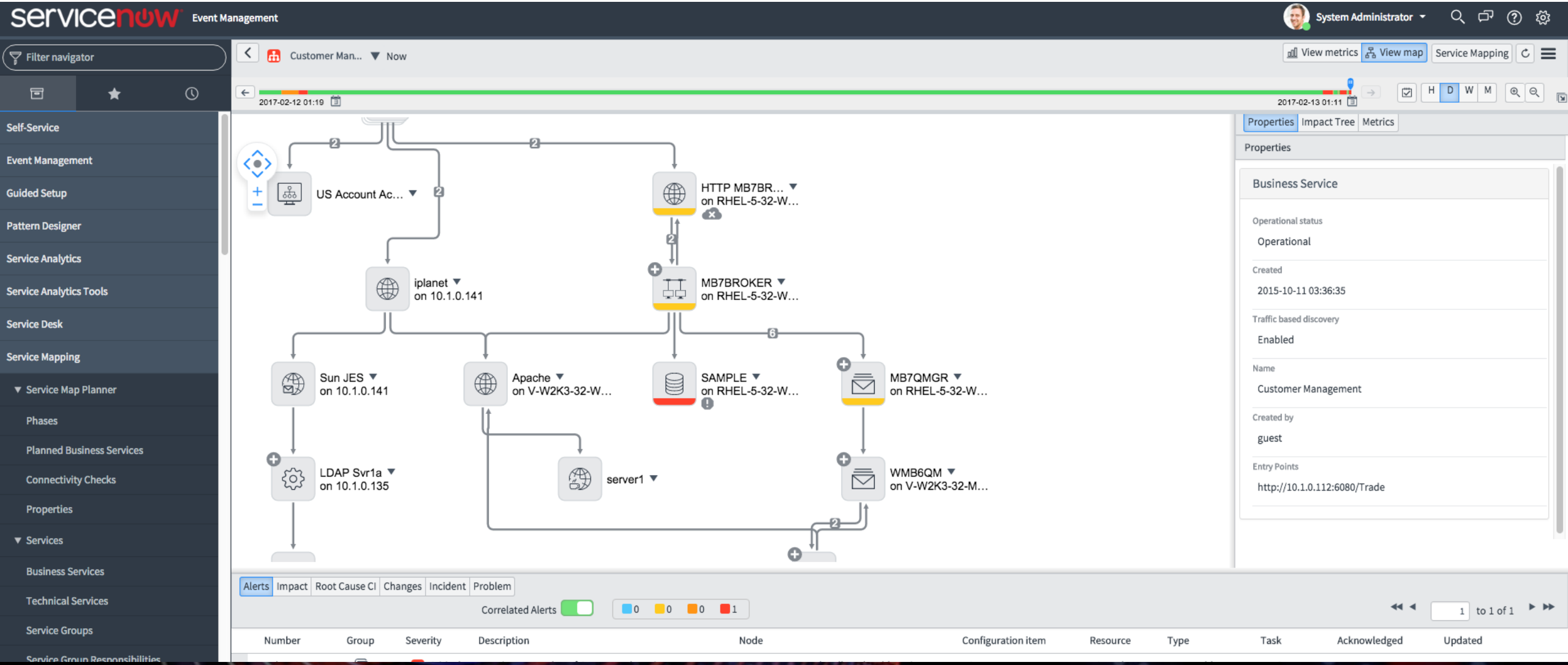
© 2017 ServiceNow All Rights Reserved

[Dashboard] Automatic Alert Grouping – Machine Learning



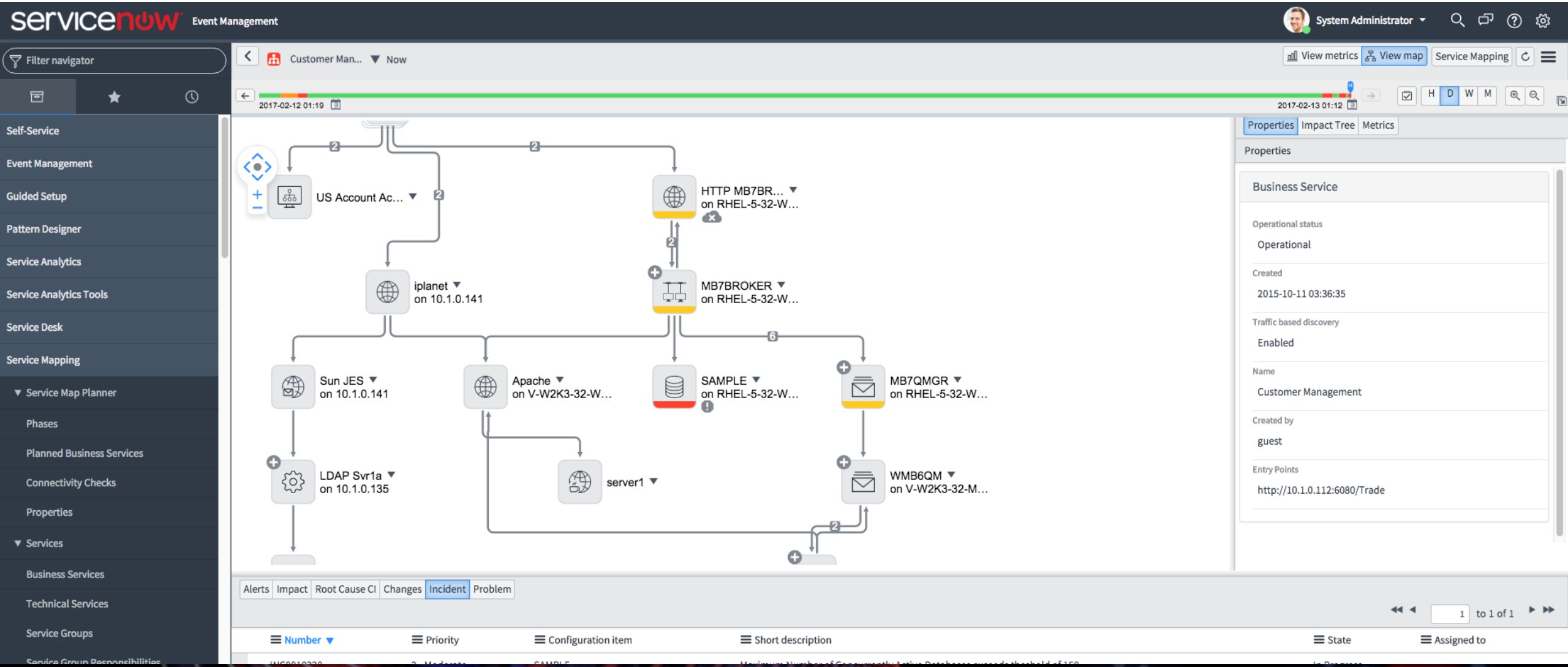
© 2017 ServiceNow All Rights Reserved

[Dashboard] Automatic Alert Grouping – Machine Learning



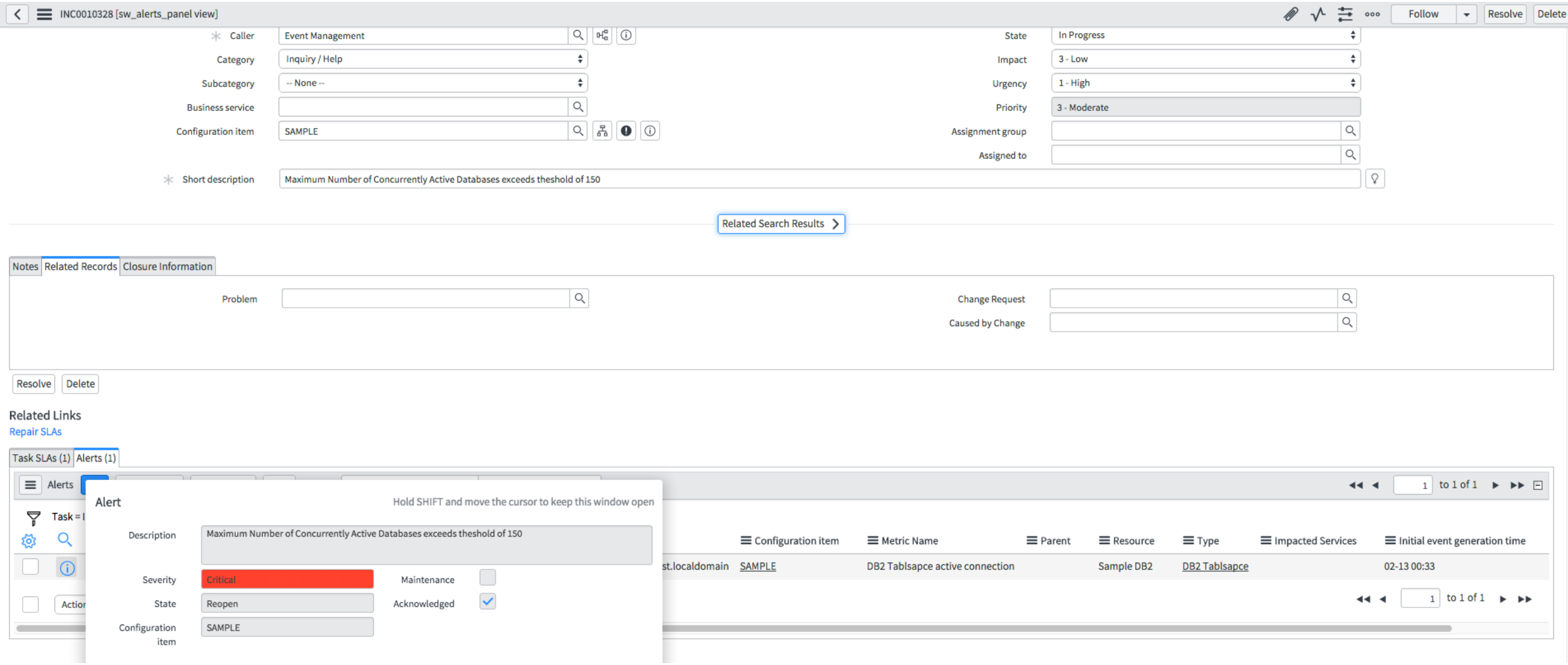
© 2017 ServiceNow All Rights Reserved

Define Automation Action on Primary Alerts



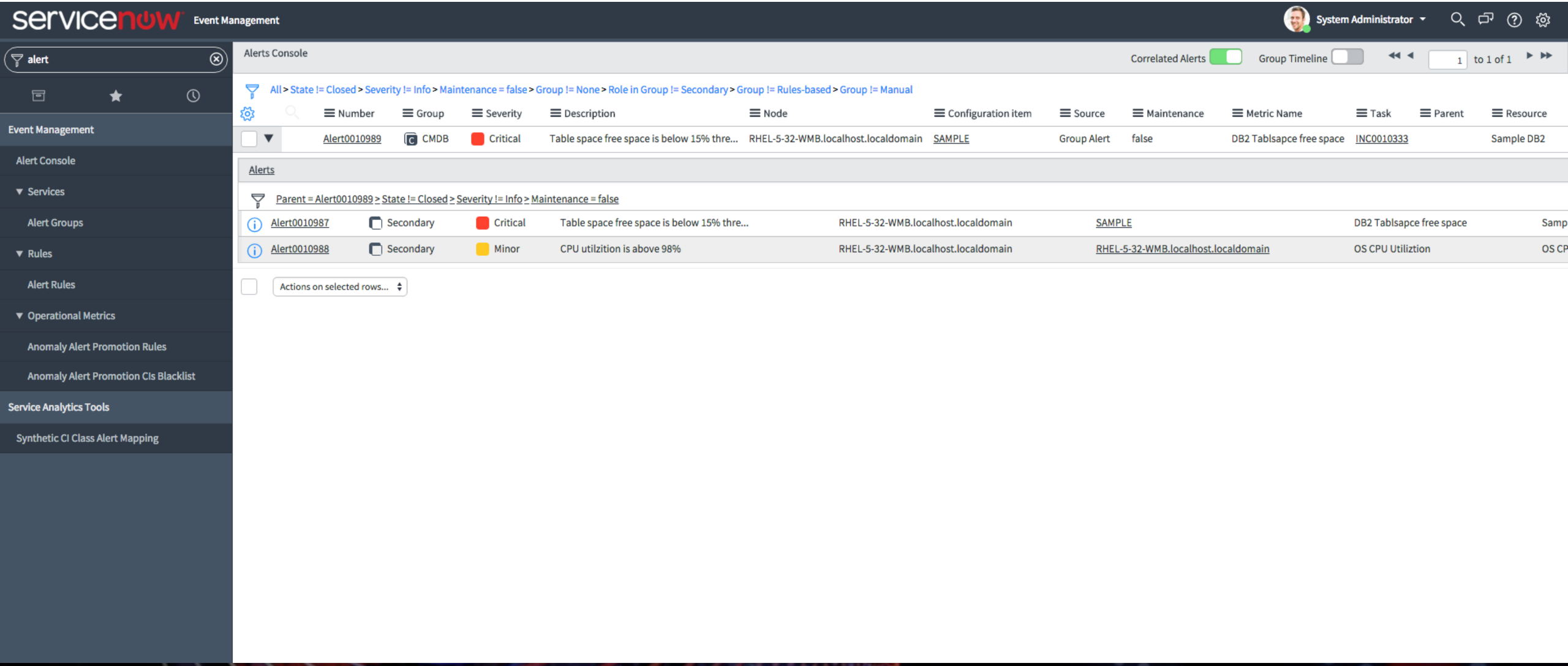
© 2017 ServiceNow All Rights Reserved

Define Automation Action on Primary Alerts



