



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.

© Copyright IBM Corporation 2014

2

Exercise instructions

Here are the steps you will perform in this lab:

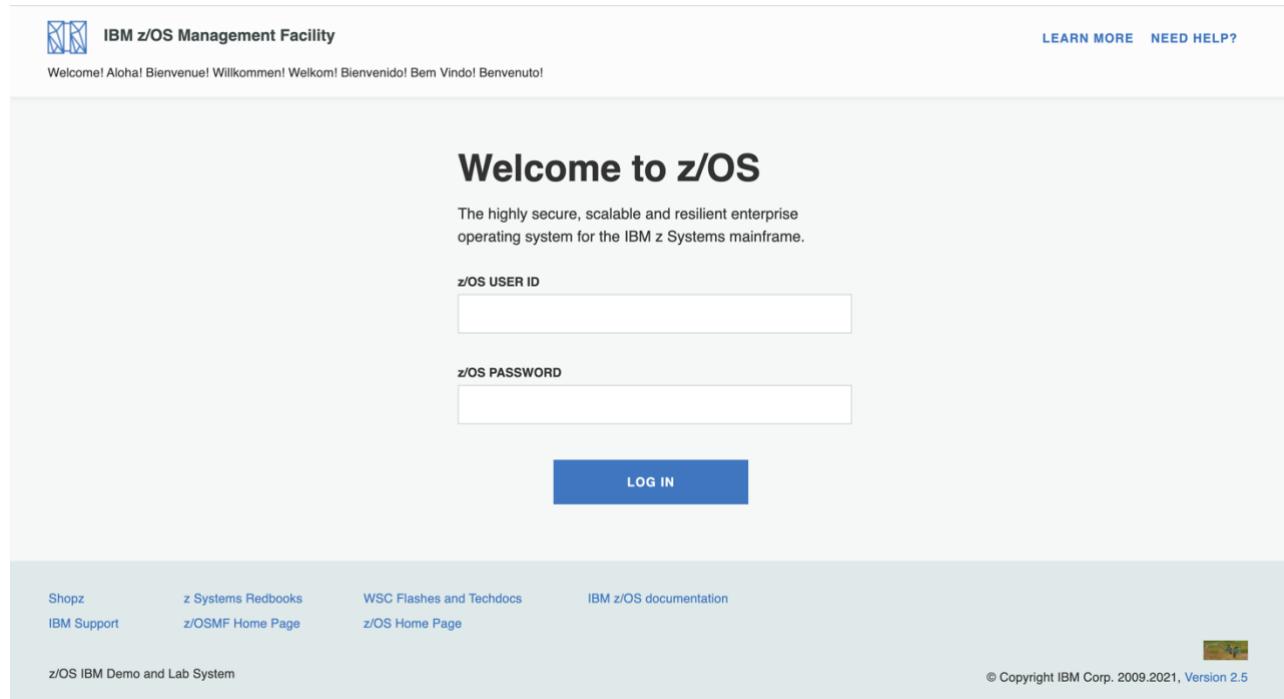
- 1. Logon to z/OSMF
 - a. Launch the Mozilla Firefox browser
 - b. Point Browser to z/OSMF – enter the following URL
<https://share.centers.ihost.com/zosmf/>
 - c. Enter the User ID (SHARCnn) and password assigned to your workstation.
- 2. View all the incidents across all the systems in your sysplex
 - 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

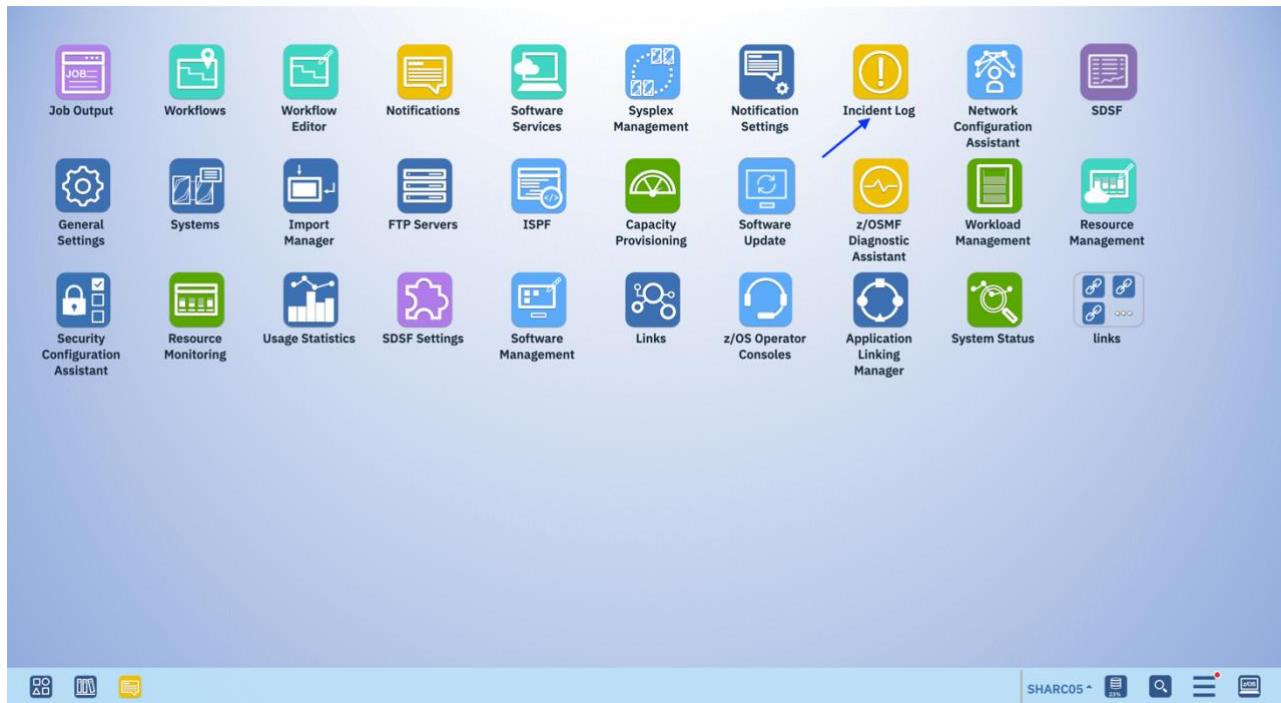
Note: All screen captures in the handout show the ID SHARC05, your browser will be slightly different to reflect the User ID that you were given.



The screenshot shows the IBM z/OS Management Facility login interface. At the top left is the IBM logo and the text "IBM z/OS Management Facility". At the top right are links for "LEARN MORE" and "NEED HELP?". Below the header, a welcome message in multiple languages (Aloha! Bienvenue! Willkommen! Welkom! Bienvenido! Bern Vindo! Benvenuto!) is displayed. The main section is titled "Welcome to z/OS" with a subtext: "The highly secure, scalable and resilient enterprise operating system for the IBM z Systems mainframe." It features two input fields: "z/OS USER ID" and "z/OS PASSWORD", each with a corresponding text input box. A blue "LOG IN" button is centered below the password field. At the bottom of the page, there is a footer navigation bar with links to "Shopz", "z Systems Redbooks", "WSC Flashes and Techdocs", "IBM z/OS documentation", "IBM Support", "z/OSMF Home Page", "z/OS Home Page", and "z/OS IBM Demo and Lab System". On the far right of the footer is a small copyright notice: "© Copyright IBM Corp. 2009.2021, Version 2.5".

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.

Incident Log

Actions ▾

o of *o* items shown. [Clear filter](#)

Incident Type Filter	Description Filter	Date and Time (GMT) past "3 days"	Sysplex Filter	System Filter	Case or Problem Number Filter	Tracking ID Filter	Notes Filter	Component Filter

There is no data to display.

Total: *o* Selected: *o*

[Refresh](#) Last refresh: Aug 23, 2022, 11:16:03 AM local time (Aug 23, 2022, 3:16:03 AM GMT)

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**.

The screenshot shows the 'Incident Log' application window. At the top, there's a toolbar with 'Incident Log', 'Help', and other standard icons. Below the toolbar is a header bar with 'Actions' and a message '0 of 0 items shown. Clear filter'. The main area is a table with several columns: 'Incident Type Filter', 'Description Filter', 'Date and Time (GMT) past "3 days"', 'Sysplex Filter', 'System Filter', 'Case or Problem Number Filter', 'Tracking ID Filter', 'Notes Filter', and 'Component Filter'. A blue arrow points to the 'Date and Time (GMT) past "3 days"' column header. Below the table, a message says 'There is no data to display.' At the bottom left, there are buttons for 'Total: 0 Selected: 0' and 'Refresh'. To the right of the refresh button, it says 'Last refresh: Aug 23, 2022, 11:16:03 AM local time (Aug 23, 2022, 3:16:03 AM GMT)'.

2.Change Amount to 2000, then click Filter.

The screenshot shows the 'Incident Log' interface with a 'Build Filter' dialog box overlaid. The dialog box contains a 'Rules' section with a dropdown for 'Date and Time (GMT)' set to 'past', a text input for '2,000', and a dropdown for 'days'. A blue arrow points to the '2,000' input field. Another blue arrow points to the 'Filter' button at the bottom of the dialog box. The main interface shows a table with columns for 'Actions', 'Incident Type', 'Description', 'Date and Time (GMT)', 'Sysplex', 'System', 'Case or Problem Number', 'Tracking ID', 'Notes', 'Release', 'Product', and 'Component Name'. The table currently displays 0 items.

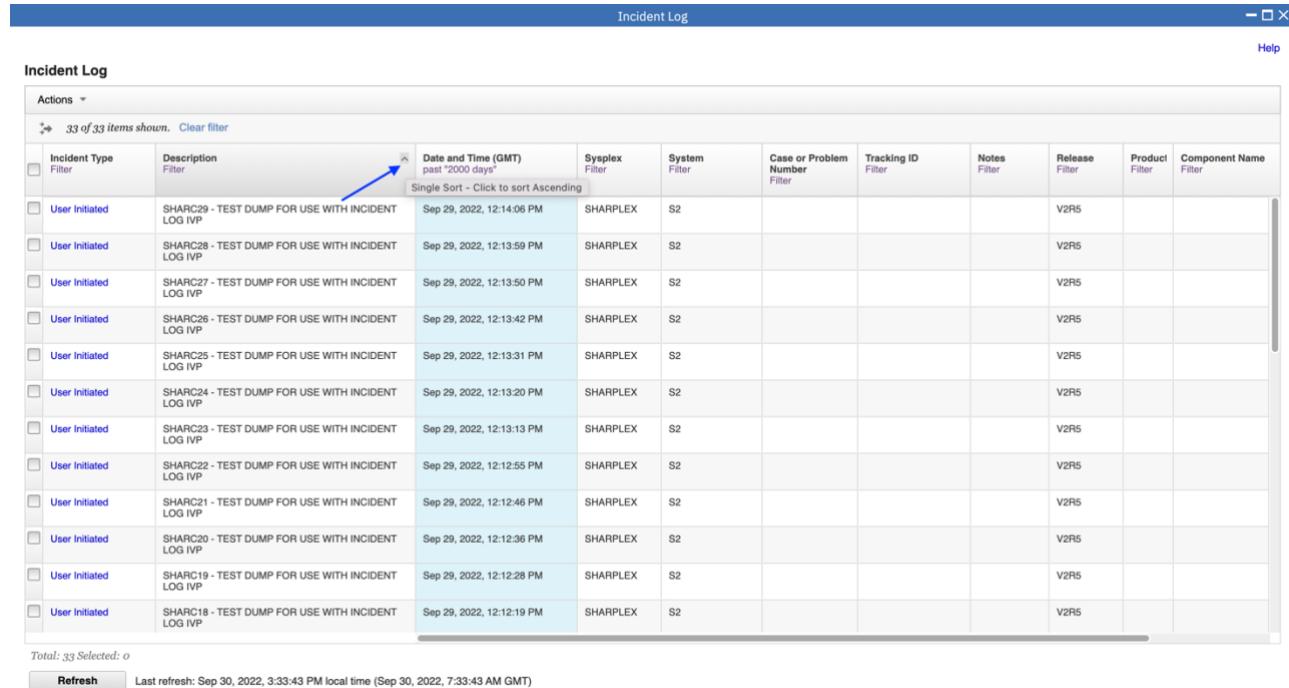
Now the list of incidents displayed on a table.

