knowledge15
April 19–24, 2015 • Mandalay Bay • Las Vegas, NV

Lab Guide

Event Management:

Consolidate and Manage Alerts in One Console

Roland Shepherd & Tony Branton

Default Login / Password:
admin / Knowledge15
itil / Knowledge15
employee / Knowledge15

This

Page

Intentionally

Left

Blank

Event Management Application Overview

This lab explains the Event Management application menu and Overview dashboard.

Lab 1.1: Event Management application menu

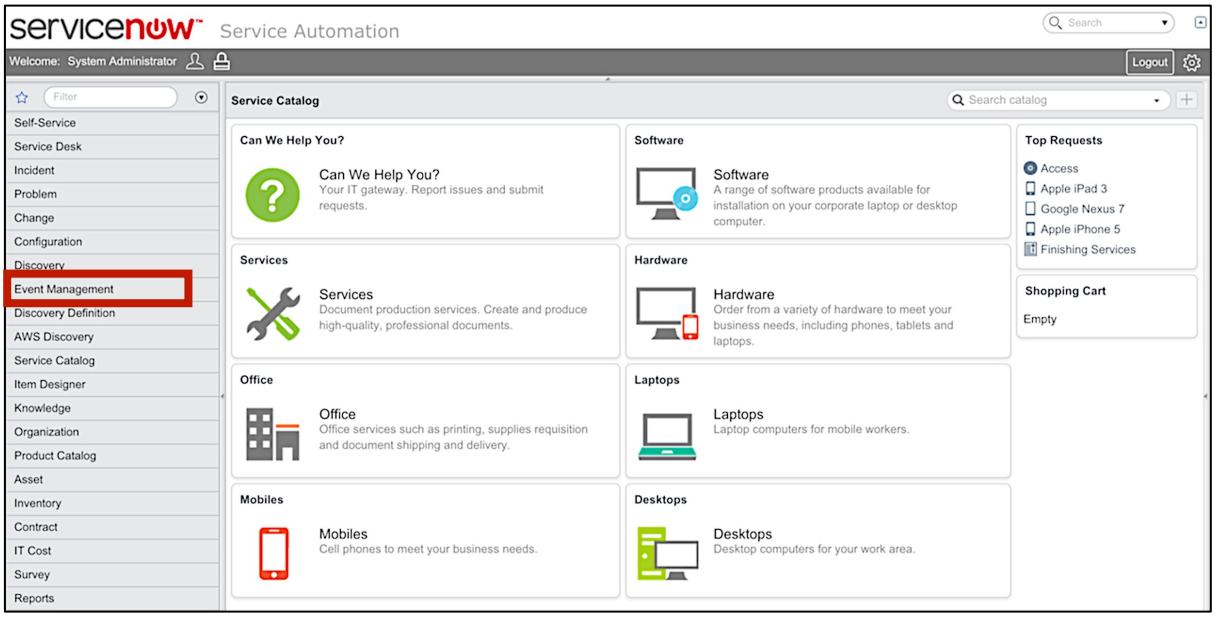
Lab 1.2: Event Management Overview dashboard

Lab 1.3: Active Alerts list view

Lab 1
Event Management Application Overview

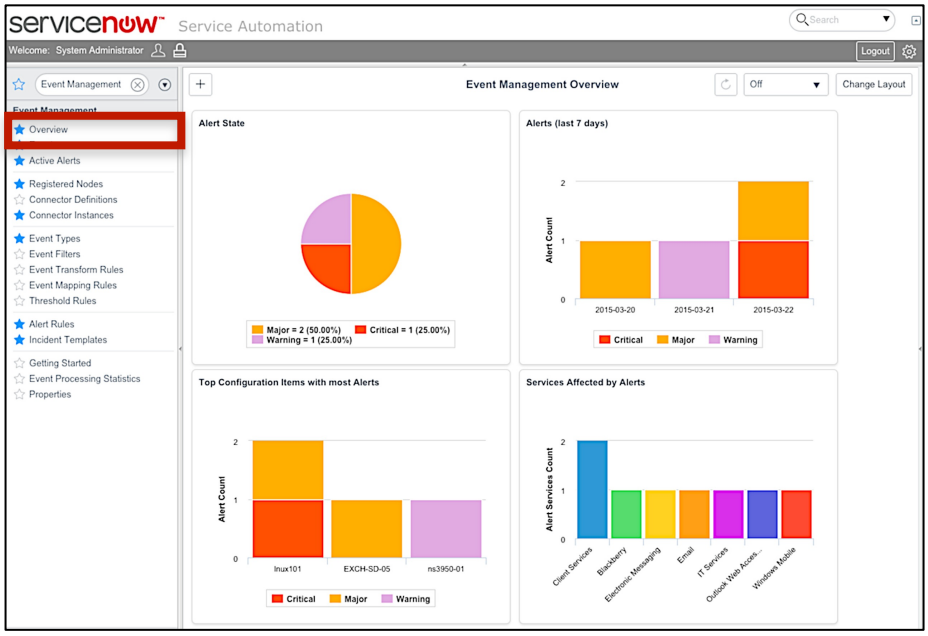
Lab 1.1: Event Management Application Menu

1. Navigate to the unique instance URL provided.
2. Log on with provided credentials.
3. While logged into your lab instance, enter event management in the navigator to locate the **Event Management** application.

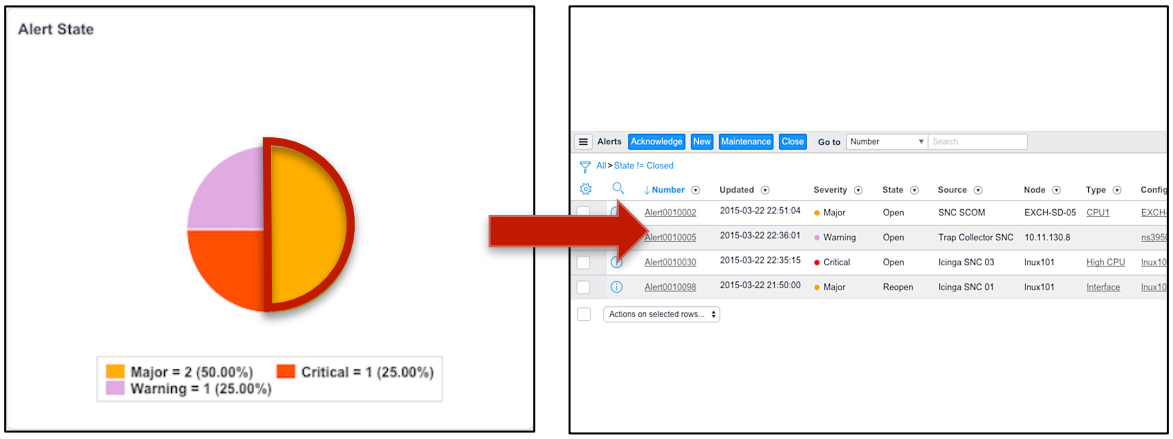


©2015 ServiceNow, Inc. All rights reserved.

4. Open the **Event Management Overview** dashboard by clicking on the menu option.

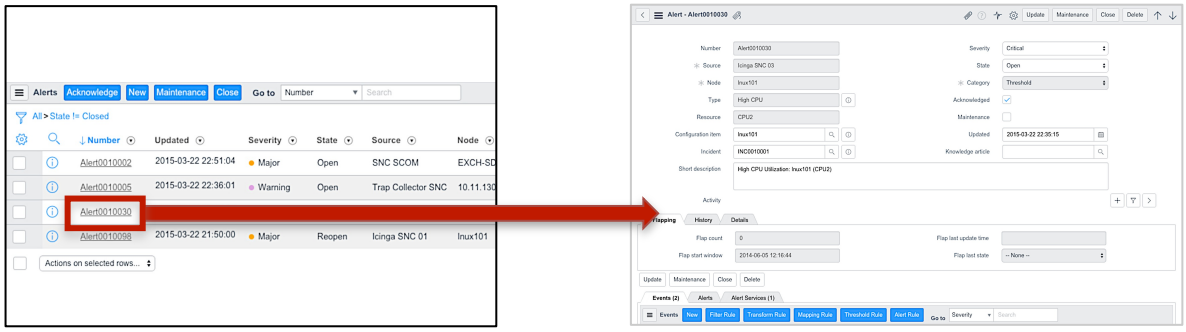


5. Click one of the segments in the **Alert State** pie chart to drill down to the related Alerts.

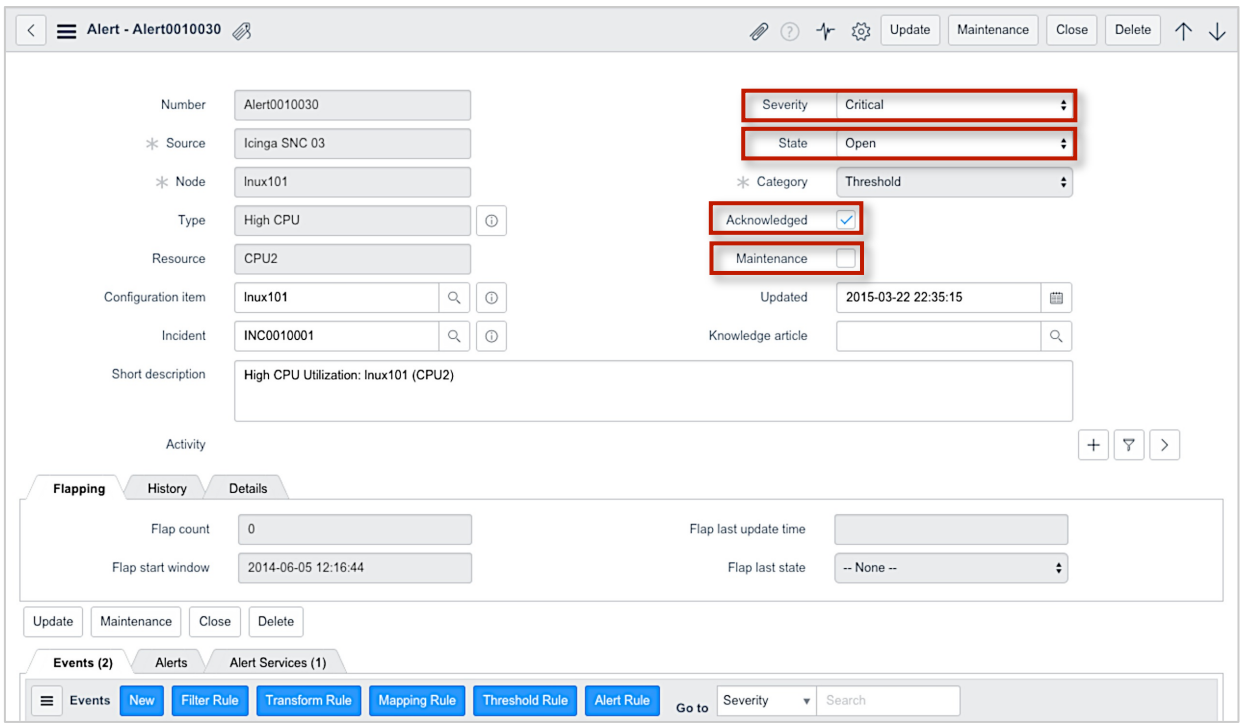


®2015 ServiceNow, Inc. All rights reserved.

6. Click an **Alert** to open and view an Alert record.

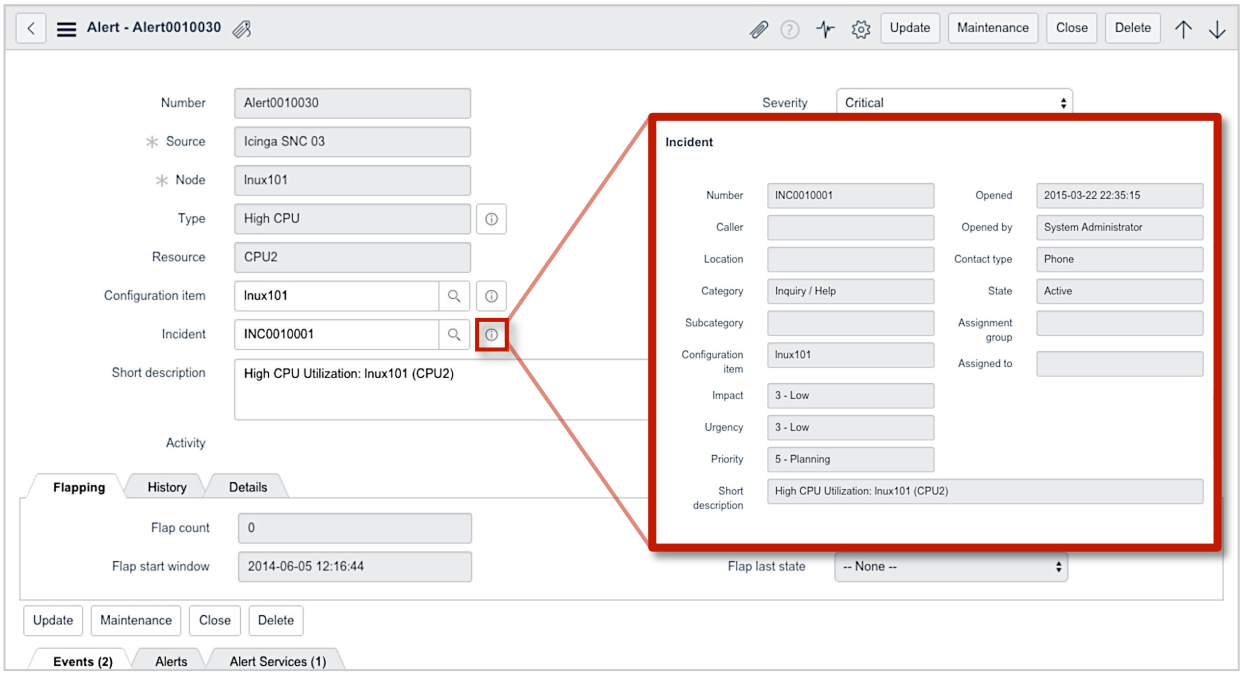


7. Click on the **Severity** and **State** field drop-down boxes to see the list of choices. Also note the **Acknowledged** and **Maintenance** fields.

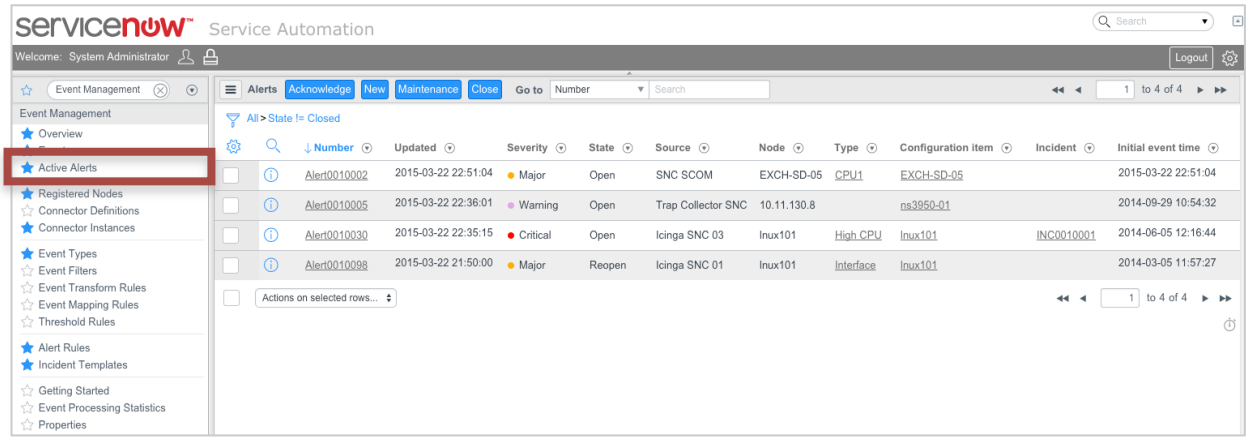


®2015 ServiceNow, Inc. All rights reserved.

