knowledge17

http://clabs.link/lab131985

WORK at LIGHTSPEED

ServiceWatch Insight: Integrating Events and Rules

Vinh Tran
Solution Architect, ITOM Practice
ServiceNow

Tony Branton
Sr. Advisory Solution Architect, ITOM Practice
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

Agenda

- Lab Objectives
- Event Integration
- Event and Alert Processing
- Labs
- Q & A

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



Name: Vinh Tran

Title: Solution Architect

Function: ITOM Practice

Company: ServiceNow

Experience: 1 year at ServiceNow, 25 years in IT industry

Expertise: Event Management, Discovery, Service Mapping, Orchestration Cloud Management

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



Name: Tony Branton

Title: Senior Advisory Solution Architect

Function: ITOM Practice

Company: ServiceNow

Experience: 3 years at ServiceNow, 15 years in ITOM industry, 25 years in IT industry

Expertise: Event Management, Discovery, Service Mapping, Orchestration, Cloud Management, Deadpool comics…

© 2017 ServiceNow All Rights Reserved

Objectives and What You Will Learn

Objectives

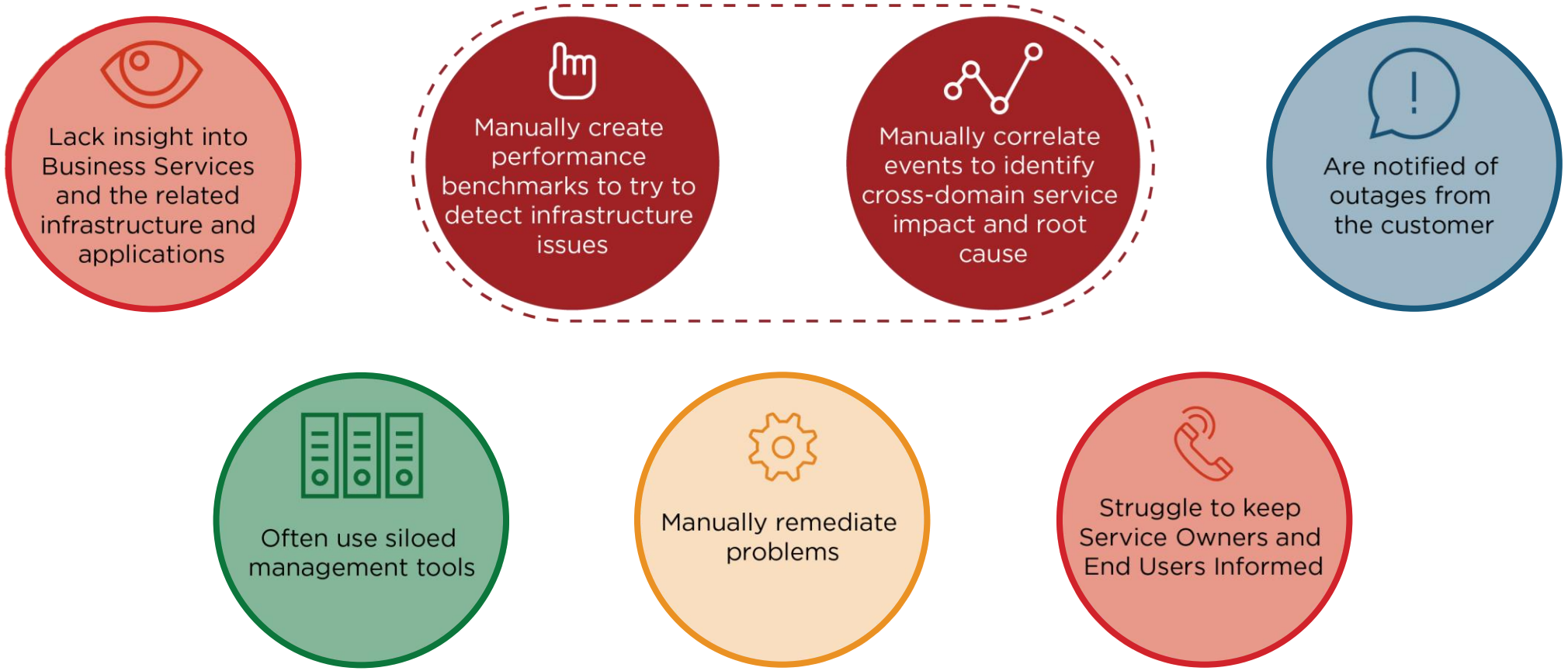
- Learn how to enhance service visibility by integrating events and alerts from third-party monitoring tools and event sources into Event Management using REST and SNMP

What you will learn

- How to integrate events using REST and SNMP
- How to configure event rules to process events
- How to configure alert rules to trigger actions
- How to correlate alerts using rules

© 2017 ServiceNow All Rights Reserved

When Problems Occur, IT Operations Teams…

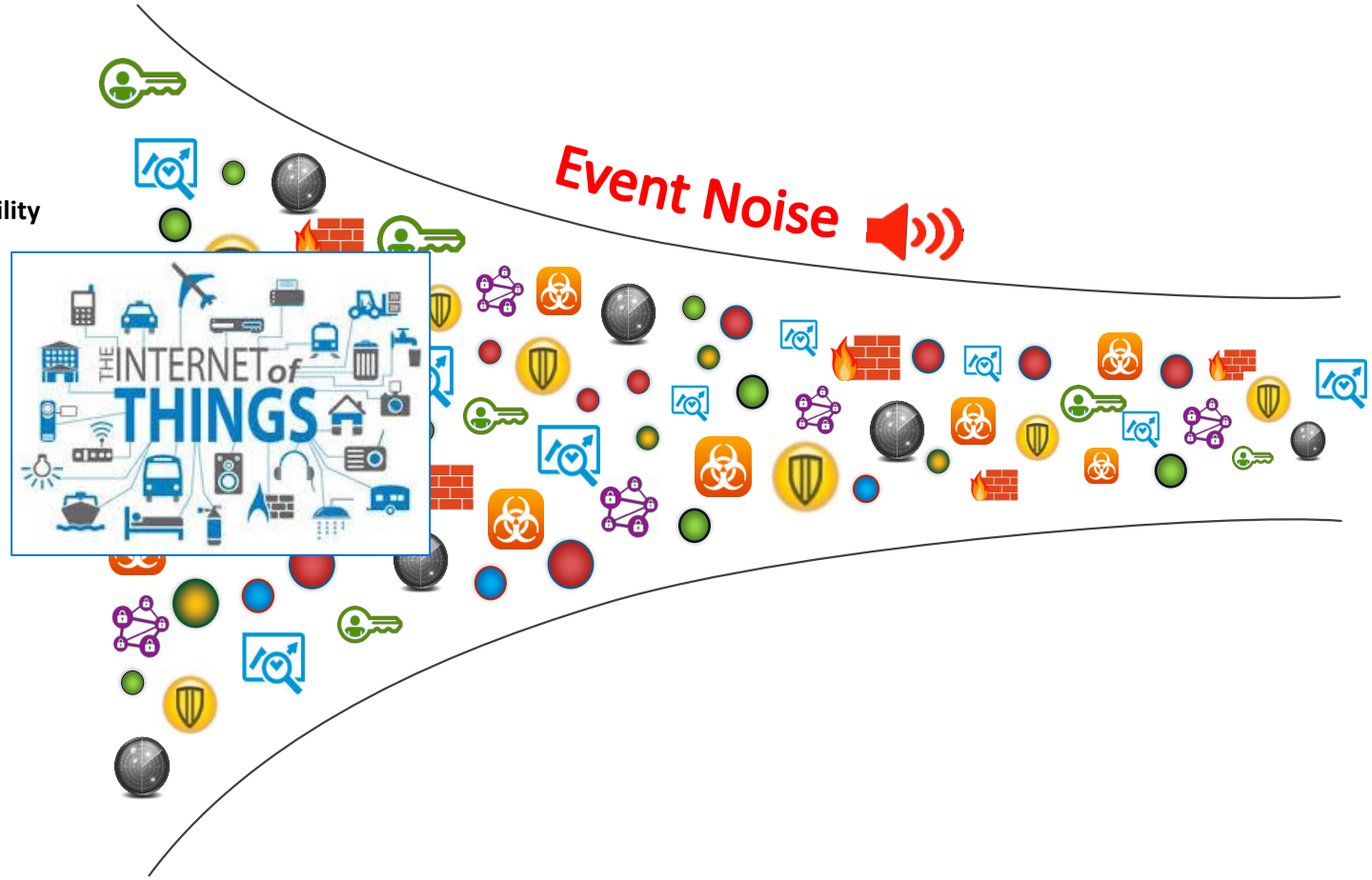


© 2017 ServiceNow All Rights Reserved

Event Noise – It's Only Getting Louder

Event Sources

- Performance & Availability
- Firewall/IPS/IDS
- End User Experience
- Identity & Access
- Threat/Intel
- Network
- Vulnerability Detection



Challenges

- Business Impact
- Priority
- Process Remediation
- Metrics Measurement
- Service Level Management
- Security Information Consolidation

© 2017 ServiceNow All Rights Reserved


HOW AM I GOING TO DEAL WITH THESE EVENTS??