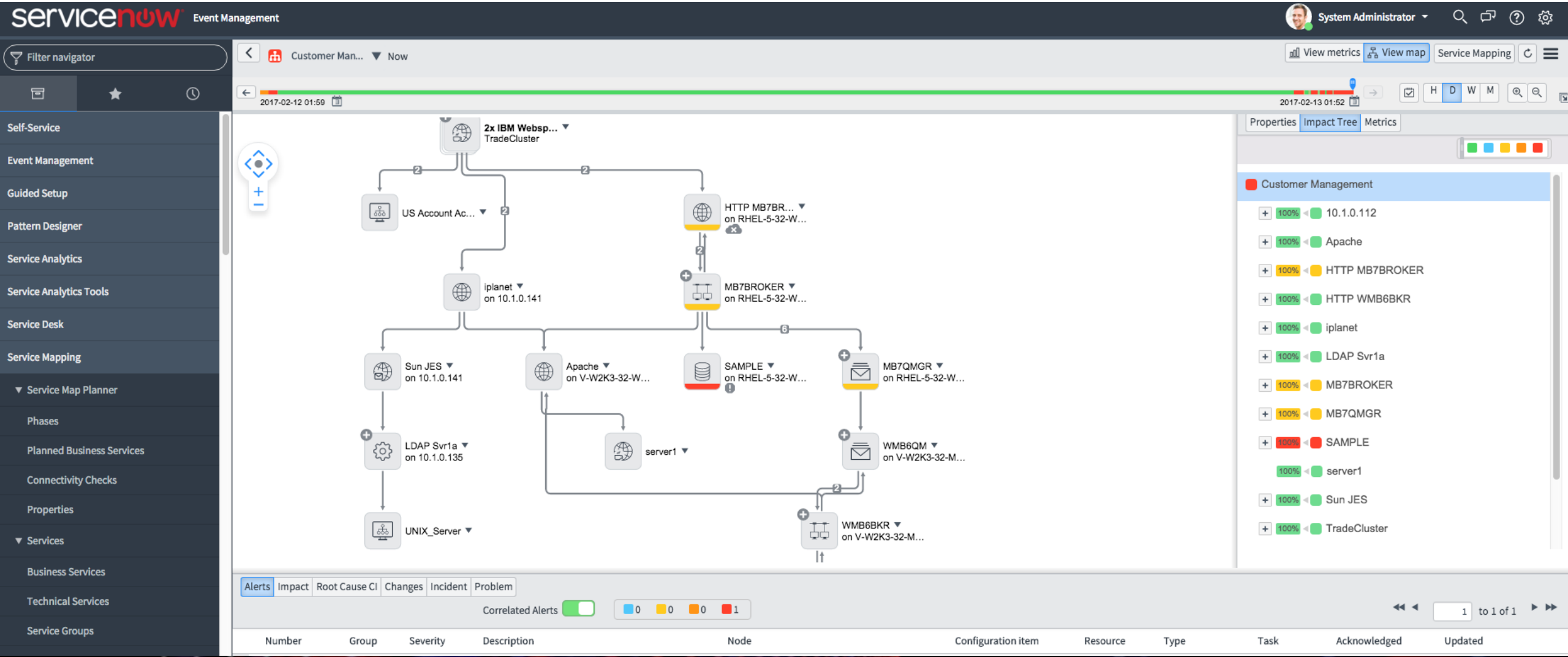
© 2017 ServiceNow All Rights Reserved

[Alert Console] Automatic Alert Grouping – CMDB



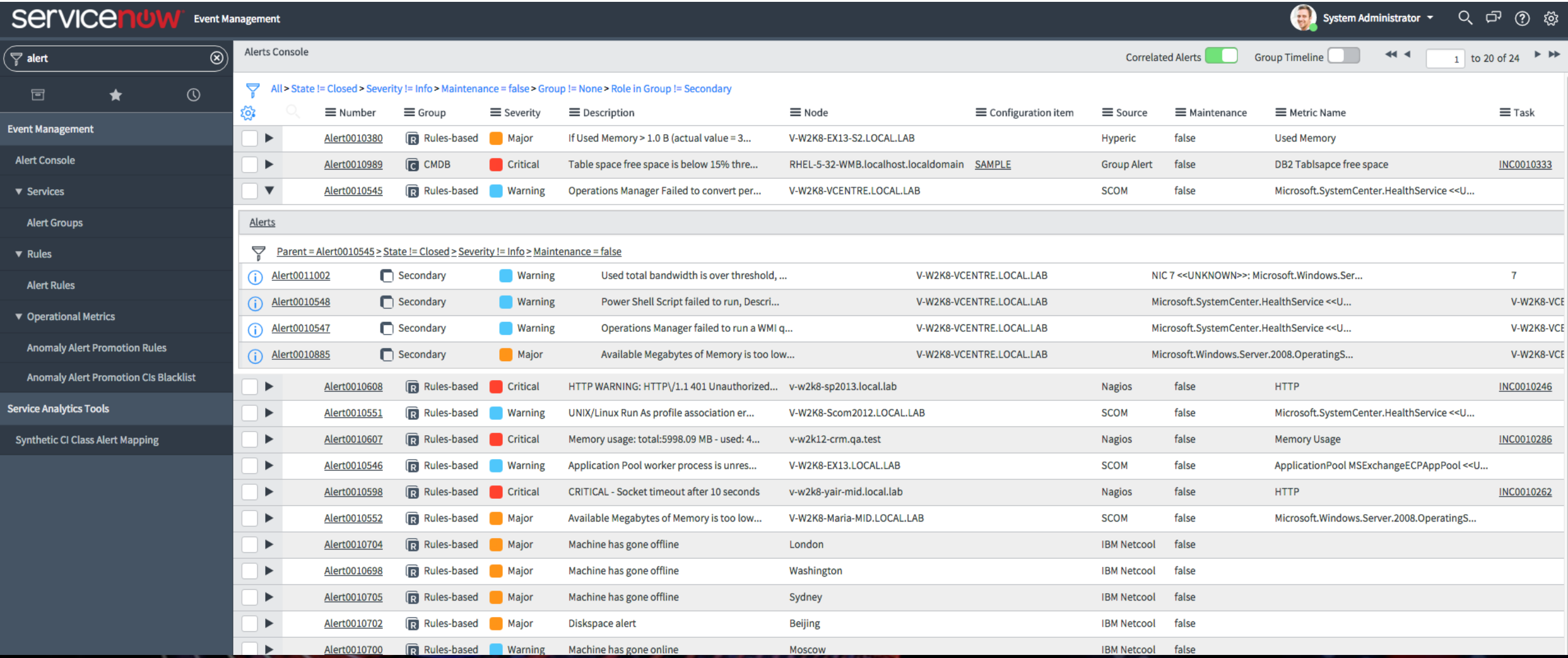
© 2017 ServiceNow All Rights Reserved

[Dashboard] Automatic Alert Grouping – CMDB Based



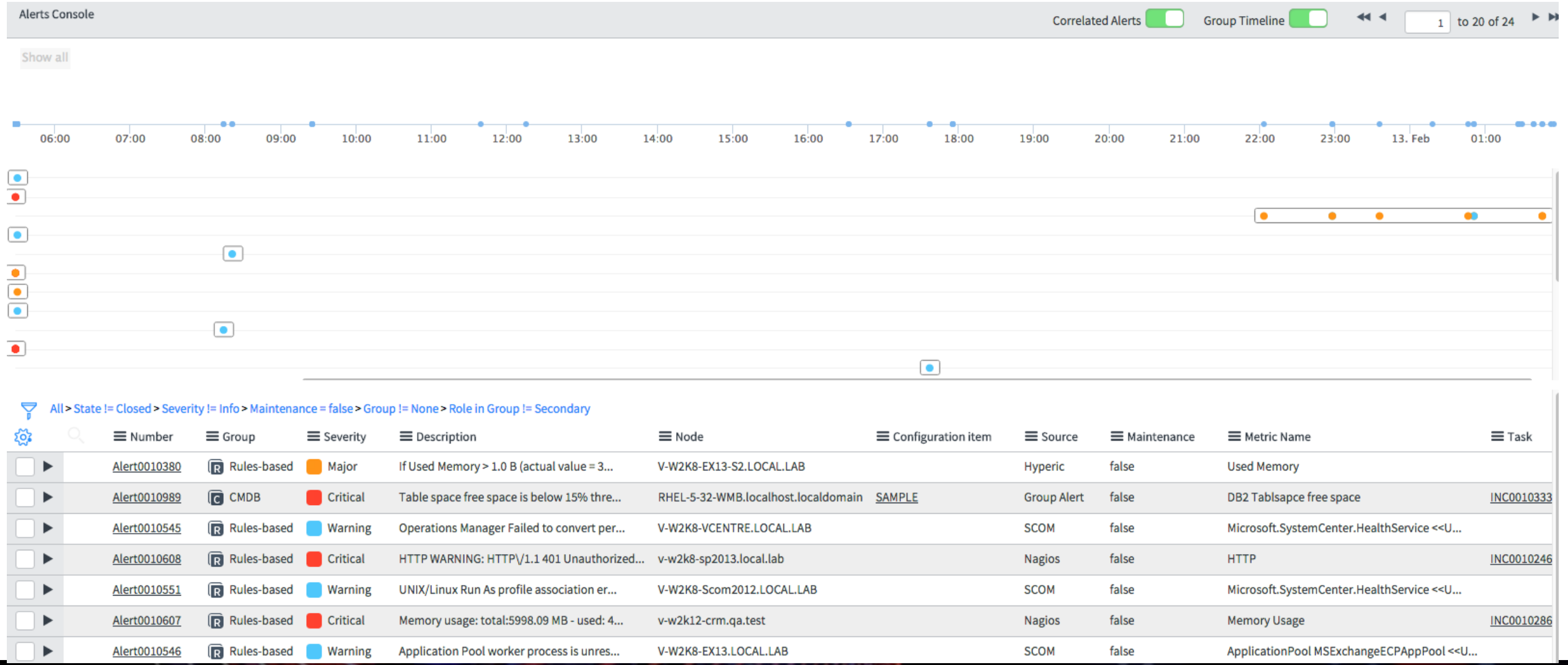
© 2017 ServiceNow All Rights Reserved

Automatic Alert Grouping – Rule Based



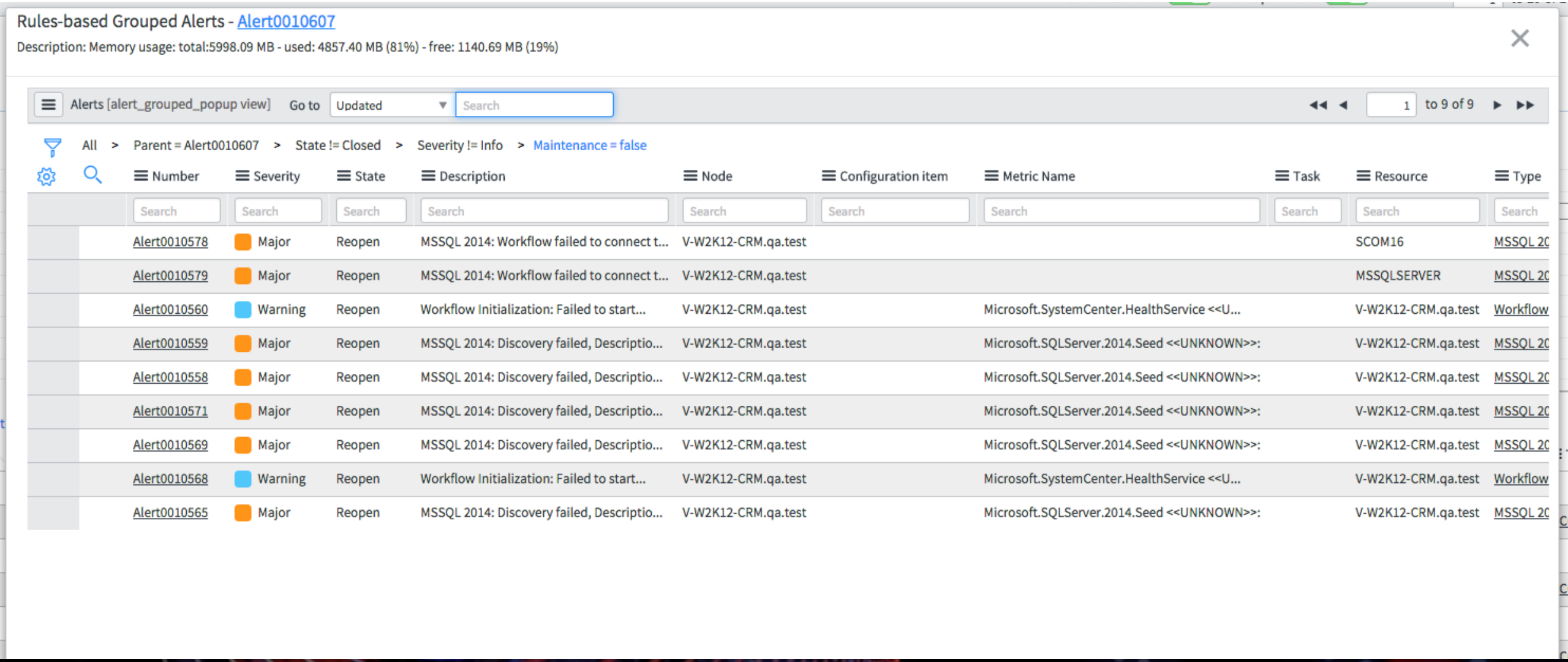
© 2017 ServiceNow All Rights Reserved

Automatic Alert Grouping – Visual Group timeline



