Lab Exercise:
z/OSMF Incident Log Hands-On Lab

Abstract:

The z/OS Management Facility (z/OSMF) provides a web-based graphical interface for system programmers on z/OS. This hand on lab will give an opportunity to learn about the functions and features in z/OSMF first hand. Attendees can navigate through the z/OSMF Incident Log task to see how it can help them manage incidents that occurred on their system, or assist in sending diagnostic data to a vendor (IBM or ISV).

This session will be useful to systems programmers and their managers who will be using (or are considering using) the z/OS Management Facility.

Introduction to z/OSMF Incident Log:

When a problem occurs on a z/OS system, you might need to determine what happened and why, and then find the fix or report the problem to IBM or an independent software vendor (ISV). Typically, you need to get to the root of the problem quickly, but the task of gathering diagnostic data and sending it to a support team can be very time-consuming. To assist you with diagnosing and reporting the problem, z/OSMF offers a problem data management solution, the Incident Log task.

The Incident Log task streamlines and automates time-consuming and manual parts of the problem data management process. Specifically, the Incident Log task gathers and displays system-detected and user-initiated incidents, collects associated logs and dumps at the time of the problem, and facilitates sending that data to IBM or another vendor for further diagnostics. Using the Incident Log task reduces the possibility of errors while obtaining, aggregating and sending the collection of diagnostic data to IBM or an ISV.

Key features of the z/OSMF Incident Log Task

With the Incident Log task, you can:

- **Manage the incidents that occurred on a system or in a sysplex.** The Incident Log task provides a consolidated view of all incidents occurring on all participating systems in the sysplex (those that communicate through the same sysplex dump directory).
- **Browse the logs collected for an incident.** When an incident occurs, the Incident Log task collects and saves the associated SVC dumps and diagnostic log snapshots. You can browse the error log, error log summary, and operations log.
- **Allow the next dump of an incident with the same MVS symptom string.** The Incident Log task provides the ability to update the DAE data set, so that you can capture the next instance of an SVC dump being suppressed by DAE.
- **Send diagnostic data and attachments to IBM or another vendor for further diagnostics.** The Incident Log task provides a wizard that you can use to send diagnostic data and additional attachments to IBM or another vendor. You can send files using standard FTP or using the z/OS Problem Documentation Upload Utility (PDUU), which supports parallel FTP, HTTPS and encryption. For more information about PDUU, see z/OS MVS Diagnosis: Tools and Service Aids.
- **Associate the incident with problems recorded in other problem management systems.** The Incident Log task allows you to correlate an incident with an IBM problem number, an ISV problem number, or with a problem record in your installation's problem management system.
- **Track additional information with an incident.** The Incident Log task allows you to specify additional information that you want to track about an incident, such as who is assigned to resolve the issue, which business applications are impacted,

which component is the source of the issue, and which solution has been implemented.

- **Monitor the status of an FTP job.** An FTP job is created when you send diagnostic data to IBM or another vendor. The Incident Log task allows you to browse or cancel FTP jobs and view or delete the status of FTP jobs.

Incident log Lab

This lab consists of 8 tasks, plus 2 additional optional tasks.

1. Log on to z/OSMF
2. View all the incidents across all the systems in your sysplex
3. Customize your view of these incidents
4. View the details of a user incident
5. FTP the diagnostic data captured for an incident to your service provider
6. View the status of the FTP for that incident
7. Manually create an incident
8. APAR search – Quick search or build your own search

Optional tasks if you have time and interest

9. View FTP destinations
10. View firewall proxy

It is recommended that you execute these tasks in the order listed above. As you get familiar with the Incident Log, you will be able to work directly with the task you need to accomplish.

As with all the labs in this session, all the teams will be working with the same z/OSMF instance. Each team will be given a unique id to work with. However, you must remember that as you work with a given incident, that incident is also available to the other teams to work with. When you are working with updating an incident please make sure you work with the user defined incident assigned to your team to avoid confusing the other teams.

Lab Hints and Tips

- At any time you can use the Help facilities by clicking on the link in the upper right hand corner of the screen
- You are encouraged to follow the instructions provided, but you can use the new views and reports on any defined software instance
  - Please note that the closer you follow the instructions, the easier it will be to assist you if you go astray
  - The handout contains screen captures and guidance to lead you through the lab
- **Do NOT use the Browser BACK button to go to the prior screen!!!**
  - Use z/OSMF “breadcrumbs” instead
- Also note that if you change the browser display size (Ctrl/+, or Ctrl/-) then what you see may not exactly match the handout.

 2

Exercise instructions

Here are the steps you will perform in this lab:

__ **1.** Logon to z/OSMF

- __ **a.** Launch the Mozilla Firefox browser
- __ **b.** Point Browser to z/OSMF – enter the following URL **https://share.centers.ihost.com/zosmf/**
- __ **c.** Enter the User ID (SHARCnn) and password assigned to your workstation.

__ **2.** View all the incidents across all the systems in your sysplex

- __ **a.** Double click Incident Log on Desktop

__ **3.** Customize your view of these incidents

- __ **a.** Filter columns
- __ **b.** Sort columns
- __ **c.** Configure the columns
- __ **d.** Rearrange the order of the columns as you would like to see them

__ **4.** View the details of a user initiated incident

- __ **a.** Select a user initiated incident with the same suffix as your User ID.
- __ **b.** View Diagnostic Details of the incident
- __ **c.** Update the incident with tracking information and notes
- __ **d.** Browse diagnostic data

__ **5.** FTP the diagnostic data captured for an incident to your service provider

- __ **a.** Select a user initiated incident with the same suffix as your User ID.
- __ **b.** Send Diagnostic Data for the incident
- __ **c.** Select the FTP Server (destination)
- __ **d.** Specify Security Settings
- __ **e.** Select FTP Profile
- __ **f.** Define Job Settings
- __ **g.** Review FTP Information
- __ **h.** Submit FTP Jobs

__ **6.** View the status of the FTP for that incident

- __ **a.** Select FTP Job Status for the incident that you just sent

__ **7.** Manually create an incident

__ **a.** Create incident

__ **8.** Search APAR

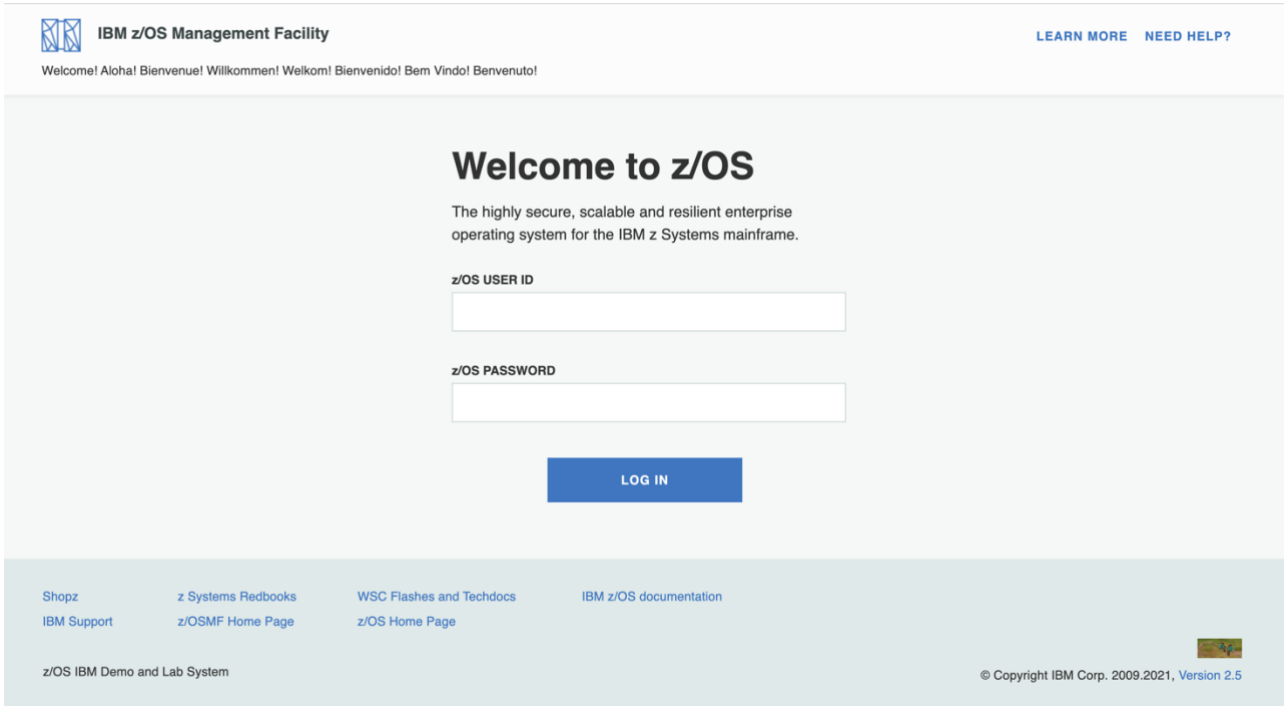
__ **a.** APAR Quick Search

__ **b.** Build your own search

1. Logon to zOSMF

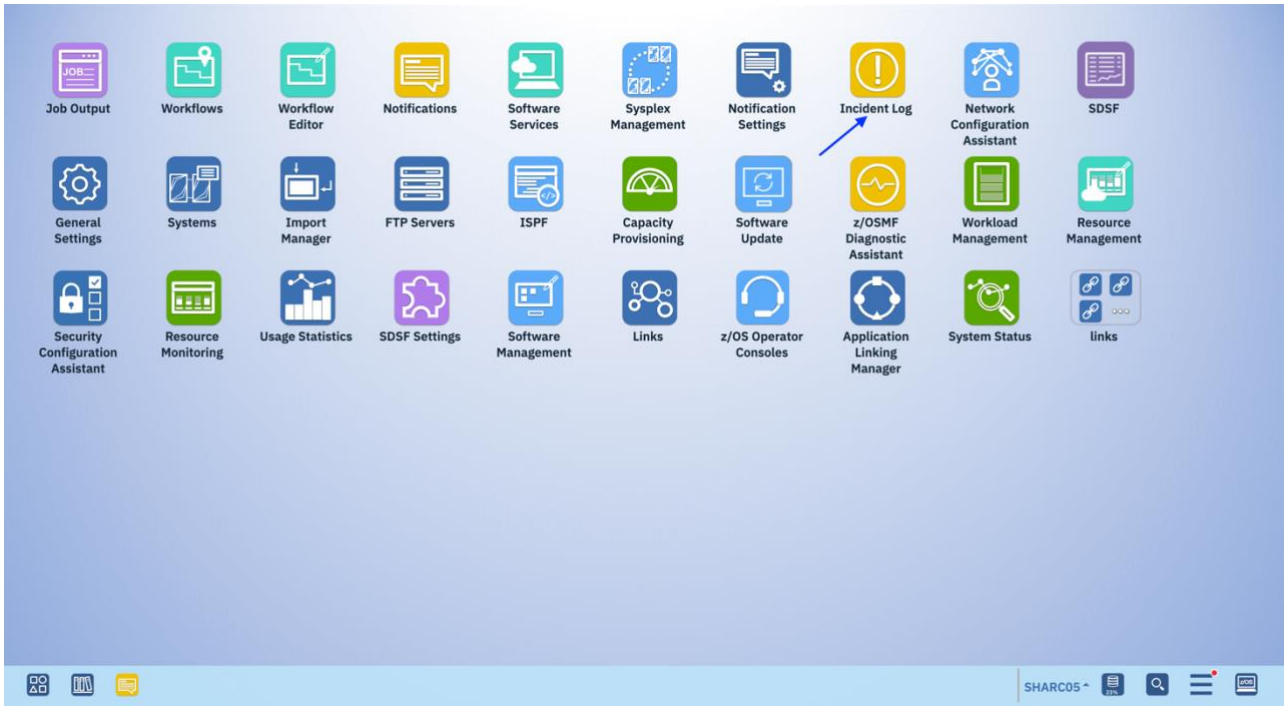
- Launch browser from your workstation
- Point browser to z/OSMF – enter the following URL
  https://share.centers.ihost.com/zosmf/
- Login with SHARE userid/pw as provided by the lab instructor
  - Each workstation has been assigned a unique z/OS user id

Note: All screen captures in the handout show the ID SHARC05, your browser will be slightly different to reflect the User ID that you were given.



2. View all incidents across the systems in your sysplex

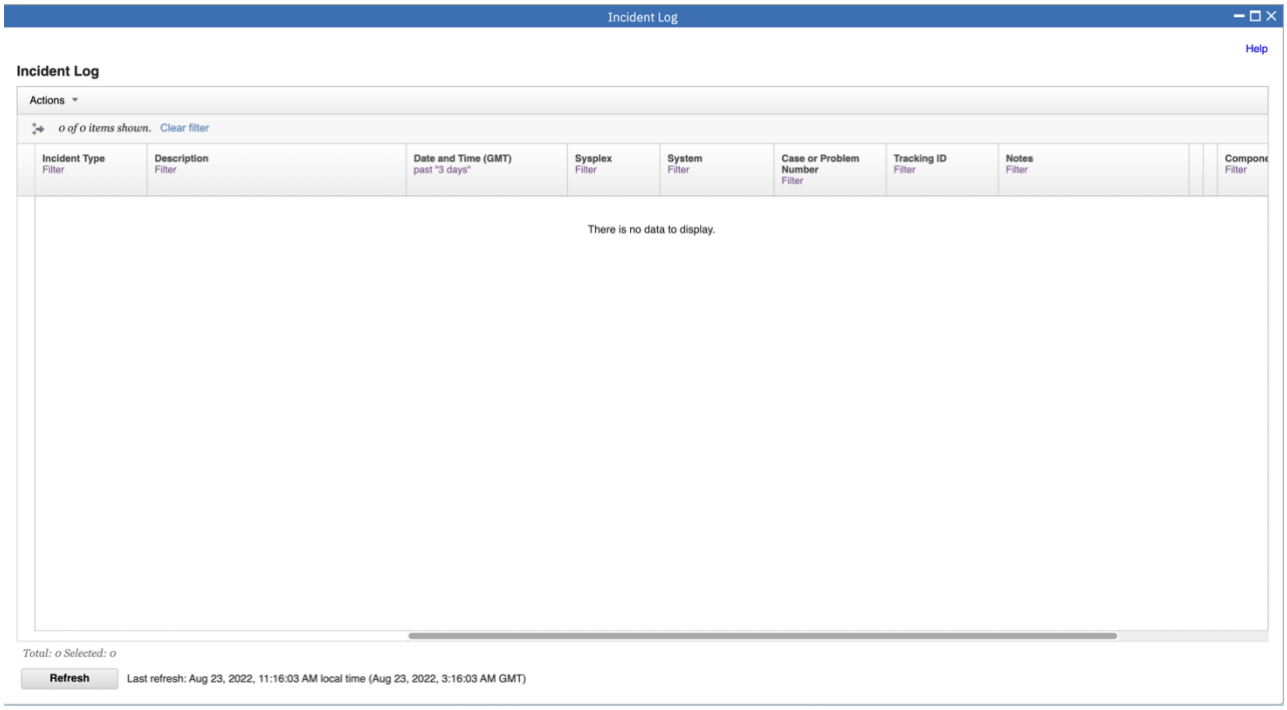
Step 2a: Double click Incident Log on Desktop



The first panel that opens is the main panel of the Incident Log. Here you will see a summary view of all the Incidents across all the systems in the sysplex. Take some time to scroll through and look at all the columns.

Note: You will not see any incidents yet, because the default is to only show incidents that occurred in the last 3 days. In the next task you will be able to see incidents!

The list of incidents that meet your filter criteria are displayed. Unfortunately, no incidents meet the current criteria.



3. Customize Your View of These Incidents

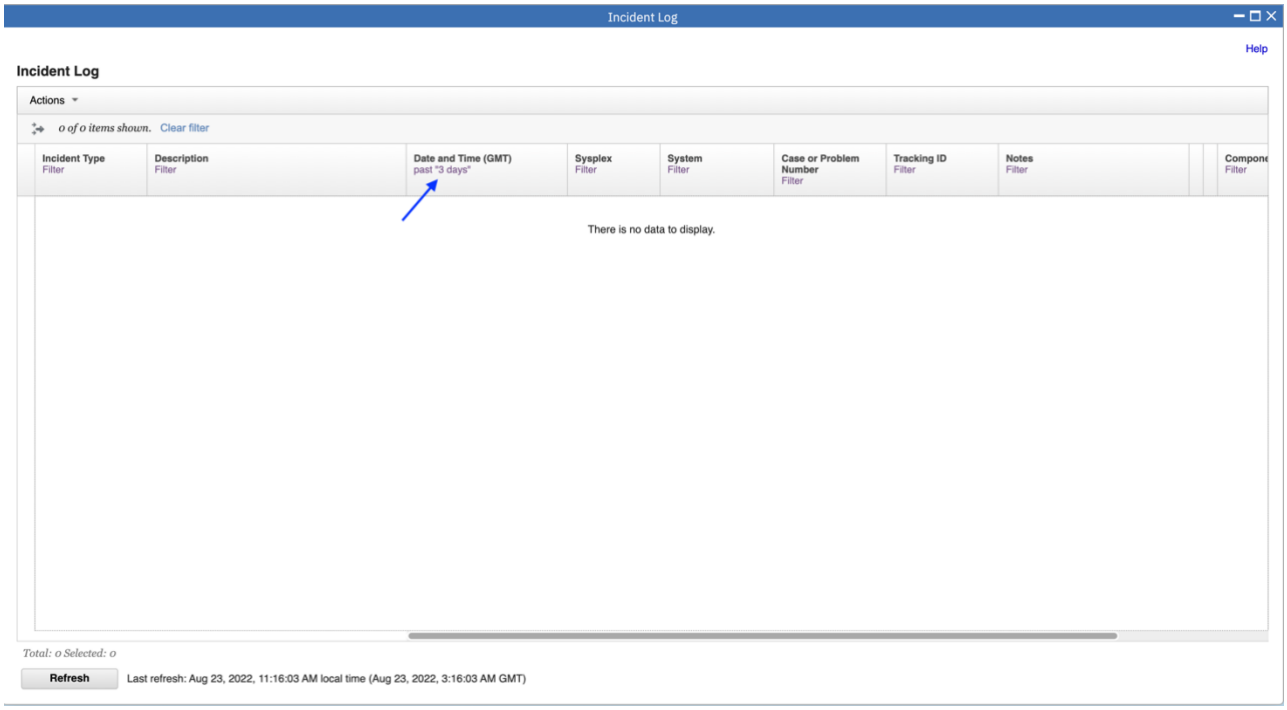
You have the ability to control what data you see in terms of configuring what columns are displayed and the order of those columns. You can also control the data you see, which is you can filter on different columns. You can also sort the columns to view the data in different sort orders. You can sort on up to 3 columns at a time!

Remember that all customizations are saved on a per user basis.

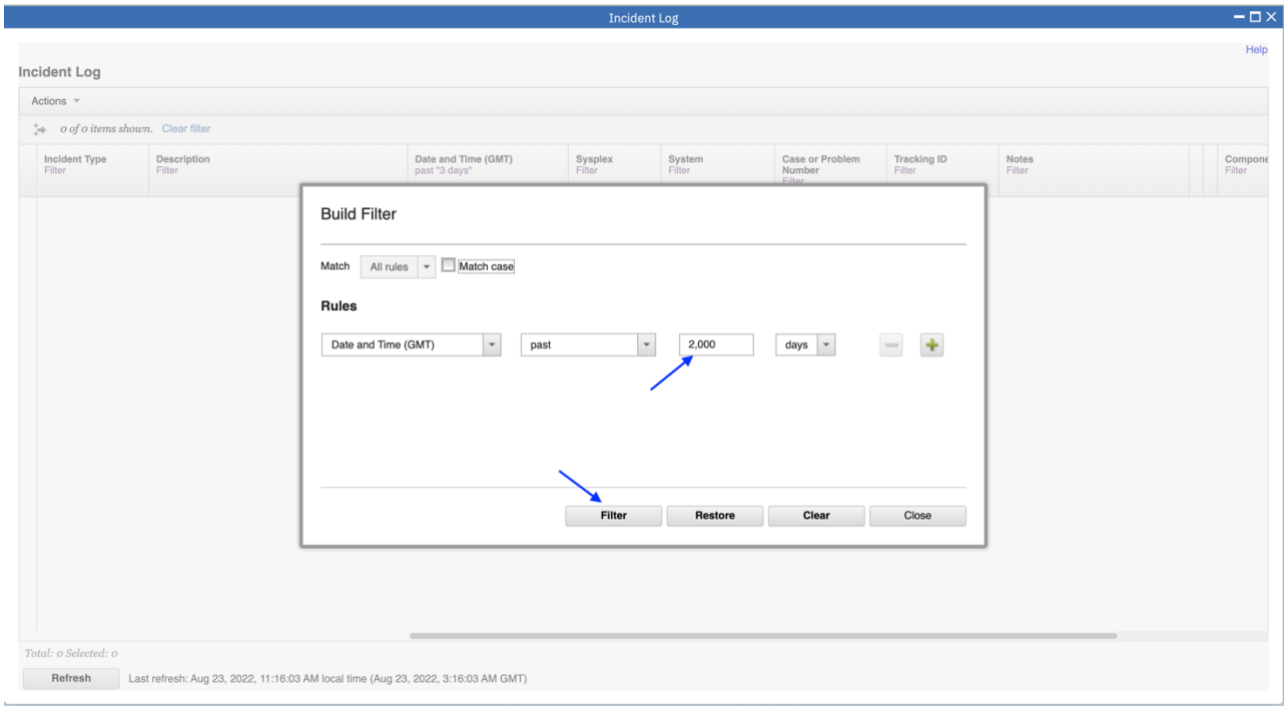
Step 3a: Change the Date Filter

By default, you will get all the incidents that have occurred in the last 3 days. You can change this.