8. Hover over the information buttons for the **Incident** field to view the related Incident record.



9. Click **Active Alerts** from the Event Management menu in the navigator to open the **Active Alerts** list view.

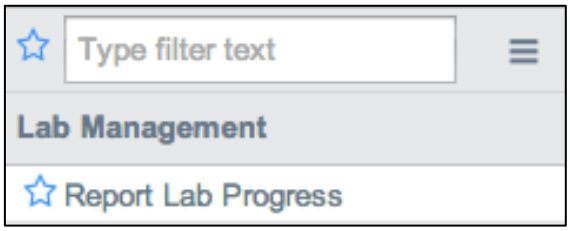


10. Note the **Acknowledge** and **Maintenance** action buttons in the view.

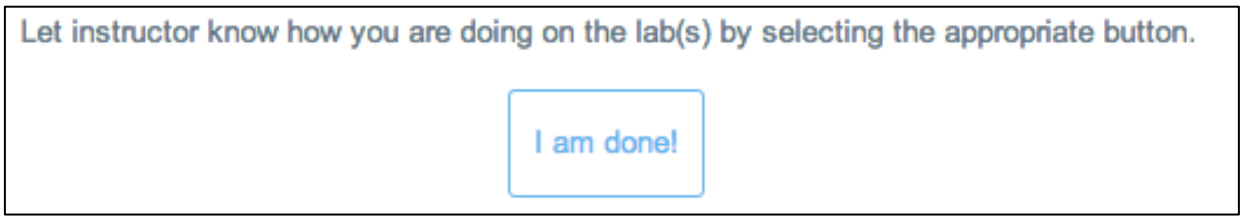
®2015 ServiceNow, Inc. All rights reserved.

Progress Report

1. Navigate to **Lab Management> Report Lab Progress**.



2. Click **I am done!**



®2015 ServiceNow, Inc. All rights reserved.

Event Integration

This lab explains how to integrate ServiceNow and Microsoft SCOM (System Center Operations Manager) to collect events and ensure events are bound to CIs.

Lab 2.1: Create an Event Connector Instance for SCOM

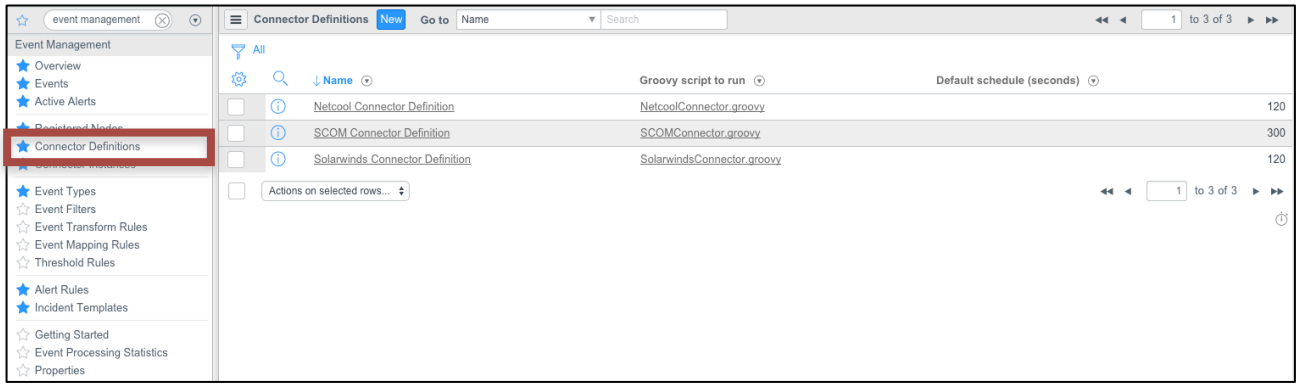
Lab 2.2: Register Nodes

Lab 2
Event
Integration

Lab 2.1: Create a Connector Instance for SCOM

This lab explains how to configure a connection to Microsoft SCOM to collect events.

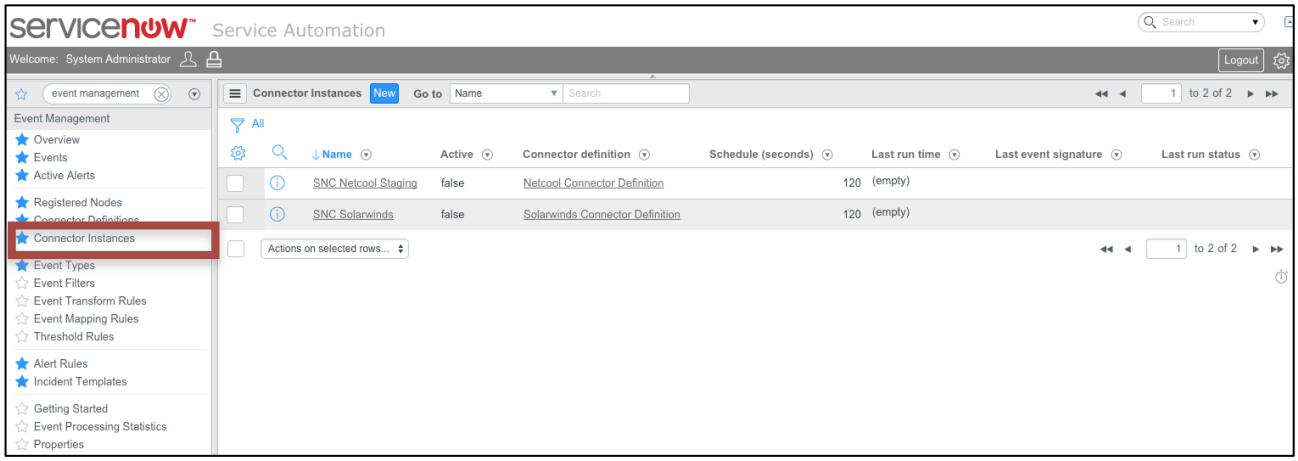
1. Navigate to **Event Management** > **Connector Definitions** to view the list of OOTB connectors.



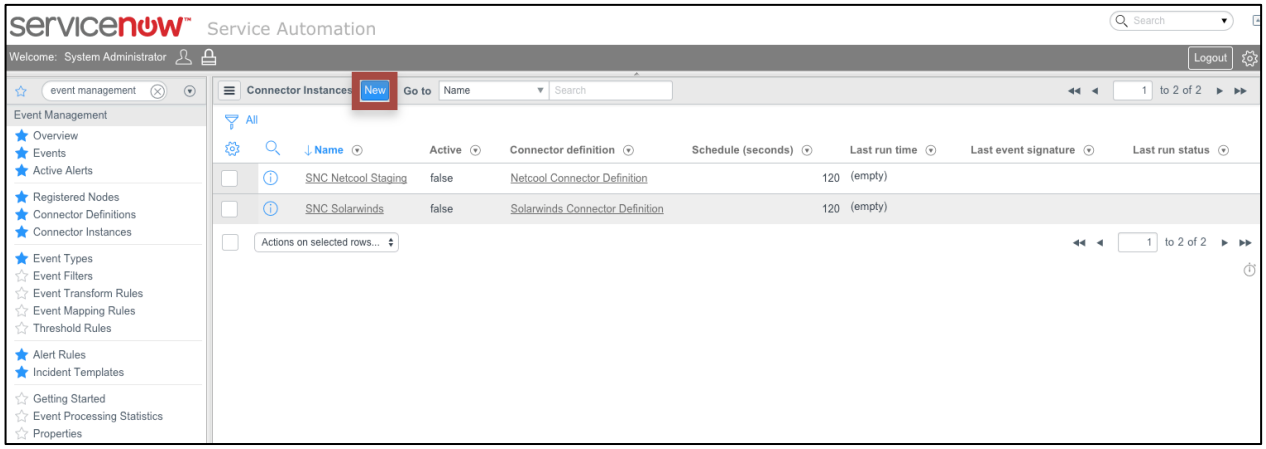
Note the available connector definitions, including one for SCOM.

©2015 ServiceNow, Inc. All rights reserved.

2. Navigate to **Event Management** > **Connector Instances**.



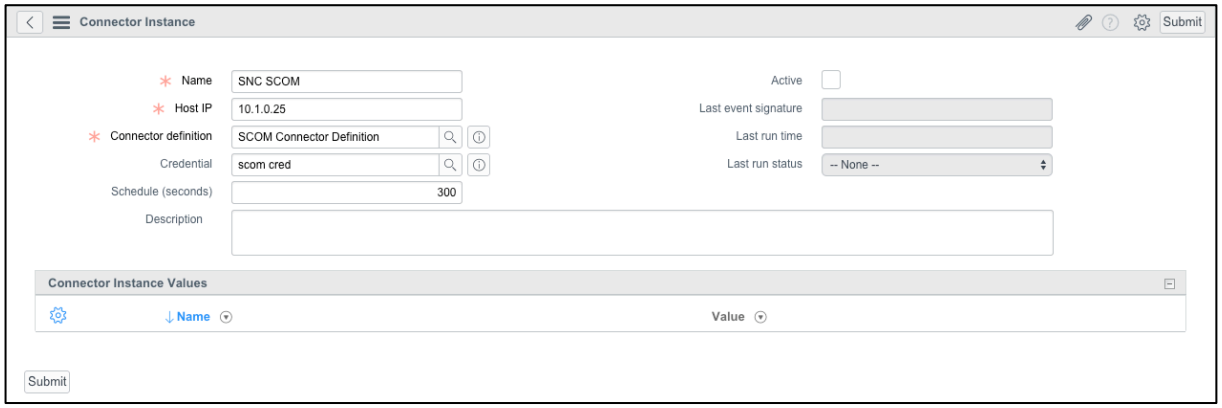
3. Click the **New** action button.



®2015 ServiceNow, Inc. All rights reserved.

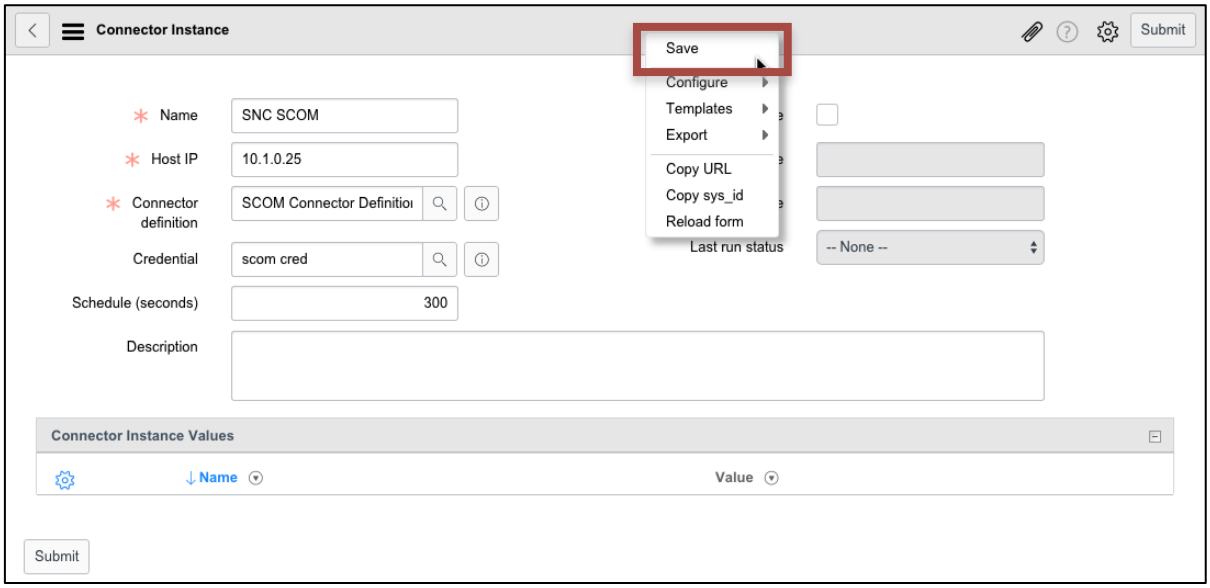
4. Enter the following information for the Connector Instance:

   Name: **SNC SCOM**
   Host IP: **10.1.0.25**
   Connector definition: **SCOM Connector Definition**
   Credential: **scom creds**
   Schedule (seconds): **300**



Note: The **Active** checkbox is *not* enabled in this lab since we do not have a SCOM environment available.

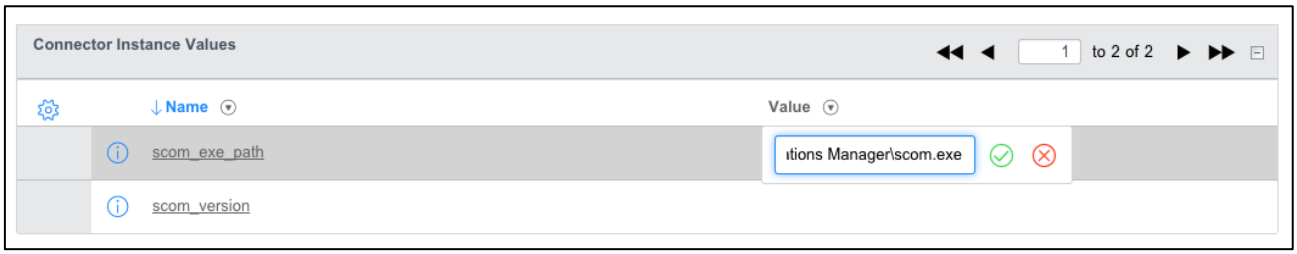
5. Right-click on the grey bar at the top of the form and select **Save** from the pop-up menu.



©2015 ServiceNow, Inc. All rights reserved.

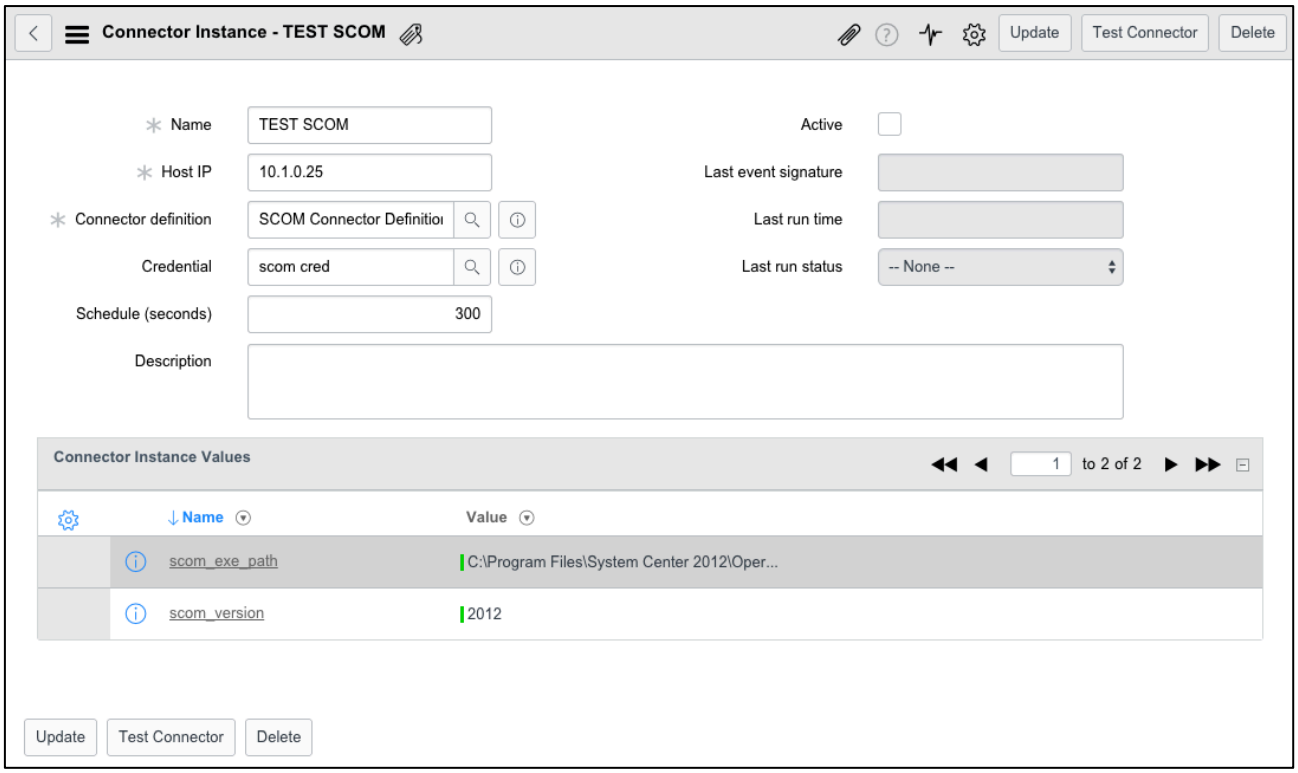
6. You will see two entries appear in the Connector Instance Values section. Double-click in the **Value** column in the row with the name **scom_exe_path** and enter:

