

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

Session ID: 25293, 25850

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 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 an 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://mvs1.centers.ihost.com/zosmf/>
 - __ c. Enter the User ID (SHARAnn) and password assigned to your workstation.
- __2. View all the incidents across all the systems in your sysplex
 - __ a. Expand the Problem Determination Category in the Left Navigation Tree
 - __ b. Click on Incident Log
- __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 an 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://mvs1.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
 - **Please unselect the checkbox “Use desktop interface” for this lab.**

Note: All screen captures in the handout show the ID SHARA20, your browser will be slightly different to reflect the User ID that you were given.

IBM z/OS Management Facility

LEARN MORE NEED HELP?

Welcome to z/OS

The highly secure, scalable and resilient enterprise operating system for the IBM z Systems mainframe.

z/OS USER ID

z/OS PASSWORD

Use desktop interface

LOG IN

Shopz

IBM Support

z Systems Redbooks

z/OSMF home Page

WCS Flashes and Techdocs

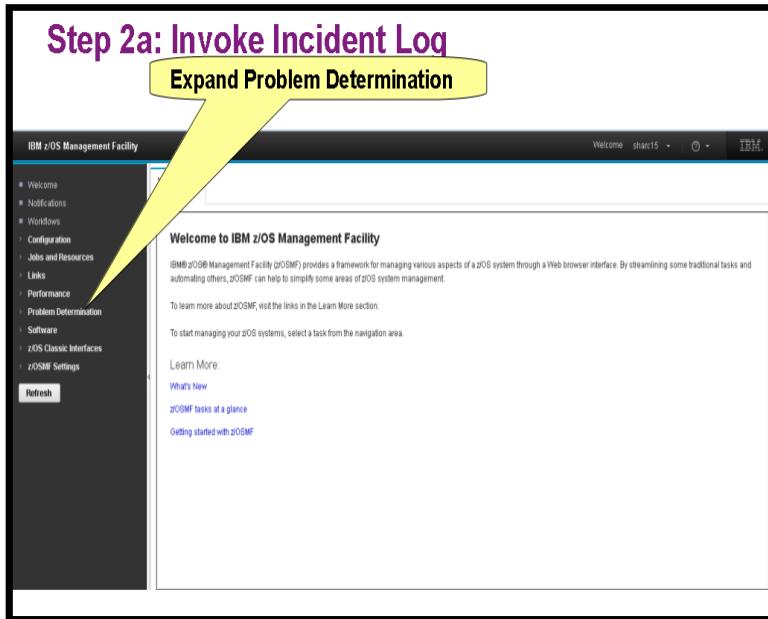
z/OS home Page

z/OS Knowledge Center

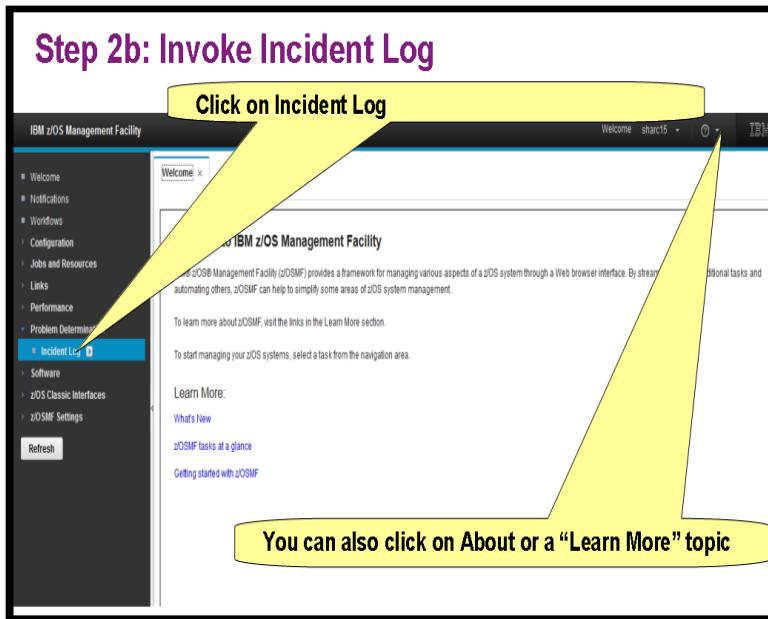
© Copyright IBM Corp. 2009.2019, Version 2.3

2. View all incidents across the systems in your sysplex

Step 2a: Expand the Problem Determination Category in the Left Navigation Tree



Step 2b: Click on Incident Log



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!

Step 2b: Invoke Incident Log ...