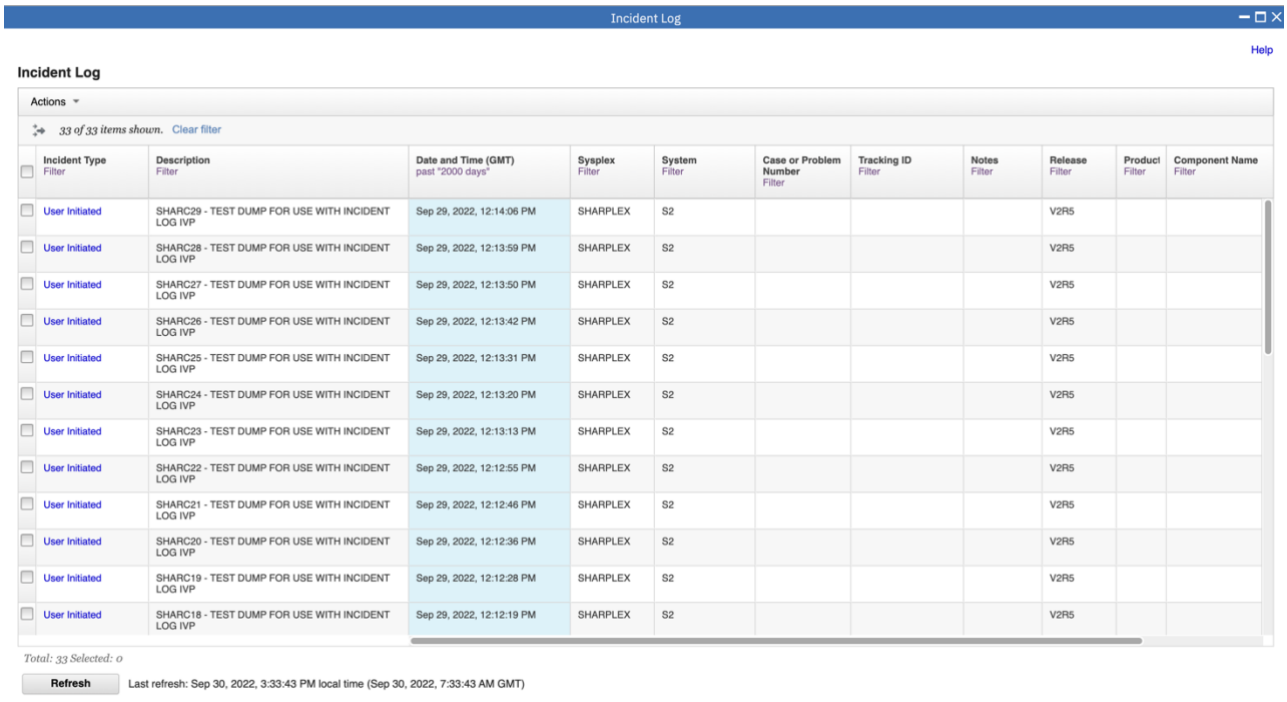
1.Click on the filter displayed under a column header to change the filter. For this example, let us say we want to look at incidents from the last **2000 days**.



2.Change Amount to 2000, then click Filter.



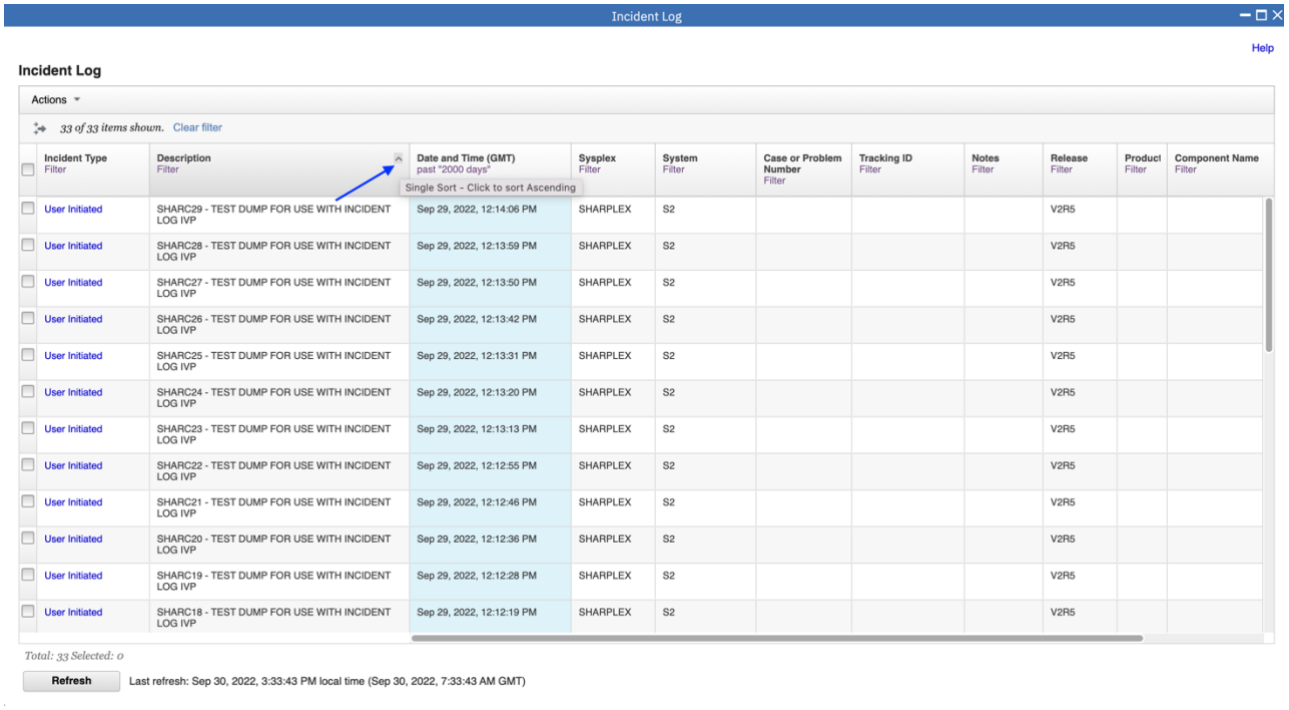
Now the list of incidents displayed on a table.



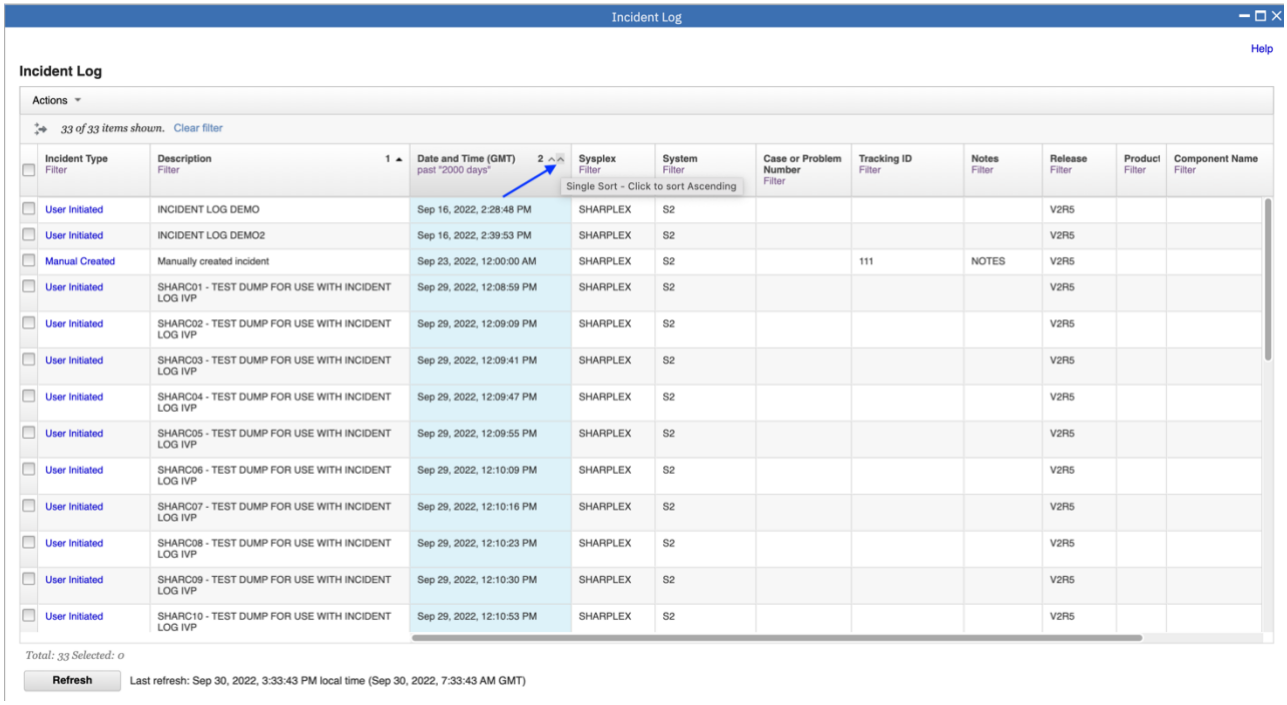
Step 3b: Sort the Columns

You can sort the columns in the table display by clicking on the column header of the column you want to sort on. The first time you click on it, it will sort it in ascending order, the second time in descending order and the third time it will clear the sort. In this exercise you will create an ascending sort based on Description and a descending sort based on the Date and Time column. Notice the arrows that show up for ascending and down for descending. Also, notice that the sort order numbers that show up on the column headers.

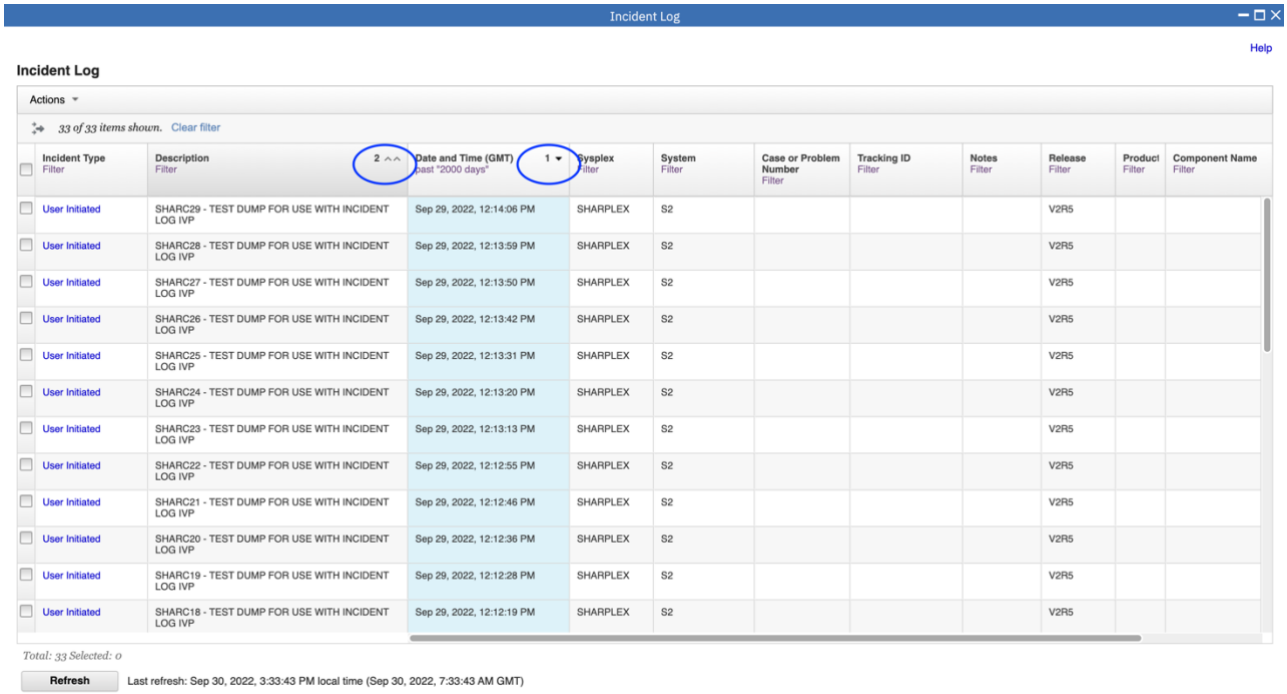
1.Click once on the Description column to put the incidents in ascending order.



2.Click twice on the Date and Time(GMT) column to arrange that column in descending order.



Now the columns have a primary sort criteria (1) based on Date and Time (descending) and a secondary sort (2) on Description (ascending). Note: If you click Date and Time a third time that column's sort will be removed.

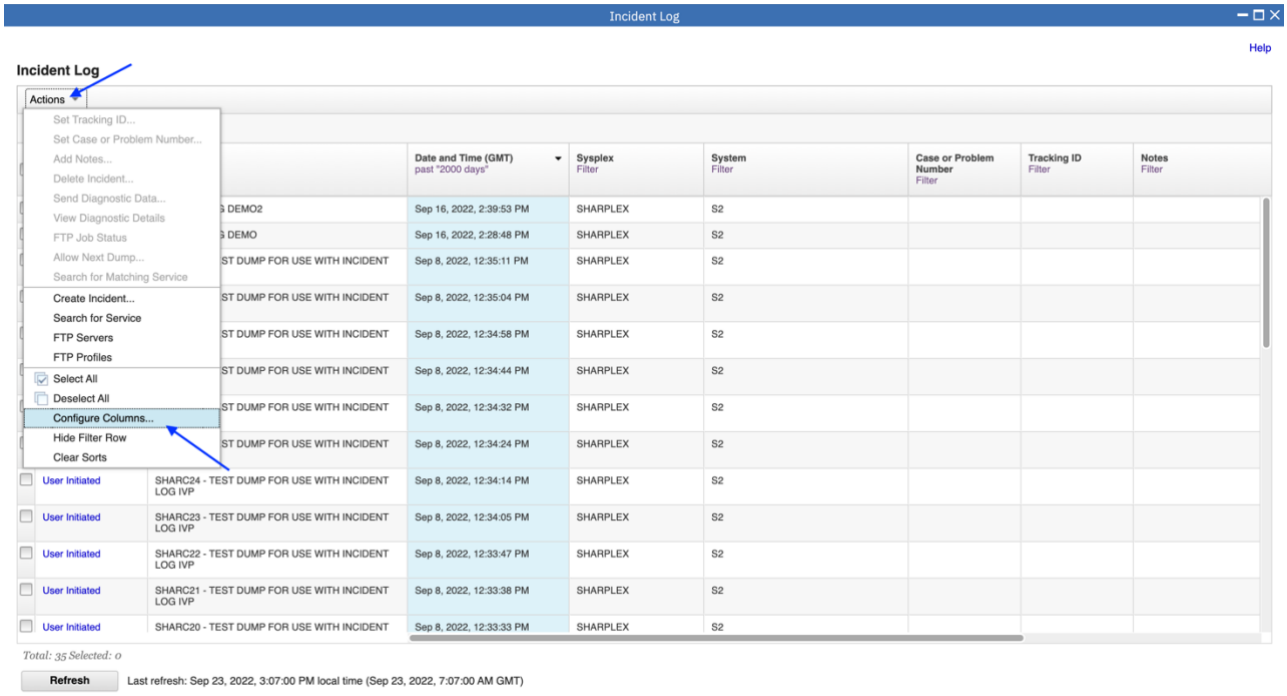


Step 3c: Configure the columns as you would like to see them

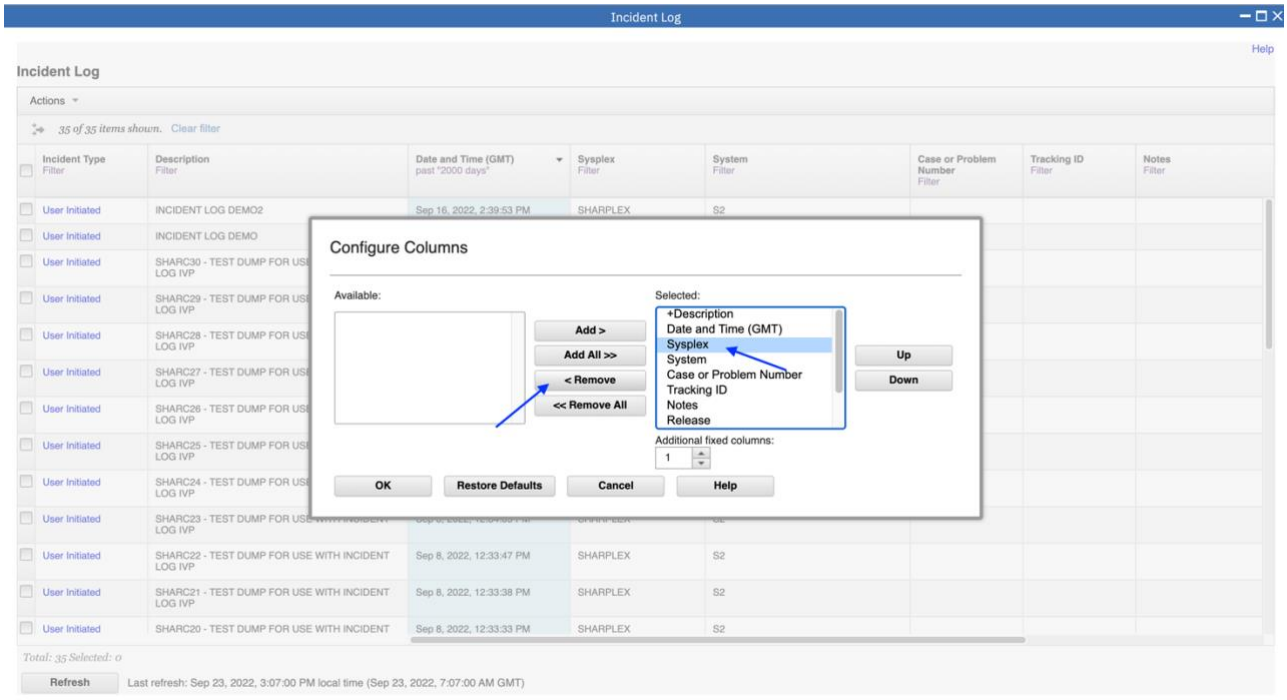
You can configure which columns are displayed and the order in which they are presented. In this exercise, you will remove the Sysplex and System columns. The lab environment is a monoplex, so all incidents were taken on the same system in the same sysplex (not very interesting and therefore for this lab you can remove them). You will also rearrange the columns to move the 'Component Name' column next to the Date and Time column.

Now you will see how z/OSMF lets you reconfigure the columns that are displayed. First we will configure which columns are displayed.

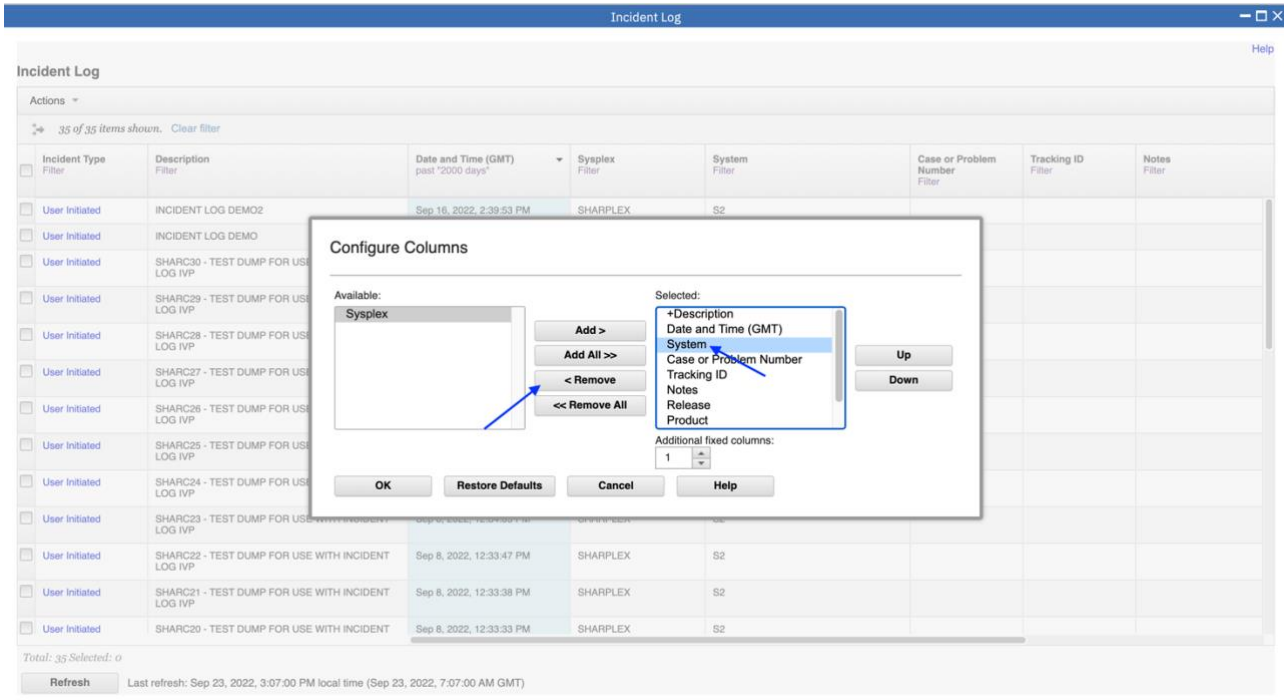
1.Click Actions, then Configure Columns.