   C:\Program Files\System Center 2012\Operations Manager\scom.exe



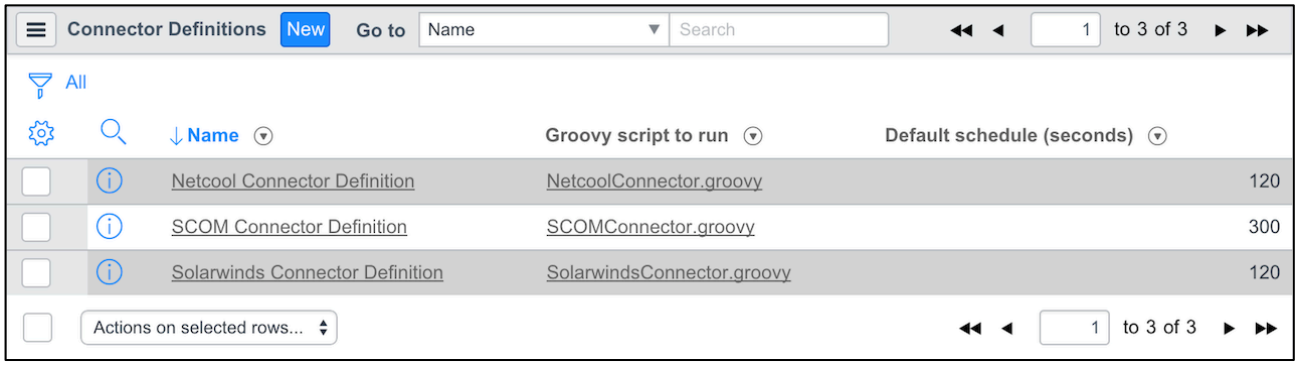
7. Double-click on the **Value** column in the row with the name **scom_version** and enter: **2012**

8. The Connector Instance should now look as shown below:



©2015 ServiceNow, Inc. All rights reserved.

9. Click on **Update** to save the SCOM Connector Instance.

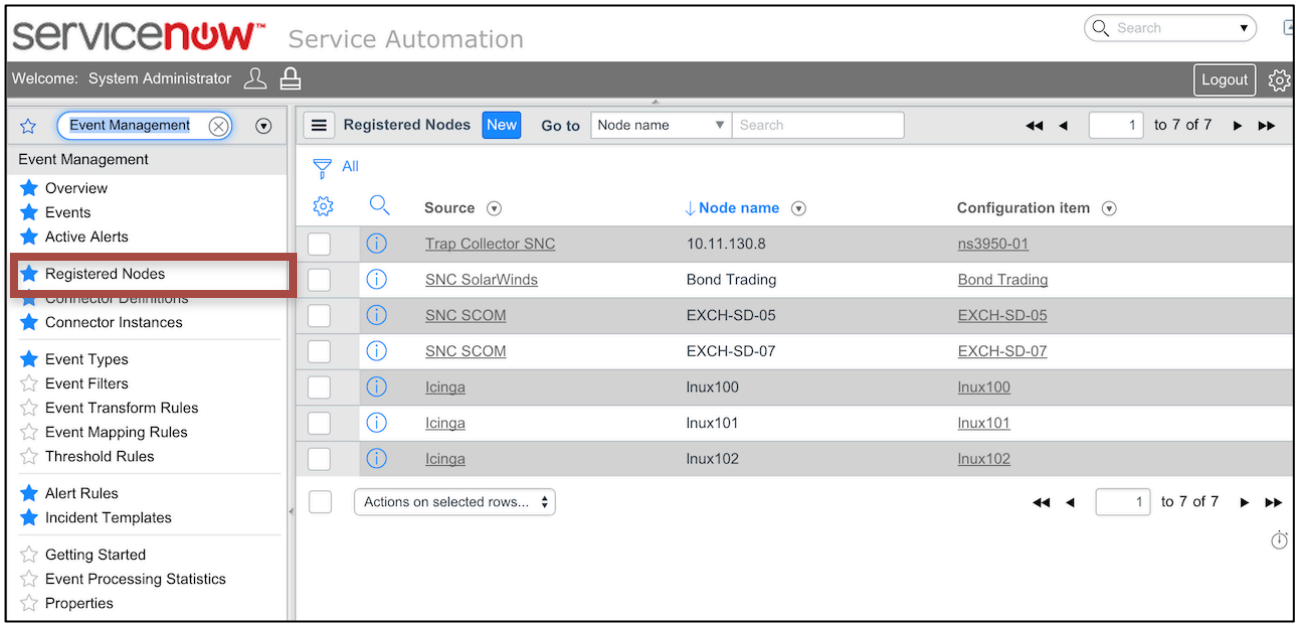


®2015 ServiceNow, Inc. All rights reserved.

Lab 2.2: Register Nodes

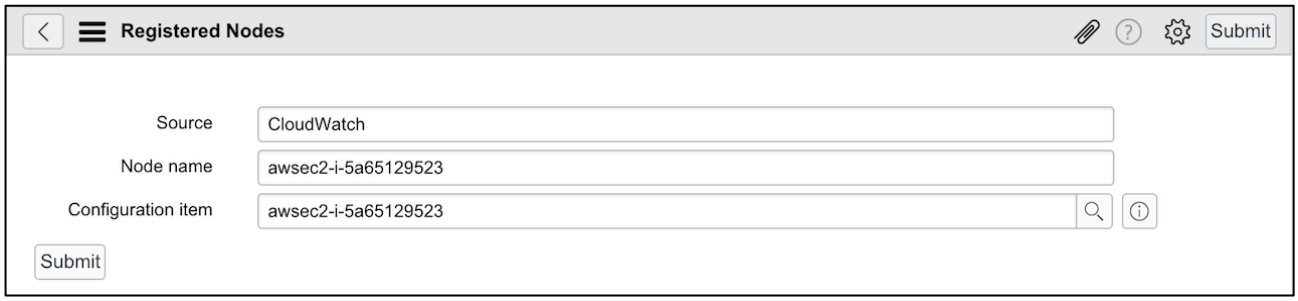
This lab explains how to register nodes allowing events and alerts to be automatically bound to CIs.

1. Navigate to **Event Management > Registered Nodes**.



2. Click the **New** action button and enter the following information in the **Register Nodes** form:

   Source: **CloudWatch**
   Node: **awsec2-i-5a65129523**
   Configuration item: **awsec2-i-5a65129523**



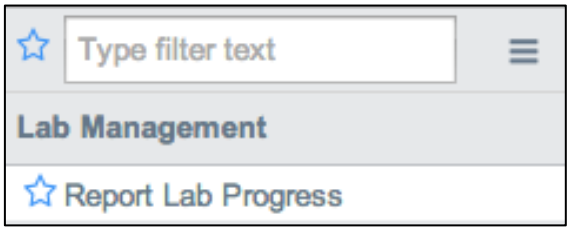
©2015 ServiceNow, Inc. All rights reserved.

3. Click on **Submit** and register another node using the information below:

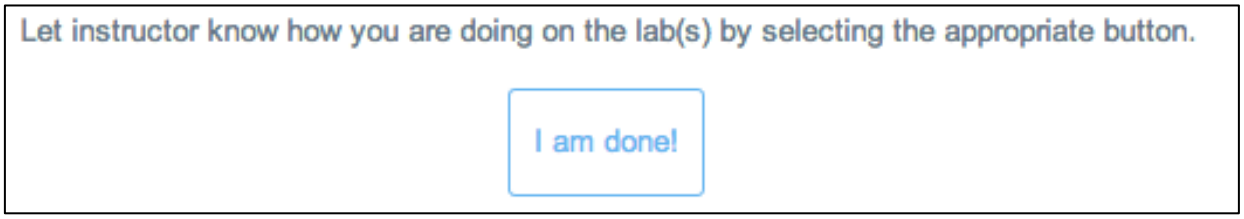
   Source: **SNC SCOM**
   Node: **SAP ORA01**
   Configuration item: **SAP ORA01**

Progress Report

1. Navigate to **Lab Management> Report Lab Progress**.



2. Click **I am done!**



©2015 ServiceNow, Inc. All rights reserved.

Event Processing Rules

This lab explains how to configure rules to filter events, and transform and map events to produce meaningful alerts.

Lab 3.1: Event Filter Rule

Lab 3.2: Event Transform Rule

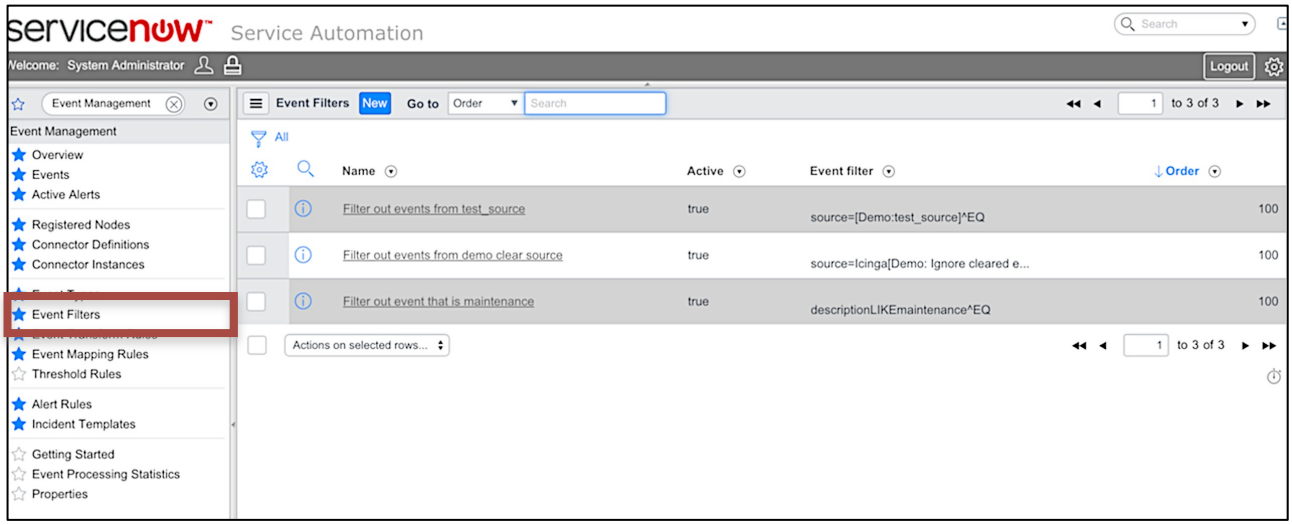
Lab 3.3: Event Mapping Rule

Lab 3
Event
Processing
Rules

Lab 3.1: Event Filter Rule

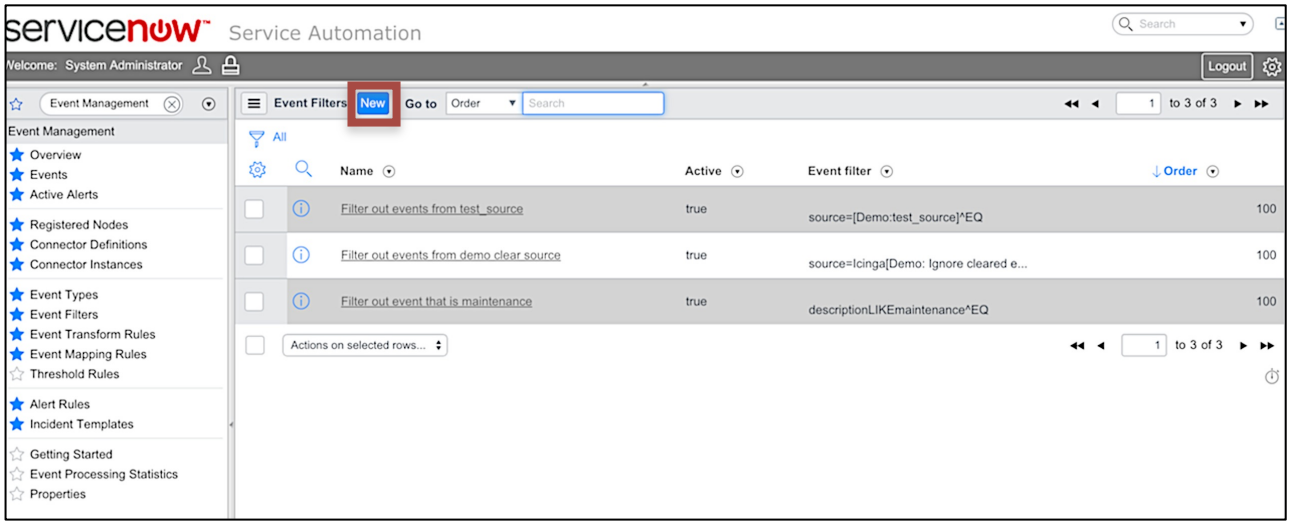
Event filter rules can be configured quickly to filter irrelevant events. This lab explains how to configure a rule to filter out events for WebTrafficAudit resource and Info severity.

1. Navigate to **Event Management > Event Filters**.



®2015 ServiceNow, Inc. All rights reserved.

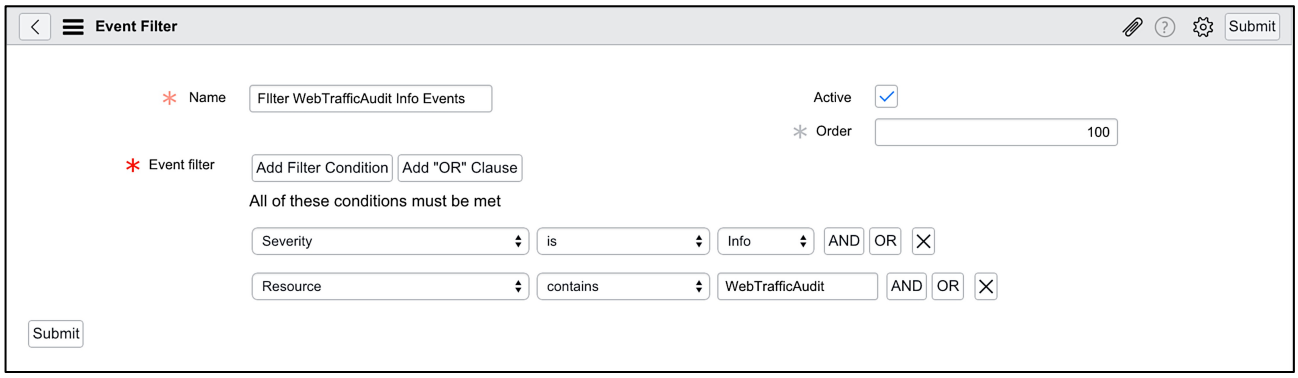
2. Click on the **New** action button to create a new Event Filter rule.



3. Configure the rule with the following information:

   Name: **Filter WebTrafficAudit Info Events**
   Event filter: **Severity is Info AND**
   Resource contains WebTrafficAudit

   The rule should look like the one in the example.