The screenshot shows the 'Incident Log' interface displaying a list of 33 incidents. The table includes columns for 'Actions', 'Incident Type', 'Description', 'Date and Time (GMT)', 'Sysplex', 'System', 'Case or Problem Number', 'Tracking ID', 'Notes', 'Release', 'Product', and 'Component Name'. All incidents listed are of type 'User Initiated' and occurred on Sep 29, 2022, between 12:14:06 PM and 12:28 PM. The 'Date and Time (GMT)' column shows values like 'past 2,000 days', 'Sep 29, 2022, 12:14:06 PM', etc. The 'Sysplex' and 'System' columns are both 'SHARPLEX'. The 'Case or Problem Number' column contains unique identifiers such as SHARC29 through SHARC18. The 'Tracking ID', 'Notes', 'Release', 'Product', and 'Component Name' columns are all empty or show their respective filter headers.

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.



The screenshot shows a table titled "Incident Log" with various columns for filtering and sorting. The "Description" column header has an upward-pointing arrow indicating an ascending sort. The table lists 33 items, all of which are "User Initiated" type, with descriptions ranging from "SHARC29 - TEST DUMP FOR USE WITH INCIDENT LOG IVP" to "SHARC18 - TEST DUMP FOR USE WITH INCIDENT LOG IVP". The last item listed is highlighted in light blue.

Incident Log										
Actions ▾										
33 of 33 items shown. Clear filter										
Incident Type Filter	Description Filter	Date and Time (GMT) past "2000 days" Single Sort - Click to sort Ascending	Sysplex Filter	System Filter	Case or Problem Number Filter	Tracking ID Filter	Notes Filter	Release Filter	Product Filter	Component Name Filter
<input type="checkbox"/> User Initiated	SHARC29 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:14:06 PM	SHARPLEX	S2				V2R5		
<input type="checkbox"/> User Initiated	SHARC28 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:13:59 PM	SHARPLEX	S2				V2R5		
<input type="checkbox"/> User Initiated	SHARC27 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:13:50 PM	SHARPLEX	S2				V2R5		
<input type="checkbox"/> User Initiated	SHARC26 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:13:42 PM	SHARPLEX	S2				V2R5		
<input type="checkbox"/> User Initiated	SHARC25 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:13:31 PM	SHARPLEX	S2				V2R5		
<input type="checkbox"/> User Initiated	SHARC24 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:13:20 PM	SHARPLEX	S2				V2R5		
<input type="checkbox"/> User Initiated	SHARC23 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:13:13 PM	SHARPLEX	S2				V2R5		
<input type="checkbox"/> User Initiated	SHARC22 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:12:55 PM	SHARPLEX	S2				V2R5		
<input type="checkbox"/> User Initiated	SHARC21 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:12:46 PM	SHARPLEX	S2				V2R5		
<input type="checkbox"/> User Initiated	SHARC20 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:12:36 PM	SHARPLEX	S2				V2R5		
<input type="checkbox"/> User Initiated	SHARC19 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:12:28 PM	SHARPLEX	S2				V2R5		
<input type="checkbox"/> User Initiated	SHARC18 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:12:19 PM	SHARPLEX	S2				V2R5		

Total: 33 Selected: 0

Refresh

Last refresh: Sep 30, 2022, 3:33:43 PM local time (Sep 30, 2022, 7:33:43 AM GMT)

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

Incident Log										
Actions ▾										
33 of 33 items shown. Clear filter										
Incident Type Filter	Description Filter	1 ↘ Date and Time (GMT) past "2000 days"	2 ↗ Sysplex Filter	System Filter	Case or Problem Number Filter	Tracking ID Filter	Notes Filter	Release Filter	Product Filter	Component Name Filter
User Initiated	INCIDENT LOG DEMO	Sep 16, 2022, 2:28:48 PM	SHARPLEX	S2				V2R5		
User Initiated	INCIDENT LOG DEMO2	Sep 16, 2022, 2:39:53 PM	SHARPLEX	S2				V2R5		
Manual Created	Manually created incident	Sep 23, 2022, 12:00:00 AM	SHARPLEX	S2		111	NOTES	V2R5		
User Initiated	SHARC01 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:08:59 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC02 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:09:09 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC03 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:09:41 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC04 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:09:47 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC05 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:09:55 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC06 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:10:09 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC07 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:10:16 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC08 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:10:23 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC09 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:10:30 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC10 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:10:53 PM	SHARPLEX	S2				V2R5		

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.

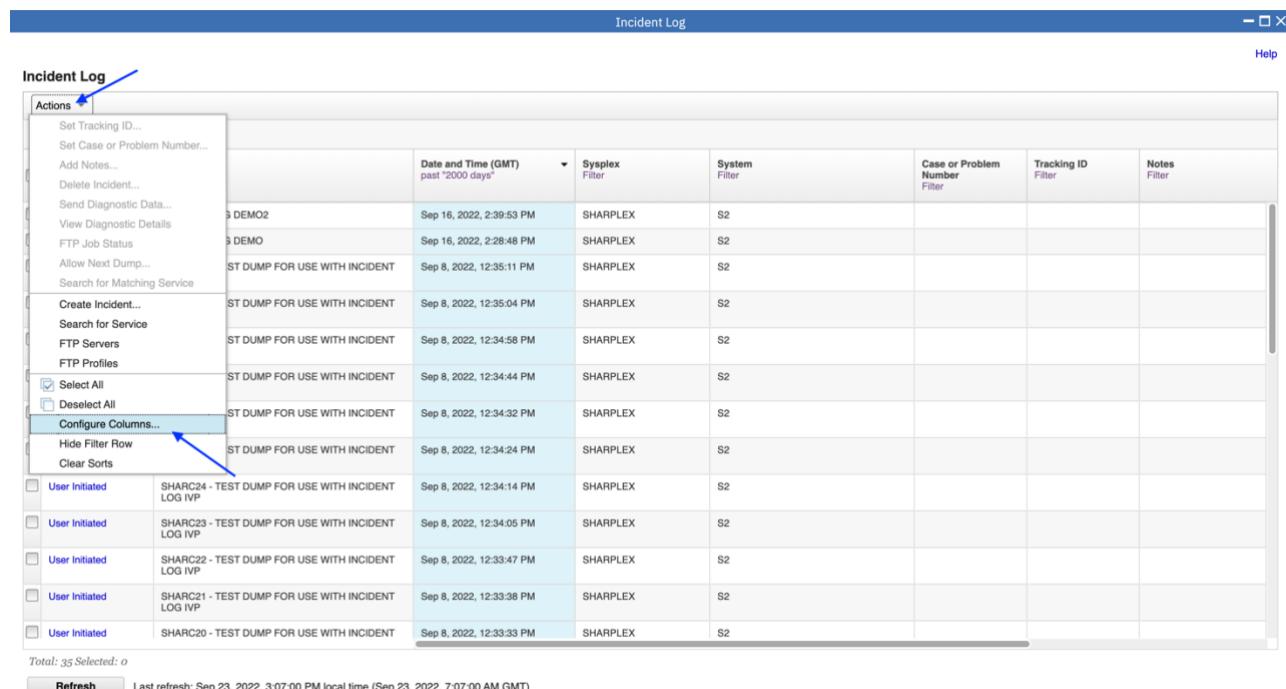
Incident Log										
Actions ▾										
33 of 33 items shown. Clear filter										
Incident Type Filter	Description Filter	2 ↗ Date and Time (GMT) past "2000 days"	1 ↘ Sysplex Filter	System Filter	Case or Problem Number Filter	Tracking ID Filter	Notes Filter	Release Filter	Product Filter	Component Name Filter
User Initiated	SHARC29 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:14:06 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC28 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:13:59 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC27 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:13:50 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC26 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:13:42 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC25 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:13:31 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC24 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:13:20 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC23 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:13:13 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC22 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:12:55 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC21 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:12:46 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC20 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:12:36 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC19 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:12:28 PM	SHARPLEX	S2				V2R5		
User Initiated	SHARC18 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:12:19 PM	SHARPLEX	S2				V2R5		

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.



The screenshot shows the 'Incident Log' interface. On the left, a sidebar titled 'Actions' is open, displaying various options: Set Tracking ID..., Set Case or Problem Number..., Add Notes..., Delete Incident..., Send Diagnostic Data..., View Diagnostic Details, FTP Job Status, Allow Next Dump..., Search for Matching Service, Create Incident..., Search for Service, FTP Servers, FTP Profiles, Select All, Deselect All, Configure Columns..., Hide Filter Row, Clear Sorts, User Initiated, SHARC24 - TEST DUMP FOR USE WITH INCIDENT LOG IVP, SHARC23 - TEST DUMP FOR USE WITH INCIDENT LOG IVP, SHARC22 - TEST DUMP FOR USE WITH INCIDENT LOG IVP, SHARC21 - TEST DUMP FOR USE WITH INCIDENT LOG IVP, and SHARC20 - TEST DUMP FOR USE WITH INCIDENT LOG IVP. The 'Configure Columns...' option is highlighted with a blue arrow. At the bottom of the sidebar, there is a note: 'Total: 35 Selected: 0'. Below the sidebar, a message says 'Last refresh: Sep 23, 2022, 3:07:00 PM local time (Sep 23, 2022, 7:07:00 AM GMT)'. The main area shows a table with columns: Date and Time (GMT) past "2000 days", Sysplex Filter, System Filter, Case or Problem Number Filter, Tracking ID Filter, and Notes Filter. The table contains several rows of incident data, such as 'ST DUMP FOR USE WITH INCIDENT' at Sep 8, 2022, 12:35:11 PM, and 'SHARC24 - TEST DUMP FOR USE WITH INCIDENT LOG IVP' at Sep 8, 2022, 12:34:14 PM.

