

# How to integrate IBM Control Desk into your cloud service management toolchain for incident recording, trending, and problem readiness

1. Introduction
  - 1.1. IBM's Control Desk Features
2. Solution overview
  - 2.1. Service Management Architecture Overview
  - 2.2. Incident management architecture overview
3. Use cases and personas
4. How to use IBM Control Desk
  - 4.1. Site reliability engineer reviews weekly past incidents for trends
    - 4.1.1. Other steps or actions from the Start Center
    - 4.2. First responder responds to an incident created through Control Desk
      - 4.2.1. Other step or actions a first responder can take
5. Prerequisites for setup
6. Configuration of Control Desk
  - 6.1. Create and define Start Centers
    - 6.1.1. Start Centers
    - 6.1.2. Creating queries
    - 6.1.3. Creating KPIs
  - 6.1. Classification structure
  - 6.2. Escalations
  - 6.3. Configuring fields for integration to Slack
  - 6.4. send a message to Slack when the status of the ticket changes to CLOSED
7. How to set up the integration of NOI with IBM Control Desk
  - 7.1. Netcool Operations Insight to Control Desk Integration
    - 7.1.1. TSRM gateway installation
    - 7.1.2. Basic TSRM gateway configuration:
    - 7.1.3. Integration customizations
8. Conclusion
9. Glossary of Control Desk terms

# 1. INTRODUCTION

---

IBM Bluemix is a Platform as a Service (PaaS) application that lets you rapidly build and deploy an application. Applications may run in native Bluemix or in a hybrid fashion.

The purpose of incident recording and trending is to analyze the number, frequency, and types of incidents and to implement preventative measures to eliminate or reduce the volume, frequency, and severity of the outages or performance degradation. Identifying the causes of incidents and setting up measures to stop them in the future ensures fast and reliable services in Bluemix or hybrid architectures.

In this guide, we show you how to set up IBM Control Desk to connect with other applications in the middle of the cloud service management toolchain. We also demonstrate the interaction of Control Desk with other components of the toolchain.

Refer to [IBM Control Desk documentation](#) in the IBM Knowledge Center for steps on how to install IBM Control Desk.

## 1.1. IBM'S CONTROL DESK FEATURES

IBM Control Desk's unified IT asset and cloud service management software provides a common control center for managing business processes for both digital and physical assets. It enables control, governance, and compliance for applications, endpoints, and assets to protect critical data and prevent outages.

Control Desk is IT Infrastructure Library (ITIL)-compliant, accessible through mobile devices, and integrates with social media and development tools.

IBM Control Desk enables the business to support the user community for the full lifecycle of request, issue, and ongoing maintenance and support to systems and infrastructure the users need to do their jobs and to drive revenue for the overall business.

Control Desk provides the following functionality:

**Improves operational efficiency** with near real-time and historical analytics:

- o Prioritizes incident response based on business service impact.
- o Speeds problem resolution with a searchable solutions knowledge base and embedded remote diagnostics. Agents can remotely take over workstations and chat with users for faster request fulfillment.
- o Provides ticket templates and pre-populates work order fields with service request information through integration with telephony software.
- o Automatically classifies tickets based on keywords and detail fields.
- o Processes emails into inbound service requests. Service requests can be created, viewed and approved using mobile devices.

**Identifies incident trends and patterns** with search analytics:

- o Use advanced search, queries, and reporting to identify repeat incidents and patterns to focus communication and information to developers and first responders.
- o Provide visibility to first responder, site reliability engineers, and incident managers as well as developers.

## 2. SOLUTION OVERVIEW

### 2.1. SERVICE MANAGEMENT ARCHITECTURE OVERVIEW

Cloud-based applications need to be available all the time. To ensure availability and performance, you need proper processes including incident and problem management to respond to outages. As part of this, you need to properly record incidents and problems so you can study trends and root cause analysis to correct or eliminate the issue through communication and change management processes.

Figure 1 shows a typical cloud service management architecture. For full details, [visit the IBM Cloud Architecture Center](#).

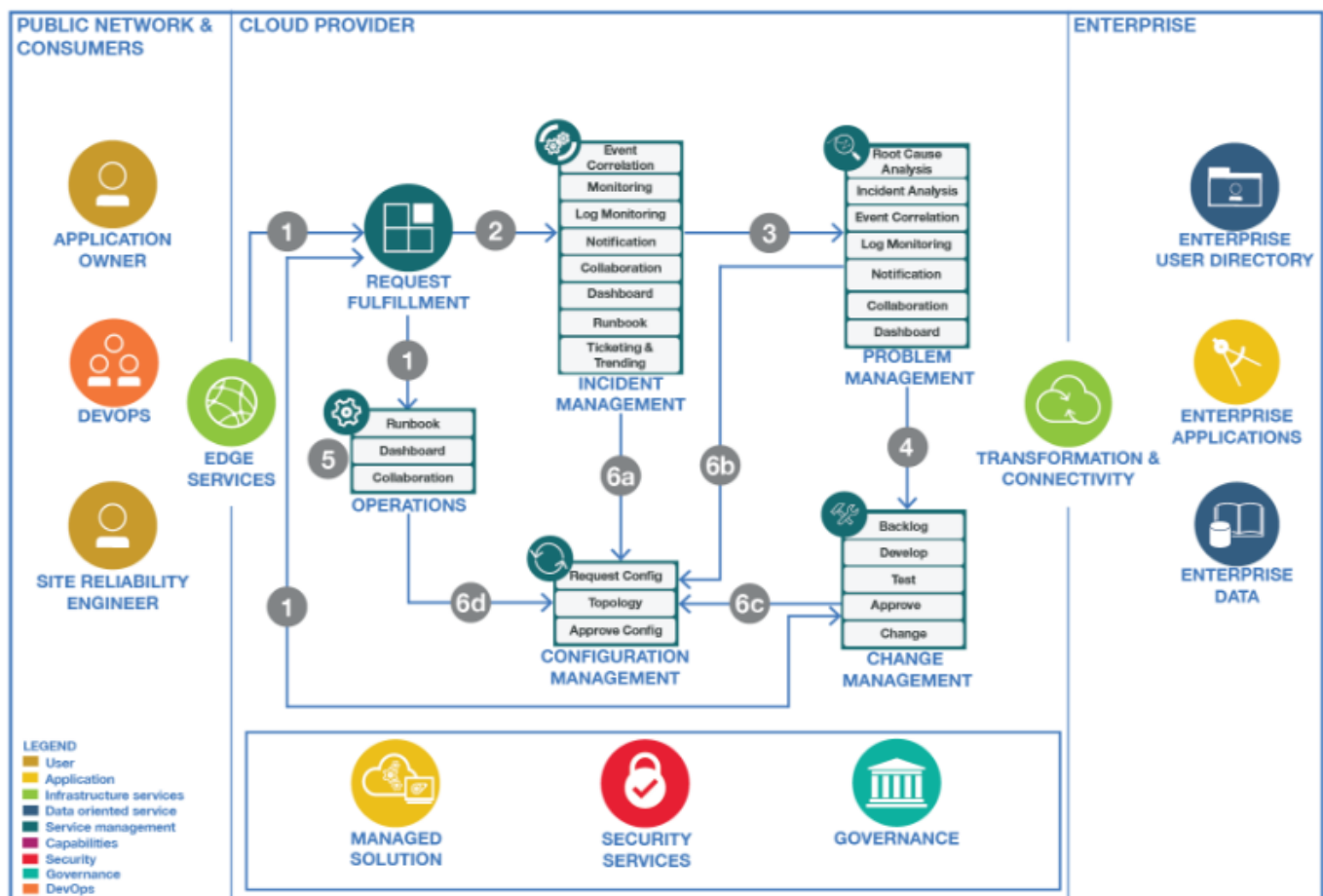


Figure 1 – Service Management Architecture Overview

The following are the runtime flow details of the overall Service Management Architecture image.

1. The client or support system reports an incident and request a change or seeks the status of an application. The service management users interact with clients to gather more information to diagnose incidents.
2. Incident management processes are optimized to restore the service as quickly as possible. This is done through a First Responder team, equipped with automation and well-defined Runbooks. Sophisticated monitoring is performed to detect issues early, before the service is affected. For complex incidents, subject matter experts collaborate on the investigation and resolution. Stakeholders (e.g. the application owner) are continuously informed about the status of the incident.
3. Once the service is restored, recorded tickets and collaborating data enable the Problem Management teams or individuals to investigate the root cause of the problem. Once the team understands what went wrong, they use counter measures to prevent the incident from happening again.
4. A change request is created to address the root cause of the incident. The change can be against the application, the infrastructure, or the supporting environment. Changes are prioritized and approved and put to the backlog to be addressed in an agile manner.
5. The operations team handles the integration, usage, and delivery of key services to business applications and the enterprise whether it is participating in incident management, architectural patterns, deployment, or the like. Operations integrate with or drive key processes to ensure the enterprise achieves its key performance indicators (KPIs).
6. The Configuration Management teams and tools support these processes (incident, problem, change management) as well as operations. Configuration Management maintains knowledge about the contributing components as well as their relationships.

## **2.2. INCIDENT MANAGEMENT ARCHITECTURE OVERVIEW**

Incident management and its operations are key to cloud service management. Incident management is optimized to restore the normal service operations as quickly as possible, ensuring the best possible levels of service quality and availability are maintained. Figure 2 shows an overview of an Incident Management architecture.