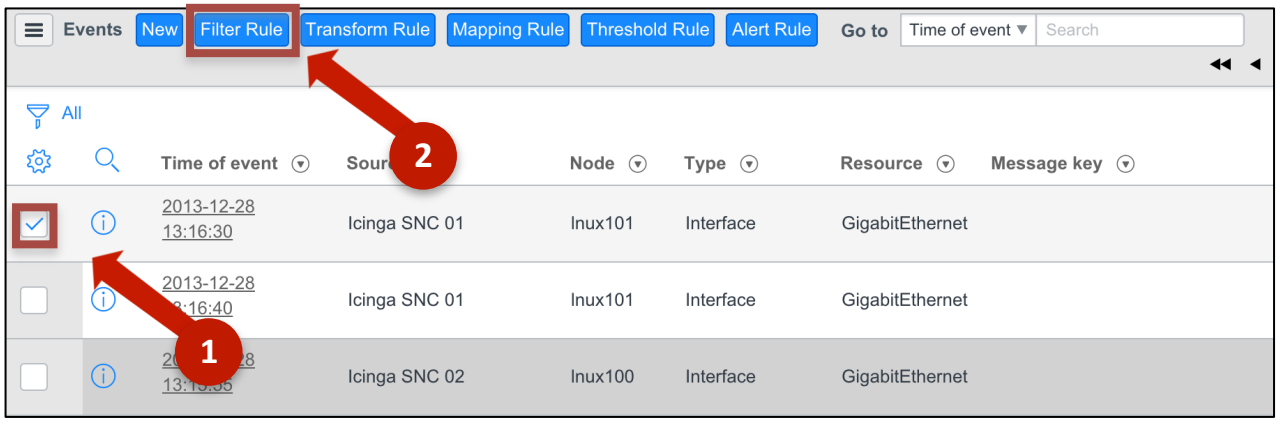
4. Click on **Submit** to save the event filter rule.

©2015 ServiceNow, Inc. All rights reserved.

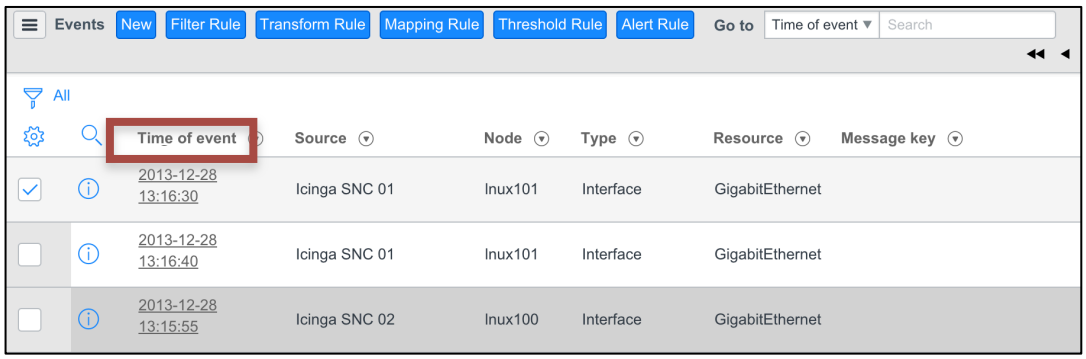
5. Now generate some events to test the filter. Navigate to **Event Management > Events**. Click **All** in the list view filter.



6. Select an event in the list (1) and click on the **Filter Rule** action button (2).

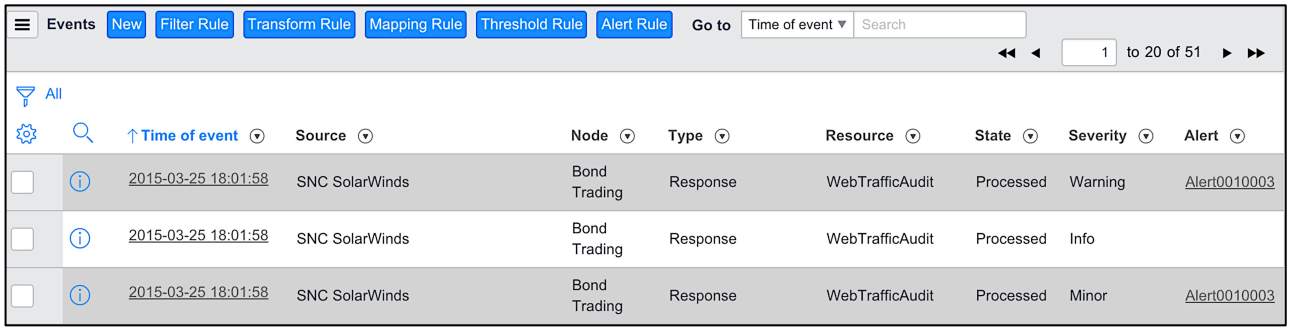


7. Sort the event list so the most recent events are at the top by clicking the **Time of event** column.



©2015 ServiceNow, Inc. All rights reserved.

8. Three events were received; however, only two of the events were associated with an Alert.

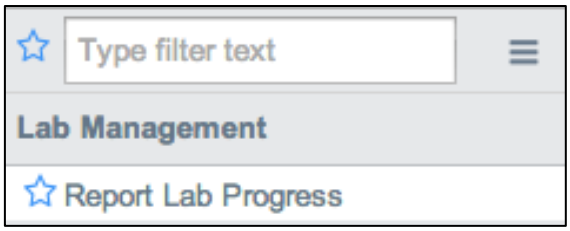


Time of event	Source	Node	Type	Resource	State	Severity	Alert
2015-03-25 18:01:58	SNC SolarWinds	Bond Trading	Response	WebTrafficAudit	Processed	Warning	Alert0010003
2015-03-25 18:01:58	SNC SolarWinds	Bond Trading	Response	WebTrafficAudit	Processed	Info	
2015-03-25 18:01:58	SNC SolarWinds	Bond Trading	Response	WebTrafficAudit	Processed	Minor	Alert0010003

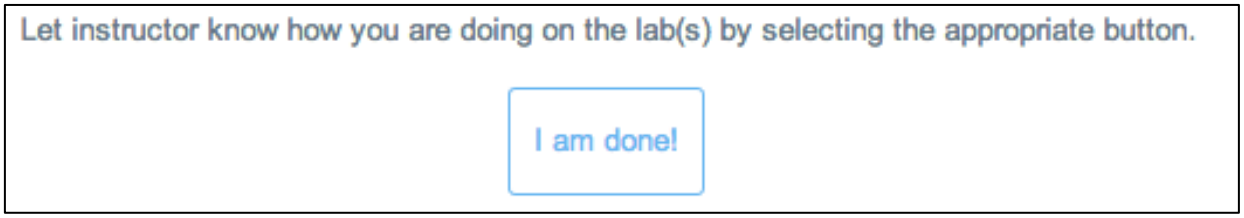
The first event received created a new Alert, the second event received matched the filter rule and was ignored, and the third event updated the Alert created by the first event.

Progress Report

1. Navigate to **Lab Management> Report Lab Progress**.



2. Click **I am done!**

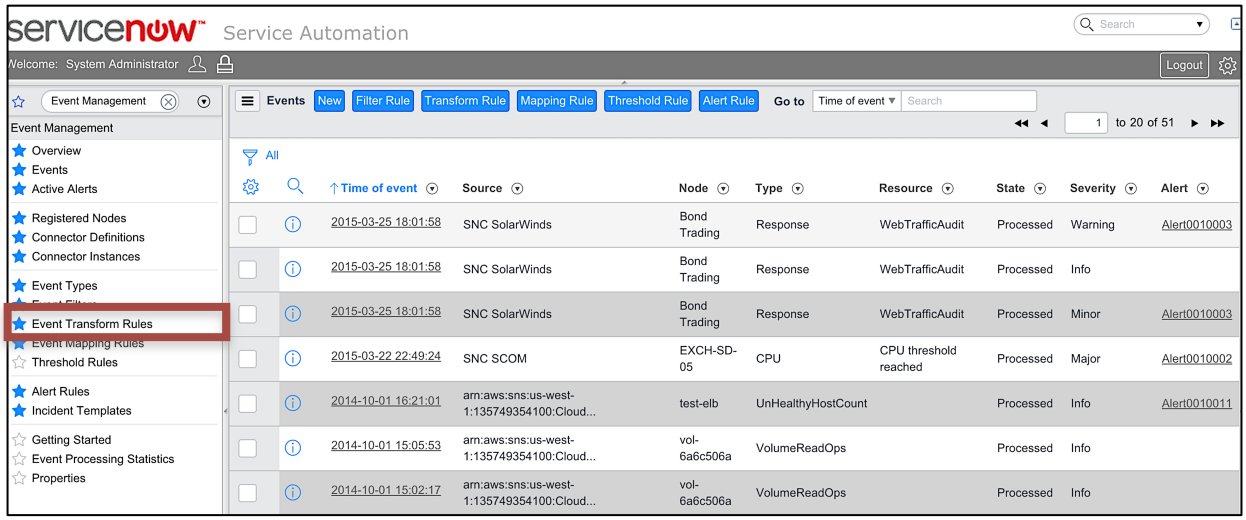


®2015 ServiceNow, Inc. All rights reserved.

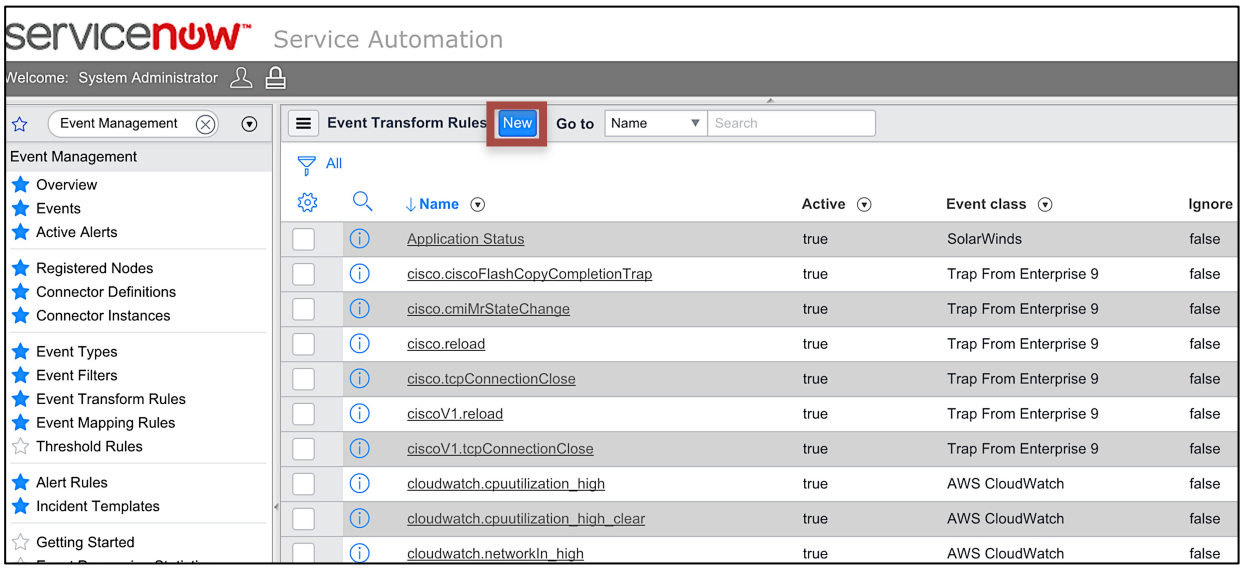
Lab 3.2: Event Transform Rule

ServiceNow Event Management can extract information from an event that matches specific criteria to create meaningful Alerts using Event Transform Rules. In this lab you will configure a simple Event Transform Rule and use it to process an event.

1. Navigate to **Event Management > Event Transform Rules**.

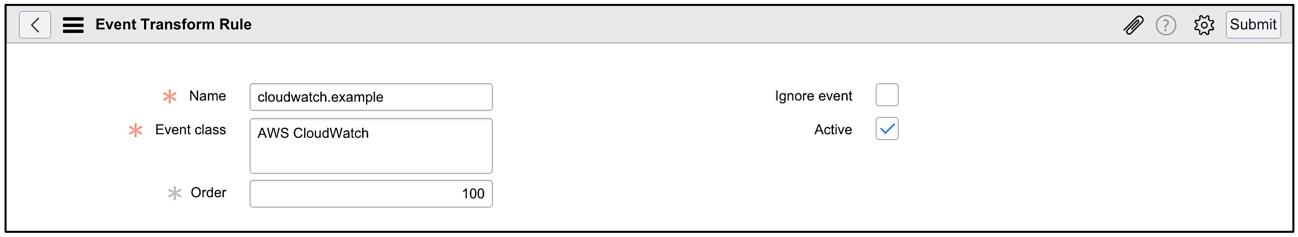


2. Click the **New** action button to create an Event Transform Rule.



©2015 ServiceNow, Inc. All rights reserved.

3. Name the Event Transform Rule **cloudwatch.example**, and use **AWS CloudWatch** as the Event class.

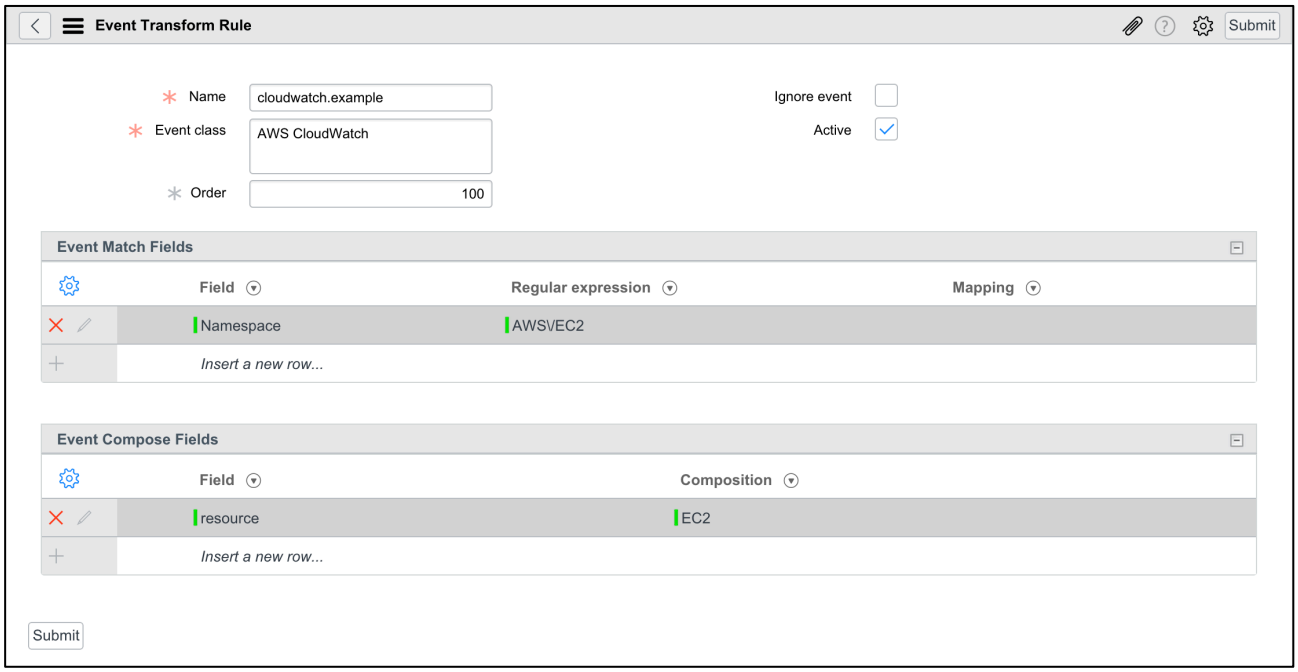


4. Click the text *Insert a new row…* under the **Field** column heading in the Event Match Fields section and type **Namespace**. Double-click in the same row under the **Regular expression** column and type **AWS\/EC2**. (“AWS back-slash forward-slash EC2”).