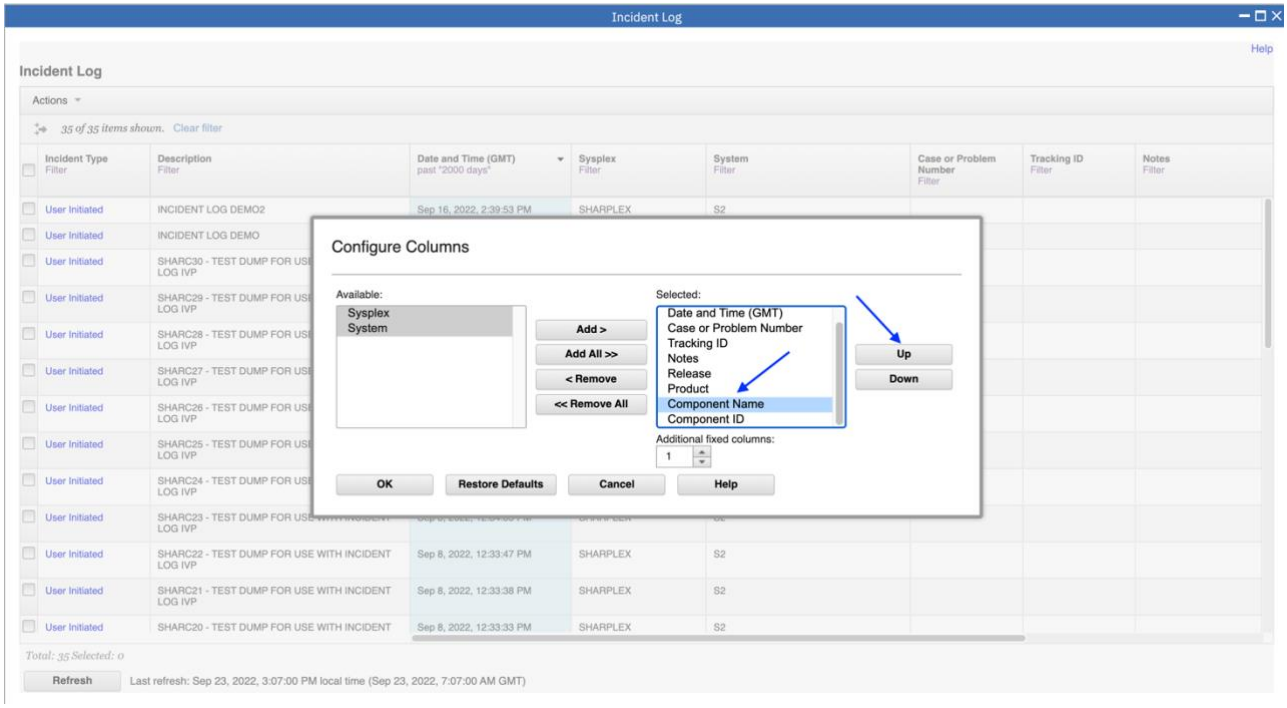
2.Click “Sysplex”, then “< Remove”.



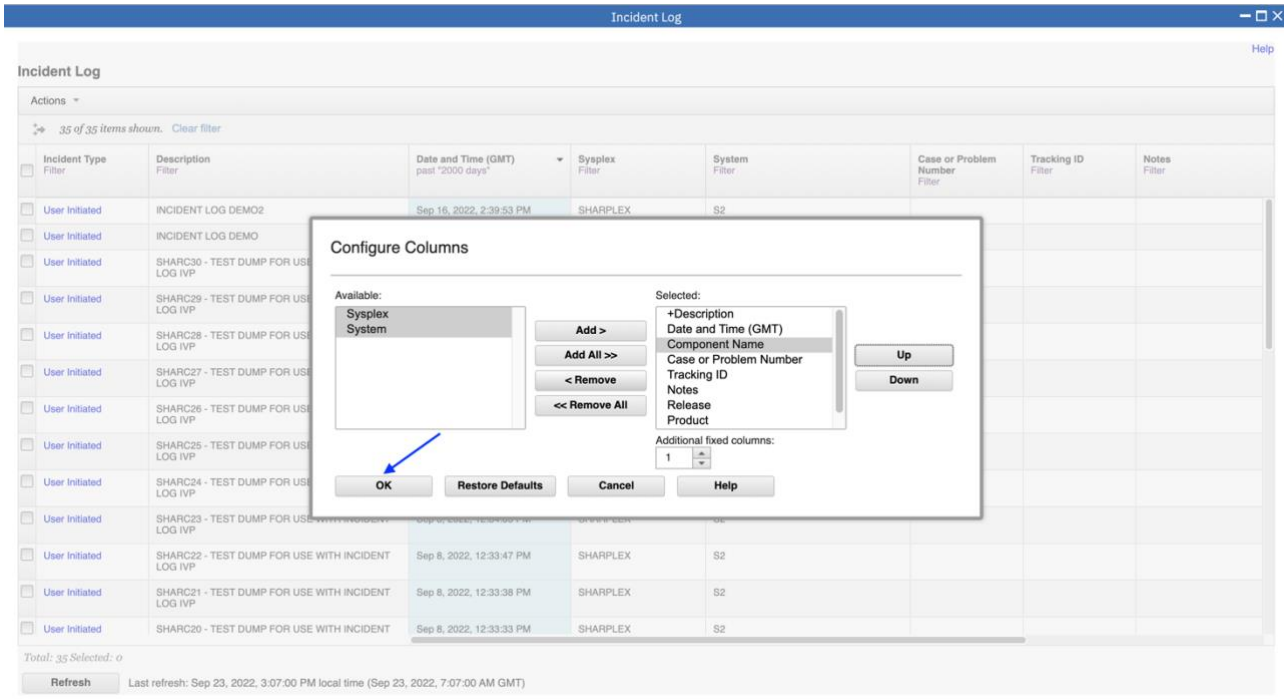
3.Click “System”, then “< Remove”.



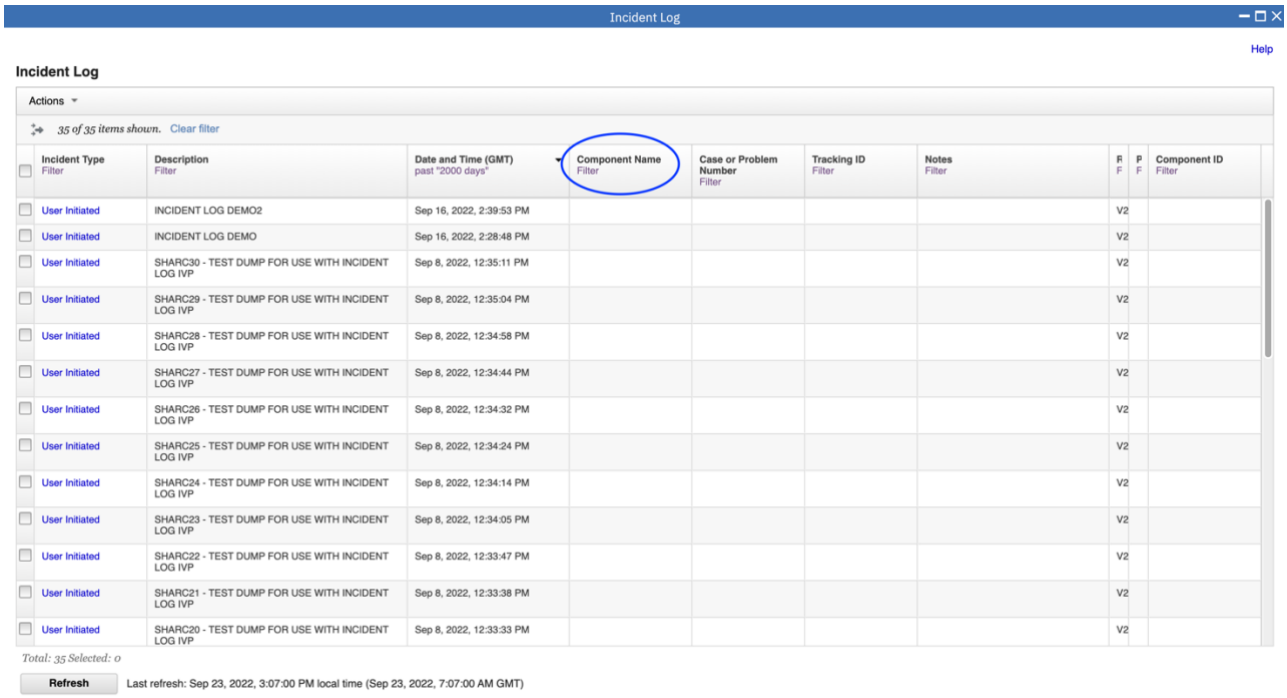
Now you configure the order in which columns are displayed. Click “Component Name” then use the “Up” button to position it after Date and Time.



4.Then click OK.



Now you can see that the Sysplex and System columns are no longer displayed and the component name column appears after Incident Type, Description and Date and Time.



You have successfully customized your workspace! You are only viewing the columns you want, in the order you want, for a range of data that you filtered, in the sort order that you want.

4. View the details of a user initiated incident

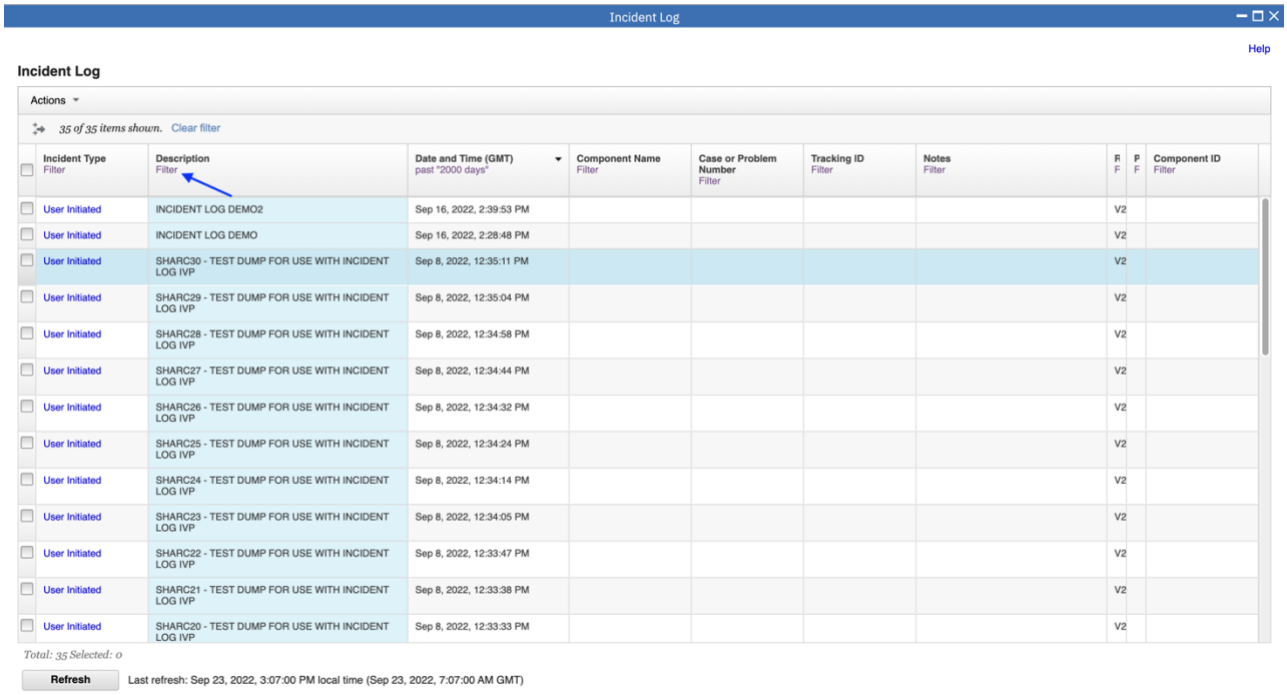
Now that you've customized your workspace, let us dive deeper into an individual Incident.

Step 4a: Select a User Initiated Incident with the Same Suffix as Your User ID

You will need to filter the Description column to display only incidents that have the same suffix as your User ID (for example, "SHARAC05 – TEST DUMP FOR USE WITH INCIDENT LOG IVP" if your User ID is SHARC05).

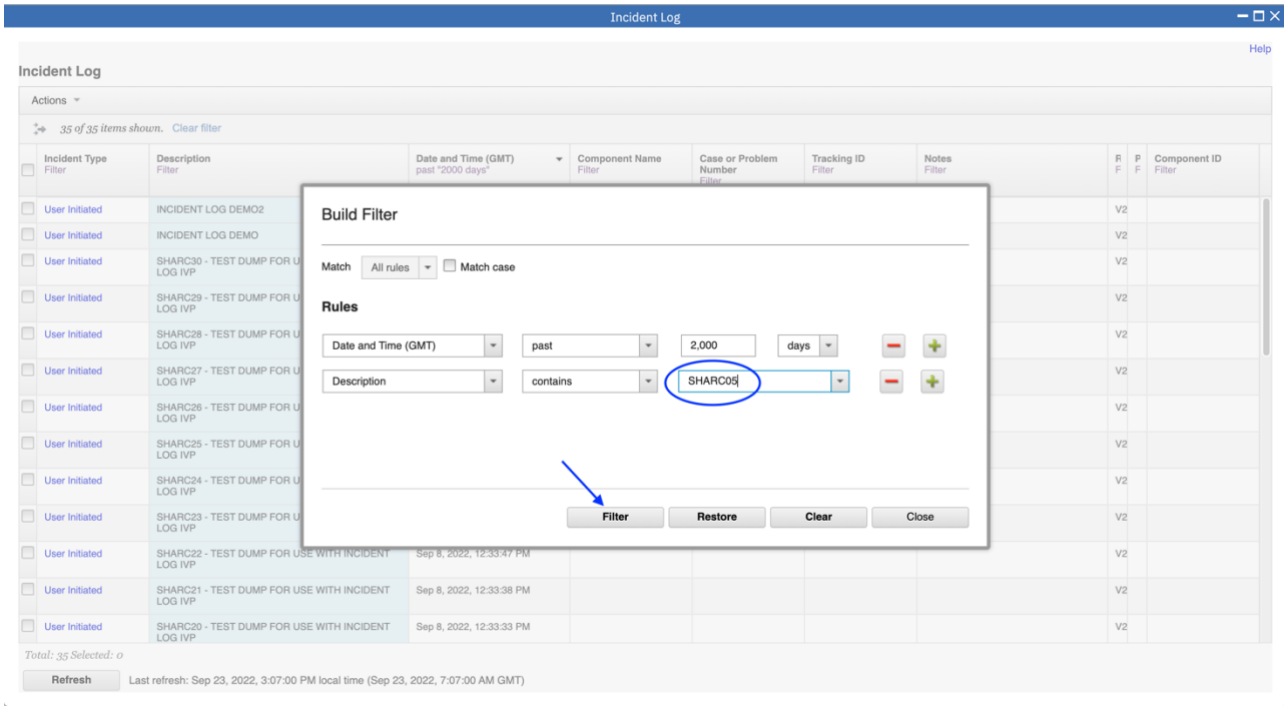
Now you will view details of a user initiated incident. Unique incidents have been created for each user ID. You will use the filter to view incidents with the same suffix as your user ID.

1.Click on Filter under Description.



2.Change to an incident that has the same suffix as your User ID(e.g., SHARC05 for SHARC05).

Then click Filter.



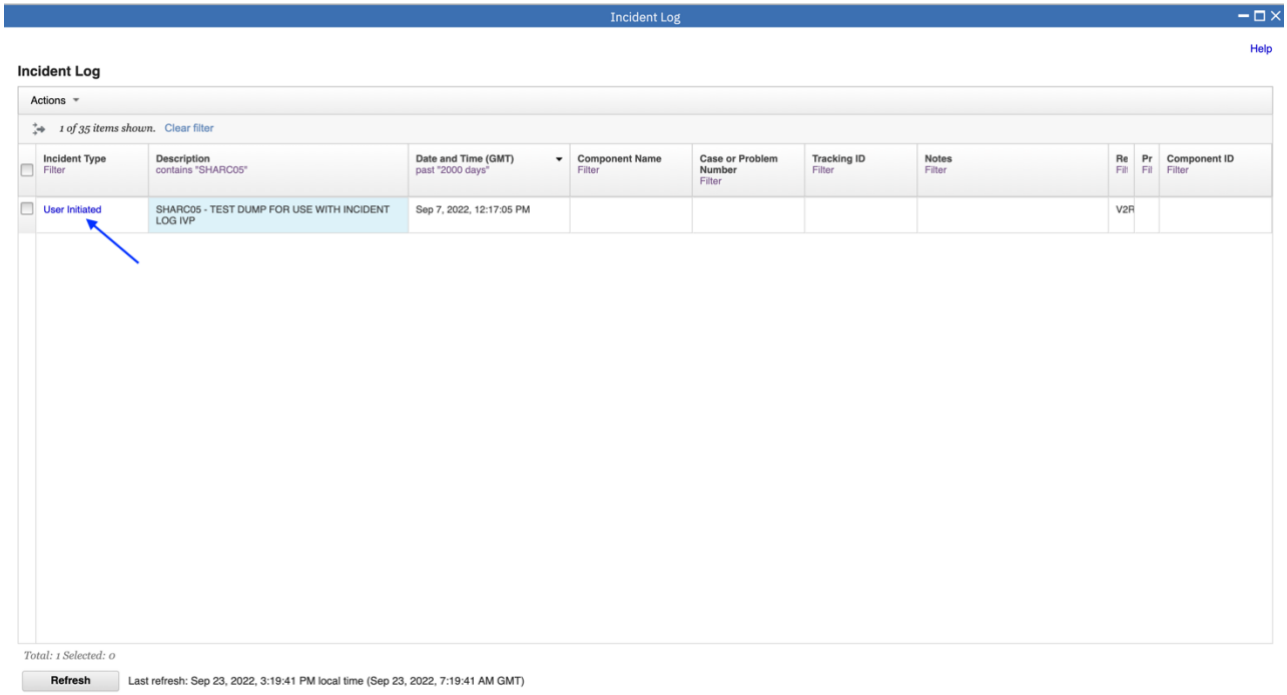
Step 4b: View Diagnostic Details of a User Initiated Incident

The incident with the same suffix as your user ID is now displayed. To view the details you can either:

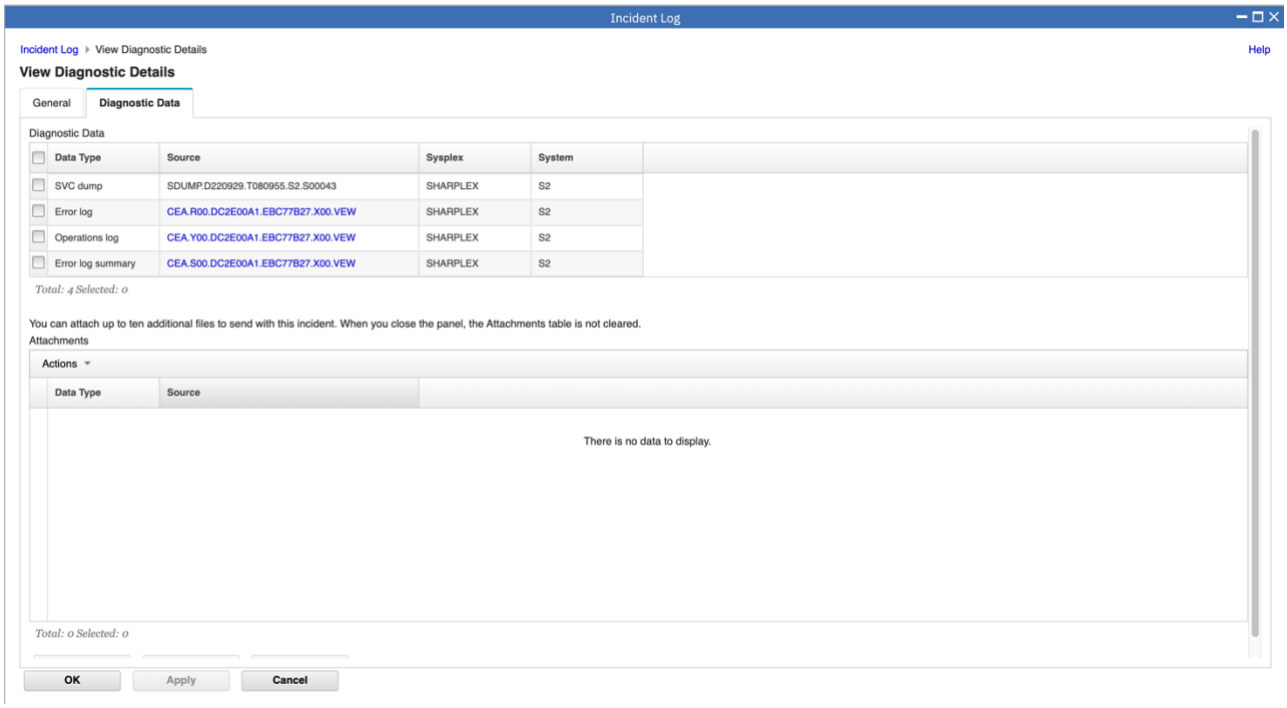
- Click on “User Initiated” in the Incident Type column;
- Click on the selection box, then select Actions, followed by View Diagnostic Details; or
- Right click on “User Initiated” in the Incident Type column to view a context sensitive list of Actions, then select View Diagnostic Details.

For this exercise, it is recommended that you use the first option.