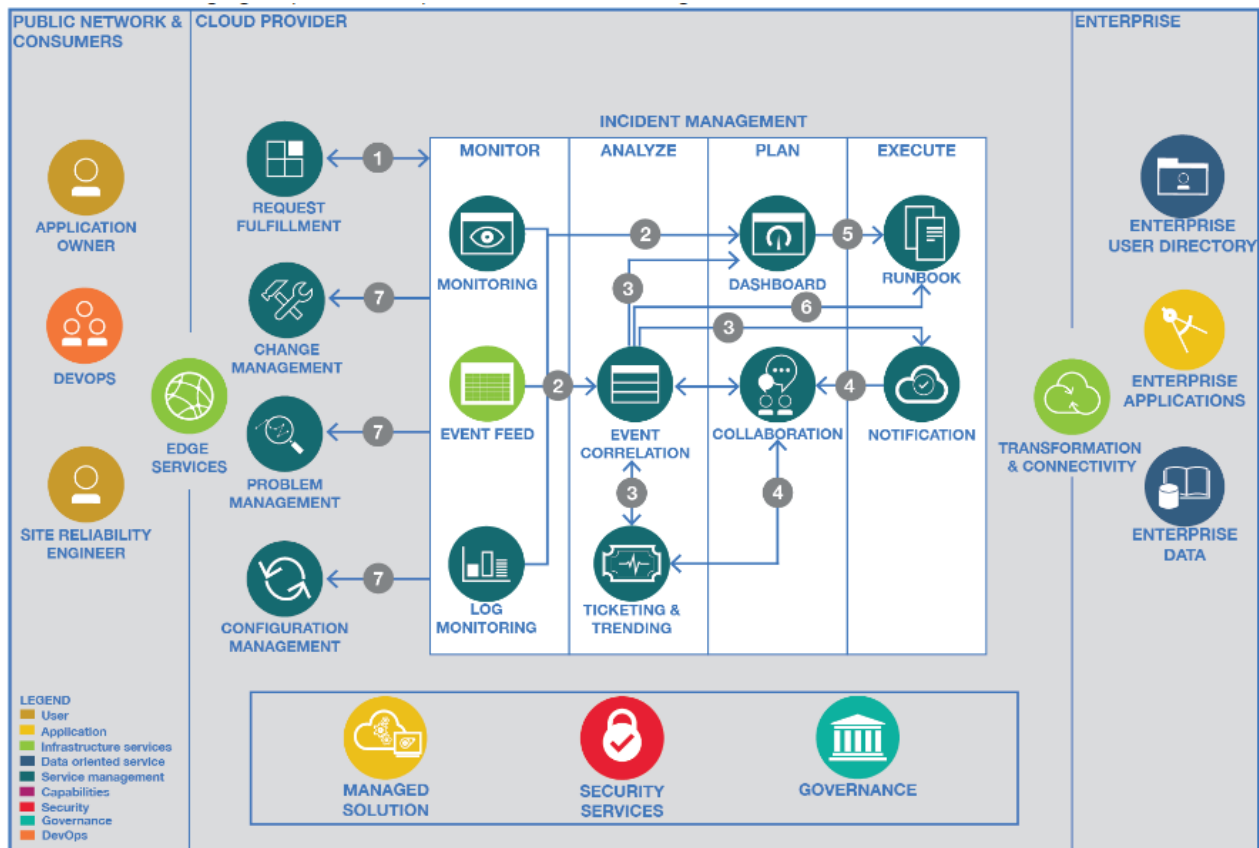


Figure 2 - Incident Management architecture overview

The following list describes the flow of the Incident Management Architecture:

1. The user or request fulfillment system reports an incident. Stakeholders (for example, the application owners) are continuously informed about the status of the incident.
2. The sophisticated monitoring and logging tools, including IBM or third-party tools, connected to the managed solutions detect the issues early and send alerts to the event correlation tool and unified dashboard.
3. The event correlation tool correlates events from multiple sources and identifies and isolates the problem by alerting the collaboration and notification systems. The first responder team examines the correlated events to narrow down the issue instantly. For complex issues, the incident owner and subject matter experts collaborate on the investigation and resolution.
4. The notification system creates collaboration channels with alerts that are specific to an incident, giving incident owners and subject matter experts records within the incident investigation and mitigation.
5. The notification system creates an incident record with specific details to allow the first responders to resolve the issue independently or in collaboration with others in a channel.
6. The dashboards are preconfigured to provide a single view of various sources of events from the event correlation and monitoring systems, helping the first responders and subject matter experts to isolate and resolve the issues by executing Runbooks.
7. The First Responder Team uses automation and well-defined Runbooks to resolve the issue instantly. The automated processes also update the status of the event so that the dashboard, notification, and collaboration channels are synchronized.
8. The site reliability engineer uses a set of queries, KPIs, and result sets to allow for trending and commonalities of records to be found and recorded for trending review and analysis.

- Once the incident is closed, a site reliability engineer opens the problem ticket is opened by the site reliability engineer to determine the root cause of the issue. If a configuration change is needed, the incident owner opens a ticket in the Configuration Management system.

Figure 3 shows an architectural diagram for IBM Control Desk, including its components and integrated tools for incident management and their interactions. One of the key takeaways from the diagram is that the solution supports a strong integration mixture of products and solutions, each feeding or being fed by the central IBM Netcool Operations Insight (NOI) solution.

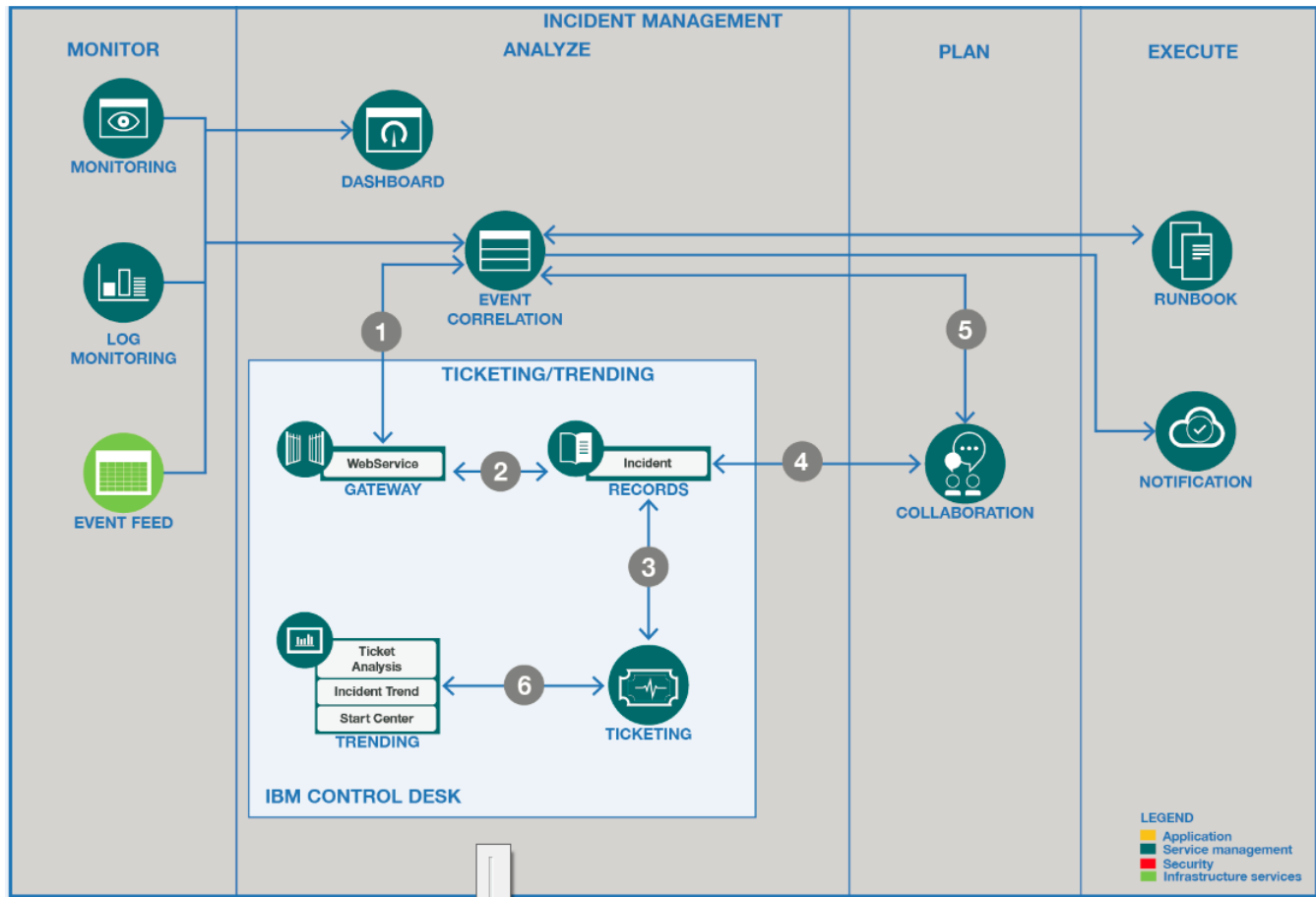


Figure 3 – System Context Diagram for IBM Control Desk

The following flow describes the setup and operations of this solution in an overall cloud service management space:

- An event system receives an alert, determines the severity of the issue, and creates an incident in IBM Control Desk. At the same time that the incident is being created, a collaboration channel is being opened. If the severity of the incident is a one (1) it will be a dedicated collaboration channel. If it is anything lower, it would be set in a general channel.
- Once the collaboration channel is open, the event system will update the Control Desk incident with the details of the channel (URL).

3. The next step in the flow is a decision action. Once the decision is made, the flow will follow one of the following paths:
  - a. In this path, the users are in the channel collaborating to determine a solution. When the solution is provided, the user can type in Slack noi resolve and the exact ticket number, and the ticket will be set to resolved.
  - b. If the flow follows this path, the event system determines if there is a runbook that can be executed to resolve the issue. This process can be either manual or automated.
4. Once the runbook has completed, the event system continues monitoring to ensure the exact issue is resolved. If it is resolved, the event system updates the incident as “resolved” in the Control Desk.
5. Additionally, the collaboration data from the channel is retrieved and stored in a work log entry in Control Desk for future use and trend analysis.

### 3. USE CASES AND PERSONAS

---

The following personas are often involved in IBM Control Desk in the cloud service management toolchain.

#### **First responder (on call):**

Steps a first responder takes include:

1. The first responder receives an alert to support an issue. The responder is alerted via the Slack channel. He or she views IBM Control Desk to see if this sort of issue has occurred before, and, if so, how it was resolved.
2. If a solution to the current incident is found, the first responder uses Control Desk to create a work log of the solution.
3. The first responder uses the work log from a similar incident to determine who worked on incidents of the same type and may be able to assist more timely now.

#### **Site reliability engineer:**

Steps a site reliability engineer takes include:

1. Conducts an analysis of the recent incidents to look for trends and frequency changes.
2. Investigates the incidents, which are like another incident to solve the current incident faster.
3. Finds possible patterns and establishes problem records for a review of the root causes.
4. Locates resolution to previous incidents.
5. Determines what team or resource worked on a previous, similar incident.

