Lab Guide

Effective Major Incident Handling 201

Dave Peters & Joe Hehle

Default Login / Password: Knowledge17

admin / Knowledge17

itil / Knowledge17

employee / Knowledge17

Lab Sponsored by Microsoft Azure



This
Page
Intentionally
Left
Blank

Lab Goal

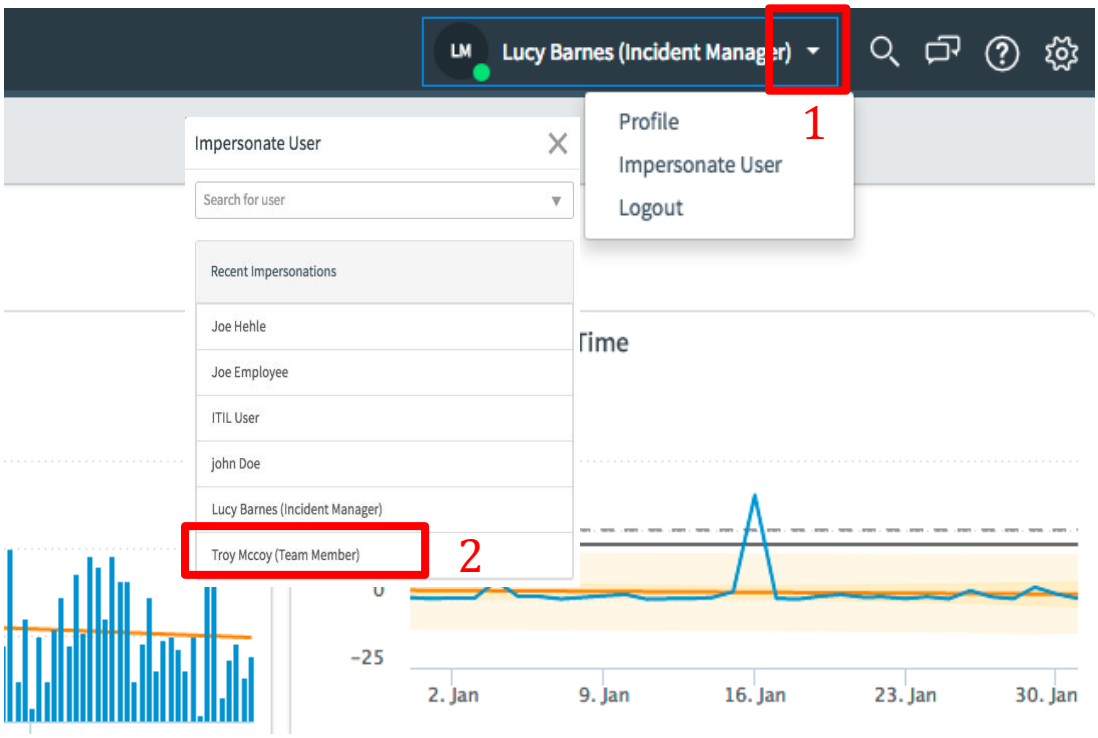
This lab explains how to create an **Incident Alert**.

Lucy Barnes is an Incident Manager and she wants to review existing incidents to determine if any Major Incidents are occurring. She decides to open an Incident Alert to communicate the outage and get the right people involved.