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

The screenshot shows the z/OSMF Incident Log interface. On the left, a navigation sidebar lists various sections like Welcome, Notifications, Workflows, Configuration, Jobs and Resources, Links, Performance, Problem Determination, Incident Log (which is selected and highlighted in blue), Software, z/OS Classic Interfaces, and z/OSMF Settings. A Refresh button is also present. The main content area is titled 'Incident Log' and contains a table header with columns: Incident Type Filter, Description Filter, Date and Time (GMT) post "30 days" Filter, Sysplex Filter, System Filter, Problem Number Filter, Tracking ID Filter, and Notes Filter. Below the table, a message states 'There is no data to display.'

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.

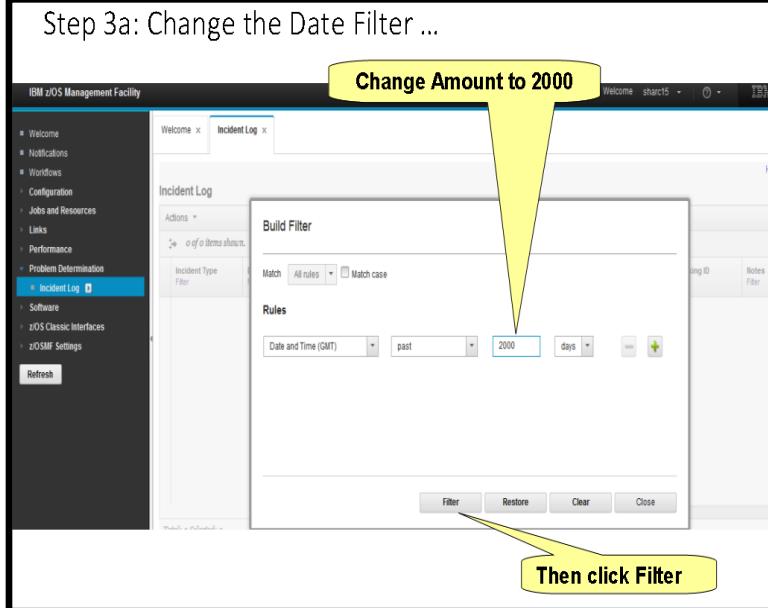
Step 3a: Change the Date Filter

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

Step 3a: Change the Date Filter

The screenshot shows the IBM zOS Management Facility interface. On the left is a navigation sidebar with links like Welcome, Notifications, Workflows, Configuration, Jobs and Resources, Links, Performance, Problem Determination, Incident Log (which is selected and highlighted in blue), Software, zOS Classic Interfaces, and zOSMF Settings. Below the sidebar is a 'Refresh' button. The main area is titled 'Incident Log' and shows a table with columns: Incident Type Filter, Description Filter, Date and Time (GMT) Filter, Sysplex Filter, System Filter, Problem Number Filter, Tracking ID Filter, and Notes Filter. A yellow callout bubble points to the 'Date and Time (GMT)' filter button. The table below it displays the message 'There is no data to display.'

Step 3a: Change the Date Filter ...



Step 3a: Change the Date Filter ...

Now the list of 42 incidents are displayed on a table

Incident Type	Description	Date and Time (GMT)	Sysplex	System	Problem Number	Tracking ID	Notes
ABEND S0106	ABEND=S106,RC=000F,COMPON=SDSF-ESTAE,COMPND=6550-205,ISSUEH=SFSTAE,SDSF ABEND ROUTINE	Nov 25, 2014, 2:26:34 PM	SHARPLEX	S1			
ABEND S0108	COMPON=CEA,COMPD=SCCEA,ISSVER=CEAMREC,MODU	Oct 9, 2014, 9:05:32 PM	SHARPLEX	S1			
User Initiated	" MFUSR30 - TEST DUMP FOR USE WITH INCIDENT LOG /IP "	Oct 8, 2014, 10:29:51 PM	SHARPLEX	S1			
ABEND S0001	(EJES DIAGNOSTIC SVC DUMP - ABCODE 0C1000	Oct 8, 2014, 9:41:38 PM	SHARPLEX	S1			
User Initiated	" MFUSR30 - TEST DUMP FOR USE WITH INCIDENT LOG /IP "	Oct 8, 2014, 9:36:59 PM	SHARPLEX	S1			
User Initiated	" MFUSR29 - TEST DUMP FOR USE WITH INCIDENT LOG /IP "	Oct 8, 2014, 9:36:39 PM	SHARPLEX	S1			

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.