2.Click “Sysplex”, then “< Remove”.

The screenshot shows the 'Incident Log' interface with a 'Configure Columns' dialog box overlaid. The 'Selected' list includes 'Description', 'Date and Time (GMT)', 'Sysplex', 'System', 'Case or Problem Number', 'Tracking ID', 'Notes', and 'Release'. The 'Sysplex' item is selected and highlighted with a blue border. A blue arrow points from the 'Selected' list to the '< Remove' button. Other items like 'Description' and 'Date and Time (GMT)' also have arrows pointing to their respective buttons.

3.Click “System”, then “< Remove”.

The screenshot shows the 'Incident Log' interface with a 'Configure Columns' dialog box overlaid. The 'Selected' list includes 'Description', 'Date and Time (GMT)', 'System', 'Case or Problem Number', 'Tracking ID', 'Notes', 'Release', and 'Product'. The 'System' item is selected and highlighted with a blue border. A blue arrow points from the 'Selected' list to the '< Remove' button. Other items like 'Description' and 'Date and Time (GMT)' also have arrows pointing to their respective buttons.

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.

The screenshot shows a table titled "Incident Log" with the following data:

Actions	Incident Type Filter	Description Filter	Date and Time (GMT) past "2000 days"	Component Name Filter	Case or Problem Number Filter	Tracking ID Filter	Notes Filter	R Filter	P Filter	Component ID Filter
			Sep 16, 2022, 2:39:53 PM					V2		
	User Initiated	INCIDENT LOG DEMO2	Sep 16, 2022, 2:28:48 PM					V2		
	User Initiated	INCIDENT LOG DEMO	Sep 8, 2022, 12:35:11 PM					V2		
	User Initiated	SHARC30 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:35:04 PM					V2		
	User Initiated	SHARC29 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:34:58 PM					V2		
	User Initiated	SHARC28 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:34:44 PM					V2		
	User Initiated	SHARC27 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:34:32 PM					V2		
	User Initiated	SHARC25 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:34:24 PM					V2		
	User Initiated	SHARC24 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:34:14 PM					V2		
	User Initiated	SHARC23 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:34:05 PM					V2		
	User Initiated	SHARC22 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:33:47 PM					V2		
	User Initiated	SHARC21 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:33:38 PM					V2		
	User Initiated	SHARC20 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:33:33 PM					V2		

Total: 35 Selected: 0

Refresh

Last refresh: Sep 23, 2022, 3:07:00 PM local time (Sep 23, 2022, 7:07:00 AM GMT)

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.

Incident Log								
Actions ▾								
35 of 35 items shown. Clear filter								
<input type="checkbox"/> Incident Type Filter	Description Filter	Date and Time (GMT) past "2000 days"	Component Name Filter	Case or Problem Number Filter	Tracking ID Filter	Notes Filter	R F	P F Component ID Filter
<input type="checkbox"/> User Initiated	INCIDENT LOG DEMO2	Sep 16, 2022, 2:39:53 PM					V2	
<input type="checkbox"/> User Initiated	INCIDENT LOG DEMO	Sep 16, 2022, 2:28:48 PM					V2	
<input type="checkbox"/> User Initiated	SHARC30 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:35:11 PM					V2	
<input type="checkbox"/> User Initiated	SHARC29 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:35:04 PM					V2	
<input type="checkbox"/> User Initiated	SHARC28 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:34:58 PM					V2	
<input type="checkbox"/> User Initiated	SHARC27 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:34:44 PM					V2	
<input type="checkbox"/> User Initiated	SHARC26 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:34:32 PM					V2	
<input type="checkbox"/> User Initiated	SHARC25 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:34:24 PM					V2	
<input type="checkbox"/> User Initiated	SHARC24 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:34:14 PM					V2	
<input type="checkbox"/> User Initiated	SHARC23 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:34:05 PM					V2	
<input type="checkbox"/> User Initiated	SHARC22 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:33:47 PM					V2	
<input type="checkbox"/> User Initiated	SHARC21 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:33:38 PM					V2	
<input type="checkbox"/> User Initiated	SHARC20 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:33:33 PM					V2	

Total: 35 Selected: 0

Refresh Last refresh: Sep 23, 2022, 3:07:00 PM local time (Sep 23, 2022, 7:07:00 AM GMT)

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

Then click Filter.

Incident Log

Actions ▾ 35 of 35 items shown. Clear filter

Incident Type Filter	Description Filter	Date and Time (GMT) Filter	Component Name Filter	Case or Problem Number Filter	Tracking ID Filter	Notes Filter	R F	P F	Component ID Filter
User Initiated	INCIDENT LOG DEMO2	past "2000 days"					V2		
User Initiated	INCIDENT LOG DEMO						V2		
User Initiated	SHARC20 - TEST DUMP FOR U LOG IVP						V2		
User Initiated	SHARC29 - TEST DUMP FOR U LOG IVP						V2		
User Initiated	SHARC28 - TEST DUMP FOR U LOG IVP						V2		
User Initiated	SHARC27 - TEST DUMP FOR U LOG IVP						V2		
User Initiated	SHARC26 - TEST DUMP FOR U LOG IVP						V2		
User Initiated	SHARC25 - TEST DUMP FOR U LOG IVP						V2		
User Initiated	SHARC24 - TEST DUMP FOR U LOG IVP						V2		
User Initiated	SHARC23 - TEST DUMP FOR U LOG IVP						V2		
User Initiated	SHARC22 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:33:47 PM					V2		
User Initiated	SHARC21 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:33:38 PM					V2		
User Initiated	SHARC20 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:33:33 PM					V2		

Total: 35 Selected: 0

Refresh Last refresh: Sep 23, 2022, 3:07:00 PM local time (Sep 23, 2022, 7:07:00 AM GMT)

Build Filter

Match All rules Match case

Rules

Date and Time (GMT) past 2,000 days Description contains SHARC05

Filter Restore Clear Close

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”.

The screenshot shows a web-based 'Incident Log' application. At the top, there's a header bar with tabs for 'Incident Log' (selected), 'Help', and other options. Below the header is a search/filter section with dropdowns for 'Actions', 'Description', 'Date and Time (GMT)', 'Component Name', 'Case or Problem Number', 'Tracking ID', 'Notes', and 'Component ID'. There are also 'Re Filter', 'Pr Filter', and 'Component ID Filter' buttons. The main area is a table titled 'Incident Log' with the following columns: Incident Type, Description, Date and Time (GMT), Component Name, Case or Problem Number, Tracking ID, Notes, Re Filter, Pr Filter, and Component ID. One row is highlighted in light blue, and the 'User Initiated' link in the first column of this row is highlighted with a blue arrow pointing to it. The table has a total of 35 items shown. At the bottom left, there's a 'Refresh' button and a note about the last refresh time: 'Last refresh: Sep 23, 2022, 3:19:41 PM local time (Sep 23, 2022, 7:19:41 AM GMT)'.

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.

The screenshot shows the 'Incident Log' interface with the 'View Diagnostic Details' tab selected. At the top, there are tabs for 'General' and 'Diagnostic Data', with 'Diagnostic Data' being the active one. Below the tabs is a table titled 'Diagnostic Data' with four columns: 'Data Type', 'Source', 'Sysplex', and 'System'. The table contains four rows of data:

Data Type	Source	Sysplex	System
SVC dump	SDUMP.D220929.T080955.S2.S00043	SHARPLEX	S2
Error log	CEA.R00.DC2E00A1.EBC77B27.X00.VEW	SHARPLEX	S2
Operations log	CEA.Y00.DC2E00A1.EBC77B27.X00.VEW	SHARPLEX	S2

Total: 4 Selected: 0

You can attach up to ten additional files to send with this incident. When you close the panel, the Attachments table is not cleared.

Attachments

Actions

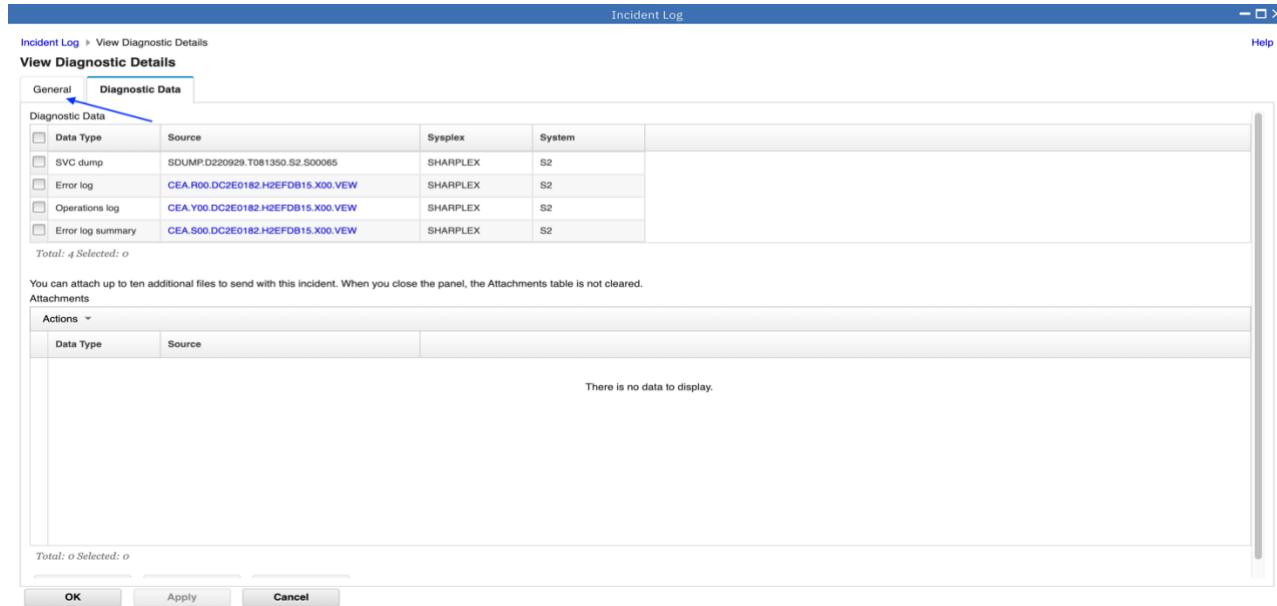
Total: 0 Selected: 0

OK Apply Cancel

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.