Lab 1.0
Create
Incident Alert

Create an Incident Alert from an Existing Incident

1. Click **Impersonate User** to log in as Lucy Barnes.

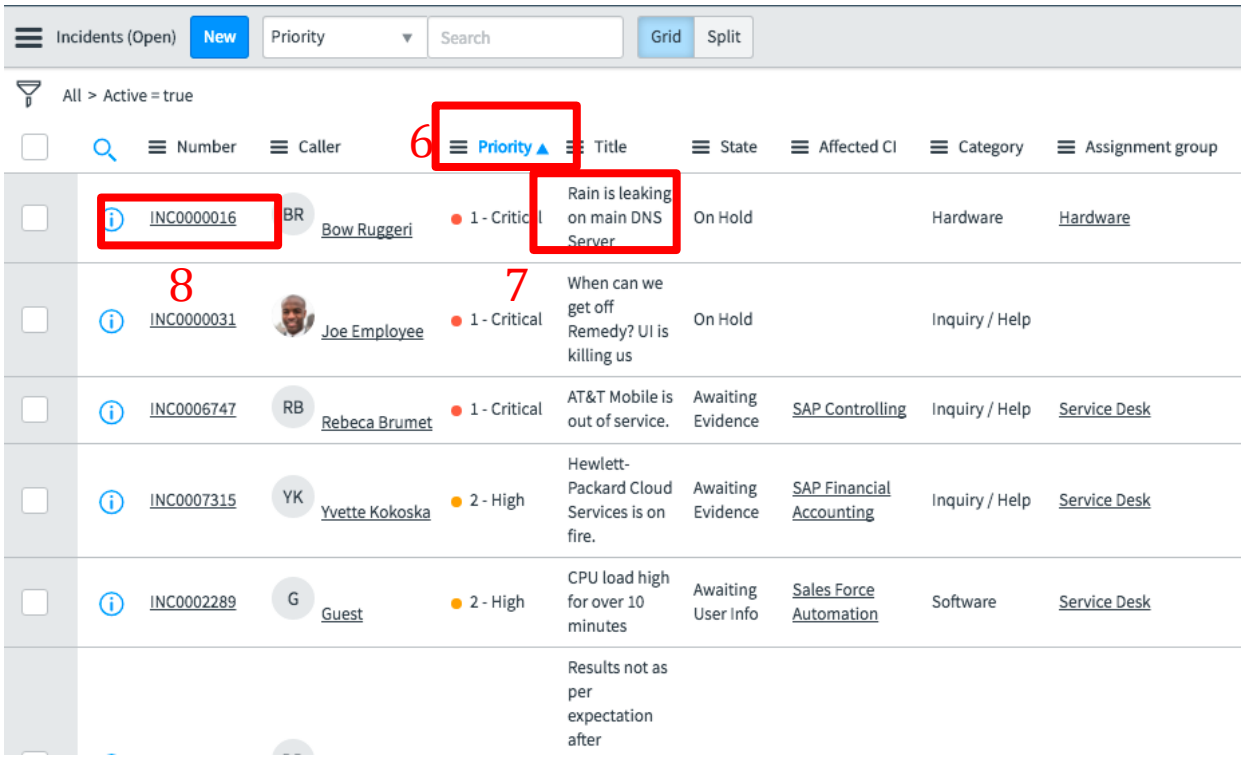


2. After the Impersonate User dialog appears, type **Lucy Barnes** and select her in the drop-down list.

3. Click **OK**.

4. After you are logged in as Lucy, type **incident** in the Filter Text box.

5. Click **Open** under the Incident Application.

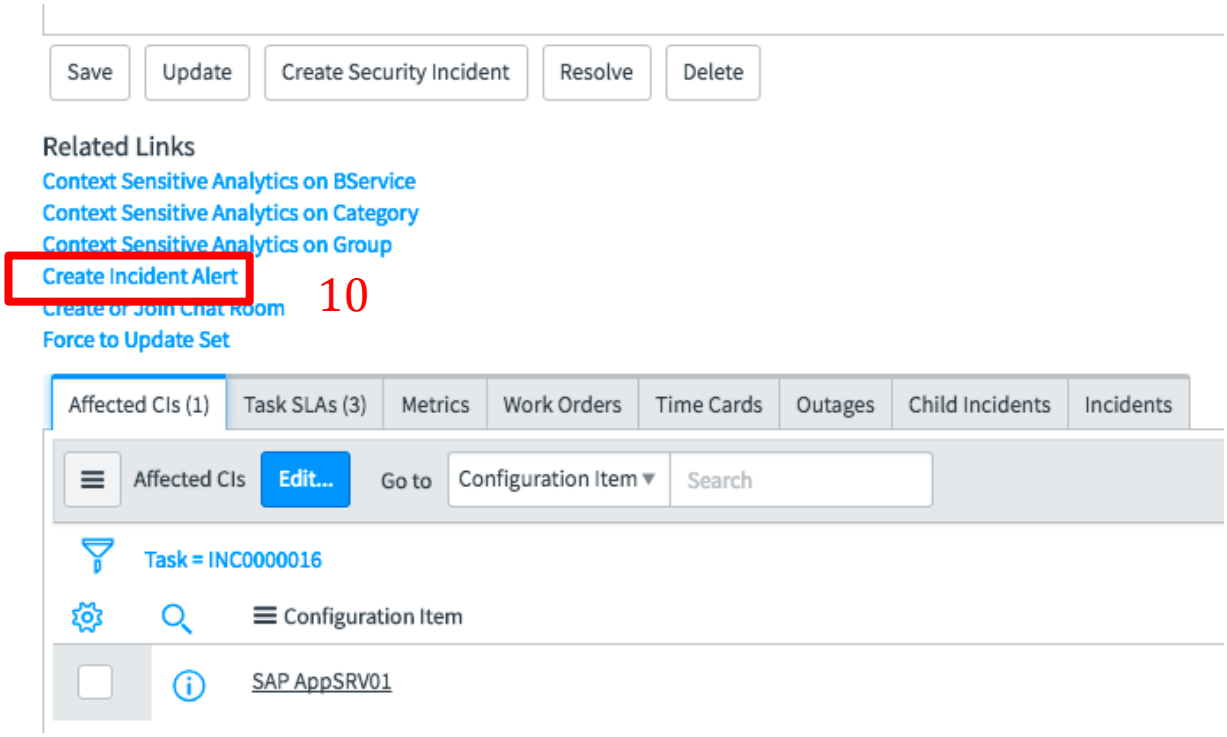


6. Lucy wants to focus on Critical Priority incidents. This can be done by several methods in ServiceNow. For this lab, click the **Priority** column heading to sort the list with **1-Critical Priority** incidents at the top of the list.

7. Lucy notices that a DNS Server is at risk of environmental exposure and has been reported as down in Incident I**NC0000016**.

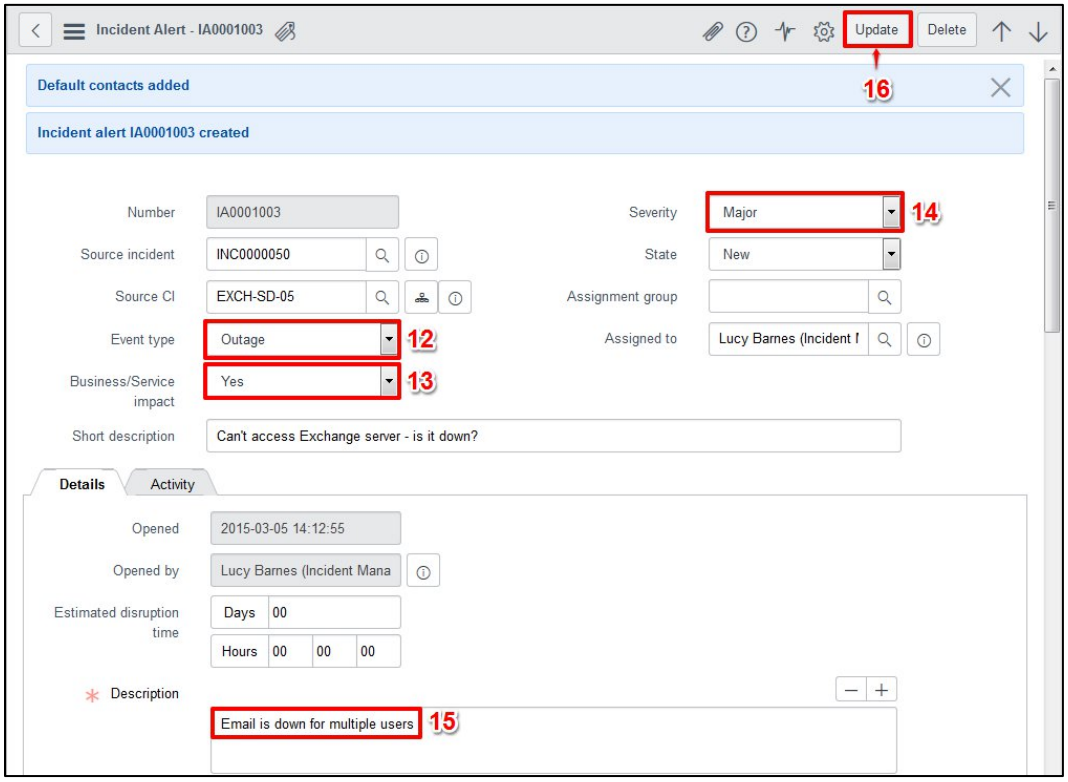
8. Click **INC0000016** in the list.

9. Lucy notices that the server is unavailable and multiple users are impacted by this incident. She wants to create an Incident Alert for this incident to communicate this outage. Scroll to the **Related Links** list.



10. Click **Create new incident alert**.

11. Once the Incident Alert record is created, notice that the Source Incident, Source CI, and Short Description are copied from INC0000050. Now, details about the Incident Alert need to be set.



12. Set the Event type to **Outage**.

13. Set the Business/Service Impact to **Yes**.

14. Set the Severity to **Major**.

15. Set the Description to **DNS is down for multiple users**.

16. Click **Update**.

17. Scroll to the bottom of the Incident and click **Show related incident alert**. Incidents can only be linked to one Incident Alert, but an Incident Alert can have many incidents linked to it.

18. Go to the Activity section (click the **Activity** tab). Notice all the updates that were done in the previous step were captured as an activity.

19. Scroll to the bottom of the **Incident Alert**. Go to the **Impacted CIs** section (or click the **Impacted CIs** tab, if tabs are enabled). Notice that all of the business services that are dependent on the **SAP AppSRV01** CI have automatically been listed. This leverages the CMDB relationship hierarchy.

20. Go to the User Contacts section (or click the **User Contacts** tab, if tabs are enabled) and notice that Lucy Barnes is listed as the Incident Manager for this Incident Alert. Incident Alert has contact responsibilities where Users and Groups can automatically be associated to an Incident Alert.