## 4. HOW TO USE IBM CONTROL DESK

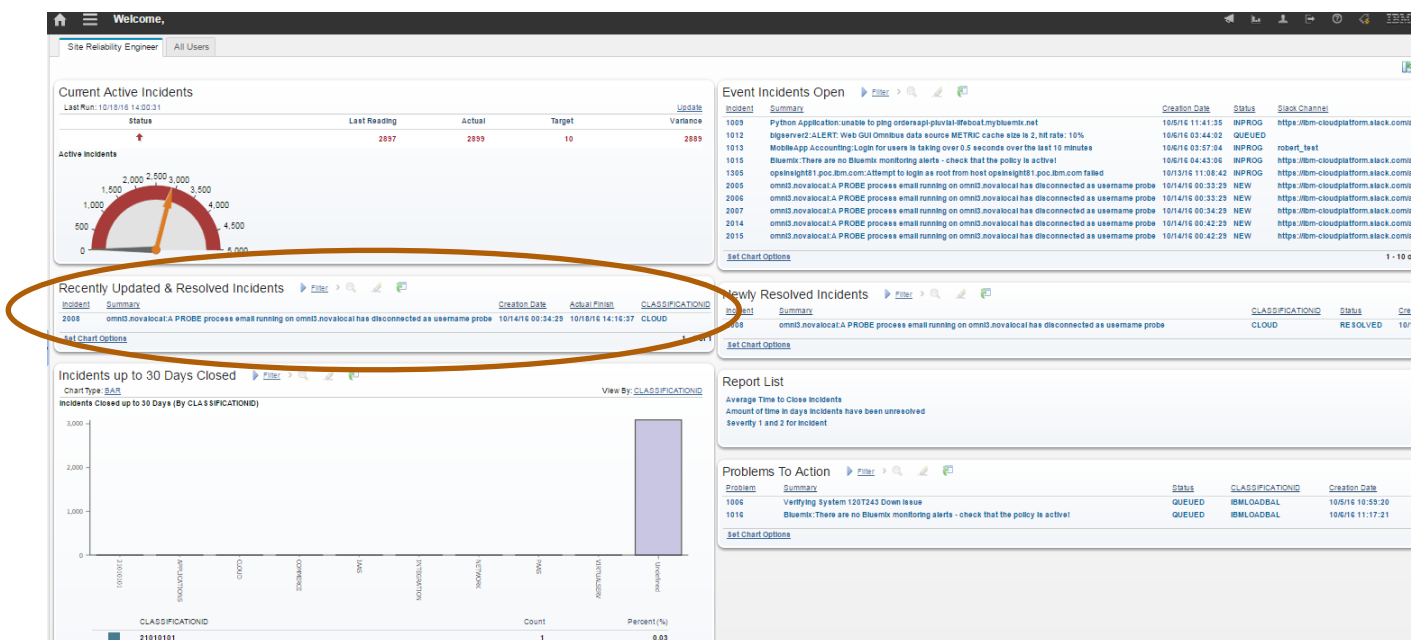
IBM Control Desk is operated through a web-based GUI. Your exact URL is based on how you install or use cloud-based solutions. It's usually in the following format: <http://<servername>/maximo> where you insert the name of your specific server.


The following steps show how a reliability engineer or first responder conduct a certain process. As users, they may perform many activities and processes with the data available to them in IBM Control Desk. The additional activities and processes are not fully described in this document.

### 4.1. SITE RELIABILITY ENGINEER REVIEWS WEEKLY PAST INCIDENTS FOR TRENDS

If you are a site reliability engineer, follow these steps to review incidents in the past week to identify any notable trends.

1. After you login, use the pre-created Start Center to view the Recently Updated & Resolved incidents. The portlet is on the lower left corner of the Start Center.



2. Click the  **Open Results in Application** icon to view the results. This presents all incidents that have a recent updated work log and were set to resolve in the last 24 hours.
3. View the application lists to scan for:
  - a. Common summaries
  - b. The priority of incidents
  - c. Whether the incident required an owner or owning group to be resolved



Use this application to view, create and modify incident records. To show My Location on the map, you need to allow the browser to share your location with the server. After the permission is granted, click the refresh button. Only the records which have the service address defined will be shown on the map. [More information](#)

List	Map - Side by Side	Map - Below
------	--------------------	-------------

Incidents	Filter	1 - 1 of 1
-----------	--------	------------

Incident	Summary	Reported By	Internal Priority	Priority	Status	Owner	Owner Group
1004	Verifying Dates on the CASE system infrastructure	MBIENFAN			3 RESOLVED		

4. Click on a specific incident for detailed information related to the incident, including:
  - a. What work log updates were added to give insight as to the runbooks used
  - b. The related conversation in the Slack channel
  - c. The first responders who may have added a log for a worthy note of detail

Work Logs	Filter	1 - 1 of 1
-----------	--------	------------

Record	Class	Created By	Date	Type	Summary
1005	INCIDENT	MBIENFAN	10/5/16 10:43:09	CLIENTNOTI	Slack update - channel open

5. As you review the incidents, if you notice a reoccurrence or an issue that you believe needs further research as a problem record, it may be best to classify the incident or the problem record as needing next steps or future reporting steps.

6. To classify the incident record, click the double arrows next to the field Classification Path. Use the dialogue to select a proper classification.

#### Incident Details

Summary:  
Verifying System 120T243 Down issue

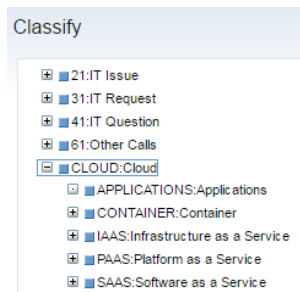
Details:  
down

Classification Path:  
IBMIT \ IBMNETEQ \ IBMLOADBAL

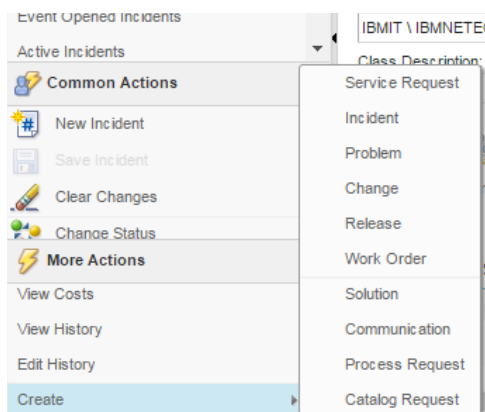
Class Description:  
Load Balancer

Internal Priority:

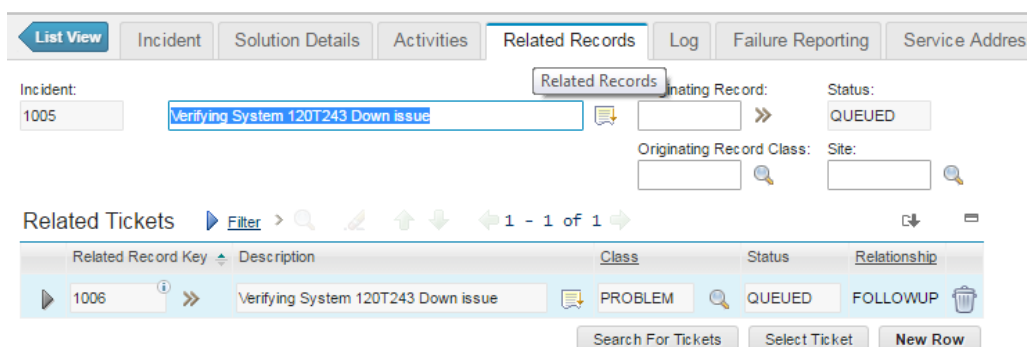
7. After you select the classification, check the blue box next to the best classification. That closes the dialogue and updates the classification field.



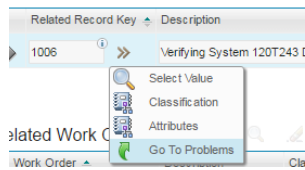
8. To create a problem record for further root cause analysis, go to the More Action section of the left-hand navigation panel and select **Create > Problem**. Once the problem is created, it creates a bridge from incident management to problem management.



9. After you create the problem, you can view the problem record from the Related Records Tab.



10. Navigate to the problem record from the incident. You need to update the problem record with the following information:
  - a. Assign to a person or group
  - b. Set Start Dates
  - c. Categorize the problem to make it available a comprehensive root cause review by the problem team.
11. Use the double arrows next to the Related Record Key field and Select **Go to Problems**



12. Double check that the problem record is classified. If the incident record was classified before you created the problem record, the problem record will be classified based on the classification and auto assigned to an owner group based on classification.

Classification:

Classification Path:

Class Description:

---

1006 **Verifying System 120T243 Down issue**

Owner:

Internal Priority:

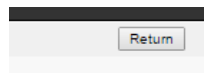
Target Finish:

13. If the classification does not pre-populate the owner group, go to Common Action on the left navigation menu, click **Select Owner**, and search for the group that you want to review the problem for root cause.
14. You may also do one or both of the following:
  - a. Give the problem record an urgency setting to help prioritize finding the root.
  - b. Set the Target Start or Target Finish to ensure analysis and work are performed in a timely manner.

Target Start:

Target Finish:

15. To return to the Incident and the trending analysis, click **Return** in the upper right hand corner.



16. To add a work log, click **New row** on the main incident screen, under the work log section. Record what analysis you performed and add any information about why this incident and others like it should be reviewed for root cause analysis.

Work Logs [Filter](#) > 1 - 2 of 2

Record	Class	Created By	Date	Type	Summary	View
1005	INCIDENT	MBIENFAN	10/5/16 11:24:33	UPDATE	Analysis Complete - Candidate for RCA - Prot	
1005	INCIDENT	MBIENFAN	10/5/16 10:43:06	CLIENTNOT	Slack update - channel open	

**Details**

Record: 1005

Class: INCIDENT

Created By: MBIENFAN

Date: 10/5/16 11:24:33

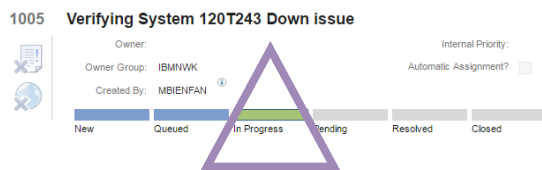
Type: UPDATE

Viewable? ☐

Summary:  
Analysis Complete - Candidate for RCA - Problem Created

Details:  
This issue has occurred with high frequency on Wednesdays at 8am Eastern. It is recommended a full root cause analysis and change be performed.

17. After recording the work entry on analysis, set the status to “In Progress” until the incident is resolved.



18. If you determine that several incidents are the same kind or could be related, you can relate the incidents using the Related Records tab. Showing this relation doesn’t cause the incidents to all be actioned the same. It simply shows the correlation between the events and the incidents that were created.

19. On the Related Records tab, click **Select Ticket** to add related ticket numbers (if you know them). You can also use the Search for Tickets function if you want to look for related events. .

Related Tickets [Filter](#) > 1 - 1 of 1

Related Record Key	Description	Class	Status	Relationship
1006	Verifying System 120T243 Down issue	PROBLEM	QUEUED	FOLLOWUP

[Search For Tickets](#) [Select Ticket](#) [New Row](#)

20. When using the Search for Tickets button, check the box for **Only Show Open Incidents** and select **Search**. The results will show in the section of the dialogue for search results. You can further filter the list by using the fields at the top of the dialogue or by using the filter row in the Search Results to find tickets in the results.

**Search For Tickets**

Search Incidents Search Service Requests Search Problems

Search incidents. Use one or more of the following fields to specify search criteria. [More information](#)

Search Terms (optional):

Classification: Asset:

Site: Configuration Item:

Show only global incidents that are not in CLOSED or RESOLVED state

Only show active global incidents?

Only show open incidents?

Search Clear fields

**Search Results** Filter > 1 - 5 of 6

Is Global?	Incident	Description	Status	Status Changed	In Attachment
<input type="checkbox"/>	1005	Verifying System 120T243 Down issue	INPROG	10/5/16 11:43:27	
<input type="checkbox"/>	1009	Python Application:unable to ping ordersapi-pluvial-lifeboat.mybluemix.net	NEW	10/5/16 11:41:35	

Close

21. To relate a record, check the box near the record row in the search results. Select **Relate Selected Tickets**. Then click **Close** to return to the record where the related tickets will display.