Step 3b: Sort the Columns

Now you will sort the columns in the table

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

Incident Type	Description	Date and Time (GMT) past '2000 days'	Sysplex	System	Problem Number	Tracking ID	Notes
User Initiated	(EJES DIAGNOSTIC SVC DUMP - ABCODE:0C1000)	Sep 30, 2014, 7:38:07 PM	SHARPLEX	S1			
User Initiated	ABEND S00C1	Oct 8, 2014, 9:41:38 PM	SHARPLEX	S1			
User Initiated	"MFUSR01 - TEST DUMP FOR USE WITH INCIDENT LOG MP = "	Jun 19, 2013, 2:58:16 PM	SHARPLEX	S1			
User Initiated	"MFUSR01 - TEST DUMP FOR USE WITH INCIDENT LOG MP = "	May 8, 2013, 8:17:23 PM	SHARPLEX	S1			
User Initiated	"MFUSR02 - TEST DUMP FOR USE WITH INCIDENT LOG MP = "	May 8, 2013, 8:17:53 PM	SHARPLEX	S1			
User Initiated	"MFUSR03 - TEST DUMP FOR USE WITH INCIDENT LOG MP = "	May 8, 2013, 8:18:20 PM	SHARPLEX	S1			
User Initiated	"MFUSR04 - TEST DUMP FOR USE WITH INCIDENT LOG MP = "	May 8, 2013, 8:24:37 PM	SHARPLEX	S1	7134	151008	Testing

Step 3b: Sort the Columns ...

IBM z/OS Management Facility

Welcome x Incident Log x

Incident Log

Actions ▾

42 of 42 items shown. Clear filter

Incident Type	Description	2 ▾	Date and Time (GMT) past '2000 days'	1 ▾	Sysplex	System	Problem Number	Tracking ID	Notes
ABEND S0106	ABEND=5108,RC=400F,COMPON=SSSF-ESTAE,COMPID=6550-Z05,BSUSER=DFSTATE,SDSF ABEND ROUTINE		Nov 25, 2014, 2:26:34 PM		SHARPLEX	S1			
ABEND S0106	COMPON=CEA,COMPID=SCCEA,ISSUER=CEAMREC,WODU		Oct 9, 2014, 9:05:32 PM		SHARPLEX	S1			
User Initiated	"MFUSRQ3 - TEST DUMP FOR USE WITH INCIDENT LOG MP "		Oct 8, 2014, 10:29:51 PM		SHARPLEX	S1			
ABEND S00C1	(EJES DIAGNOSTIC SVC DUMP - ABCODE 0C1000		Oct 8, 2014, 9:41:38 PM		SHARPLEX	S1			
User Initiated	"MFUSRQ3 - TEST DUMP FOR USE WITH INCIDENT LOG MP "		Oct 8, 2014, 9:36:58 PM		SHARPLEX	S1			
User Initiated	"MFUSRQ3 - TEST DUMP FOR USE WITH INCIDENT LOG MP "		Oct 8, 2014, 9:36:39 PM		SHARPLEX	S1			

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

Step 3b: Sort the Columns ...

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

IBM z/OS Management Facility

Welcome x Incident Log x

Incident Log

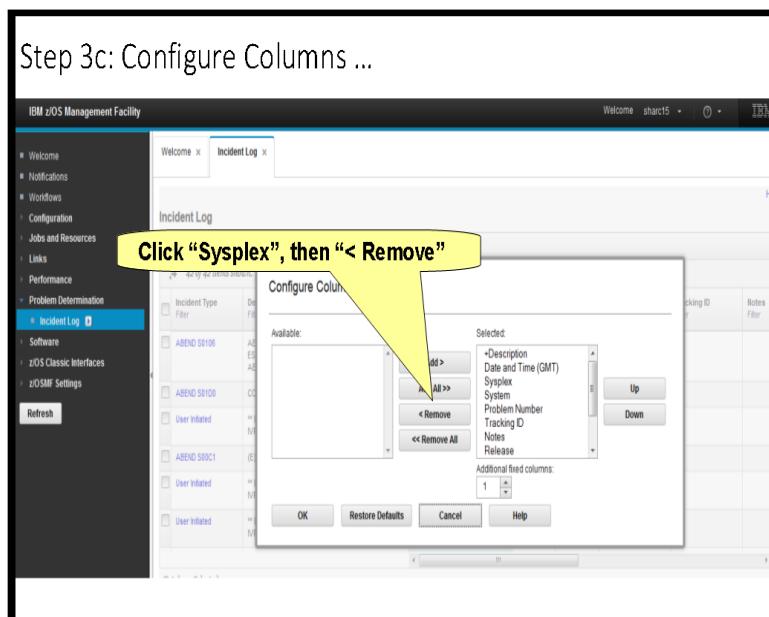
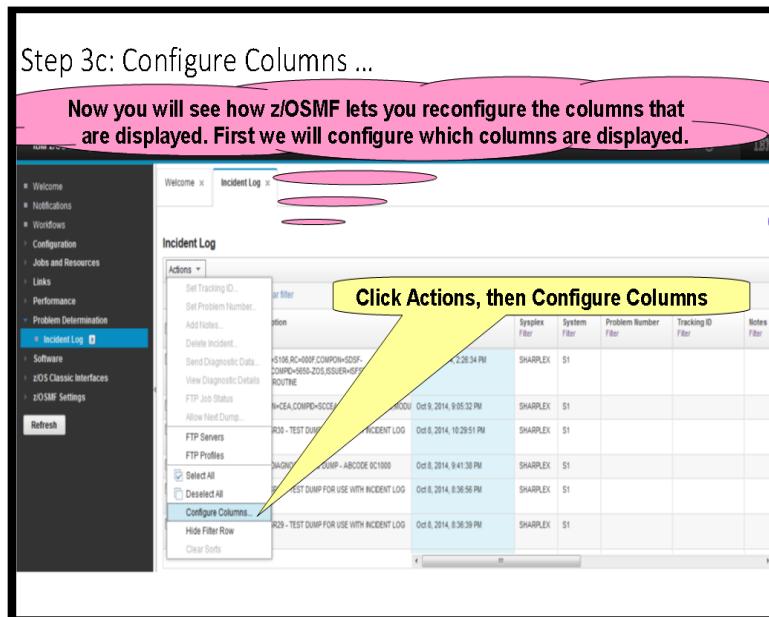
Actions ▾