21. Go to the Group Contacts section (or click the **Group Contacts** tab, if tabs are enabled) and notice that several groups were added to this Incident Alert. Incident Alert has contact responsibilities where Users and Groups can automatically be associated to an Incident Alert.

22. Go to the Related Incidents section (or click the **Related Incidents** tab, if tabs are enabled) and notice that INC0000016 is listed automatically. Incident Alerts can have multiple Incidents associated to them. If INC0000016 was a parent of multiple incidents, the child incidents would also be listed here.

Lab Success

1. You created an incident alert, and you successfully generated an email message from the Incident Alert.

Lab Goal

This lab explains how to create a new contact definition to add a Communications Manager to Incident Alerts that are of type Outage where the Severity is Major.

Lab 2.0 Modify Contact Definitions

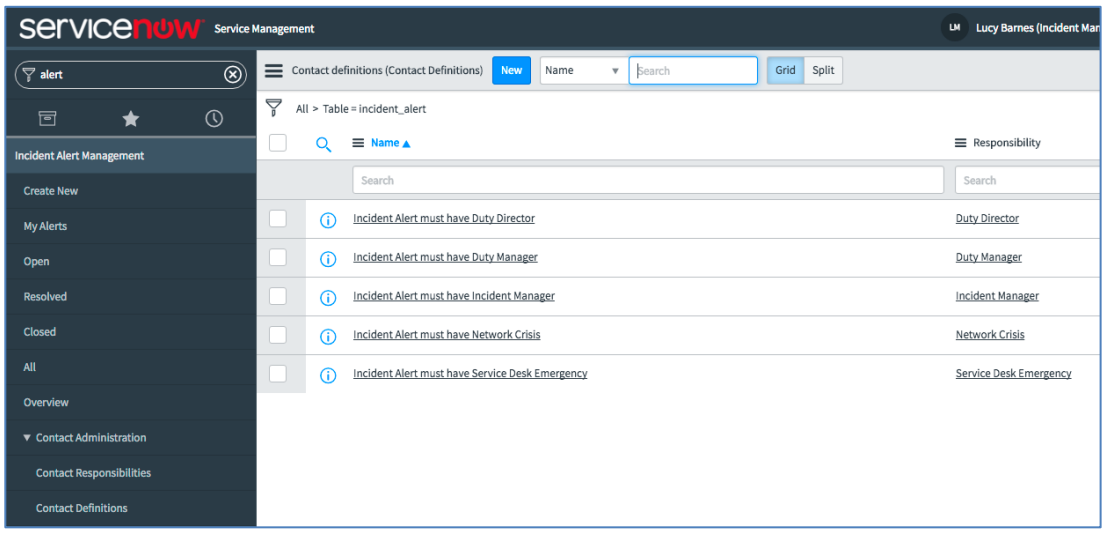
Create a New Contact Definition for an Incident Alert

1. In the Filter Text box, type **alert**.

2. Click **Contact Responsibilities** in the Incident Alert Management application. This is a list of the out-of-the-box Responsibilities included with the product. New contact responsibilities can easily be added by Administrators and Incident Alert Administrators.

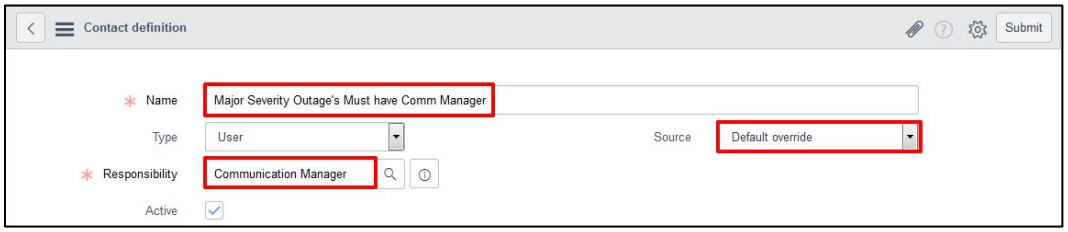
3. Click **Contact Definitions**. Notice that ServiceNow has several out-of-the-box contact definitions. You saw a demonstration of these when you created the incident alert in the previous exercise in which a Duty Director, Incident Manager, and Duty manager were added along with the Service Desk Emergency and Network Crisis Groups.

4. Click **New**.



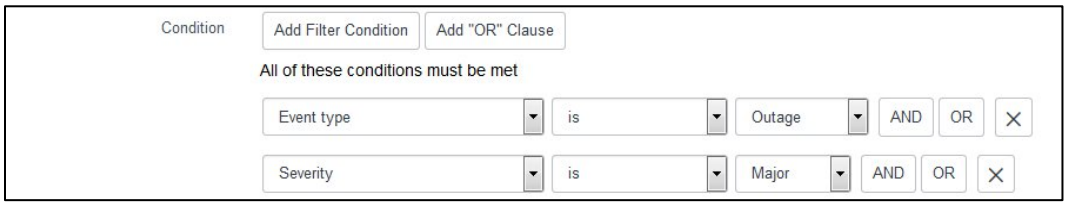
5. Enter the following Information:

   Name: **Major Severity Outage's Must have Comm Manager**
   Responsibility: **Communication Manager**
   Source: **Default override**

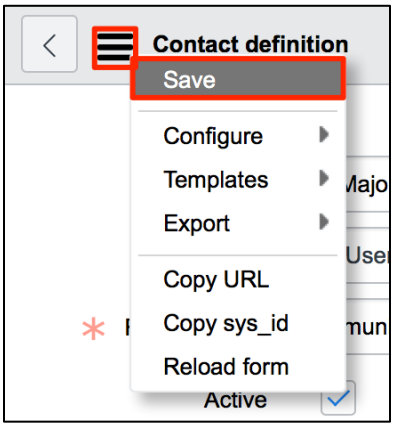


6. Add the condition to add the Communication Manager only if the Incident Alert type is **Outage** and the Severity is **Major**. In the condition, click **choose field** and select **Event Type**. Leave the middle box set to **is**. Click the right **None** select box and choose **Outage**.