**Search Results** Filter > 1 - 5 of 6

Is Global?	Incident	Description	Status	Status Changed	In Attachment
<input type="checkbox"/>	1005	Verifying System 120T243 Down issue	INPROG	10/5/16 11:43:27	
<input checked="" type="checkbox"/>	1009	Python Application:unable to ping ordersapi-pluvial-lifeboat.mybluemix.net	NEW	10/5/16 11:41:35	
<input type="checkbox"/>	1008	Bluemix RSS:dashDB service (Enterprise MPP plans)	NEW	10/5/16 11:26:32	
<input checked="" type="checkbox"/>	1007	omni3.novalocal:Event count (alerts.status): 258	NEW	10/5/16 11:25:32	
<input type="checkbox"/>	1003	ibm.env5:INCIDENT: ibm.env5 (2 active alarms)	NEW	9/25/16 15:00:39	

Relate Selected Tickets

22. To see a list of related tickets to your problem ticket, look at Related Tickets section and take note of the relationships.

**Related Tickets** Filter > 1 - 3 of 3

Related Record Key	Description	Class	Status	Relationship
1006	Verifying System 120T243 Down issue	PROBLEM	QUEUE	FOLLOWUP
1009	Python Application:unable to ping ordersapi-pl	INCIDENT	NEW	RELATED
1007	omni3.novalocal:Event count (alerts.status): 2	INCIDENT	NEW	RELATED

23. To return to the original list of incidents that were recently updated and resolved, click the **List View** Arrow next to Incident header.

List View Incident

#### 4.1.1. Other steps or actions from the Start Center

As the site reliability engineer, you can use the Control Desk to see extensive data that helps you review trends and conduct incident analysis for the support of cloud or hybrid applications. These reviews and analysis can help you conduct problem management and understand the need for corrective action (runbooks), solutions (documented knowledge), or communications (to developers for change of behavior).

We've covered a few ways that you can use the portlets and data presented in the Start Center to conduct Incident Management. Other Start Center portlets include:

- a. KPI of Current Active Incidents
  - i. Enables the engineer and responders to understand the level of volume/impact the current incidents may be having in the infrastructure. For example, if only five or 10 incidents should be open at any given time and the current volume is more than this number, it highlights the need to take more proactive steps to decreasing incidents.
- b. Incidents up to 30 days closed, sorted by classification
  - i. The engineer may want to focus on the incidents he or she has classified as those were likely the incidents that showed interests in the trends occurring recently.
  - ii. This query view allows for the users to understand the number of incidents being worked and reviewed or analyzed for impact to the overall infrastructure.
- c. Severity 1 Event Incidents
  - i. This result set focuses on the top severity of the incidents occurring that are still in an Active state.
- d. Severity 2,3,4 Event Incidents
  - i. These incidents are "active" and not yet resolved through automation or manual steps and are of a lower severity than one.
- e. Newly Resolved Incidents
  - i. These incidents have recently been resolved and could be of interests for analysis and trending.
- f. Report List
  - i. These are just a few reports which can be launched from the Start Center to aid in the review of data being gathered and assimilated in Control Desk.
- g. Problems to Action
  - i. These are records where root analysis would be performed and corrective changes would be completed.

You can use these result sets and portlets directly in the Start Center or the go-to list view icon to work with the data in the list to filter, open and pare down the results to those showing the trends.

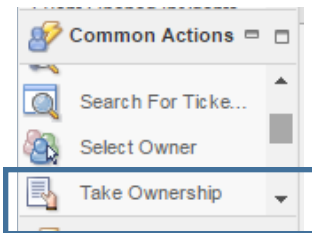
A site reliability engineer's pre-configured Start Center can be further configured to include additional portlets. You can also update the configuration to reflect additional parameters, lists, and queries.

[Learn more about Start Centers.](#)

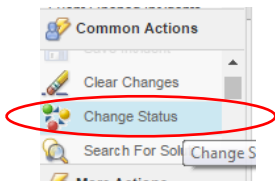
## 4.2. FIRST RESPONDER RESPONDS TO AN INCIDENT CREATED THROUGH CONTROL DESK

As a first responder, you can follow these steps to respond to an incident created through the Control Desk.

1. Go to the Start Center to view the Event Driven Incidents or Active Incidents -Assigned to Me. The portlets allow you to pick up or return to work you have recently worked on.
2. Select an incident from the list of Event Driven Incidents and click on the record in the result set to open the incident.
3. Once you open the record and decide to work on the incident, go to the left navigation under Common Actions and select **Take Ownership**. This assigns the incident to you to work and resolve.



The status of this incident automatically updates to a status of Queued. To begin work on the incident, go to the Common Actions section, click the incident, and change the status to In Progress.



4. Once in progress, scroll slightly to the middle of the record and locate the supporting Slack channel where others may be collaborating to resolve the incident.

### Incident Details

Summary:  
omni3.novalocal: A PROBE process email running on omni3.n

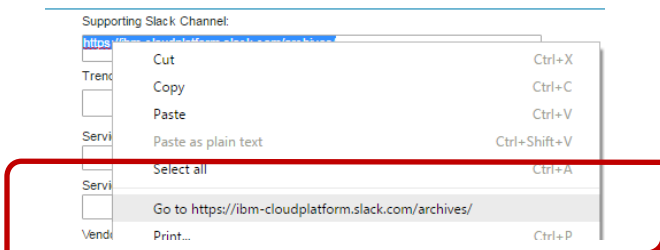
Details:

Supporting Slack Channel:

<https://ibm-cloudplatform.slack.com/archives/>

Trending Slack Channel:

5. Highlight the channel in the field and right-click **Go**. This takes you directly to the Slack channel. Use the channel to collaborate and find a solution to the issue.



- You might also want to review any trending Slack channel where the site reliability engineer or other responders are specifically reviewing incidents of a pattern or type. If there is a trending channel, you probably want to review and participate as necessary.

- To add comments or updates to the incident, scroll to the section called Work Logs, and click **New Row**. This creates an entry where you can provide updates. This shows you notes of the incident activities, entries from the Slack Channel, and information from NOI directly.

The following image shows an entry in the Incident recorded by Slack.

▶	1011	»	INCIDENT	MXINTADM ⓘ	10/6/16 09:42:33	CLIENTNOT ⓘ	Ownership of alert taken by case.	<input type="checkbox"/>
---	------	---	----------	------------	------------------	-------------	-----------------------------------	--------------------------

And this shows what it looks like when the entry is updated by NOI.

Work Logs [Filter](#) > 1 - 1 of 1

Record	Class	Created By	Date	Type	Summary	Viewable?
1007	INCIDENT	MXINTADM	10/6/16 09:48:50	CLIENTNOTE	Alert assigned to root by case.	<input type="checkbox"/>

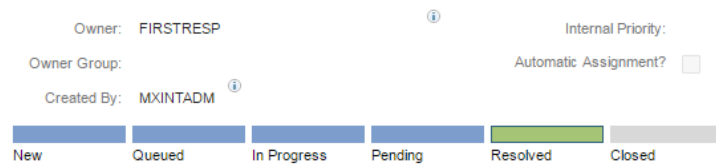
New Row

- As an optional task, you can classify the record if the known issue is identified, recognized and found in the Cloud Classifications structure. Use the double arrows next to Classification Path field and click **Classify**. To select the classification, use the blue box next to the word. To expand and see more hierarchy, use the plus sign.



- a. Once the incident issue is resolved, you can mark the incident as “resolved.” This can be done by using the change status under Common Actions in Control Desk or by writing the following command in the Slack channel for the incident:

noi resolve <eventNumber>



These are custom slackbots that integrate the communications of various tools in the overall toolchain.

This command works both from the "global" channel (that is, resolve any event) and from the dedicated channel for a specific event.

If the incident is a global incident that affects many systems, you can set the incident to a global incident and relate other records to it. [Visit the IBM Knowledge Center for detailed steps.](#)

#### 4.2.1. Other step or actions a first responder can take

As a first responder, you can use the Control Desk to update and review data of incidents that are in support of cloud or hybrid applications. These actions and updates:

- Ensure accurate data for analysis
- Help you find other incidents with similar solutions and runbooks,
- Return to a slack channel to find past collaborators for resolution or find past actions taken for an incident of similar type
- Discover communications to developers for change of behavior

We have already discussed a few portlets, but there are a number of portlets in the Start Center that you can use to review active incidents, resolve incidents, take ownership, and find similar incidents or trends to resolve incidents quickly.

Other portlets available to the responder through the Start Center are:

- a. Quick Inserts
  - i. To create Incidents or problems for future action
- b. Open Incidents – KPI
  - i. Enables the engineer and responders to understand the level of volume/impact the current incidents may be having in the infrastructure. For example, if only five or 10 incidents should be open at any given time and the current volume is more than this number, it highlights the need to take more proactive steps to decreasing incidents.
- c. Average Incident Work Time – KPI

- i. This key performance indicator represents how long an incident is worked before it is resolved.
- d. Active Incidents Assigned to Me
  - i. This shows incidents that belong to you. This ensure no one else works on this incident or that they have a follow-up action or interest.
- e. Severity 1 Incidents – Open
  - i. This result set focuses on the top severity of the incidents occurring that are still in an Active state.
- f. Severity 2, 3, 4, Incidents – Open
  - i. These incidents are “active” and not yet resolved through automation or manual steps and are of a lower severity than one.
- g. Newly Created Problems
  - i. These are records where root cause analysis would be performed and corrective changes would be completed.

These result sets and portlets can be used directly in the Start Center or the go-to list view icon to work with the data in the list view to filter, open and pare down the results to those the responder wishes to work with or review.

[Learn more about the Start Center in the IBM Knowledge Center.](#)

## 5. PREREQUISITES FOR SETUP

---

For this toolchain integration, you need the following components of IBM Control Desk, Netcool Operations Insight / Omnibus, and Slack: You need to have IBM Control Desk installed. Follow the instructions in the following links to learn how to install based on whether you have an on-premises environment or a cloud-based environment.

- [Installation of IBM Control Desk - On Premise](#)
- [How to Access IBM Control Desk - On Cloud](#)

You need to have Omnibus installed. Use the following links and choose the instructions that match your local requirements (connections to LDAP, choice of operating system and database, H/A considerations and so on). The integration of Omnibus into the toolchain is loosely coupled and will function with any IBM-supported configuration of Omnibus.

- [Omnibus v8.1 installation documentation](#)
- [Netcool Operations Insight v1.4 installation documentation](#)
- [Installation best practices](#)

## 6. CONFIGURATION OF CONTROL DESK

---

### 6.1. CREATE AND DEFINE START CENTERS

#### 6.1.1. Start Centers

To set up the Start Centers used in this business flow, you will create a Start Center template using several items, queries, “where” clauses, KPIs, and the create and update commands..