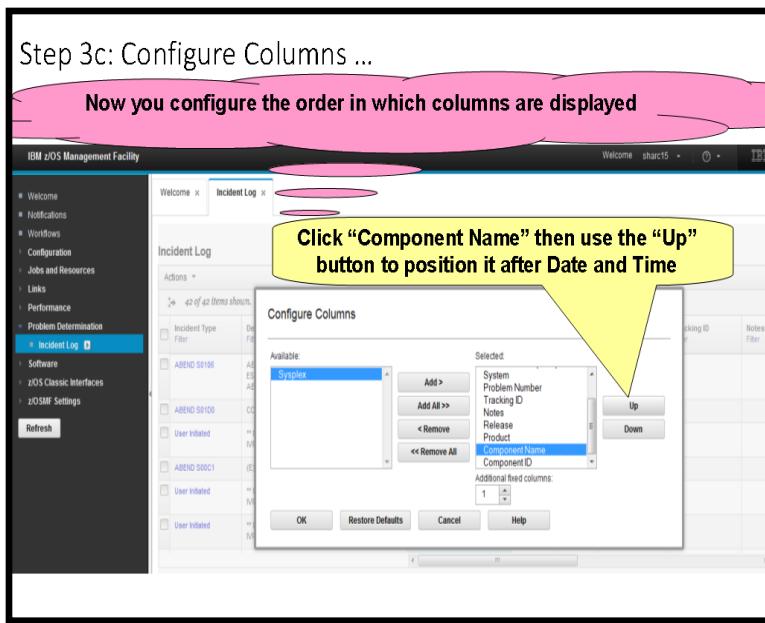
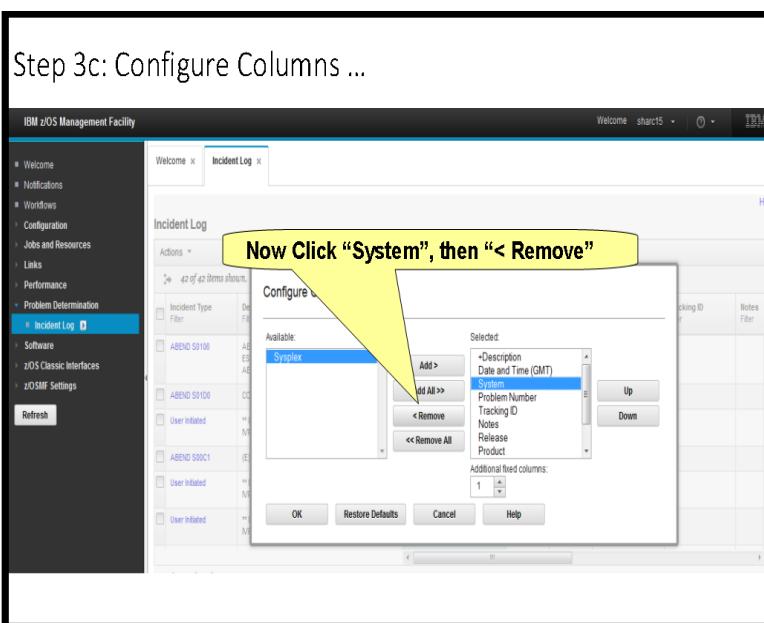
42 of 42 items shown. Clear filter