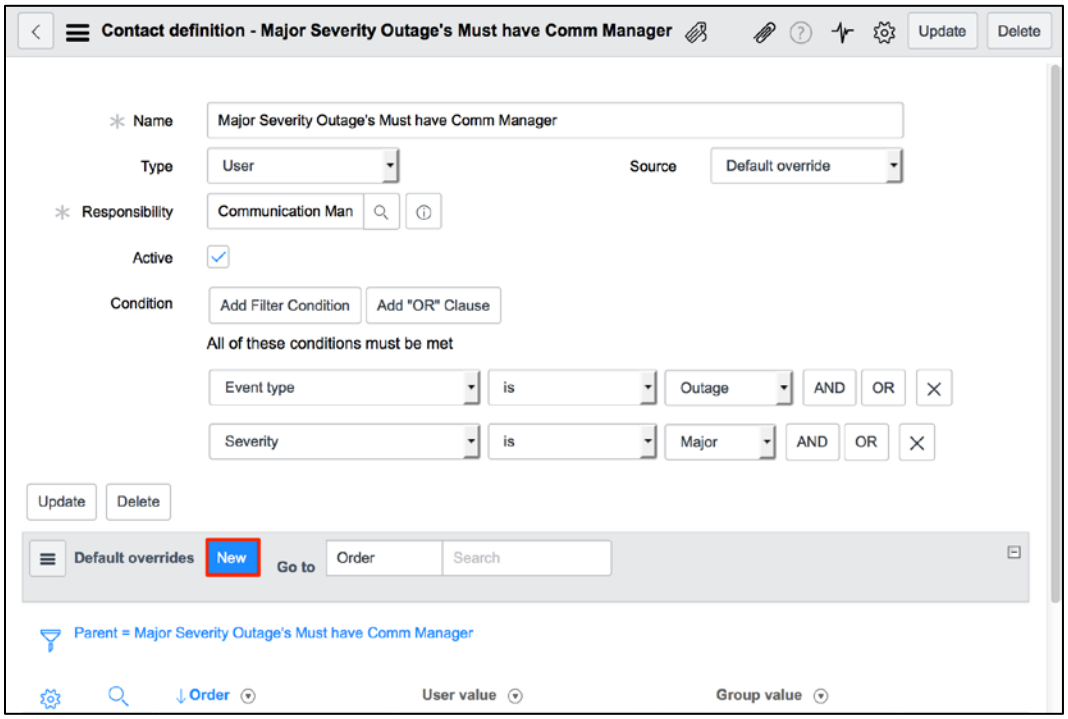
7. Click the **AND** button beside **Outage** to add another condition and repeat for Severity. Click **choose field** and select **Severity**. Leave the middle box set to **is**. Click the right **None** select box and choose **Major**.



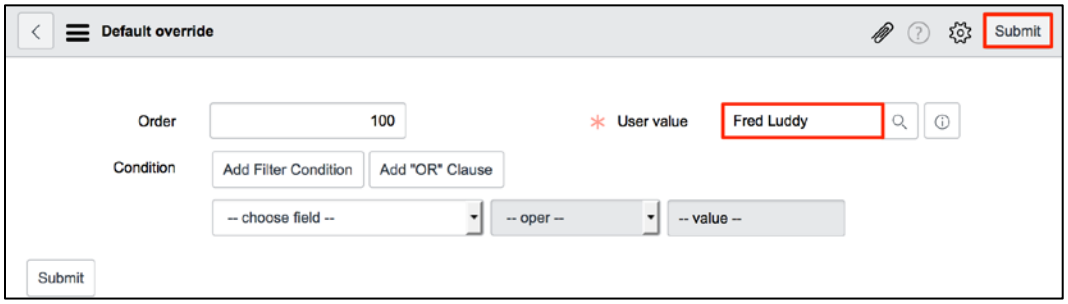
8. Click **Additional actions** and select **Save**, which leaves the screen on this record.



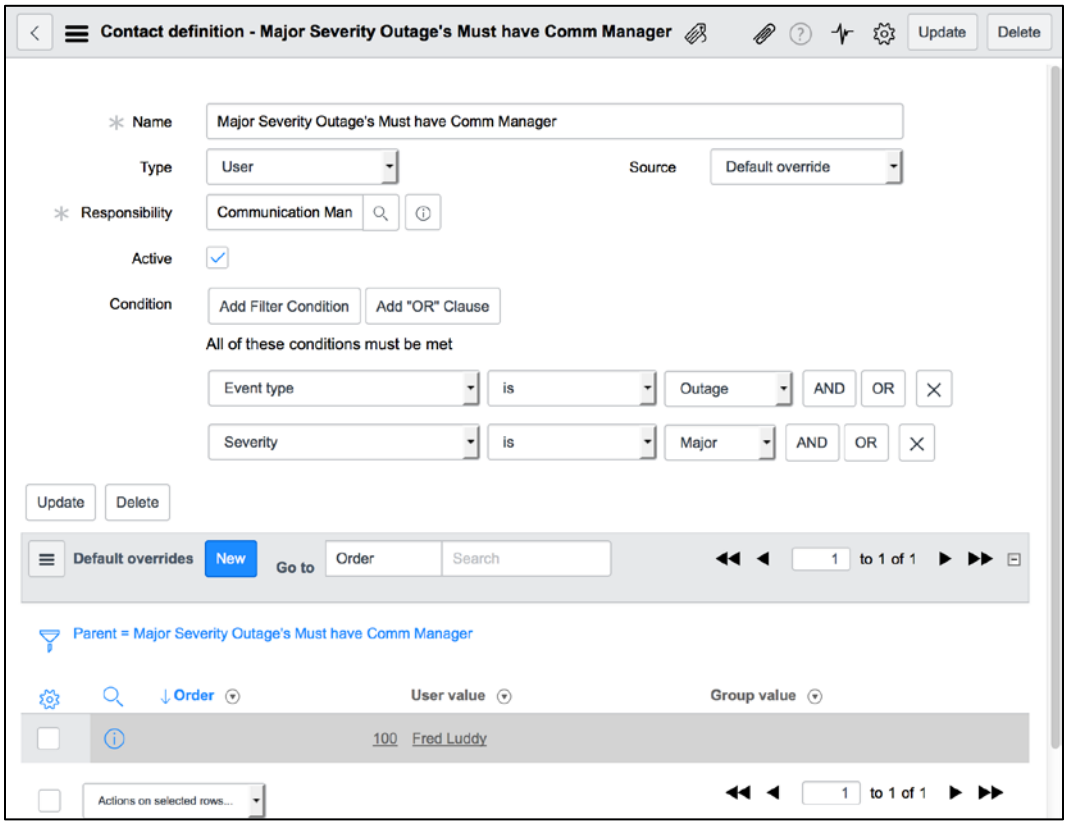
9. Click **New** in the **Default overrides** section at the bottom of the form.



10. In the **User value** field, type **Fred Luddy** and click **Submit**.



11. After these steps, your Contact Definition should look like the example.

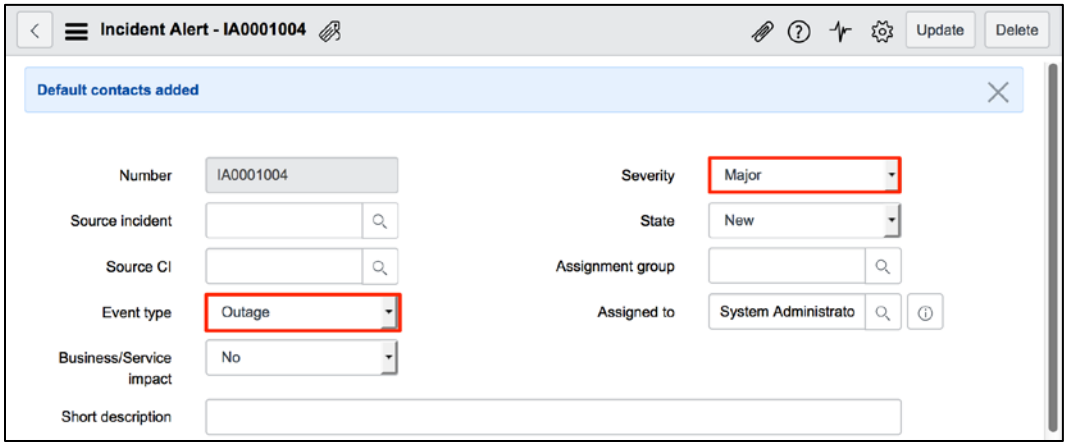


12. Test this new rule. Click **Create New** in the Incident Alert Management application.

13. Leave all the default selections as they are, but enter some text in the required **Description** field. Click **Additional actions** and select **Save** to remain on the record.