1.Click on “User Initiated”.



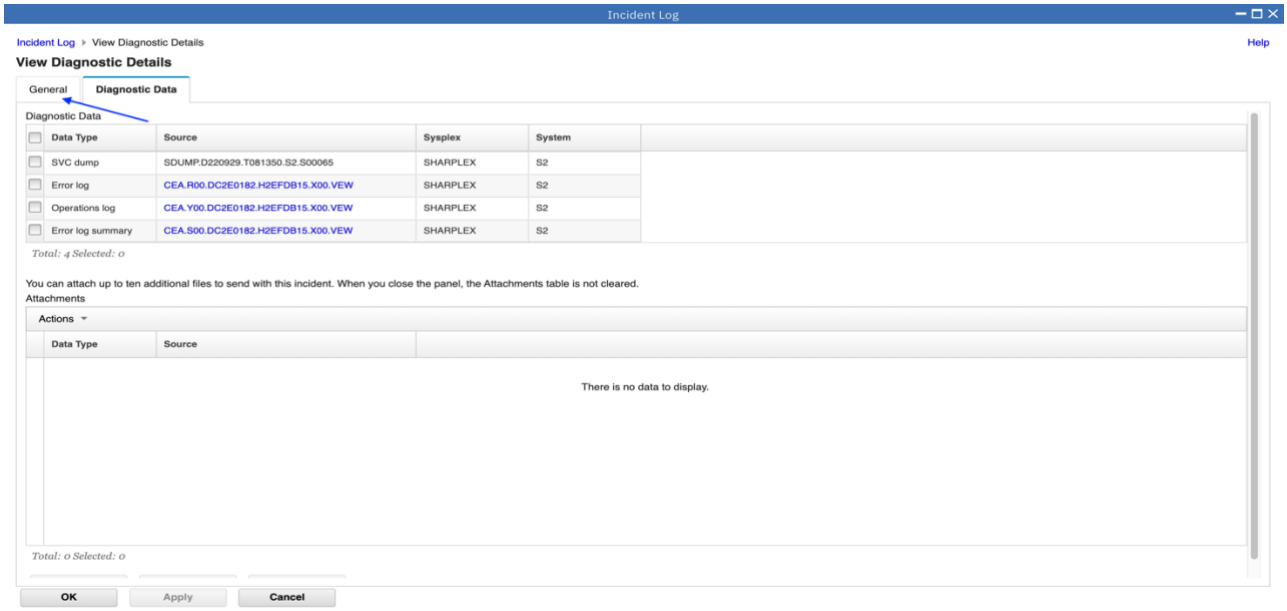
You now see a 2 tabbed display(General and Diagnostic Details). In the Diagnostic Details tab, you see the data that was captured for this incident. If you associated any other diagnostic data with this incident it would also be displayed.



On this panel you can see all the pieces of diagnostic data that have automatically captured for this Incident by the backend instrumentation. Take some time to look at this. Observe that you also have the ability to attach additional pieces of diagnostic data (for example a trace file)

2.Once you've finished with this tab, let's move on to the other tab – General.

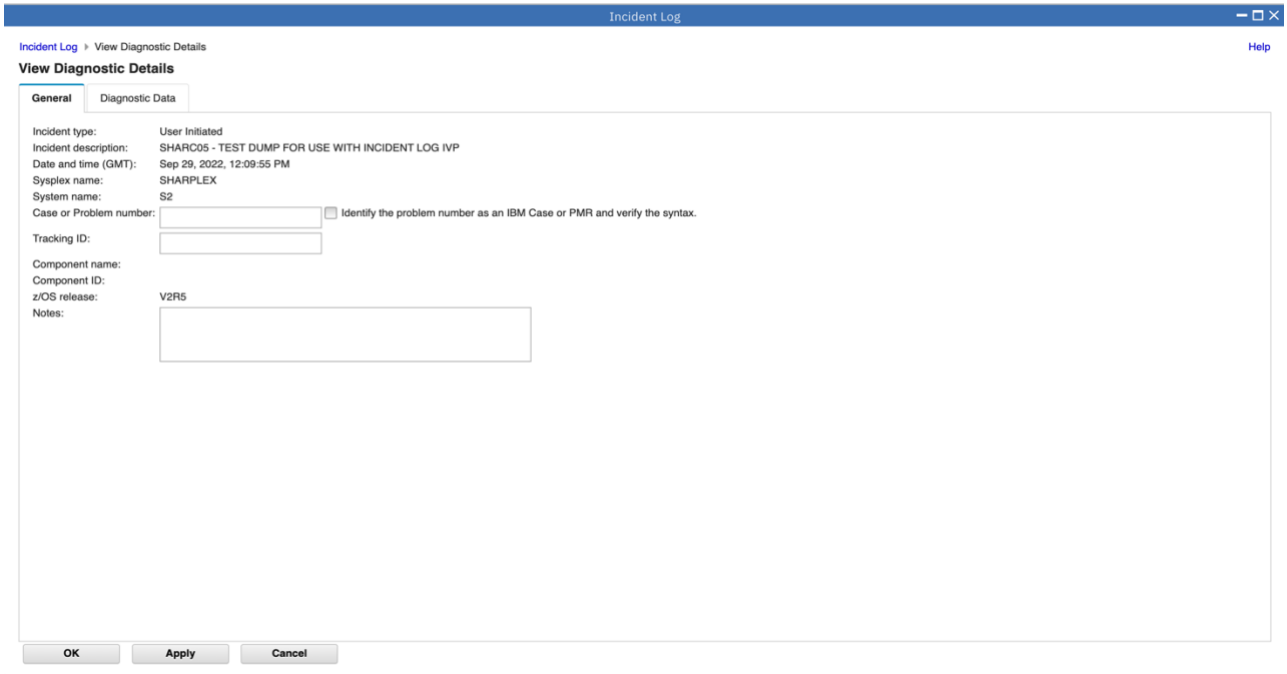
Click on the General Tab.



Step 4c: Update the Incident

Using the General tab, you can optionally enter a vendor problem number, an installation problem tracking number, and notes. For this exercise, you can enter "TS123456789" as the problem number, "TRKabc" as the Tracking ID, and optionally enter any text for Notes.

In the General tab you see the information about the incident that was displayed in the table of incidents.

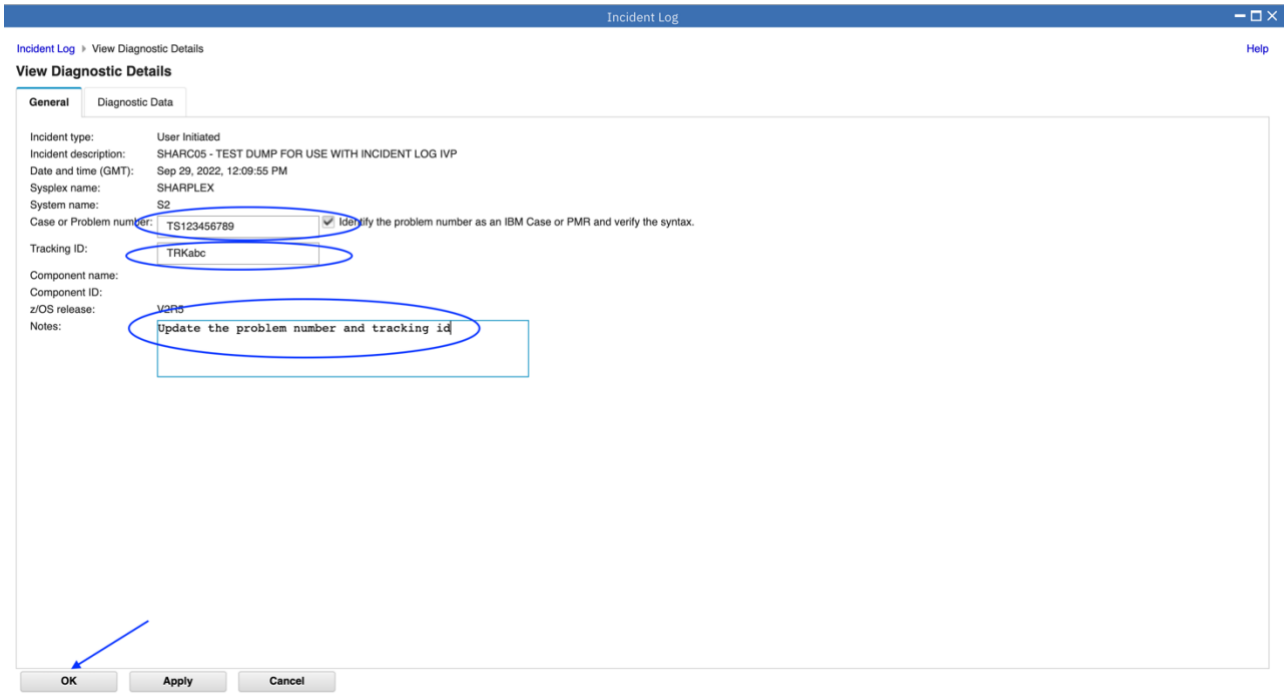


1. Enter “TS123456789” for problem number

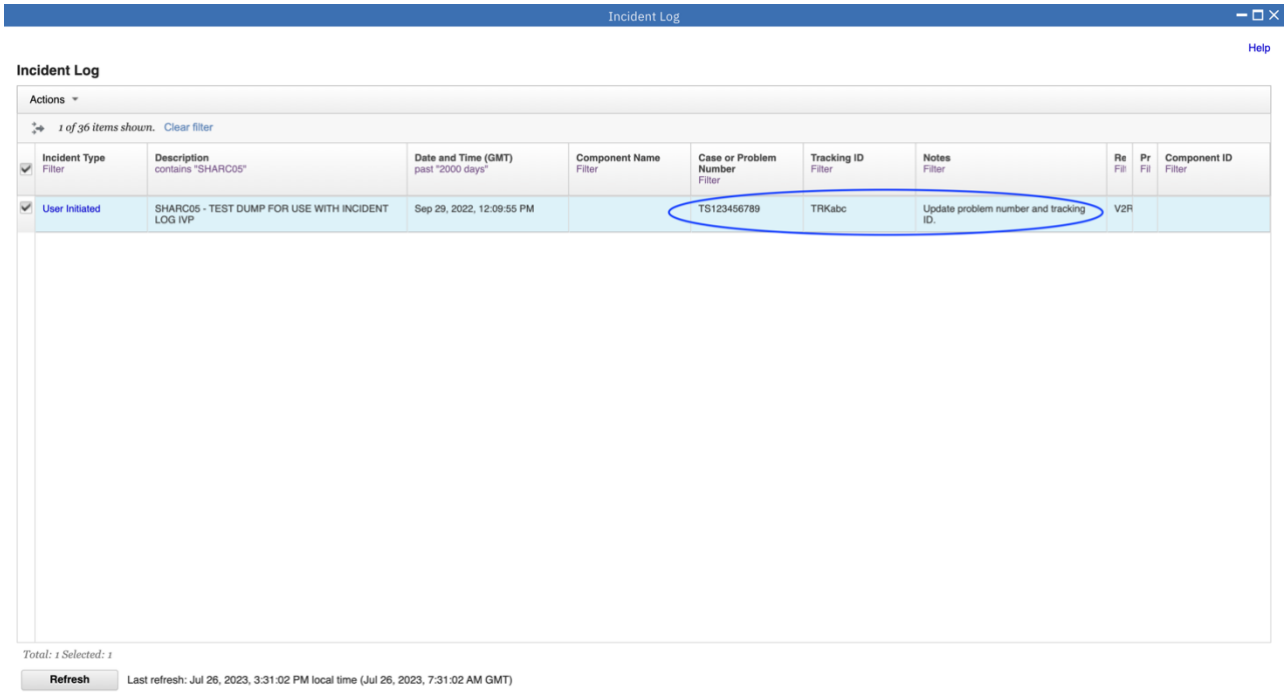
2. Optionally check to identify the number as an IBM Case

3.Then enter “TRKabc” for the Tracking ID, optionally, enter any text for notes, such as “Update the problem number and tracking id”

4.When you are done, click OK.



Once you have entered the problem number and tracking ID and clicked OK, you can now see those values in the table of incidents. You now see the additional information in the table display.



Step 4d: Browse Diagnostic Data

Since z/OSMF V1.13, you can browse the logs captured for an Incident. To browse the logs you can either:

- Using z/OSMF ISPF Browse;
- Using z/OSMF Desktop Editor

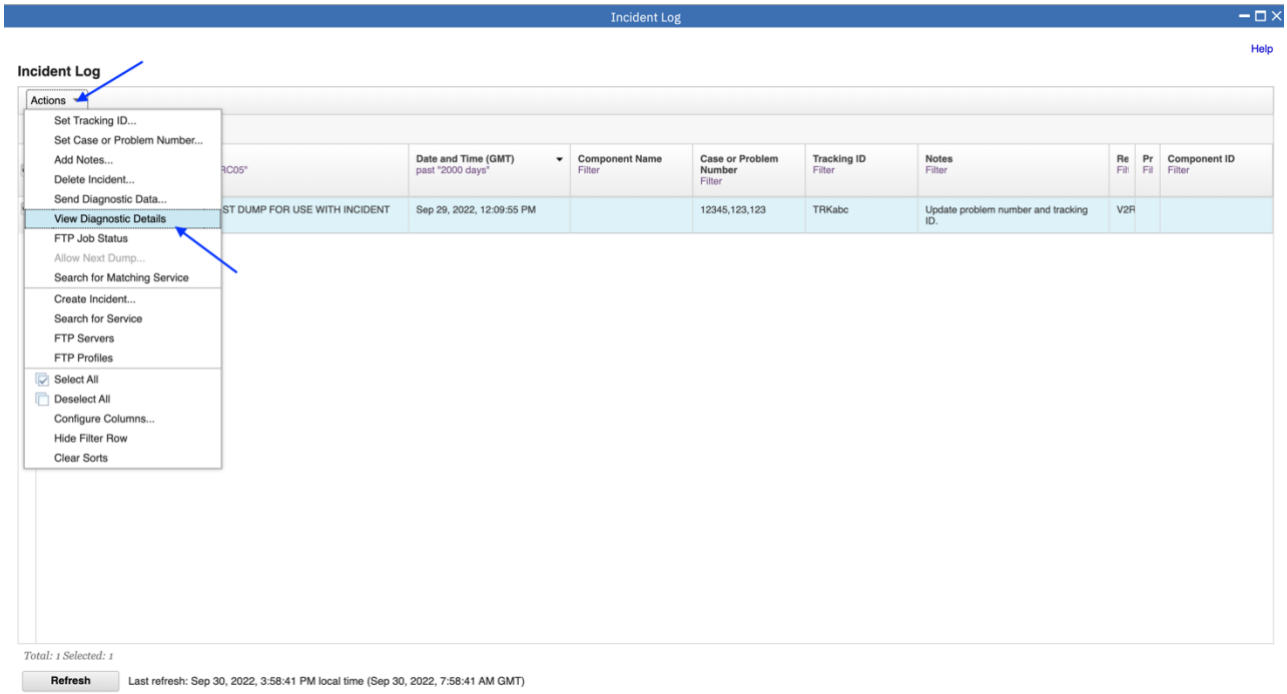
For this exercise, it is recommended that you use z/OSMF Desktop Editor.

To select browse snapshots of diagnostic data, you must first view diagnostic details again. This time, since the incident with your suffix is already selected, you should try clicking Actions then View Diagnostic Data to bring up the diagnostic data.

You will see the diagnostic data elements captured for that Incident. Note the Source name of the data element. It is a hyperlink.

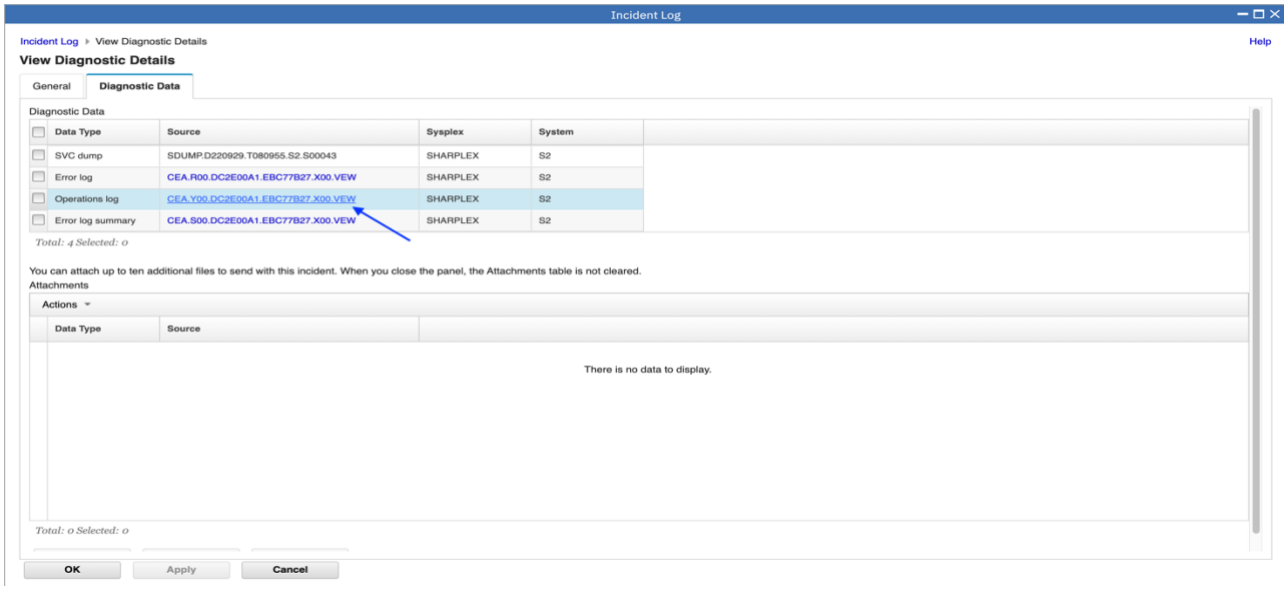
In this exercise, you will browse the Operation Log snapshot.

1.To browse diagnostic data, you must first view the details of your incident again. This time you will select Actions, then View Diagnostic Details.

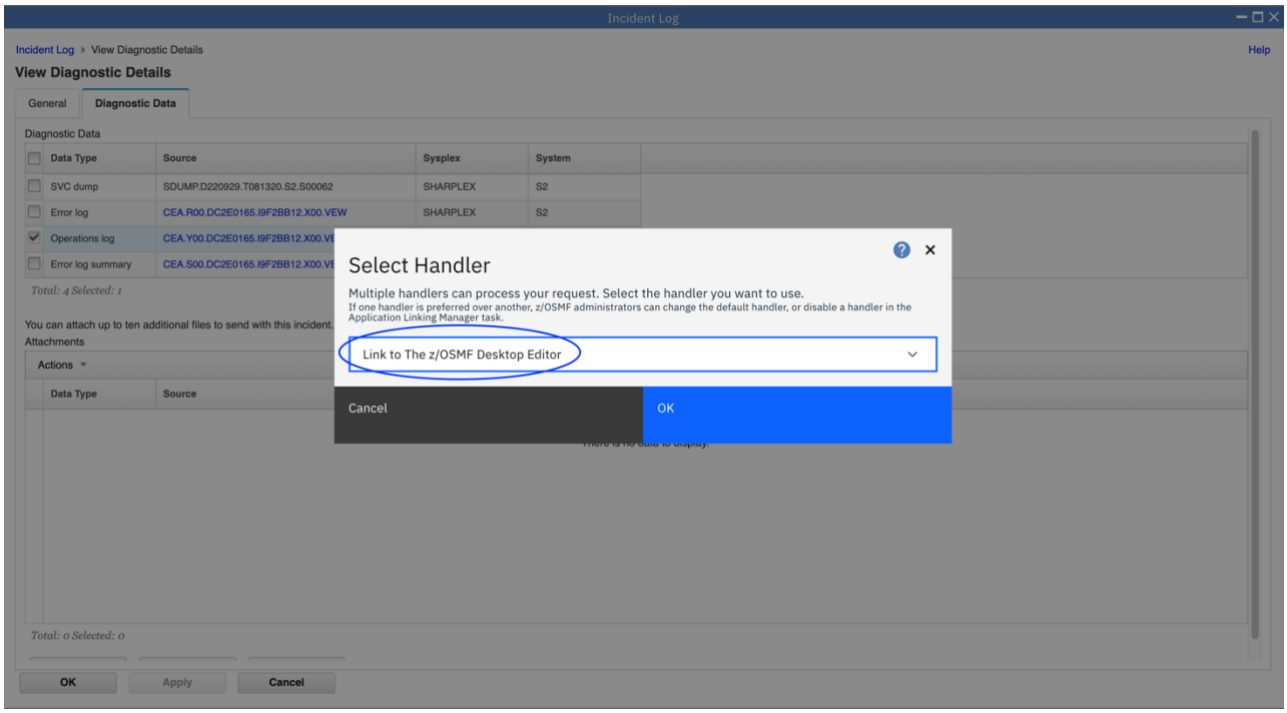


Clicking on the Source name will enable you to browse that data element. For example, clicking on the Operations Log Source will cause z/OSMF to application link to z/OSMF Desktop Editor to enable you to browse the snapshot of SYSLOG data.