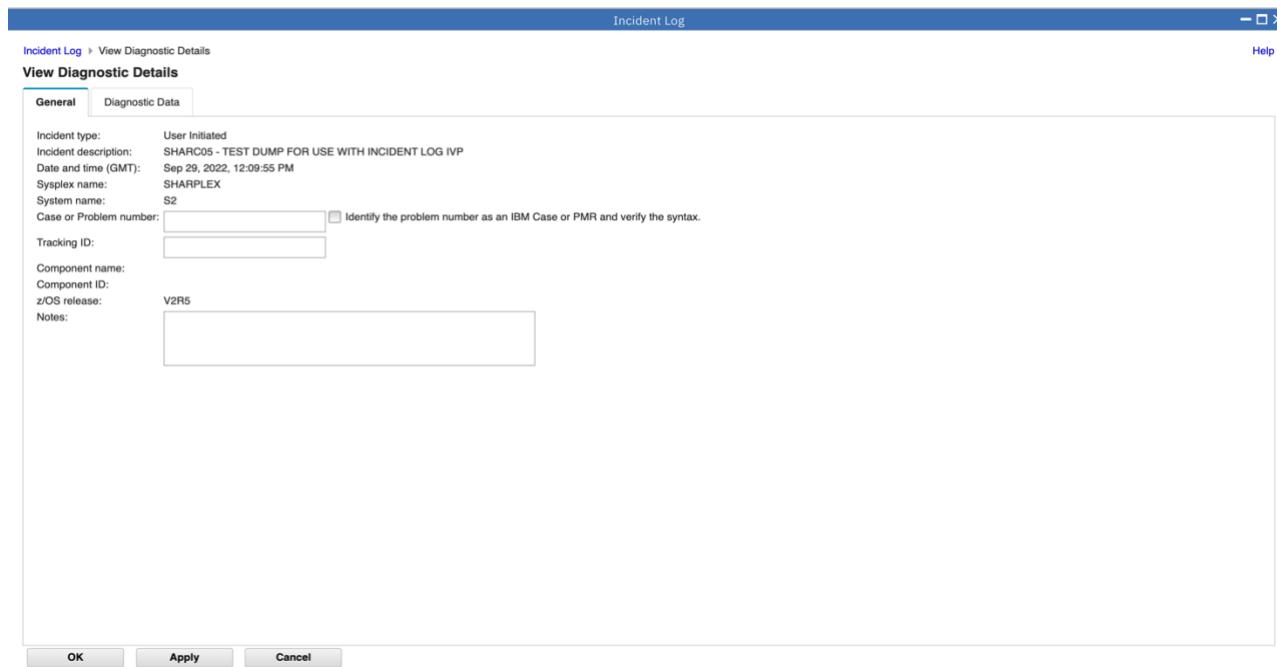
Click on the General Tab.



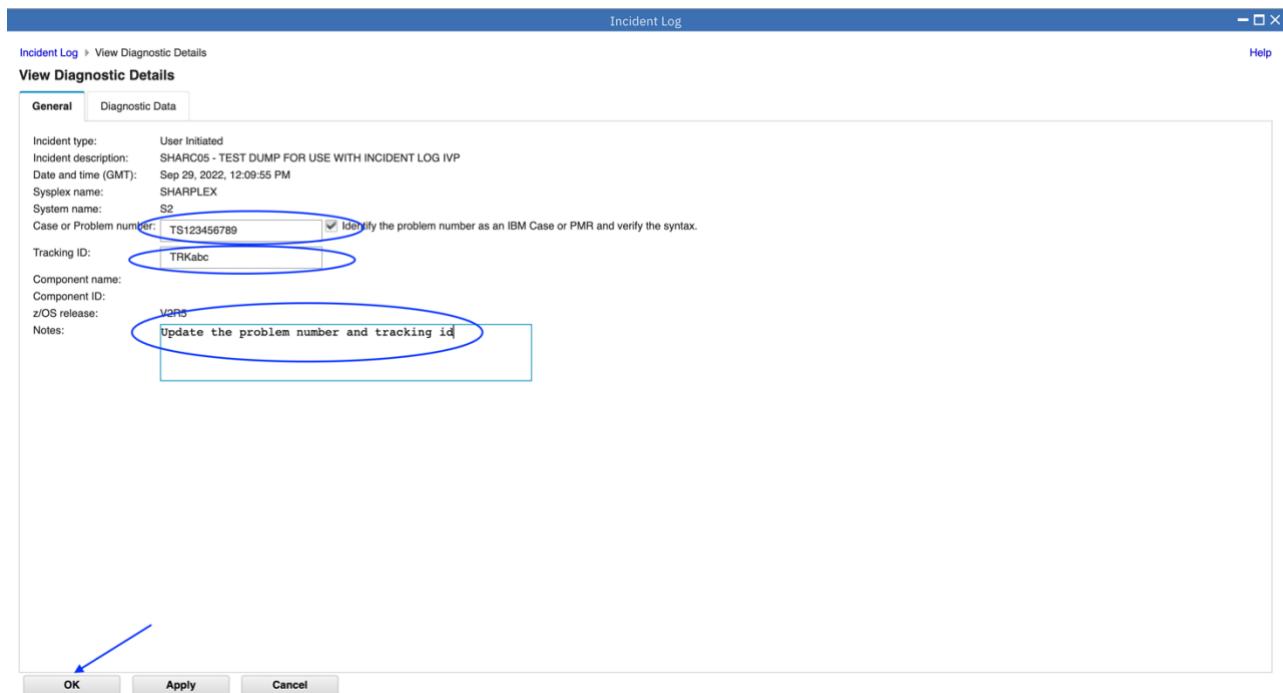
Step 4c: Update the Incident

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.

Incident Log

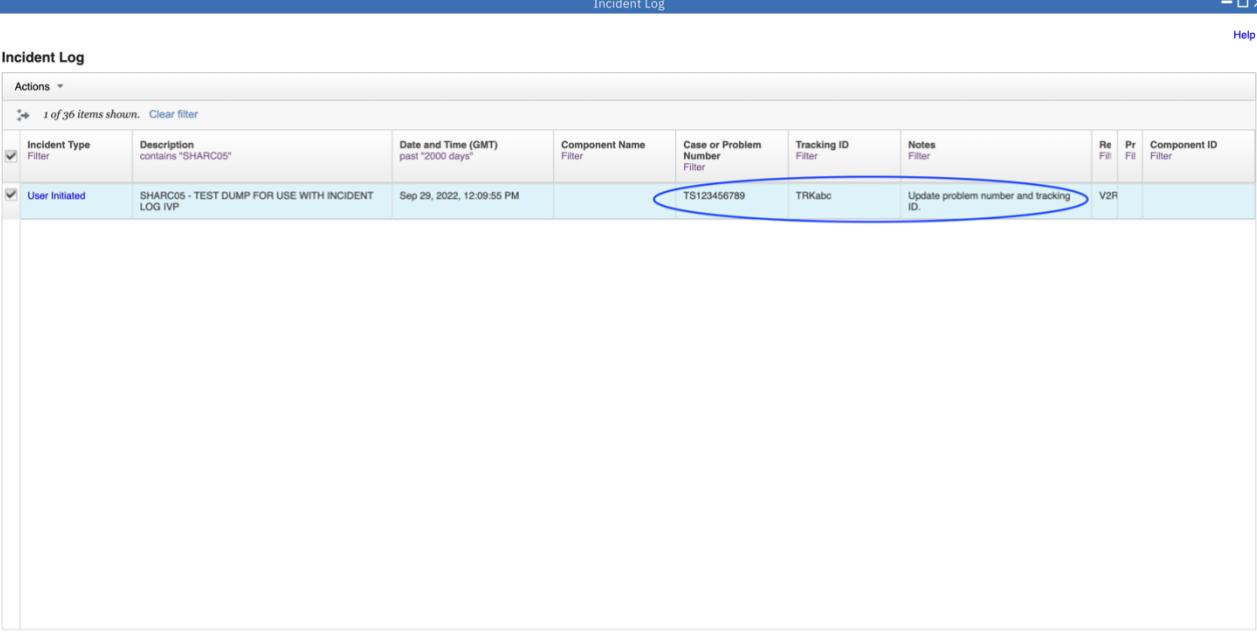
Actions ▾

1 of 36 items shown. Clear filter

<input checked="" type="checkbox"/> Incident Type Filter	Description contains "SHARC05"	Date and Time (GMT) past "2000 days"	Component Name Filter	Case or Problem Number Filter	Tracking ID Filter	Notes Filter	Re Fil	Pr Fil	Component ID Filter
<input checked="" type="checkbox"/> User Initiated	SHARC05 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:09:55 PM		TS123456789	TRKabc	Update problem number and tracking ID.	V2R		

Total: 1 Selected: 1

Refresh Last refresh: Jul 26, 2023, 3:31:02 PM local time (Jul 26, 2023, 7:31:02 AM GMT)



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.

The screenshot shows the 'Incident Log' interface. At the top, there's a header bar with 'Incident Log' and standard window controls. Below the header is a table with columns: Component Name, Date and Time (GMT), Case or Problem Number Filter, Tracking ID Filter, Notes Filter, Re Fil, Pr Fil, and Component ID Filter. A single row is visible in the table. On the left side, there's a sidebar titled 'Actions' which contains several options: Set Tracking ID..., Set Case or Problem Number..., Add Notes..., Delete Incident..., Send Diagnostic Data..., View Diagnostic Details (which is highlighted with a blue arrow), FTP Job Status, Allow Next Dump..., Search for Matching Service, Create Incident..., Search for Service, FTP Servers, and FTP Profiles. At the bottom of the sidebar, there are checkboxes for 'Select All' and 'Deselect All', along with links for 'Configure Columns...', 'Hide Filter Row', and 'Clear Sorts'. At the very bottom of the interface, there's a status bar with 'Total: 1 Selected: 1', a 'Refresh' button, and a timestamp: 'Last refresh: Sep 30, 2022, 3:58:41 PM local time (Sep 30, 2022, 7:58:41 AM GMT)'.

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.

Data Type	Source	Sysplex	System
SVC dump	SDUMP.D220929.T080955.S2.S00043	SHARPLEX	S2
Error log	CEA.R00.DC2E00A1.EBC77B27.X00.VEW	SHARPLEX	S2
Operations log	CEA.Y00.DC2E00A1.EBC77B27.X00.VEW	SHARPLEX	S2
Error log summary	CEA.S00.DC2E00A1.EBC77B27.X00.VEW	SHARPLEX	S2

Total: 4 Selected: 0

You can attach up to ten additional files to send with this incident. When you close the panel, the Attachments table is not cleared.

Attachments

Actions

Data Type Source

There is no data to display.

OK Apply Cancel

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

Incident Log > View Diagnostic Details

View Diagnostic Details

General Diagnostic Data

Diagnostic Data

Data Type	Source	Sysplex	System
SVC dump	SDUMP.D220929.T081320.S2.S00062	SHARPLEX	S2
Error log	CEA.R00.DC2E0165.I9F2BB12.X00.VEW	SHARPLEX	S2
<input checked="" type="checkbox"/> Operations log	CEA.Y00.DC2E0165.I9F2BB12.X00.VEW	SHARPLEX	S2
Error log summary	CEA.S00.DC2E0165.I9F2BB12.X00.VEW	SHARPLEX	S2

Total: 4 Selected: 1

You can attach up to ten additional files to send with this incident.