14. Scroll to the User Contacts section (click **User Contacts** tab) and notice that only the Duty Manager, Duty Director, and Incident Manager were added to this new Incident Alert.

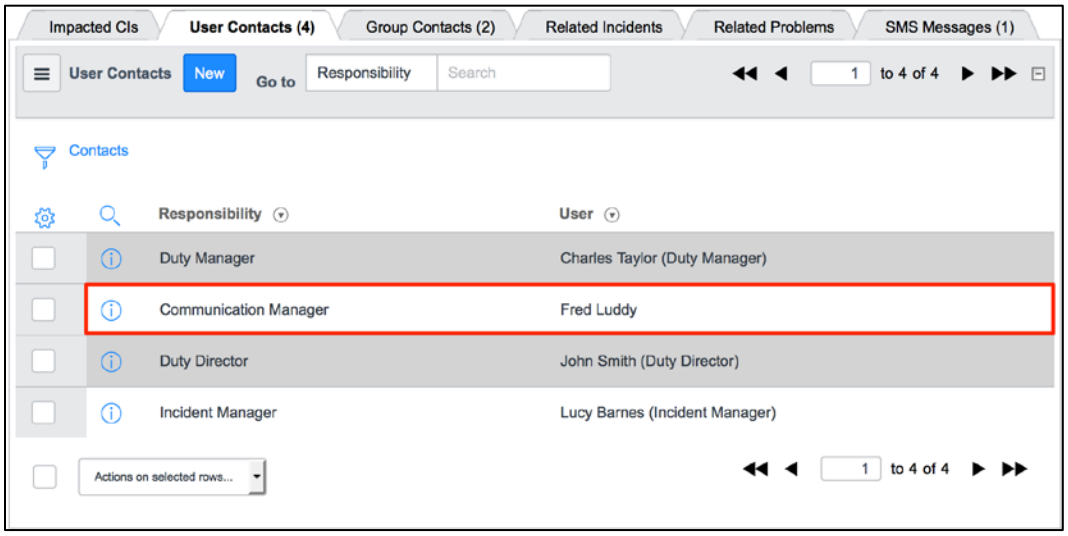
15. Scroll back to the top and set the Event type to **Outage** and the Severity to **Major**. Click **Additional actions** and select **Save** to remain on this record.



16. Scroll to the User Contacts section (click **User Contacts** tab) and notice that Fred Luddy, the Communications Manager, was added as a User Contact for this Incident Alert.

Lab Success Verification

1. A new contact definition was added that successfully adds a Communication Manager to Major Severity Outage Incident Alerts.



Lab Goal

This lab explains how to resolve an Incident Alert and capture **Post Incident Review** (PIR) details.

Lab 3.0
Resolve
Incident Alert

Resolve an Incident Alert to Show Integration to Problem Management

1. In the Filter Text box, type **alert**.
2. Click **Open** under the Incident Alert Management application.
3. In the list on the right, click **IA0001002**, or the lowest numbered Incident Alert created initially for the DNS server outage.
4. At the top, change the State to **Resolved**. Click **Additional actions** and select **save** to remain on this record.
5. Notice a new section called Post Incident Review (**Post Implementation Review** tab) appears. Scroll to this section or click the **Post Incident Review** tab.
6. Notice details about the source incident appear on this tab. Here you can enter details such as resolution notes, summary, and lessons learned.
7. Set the **Resolution Code** to **Complete**, if not set already by default.
8. Enter the following information:

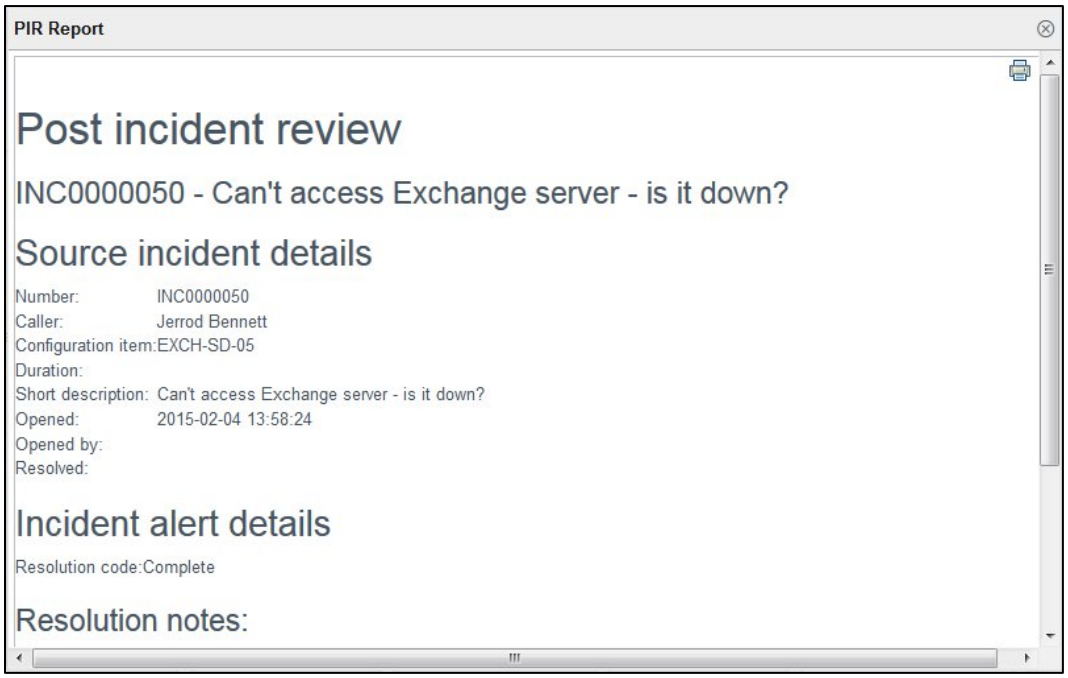
   Resolution notes: **Hardware team restarted the DNS server and service was restored. Microsoft was engaged and suggested applying an umbrella.**
   Summary: **DNS server blue screened.**
   Lessons learned: **Microsoft suggested we keep our servers up to date and dry.**

9. Click **Additional actions** and select **Save** to remain on this record.

10. Click **View PIR Report** under Related Links. This report can be printed to provide “gun-shot” report of what happened, what you did, and what to do next. It is also useful information for a formal Problem or Root Cause Analysis record.

Lab Success Verification

1. The Incident Alert opened previously is now resolved. View the Post incident review report.



Lab Goal

This lab explains how to create a gauge to view Major incidents from your homepage. This informs the service desk and facilitates the creation of duplicate incidents.