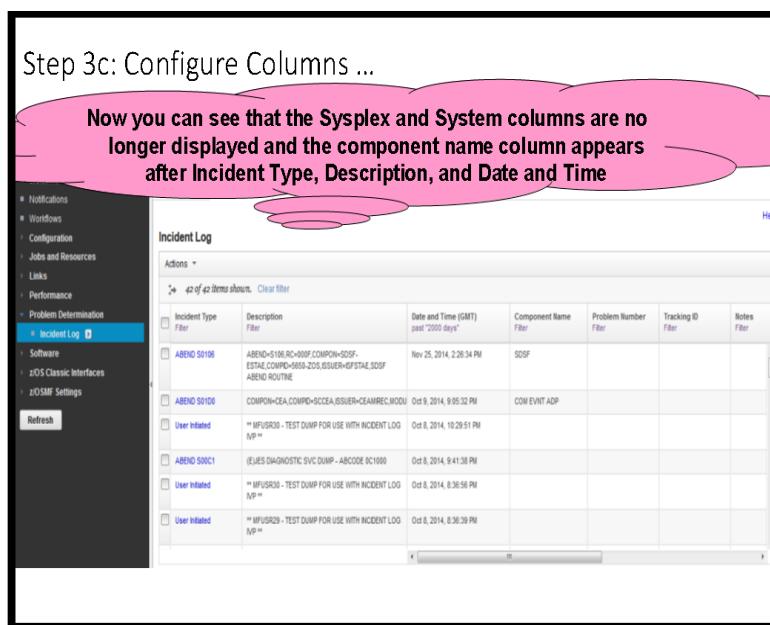
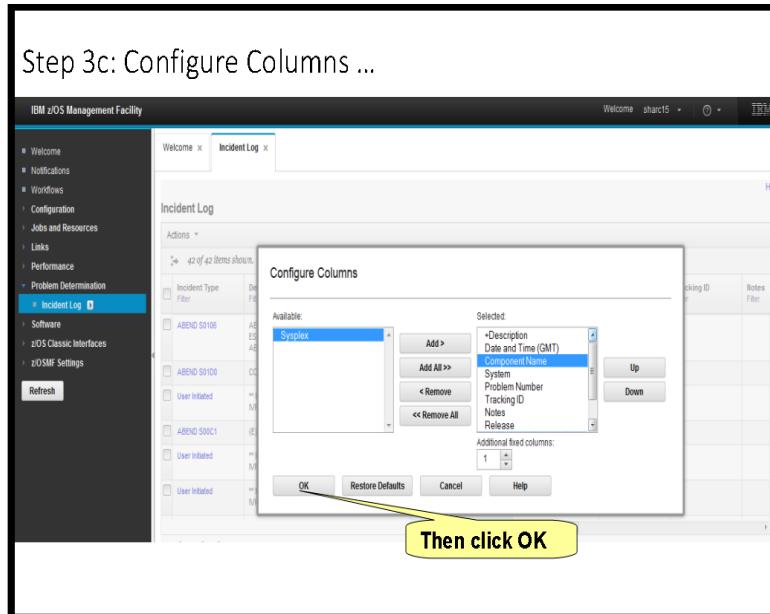
Incident Type	Description	▲	Date and Time (GMT) past '2000 days'	▼	Sysplex	System	Problem Number	Tracking ID	Notes
ABEND S0106	ABEND=5108,RC=400F,COMPON=SSSF-ESTAE,COMPID=6550-Z05,BSUSER=DFSTATE,SDSF ABEND ROUTINE		Nov 25, 2014, 2:26:34 PM		SHARPLEX	S1			
ABEND S0106	COMPON=CEA,COMPID=SCCEA,ISSUER=CEAMREC,WODU		Oct 9, 2014, 9:05:32 PM		SHARPLEX	S1			
User Initiated	"MFUSRQ3 - TEST DUMP FOR USE WITH INCIDENT LOG MP "		Oct 8, 2014, 10:29:51 PM		SHARPLEX	S1			
ABEND S00C1	(EJES DIAGNOSTIC SVC DUMP - ABCODE 0C1000		Oct 8, 2014, 9:41:38 PM		SHARPLEX	S1			
User Initiated	"MFUSRQ3 - TEST DUMP FOR USE WITH INCIDENT LOG MP "		Oct 8, 2014, 9:36:58 PM		SHARPLEX	S1			
User Initiated	"MFUSRQ3 - TEST DUMP FOR USE WITH INCIDENT LOG MP "		Oct 8, 2014, 9:36:39 PM		SHARPLEX	S1			

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.







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 an 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, “** MFUSR20 – TEST DUMP FOR USE WITH INCIDENT LOG IVP” if your User ID is SHARA20).