Attachments

Actions

Data Type Source

Select Handler

Multiple handlers can process your request. Select the handler you want to use.
If one handler is preferred over another, z/OSMF administrators can change the default handler, or disable a handler in the Application Linking Manager task.

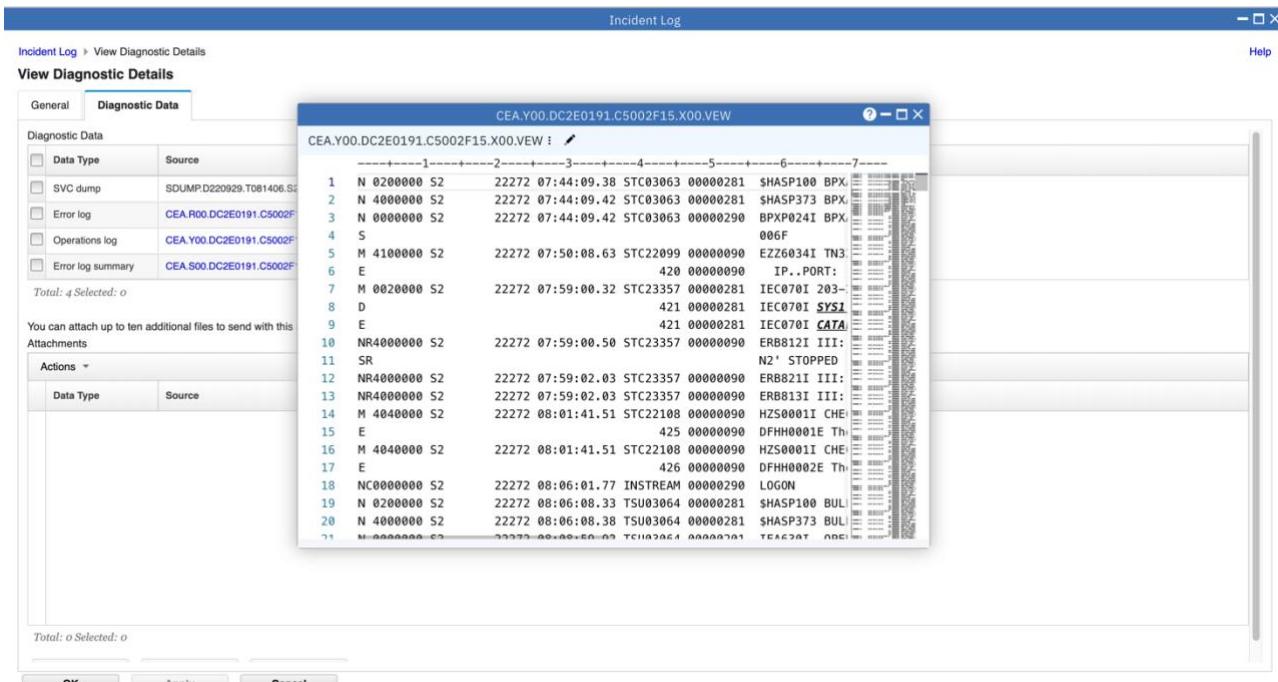
Link to The z/OSMF Desktop Editor

Cancel OK

There is no data to display.

OK Apply Cancel

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.

The screenshot shows the 'View Diagnostic Details' panel within the 'Incident Log' application. The 'Diagnostic Data' tab is selected. A table displays four rows of diagnostic data:

Data Type	Source	Sysplex	System
SVC dump	SDUMP.D220929.1080955.S2.500043	SHARPLEX	S2
Error log	CEA.R00.DC2E00A1.EBC77B27.X00.VEW	SHARPLEX	S2
Operations log	CEA.V00.DC2E00A1.EBC77B27.X00.VEW	SHARPLEX	S2

Total: 4 Selected: 0

You can attach up to ten additional files to send with this incident. When you close the panel, the Attachments table is not cleared.

Attachments

Actions

Total: 0 Selected: 0

Send **View Status** **View Log**

OK **Apply** **Cancel**

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

The screenshot shows the 'Incident Log' table. A context menu is open over the first row, which has 'User Initiated' selected. The menu options include:

- Set Tracking ID...
- Set Case or Problem Number...
- Add Notes...
- Delete Incident...
- Send Diagnostic Data...** (highlighted with a blue arrow)
- View Diagnostic Details
- FTP Job Status
- Allow Next Dump...
- Search for Matching Service

Total: 1 Selected: 1

Refresh Last refresh: Sep 23, 2022, 3:27:55 PM local time (Sep 23, 2022, 7:27:55 AM GMT)

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.

Incident Log

Incident Log > Send Diagnostic Data

Send Diagnostic Data

Welcome

Use this wizard to prepare and send diagnostic data to an FTP server. To begin, review the selected diagnostic data and enter a Case or Problem Number.

Incident

Incident Type	Description	Date and Time (GMT)
User Initiated	SHARC05 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 29, 2022, 12:09:55 PM

Diagnostic Data to Send

Data Type	System
Error log	S2
Operations log	S2
Error log summary	S2

* Case or Problem number: Identify the problem number as an IBM Case or PMR and verify the syntax.

< Back **Next >** Finish Cancel

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.

Incident Log > Send Diagnostic Data

Send Diagnostic Data

Select FTP Server

Select the FTP server to which you want to send the diagnostic data files.

Actions ▾

No filter applied

Name Filter	Activity Filter	Host Filter	Path Name Filter	Port Number Filter	Description Filter	Transf Filter
<input checked="" type="radio"/> IBM-ecurep-mvs-pduu-https		www.secure.ecurep.ibm.com	/t0ibm/mvs			PDUU
<input type="radio"/> IBM-ecurep-mvs-sftp		sftp.ecurep.ibm.com	/t0ibm/mvs			SFTP
<input type="radio"/> IBM-ecurep-tivoli-pduu-https		www.secure.ecurep.ibm.com	/t0ibm/tivoli			PDUU
<input type="radio"/> IBM-ecurep-tivoli-sftp		sftp.ecurep.ibm.com	/t0ibm/tivoli			SFTP
<input type="radio"/> IBM-testcase-mvs-pduu-https		testcase.boulder.ibm.com	/t0ibm/mvs			PDUU
<input type="radio"/> IBM-testcase-mvs-sftp		testcase.boulder.ibm.com	/t0ibm/mvs			SFTP
<input type="radio"/> IBM-testcase-tivoli-pduu-https		testcase.boulder.ibm.com	/t0ibm/tivoli			PDUU
<input type="radio"/> IBM-testcase-tivoli-sftp		testcase.boulder.ibm.com	/t0ibm/tivoli			SFTP

Total: 8 Selected: 1

Last refresh: Jul 26, 2023, 3:48:43 PM local time (Jul 26, 2023, 7:48:43 AM GMT)

< Back Next > Finish Cancel

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.

Incident Log > Send Diagnostic Data

Send Diagnostic Data

- ✓ Welcome
- ✓ Select FTP Server
- Specify Security Settings**
- ✓ Select FTP Profile
- Define Job Settings
- Review FTP Information

Specify Security Settings

If the FTP server requires logging in with a user ID and password, select *Specify a user ID and password* to enter these values. For transmissions to IBM, enter a cipher key to encrypt the data and add the key to the PMR so that IBM can decrypt it. For UNIX files, encryption and parallel FTP are not supported.

Use anonymous user ID and password
 Specify a user ID and password

* User ID: ibmuser
* Password: ****

Cipher key:

* Https key ring: *AUTH*/*

< Back **Next >** Finish Cancel

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.

Incident Log > Send Diagnostic Data

Send Diagnostic Data

- ✓ Welcome
- ✓ Select FTP Server
- ✓ Specify Security Settings
- Select FTP Profile**
- Define Job Settings
- Review FTP Information

Select FTP Profile

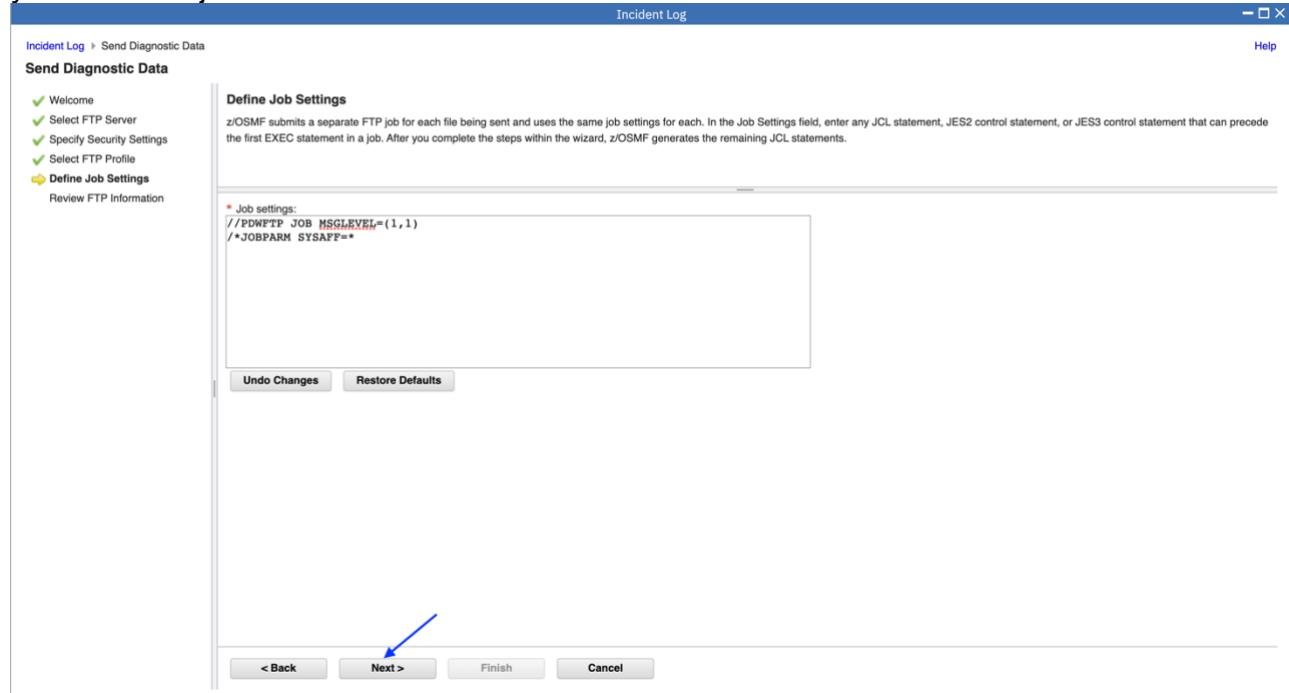
Select the profile that specifies the settings required to transfer data across your company's firewall or proxy, or select the **No Firewall or Proxy** profile.

* FTP profile: **No Firewall or Proxy**

< Back **Next >** Finish Cancel

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.

Incident Log

Send Diagnostic Data

Review FTP Information

Review the FTP information. To make changes, return to the appropriate panel by clicking **Back**. When you are ready to send the data, click **Finish**.