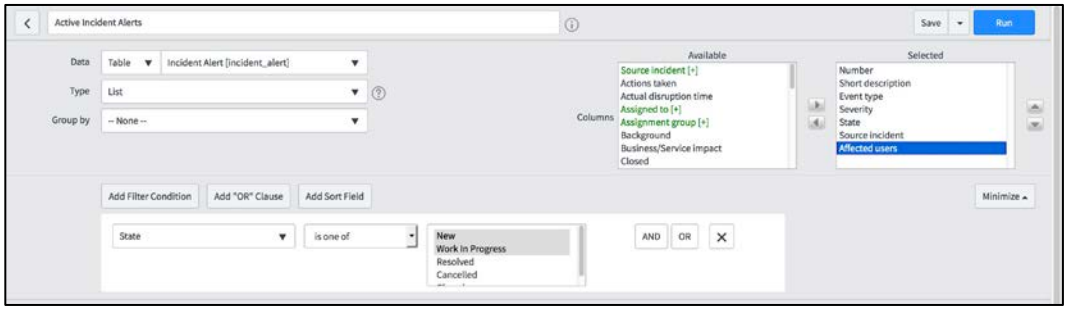
Lab 4.0
Create Major Incident Gauge

1. Navigate to Reports – View/Run.

2. Press the **Create a report** button.

   Fill out the form as follows:

   Name: **Active Incident Alerts**
   Data: **Table | Incident (Incident)**
   Type: **List**
   Selected Columns: **Number, Short Description, Event Type, Severity, State, Source Incident, Affected Users**
   (press "**Add filter condition**" button)
   Filter Condition (use shift to select multiple values): **State| Is one of | New, Work in progress**



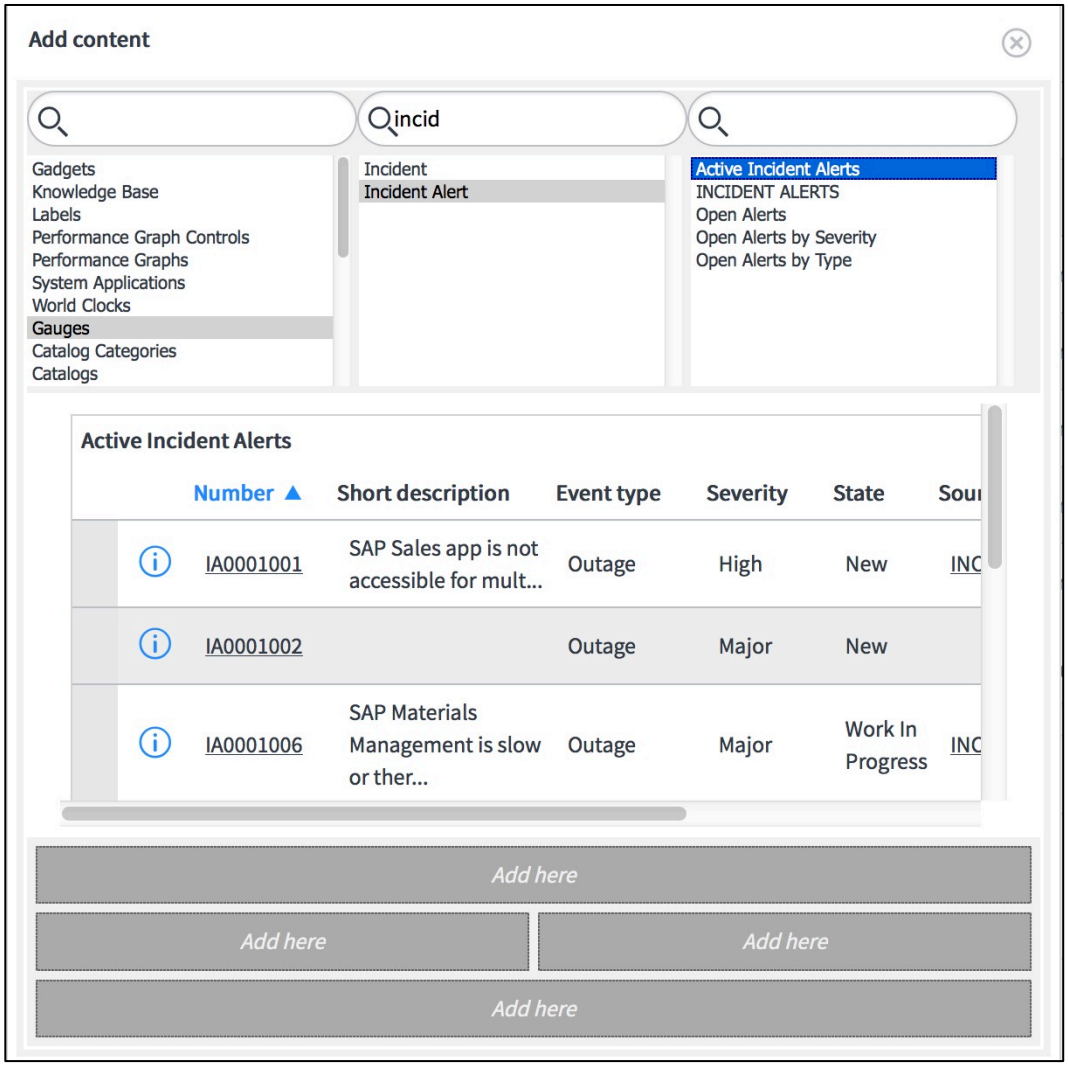
3. **Save** the report.

4. Use the drop-down arrow next to Save. Select **make gauge**.

5. Add the gauge to your homepage. Navigate to your Home Page in the Navigator Bar: **Self Service > Home**, or by clicking the banner in the upper left:

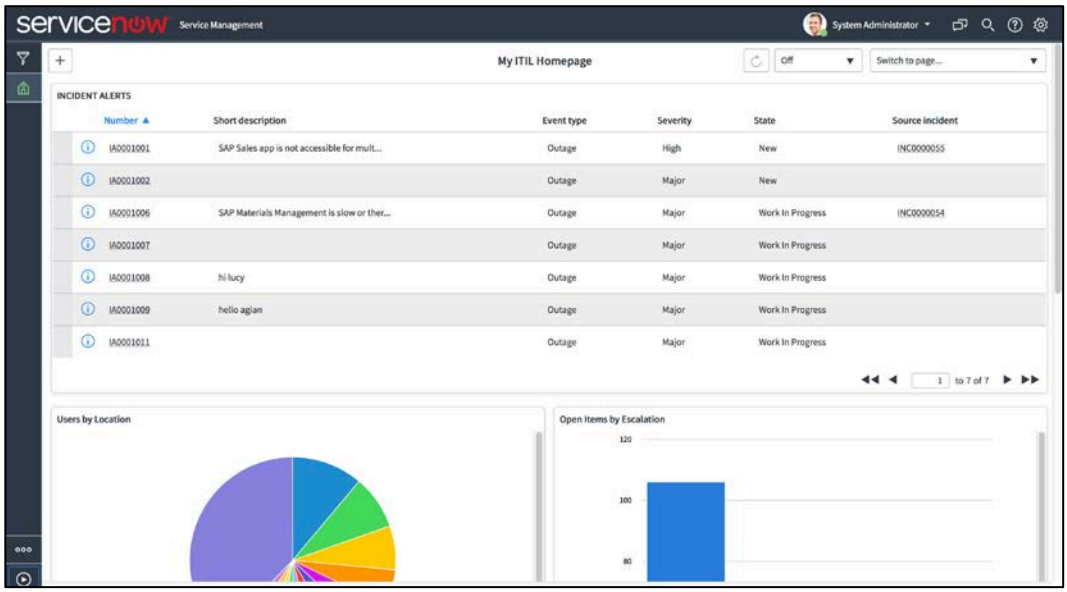
   Press the **+** button in the upper left of your homepage
   The Add Content window will pop up, select as follows:
   Gauges| Incident Alert| Active Incident Alerts