Operational Intelligence



Improve availability by combining events and service maps to optimize service health

- Consolidate events from different sources
- Filter events to reduce noise and generate qualified alerts
- Automated Alert aggregation and causal analysis
- Early issue detection through anomalies in performance metrics
- Understand impact to service health via service availability dashboard
- Automatically create any ServiceNow task for an alert
- Automatically or manually apply corrective actions to restore services fast

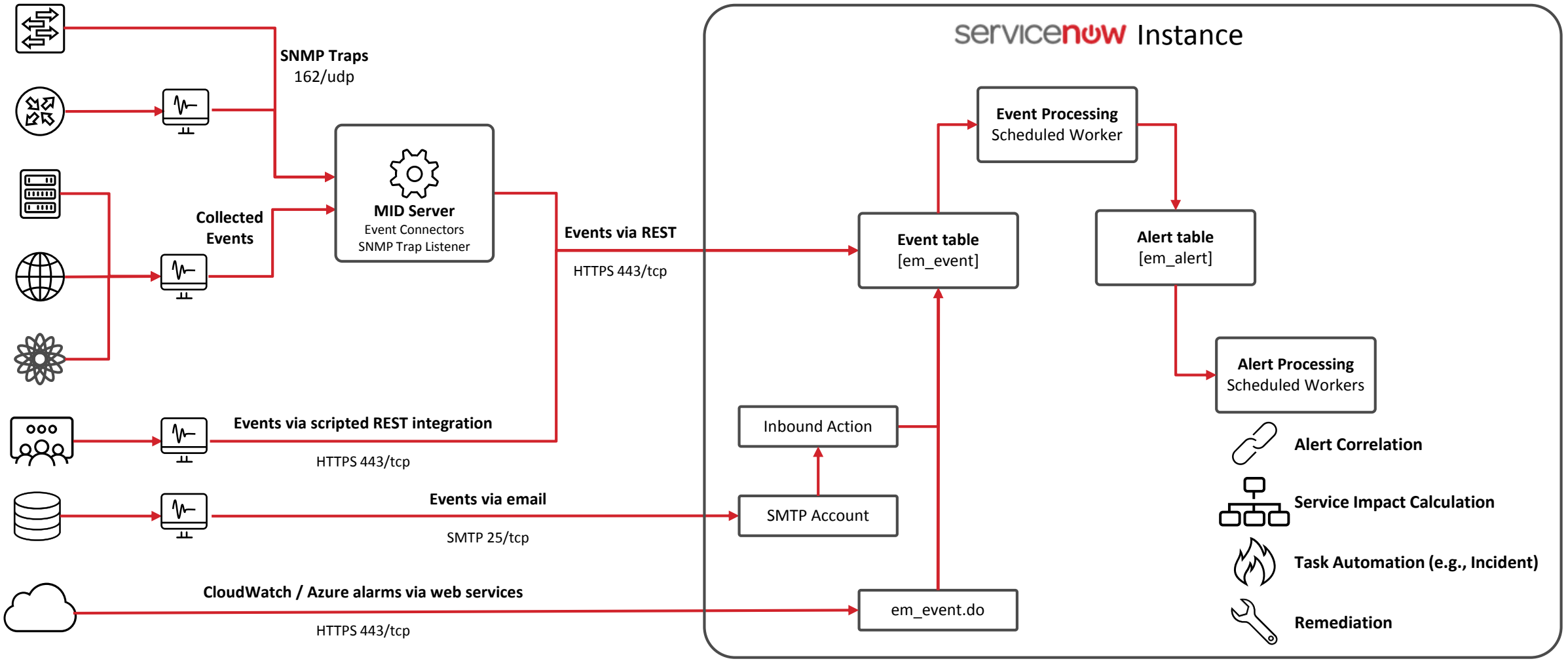


© 2017 ServiceNow All Rights Reserved

Event Integration

© 2017 ServiceNow All Rights Reserved

Event Integration Overview



Infrastructure | Monitoring | Event Collection | Event Processing

© 2017 ServiceNow All Rights Reserved

Event Integration (Jakarta Release)

- OOTB Connectors:
  - Amazon CloudWatch
  - BMC TrueSight
  - HP OM
  - HP OMi
  - Hyperic
  - IBM Netcool/OMNIbus
  - Microsoft Azure
  - Microsoft SCOM
  - Nagios XI
  - Nectar
  - Oracle Enterprise Manager
  - SolarWinds
  - Splunk
  - VMware vRealize Operations
  - Zabbix
- 3rd-Party Connectors
  - Sumo Logic
  - AppDynamics (Developed by DoItWise)
  - CA APM
  - CA Nimsoft / UIM
  - CA Spectrum
  - Dynatrace
  - HP SiteScope
  - New Relic
  - Datadog
  - Panopta
- REST API
- Web Services
- SNMP Traps
- Email (via Inbound Actions)

© 2017 ServiceNow All Rights Reserved

Lab Time…

- Lab Guide Errata
  - **Important** pre-requisites
  - Last minute corrections to the lab guide
  - Download from:
    https://servicenow.box.com/v/K17-LAB131985-Errata

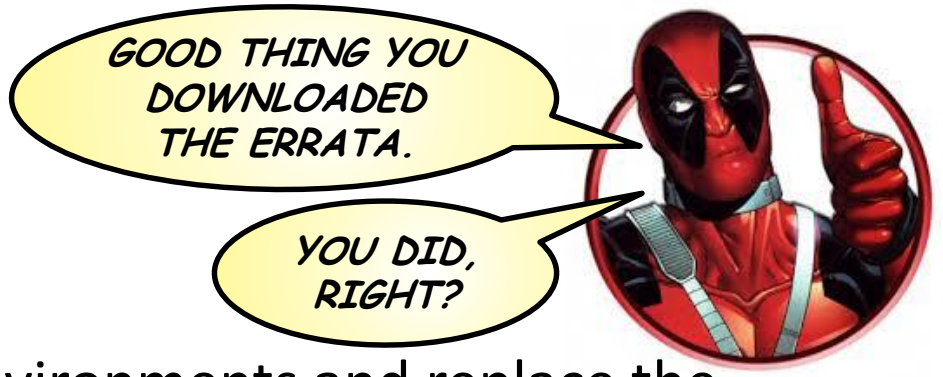
- Call a Lab Guru if you need assistance

- Have fun!



© 2017 ServiceNow All Rights Reserved

Lab Pre-requisites



- **Page 3, Step 6** should read:

  Click on the K17 Labs Environment entry in the list of environments and replace the value for the **snow_inst** Key with **your_instance_name.** Note down the value used for **passwd** and click **Update**.

- **Page 4, Step 3** should read:

  On your MID Server, login to your ServiceNow lab instance using Internet Explorer.

© 2017 ServiceNow All Rights Reserved


NOT SURE IF THIS IS WHAT HE MEANT BY "INTEGRATION"
IT'S TIME FOR LAB 1...