Diagnostic Data:

SVC dump	SHARPLEX S2
Error log	SHARPLEX S2
Operations log	SHARPLEX S2
Error log summary	SHARPLEX S2

Case or Problem number: 12345,123,123 Is IBM Case or PMR number

FTP server:

Name:	IBM-eurep-mvs-pduu-https
Host:	www.secure.eurep.ibm.com
Path name:	/t0ibm/mvs
Port number:	

Transfer method: z/OS Problem Documentation Upload Utility with HTTPS(PDUU with HTTPS)

Security settings:

User ID:	ibmuser
Password:	*****
Https key ring:	*AUTH*

FTP profile:

Name:	No Firewall or Proxy
Firewall host:	
Firewall port:	

View JCL **Edit JCL**

< Back Next > **Finish** Cancel

7. After reviewing each tab, click Close.

Incident Log

Send Diagnostic Data

View JCL

SVC dump Error log Operations log Error log summary

Data Type	Sysplex	System
SVC dump	SHARPLEX	S2

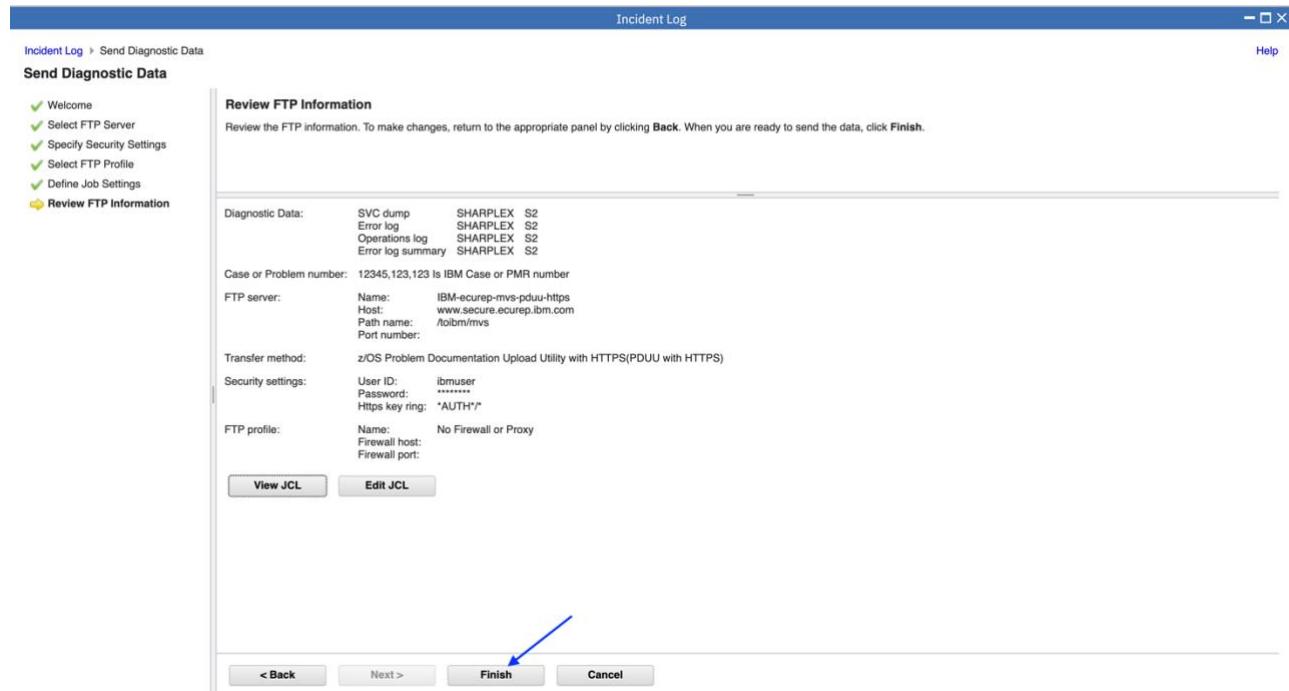
```

//P0WPTP JOB MSGLEVEL=1,1
//&JOBPARM SYSAFF=*
//*
//& COPY CLIST TO TEMP PDS
//*
//STEP0010 EXEC PGM=IEBRGENER,REGION=50M
//SYSIN DD DUMMY
//SYSUT2 DD DSN=6&PDS(PDW),UNIT=SYSSALLDA,DISP=(NEW,PASS),
//  SPACE=(TRK,(1,1,1)),DCB=(LRECL=80,BLKSIZE=3120,RECFM=FB,DSORG=PO)
//SYSUT1 DD *
PROC 1 FN
CONTROL LIST ASIS NOFLUSH
ERROR DD
  SET RC=&LASTCC
  RETURN
END
IF &FN = 1 THEN DO
  OCOPY INDD(INPUT1) OUTDD(HFSOUT1) BINARY TO1047
  OCOPY INDD(INPUT1) OUTDD(STDOUT)
  OCOPY INDD(INPUT2) OUTDD(HFSOUT2) TO1047
  IF &MAXCC > 0 THEN DO
    WRITE Setup failed.
    EXIT CODE(10)
  END
  ELSE EXIT CODE(0)
END
IF &FN = 2 THEN DO
  WRITE Program wbemexec was not found.
  EXIT CODE(10)

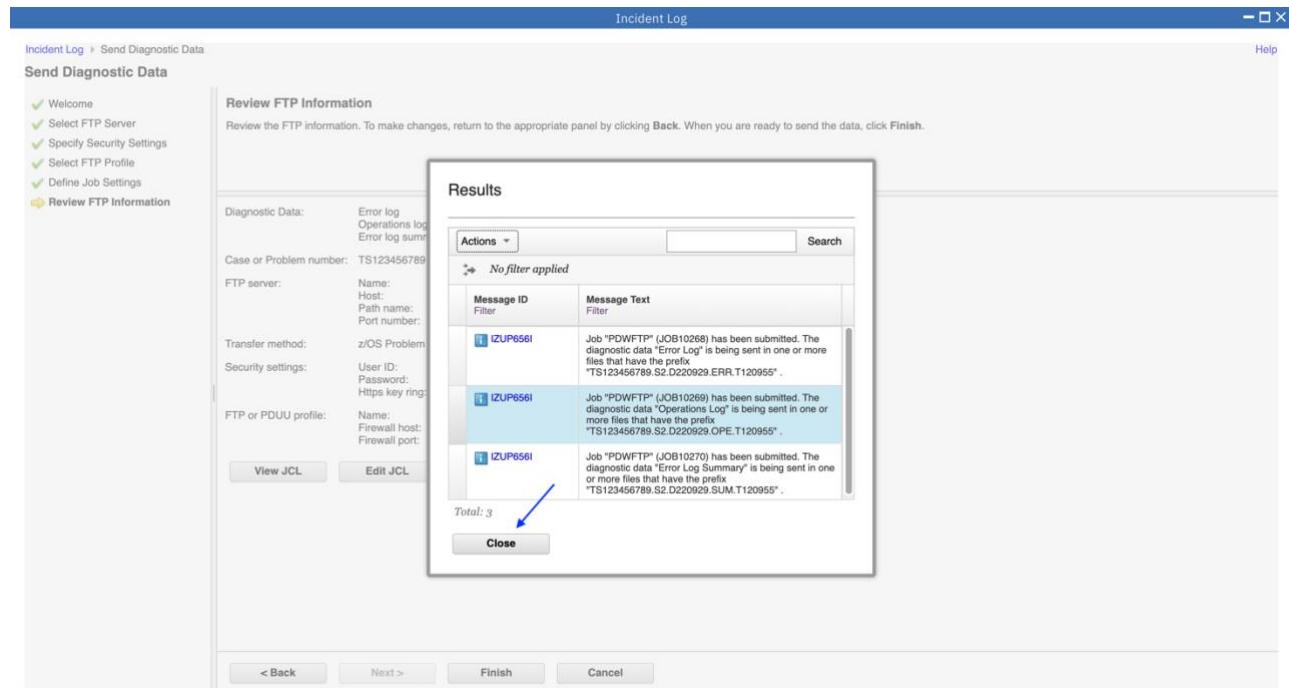
```

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

The screenshot shows the 'Incident Log' interface with a single item selected: 'SHARC05 - TEST DUMP FOR USE WITH INCIDENT LOG.IVP'. A context menu is open over this item, with the 'FTP Job Status' option highlighted and a blue arrow pointing to it. The menu also includes other options like 'Set Tracking ID...', 'Set Case or Problem Number...', 'Add Notes...', 'Delete Incident...', 'Send Diagnostic Data...', 'View Diagnostic Details', 'Allow Next Dump...', and 'Search for Matching Service'.

Actions	Description	Date and Time (GMT)	Component Name	Case or Problem Number	Tracking ID	Notes	Re	Pr	Component ID	
<input checked="" type="checkbox"/> Incident Type Filter	Description contains "SHARC05"	past "2000 days"	Date and Time (GMT) Filter	Component Name Filter	Case or Problem Number Filter	Tracking ID Filter	Notes Filter	Re Filter	Pr Filter	Component ID Filter
<input checked="" type="checkbox"/> User Initiated	SHARC05 - TEST DUMP FOR USE WITH INCIDENT LOG.IVP	Sep 29, 2022, 12:09:55 PM		TS123456789	TRKabc	Update problem number and tracking ID.	V2R			

Total: 1 Selected: 1

Refresh Last refresh: Jul 26, 2023, 3:55:36 PM local time (Jul 26, 2023, 7:55:36 AM GMT)

- 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.

The screenshot shows the 'FTP Job Status' details view for the selected incident. It displays three rows of job information, each with a circled 'Status' column showing 'Failed'. The columns include 'Incident Type', 'Description', 'Date and Time (GMT)', 'FTP Server Host', 'FTP Server Path', 'Start Time (GMT)', 'User ID', and 'Job ID'.

Incident Type	Description	Date and Time (GMT)	FTP Server Host	FTP Server Path	Start Time (GMT)	User ID	Job ID
User Initiated	SHARC05 - TEST DUMP FOR USE WITH INCIDENT LOG.IVP	Sep 29, 2022, 12:09:55 PM	www.secure.ecurep.ibm.com	/0ibm/mvs	Jul 26, 2023, 7:53:38 AM	SHARC05	JC
Operations log	CEA.Y00.DC2E00A1.EBC77B27.X00.VEW		www.secure.ecurep.ibm.com	/0ibm/mvs	Jul 26, 2023, 7:53:38 AM	SHARC05	JC
Error log	CEA.R00.DC2E00A1.EBC77B27.X00.VEW		www.secure.ecurep.ibm.com	/0ibm/mvs	Jul 26, 2023, 7:53:38 AM	SHARC05	JC

Total: 3 Selected: 0

Refresh Last refresh: Jul 26, 2023, 3:59:05 PM local time (Jul 26, 2023, 7:59:05 AM GMT)

Close

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.