We created two Start Centers for this scenario, one labeled Site Reliability Engineer and the other labeled First Responder.

Use the screen shots in this document along with the queries and KPIs accompanying the instructions to create your own reusable Start Centers.

First, you need to create a template. Follow the standard instructions in the IBM Knowledge Center to get started:

[Managing Start Center templates](#)

[Get Started with Control Desk: Start Desk](#)

#### 6.1.2. Creating queries

Follow the steps in the Knowledge Center’s IBM Control Desk documentation, [Working with work view queries](#), to create predefined and saved queries that you can use for the Start Centers to have them available in the applications.

Visit the IBM Knowledge Center’s [SQL WHERE clause searches](#) documentation for instructions and steps for creating WHERE clause queries

We created and defined several queries to support the Start Centers. The queries are listed below so you can easily and quickly recreate them.

Recently resolved incidents	(status = 'RESOLVED' and upper(externalsystem) = 'EVENTMANAGEMENT')
Recently updated and resolved incidents	ticketid in ( select recordkey from worklog where modifydate > current timestamp - decimal(240000,6,0) ) and status in (select value from synonymdomain where maxvalue in ('RESOLVED') and domainid = 'INCIDENTSTATUS') and (current timestamp > actualfinish) order by internalpriority ASC
Priority 2,3,4 incidents	((status = 'INPROG' or status = 'NEW' or status = 'PENDING' or status = 'QUEUED') and upper(externalsystem) = 'EVENTMANAGEMENT' and (reportedpriority = 2 or reportedpriority = 3 or reportedpriority = 4))
Priority 1 incidents	((status = 'INPROG' or status = 'NEW' or status = 'PENDING' or status = 'QUEUED') and upper(externalsystem) = 'EVENTMANAGEMENT' and reportedpriority = 1)
Incidents closed up to 30 days	(status = 'CLOSED') and actualfinish > (current timestamp - 30 days) order by internalpriority ASC
All event management incidents	((status = 'INPROG' or status = 'NEW' or status = 'PENDING' or status = 'QUEUED') and upper(externalsystem) = 'EVENTMANAGEMENT')
Incidents assigned to logged in user	((status = 'INPROG' or status = 'NEW' or status = 'PENDING' or status = 'QUEUED')) and (owner = :USER)

Open problems	(historyflag = 0) and (status in (select value from synonymdomain where maxvalue in ('NEW','PENDING','QUEUED','INPRG') and domainid in ('PROBLEMSTATUS'))))
---------------	---

### 6.1.3. Creating KPIs

We used several Key Performance Indicators (KPIs) to create the Start Centers for these use cases. Visit the IBM Knowledge Center documentation, [Creating key performance indicators](#), to learn how to create or reuse KPIs.

The following statements are the basis for how we created the KPIs we used in this guide.

Open incidents	select count(*) from INCIDENT where status in (select value from synonymdomain where maxvalue in ('NEW','QUEUED','PENDING','INPROG'))
Average work time of incidents	select avg(TIMESTAMPDIFF(8, char(ACTUALFINISH-ACTUALSTART))) from Incident

## 6.1. CLASSIFICATION STRUCTURE

A new cloud classification hierarchy was created to properly support and categorize the incidents being created in Control Desk by the event monitoring system and by the first responders. To create classifications in IBM Control Desk, use the Administration > Classification Application.

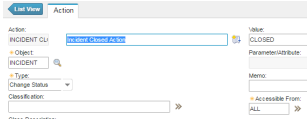
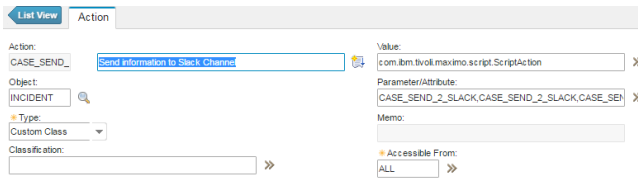
The following table shows the cloud classification structure recommended for use in the support of cloud infrastructure. You can expand and personalize this classification structure into other classification hierarchies.

Parent	Level 1	Level 2	Level 3
Cloud	IaaS	Virtual Server	
		Network	Load Balancer
		Storage	Block Storage
			Object Storage
		Netflix OSS	Zuul
			Eureka
			Hystrix
			Ribbon
	Container	Container Image	
		Container Runtime	
		Container Orchestration	
		Container Registry	
	PaaS	Runtimes	Liberty for Java
			Runtime for Swift
			Node.js
			Python
			Ruby
		Data	MongoDB
			Claudant NoSQL DB
			IBM Graph
		Analytics	BigInsights for Apache Hadoop
			Apache Spark
		Watson	
		Mobile	
		DevOps	
		Web & Application	
		Network	Content Delivery
			Virtual Private Network
		Integration	
		Security	
		Storage	
		Business Analytics	
		Internet of Things	
		APIs	
	SaaS	Commerce	IBM Digital Commerce
		HR	IBM Recruitment
			IBM HR Administration
	Application		

## 6.2. ESCALATIONS

You can configure escalations to automatically monitor the critical processes in your enterprise. You can also use escalations for events, such as contract expiration, a change in the status of a records, or a change in the ownership of a record.

The following escalations are used in this implementation for updating the incident status or to take an action to send data to integration points.

Close resolved Incidents after 5 days	STATUS IN (SELECT VALUE FROM SYNONYMDOMAIN WHERE DOMAINID = 'INCIDENTSTATUS' AND MAXVALUE = 'RESOLVED')	Escalation point is 5 days	<b>Action of Incident Close –</b> 
Process closed incidents – Slack	STATUS='CLOSED'	No Escalation Point	<b>*Action of Send information to Slack Channel</b> 

*\*Additional details on the script used for the Process closed incidents can be found in section 5.4 of this document.*

The following documentation in the IBM Knowledge Center gives you more information about escalations:

- [Escalations overview](#)
- [Working with escalations](#)
- [Activating escalations](#)

## 6.3. CONFIGURING FIELDS FOR INTEGRATION TO SLACK

### Field additions for integration to Slack

To connect IBM Control Desk, Slack, and push and pull data from the systems, you need to add fields in Control Desk to display Slack data. To do so, follow these steps:

In database configuration:

- 1) Add the new attribute CASE\_SC\_TRENDING to TICKET table. ALN(300), Trending Slack Channel
- 2) Add the new attribute CASE\_SLACK\_CHANNEL to TICKET table. ALN(300), Supporting Slack Channel
- 3) Turn on Admin mode
- 4) Apply configuration changes
- 5) Turn off Admin mode

In application designer

6) Add a new attribute, INCIDENT.CASE\_SC\_TRENDING and INCIDENT.CASE\_SLACK\_CHANNEL, to Incident application above the Service Group.

#### **6.4. SEND A MESSAGE TO SLACK WHEN THE STATUS OF THE TICKET CHANGES TO CLOSED**

To send a message to Slack when the status of the ticket changes to CLOSED

##### **Create script with action launch point**

1. Call the script SendToSlack.sh (on Linux) with three parameters  
  
CASE\_SLACK\_CHANNEL: SlackChannel  
  
TICKETID: Ticket #  
  
STATUSDATE: Date of closure
2. Navigate to > System Configuration > Platform Configuration > Automation Scripts > More Action > Create > Script with Action Launch Point
3. In the Launch Point field, type "CASE\_SEND\_2\_SLACK."
4. In the Description field, type "Send information to Slack channel."
5. In the Action field, type "CASE\_SEND\_2\_SLACK."
6. In the Description field, type "Send information to Slack channel."
7. For the Object field Object, click the search icon and type "incident." Select Incident.
8. Check the box for Active.
9. Under Script, check "New" in the Boolean field.
10. Select the Next button.

Create Script with Action Launch Point : Step 1 of 3

Specify the object and an action that launch the script. You can reuse an existing script or specify a new one. If you choose a new script, the wizard guides you through the script creation process. [More information](#)

\* Launch Point:

CASE\_SEND\_ Send information to Slack Channel

Action:

CASE\_SEND\_ Send information to Slack Channel

Object:

INCIDENT

Active?

☒

Script

☒ New

☐ Existing: Script:

Cancel Next

11. Define the four Variable parameters for the script.
12. Select the Variables tab of the automation script.
13. To add each variable you will select the new row button.
14. In the first variable, type "in\_CASE\_SLACK\_CHANNEL".
15. In the description field, add in\_CASE\_SLACK\_CHANNEL.
16. Set the Binding Type field to Attribute.
17. Set the variable Type to IN.
18. Check the box next to Override?
19. In the Launch Point Variable field, type "CASE\_SLACK\_CHANNEL".
20. All other fields will be left null or blank.

Create Script with Action Launch Point : Step 2 of 3

Launch Point: CASE\_SEND\_ Send information to Slack Channel

Object: INCIDENT

Script: CASE\_SEND\_2\_SLACK Send information to Slack Channel

Log Level: DEBUG

Script Language: python

You can import a script file that you created in another application or you can enter a script in the Source Code field in the next step.

Import a Script File:

Variables  1 - 1 of 1

Variable	Variable Type	Binding Type	Binding Value	Override?
in_CASE_SL	IN	ATTRIBUTE		<input checked="" type="checkbox"/>

Details

Specify a variable to use in the script, including the variable type and the binding type. Depending on the binding type that you specify, you must enter additional values in the associated fields. [More information](#)

Details

Variable: in\_CASE\_SL

Variable Type: IN

Binding Type: ATTRIBUTE

Literal Data Type:

Global Binding Value:

Launch Point Attribute: CASE\_SLACK\_CHANNEL

Override? ☒

Suppress Validation? ☐

Suppress Access Control? ☐

Suppress Action? ☐

21. For the second variable, type "in\_STATUS" in the Variable field.
22. In the Description field, add "in STATUS".
23. Set the Binding Type field to Attribute.
24. Set the variable Type to IN.
25. Check the box next to Override?
26. In the Launch Point Variable field, type "STATUS".
27. All other fields will be left null or blank.



Create Script with Action Launch Point : Step 2 of 3

Launch Point: CASE\_SEND\_ Send information to Slack Channel Object: INCIDENT

Script: CASE\_SEND\_2\_SLACK Send information to Slack Channel Log Level: DEBUG

Script Language: python

You can import a script file that you created in another application or you can enter a script in the Source Code field in the next step.