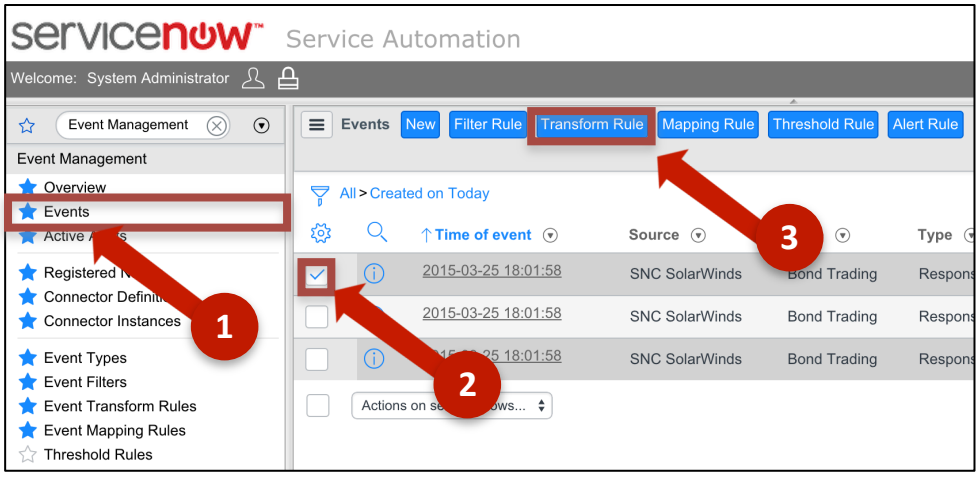
®2015 ServiceNow, Inc. All rights reserved.

5. Click the text *Insert a new row…* under the **Field** column heading in the Event Compose Fields section and type **resource**. Double-click in the same row under the **Composition** column and type **EC2**.



6. Click **Submit** to save the new Event Transform Rule.

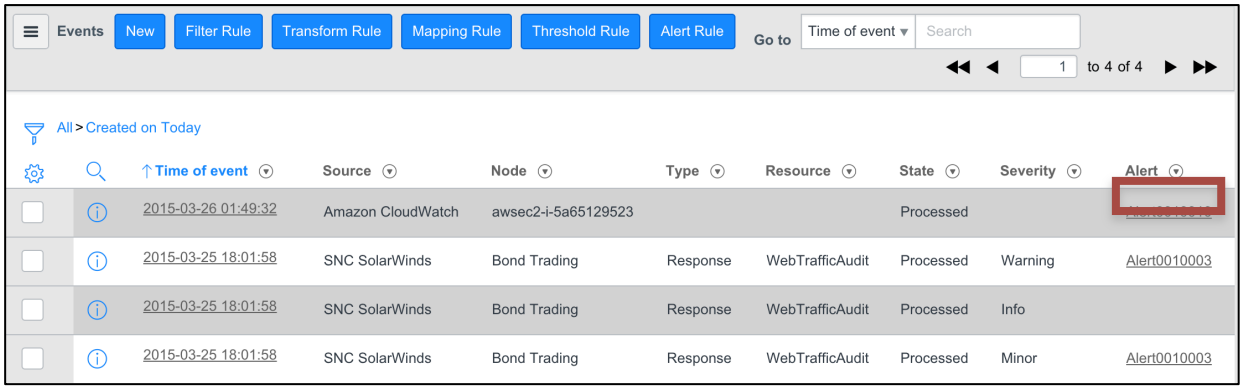
7. Navigate to **Event Management > Events** (1), select an event in the list (2) and click the **Transform Rule** action button (3).



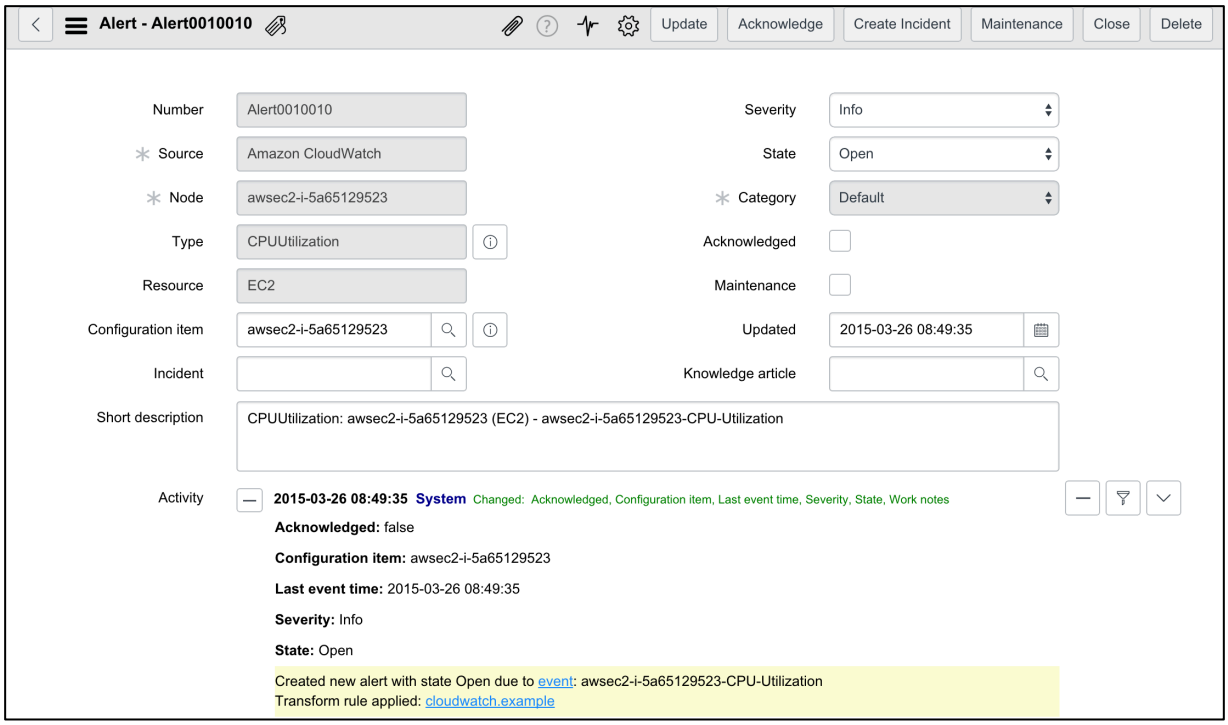
©2015 ServiceNow, Inc. All rights reserved.

8. Wait a few seconds. Then click on the List controls button (≡) and select **Refresh List** from the pop-up menu to refresh the Events list. An Alert appears in the Alert column of the list view when the event is processed. If it does not appear, refresh the list.

9. An event sent from Amazon CloudWatch was processed by the Event Transform Rule and raised an Alert. Click the **Alert** link to open the Alert record.



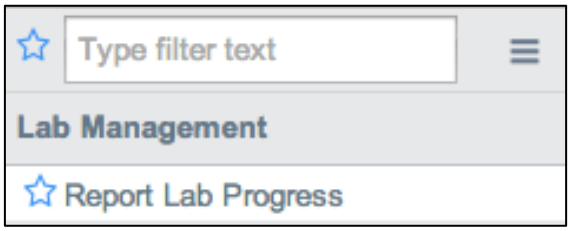
10. The Activity journal field shows the Transform rule that was applied when the event was processed to create the Alert.



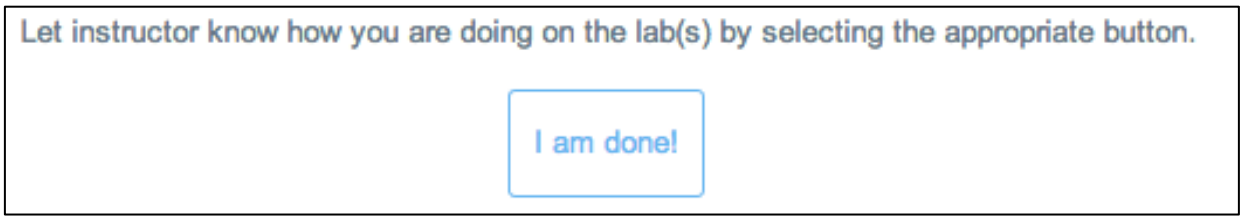
©2015 ServiceNow, Inc. All rights reserved.

Progress Report

1. Navigate to **Lab Management> Report Lab Progress**.



2. Click **I am Done!**

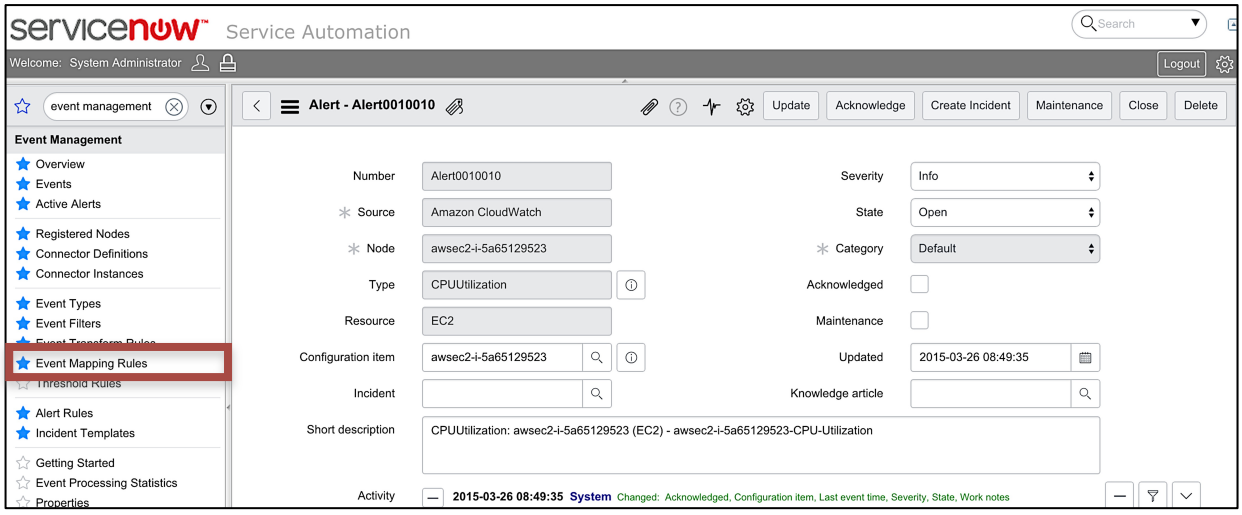


®2015 ServiceNow, Inc. All rights reserved.

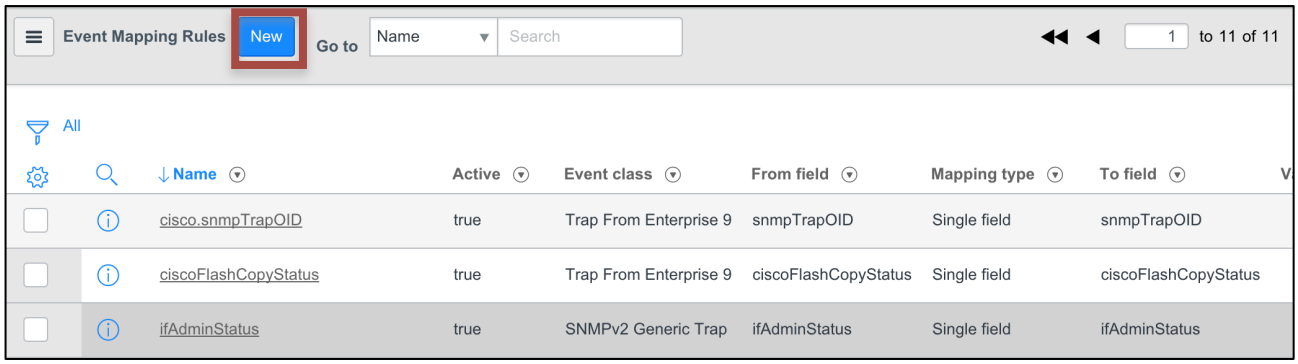
Lab 3.3: Event Mapping Rule

ServiceNow Event Management can substitute values for information included in an Event to provide consistency in Alert fields. This lab explains how to configure a simple Event Mapping Rule and use it to process an event.

1. Navigate to **Event Management > Event Mapping Rules**.



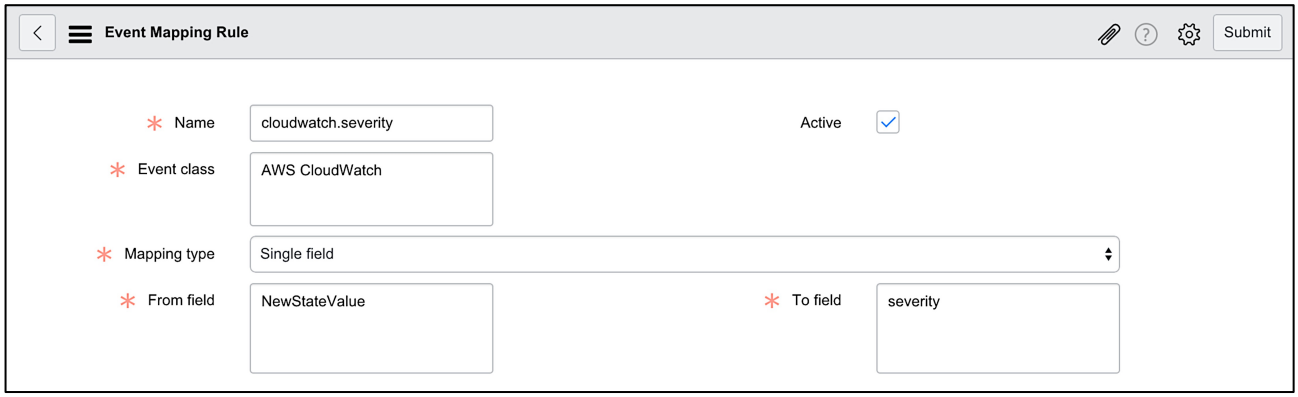
2. Click the **New** action button to create an Event Mapping rule.



©2015 ServiceNow, Inc. All rights reserved.

3. Enter the following information in the Event Mapping Rule form:

   Name: **cloudwatch.severity**
   Event class: **AWS CloudWatch**
   Mapping type: **Single field**
   From field: **NewStateValue**
   To field: **severity**

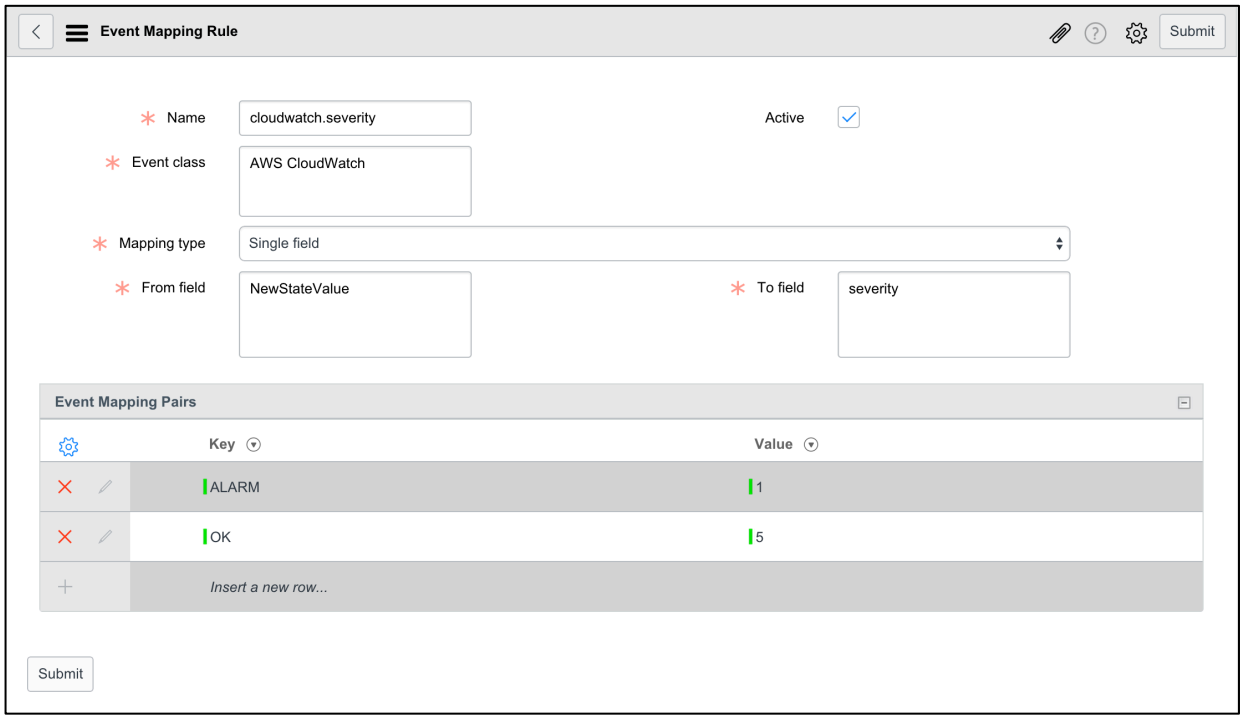


4. Click the text *Insert a new row…* under the **Key** column heading in the Event Mapping Pairs section and type **ALARM**. Double-click in the same row under the **Value** column and type **1**.