The screenshot shows the 'Incident Log' interface. On the left, a sidebar contains a 'Actions' dropdown menu with various options like 'Set Tracking ID...', 'Create Incident...', and 'Search for Service'. The 'Create Incident...' option is highlighted with a blue arrow. The main pane displays a table of incidents with columns for Component Name, Case or Problem Number, Tracking ID, Notes, Release, Priority, and Component ID. One row is selected, showing details: Component Name is 'TRKabc', Case or Problem Number is '12345,123,123', Tracking ID is 'V2R', Notes is 'Update the problem number and tracking ID.', Release is 'V2R', Priority is '2', and Component ID is '222'. At the bottom, there are buttons for 'Refresh' and 'Last refresh: Sep 23, 2022, 3:27:55 PM local time (Sep 23, 2022, 7:27:55 AM GMT)'.

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;

Incident Log > Create Incident

Create Incident

Description:
Manually created incident

System name(sysplex.system):
SHARPLEX.S2

Date and Time(GMT):
9/23/2022 12:00 AM

Dump data set name:

z/OS release:
V2R5

Tracking ID:
111

Case or PMR number:

Identify the problem number as an IBM Case or PMR and verify the syntax.

Abend code:
U0999

Component ID:
222

CSECT:
333

Load module:
444

Notes:
NOTES

Create **Cancel**

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.

Incident Log

Actions ▾

36 of 36 items shown. Clear filter

Incident Type Filter	Description Filter	Date and Time (GMT) past "2000 days"	Component Name Filter	Case or Problem Number Filter	Tracking ID Filter	Notes Filter	R F	P F	Component ID Filter
<input checked="" type="checkbox"/>	Manual Created	Sep 23, 2022, 12:00:00 AM			111	NOTES	V2	222	
<input type="checkbox"/>	User Initiated	Sep 16, 2022, 2:39:53 PM					V2		
<input type="checkbox"/>	User Initiated	Sep 16, 2022, 2:28:48 PM					V2		
<input type="checkbox"/>	User Initiated	Sep 8, 2022, 12:35:11 PM					V2		
<input type="checkbox"/>	User Initiated	Sep 8, 2022, 12:35:04 PM					V2		
<input type="checkbox"/>	User Initiated	Sep 8, 2022, 12:34:58 PM					V2		
<input type="checkbox"/>	User Initiated	Sep 8, 2022, 12:34:44 PM					V2		
<input type="checkbox"/>	User Initiated	Sep 8, 2022, 12:34:32 PM					V2		
<input type="checkbox"/>	User Initiated	Sep 8, 2022, 12:34:24 PM					V2		
<input type="checkbox"/>	User Initiated	Sep 8, 2022, 12:34:14 PM					V2		
<input type="checkbox"/>	User Initiated	Sep 8, 2022, 12:34:05 PM					V2		
<input type="checkbox"/>	User Initiated	Sep 8, 2022, 12:33:47 PM					V2		
<input type="checkbox"/>	User Initiated	Sep 8, 2022, 12:33:38 PM					V2		

Total: 36 Selected: 0

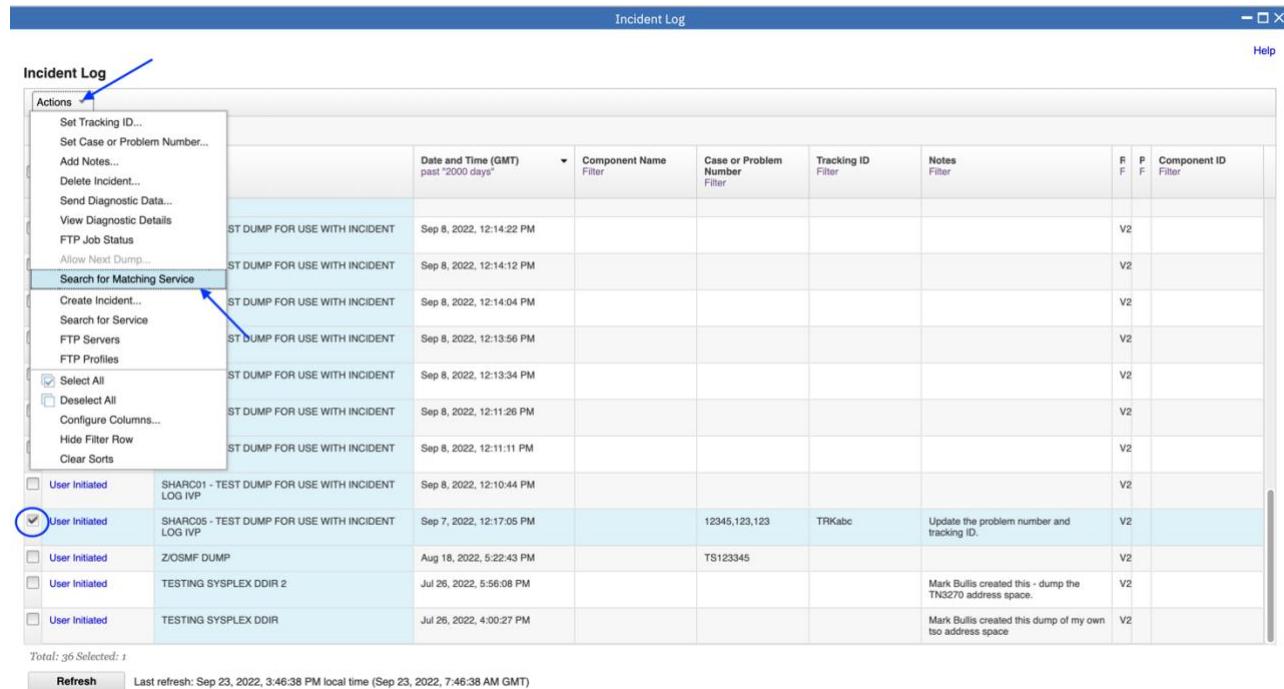
Refresh Last refresh: Sep 23, 2022, 3:46:38 PM local time (Sep 23, 2022, 7:46:38 AM GMT)

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

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



The screenshot shows the Incident Log application window. On the left, there is a sidebar with various actions like Set Tracking ID, Set Case or Problem Number, Add Notes, Delete Incident, Send Diagnostic Data, View Diagnostic Details, FTP Job Status, Allow Next Dump, and a prominent 'Search for Matching Service' option which is highlighted with a blue arrow. Below this is a list of incidents. One incident, 'SHARC05 - TEST DUMP FOR USE WITH INCIDENT LOG IVP', has a checkmark next to it and is also highlighted with a blue circle. At the bottom, there is a 'Refresh' button and a status message: 'Last refresh: Sep 23, 2022, 3:46:38 PM local time (Sep 23, 2022, 7:46:38 AM GMT)'.

	Date and Time (GMT) past "2000 days"	Component Name Filter	Case or Problem Number Filter	Tracking ID Filter	Notes Filter	F F	P F	Component ID Filter
ST DUMP FOR USE WITH INCIDENT	Sep 8, 2022, 12:14:22 PM					V2		
ST DUMP FOR USE WITH INCIDENT	Sep 8, 2022, 12:14:12 PM					V2		
ST DUMP FOR USE WITH INCIDENT	Sep 8, 2022, 12:14:04 PM					V2		
ST DUMP FOR USE WITH INCIDENT	Sep 8, 2022, 12:13:56 PM					V2		
ST DUMP FOR USE WITH INCIDENT	Sep 8, 2022, 12:13:34 PM					V2		
ST DUMP FOR USE WITH INCIDENT	Sep 8, 2022, 12:11:26 PM					V2		
ST DUMP FOR USE WITH INCIDENT	Sep 8, 2022, 12:11:11 PM					V2		
SHARC01 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 8, 2022, 12:10:44 PM					V2		
SHARC05 - TEST DUMP FOR USE WITH INCIDENT LOG IVP	Sep 7, 2022, 12:17:05 PM	12345,123,123	TRKabc	Update the problem number and tracking ID.		V2		
ZOSMF DUMP	Aug 18, 2022, 5:22:43 PM	TS123345				V2		
TESTING SYSPLEX DDIR 2	Jul 26, 2022, 5:56:00 PM				Mark Bullis created this - dump the TN3270 address space.	V2		
TESTING SYSPLEX DDIR	Jul 26, 2022, 4:00:27 PM				Mark Bullis created this dump of my own tso address space	V2		

Total: 36 Selected: 1

Refresh Last refresh: Sep 23, 2022, 3:46:38 PM local time (Sep 23, 2022, 7:46:38 AM GMT)

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.

The screenshot shows the 'Search for Matching Service' page with the 'Quick Searches' tab selected. At the top, there is a header bar with 'Incident Log' and 'Help' buttons. Below the header, the URL is listed as <http://www-01.ibm.com/support/search.wss?q=&tc=SG004FV+SWG90&dc=DB550&dtm>. There are dropdown menus for 'Results to display per page' (set to 20) and 'Sorts' (set to 'Relevance'). Below these, there are two tabs: 'Quick Searches' (selected) and 'Search Builder'. Under the 'Quick Searches' tab, there are three sections: 'Search Component ID' (Incident does not contain component ID), 'Search Release and Product IDs' (<http://www-01.ibm.com/support/search.wss?q=V2R5&tc=SG004FV+SWG90&dc=DB550&dtm&sortby=asc&hpp=20>), and 'Search Program in Error' (Incident does not contain Load Module). A blue oval highlights the 'Search Release and Product IDs' section.

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.

The screenshot shows the IBM Support website with the search term 'V2R5' entered in the search bar. The results page displays 1 - 10 of 438 results. The first few results are:

- PH38243: V2R5 ROLLUP APAR**
3 September 2021
V2R5 Rollup APAR
Search result URL: <https://www.ibm.com/support/pages/apar/PH38243>
- PH39851: ROLLBACK FROM V2R5**
10 December 2021
This is a rollback APAR from **V2R5** for z/OS data set and file REST service.
Search result URL: <https://www.ibm.com/support/pages/apar/PH39851>
- OA61409: IBM Z OMEGAMON NETWORK MONITOR WILL NOT INITIALIZE ON Z/OS V2R5**
4 June 2021
IBM Z OMEGAMON Network Monitor will not initialize on z/OS **V2R5** because it is not recognizing the **V2R5** VTAM level.
Search result URL: <https://www.ibm.com/support/pages/apar/OA61409>
- OA61452: DFMSHSHM ROLL UP OF PRE RELEASE APARS INTO R250.**
<https://www.ibm.com/mysupport/>

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.