Lab 1.1 Integrate Events with the REST API



- **Page 6, Step 3** should read:

  Enter the following details:

  User ID: **event**
  First name: **Event**
  Last name: **Integration**

- **Page 6, Step 4** should read:

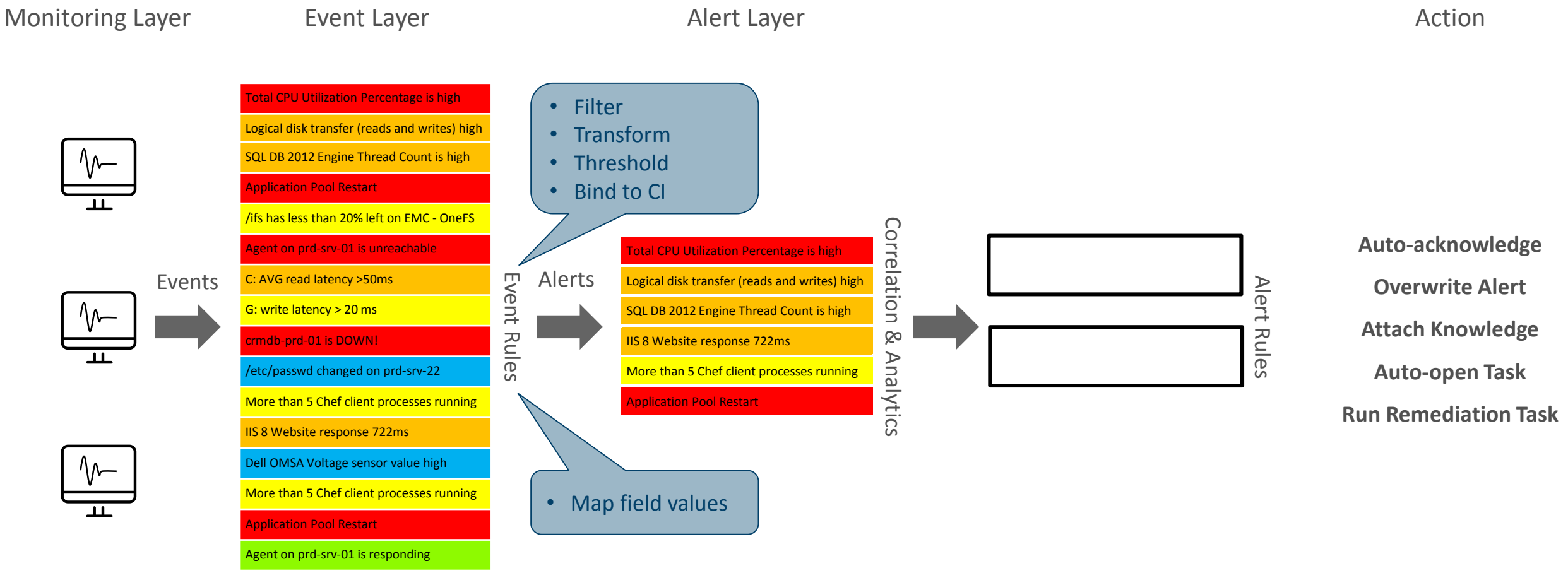
  Use the passwd value you obtained from the Postman K17 Labs Environment in the Lab Prerequisites (Page 3, Step 6) for the **Password** field.

© 2017 ServiceNow All Rights Reserved

Event Rules

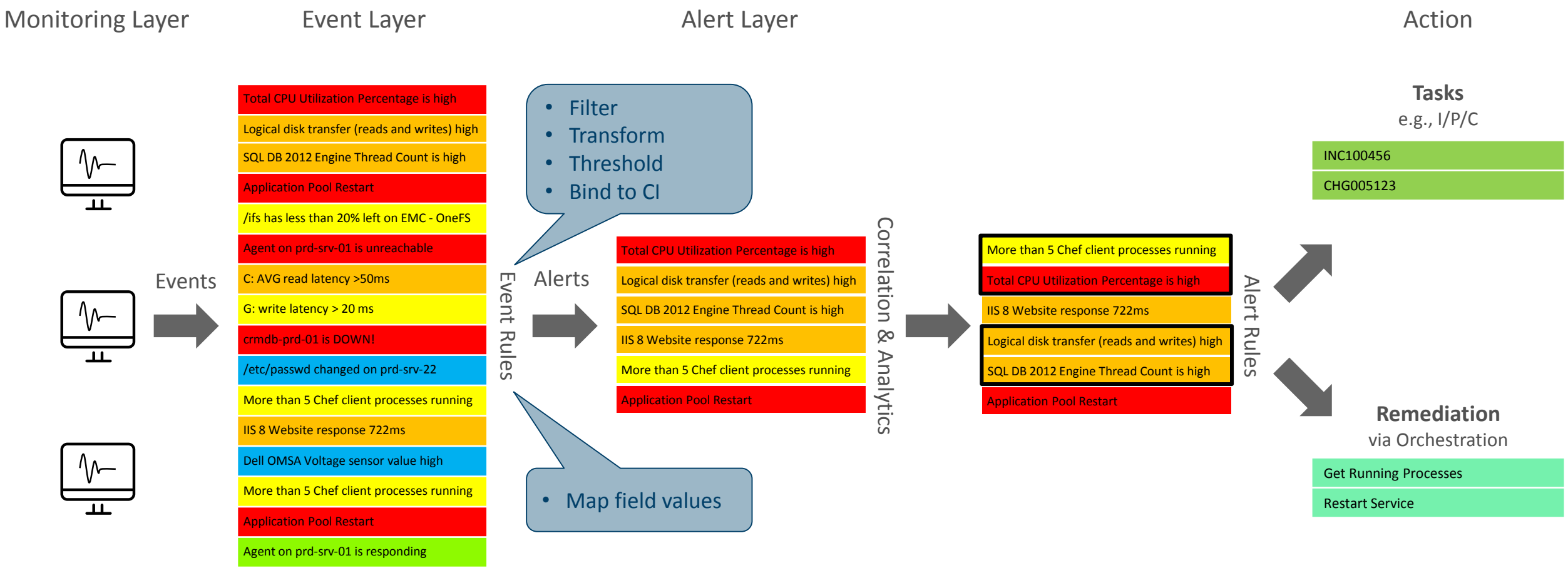
© 2017 ServiceNow All Rights Reserved

Event Processing Flow



© 2017 ServiceNow All Rights Reserved

Event Processing Flow



© 2017 ServiceNow All Rights Reserved

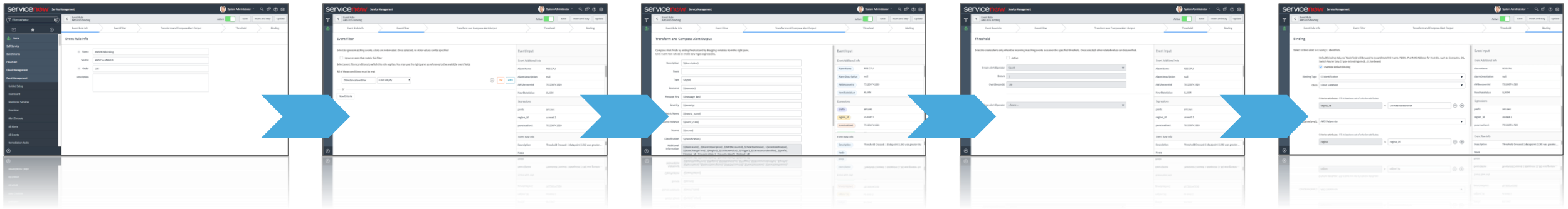
Event Rules

© 2017 ServiceNow All Rights Reserved

Event Rule Designer

- New UI for Administrators to create and update Event Rules
- Create an Event Rule directly from an Event
- Guided, process-driven approach
- Automated field selection, using sampled Event data
- CMDB Identification Engine integration for CI binding