© 2017 ServiceNow All Rights Reserved

Automatic Alert Grouping – Drill Down to Group Members



© 2017 ServiceNow All Rights Reserved



Integrate with 3rd Party Source

Receive event from any 3rd party source

Use Event Rule designer to compose

© 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

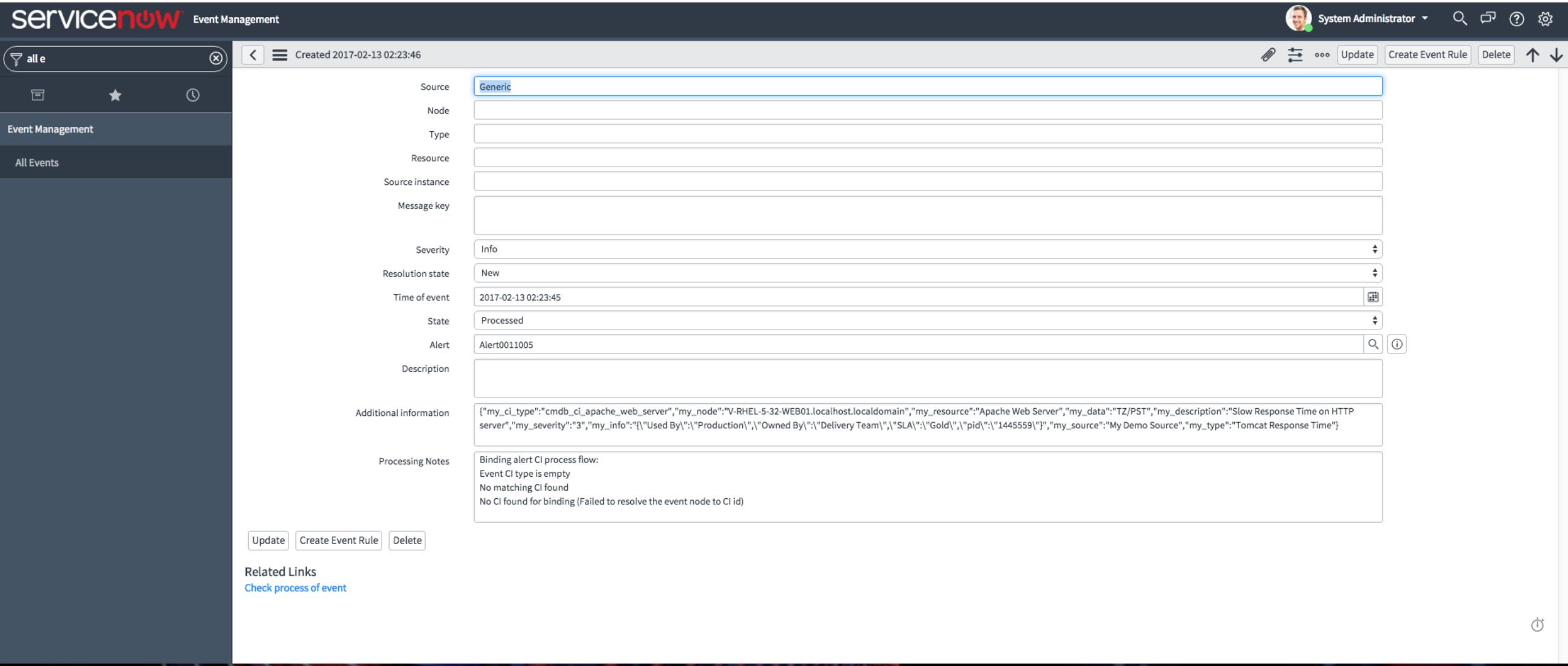
form-data | x-www-form-urlencoded | raw | binary | JSON (application/json)

```
{
    "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"

}
```