Import a Script File: Browse... Import

Variables Filter 1 - 2 of 2

Variable	Variable Type	Binding Type	Binding Value	Override?
in_CASE_SL	IN	ATTRIBUTE		<input checked="" type="checkbox"/>
in_TICKETID	IN	ATTRIBUTE		<input checked="" type="checkbox"/>

Details

Specify a variable to use in the script, including the variable type and the binding type. Depending on the binding type that you specify, you must enter additional values in the associated fields. [More information](#)

Details

Variable: in\_TICKETID

Variable Type: IN

Binding Type: ATTRIBUTE

Literal Data Type:

Global Binding Value:

Launch Point Attribute: TICKETID

Override? ☒

Suppress Validation? ☐

Suppress Access Control? ☐

Suppress Action? ☐

New Row

28. For the third variable, type "in\_STATUSDATE" in the Variable field
29. In the Description field, add in\_STATUSDATE.
30. Set the Binding Type field to Attribute.
31. Set the variable Type to IN.
32. Check the box next to Override?
33. In the Launch Point Variable field, type "STATUSDATE".
34. All other fields will be left null or blank

Create Script with Action Launch Point : Step 2 of 3

Launch Point: CASE\_SEND\_ Send information to Slack Channel

Object: INCIDENT

Script: CASE\_SEND\_2\_SLACK Send information to Slack Channel

Log Level: DEBUG

Script Language: python

You can import a script file that you created in another application or you can enter a script in the Source Code field in the next step.

Import a Script File:

Variables  1 - 4 of 4

Variable	Variable Type	Binding Type	Binding Value	Override?
in_CASE_SL	IN	ATTRIBUTE		<input checked="" type="checkbox"/>
in_TICKETID	IN	ATTRIBUTE		<input checked="" type="checkbox"/>
in_STATUSC	IN	ATTRIBUTE		<input checked="" type="checkbox"/>
in_STATUS	IN	ATTRIBUTE		<input checked="" type="checkbox"/>

Details

Specify a variable to use in the script, including the variable type and the binding type. Depending on the binding type that you specify, you must enter additional values in the associated fields. [More information](#)

Details

Variable: in\_STATUS

Variable Type: IN

Binding Type: ATTRIBUTE

Literal Data Type:

Global Binding Value:

Launch Point Attribute: STATUS

Override? ☒

Suppress Validation? ☐

Suppress Access Control? ☐

Suppress Action? ☐

35. For the fourth variable, type “in\_TICKETID” in the Variable field.
36. In the description field, add in\_TICKETID.
37. Set the Binding Type field to Attribute.
38. Set the variable Type to IN.
39. Check the box next to Override?
40. In the Launch Point Variable field, type “TICKETID.”
41. All other fields will be left null or blank.

Create Script with Action Launch Point : Step 2 of 3

Launch Point: CASE\_SEND\_ Send information to Slack Channel

Object: INCIDENT

Script: CASE\_SEND\_2\_SLACK Send information to Slack Channel

Log Level: DEBUG

Script Language: python

You can import a script file that you created in another application or you can enter a script in the Source Code field in the next step.

Import a Script File:  Browse... Import

Variables [Filter](#) > [1 - 3 of 3](#)

Variable	Variable Type	Binding Type	Binding Value	Override?
in_CASE_SL	IN	ATTRIBUTE		<input checked="" type="checkbox"/>
in_TICKETID	IN	ATTRIBUTE		<input checked="" type="checkbox"/>
in_STATUSD	IN	ATTRIBUTE		<input checked="" type="checkbox"/>

Details

Specify a variable to use in the script, including the variable type and the binding type. Depending on the binding type that you specify, you must enter additional values in the associated fields. [More information](#)

Details

Variable: in\_STATUSD

Variable Type: IN

Binding Type: ATTRIBUTE

Literal Data Type:

Global Binding Value:

Launch Point Attribute: STATUSDATE

Override? ☒

Suppress Validation? ☐

Suppress Access Control? ☐

Suppress Action? ☐

New Row

42. Once all variables and parameters are added, click Next.

43. Copy and paste the script "Create Script with Action Launch Point" found on [GitHub in the field Source Code](#).

44. Click the box Create.

Create Script with Action Launch Point : Step 3 of 3

You can enter a script in the Source Code field, or you can import a script file in the previous step.

Launch Point: CASE\_SEND\_ Send information to Slack Channel

Object: INCIDENT

Script: CASE\_SEND\_2\_SLACK Send information to Slack Channel

Source Code:

```
# Python Automation script for TPAe 7.1.1.7 and above to execute a command on the Application Server
import sys
from java.io import *
from java.lang import Runtime

#
# script CASE_SEND_2_SLACK.py
#
# Inputs:
# in_CASE_SLACK_CHANNEL
# - Slack Channel for this incident
# in_TICKETID
```

Cancel Previous Create

## Creating escalation

1. Navigate to > System Configuration > Platform Configuration > Escalations
2. For the Title of the Escalation type> CASE\_C\_INCIDENTS
3. Give it a description of > Process closed incident records.
4. Select INCIDENT for the Applies to field (object).
5. Type STATUS=='CLOSED' in the Condition field.
6. Select 2m,\* ,\* ,\* ,\* ,\* ,\* ,\* in the Schedule field.

The screenshot shows the IBM Escalations configuration interface. The 'Escalation' tab is active, displaying the following fields:

- Escalation:** CASE\_C\_INCIDENTS
- Process closed incident records**
- Site:** (empty)
- Active?:** (checked)
- Organization:** (empty)
- Schedule:** 2m,\* ,\* ,\* ,\* ,\* ,\* ,\*
- Calendar Organization:** (empty)
- Calendar:** (empty)
- Shift:** (empty)
- Condition:** STATUS=='CLOSED'
- Create Successful Execution Entry?:** (unchecked)
- Last Run Time:** (empty)

Below the main form, the 'Validation Results' section shows a table with one row:

Escalation Point	Elapsed Time Attribute	Elapsed Time Interval	Interval Unit of Measure	Organization	Calendar	Shift
1						

The 'Details' section for the first escalation point is also visible, showing fields for Elapsed Time Attribute, Elapsed Time Interval, Interval Unit of Measure, Repeat?, Organization, Calendar, and Shift.

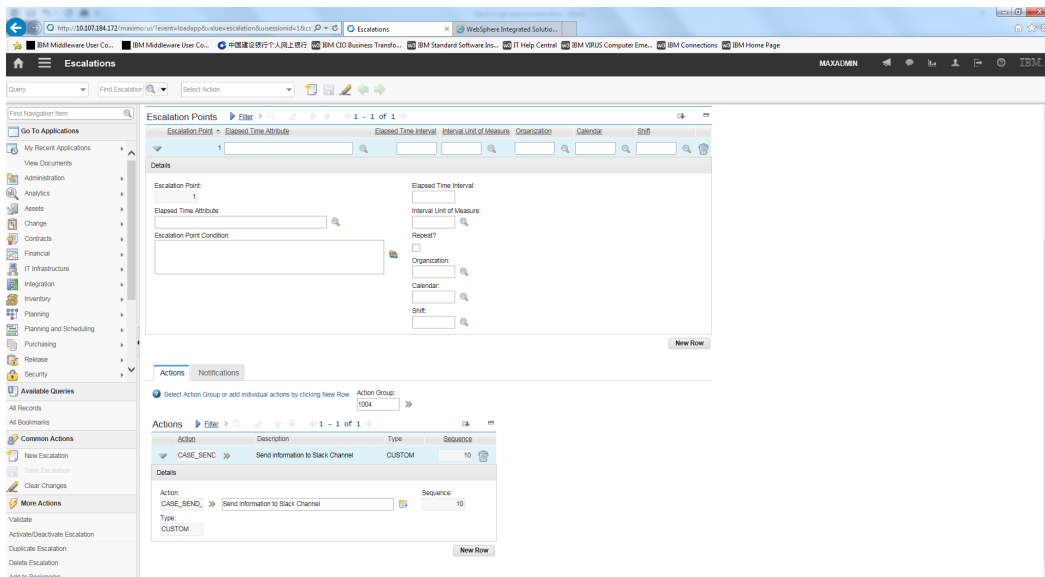
7. Click New Row to add one escalation point.

The screenshot shows the IBM Escalations configuration interface after adding a new escalation point. The 'Escalation Points' table now has two rows:

Escalation Point	Elapsed Time Attribute	Elapsed Time Interval	Interval Unit of Measure	Organization	Calendar	Shift
1						
2						

The 'Details' section for the second escalation point is also visible, showing fields for Elapsed Time Attribute, Elapsed Time Interval, Interval Unit of Measure, Repeat?, Organization, Calendar, and Shift.

8. For the one Escalation Point, click on the new row to Add one Action: Search for action CASE\_SEND\_2\_SLACK.



9. Save the Escalation

10. Under More actions, use the action Validate, to validate the escalation.

11. Under More actions, use the action Activate, to activate the escalation of a status.

## 7. HOW TO SET UP THE INTEGRATION OF NOI WITH IBM CONTROL DESK

### 7.1. NETCOOL OPERATIONS INSIGHT TO CONTROL DESK INTEGRATION

Please note that, for historical reasons, many of the technical assets are called Maximo, TSRM, or SCCD as well as ICD. These all refer to the same product and are functionally synonyms.

#### 7.1.1. TSRM gateway installation

The integration is based on the TSRM gateway.

Install the TSRM gateway per the standard IBM instructions detailed in the following links. Adjust them for your local requirements.

- [Gateway documentation](#)
- [Gateway download instructions](#)

The following videos explain how to perform the basic installation and configuration:

- [Installing the TRSM Gateway on Omnibus 8.1](#)
- [Netcool TSRM Integration : Viewing created incidents from Omnibus in TSRM](#)

#### 7.1.2. Basic TSRM gateway configuration:

After installing the gateway, configure it to communicate with ICD and test the base configuration before implementing the customizations detailed in section 8.1.3. Follow the instructions in these IBM Knowledge Center documents:

- [Installing the gateway](#)
- [Testing Netcool/OMNIBus communication with TSRM](#)

#### 7.1.2.1. Journal updates

To enable NOI to update ICD with any NOI journal entries or Slack messages, you must activate the journal integration.

Follow the instructions in this IBM Knowledge Center document:

[Configuring TSRM to receive journal entries from Netcool/OMNIBus events](#)

Or watch the video, [TSRM gateway: Configure TSRM to receive journal entries from Netcool/OMNIBus alerts](#)

Optional configurations

The following configurations are not mandatory for NOI-ICD integration, but many customers implement them.

- [Extend the size of the summary field to match possible long NOI messages](#)
- [Create a custom message object for improved performance](#)
- [Fine tuning the performance of gateway event processing](#)

#### 7.1.3. Integration customizations

The best practices in this guide depend on the following customizations to the default integration:

For the purposes of this documentation, we assume that you've named your gateway G\_ICD.

##### 7.1.3.1. Change Ticket content details

The configuration file `$NCHOME/netcool/omnibus/gates/tsrm/tsrm.mapping` contains the translation between NOI field and ICD fields.