6. Click the top **Add Here** block at the bottom of the Add Content window.



Lab Success Verification

1. View your homepage. Verify the major incident gauge is visible.



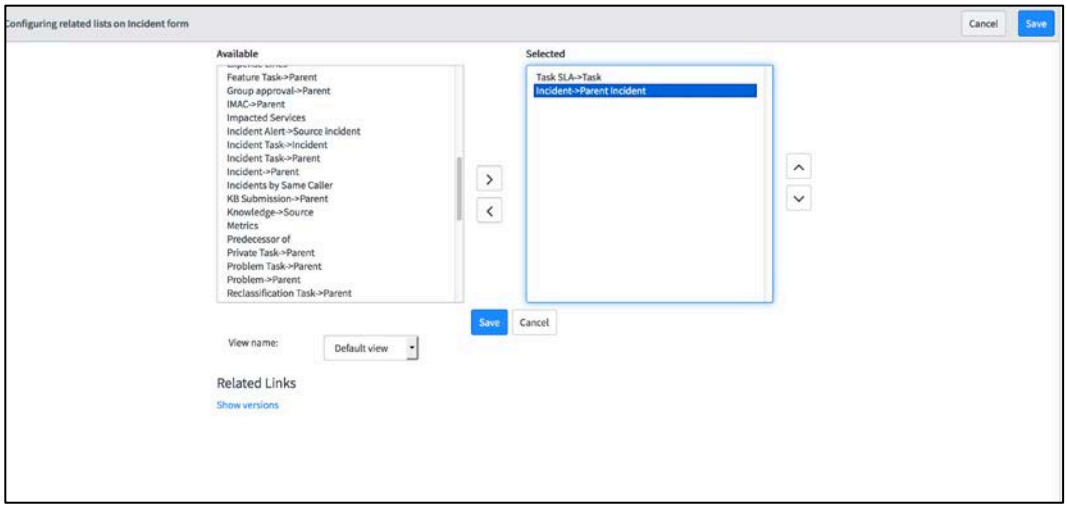
Lab Goal

Major Incidents often result in multiple Incident reports from affected users. Acme wants to be able to track Parent and Child relationships between Incidents. This lab explains how to enhance the default Incident Management form to include references to parent and child incidents.

Lab 5.0 Modify Incident Form

Modify Incident Form to Show Child Incidents

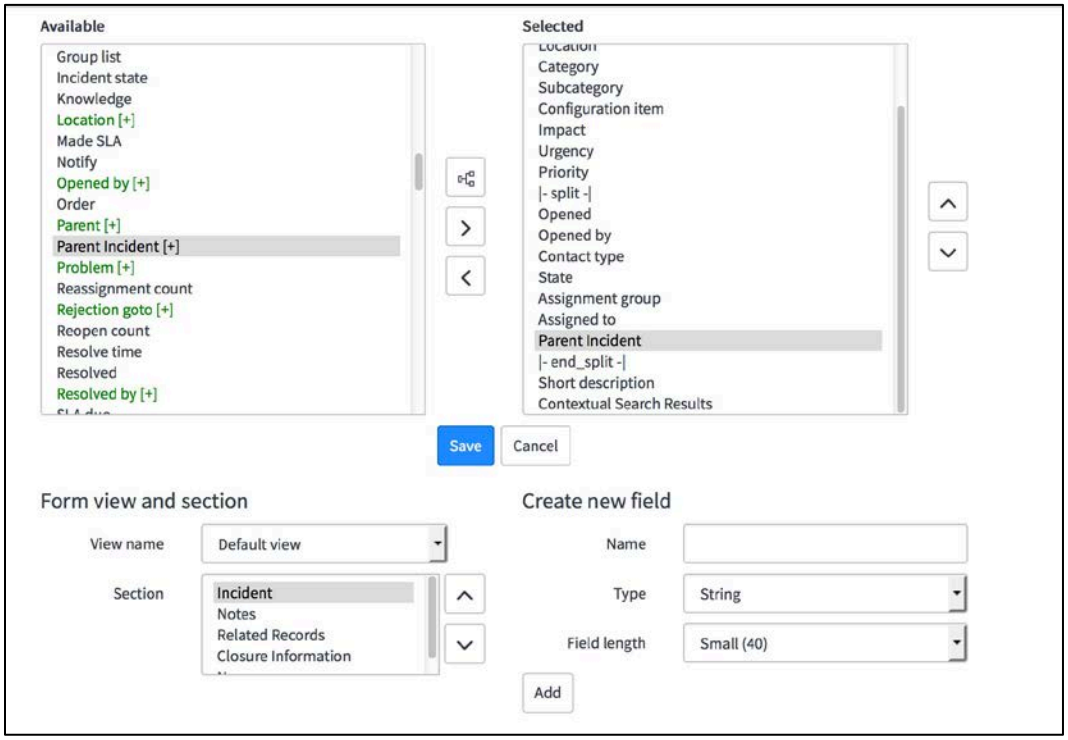
1. Navigate to **Incidents > open** and select one to open the incident form.
2. Right-click on the incident context bar. Select **Configure > Related Lists**.
3. In the Available section, double-click the **Incident -> Parent incident** related list to select it.