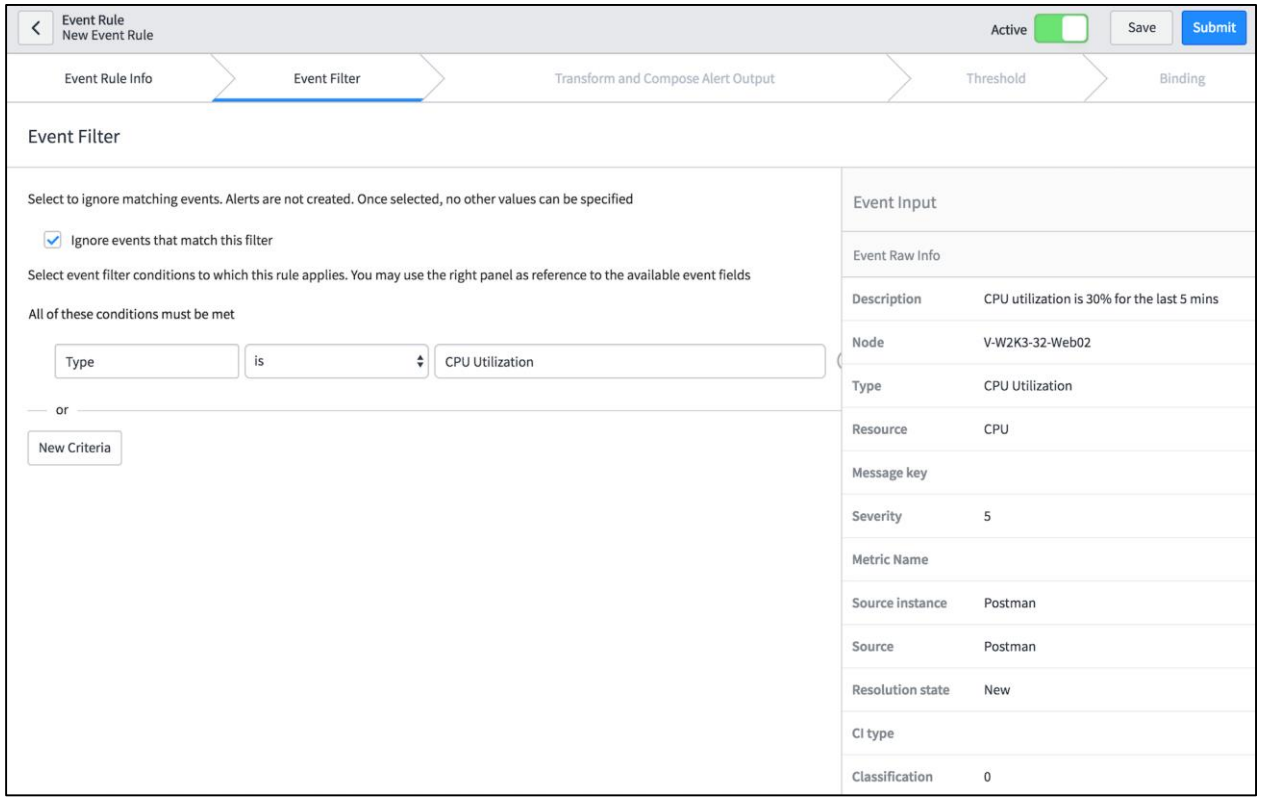
Define Filter Transform Threshold Bind



© 2017 ServiceNow All Rights Reserved

Filtering Events

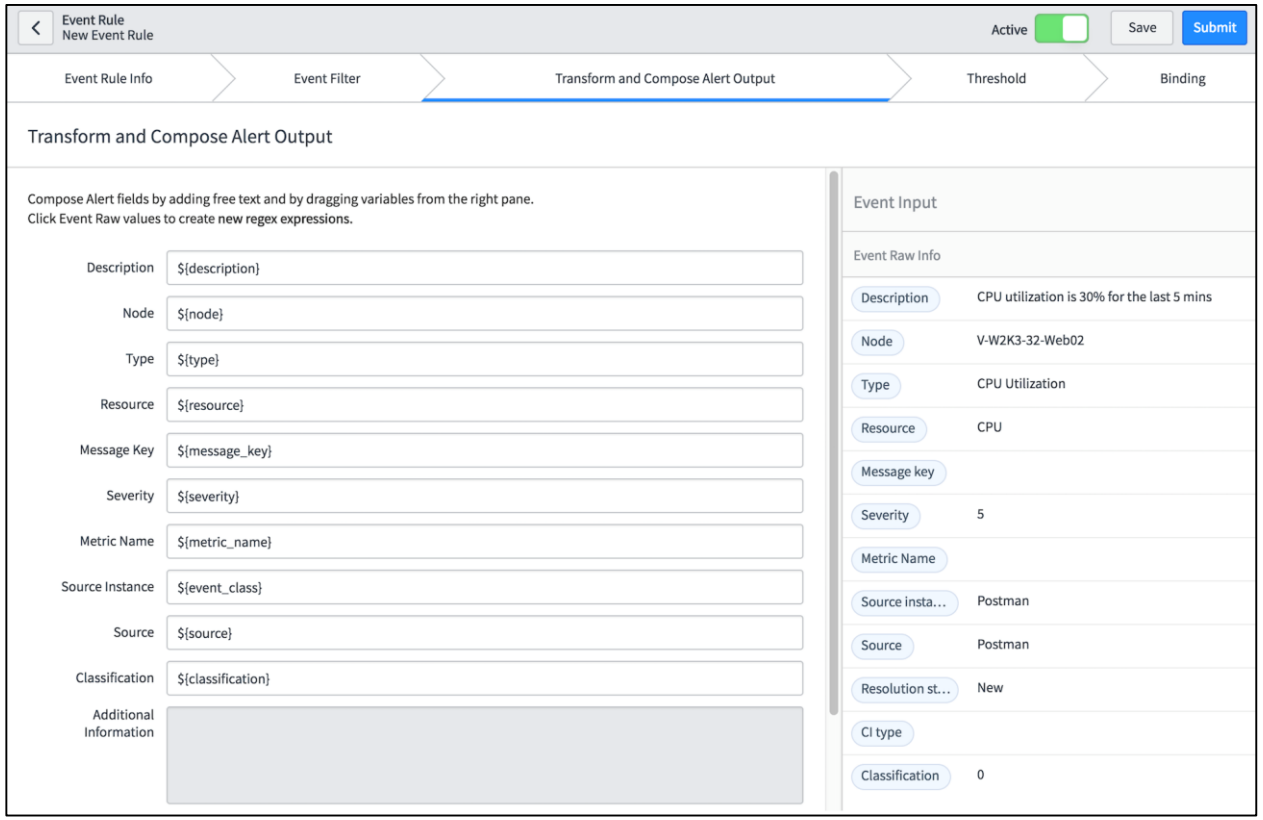
- Use an Event Rule to filter events to prevent alerts being created.
- In the Event Rule:
  - Click the **Event Filter** tab
  - Check the **Ignore event that match this filter** check box
  - Set a filter condition to select events



© 2017 ServiceNow All Rights Reserved

Transforming Events

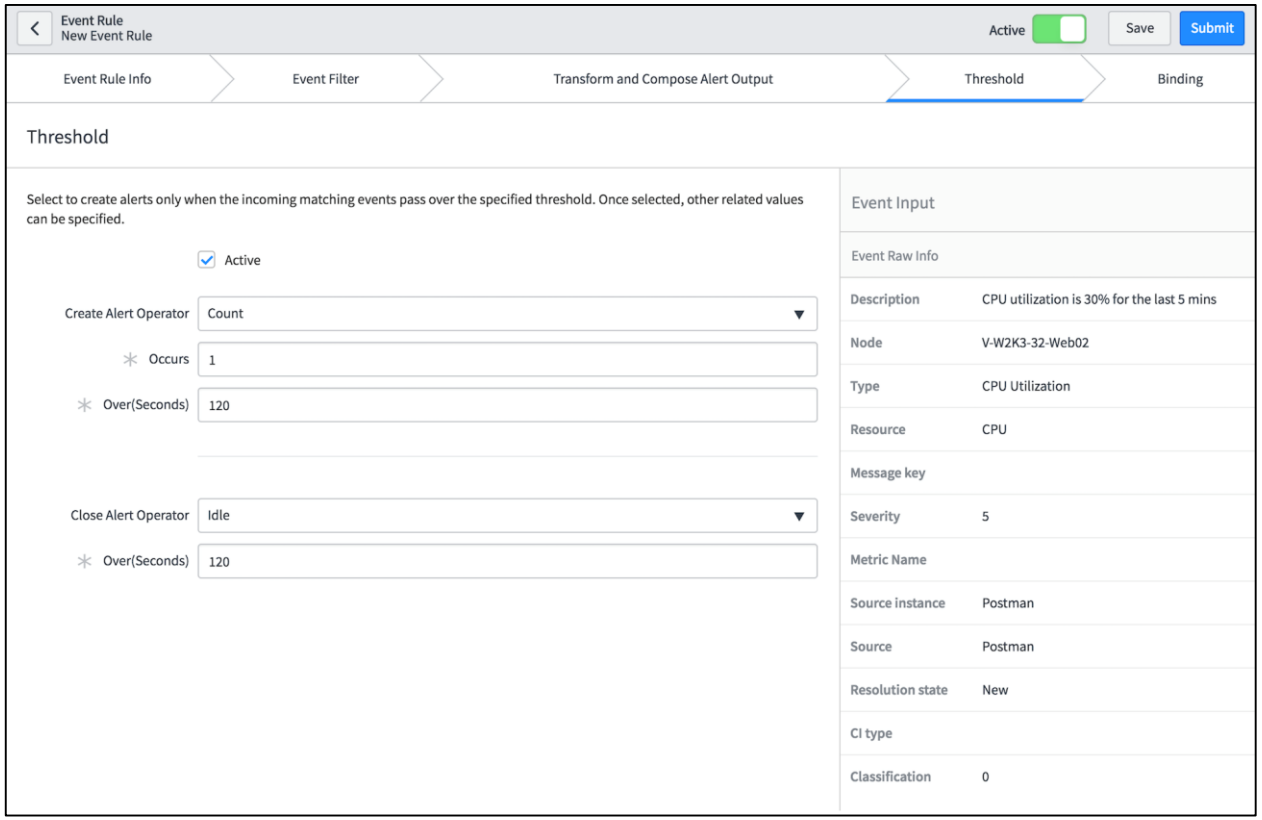
- Consolidating events involves more than integration – once events arrive at the ServiceNow instance, they must be transformed into a consistent format.
- Use an Event Rule to extract data from event fields and set field values in an Alert.