5. Click the text *Insert a new row…* under the ALARM key in the **Key** column heading in the Event Mapping Pairs section and type **OK** Double-click in the same row under the **Value** column and type **5**.

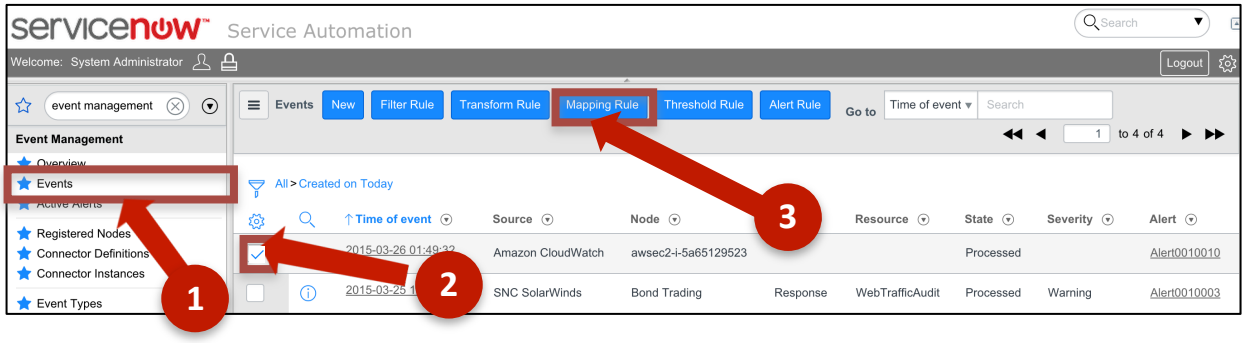
®2015 ServiceNow, Inc. All rights reserved.

6. The Event Mapping Rule should look like the example.



7. Click **Submit** to save the Event Mapping Rule.

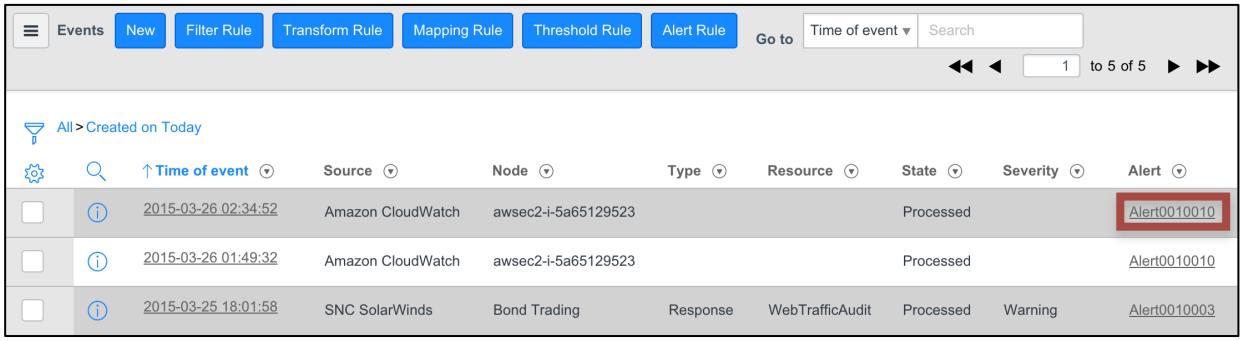
8. Navigate to **Event Management > Events** (1), select an event (2), and click the **Mapping Rule** action button (3).



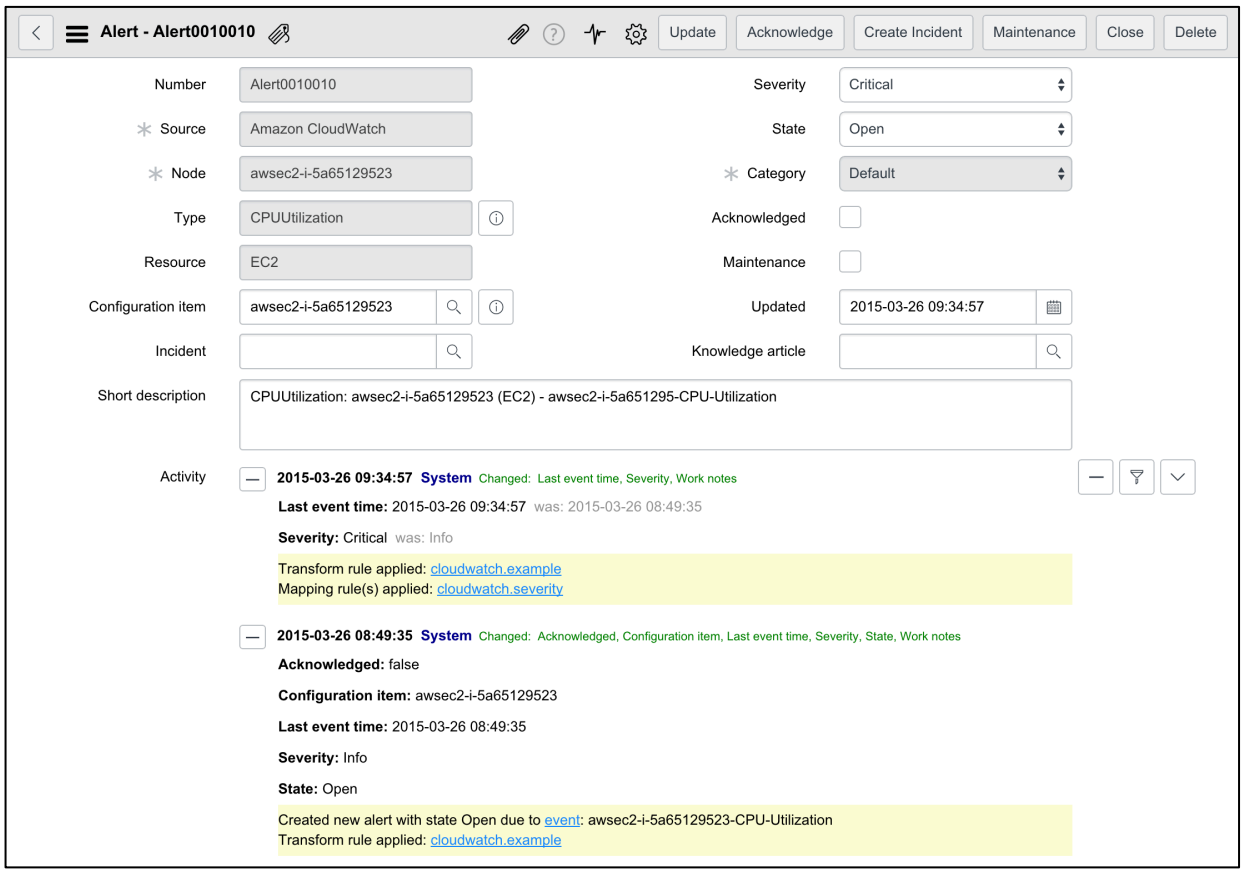
9. Wait a few seconds. Then click on the List controls button (☰) and select **Refresh List** from the pop-up menu to refresh the Events list. An Alert appears in the Alert column of the list view when the new event is processed. If it does not appear, refresh the list.

©2015 ServiceNow, Inc. All rights reserved.

10. An event sent from Amazon CloudWatch was processed by the Event Mapping Rule and updated the previous Alert. Click the **Alert** link to open the Alert record.



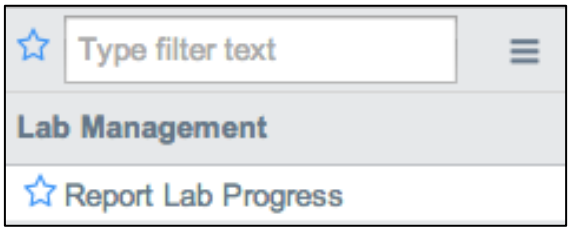
11. The Activity journal field shows the Transform and the Mapping rules applied when the event was processed to update the Alert.



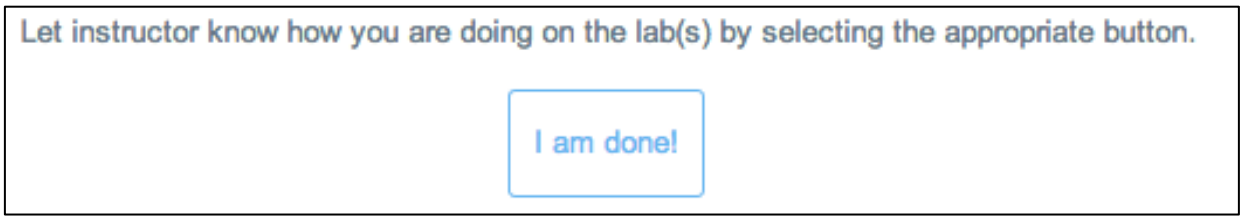
©2015 ServiceNow, Inc. All rights reserved.

Progress Report

1. Navigate to **Lab Management> Report Lab Progress**.



2. Click **I am done!**



©2015 ServiceNow, Inc. All rights reserved.

Alert Automation

This lab explains how to automate Alert actions using Alert Rules. It also explains how Incident Templates can be used to pre-fill fields in Incidents automatically created for Alerts meeting specific criteria as well as how an Alert rule can be used to automatically associate Knowledge articles with Alerts.

Lab 4.1: Incident Template

Lab 4.2: Simple Alert Rule

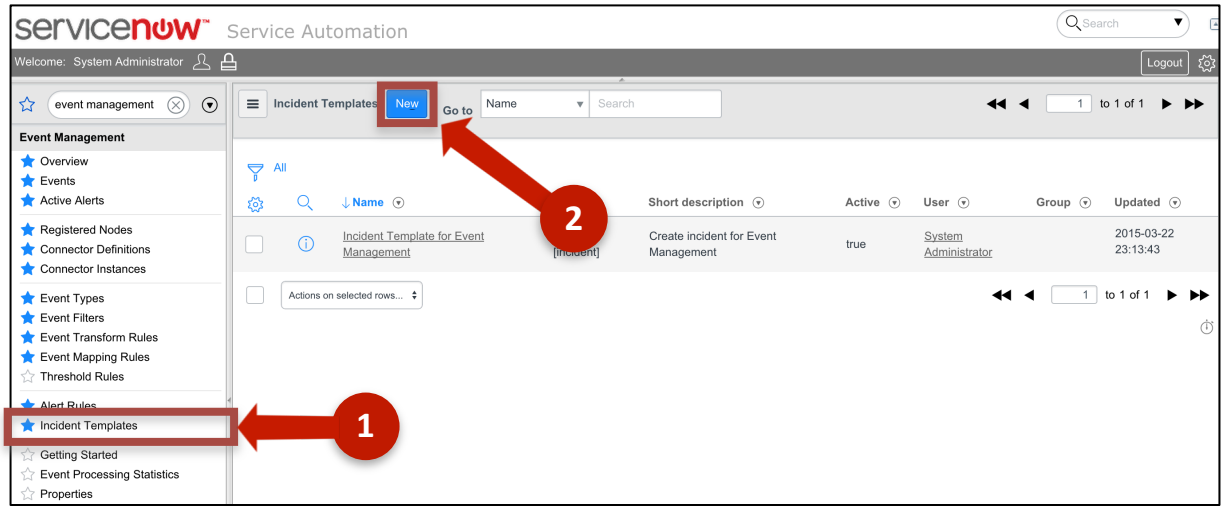
Lab 4.3: Advanced Alert Rule

Lab 4
Alert
Automation

Lab 4.1: Incident Template

Incident templates can be used to automatically pre-fill fields in Incidents. This lab explains how to configure an Incident template to be used in an Alert rule that you create in the next lab.

1. Navigate to **Event Management > Incident Templates** (1) and click **New** to create an Incident Template (2).



©2015 ServiceNow, Inc. All rights reserved.

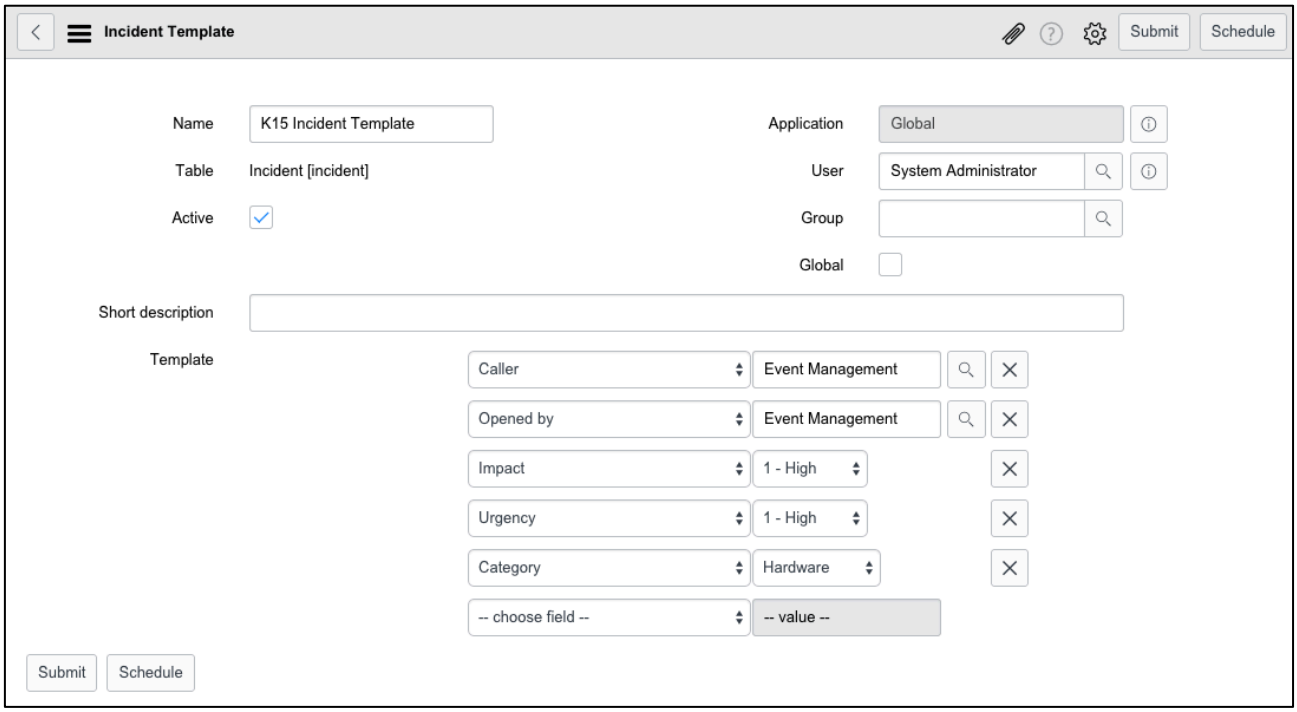
2. Name the Incident Template **K15 Incident Template**.