4. Press **Save**.

Add the Parent Incident Field to the Incident Form

1. Right-click the incident context bar. Select **Configure -> form layout**.

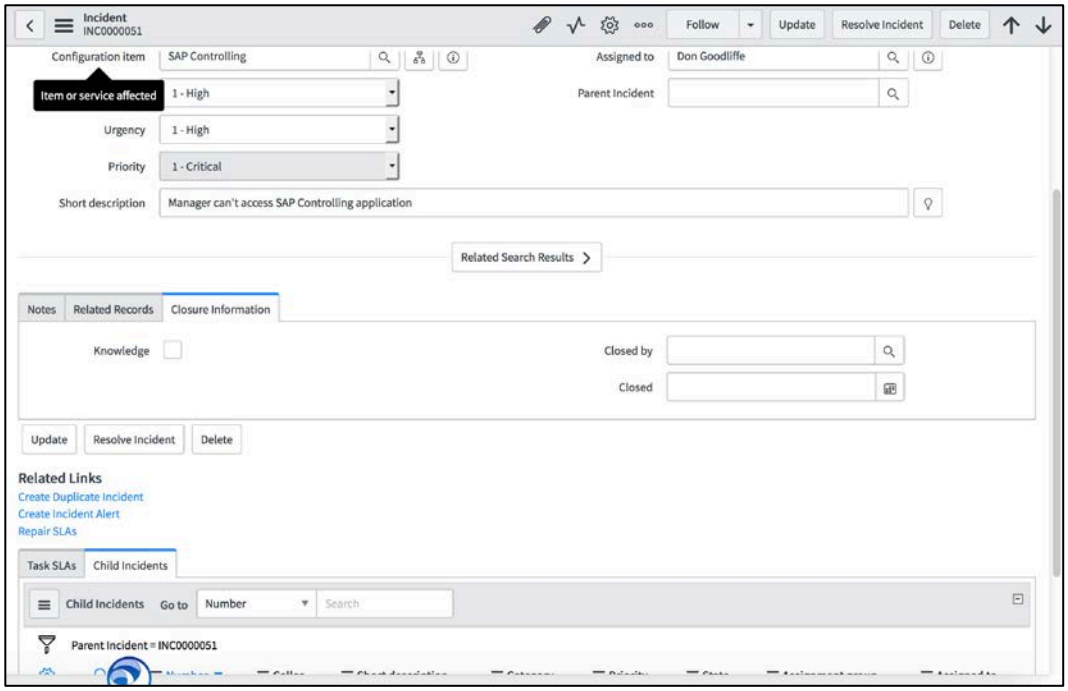


2. Add the **parent incident** field to the default view under the “assigned to” field in the list.

3. Press **Save**.

Lab Success Verification

1. You return to the incident after saving the form layout.
2. Note the additional field and related list.



Lab Goal

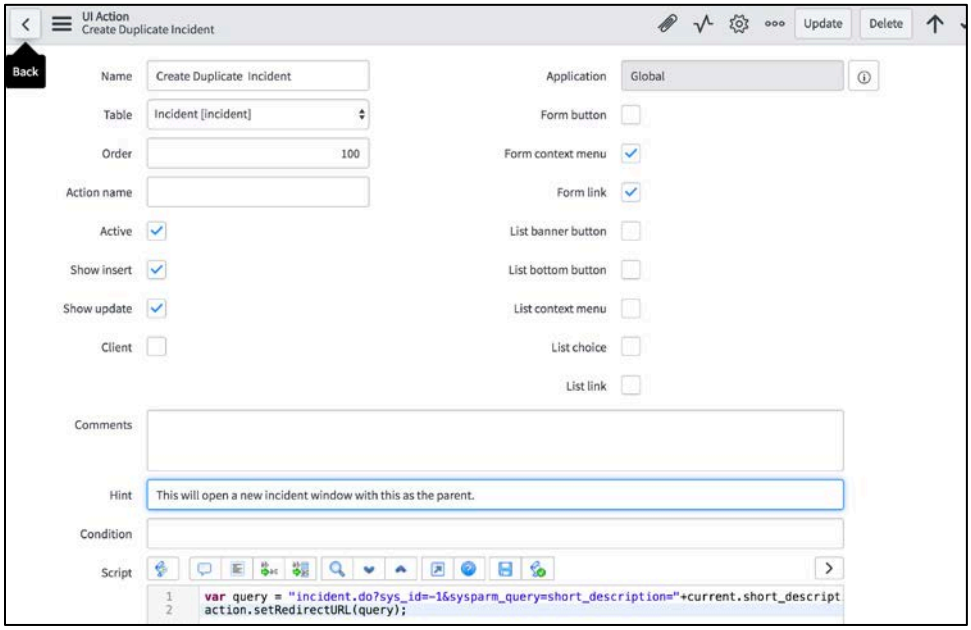
Acme wants to be able to track users impacted by a major incident by creating duplicate incidents for these users. This lab explains how to enhance the Incident Management form to allow for the simple creation of related incidents via a custom UI action.

Lab 6.0 Add UI Action to the Incident Form

1. Navigate to **Incidents > open** and select one to open the incident form.
2. Right-click on the incident context bar. Select **Configure > UI actions**.
3. Click **New**.

4. Fill out the form as follows:

   Name: **Create Duplicate Incident**
   Table: **Incident (Incident)**
   Active: **True**
   Show Insert: **True**
   Show Update: **True**
   Form Context Menu: **True**
   Form Link: **True**
   Order: **100**



5. Copy and paste the following into the script section:

   -----Copy Below-----

var query = "incident.do?sys_id=-1&sysparm_query=short_description="+current.short_description+"^description="+current.description+"^impact="+current.impact+"^risk="+current.risk+"^requested_by="+current.requested_by+"^priority="+current.priority +"^cmdb_ci="+current.cmdb_ci+"^category="+current.category+"^assignment_group="+current.assignment_group+"^watch_list="+current.watch_list+"^type="+current.type+"^parent_incident="+current.number;

action.setRedirectURL(query);

----Copy Above----

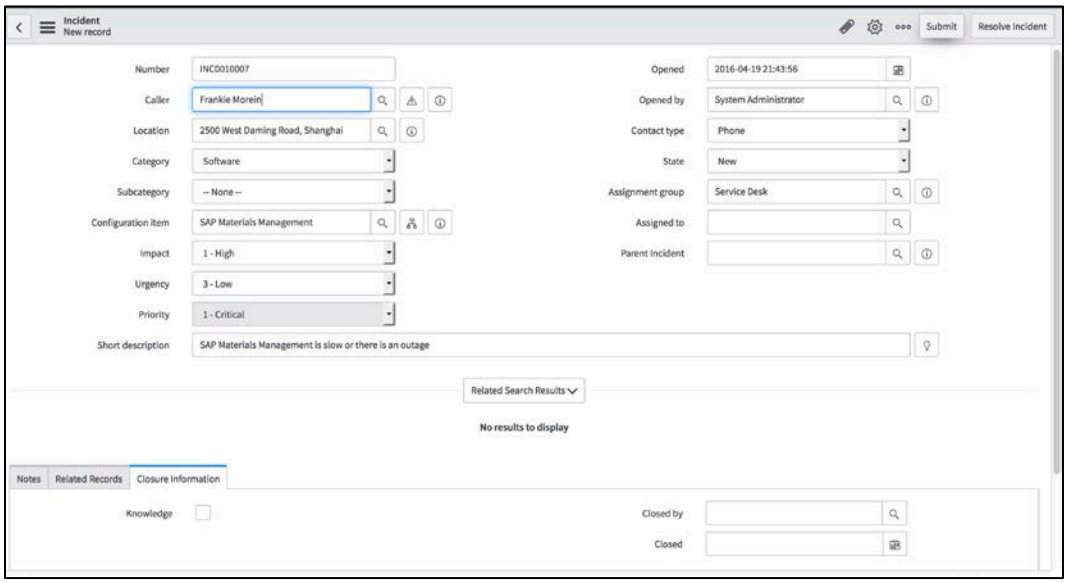
6. **Save** the UI action.

Lab Success Verification

1. Open an incident and press the **Create Duplicate Incident** link.



2. You see a new incident that is ready to submit.



1. Fill in the **Caller** field and **Save** the incident.

3. Return to the original incident and scroll down to the related lists. You see **Child Incidents** and your new duplicate incident in the list.