© 2017 ServiceNow All Rights Reserved

Thresholding Events

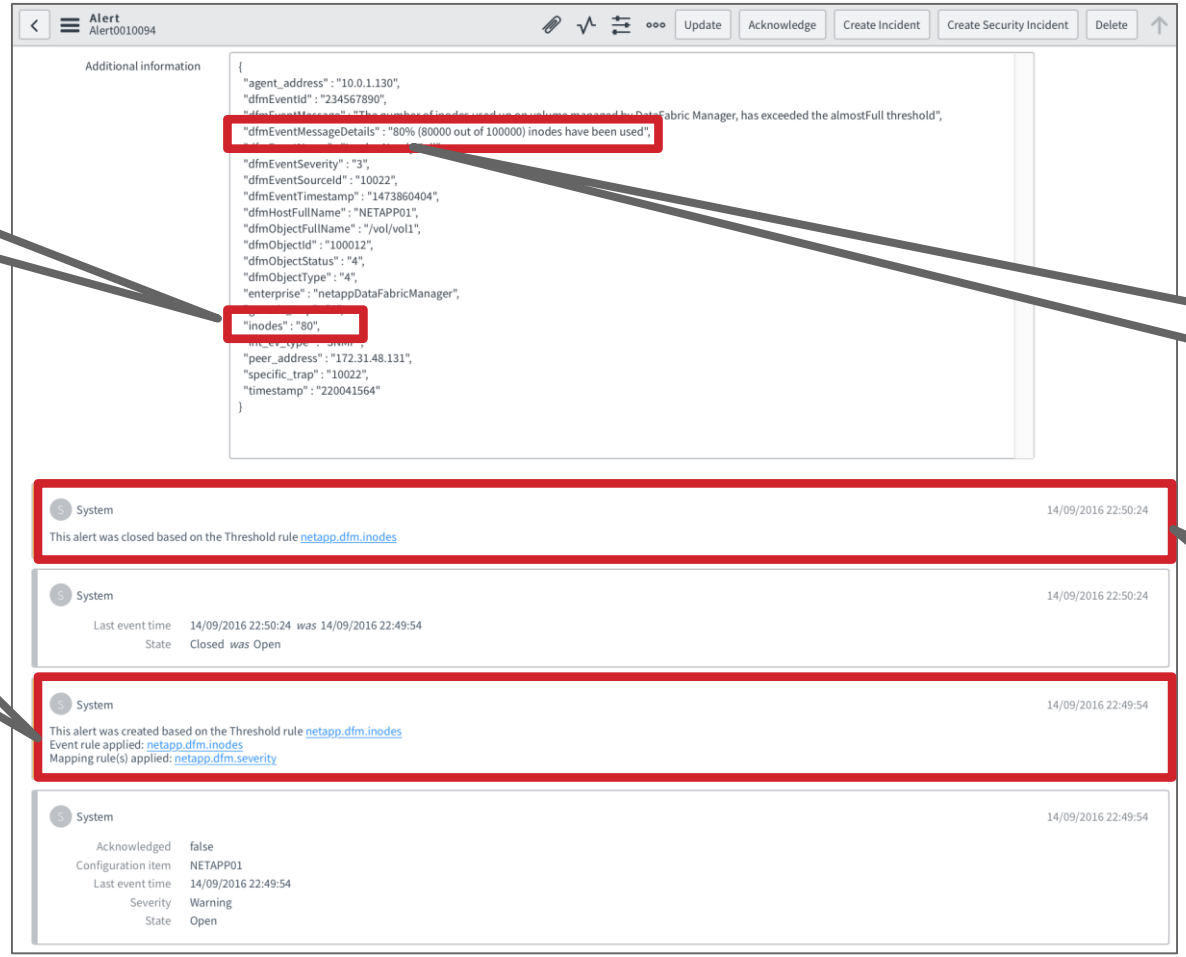
- Threshold operation allows creation of Alerts when specific event values are met or exceeded.
- Threshold Event Rules rely on a **Threshold metric** extracted from an event. This metric and its value must be listed in the event's **Additional information** field.
- The Threshold metric value is compared with a condition and if this evaluates to true, an alert is created.



© 2017 ServiceNow All Rights Reserved

Thresholding Events

Example of an alert created and then closed by a Threshold operation:



Threshold metric…

… extracted from Additional Information via Transform operation...

… meets Threshold condition, creating an alert...

... when the metric value drops *below* a threshold the alert is closed.

© 2017 ServiceNow All Rights Reserved

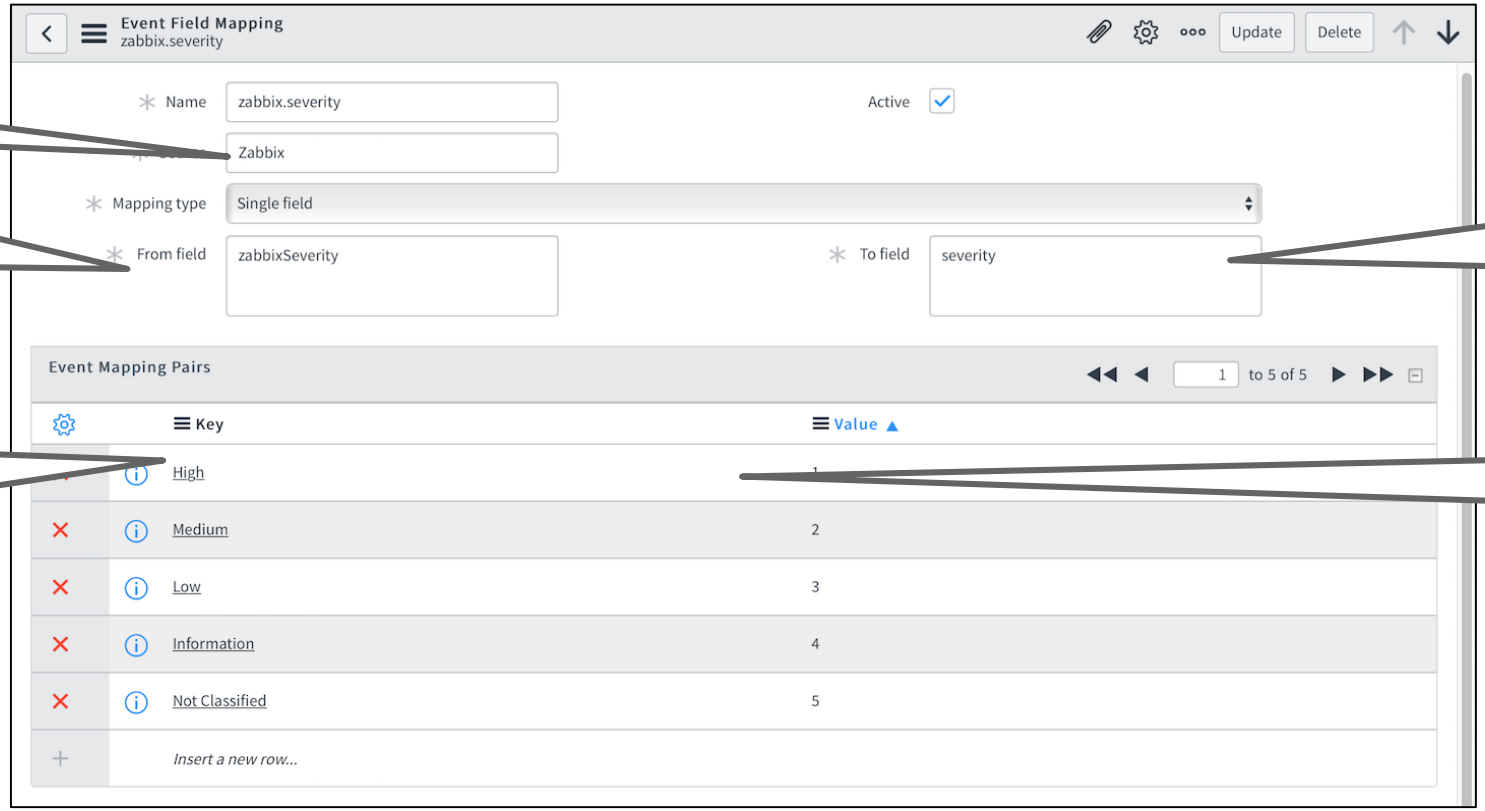
Event Field Mapping Rules

- Event Field Mapping Rules are used to map values from specific fields to values in other fields.
- Event Field Mapping Rules are applied after Event Rule processing and just prior to alert generation.
- More than one Event Field Mapping Rule can be applied to an event.
- Often used for mapping event severity values.