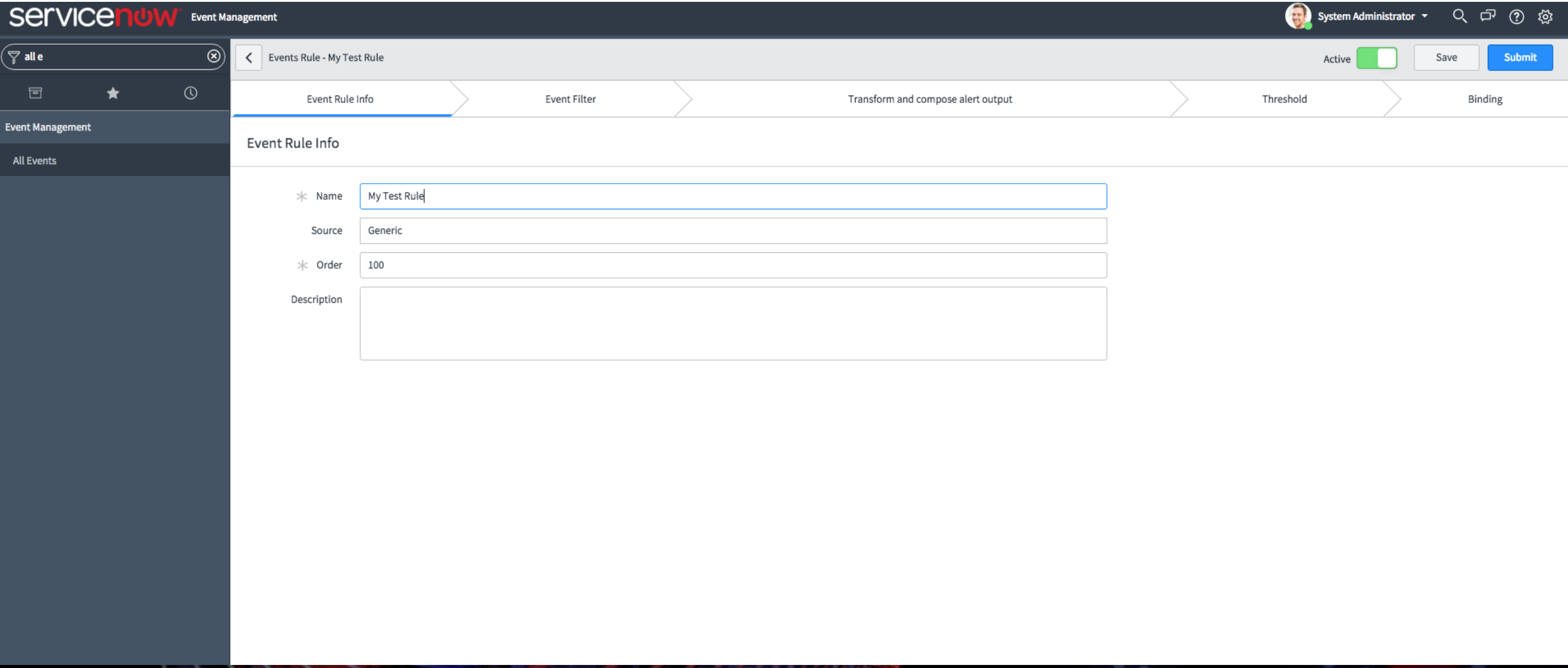

© 2017 ServiceNow All Rights Reserved

Custom Event can be Easily Captured and Transformed



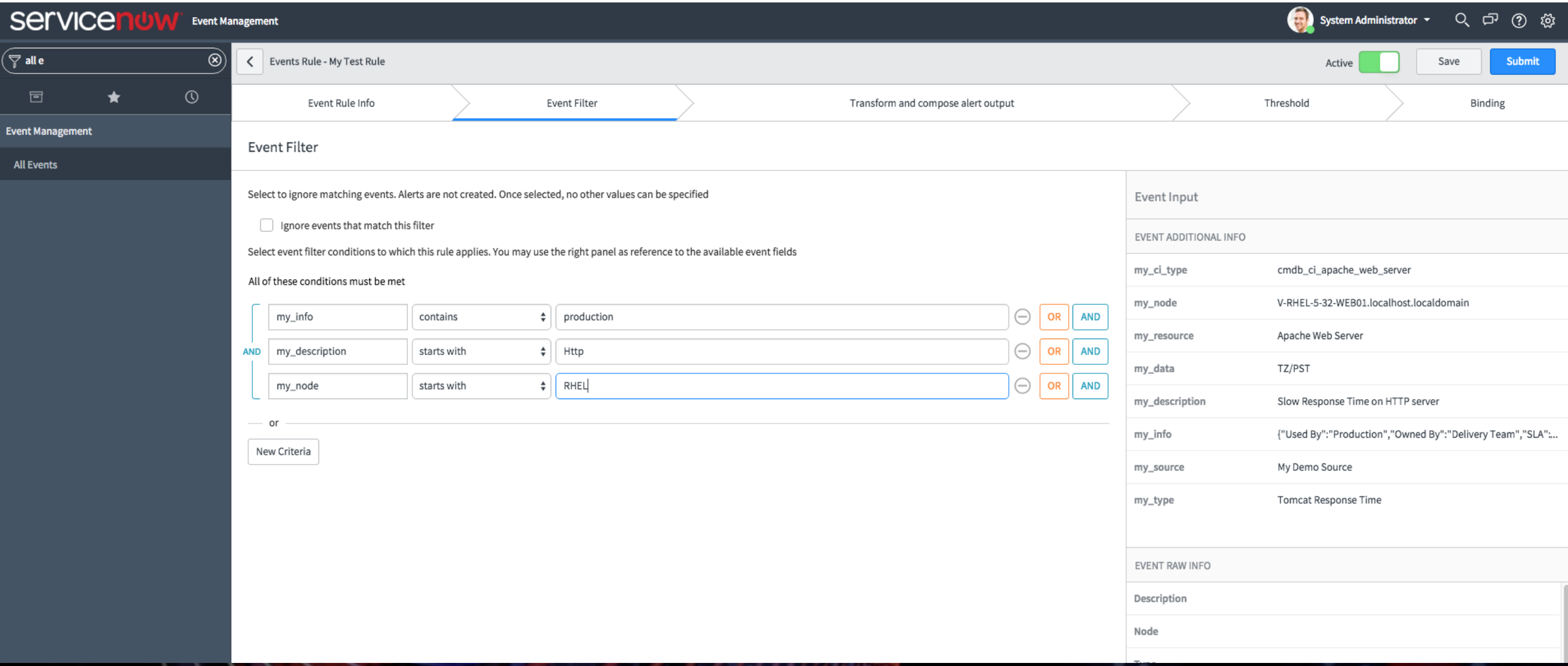
© 2017 ServiceNow All Rights Reserved

Use the Event Rule Designer to Compose New Alert



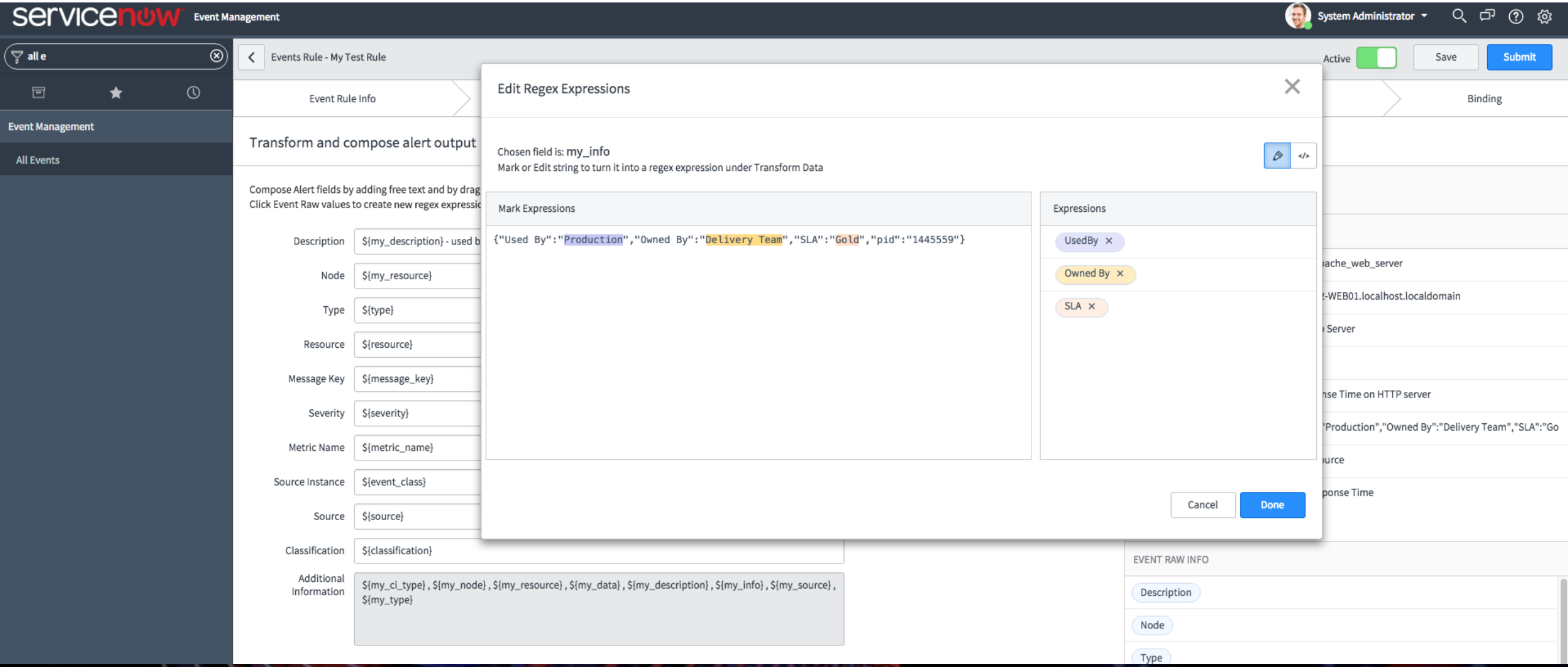
© 2017 ServiceNow All Rights Reserved

Use the Event Rule Designer to Compose New Alert - Filter



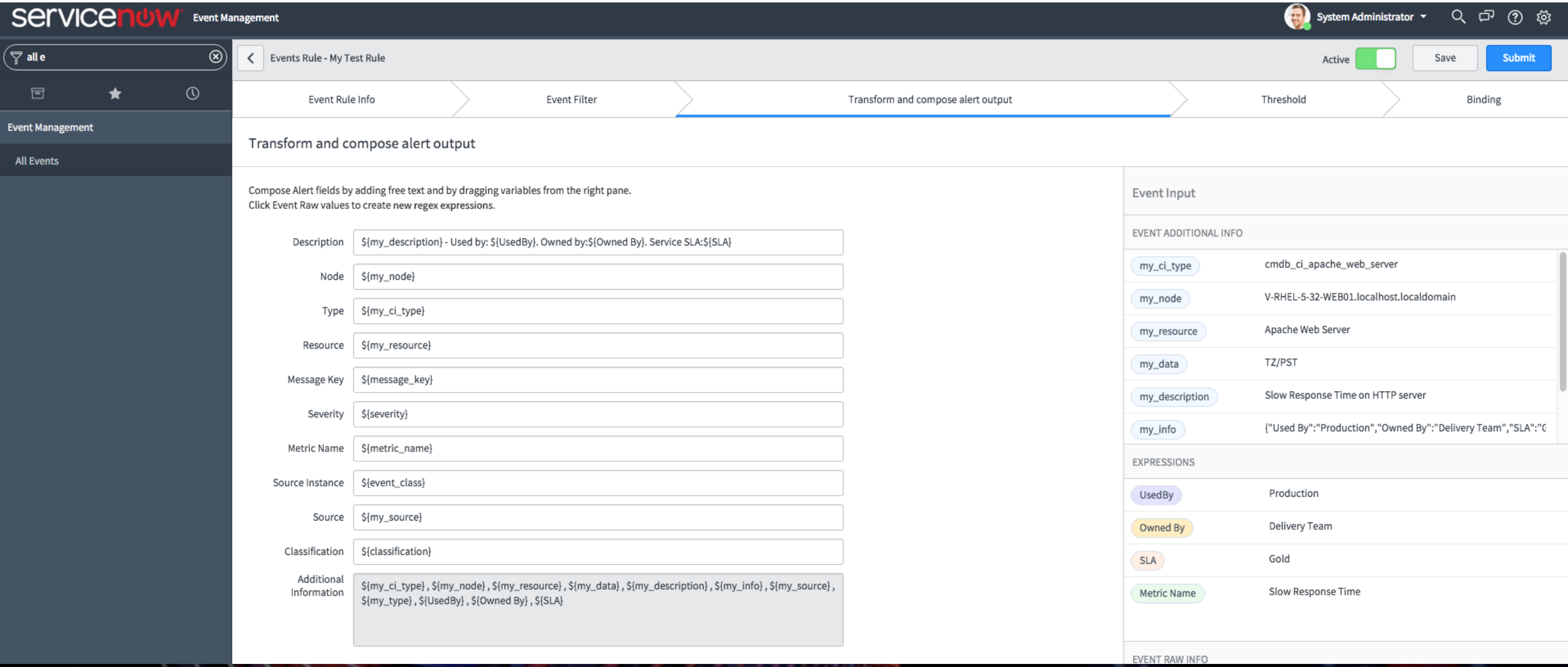
© 2017 ServiceNow All Rights Reserved

Use the Event Rule Designer to Compose New Alert - Transform



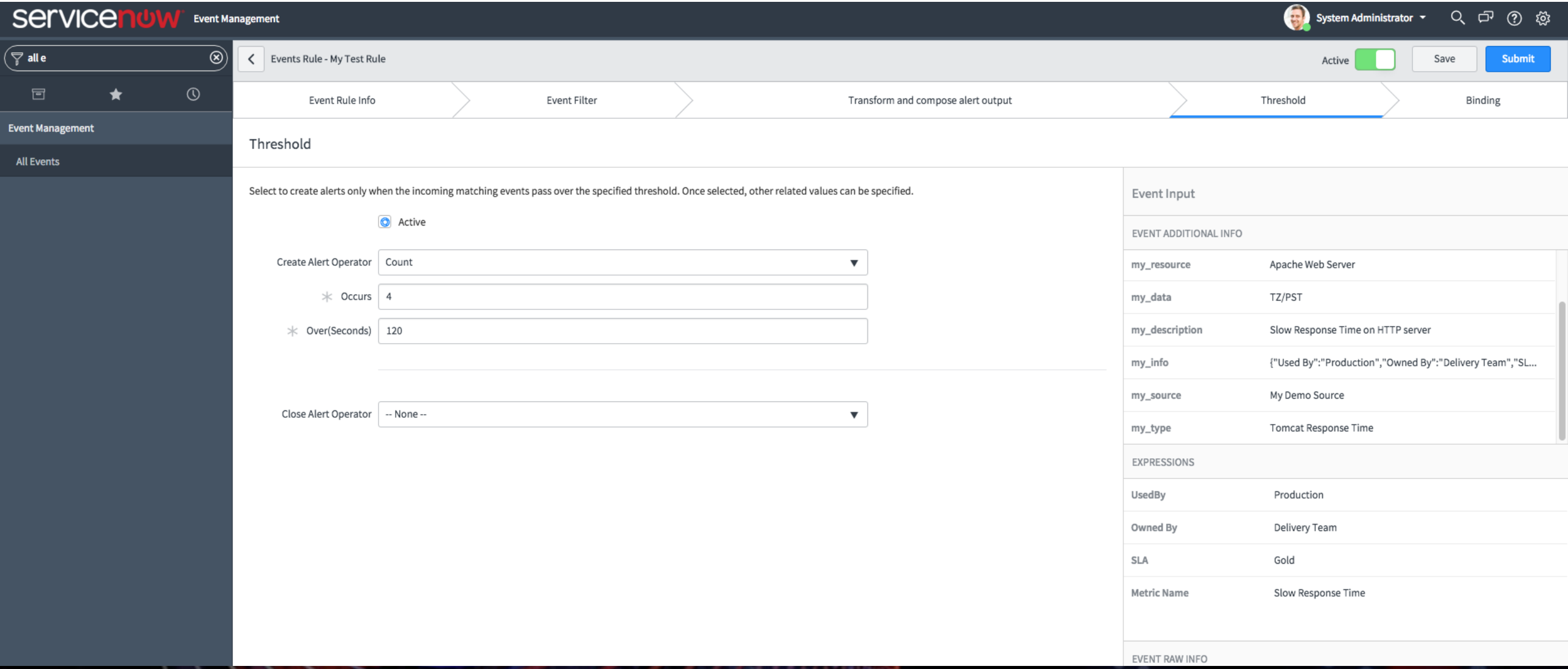
© 2017 ServiceNow All Rights Reserved

Use the Event Rule Designer to Compose New Alert - Transform



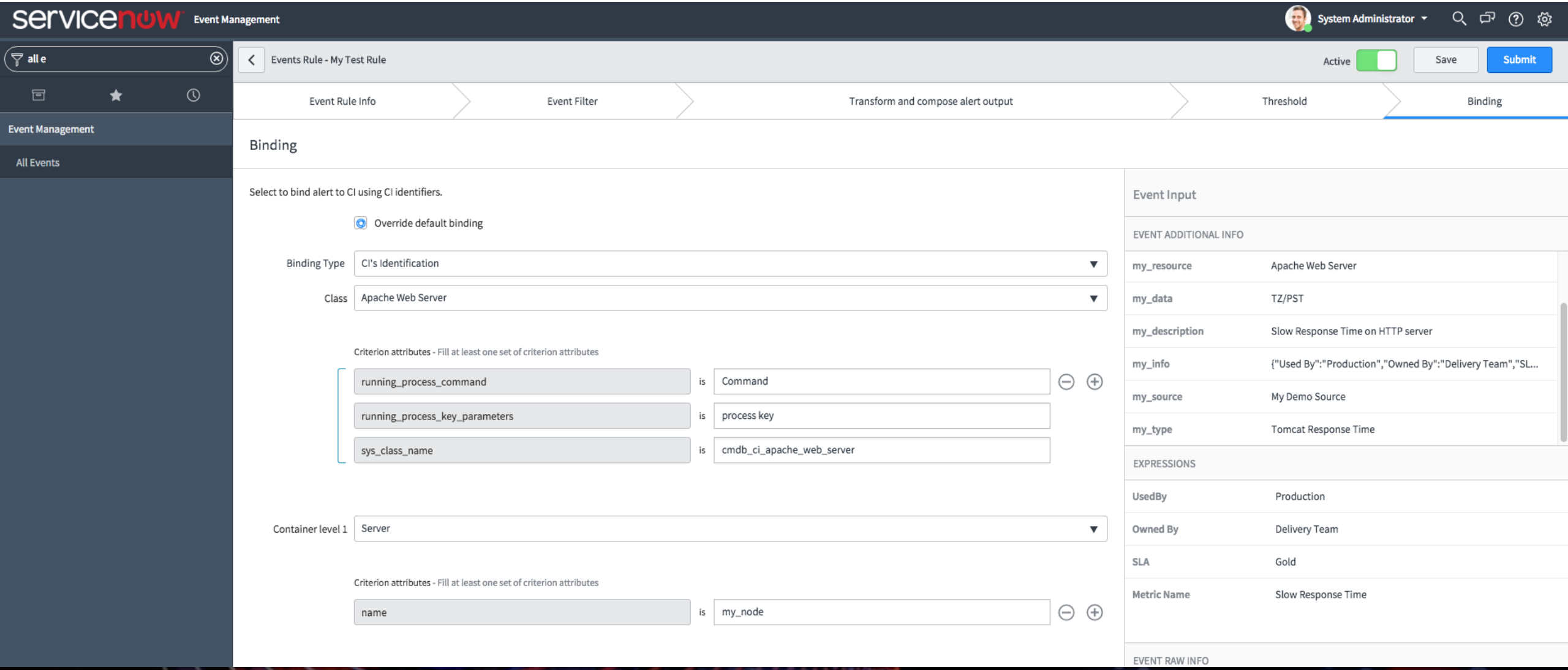
© 2017 ServiceNow All Rights Reserved

Use the Event Rule Designer to Compose New Alert - Threshold



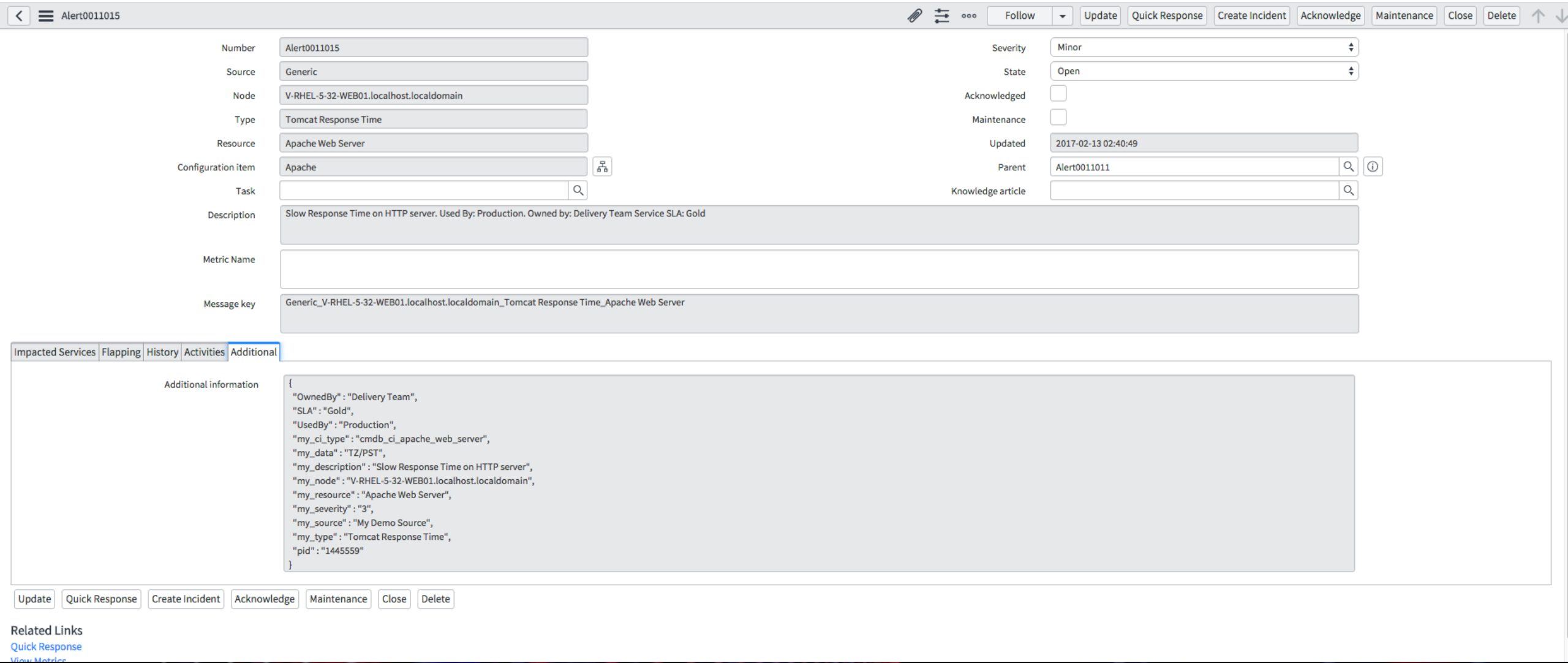
© 2017 ServiceNow All Rights Reserved

Use the Event Rule Designer to Compose New Alert - Binding



© 2017 ServiceNow All Rights Reserved