3. In the Template section, select **Caller** from the drop down list and set the value to Event **Management**.

4. Similarly, select the fields and set their values as follows:

   Opened by: Event Management
   Impact: 1 – High
   Urgency: 1 – High
   Category: Hardware

5. The Incident Template should look like the example.



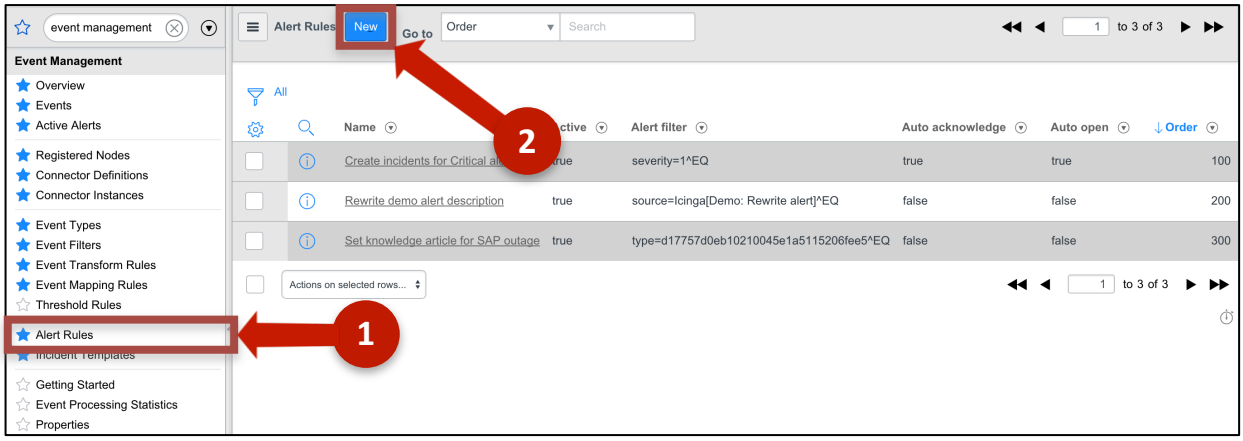
6. Click **Submit** to save the Incident Template.

®2015 ServiceNow, Inc. All rights reserved.

Lab 4.2: Simple Alert Rule

Alert Rules can be used to automate actions for Alerts meeting specific criteria. In this lab, you will create an Alert rule that automatically creates an Incident for an Alert using the Incident template created in the previous lab.

1. Navigate to **Event Management > Alert Rules** (1) and click **New** to create an Alert Rule (2).



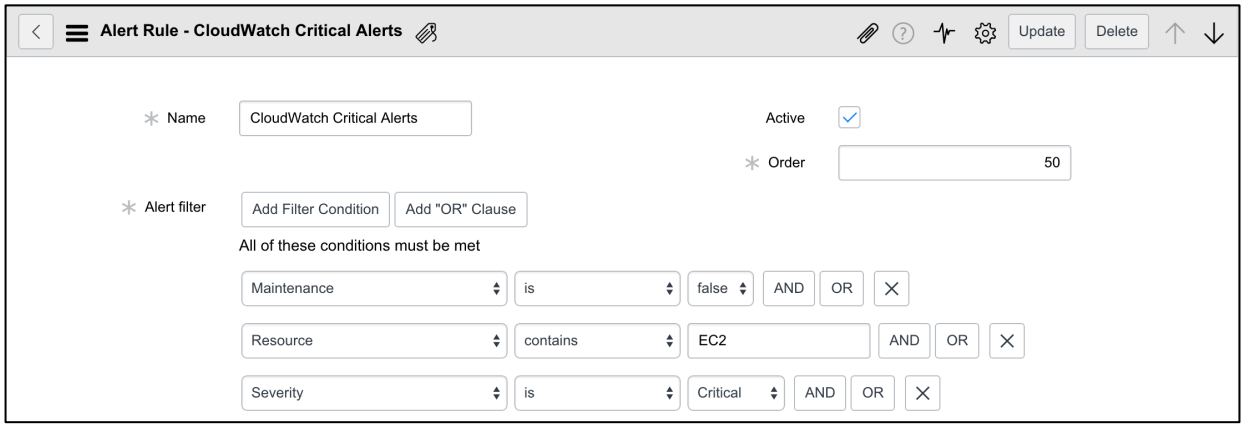
2. Name the Alert Rule **CloudWatch Critical Alerts**. Change the Order from 100 to **50**.

3. Under the Alert filter section, build the following condition:

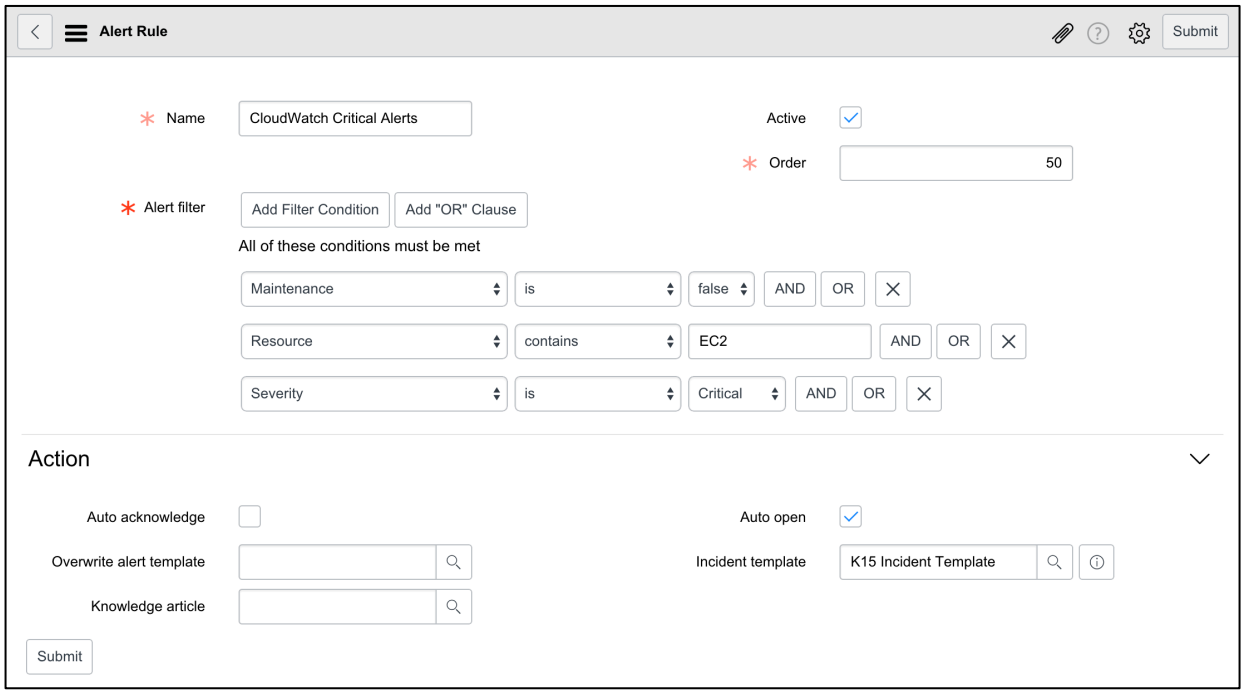
Maintenance	**is**	**false**	**AND**
Resource	**contains**	**EC2**	**AND**
Severity	**is**	**Critical**	

©2015 ServiceNow, Inc. All rights reserved.

4. The Alert filter should resemble the one shown in the example.



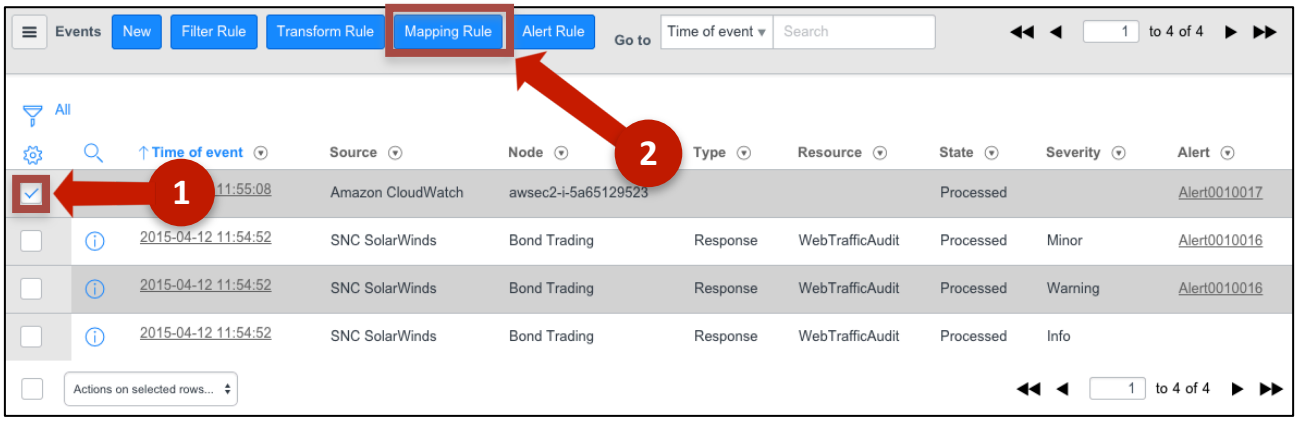
5. In the Action section, enable the **Auto open** checkbox, and then select **K15 Incident Template** for the Incident template field. The Alert Rule should look like the example.



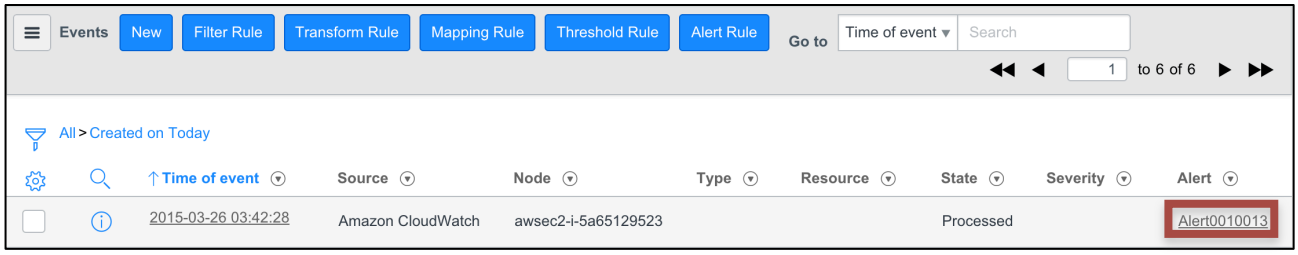
6. Click **Submit** to save the Alert Rule.

©2015 ServiceNow, Inc. All rights reserved.

7. Navigate to **Event Management > Events**, select an event (1) and click the **Mapping Rule** action button (2).

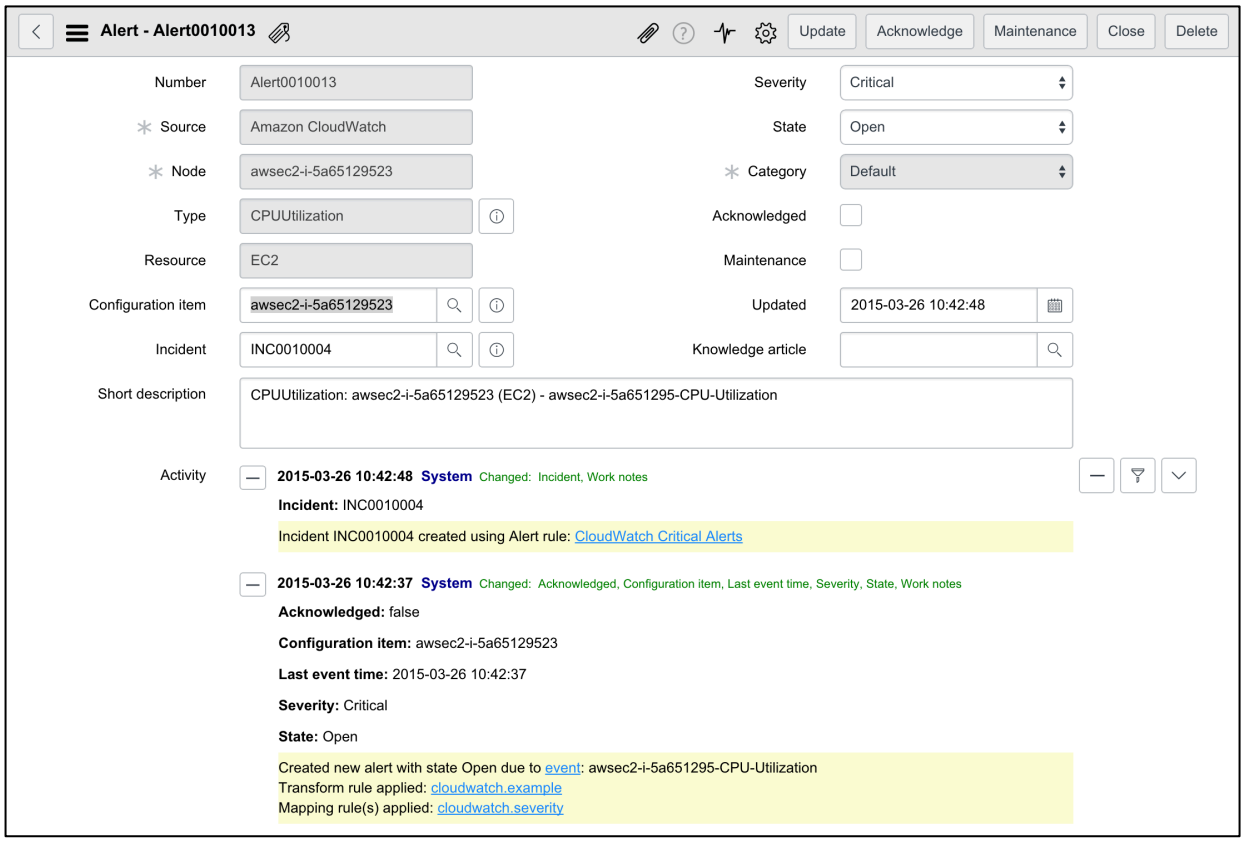


8. Wait approximately 30 seconds. Then refresh the Event list. Click the Alert link for the new event to open the Alert record.



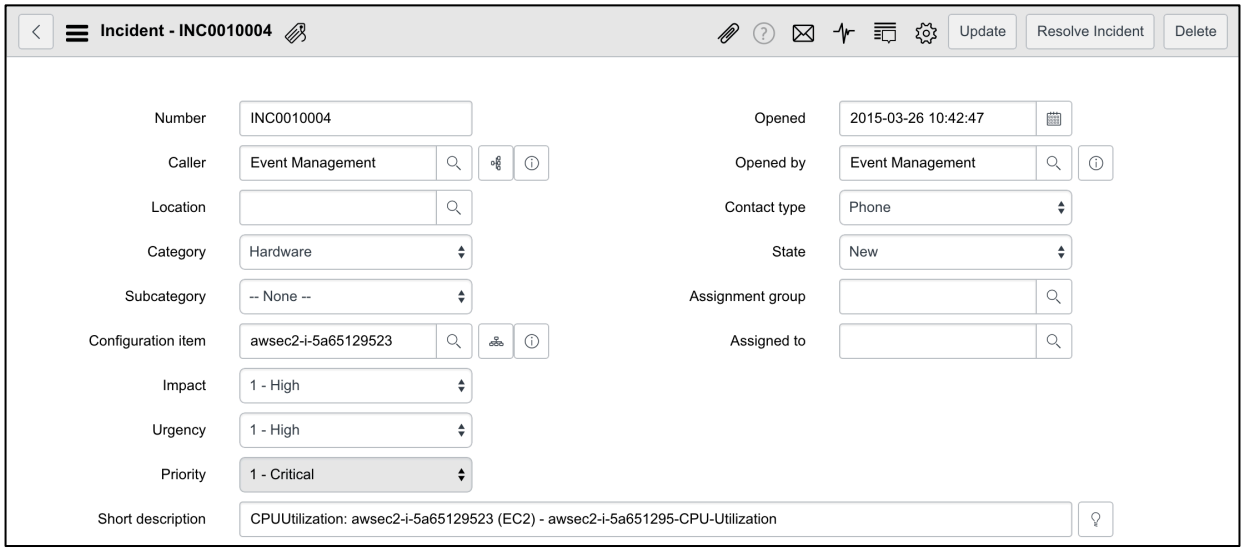
©2015 ServiceNow, Inc. All rights reserved.