© 2017 ServiceNow All Rights Reserved

Mapping Event Field Values

Event Field Mapping Rule example



Source event class

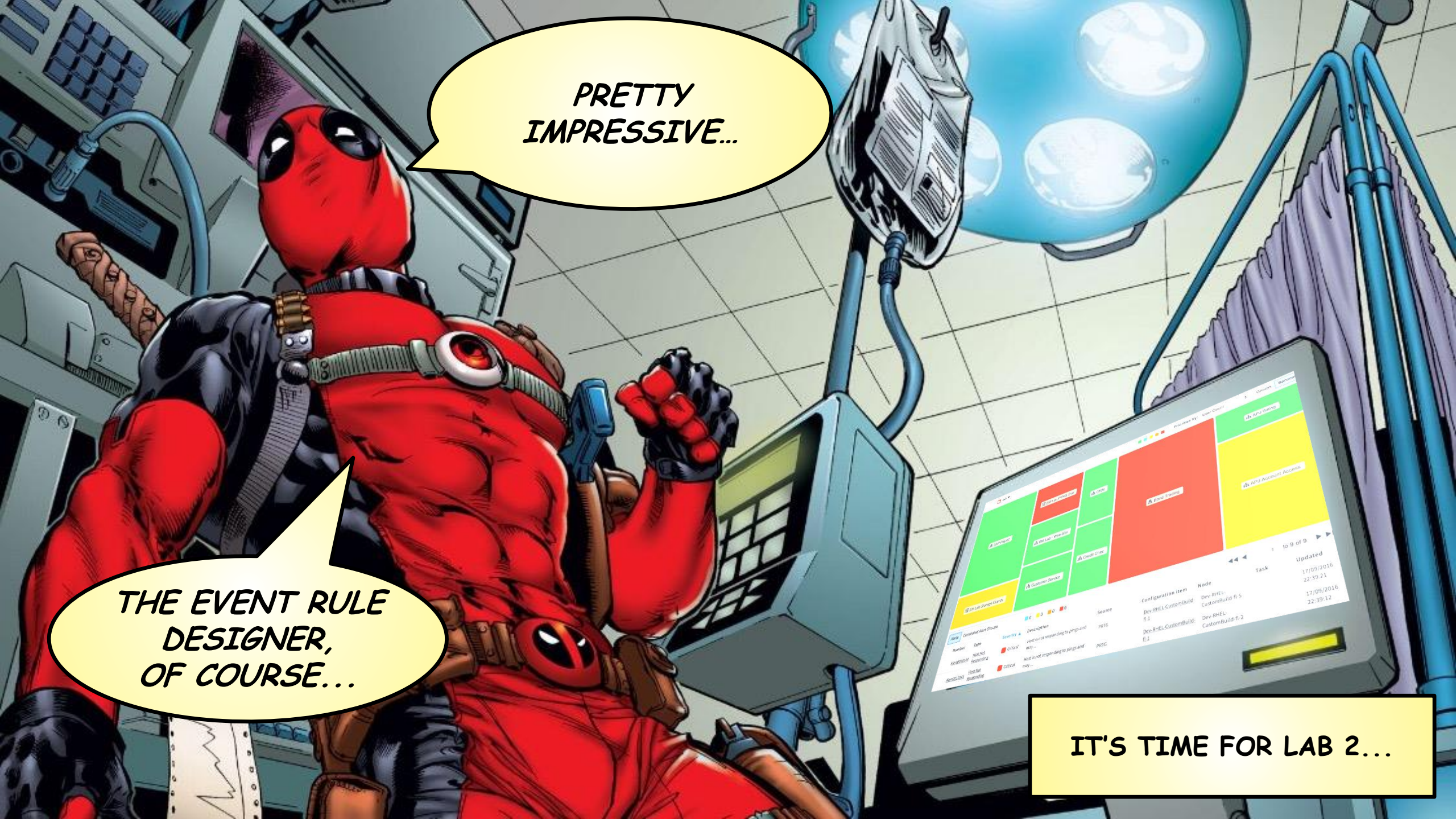
Name of field supplying source value

Possible values from the source event

Name of target field to insert mapped value

Corresponding target field value

© 2017 ServiceNow All Rights Reserved


PRETTY IMPRESSIVE...
THE EVENT RULE DESIGNER, OF COURSE...
IT'S TIME FOR LAB 2...

Lab 2.4 Threshold Events



- **Page 21, Step 2** should read:

  Navigate to **Event Management > All Events** and open one of the recent SNMP trap 789 events in the list. Ensure the **Description** field includes the text “dfmEventMessageDetails = 80%” (or any other number). Click the **Create Event Rule** button.