Resend New Event and Capture its Transformation



© 2017 ServiceNow All Rights Reserved



Triage Service Outage Using Service Metrics

Use operational metrics data to triage alerts

Correlate metric to better understand probable cause

Identify probable cause using history and change view

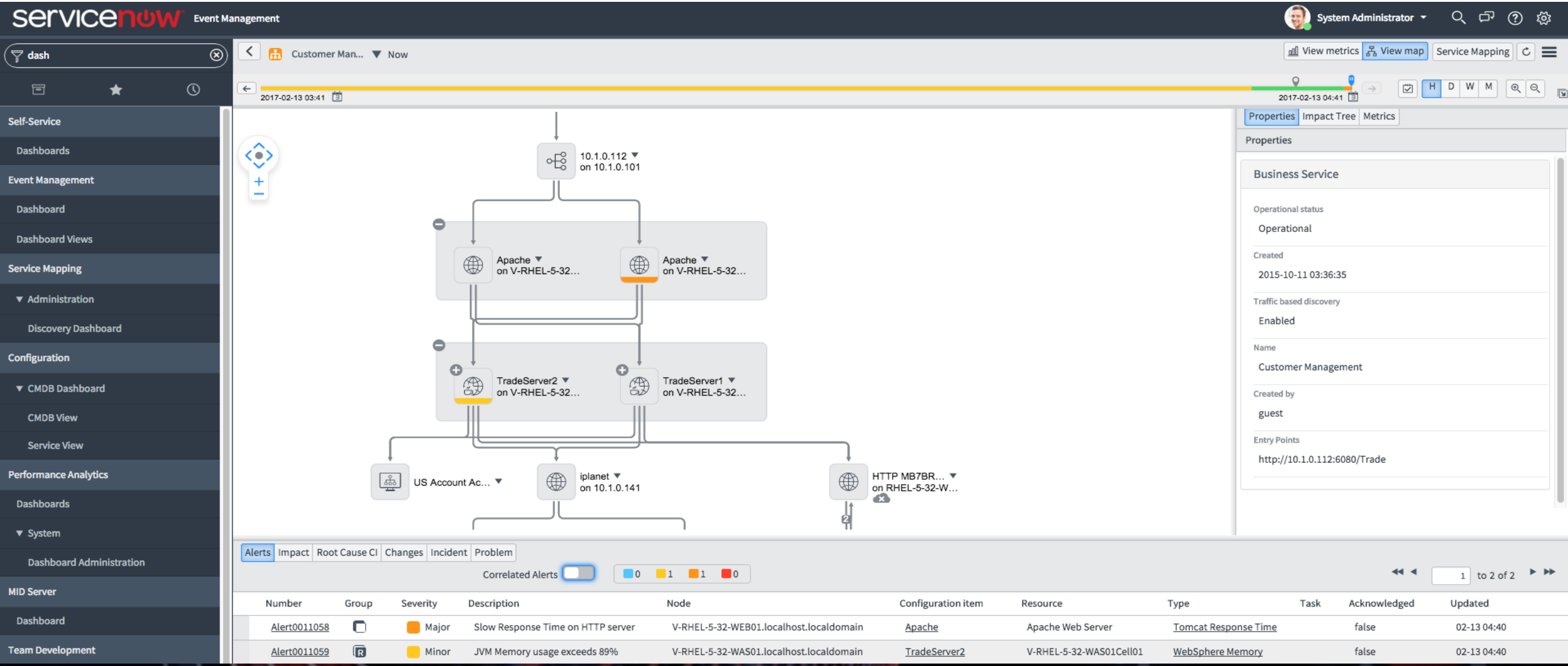
© 2017 ServiceNow All Rights Reserved

Demo – Triage Service Outage

- Detect/Sense
  - Business Services Dashboard – New incoming alert
  - Service X changes status to Critical – ‘Slow Response Time on HTTP server’ on the Web Server
    - Drill down to the service – understand impact
    - View operational metrics data for the service
- Analyze
  - Look for performance anomalies/correlations
  - Correlate alerts between CIs to analyze probable root cause and dependencies
  - Compare service to history to track configuration changes
- Response
  - An emergency change is opened to fix this change and revert to previous version
  - Run remediation actions