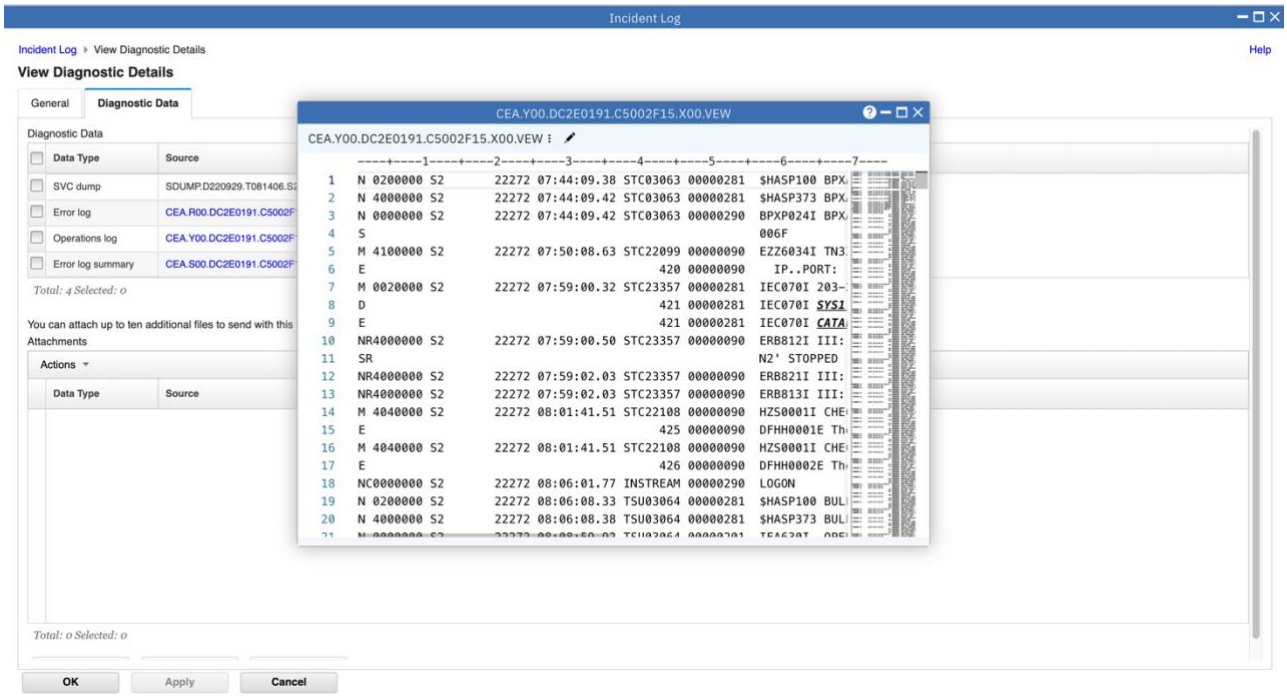
2.Click on the Operations log source.



3.Select the Link to The z/OSMF Desktop Editor, click OK directly.



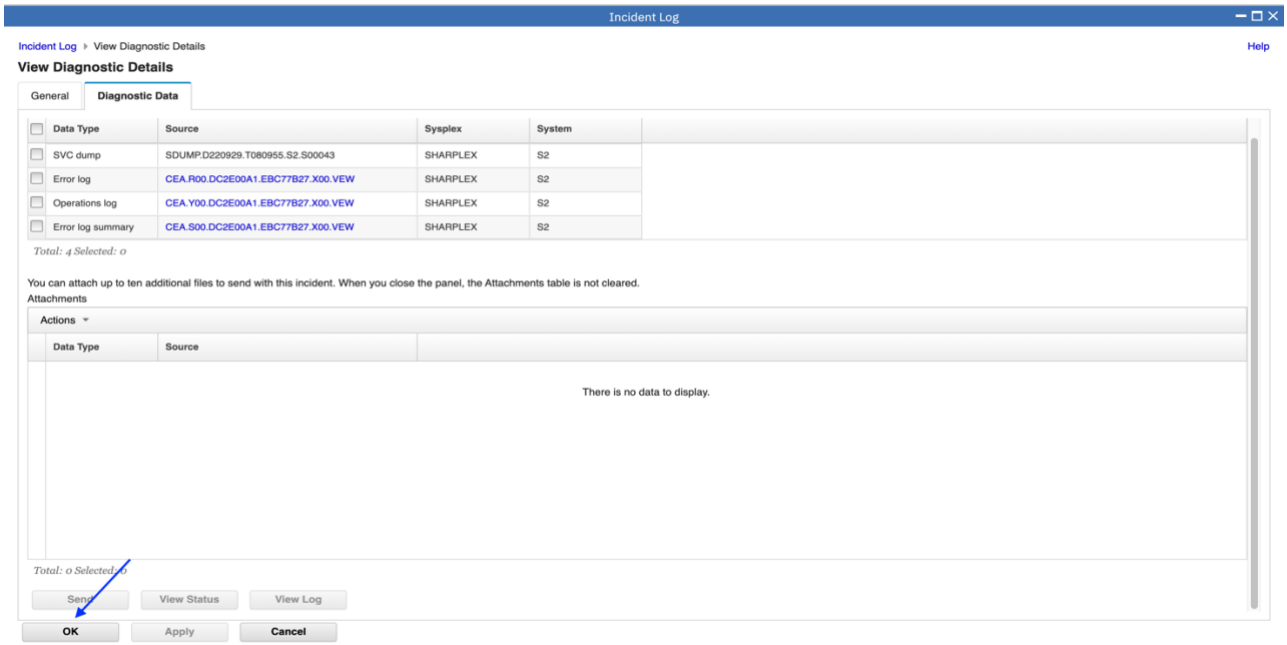
Now you see new Desktop Editor panel. And you can scroll or search the operations log.



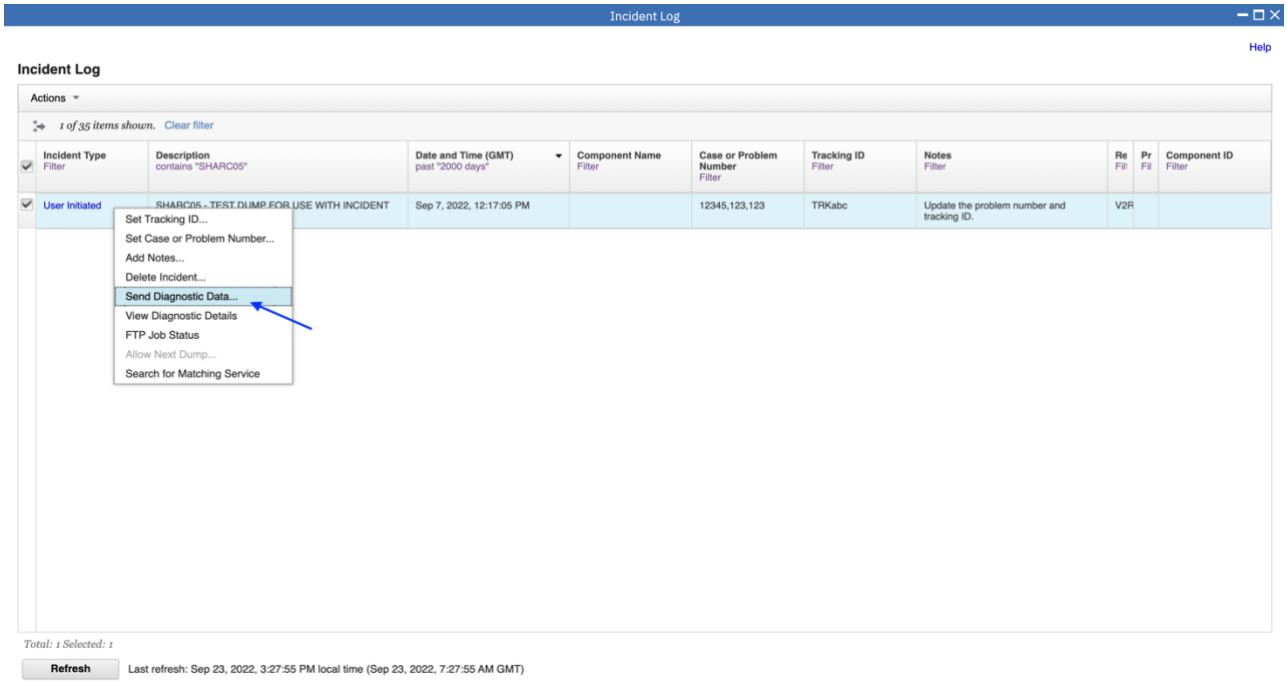
4.After you are done, click the ‘X’ of the Desktop Editor to close it.

5. FTP the diagnostic data captured for an incident to your service provider

1.Now back to the Incident Log task. Just click OK. You will go back to your filtered lists of incidents.



2.Right click on “User Initiated” in the Incident Type column. Then click on Send Diagnostic Data… in the context sensitive list of actions



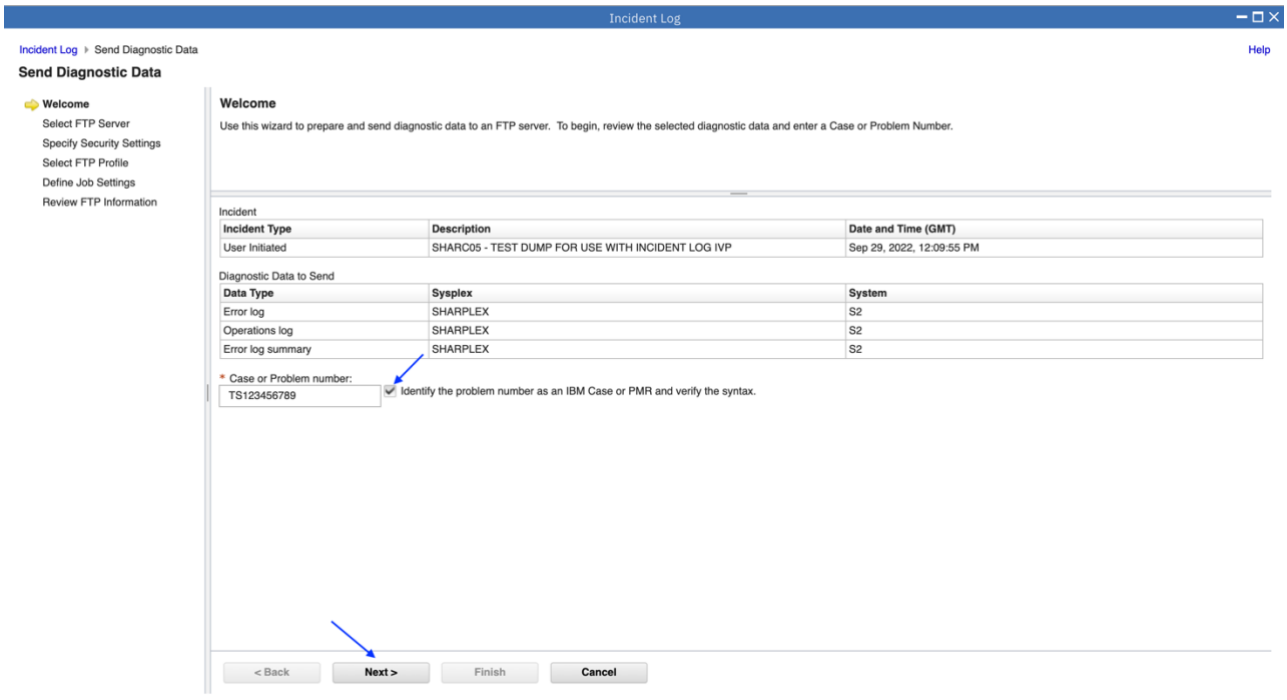
You will now be able to work with a wizard that will guide you through the steps to FTP the diagnostic data for that incident.

The first panel you see is the Welcome page. Notice that it has the steps you will be guided through on its left pane. It shows you what steps have been completed and which one is your current one

The welcome page has the details about the Incident you are working with, plus it lists the pieces of diagnostic data that is going to be sent.

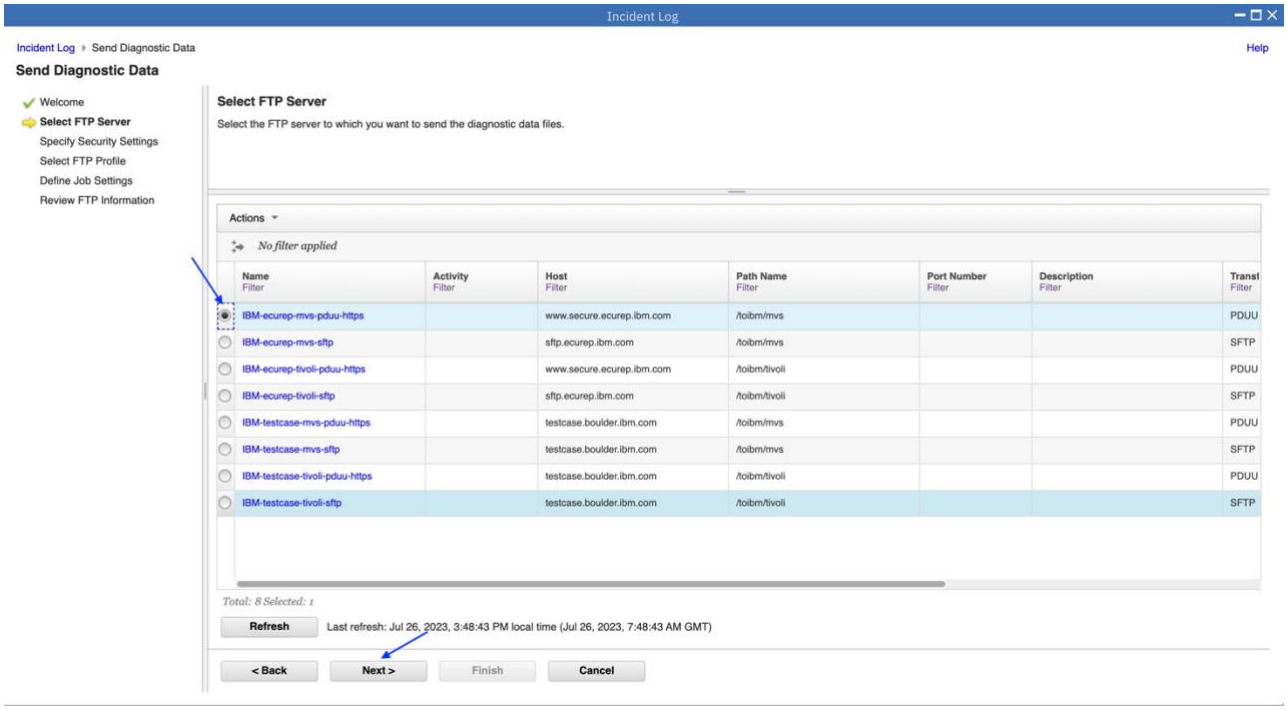
It also shows you the problem number associated with the Incident. If the incident does not have one already associated, it allows you to set one here. The problem number is required to help identify the FTP-ed files at the destination.

1.Check the checkbox and Click on Next button.

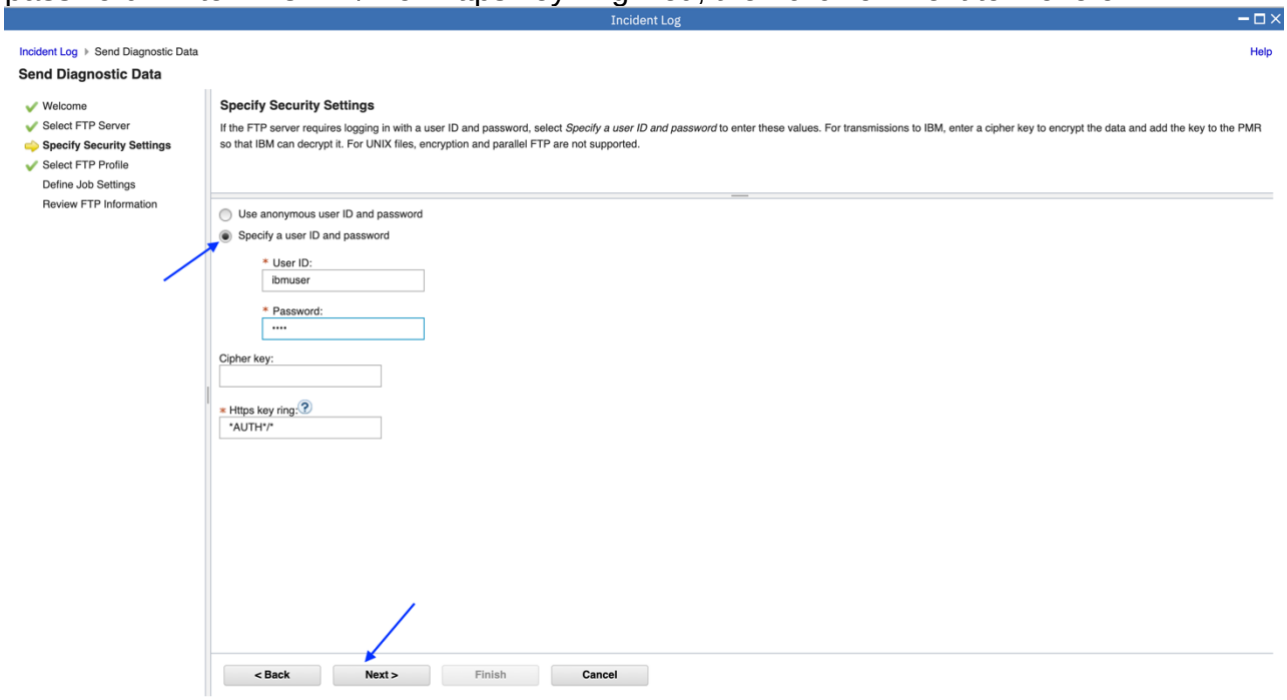


The next page in the wizard allows you to select where you want to send these files/datasets. For this exercise, select the fourth one in the list and click on Next. Note: Next is not enabled until an FTP server is selected.

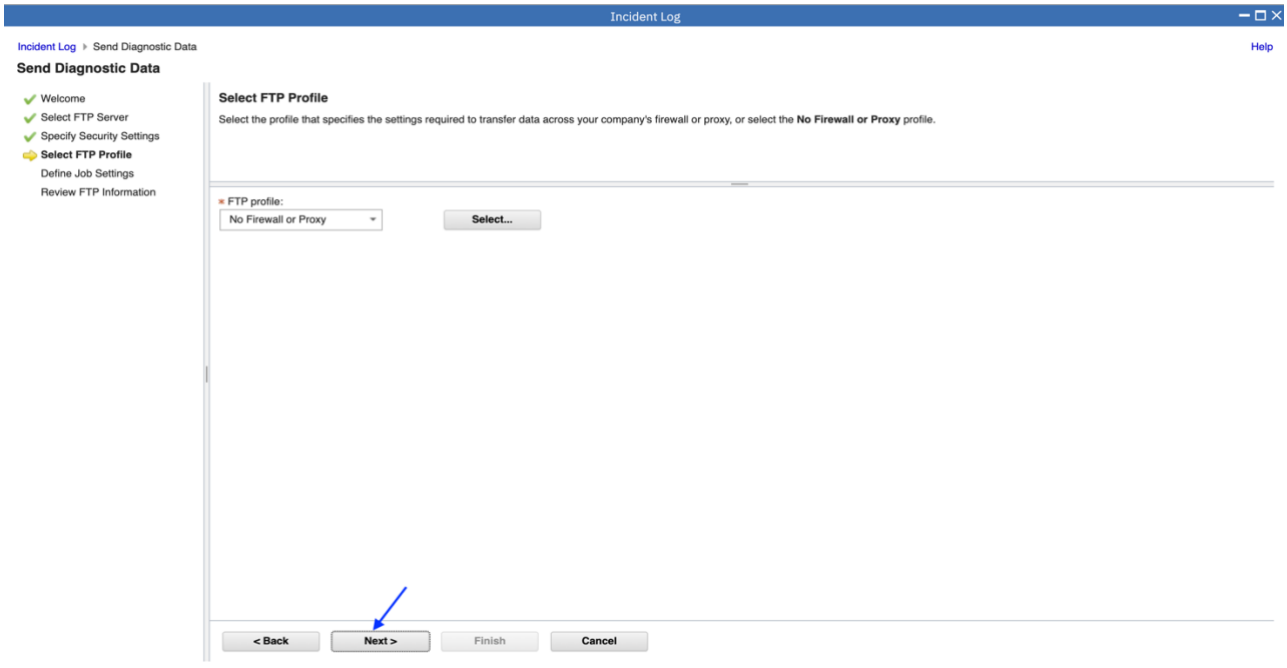
2.Select the IBM-ecurep-mvs-pduu-https server. Then click Next.



This is where you can enter the userid/password needed to access the Destination server you selected in the previous step.
3.Specify a user ID and password, you can specify ibmuser as the user ID and test as the password. Enter *AUTH*/* for Https key ring filed, then click on Next to move on.