The default mapping is as follows:

```
CREATE MAPPING StatusMap
(
    'CLASS'           = 'INCIDENT',
    'DESCRIPTION'     = '@Node' + ":" + '@Summary' ON INSERT ONLY,
    'REPORTEDBY'      = 'NETCOOL' ON INSERT ONLY,
    'REPORTDATE'      = TO_TIME('@FirstOccurrence') ON INSERT ONLY,
    'REPORTEDPRIORITY' = Lookup('@Severity','SeverityTable') ON INSERT ONLY,
    'STATUS'          = Lookup('@Severity', 'StatusTable'),
    'TTNumber'        = '@TTNumber'
);

CREATE MAPPING JournalMap
(
    'CLASS'           = 'INCIDENT'
```

You should change it to:

```
CREATE MAPPING StatusMap
(
    'CLASS'          =      'INCIDENT',
    'DESCRIPTION'     =      '@Node' + ":" + '@Summary' ON INSERT ONLY,
    'EXTERNALSYSTEM' =      'EVENTMANAGEMENT' ON INSERT ONLY,
    'REPORTDATE'      =      TO_TIME('@FirstOccurrence') ON INSERT ONLY,
    'REPORTEDPRIORITY' =      Lookup('@Severity','SeverityTable') ON INSERT ONLY,
    'STATUS'          =      Lookup('@Severity', 'StatusTable'),
    'TTNumber'        =      '@TTNumber'
);

CREATE MAPPING JournalMap
(
    'CLASS'          =      'INCIDENT',
    'Chrono'         =      '@Chrono',
    'CREATEDATE'      =      TO_TIME('@Chrono'),
    'DESCRIPTION'     =      TO_STRING('@Text1'),
    'DESCRIPTION_LONGDESCRIPTION' =      TO_STRING('@Text1') +
TO_STRING('@Text2') + TO_STRING('@Text3'),
    'ServerName' = STATUS.SERVER_NAME,
    'ServerSerial' = STATUS.SERVER_SERIAL
);
```

### 7.1.3.2. Add a journal entry for new ticket

It can be useful to add automated journal entries to NOI when ICD tickets are created or changed. The simplest way to implement this is by adding a new trigger to the NOI Object Server.

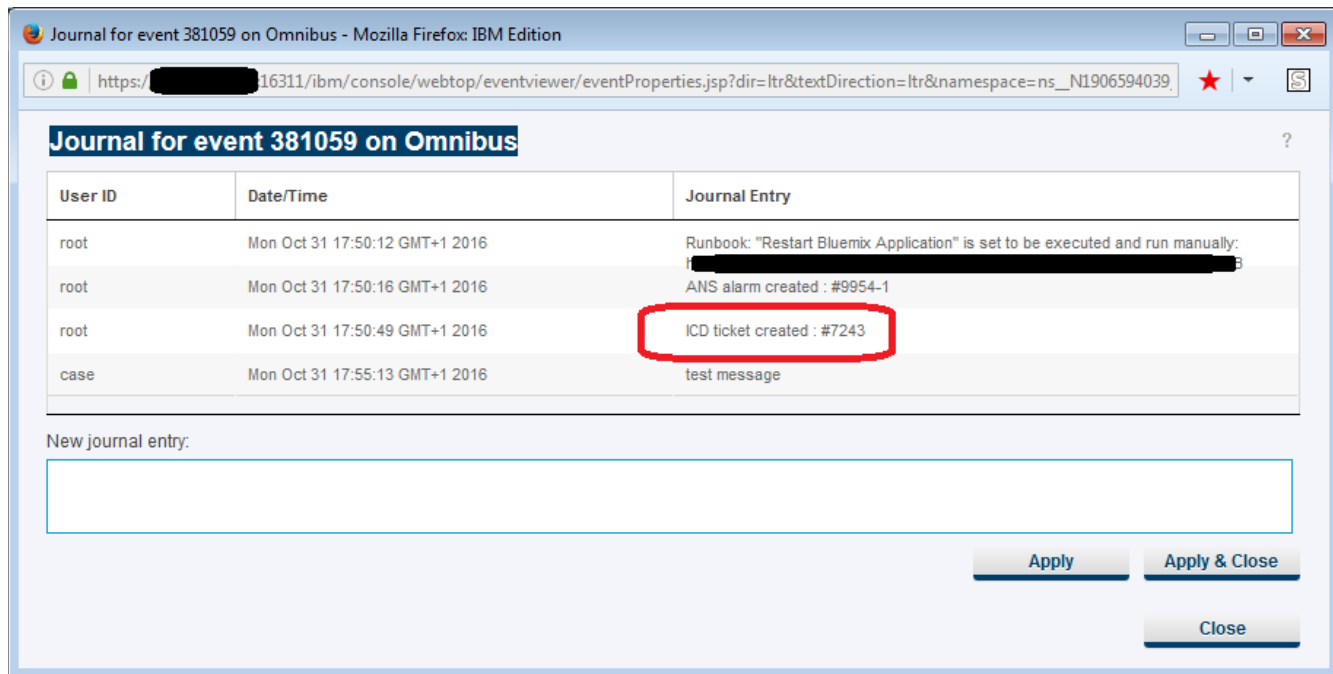
Upload the file CASE\_NOI-ICD-Journal.sql to the OMNIbus server and run the following command:

```
$OMNIHOME/bin/nco_sql -user <username> -password <password> -server <server_name>
< /tmp/CASE_NOI-ICD-Journal.sql
```

Further documentation may be found in the IBM Knowledge Center at [Starting the SQL interactive interface](#)

If you have multiple ObjectServers, you must run this command multiple times.

The trigger waits for ICD to send an update to NOI with the new ticketID and then writes a journal entry on the event, as the following image shows.



If there is integration between NOI and Slack, the journal update will be forwarded to Slack too.

#### 7.1.3.3. Automate ticket creation

OMNibus triggers can automate many tasks, such as creating ICD tickets for new events.

Two such triggers are CASE\_ICD\_Forward\_NewEvent and CASE\_ICD\_Forward\_UpdatedEvent. The first creates an ICD ticket when a new incoming event matches a specific condition (that is, the severity is 5/Critical), and the second creates a ticket when an event changes to match a specific condition (that is, an operator or another automation raised the severity of the event).

Make this change by loading the CASE\_NOI-ICD-NewTicketTriggers.sql file into the OMNibus ObjectServer.

Upload the file to the OMNibus server and run the following command:

```
$OMNIHOME/bin/nco_sql -user <username> -password <password> -server <server_name> < /tmp/ CASE_NOI-ICD-NewTicketTriggers.sql
```

You can change the threshold either by modifying the SQL file and reloading it or by changing the trigger in the OMNibus Admin console.

#### 7.1.3.4. Synchronize more fields between NOI and ICD

The file tsrm.map controls which NOI fields are sent to ICD tickets and in what format. Check out the documentation in IBM Knowledge Center for more information: [Configuring the Tivoli Netcool/OMNibus Gateway for TSRM](#).

To add more fields, such as the OWNER of the ticket, you must add an extra mapping table to the beginning of the file:

```
CREATE LOOKUP UserTable (
  {0 , 'MAXADMIN'},
  {1 , 'ICDUser #1'},
  {2 , 'ICDUser #2 },
  {65534, "  } )
```



```
DEFAULT = '';
```

And further on:

```
CREATE MAPPING StatusMap
(
    'CLASS'      = 'INCIDENT',
    'OWNER'      = Lookup('@OwnerUID','UserTable'),
```

Take care to keep the UserTable updated with the relevant mapping between NOI user id numbers and ICD user names.

The file NOI-ICD-modifications.zip includes an example of the modified file.

#### **7.1.3.5. Add new statuses to ticket status**

By default, the only change in status NOI pushes to ICD is RESOLVED when the event status changes to Clear (0). To send more statuses (for example, updating the status to INPROG when a user takes ownership of an event in NOI), you need to make the following changes:

- Create a new field in the NOI schema, called CASE\_ICD\_Status, which holds the status to be pushed to ICD
- Modify the tsrm.map file so the ICD STATUS field is mapped to CASE\_ICD\_Status and not to Severity
- Add an Omnibus trigger, CASE\_Update\_ICD\_Status, to modify the value of CASE\_ICD\_Status when the owner of a ticket changes or the severity of the ticket changes to 0.
- Add an Omnibus trigger, CASE\_Update\_ICD\_Status\_onDeDup, to make the same modification when the event is changed by an incoming event message instead of by updating an existing message.

The file NOI-ICD-modifications.zip includes the modified files and instructions.

#### **7.1.3.6. Add tools to NOI dashboard**

To open an ICD ticket on an existing event, use a SQL tool to run the following command:

```
update alerts.status set LogTicket =1 where Serial in ( $selected_rows.Serial
);
```

To launch into ICD to view the ticket, use a script tool to run the following script:

```
var str = "{@TTNumber}";
if (str != "") {
    window.open          ("http://<ICDserver>/maximo/ui/maximo.jsp?
event=loadapp&value=incident&additionalevent=useqbe&additionaleventvalue=tick
etid=" + str);
}
else
{
    window.alert("This event has no Control Desk ticket associated");
}
```

The file NOI-ICD-modifications.zip includes the tools and instructions.

#### **7.1.3.7. Update the description of journal/work orders.**

If it is set up, then NOI forwards journals entries to work orders that are attached to the Incident. However, by default, the description of the work order is hardcoded to NETCOOL JOURNAL ENTRY, which means that users must unfurl the work order to see the true description.

Change the JournalMap section of the tsrm.map file from

```
'DESCRIPTION'      =   'NETCOOL JOURNAL ENTRY',
```

to

```
'DESCRIPTION'      =   TO_STRING('@Text1'),
```

to make the proper text more visible.

Note that you will need to extend the size of the WORKORDER.DESCRPTION field to accommodate the possible longer length of the journal entry (see section 7.1.2.2 for a similar change done to the ticket's summary field).

The file NOI-ICD-modifications.zip includes a modified tsrm.map file.

#### **7.1.3.8. Synchronize more fields between ICD and NOI**

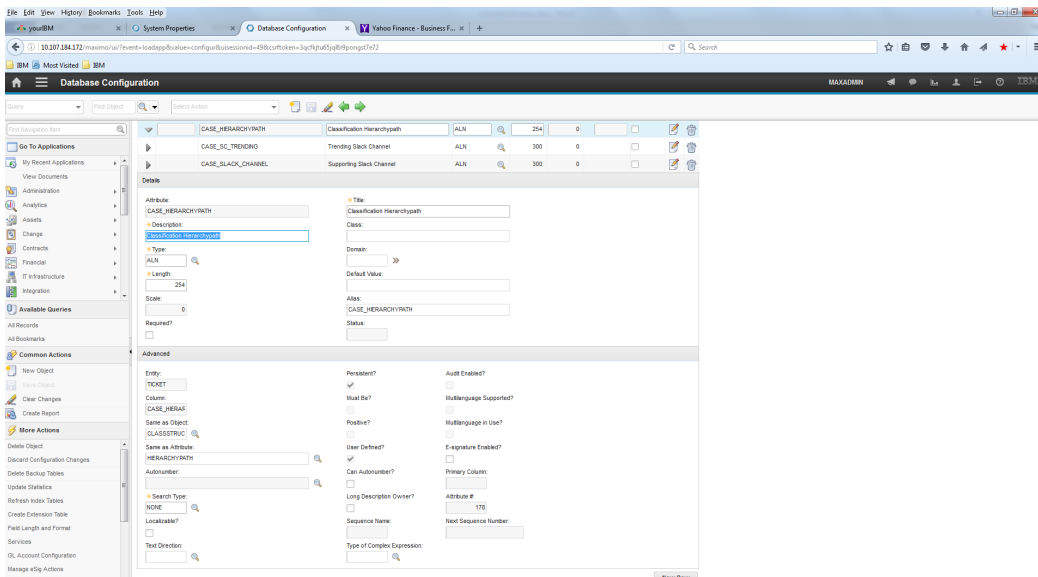
By default, the only field that is synchronized back to NOI from ICD is the ticket status (field STATUS in ICD and field TicketStatus in NOI).