Step 4a: Select a user initiated incident with the same suffix as your User ID

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

Click on Filter under Description

Incident Type	Description	Date and Time (GMT)	Component Name	Problem Number	Tracking ID	Notes
ABEND S0108	ABEND=S108 RC=000F CORPON=SCSF-ESTATE,COMPID=6660-Z05,ISSUER=ESTATE,SCSF ABEND ROUTINE	Nov 25, 2014, 2:26:34 PM	S0SF			
ABEND S0103	COMPON=EA,COMPID=SCCEA,ISSUER=CEAMREC,MODU	Oct 9, 2014, 9:05:32 PM	COM EVNT ADP			
User Initiated	** MFUSR30 - TEST DUMP FOR USE WITH INCIDENT LOG I/P **	Oct 8, 2014, 10:29:51 PM				
ABEND S00C1	(EJES DIAGNOSTIC SVC DUMP - ABCODE 0C1000	Oct 8, 2014, 9:41:38 PM				
User Initiated	** MFUSR30 - TEST DUMP FOR USE WITH INCIDENT LOG I/P **	Oct 8, 2014, 9:38:56 PM				
User Initiated	** MFUSR20 - TEST DUMP FOR USE WITH INCIDENT LOG I/P **	Oct 8, 2014, 9:38:39 PM				

Step 4a: Select a user initiated incident with the same suffix as your User ID ...

Change to an incident that has the same suffix as your User ID (e.g., MFUSR30 for SHARC30)

Then click Filter

The 'Build Filter' dialog box shows the following configuration:

- Match: All rules
- Rules:
 - Data and Time (GMT): east, 2,000 days
 - Description: contains, MFUSR30

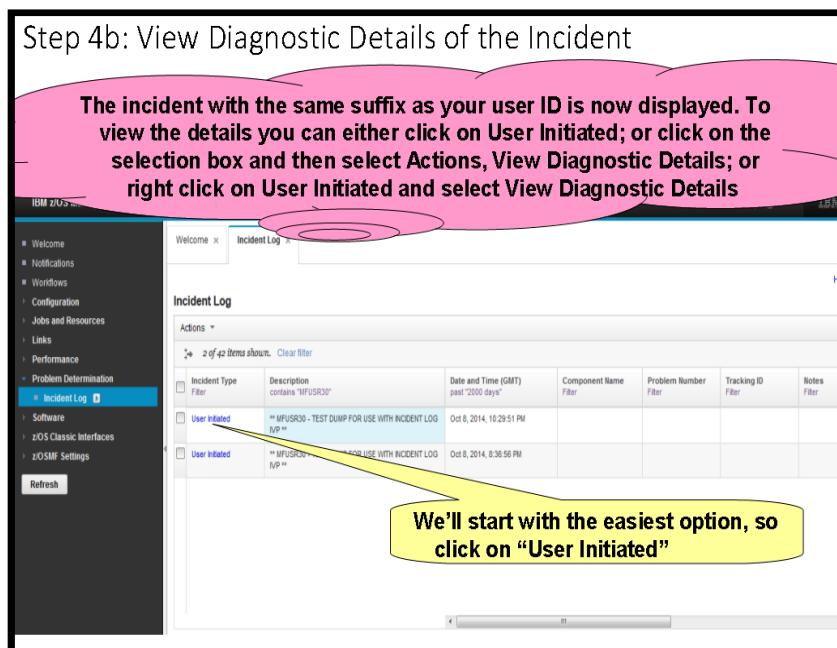
Buttons at the bottom: Filter, Restore, Clear, Close

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.



Step 4b: View Diagnostic Details of the Incident ...

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.

Data Type	Source	Sysplex	System
SVC dump	SYS1.DUMP.S1#MASTER#D14281.T102951.S00730	SHARPLEX	S1
Error log	CEA.R00.CDE01236.A70B5910.X00.VEW	SHARPLEX	S1
Operations log	CEA.Y00.CDE01236.A70B5910.X00.VEW	SHARPLEX	S1
Error log summary	CEA.S00.CDE01236.A70B5910.X00.VEW	SHARPLEX	S1

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)