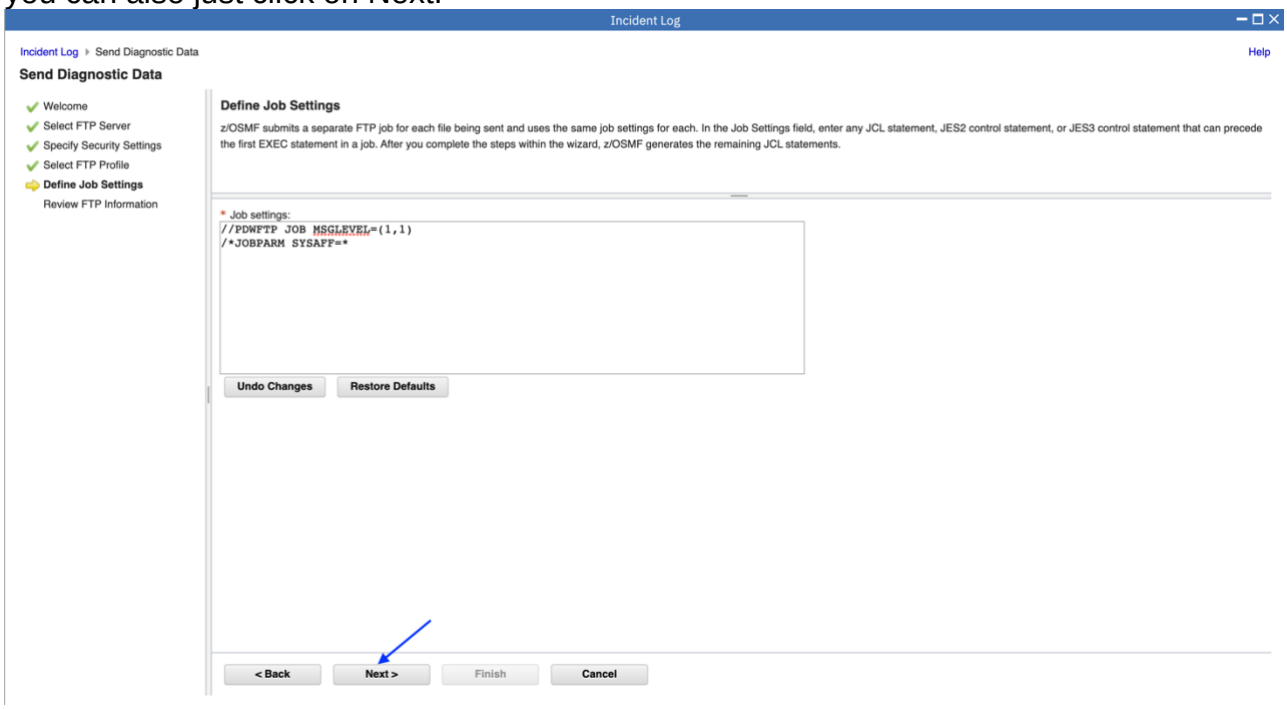


4.This is where you can specify your firewall or proxy information if needed. In this exercise, we do not have a firewall. Make sure that the No firewall or proxy option is selected in the drop down, and then click on Next.



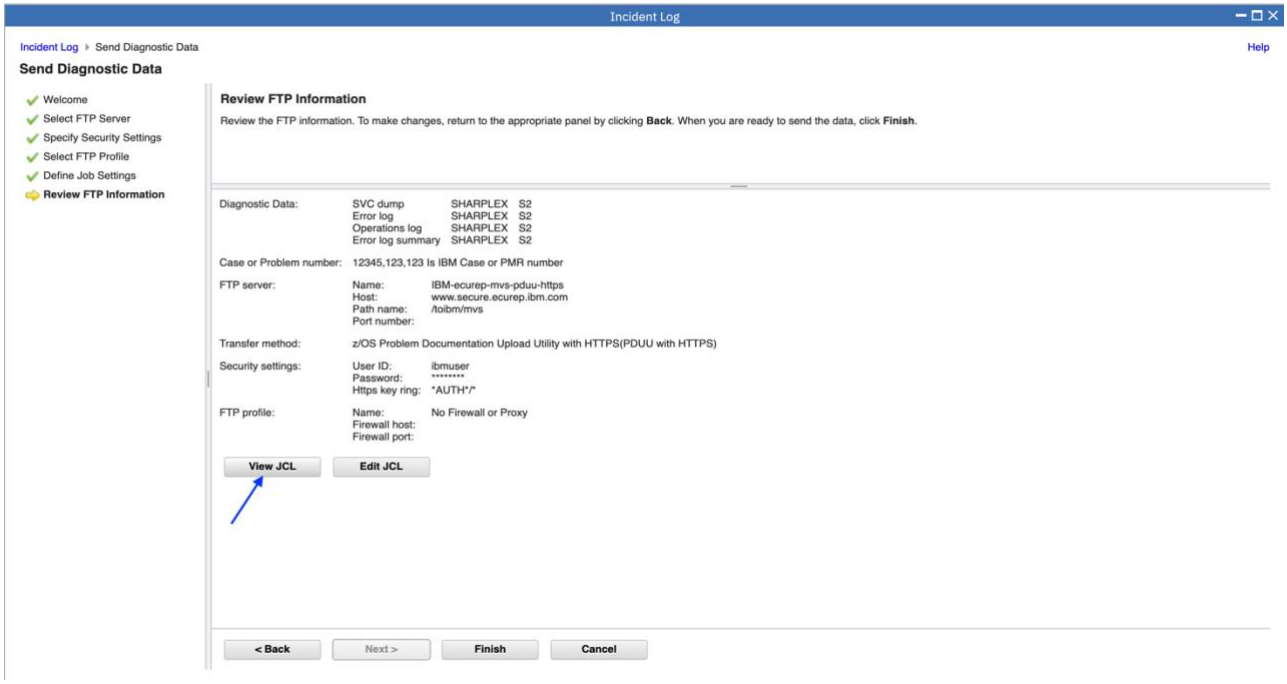
At this stage you have the ability to edit/specify the job card information for the FTP Job that is being built in the background.

5.You can make changes if you'd like. The default entries will work for our lab session, so you can also just click on Next.

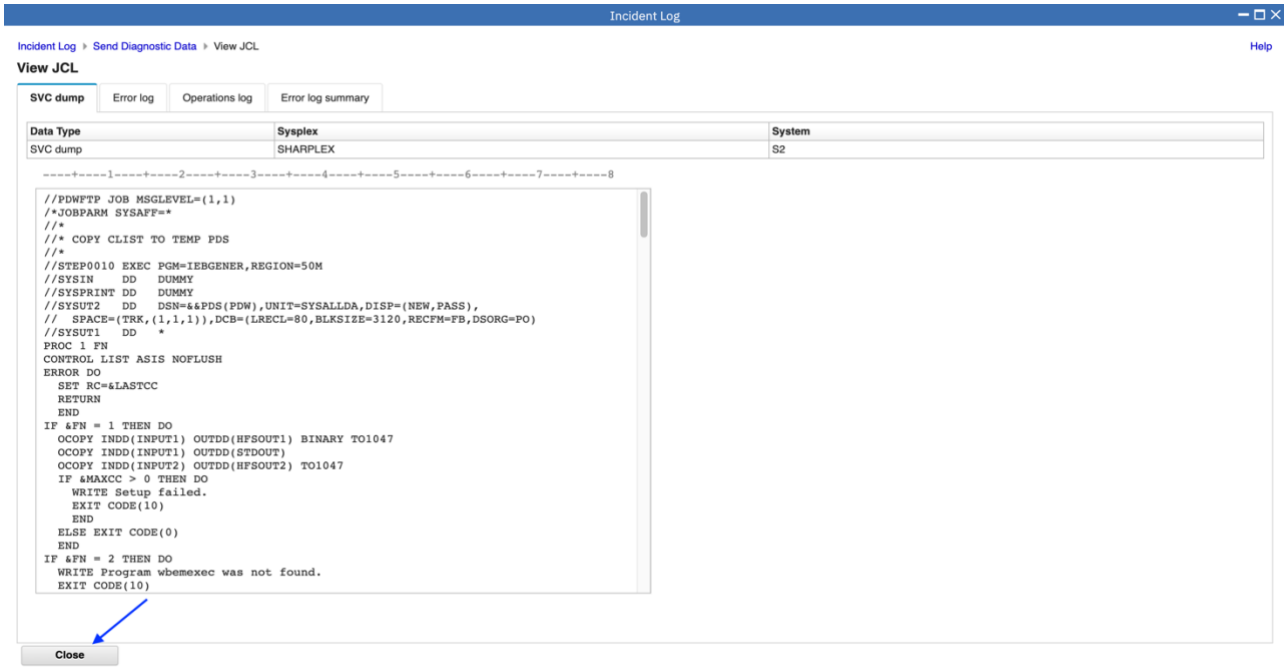


The wizard has walked you through collecting all the information needed to FTP the diagnostic data to your service provider. This page allows you to review all the data that you have provided.

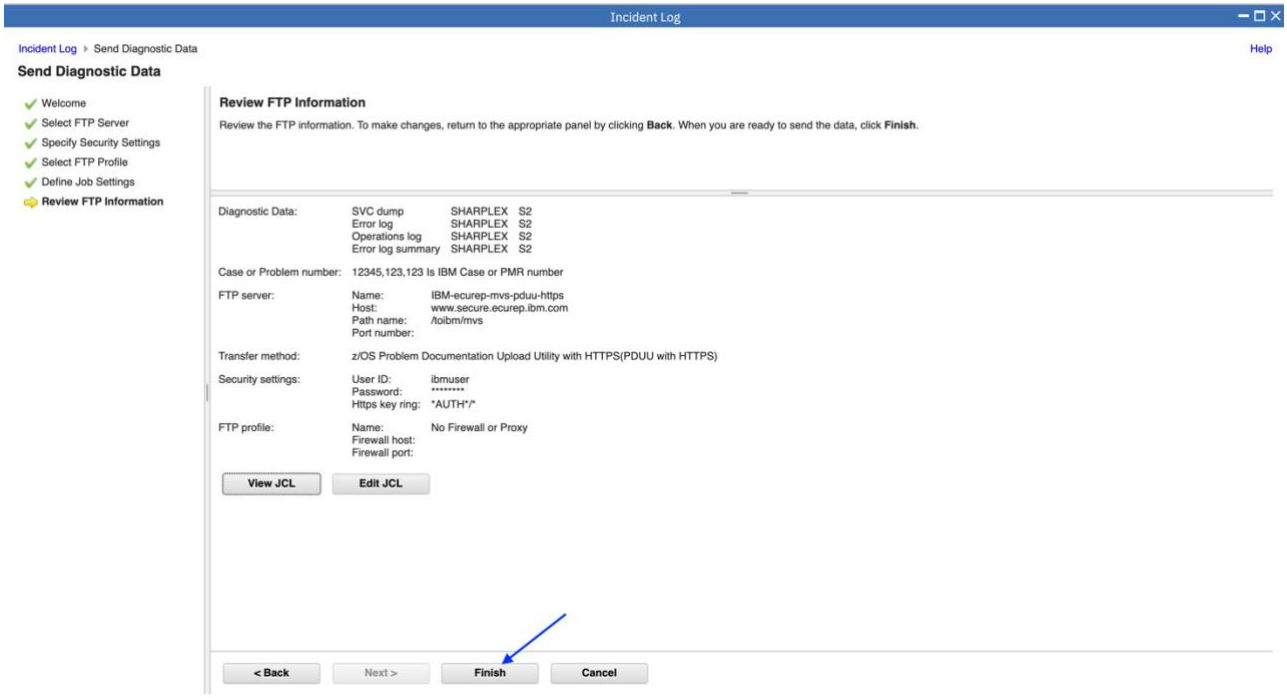
6.Optionally, you can view or edit the JCL. We do not recommend changing the JCL. The next step is to review the information that was previously entered. If you wanted to change anything you would use the Back button on the bottom of the page.



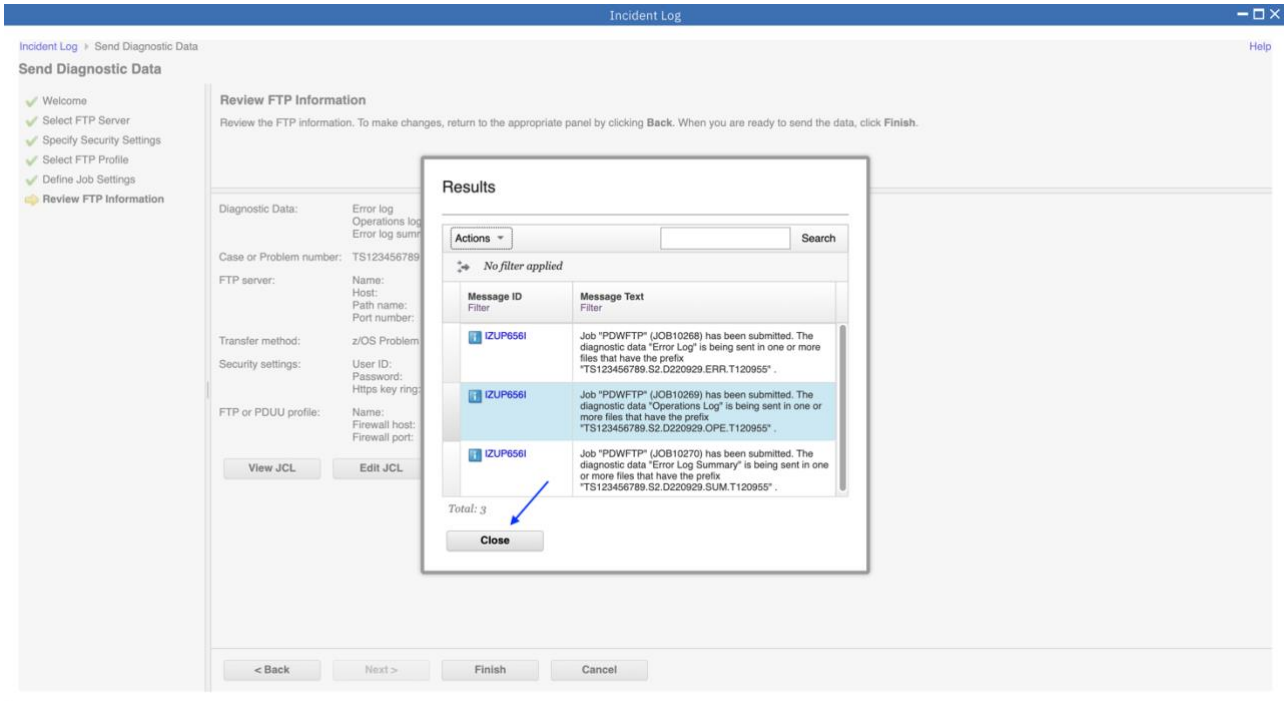
7.After reviewing each tab, click Close.



8.When you are ready to submit the FTP jobs, click on Finish. This will submit jobs to ftp the selected pieces of diagnostic data over to the selected FTP Destination.



9.A pop-up window is displayed with messages identifying the jobs that were submitted. Optionally you can click on the message to see the message description. Click Close.



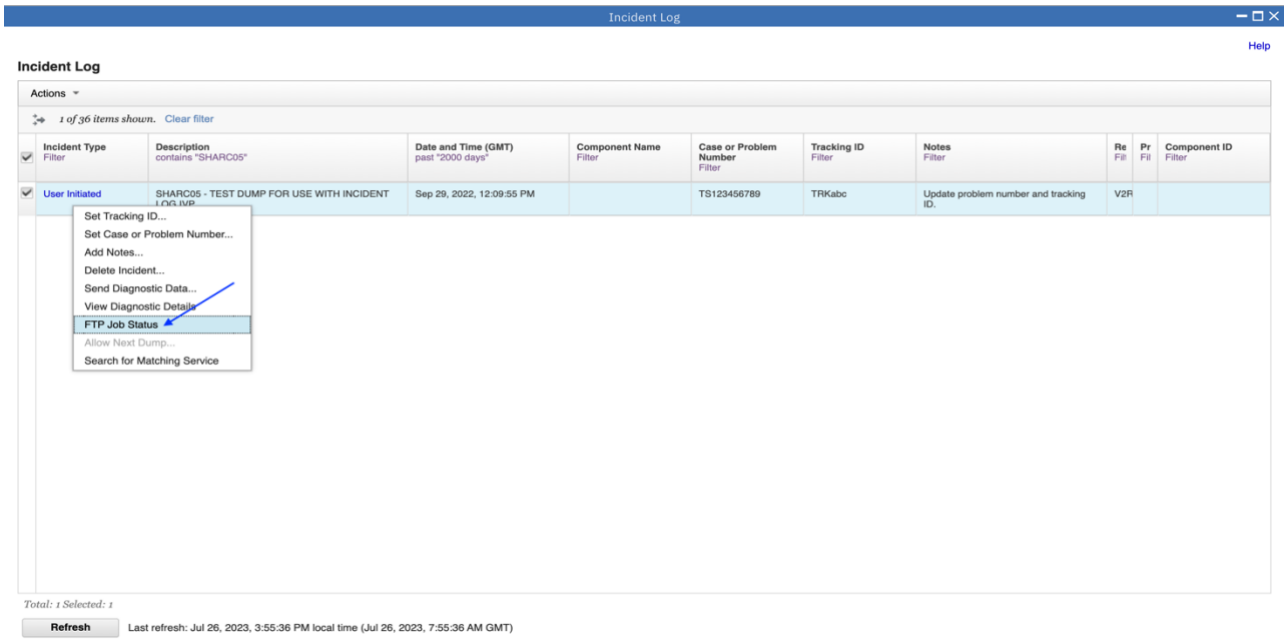
6. View the status of the FTP for that incident

This page shows you the job status for all the FTP jobs submitted for this incident. You can click on the Refresh button to update the status of the jobs.

Note: If a log snapshot does not have any entries, the job might fail.

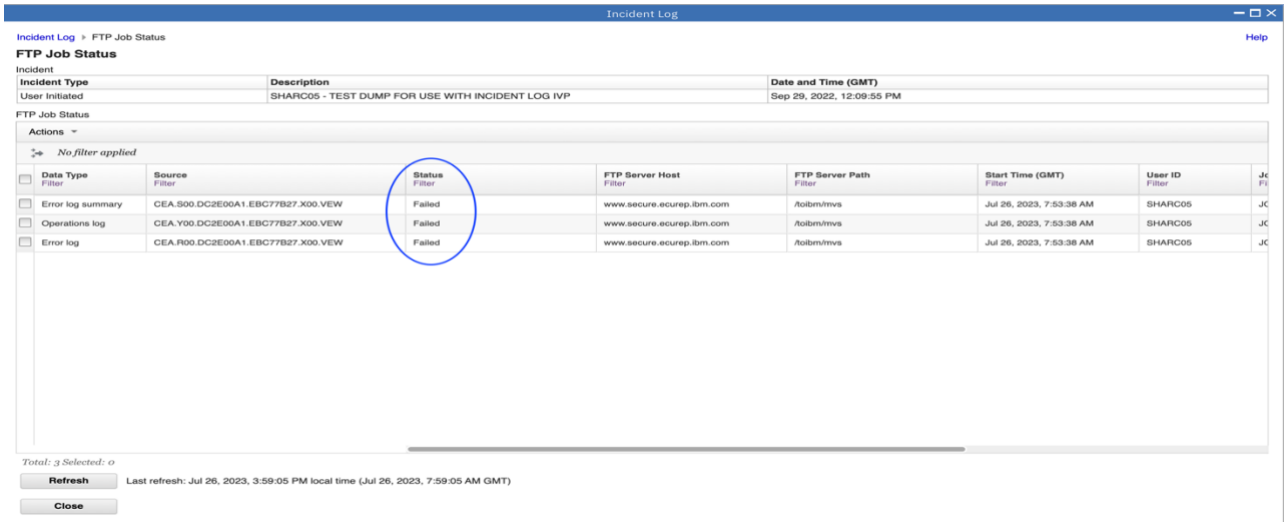
1. Right click on “User Initiated” in the Incident Type column.

2. Then click on FTP Job Status in the context sensitive list of actions



3.The Job status is displayed. After reviewing, click Close.

Note: The jobs during the lab will fail, on your system they should complete successfully.