The synchronized fields are configured in **Integration > Object Structures** in ICD and in **\$OMNIHOME/gates/tsrm/tsrm.script** in NOI.

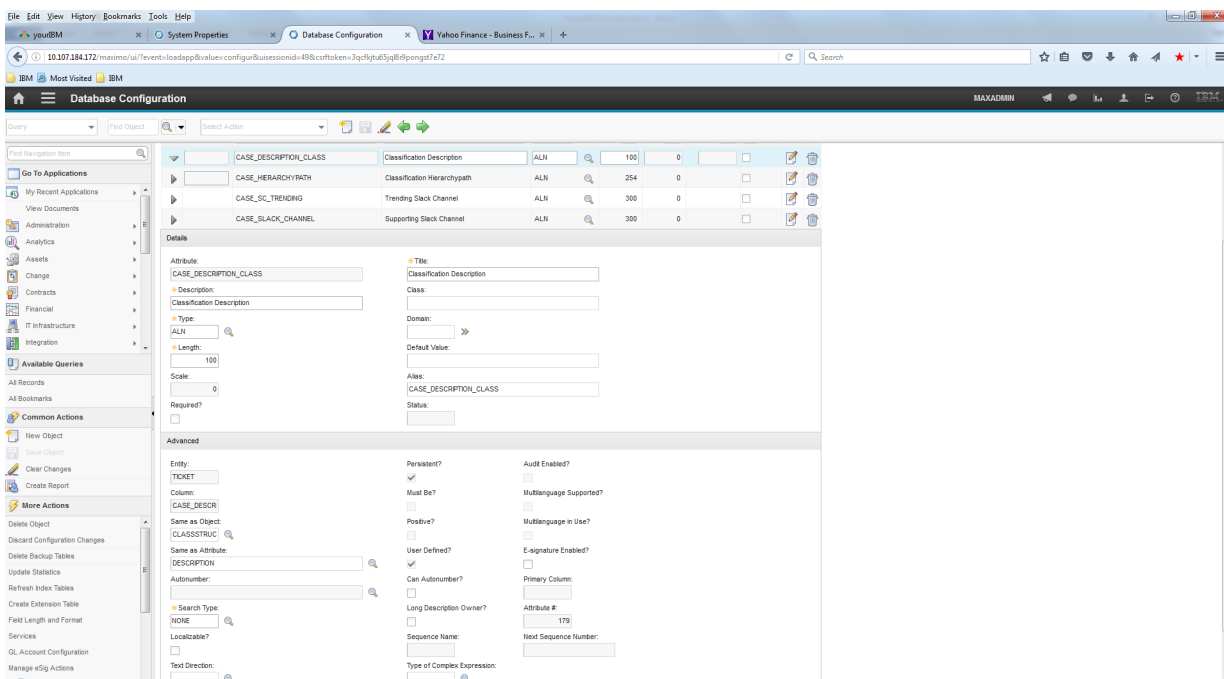
Generic instructions to add more fields can be found in the IBM Knowledge Center document: [Retrieving additional fields from TSRM](#).

One of the most important ticket attributes to synchronize is the DESCRIPTION\_CLASS, the human readable version of the ticket's classification. This field cannot be synchronized using the standard implementation because the attributes HIERARCHYPATH and DESCRIPTION\_CLASS do not reside in the incident record (in its child record CLASSSTRUCTURE), and NOI is not able to sync with the Control Desk system without a configuration change to the Ticket Table. The following steps expand on the generic instructions and detail how to add these fields to the integration. Follow the default steps and then add the following ones.

1. Add the attribute the CASE\_HIERARCHYPATH to TICKET table



## 2. Add the attribute CASE\_DESCRIPTION\_CLASS to the TICKET table



## 3. Add the Crossover fields to the domain TSDCLSSTRUCT2TK

Crossover Fields Filter 1 - 5 of 6

Source Field	Destination Field	Accept NULL value?	No Overwrite?	Sequence
CLASSIFICATIONID	CLASSIFICATIONID	<input type="checkbox"/>	<input type="checkbox"/>	
COMMODITYGROUP	COMMODITYGROUP	<input type="checkbox"/>	<input type="checkbox"/>	
DESCRIPTION_CLASS	CASE_DESCRIPTION_CLASS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
HIERARCHYPATH	CASE_HIERARCHYPATH	<input type="checkbox"/>	<input type="checkbox"/>	
INDICATEDPRIORITY	INDICATEDPRIORITY	<input type="checkbox"/>	<input type="checkbox"/>	

Source Field:  
HIERARCHYPATH

Destination Field:  
CASE\_HIERARCHYPATH

Accept NULL value?  
☐

No Overwrite?  
☐

Condition on Source:  
 >>

Condition on Destination:  
 >>

Sequence:

OK Cancel

Crossover Fields Filter 1 - 5 of 6

Source Field	Destination Field	Accept NULL value?	No Overwrite?	Sequence
CLASSIFICATIONID	CLASSIFICATIONID	<input type="checkbox"/>	<input type="checkbox"/>	
COMMODITYGROUP	COMMODITYGROUP	<input type="checkbox"/>	<input type="checkbox"/>	
DESCRIPTION_CLASS	CASE_DESCRIPTION_CLASS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
HIERARCHYPATH	CASE_HIERARCHYPATH	<input type="checkbox"/>	<input type="checkbox"/>	
INDICATEDPRIORITY	INDICATEDPRIORITY	<input type="checkbox"/>	<input type="checkbox"/>	

Source Field:  
DESCRIPTION\_CLASS

Destination Field:  
CASE\_DESCRIPTION\_CLASS

Accept NULL value?  
☒

No Overwrite?  
☐

Condition on Source:  
 >>

Condition on Destination:  
 >>

Sequence:

OK Cancel

The file SynchDescriptionClass\_ICDtoNOI.zip contains the modifications to **\$OMNIHOME/gates/tsrm/tsrm.script** and an SQL file to add the field to the NOI schema.

## 8. CONCLUSION

Hopefully, this document assists you in setting up IBM Control Desk, enabling it through an integration with Netcool Operations Insight and Slack. This enables a Service Management toolchain for your applications quickly and efficiently.

## **9. GLOSSARY OF CONTROL DESK TERMS**

Component	Purpose
IBM Control Desk	<p>IBM Control Desk on Cloud is an integrated service management solution that helps businesses manage a comprehensive range of IT processes, services, and assets.</p> <p>With IBM Control Desk on Cloud, a business can optimize the performance of their infrastructure and workforce in alignment with overall business objectives. The product features innovative functions that are focused on the following business process areas:</p> <ul style="list-style-type: none"> <li>Service desk management, including a self-service center, catalogs for fulfillment, and incident and problem management applications</li> <li>IT asset and software license management</li> <li>Change and configuration management</li> </ul> <p>For the fFirst rResponders and sitSite rReliability eEngineers to log into Control Desk to perform their work functions.</p> <p>The solution will allow for the Site Reliability Engineer to review &amp; analyze for trending across incident types, frequency and severity.</p> <p>The First Responder will be enabled to search for other incidents in the UI to search for quick solutions and re-use solutions that may have been used in the past to resolve an issue.</p>
Start Center	<p>A Start Center is a configurable page that gives you quick access to the tools and key performance indicators (KPIs) that you use most often. Each of the security groups that are defined for change management has its own Start Center.</p> <p>When you log on to the product, the Start Center that is mapped to your primary security group is displayed. If you have multiple security group assignments, you can tab to secondary Start Centers.</p>
Escalations	<p>Escalations are used to automatically monitor the critical processes in your enterprise. You can also use escalations for events, such as contract expiration, a change in the status of a records, or a change in the ownership of a record.</p>
Incident	<p>An incident record is a type of ticket. Other ticket types are service requests and problems. The ticket applications are closely related and share many features, including the ability to define relationships between tickets, link them together for information purposes, and view the linkages and details in the appropriate applications.</p> <p>For the purposes of this document, especially in the NOI-ICD integration, the use of the word ticket and incident may be interchanged.</p>
Script with Launch Action	<p>Creating an automation script with an action launch point to facilitate the development of re-usable actions, that can be configured for use in different object contexts (for example, incidents, tickets). An action launch point associates a script with an action and executes when the specified action occurs.</p>
Problem	<p>A problem record is a type of ticket. Other ticket types are service requests and incidents. The Problems, Incidents, and Service Requests applications are closely related and share many features. You can define relationships between tickets, link them for information purposes, and view details for them in the appropriate applications.</p>

Component	Purpose
KPI	Creating key performance indicators to track critical performance variables over time. You can view key performance indicators (KPIs) in the start center or in the KPI Manager application.
Reports	There are several predefined reports provided with Control Desk. Use them to gather information about the incidents created for issues in your infrastructure, conduct trending and analyze data based on the incidents and volumes being created.
Security	<p>The Security Groups application, you can grant users access to specific applications to refine security measures. Users can have read, insert, save, and delete access to an application. The application access of a security group is linked to site access. You can give a security group access to all sites, access to specific sites, or no access to sites.</p> <p>Grant user's specific options within an application. For example, you can grant managers the right to read work order histories, costs, and warranties, but not to insert work orders or service requests. You must configure each application for read access so that administrative users can select additional application access options.</p>
Work log	
Netcool Operations Insight (NOI)	<p>An event management and correlation engine which acts as a force-multiplier in the middle of the tool chain, correlating disparate events across applications, services, and infrastructure, and making sure that the most important and business-affecting events are forwarded by suppressing symptomatic events in favor of root-cause events.</p> <p>For the purposes of this document, NOI and Omnibus (the central component of NOI) are interchangeable terms.</p>
TSRM Gateway aka ICD Gateway	The NOI component which performs the bi-directional integration between NOI and ICD. Note that TSRM and ICD are synonyms and the gateway's name is TSRM for historical reasons only.
Object Server	NOI's central repository of monitoring events. This is an in-memory database that must be extended with new fields as part of the integration.
Trigger	An automation within an Object Server that can perform tasks either on a schedule or because of a change in an event.
Journal entry	A feature of NOI, allowing operators to information about a given incident. Equivalent to ICD's work logs.
Slack	Communications and collaboration platform, improves the capabilities of users to work together to solve issues faster. Also, functions as a ChatOps platform, enabling remote commands and remediation tasks as part of the chat conversation