Once you've finished with this tab, lets move on to the other tab - General

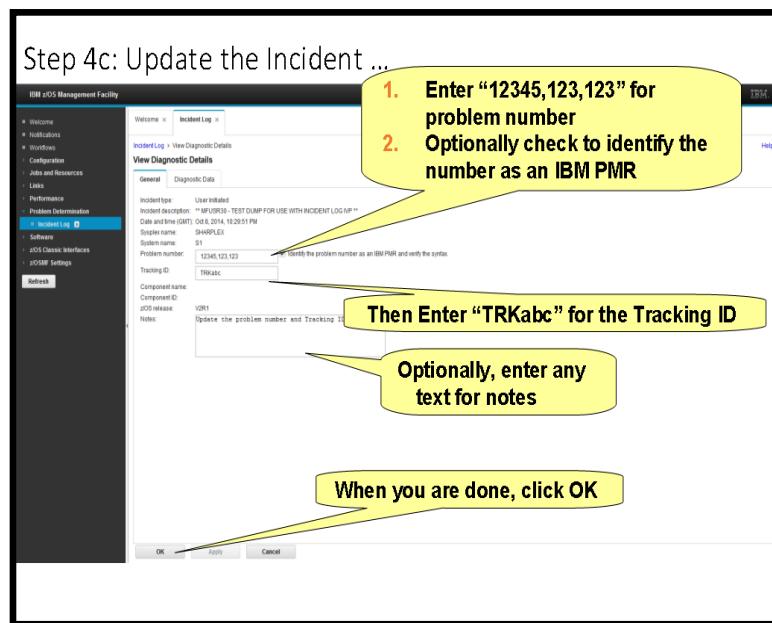
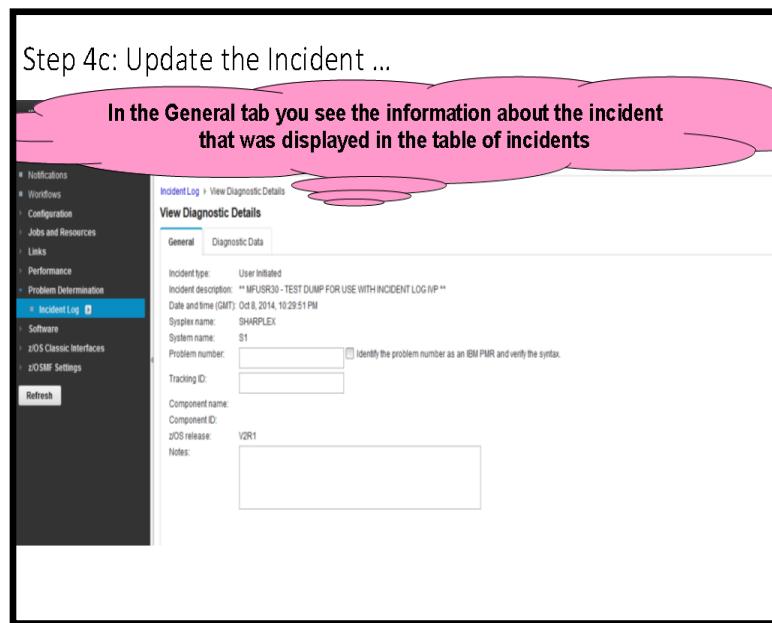
Step 4c: Update the Incident

You now add a vendor problem number and installation problem tracking number to this incident. Optionally, you can also add a note.

To update the incident, you must first 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 “12345,123,123” as the problem number, “TRKabc” as the Tracking ID, and optionally enter any text for Notes.



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

Step 4c: Update the Incident ...

You now see the additional information in the table display

The screenshot shows the 'Incident Log' page. On the left is a navigation sidebar with links like Welcome, Notifications, Configuration, Jobs and Resources, Links, Performance, Problem Determination, Incident Log (which is selected and highlighted in blue), Software, z/OS Classic Interfaces, and z/OSMF Settings. Below the sidebar is a 'Refresh' button. The main area is titled 'Incident Log' and shows a table with two rows of data. The columns are: Incident Type, Description, Date and Time (GMT), Component Name, Problem Number, Tracking ID, and Notes. The first row has a checkbox under 'Incident Type' and a dropdown under 'Description' containing 'User Initiated'. The second row also has a checkbox under 'Incident Type' and a dropdown under 'Description' containing 'User Initiated'. The 'Date and Time (GMT)' column shows 'Oct 8, 2014, 10:29:51 PM' for both rows. The 'Component Name' column shows 'MP ='. The 'Problem Number' column shows '12345,123,123'. The 'Tracking ID' column shows 'TRKabc'. The 'Notes' column shows 'Update the problem number and tracking ID.' A red oval highlights the 'Tracking ID' column for the second row. At the top of the main area, there is a message: 'You now see the additional information in the table display'.

Incident Type	Description	Date and Time (GMT)	Component Name	Problem Number	Tracking ID	Notes
<input type="checkbox"/>	User Initiated "MFISRD0 - TEST DUMP FOR USE WITH INCIDENT LOG MP ="	Oct 8, 2014, 10:29:51 PM		12345,123,123	TRKabc	Update the problem number and tracking ID.
<input type="checkbox"/>	User Initiated "MFISRD0 - TEST DUMP FOR USE WITH INCIDENT LOG MP ="	Oct 8, 2014, 8:36:59 PM				

Step 4d: Browse Diagnostic Data

Since z/OSMF V1.13, you can browse the logs captured for an Incident. z/OSMF ISPF Browse is used for this, so this feature only will work if your installation has setup and configured z/OSMF ISPF.

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.

Step 4d: Browse Diagnostic Data

To browse diagnostic data, you must first view the details of your incident again.