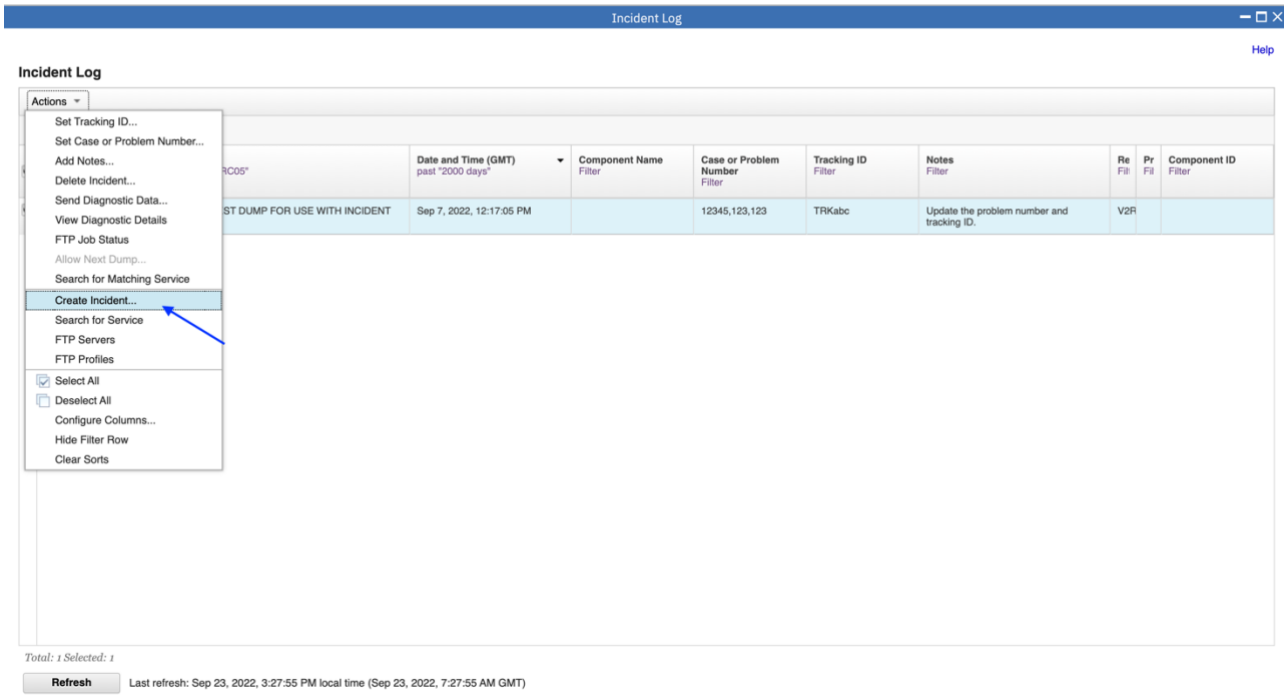


7. Manually create an incident

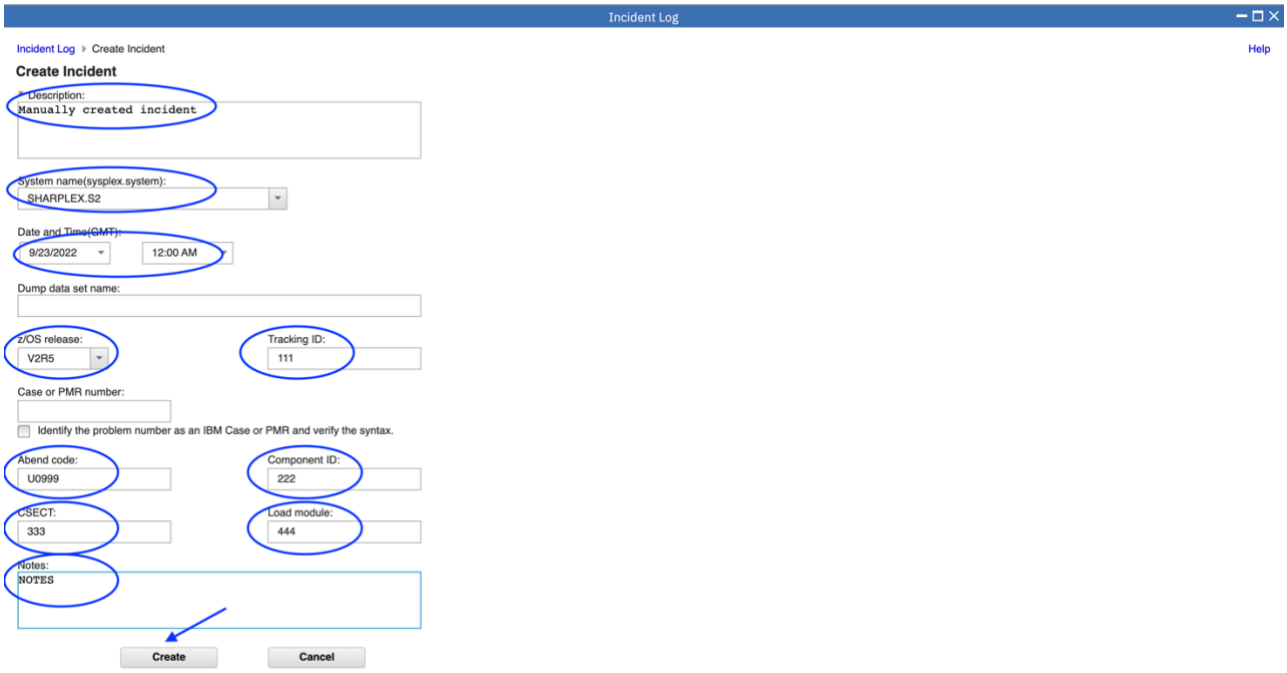
Since z/OSMF V2R2, you can manually create an incident with or without an existing dump data set.

Step 7a: Create incident

1.Click Actions drop-down menu on the main panel of Incident Log, then click “Create Incident” menu item.



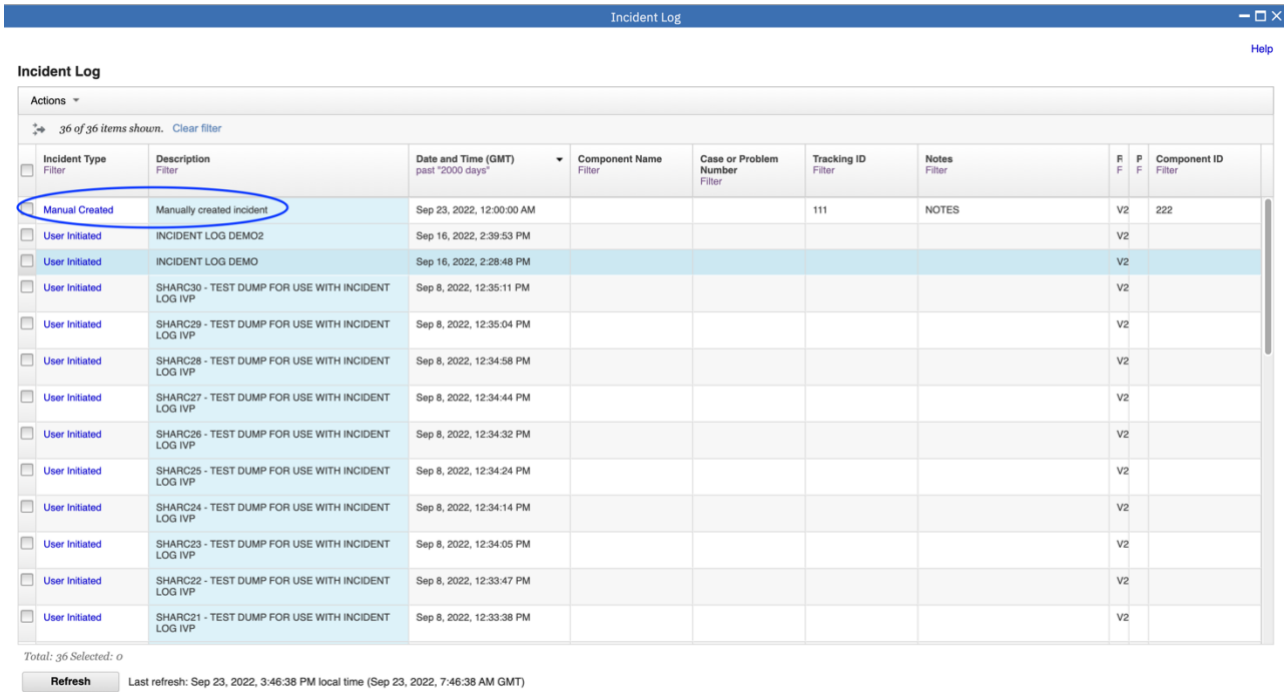
On Create Incident page, only “Description” field is required, others are not required. For this exercise, you can enter “Manually created incident” as the Description, select SHARPLE.S2 as System name, enter 7/26/2023 12:00 am as Date and Time, select V2R5 as z/OS release, enter 111 as Tracking ID, enter U0999 as Abend code, enter 222 as Component ID, enter 333 as CSECT, enter 444 as Load module, enter NOTES as Notes;



When you complete input, click “Create” button, a new incident will be shown in the main panel of Incident Log. The “Incident Type” is “Manual Created”.

There will be new record in the main panel of the Incident Log, Incident Type is Manual.

Note: You will need to remove the Filter set on the Description column, so you can see the manually created incident.

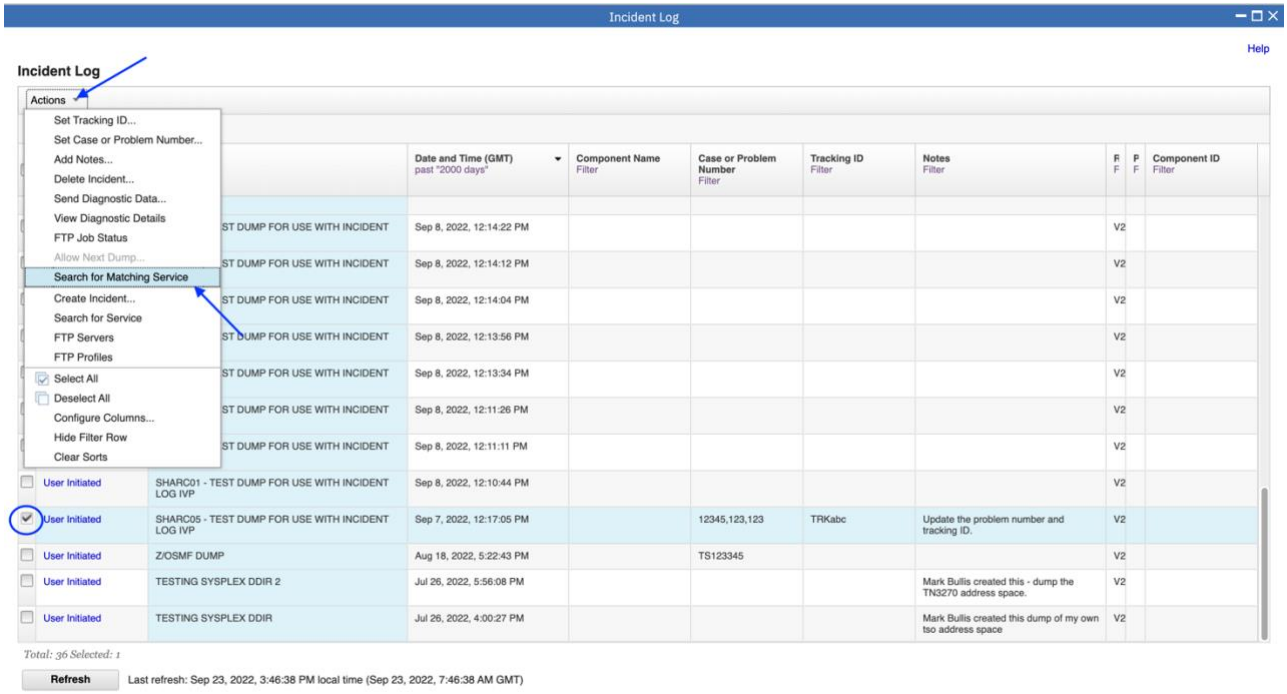


8. APAR search – Quick search or build your own search

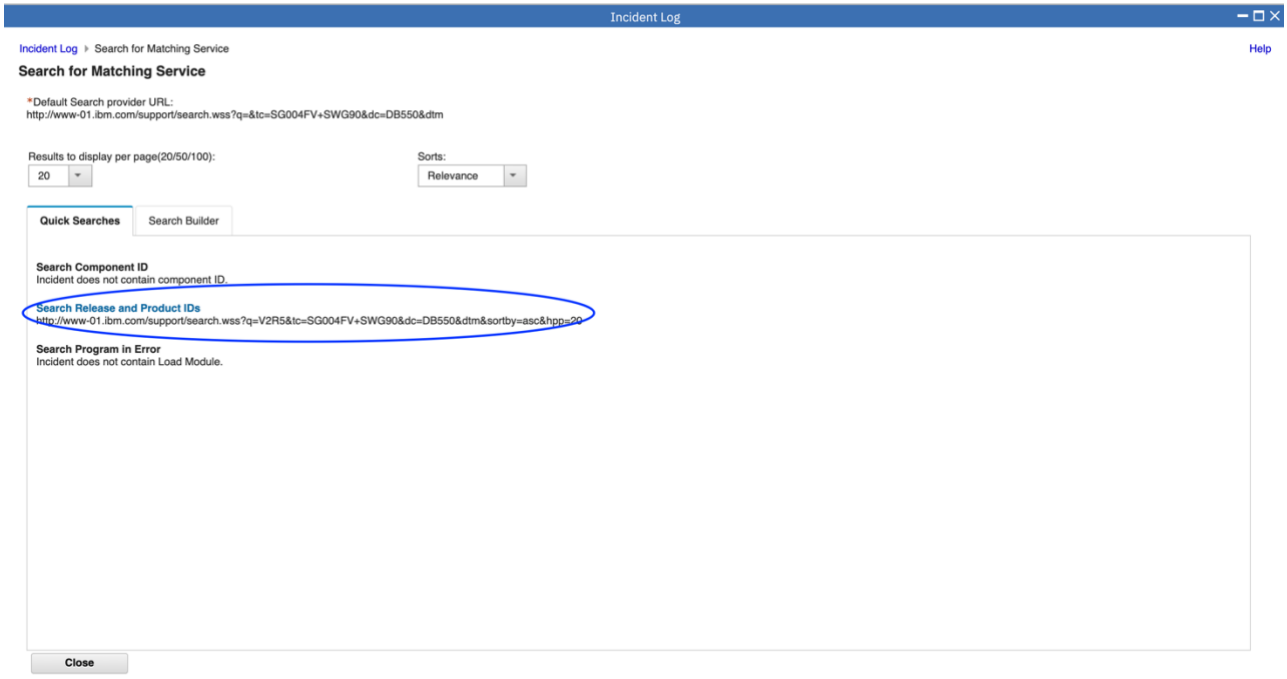
Incident Log supports quickly searching APAR according to symptom of incident associated dump. You can utilize default searches or build your own search based on conditions you want.

Step 8a: APAR Quick Search

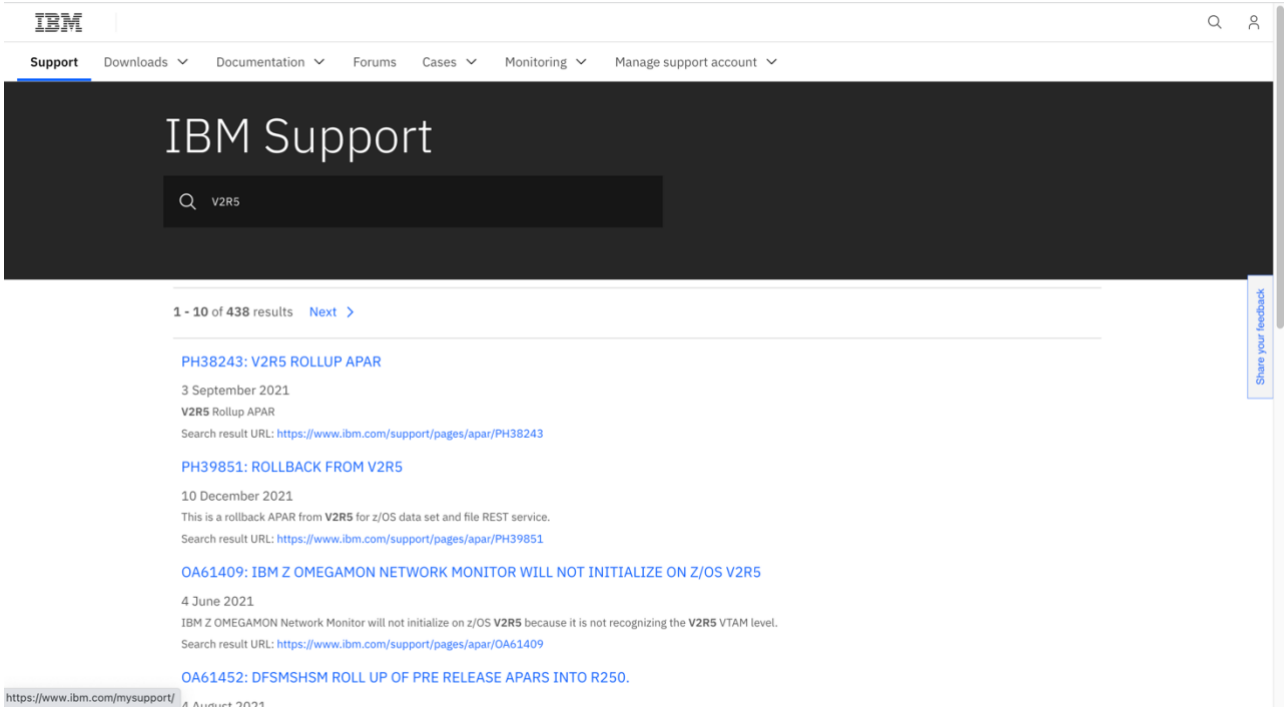
1.Select an incident, then Click “Actions” drop-down menu, click “Search for Matching Service” menu item.



On Search for Matching Service page, there are two tabs: Quick Searches and Search Builder. “Quick Searches” tab lists 3 default URLs to query APAR.



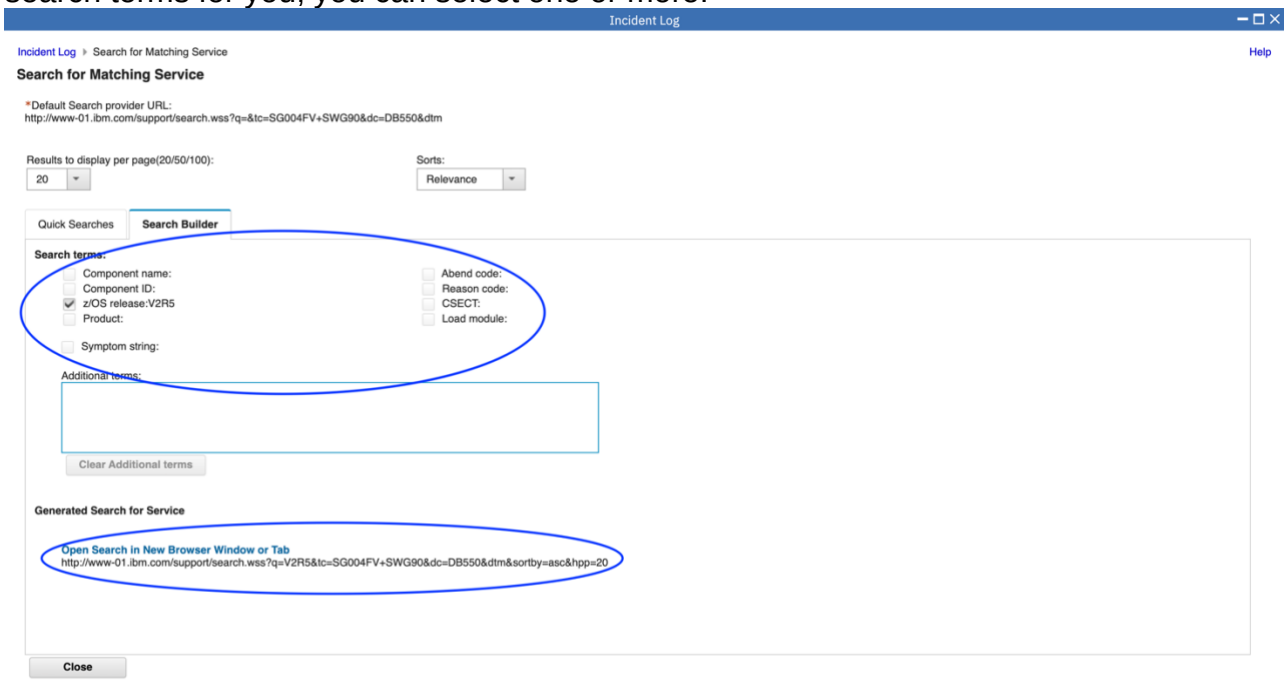
2.You can click the links to directly open search result. You can also copy the URL and open it with Browser to get corresponding APAR search results.



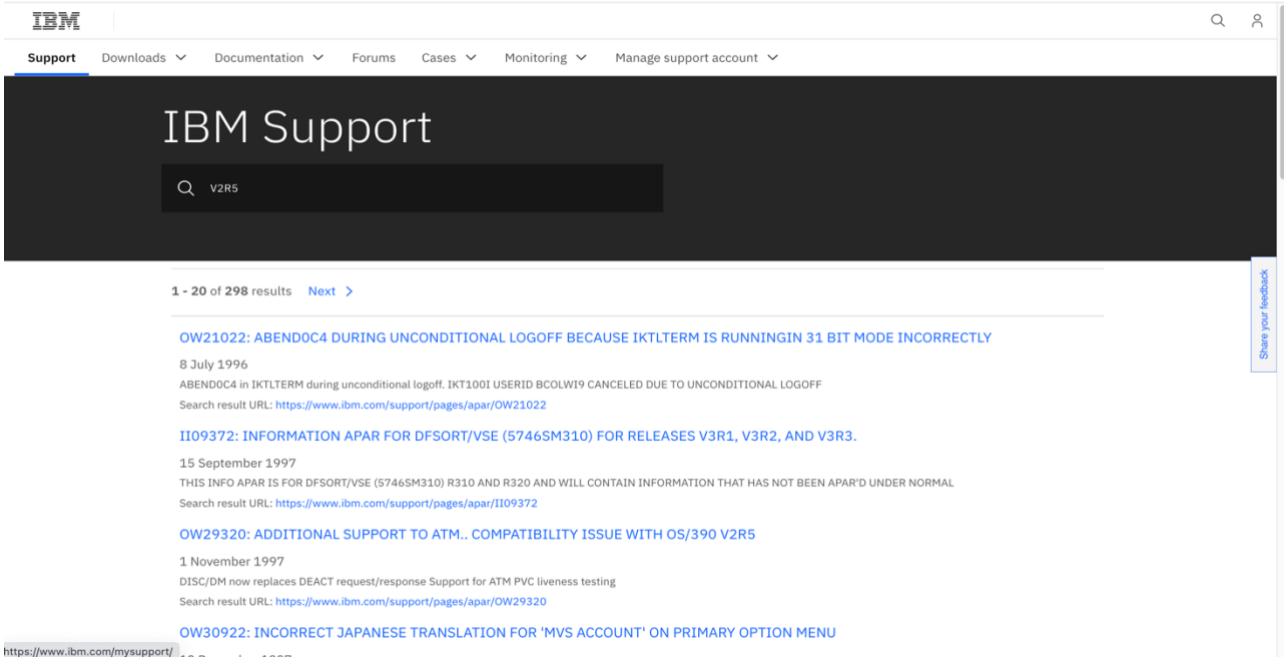
Step 8b: Build your own search

If the default query provided by “Quick Searches” tab can not fulfill your requirements, you can also build your own search in the “Search Builder” tab.