9. The Activity journal field shows the Alert Rule that was applied to automatically create an Incident for this Alert. Note also the Transform and the Mapping rules that were applied.



©2015 ServiceNow, Inc. All rights reserved.

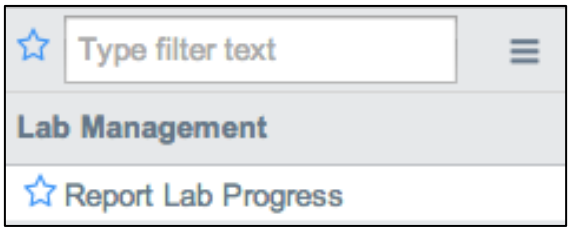
10. Click the **info** button (ⓘ) to the right of the Incident field to open the Incident.



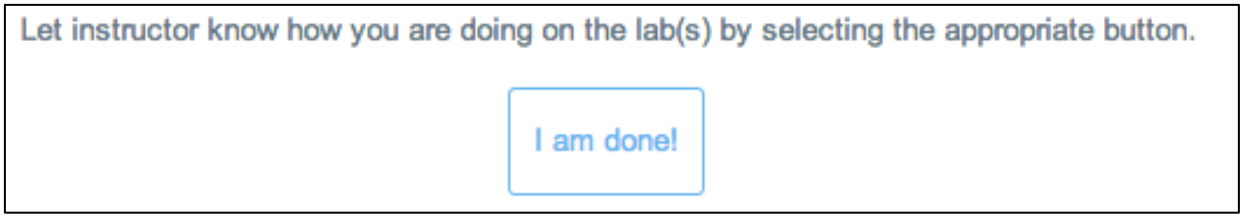
Note how the Caller, Opened By, Impact, Urgency and Priority fields have been set by the Incident Template.

Progress Report

1. Navigate to **Lab Management> Report Lab Progress**.



2. Click **I am done!**

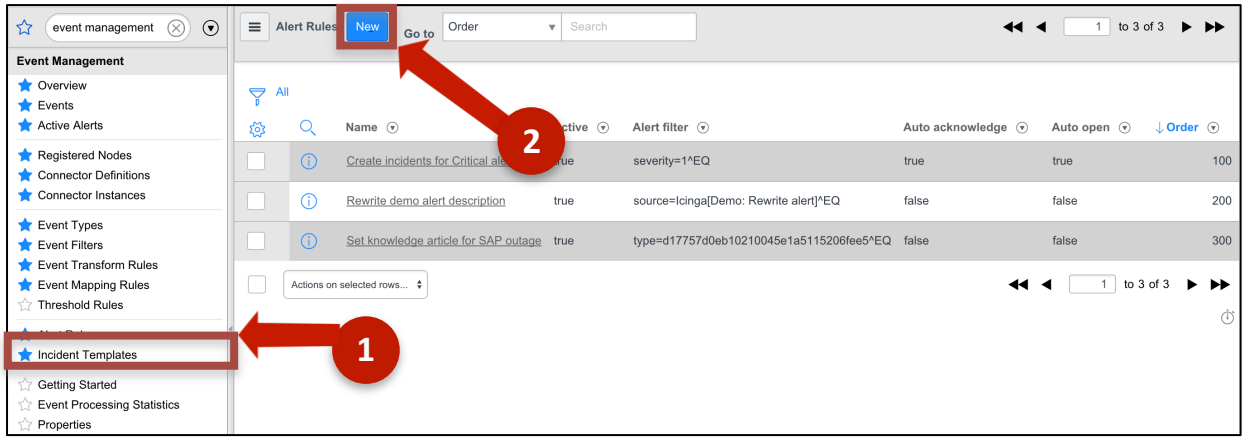


©2015 ServiceNow, Inc. All rights reserved.

Lab 4.2: Advanced Alert Rule

Knowledge articles containing information that can help resolve an issue can be automatically linked to an Alert through an Alert rule. This lab, explains how to configure an Alert Rule to associate a Knowledge article with an Alert.

1. Navigate to **Event Management** > **Alert Rules** (1) and click **New** to create an Alert Rule (2).



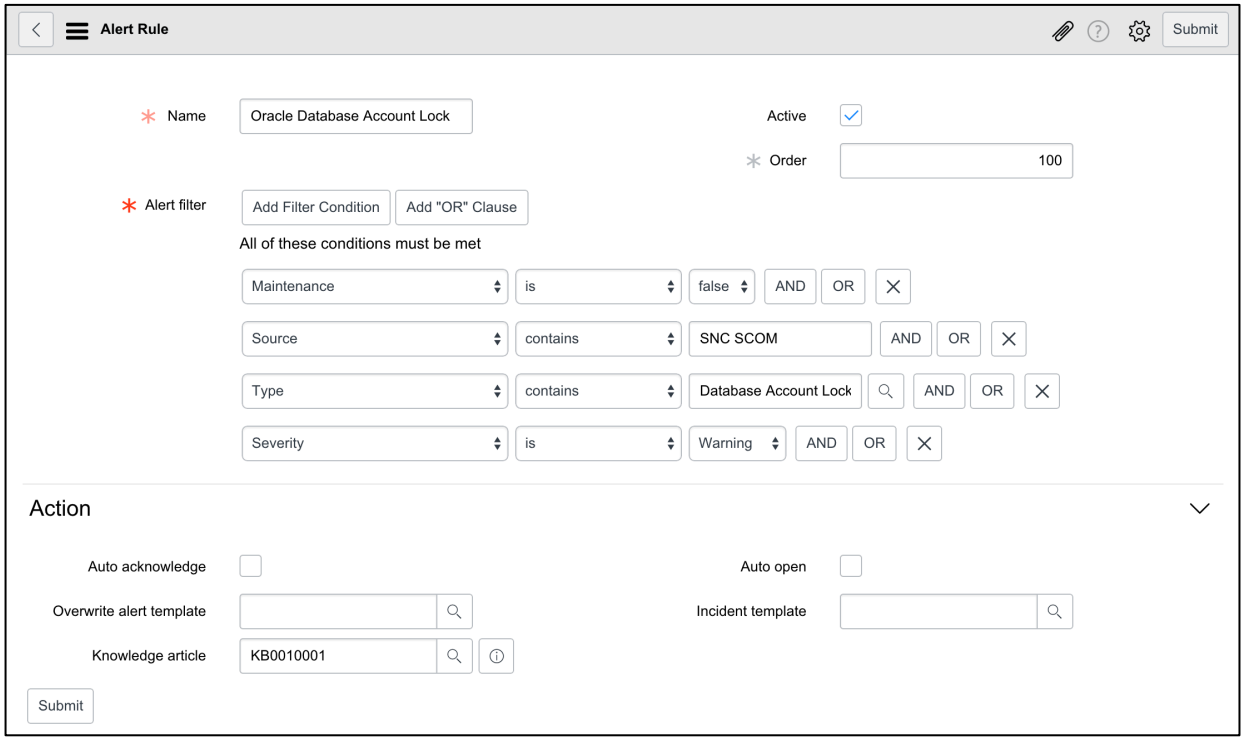
2. Name the Alert Rule **Oracle Database Account Lock**, and change the Order from 100 to **50**.

3. Under the Alert filter section, build the following condition:

Maintenance	**is**	**false**	**AND**
Source	**contains**	**SNC SCOM**	**AND**
Type	**contains**	**Database Account Lock**	**AND**
Severity	**is**	**Warning**	

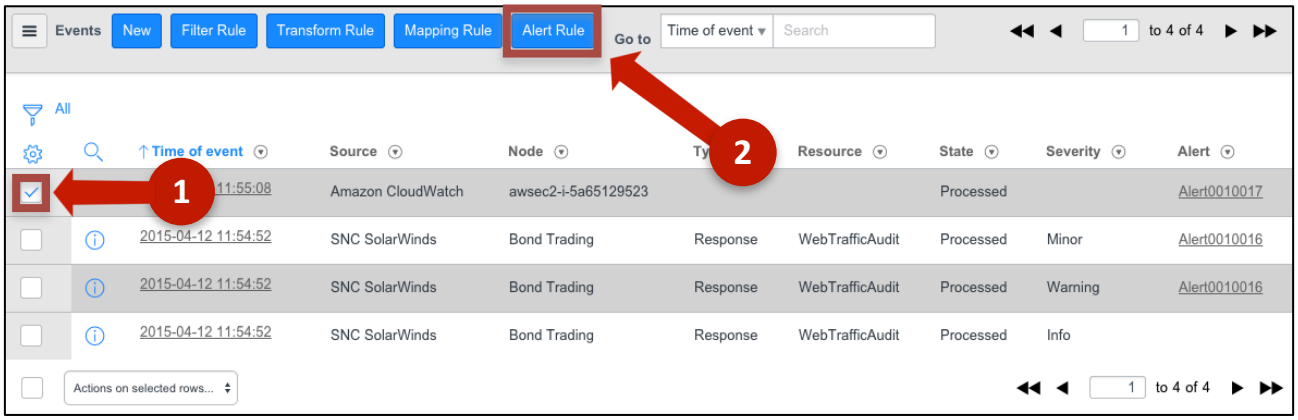
®2015 ServiceNow, Inc. All rights reserved.

4. In the Action section, click the search button for the **Knowledge article** field and select the **How to Rectify Blocked Oracle Sessions** article. The Alert Rule should look like the example.



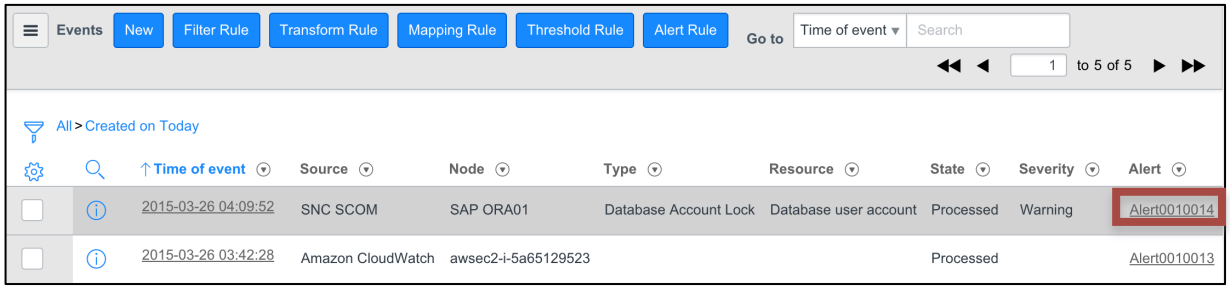
5. Click **Submit** to save the Alert Rule.

6. Navigate to **Event Management > Events**, select an event (1) and click the **Alert Rule** action button (2).



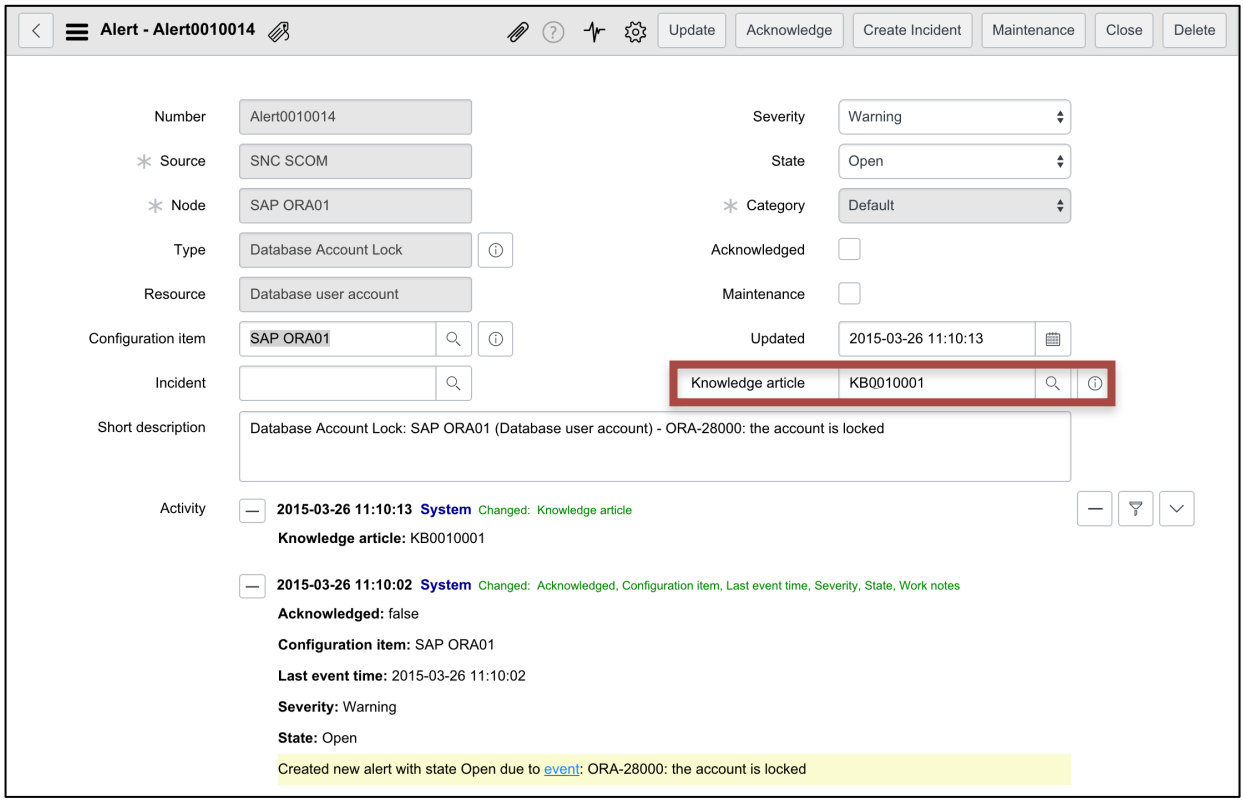
©2015 ServiceNow, Inc. All rights reserved.

7. Wait approximately 30 seconds. Refresh the Event list. Click the Alert link for the new event to open the Alert record.



®2015 ServiceNow, Inc. All rights reserved.

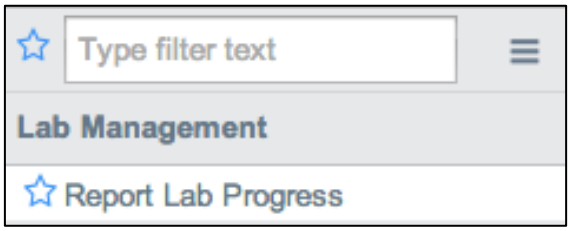
8. The Knowledge Article has been automatically associated with the Alert.



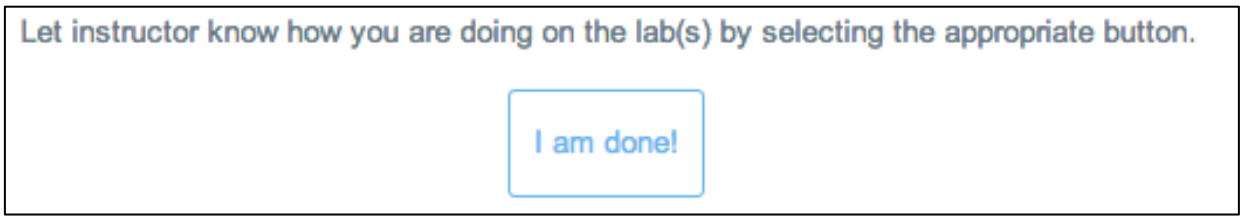
®2015 ServiceNow, Inc. All rights reserved.

Progress Report

1. Navigate to **Lab Management> Report Lab Progress**.



2. Click **I am done!**



©2015 ServiceNow, Inc. All rights reserved.