Incident Log > Search for Matching Service

Help

Search for Matching Service

*Default Search provider URL:
http://www-01.ibm.com/support/search.wss?q=&tc=SG004FV+SWG90&dc=DB550&dtn

Results to display per page(20/50/100):
20

Sorts:
Relevance

Quick Searches Search Builder

Search terms:

Component name:
 Component ID:
 z/OS release:V2R5
 Product:
 Symptom string:

Additional terms:

Clear Additional terms

Generated Search for Service

Open Search in New Browser Window or Tab
http://www-01.ibm.com/support/search.wss?q=V2R5&tc=SG004FV+SWG90&dc=DB550&dtn&sortby=asc&hpp=20

Close

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

IBM

Support Downloads Documentation Forums Cases Monitoring Manage support account

IBM Support

V2R5

1 - 20 of 298 results [Next >](#)

[OW21022: ABENDOC4 DURING UNCONDITIONAL LOGOFF BECAUSE IKTLTERM IS RUNNING IN 31 BIT MODE INCORRECTLY](#)
8 July 1996
ABENDOC4 in IKTLTERM during unconditional logoff. IKT1001 USERID BCOLWI9 CANCELED DUE TO UNCONDITIONAL LOGOFF
Search result URL: <https://www.ibm.com/support/pages/apar/OW21022>

[II09372: INFORMATION APAR FOR DFSORT/VSE \(5746SM310\) FOR RELEASES V3R1, V3R2, AND V3R3.](#)
15 September 1997
THIS INFO APAR IS FOR DFSORT/VSE (5746SM310) R310 AND R320 AND WILL CONTAIN INFORMATION THAT HAS NOT BEEN APAR'D UNDER NORMAL
Search result URL: <https://www.ibm.com/support/pages/apar/II09372>

[OW29320: ADDITIONAL SUPPORT TO ATM.. COMPATIBILITY ISSUE WITH OS/390 V2R5](#)
1 November 1997
DISC/DM now replaces DEACT request/response Support for ATM PVC liveness testing
Search result URL: <https://www.ibm.com/support/pages/apar/OW29320>

[OW30922: INCORRECT JAPANESE TRANSLATION FOR 'MVS ACCOUNT' ON PRIMARY OPTION MENU](#)
<https://www.ibm.com/mysupport/>

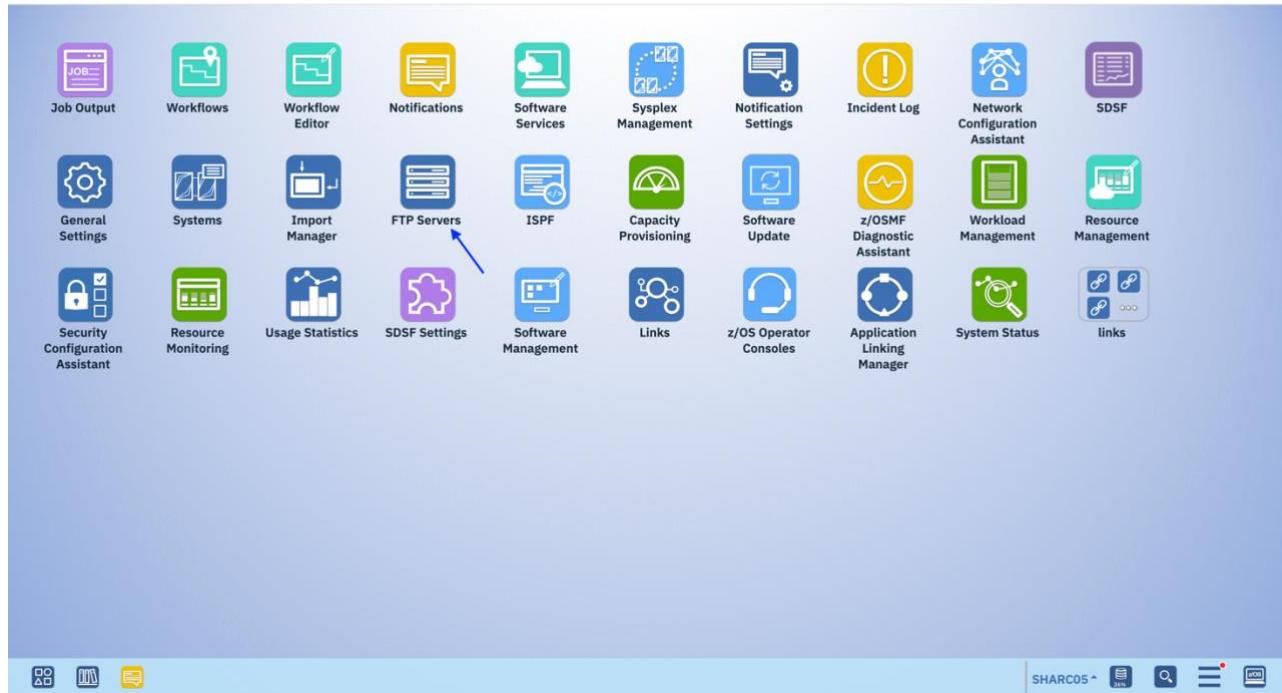
Share your feedback

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.

The screenshot shows the 'FTP Servers' list view in the z/OSMF interface. The title bar says 'FTP Servers'. The list table has columns for Name, Activity, Host, Path Name, Port Number, Description, Transfer Method, and FTP Profile. There are 8 entries listed:

Name	Activity	Host	Path Name	Port Number	Description	Transfer Method	FTP Profil
IBM-eurep-mvs-pduu-https		www.secure.eurep.ibm.com	/t0ibm/mvs			PDUU with HTTPS	No Firewall
IBM-eurep-tivoli-pduu-https		www.secure.eurep.ibm.com	/t0ibm/tivoli			PDUU with HTTPS	No Firewall
IBM-testcase-mvs-pduu-https		testcase.boulder.ibm.com	/t0ibm/mvs			PDUU with HTTPS	No Firewall
IBM-testcase-tivoli-pduu-https		testcase.boulder.ibm.com	/t0ibm/tivoli			PDUU with HTTPS	No Firewall
IBM-eurep-mvs-sftp		sftp.eurep.ibm.com	/t0ibm/mvs			SFTP	No SSH Pr
IBM-eurep-tivoli-sftp		sftp.eurep.ibm.com	/t0ibm/tivoli			SFTP	No SSH Pr
IBM-testcase-mvs-sftp		testcase.boulder.ibm.com	/t0ibm/mvs			SFTP	No SSH Pr
IBM-testcase-tivoli-sftp		testcase.boulder.ibm.com	/t0ibm/tivoli			SFTP	No SSH Pr

Total: 8 Selected: 0

Refresh Last refresh: Jul 26, 2023, 4:14:55 PM local time (Jul 26, 2023, 8:14:55 AM GMT)

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

The screenshot shows the 'FTP Servers' interface. A context menu is open over a selected server ('IBM-ecurep-mvs-sftp'). The 'Actions' menu is expanded, and the 'View' option is highlighted with a blue arrow. The main table lists various FTP servers with columns for Activity Filter, Host Filter, Path Name Filter, Port Number Filter, Description Filter, Transfer Method Filter, and FTP Profile Filter. The table shows entries like 'www.secure.ecurep.ibm.com /tibm/mvs PDUU with HTTPS No Firewall' and 'stfp.ecurep.ibm.com /tibm/mvs SFTP No SSH Pr...'. At the bottom, there are buttons for 'Refresh' and 'Last refresh: Jul 26, 2023, 4:14:55 PM local time (Jul 26, 2023, 8:14:55 AM GMT)'.

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

The screenshot shows the 'View IBM-ecurep-mvs-pduu-https' configuration dialog. It includes fields for 'FTP server name' (set to 'IBM-ecurep-mvs-pduu-https'), 'Host' (set to 'www.secure.ecurep.ibm.com'), 'Path name' (set to '/tibm/mvs'), 'Port number (must be between: 1-65535)' (set to 21), 'Transfer method' (radio buttons for 'FTP', 'SFTP (openSSH based secure FTP)', 'z/OS Problem Documentation Upload Utility (Parallel FTP with optional encryption)', and 'z/OS Problem Documentation Upload Utility with HTTPS (PDUU with HTTPS)' - the last one is selected), 'Work data set size (MB)' (set to 100), 'Number of HTTPS sessions' (set to 3), 'FTP profile' (radio buttons for 'Use the default profile' and 'Use the selected profile' - the first one is selected), 'Description' (empty), and a 'Close' button at the bottom left.

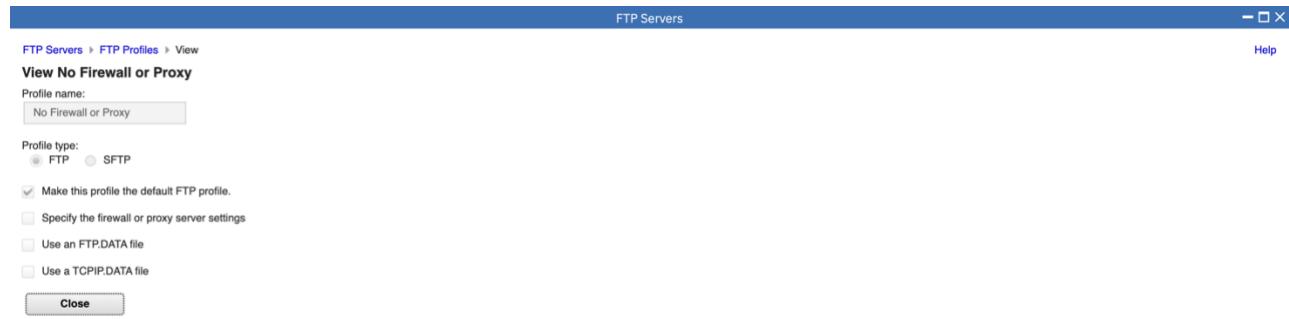
4.Click Actions, then FTP or PDUU Profiles.

The screenshot shows the 'FTP Servers' interface. On the left, a sidebar titled 'Actions' contains options like Modify, View, Copy..., Remove..., Associate FTP or PDUU Profile..., Add..., and 'FTP or PDUU Profiles...' (which has a blue arrow pointing to it). The main area displays a table of FTP servers with columns for Activity, Host, Path Name, Port Number, Description, Transfer Method, and FTP Profile. The table lists several entries, including 'www.secure.ecurep.ibm.com' and 'testcase.boulder.ibm.com'. At the bottom, there is a 'Refresh' button and a note about the last refresh time.

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

The screenshot shows the 'FTP Profiles' interface. On the left, a sidebar titled 'Actions' contains a 'Name Filter' dropdown with 'No filter applied'. The main area displays a table of profiles with columns for Name, Type, Activity, Firewall Host, Firewall User ID, Firewall Port, Firewall Commands, FTP.DATA File Name, and TCPIP.DATA File Name. The table lists two profiles: 'No Firewall or Proxy (default FTP)' (selected, indicated by a blue arrow) and 'No SSH Proxy Command (default SFTP)'. At the bottom, there is a 'Refresh' button and a note about the last refresh time.

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

Exercise Review and Wrap-Up

You now know how to:

- **Log on to z/OSMF**
- **Filter and configure tables within z/OSMF**
- **View incidents**
 - View details of incidents
- **Send diagnostic data to a vendor**

And possibly how to:

- **View information on FTP Servers**
- **View information on FTP Profiles**

© Copyright IBM Corporation 2014

57

Thank You

© Copyright IBM Corporation 2014

58

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 Java logo 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 logo, 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 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.

© Copyright IBM Corporation 2014

60