1.On Seach Builder page, there are more conditions. Move to Search Builder label. More search terms for you, you can select one or more.



2.You can click the final link to get search results or copy the URL and open it with browser.



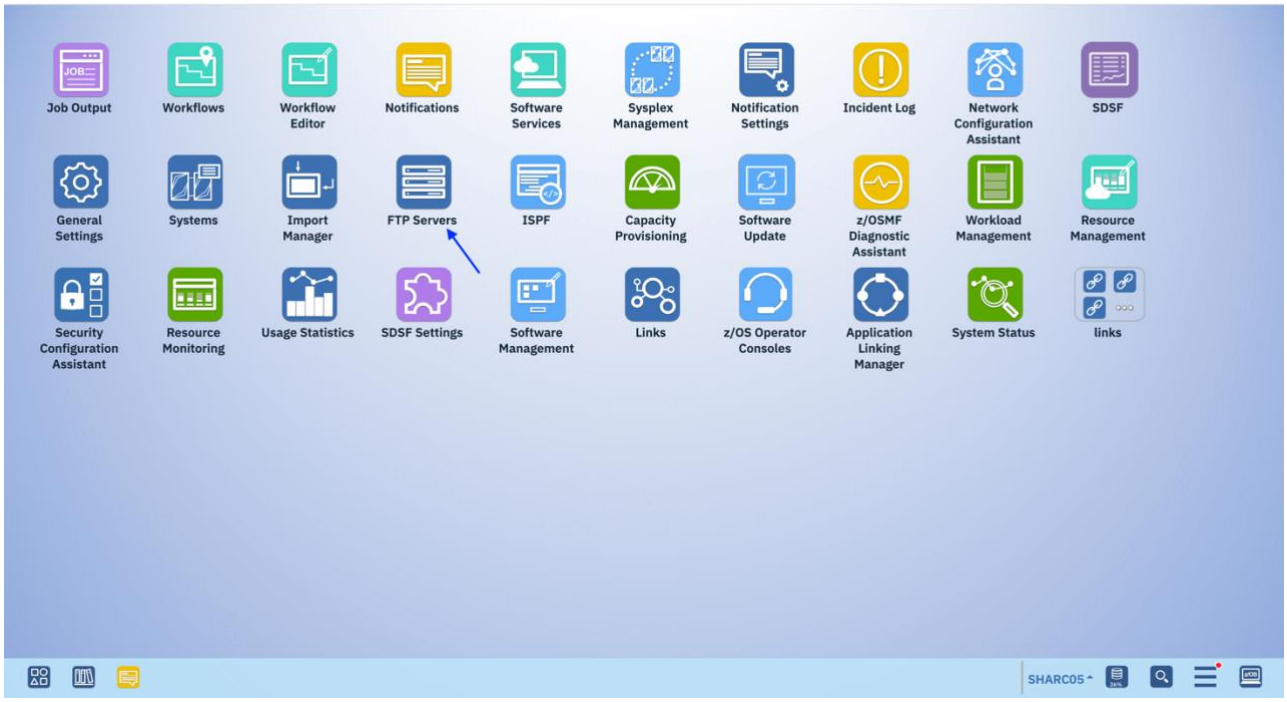
Optional Exercises

__ **9.** View FTP Destinations

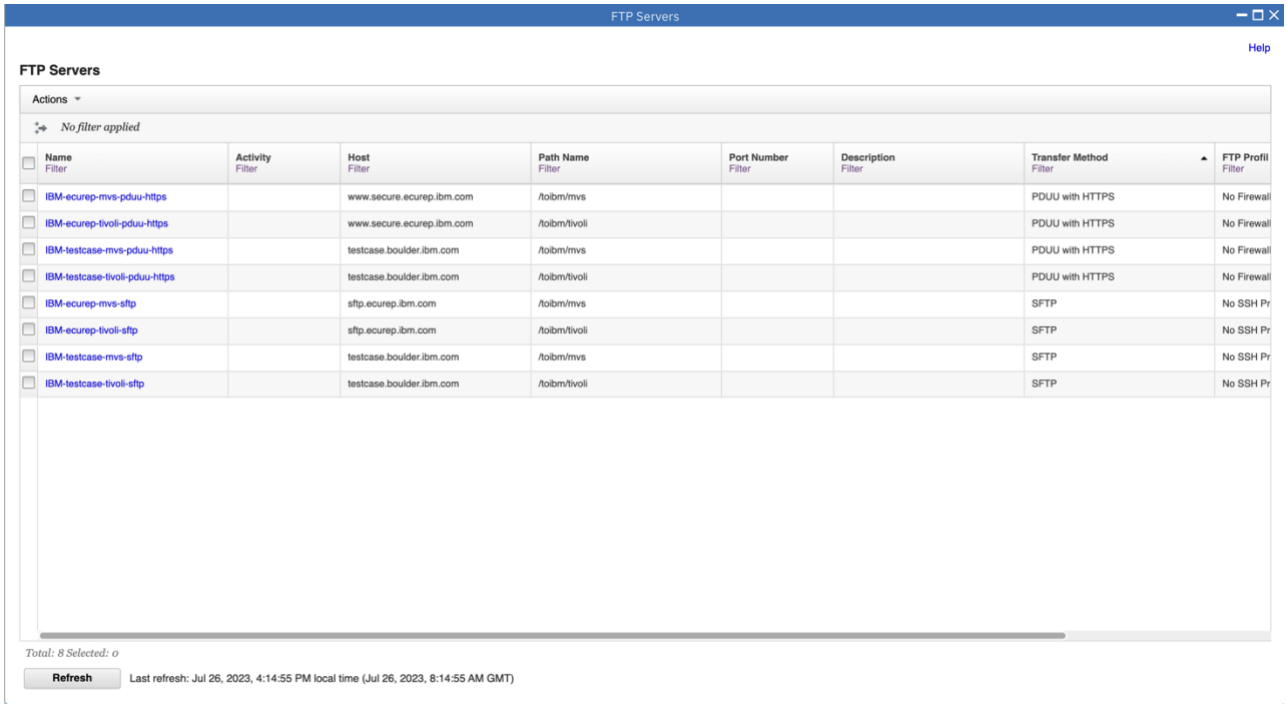
__ **10.** View FTP the diagnostic data captured for an incident to your service provider

Optional Exercise – View FTP Servers

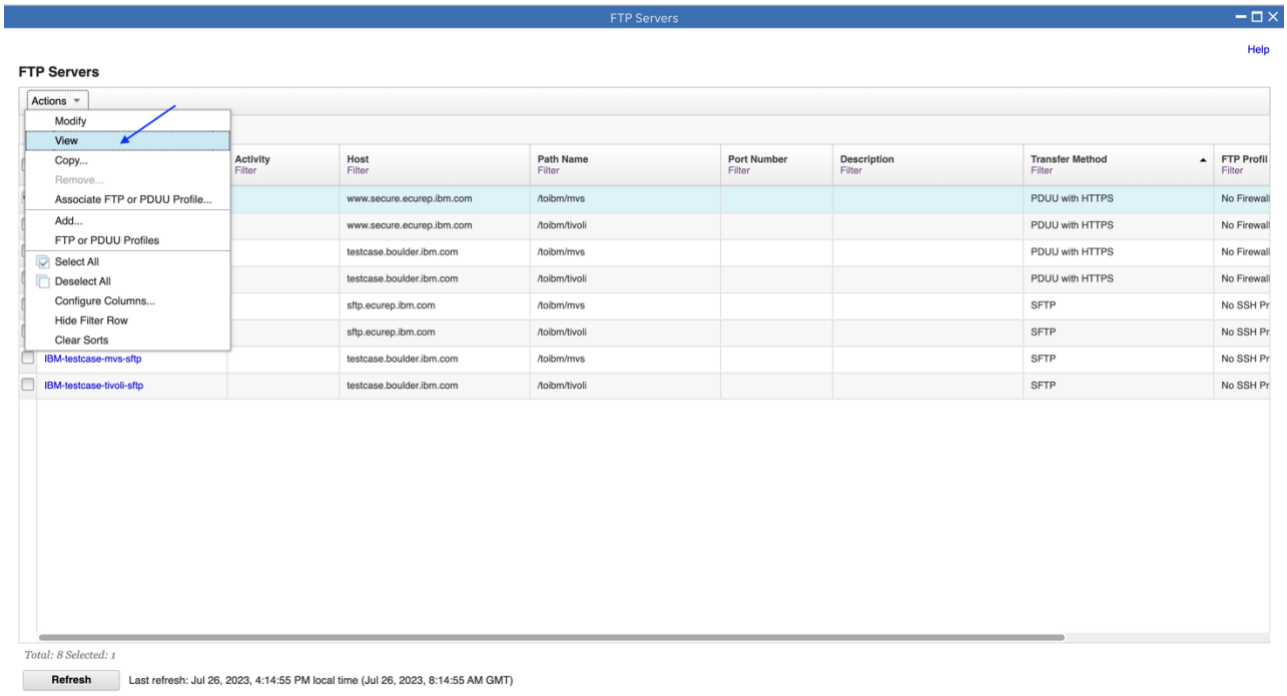
1.To get started, back to Desktop and click FTP Servers task.



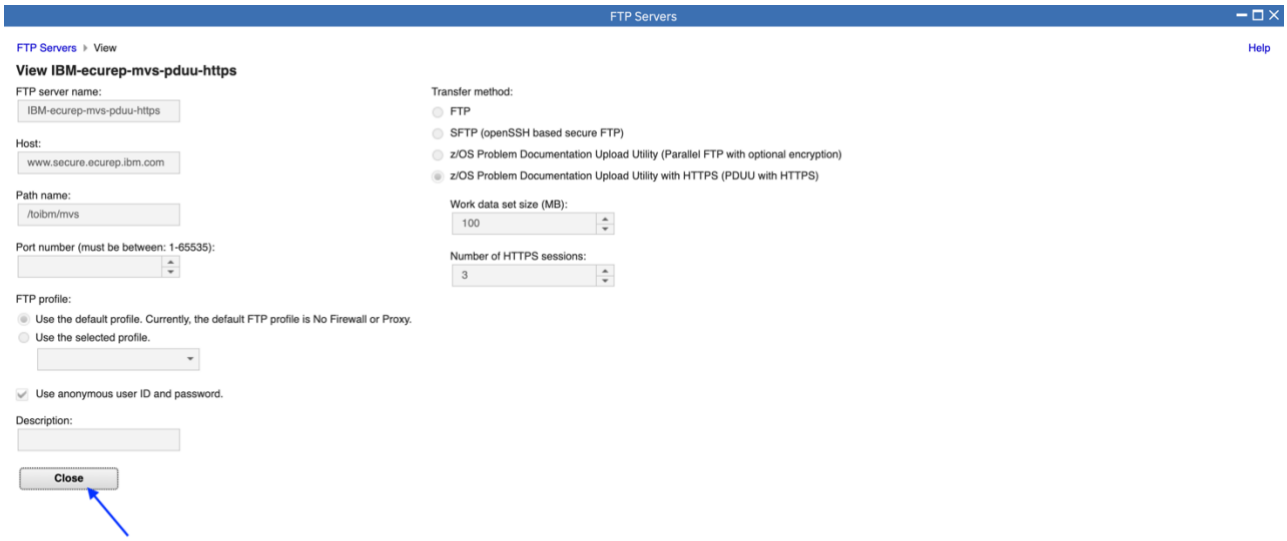
A list of defined FTP servers is displayed. The z/OSMF Administrator can add, modify, or remove an FTP Server. Servers in this list are displayed when selecting a FTP server during the Send Diagnostic Data wizard.



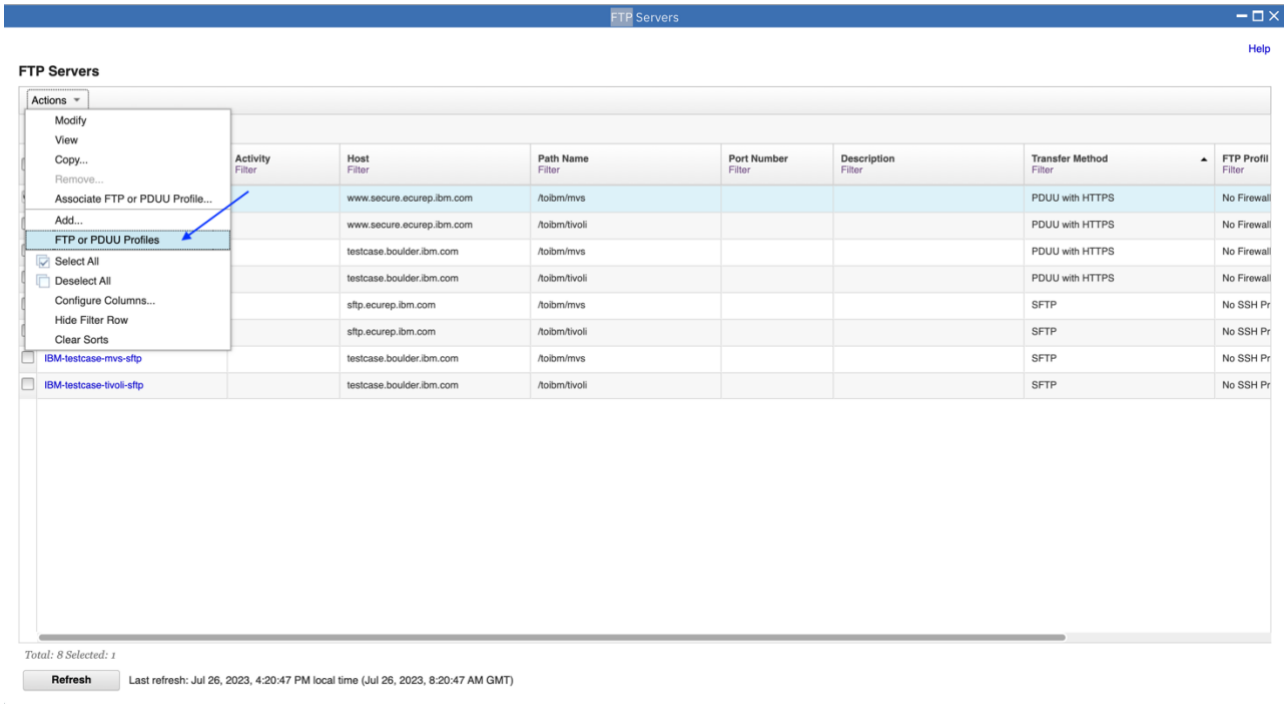
2.First select the IBM-ecurep-mvs-pduu-https server. Then click Actions, followed by View.



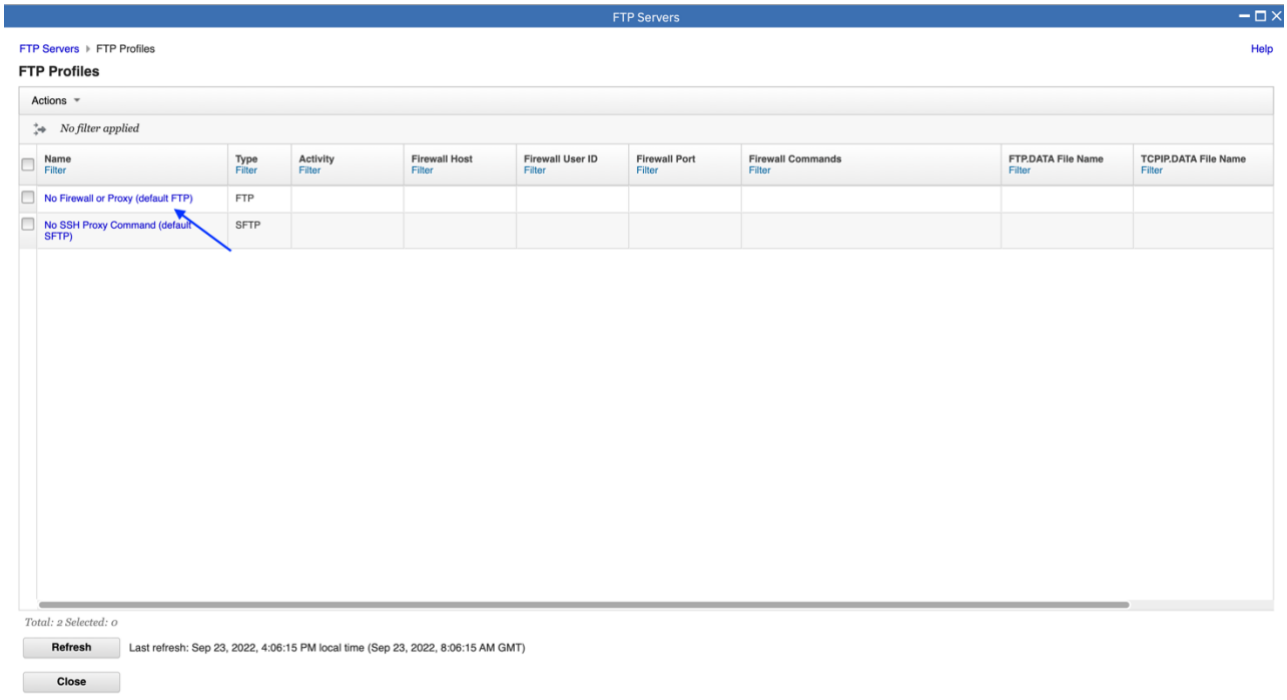
3.The properties of the Server are displayed. After reviewing, click Close.



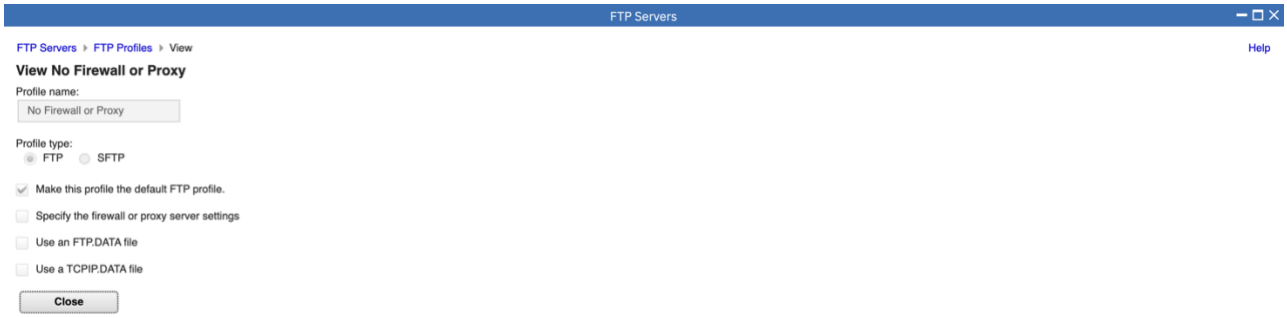
4.Click Actions, then FTP or PDUU Profiles.



5.Click on No Firewall or Proxy in the Name column.



6.The properties of the FTP Profile are displayed. After reviewing, click Close.



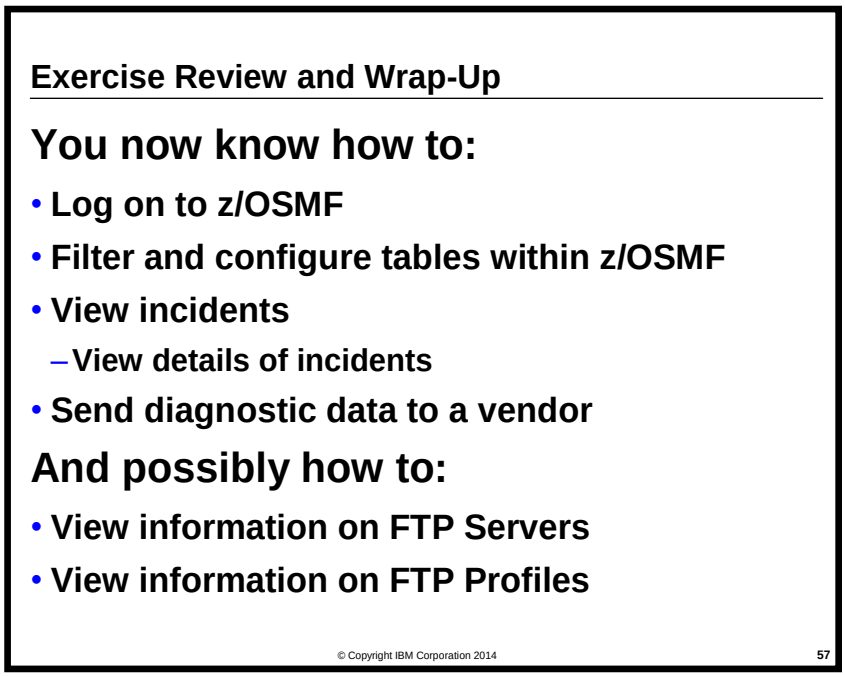
The Incident Log Exercises are complete. If you plan on trying other z/OSMF functions in the session, close the open tasks by clicking the “X” for:

- Incident Log
- FTP Servers

Otherwise, click “Log Out”

End of exercise

Exercise Review and Wrap-Up



Additional Information

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

IBM*	ServerPac*	* Registered trademarks of IBM Corporation
IBM (logo)	WebSphere*	
RACF*	z/OS*	

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Firefox is a trademark of Mozilla Foundation
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license there from.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Internet Explorer is a trademark of Microsoft Corp
InfiniBand is a trademark and service mark of the InfiniBand Trade Association.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.
* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

See url http://www.ibm.com/legal/copytrade.shtml for a list of IBM trademarks.