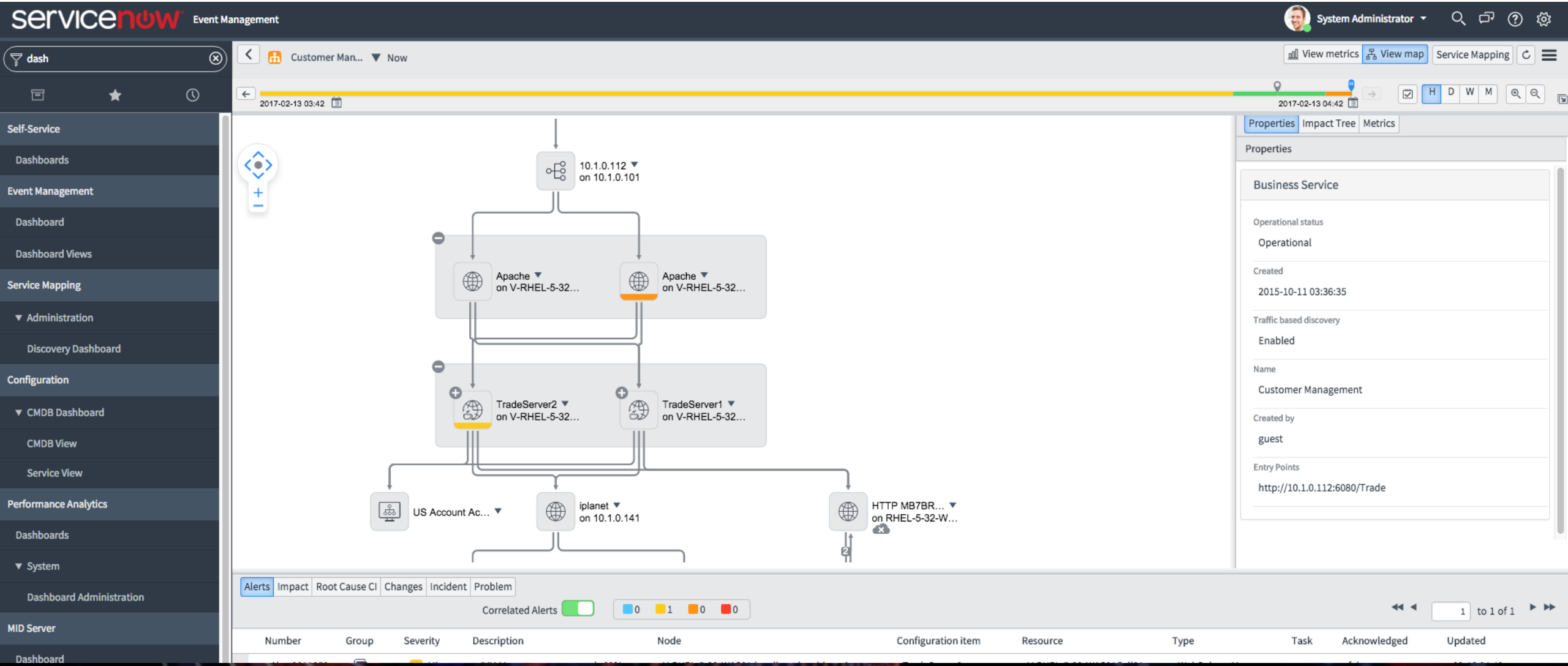
© 2017 ServiceNow All Rights Reserved

Business Services Dashboard – New Incoming Alert



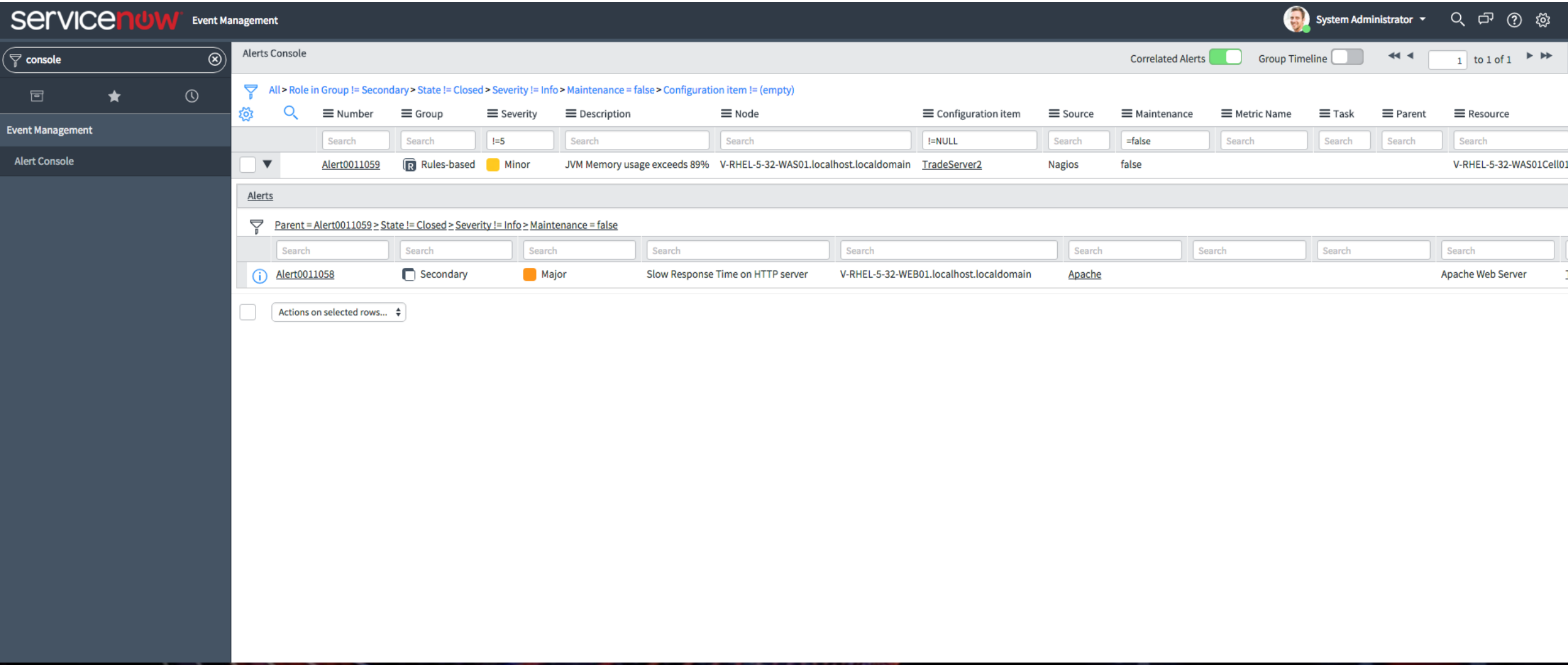
© 2017 ServiceNow All Rights Reserved

Business Services Dashboard – New Incoming Alert



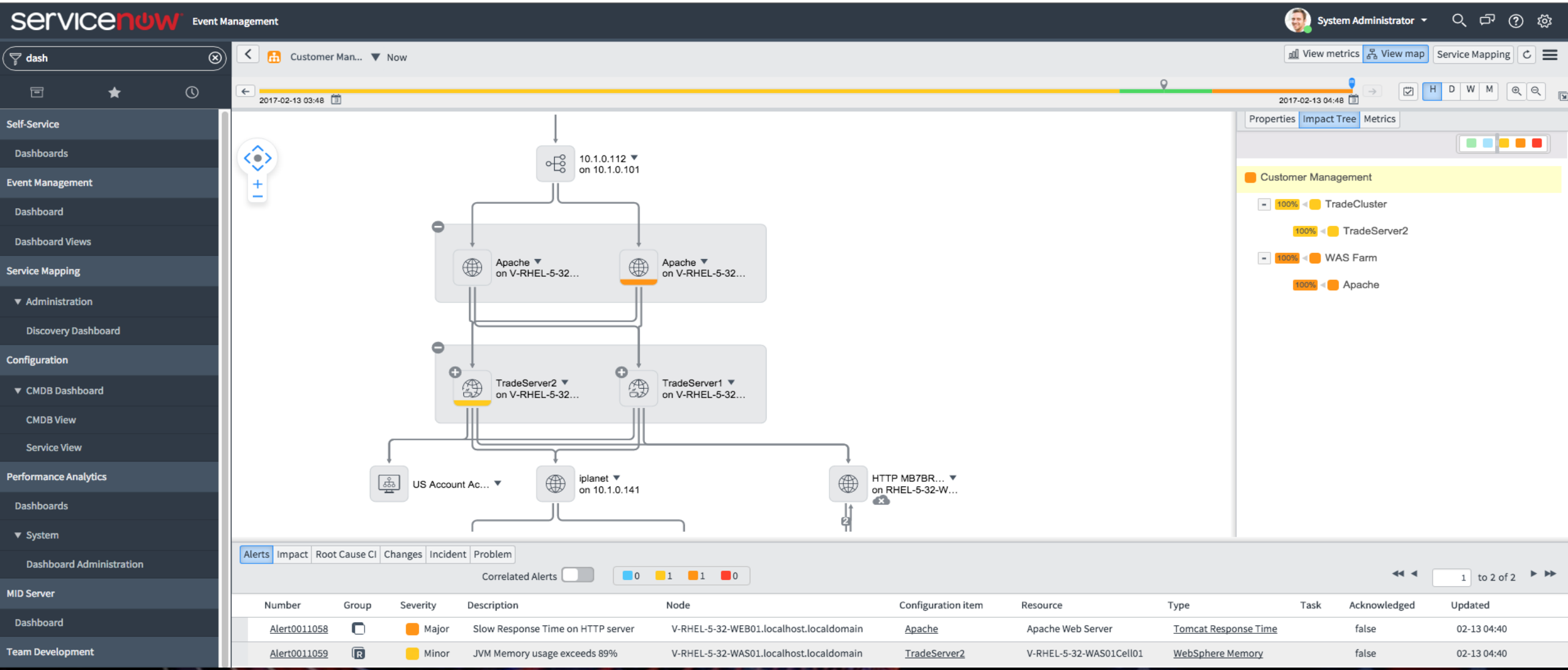
© 2017 ServiceNow All Rights Reserved

Business Services Dashboard – New Incoming Alert



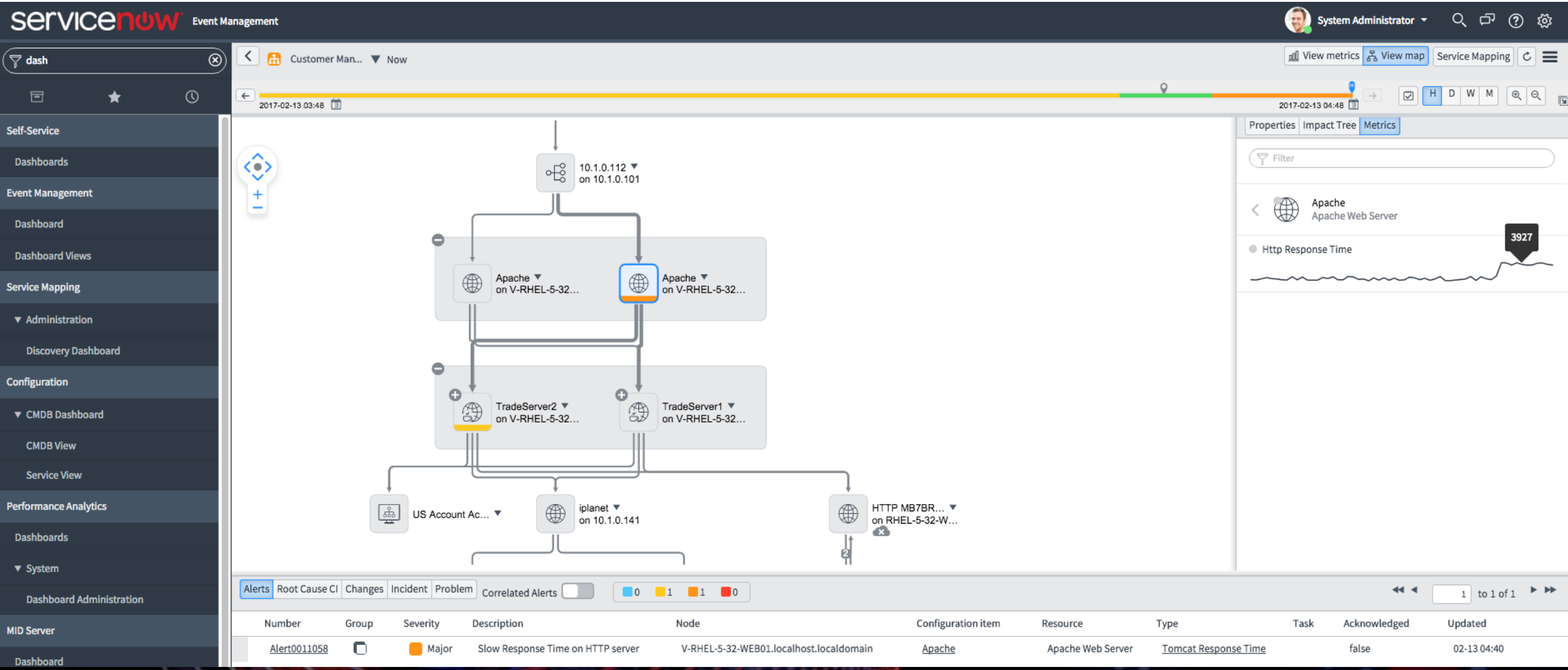
© 2017 ServiceNow All Rights Reserved

Analyze – View Operational Metrics Data



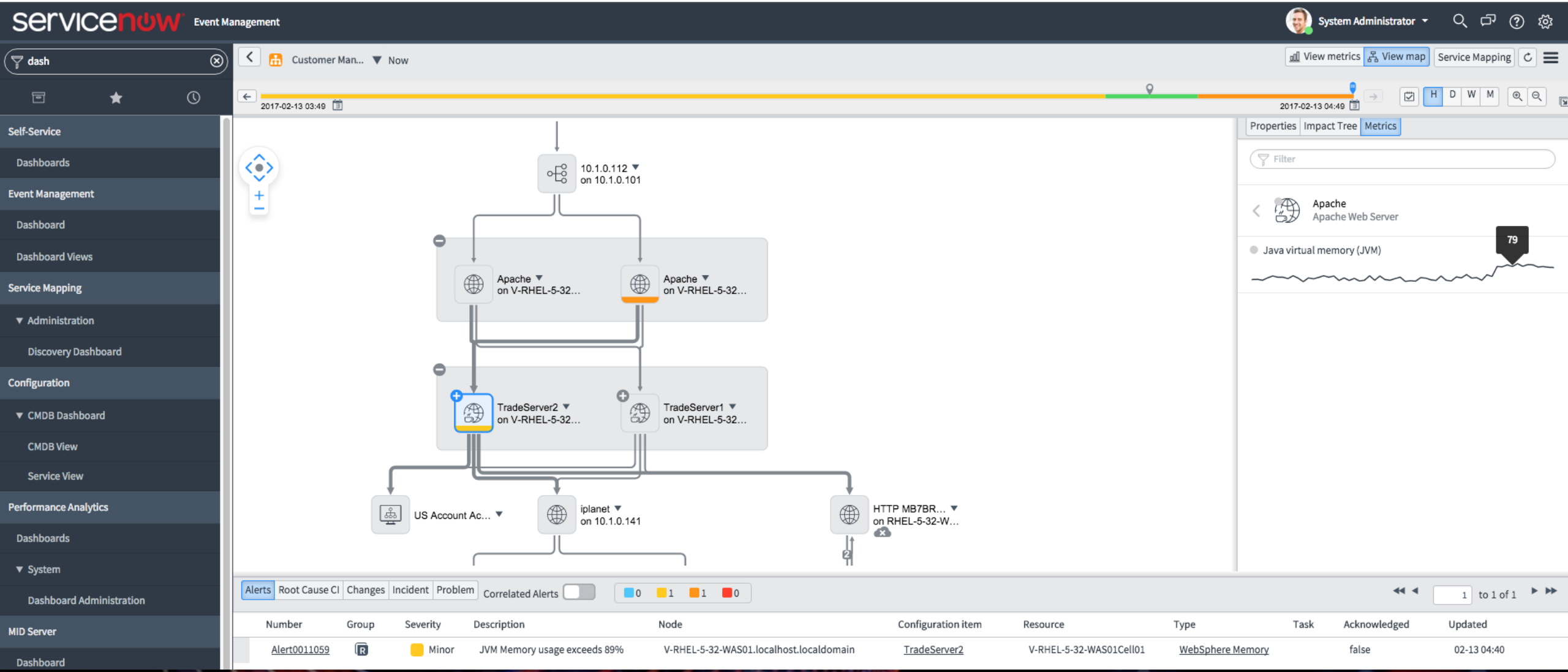
© 2017 ServiceNow All Rights Reserved

Analyze – View Operational Metrics Data



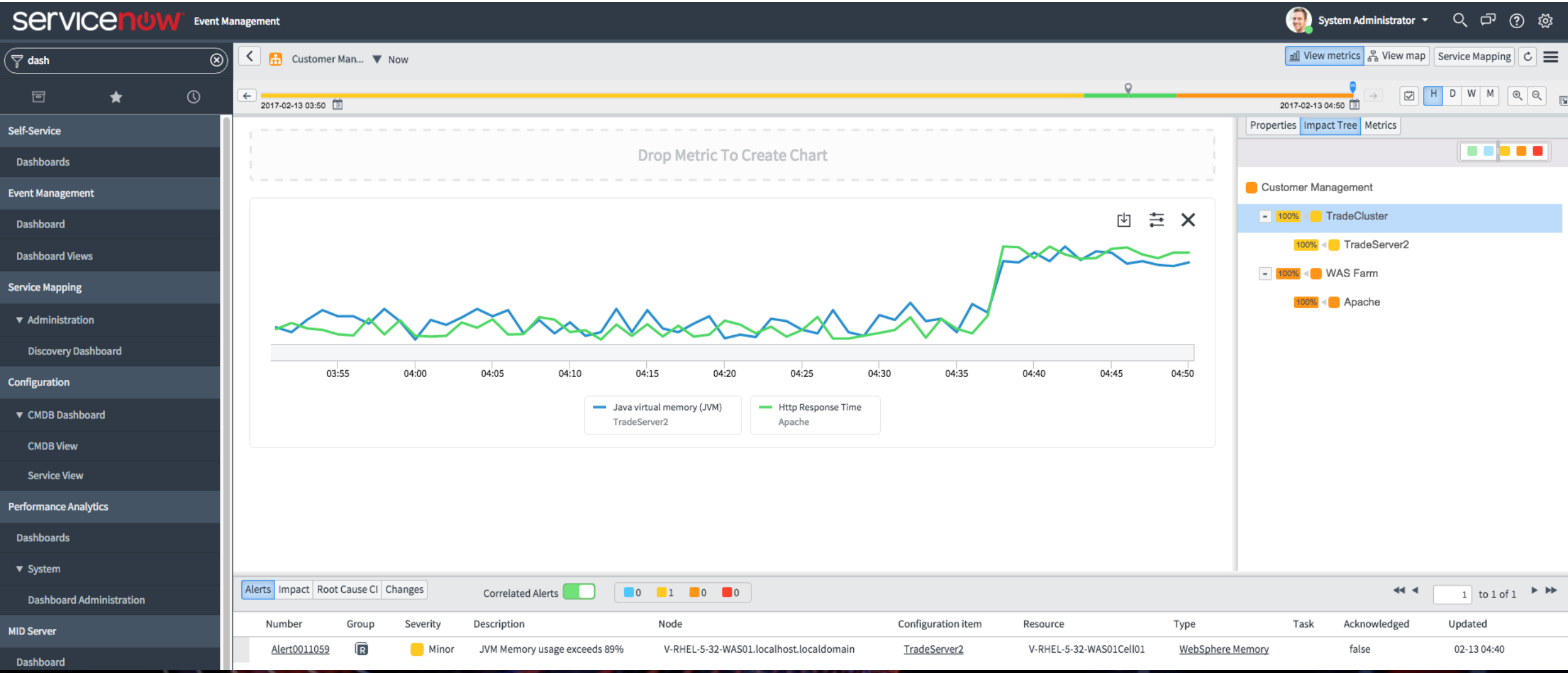
© 2017 ServiceNow All Rights Reserved

Analyze – View Operational Metrics Data



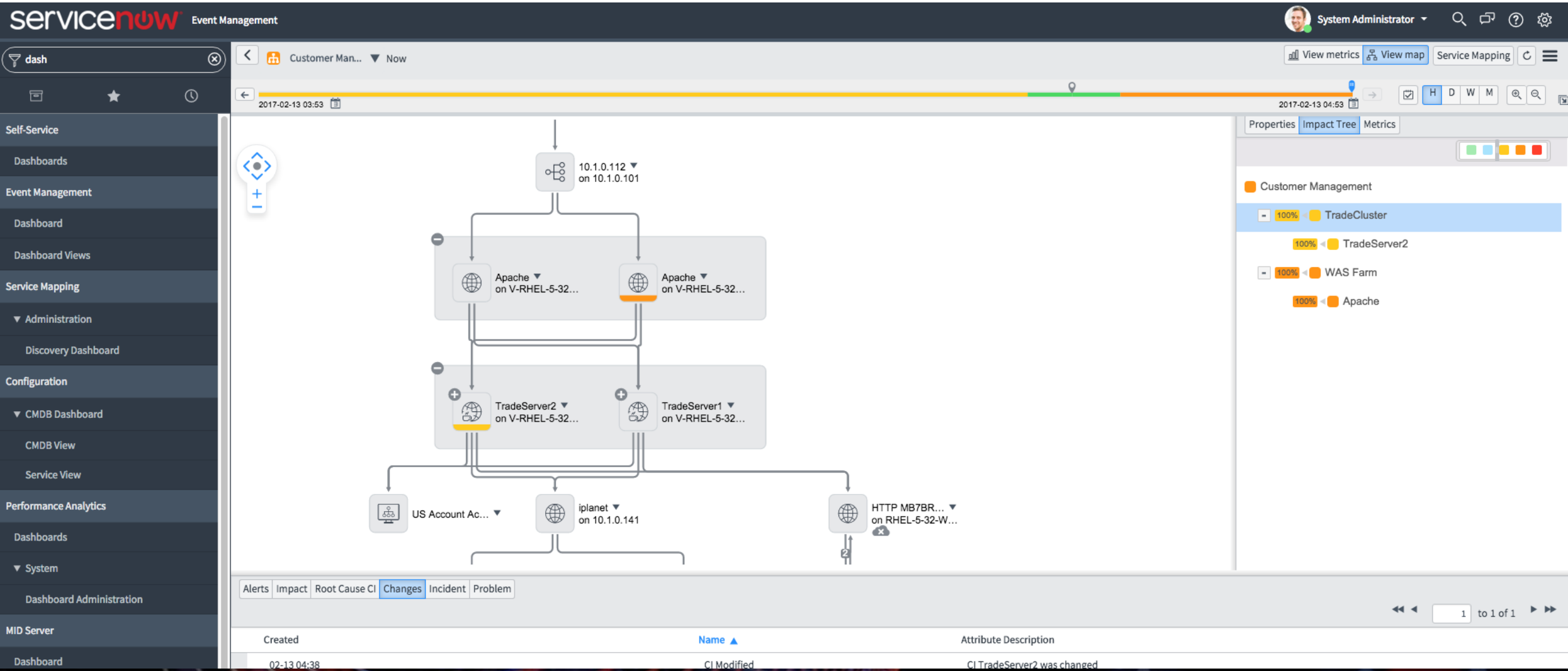
© 2017 ServiceNow All Rights Reserved