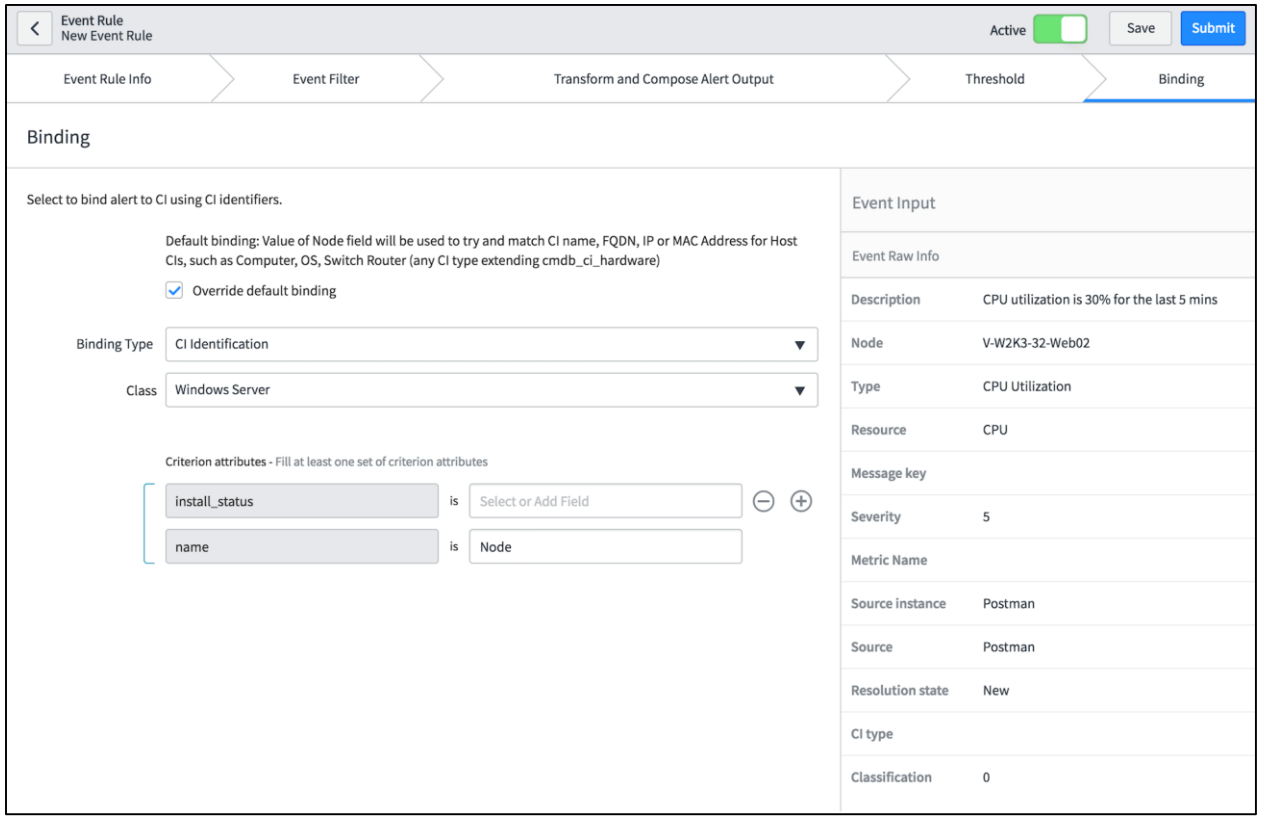
© 2017 ServiceNow All Rights Reserved

Binding Alerts to CIs

© 2017 ServiceNow All Rights Reserved

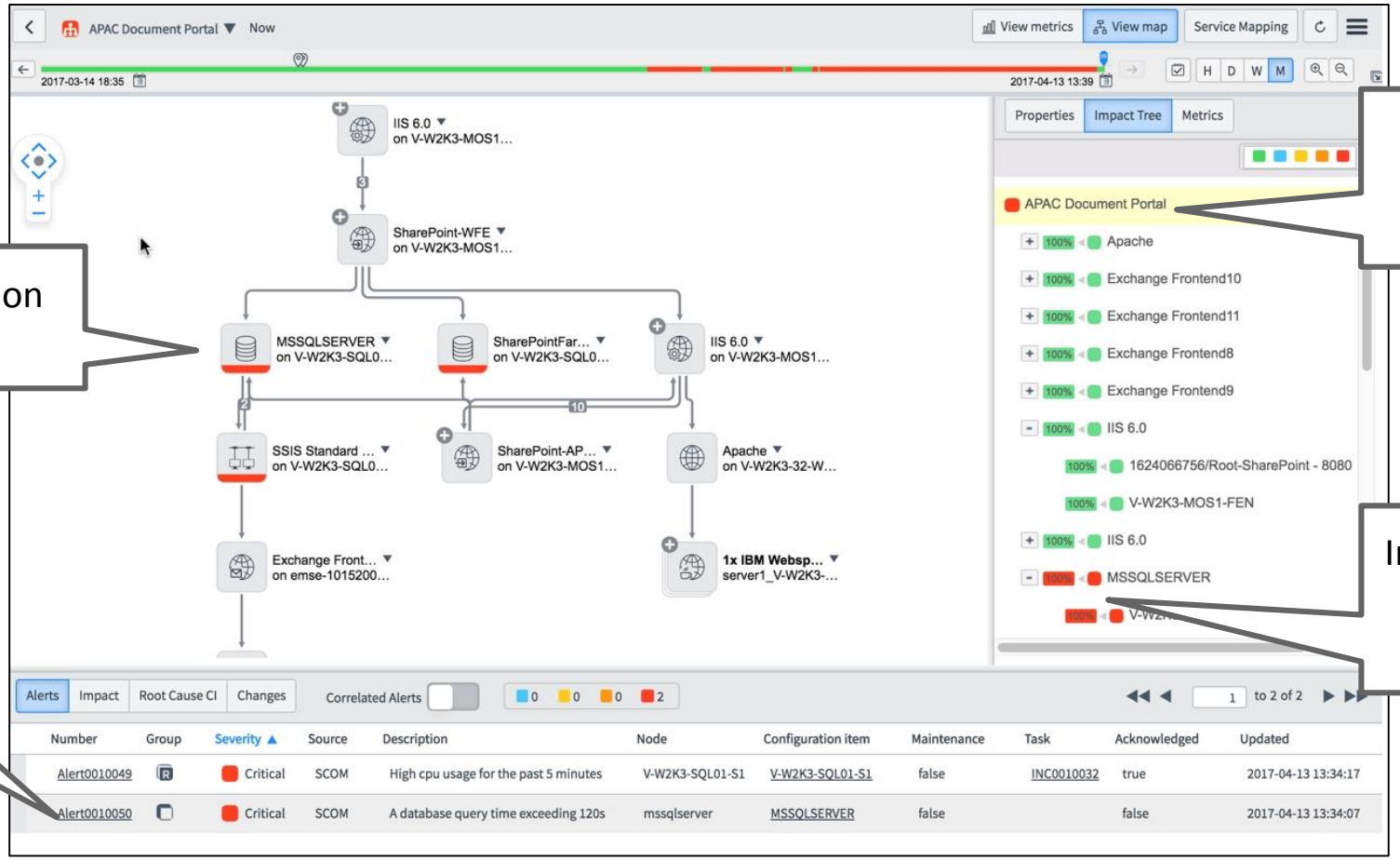
Binding to CIs

- Associating an Alert with a CI stored in the ServiceNow CMDB allows you to monitor the availability of business services related to the CI.
- Use an Event Rule to specify binding conditions that are used by the Identification Engine.



© 2017 ServiceNow All Rights Reserved

Service Availability Monitoring



Impacting CI displayed on service health map

Service availability status updated by impact calculation

Impact calculated using CI relationships in service map

Alert bound to CI via Event Rule

© 2017 ServiceNow All Rights Reserved

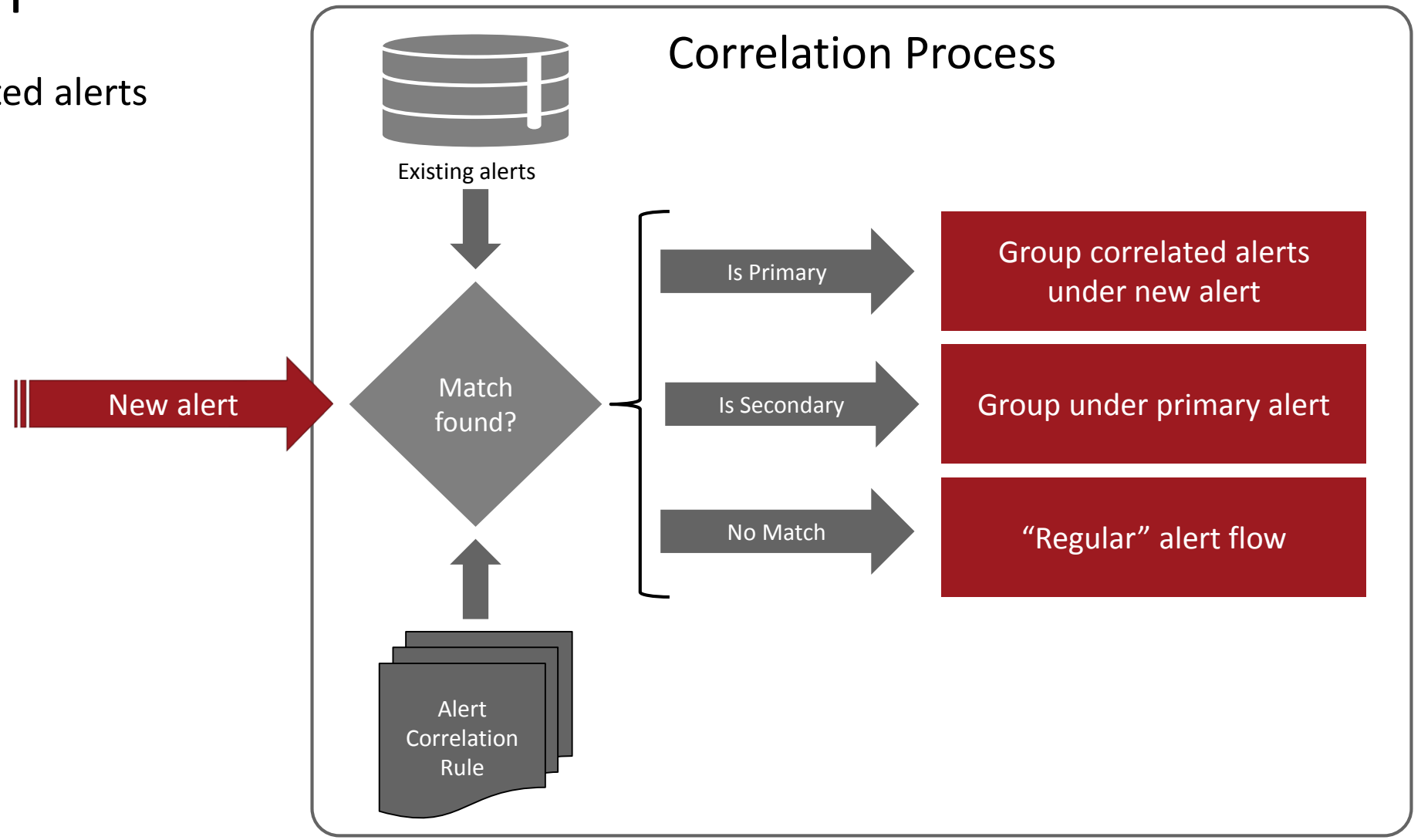

S-Mart
REALLY?! YOU'RE DOING THIS NOW?
LAB 3 WILL ONLY TAKE ME A MINUTE...