Analyze – Correlate Operational Metrics Data



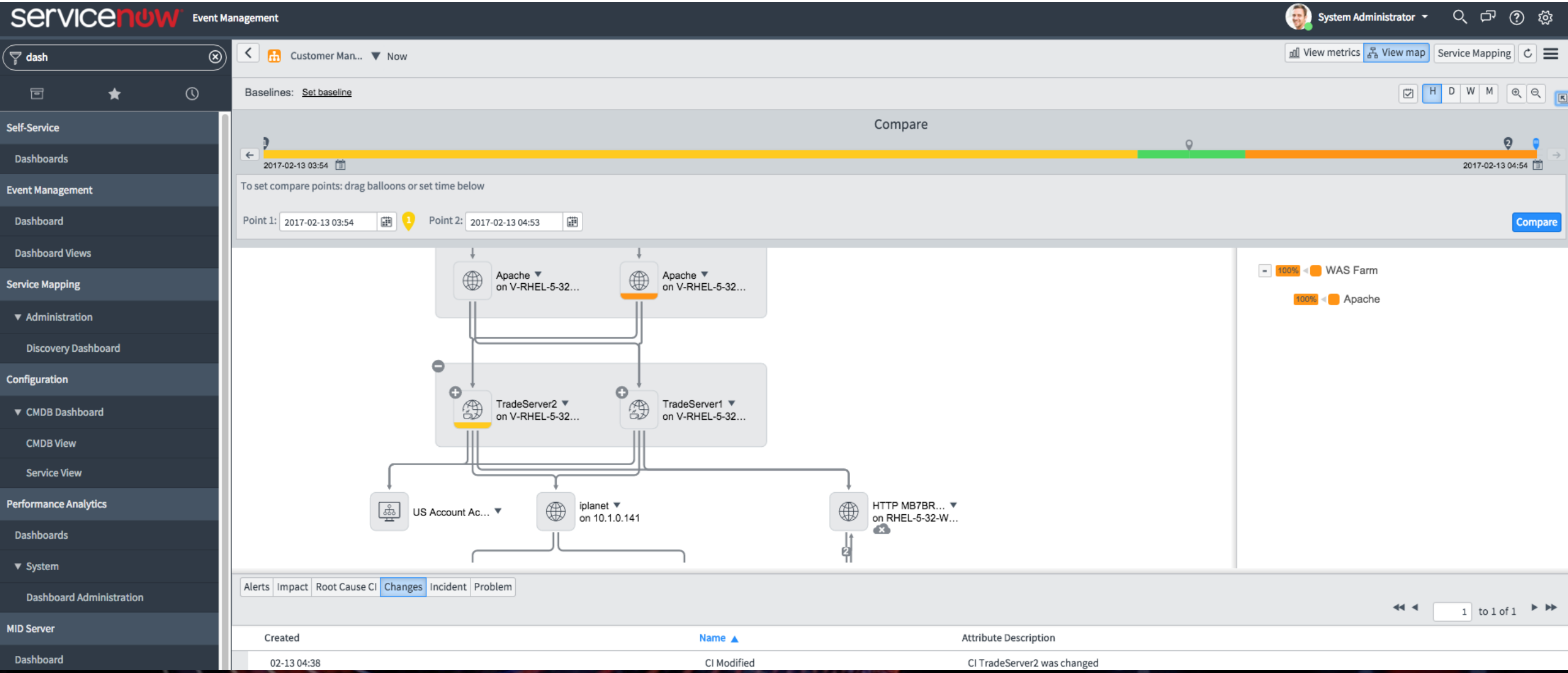
© 2017 ServiceNow All Rights Reserved

Analyze – View Service History to Track Changes



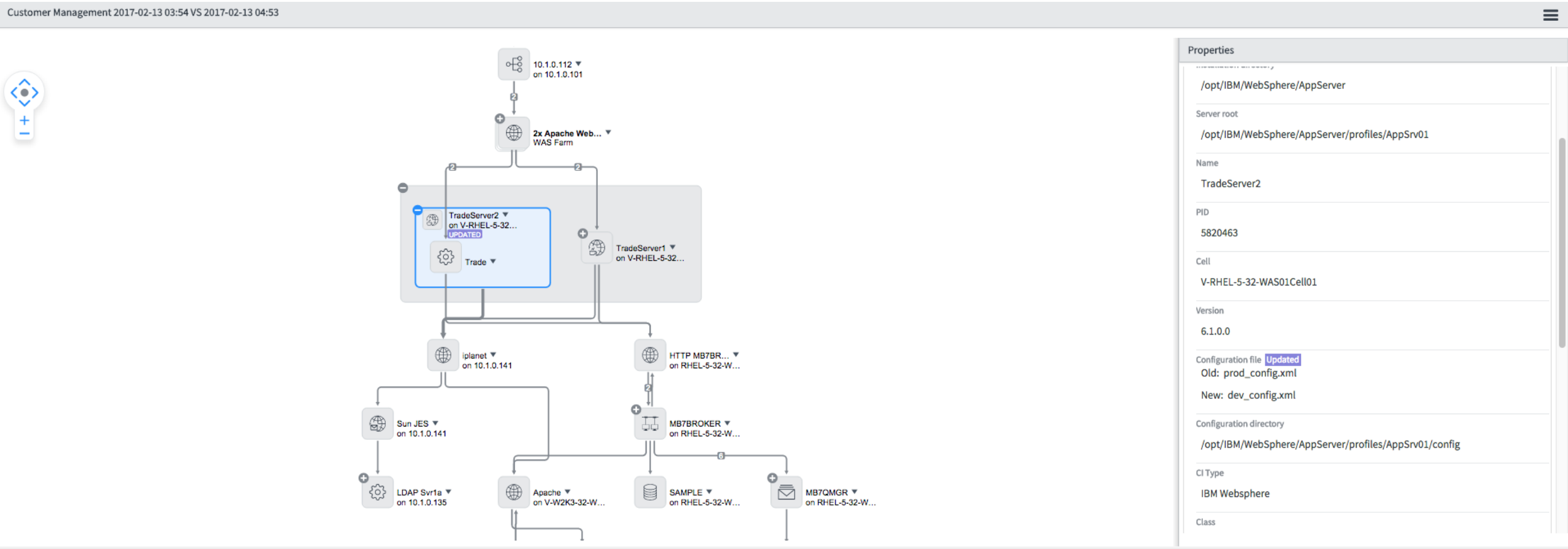
© 2017 ServiceNow All Rights Reserved

Analyze – Compare Service History to Track Changes



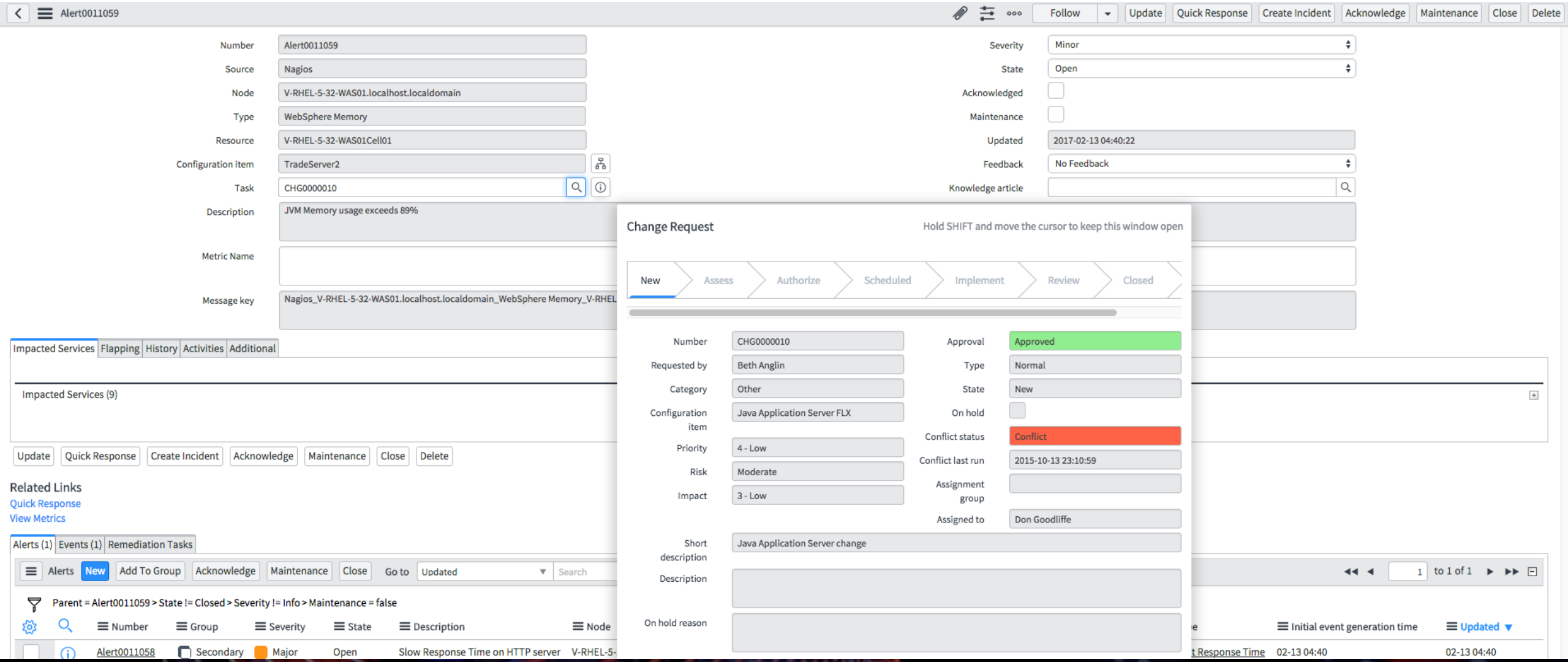
© 2017 ServiceNow All Rights Reserved

Analyze – Compare Service History to Track Changes



© 2017 ServiceNow All Rights Reserved

Response – Call for Action



© 2017 ServiceNow All Rights Reserved

Value Outcomes

Reduce noise by

99%

Of raw events

Focus on the root cause



To define new data source

3X

FASTER

Deployment time

© 2017 ServiceNow All Rights Reserved

Lessons Learned

1. Event Management is even more powerful with Service Mapping & Discovery
2. Service maps provide business context and facilitate isolation of problems
3. Operational Metric provides broader context to the service triage
4. Machine learning is embedded into the OI logic
5. Integration is easier then ever

© 2017 ServiceNow All Rights Reserved

Top Takeaways

1

Operational intelligence is de-facto solution to eliminate service outage

2

Machine learning is embedded into the OI logic and reduces dramatically the manual overhead

3

Integration is easier then ever

© 2017 ServiceNow All Rights Reserved

Thank You

BENNY MAKOVSKY
SR PRODUCT MANAGER
ServiceNow

@MakovskyBenny | #Know17

© 2017 ServiceNow All Rights Reserved

Q & A

BENNY MAKOVSKY
SR PRODUCT MANAGER
ServiceNow

© 2017 ServiceNow All Rights Reserved

Take the Survey

Please take a moment to complete a session survey in the Knowledge17 app.

Thank You

Benny Makovsky

Sr Product Manager

ServiceNow

© 2017 ServiceNow All Rights Reserved