Correlation Rules

© 2017 ServiceNow All Rights Reserved

Alert Correlation

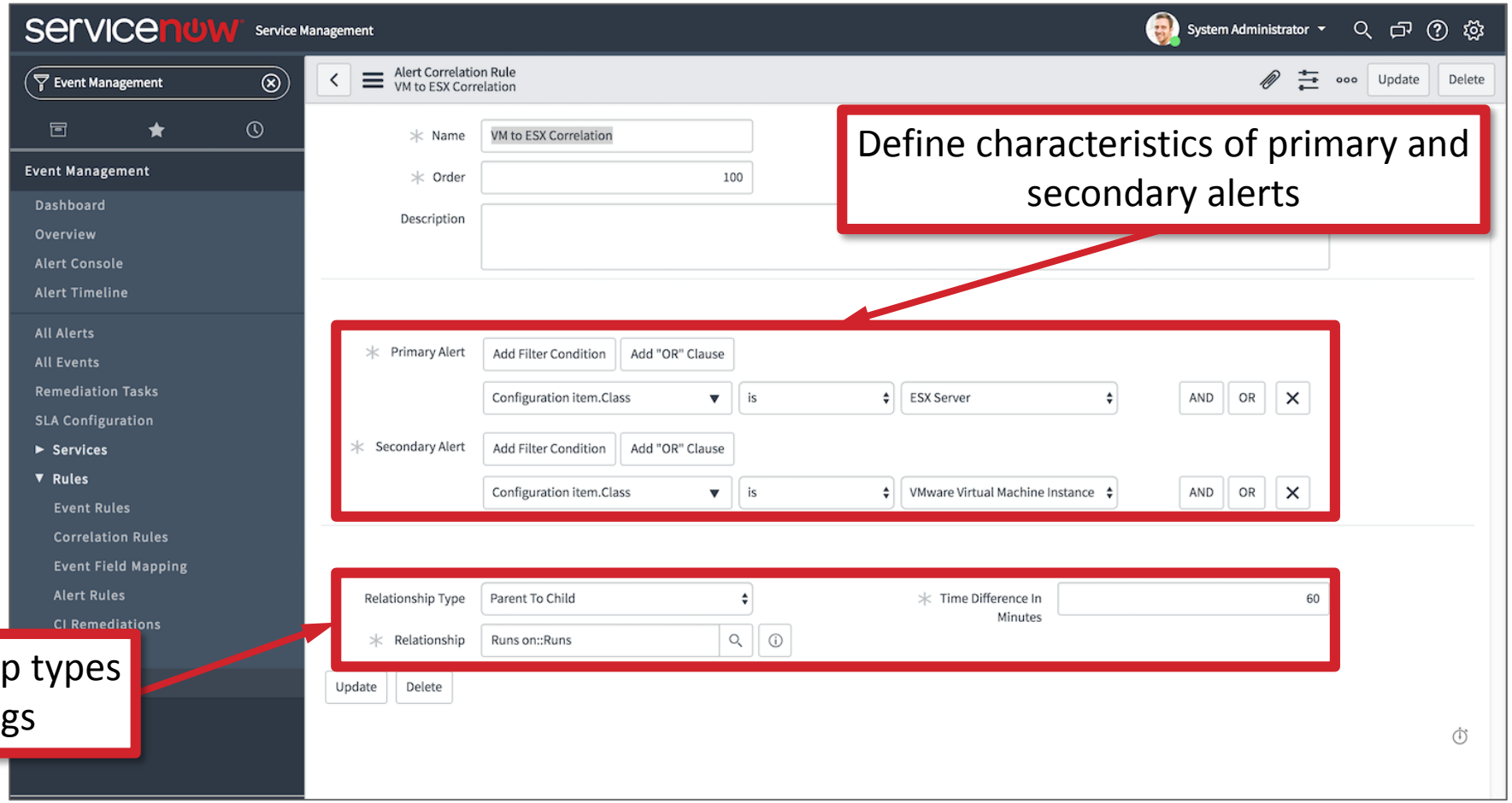
Automatically group related alerts using Correlation Rules



© 2017 ServiceNow All Rights Reserved

Correlation Rules

Flexible configuration supports CI relationships, same CI scenario or no relationship



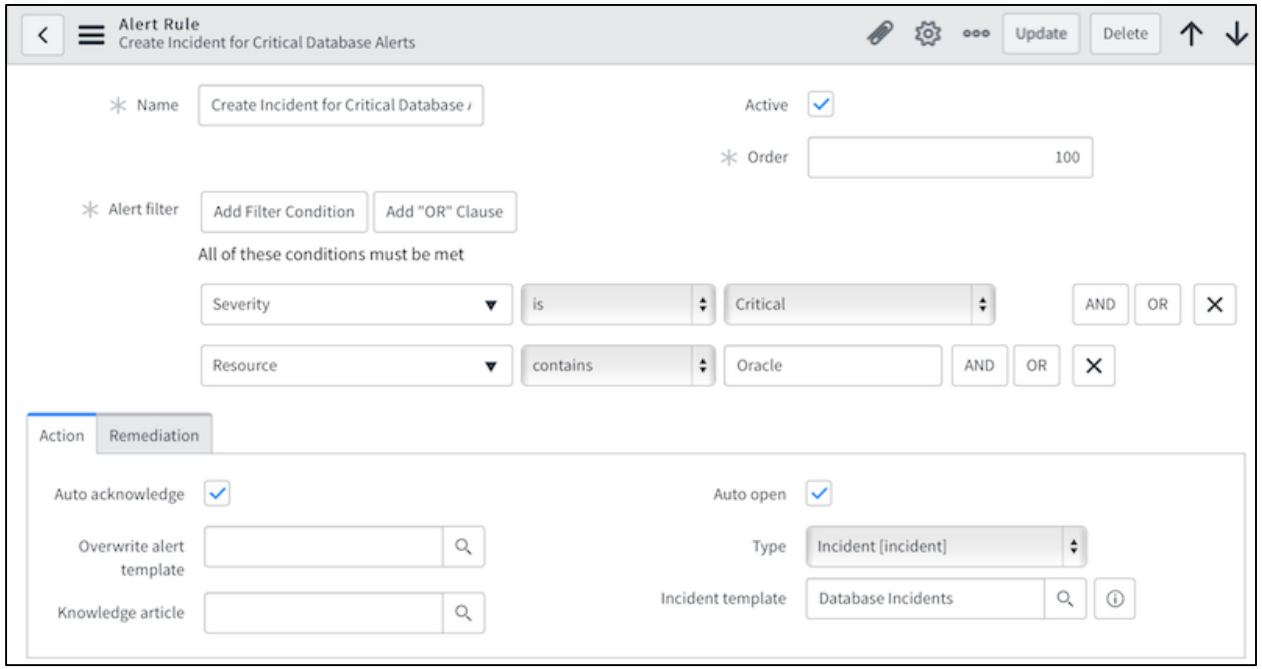
© 2017 ServiceNow All Rights Reserved

Alert Action Rules

© 2017 ServiceNow All Rights Reserved

Alert Action Rules

- Create Incidents, Changes, Requests… virtually any task in ServiceNow.
- Associate Knowledge articles
- Auto-acknowledge
- Overwrite Alert fields using Alert Templates
- Trigger remediation workflows – manually or automatically
- Combine multiple steps in a single Alert Action Rule



© 2017 ServiceNow All Rights Reserved


GREAT. ANOTHER LAB.
IT LOOKS...
...LIKE LAB 4

Lab 4



- **Page 41, Step 4** in the Check the Results section should read:

  Open the Alert, note the value of the **Role in Group** field (add the field to the Alert form if it isn't visible), and scroll down the page to see the list of correlated alerts. Note the value of the **Group** column for the correlated Alert – it should be set to **Secondary**.

- **Page 43, Step 4** should read:

  Go to the **All Alerts** list view and close and delete the primary and secondary correlated alerts. Navigate to **Incident > Open** and delete the incidents with the following **Short description** values:

  – A database query time exceeding 120s
  – High cpu usage for the past 5 minutes

© 2017 ServiceNow All Rights Reserved

Top Takeaways

1

Event integration (typically a one-time activity) is straightforward with ServiceNow

2

The Event Rule Designer takes the hard work out of creating Event Rules

3

Alerts + CIs = Business Impact

Faster time to prioritize and resolve issues

© 2017 ServiceNow All Rights Reserved

Q & A

Vinh Tran
Solution Architect, ITOM Practice
ServiceNow

Tony Branton
Sr. Advisory Solution Architect, ITOM Practice
ServiceNow

#Know17 | http://clabs.link/lab131985

© 2017 ServiceNow All Rights Reserved


CLAP
CLAP
CLAP
THAT WAS AWESOME.

Thank You

Lab Sponsored by Amazon Web Services



Vinh Tran
Solution Architect, ITOM Practice
ServiceNow

Tony Branton
Sr. Advisory Solution Architect, ITOM Practice
ServiceNow

#Know17 | http://clabs.link/lab131985

© 2017 ServiceNow All Rights Reserved