The screenshot shows the z/OSMF Incident Log interface. On the left is a navigation sidebar with various links like Welcome, Notifications, Workflows, Configuration, Jobs and Resources, Links, Performance, Problem Determination, Incident Log (which is selected and highlighted in blue), Software, z/OS Classic Interfaces, and z/OSMF Settings. Below that is a Refresh button. The main area is titled 'Incident Log' and shows a table of incidents. One incident is selected, showing details: 'Incident ID: I00 - TEST DUMP FOR USE WITH INCIDENT LOG', 'Date and Time (GMT): Oct 8, 2014, 10:29:51 PM', 'Component Name: Filter', 'Problem Number: Filter', 'Tracking ID: TRKabc', and 'Notes: Filter'. Above the table is a 'Actions' dropdown menu with options: Set Tracking ID..., Set Problem Number..., Add Notes..., Delete Incident..., Send Diagnostic Data..., View Diagnostic Details (which is highlighted in blue), FTP Job Status, Allow Next Dump..., FTP Servers, FTP Profiles, Select All, Deselect All, Configure Columns..., Hide Filter Row, and Clear Sorts. A yellow callout bubble points to the 'View Diagnostic Details' option in the Actions menu with the text: '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 ISPF inside of z/OSMF to enable you to browse the snapshot of SYSLOG data. You will see that it opens an ISPF tab if you didn't already have one open, and invoke browse in context for you.

Note: If you do not already have a z/OSMF ISPF session running, you should start the z/OSMF ISPF task first.

Step 4d: Browse Diagnostic Data ...

The screenshot shows the 'Incident Log' section of the z/OSMF interface. On the left is a navigation menu with options like Welcome, Notifications, Workflows, Configuration, Jobs and Resources, Links, Performance, Problem Determination, Incident Log (which is selected), Software, z/OS Classic Interfaces, and z/OSMF Settings. The main area shows a table titled 'Diagnostic Data' with columns for Data Type, Source, Sysplex, and System. There are four entries: 'SVC dump' (Source: SYS1.DUMP1#MASTER014281.T192951.S00739, Sysplex: SHARPLEX, System: S1), 'Error log' (Source: CEA.R08.C0E91236.AT05910.XXX.VEW, Sysplex: SHARPLEX, System: S1), 'Operations log' (Source: CEA.Y00.C0E91236.AT05910.XXX.VEW, Sysplex: SHARPLEX, System: S1), and 'Error log summary' (Source: CEA.S00.C0E91236.A75.VIEW, Sysplex: SHARPLEX, System: S1). A yellow callout with the text 'Click on the Operations log source' points to the fourth row.

Step 4d: Browse Diagnostic Data ...

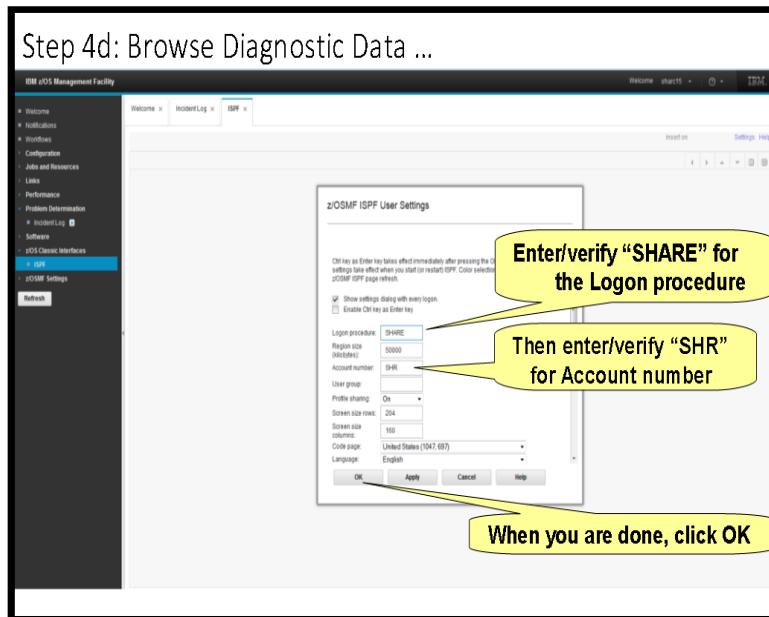
Now you see a new ISPF tab. If you are the first user with this User ID to enter ISPF, then you will see the following default z/OSMF ISPF User Settings.

The screenshot shows the 'z/OSMF ISPF User Settings' panel. At the top, there's a navigation bar with tabs for 'Welcome', 'IncidentLog', and 'ISPF'. The 'ISPF' tab is highlighted with a red circle. Below the tabs is a message about the Ctrl key setting. The main area contains several configuration options: 'Ctrl key as Enter key takes effect immediately after pressing the OK or Apply buttons. Other settings take effect when you start or restart ISPF. Color selections also take effect at the next ISPF page refresh.' with checkboxes for 'Show settings dialog with every login' and 'Enable Ctrl key as Enter key'; 'Logon procedure: SHARE'; 'Region size: 50000'; 'Account number: SHR'; 'User group: Profile sharing: On'; 'Screens size rows: 204'; 'Screens size columns: 160'; 'Code page: United States (1047,697)'; and language settings. At the bottom are 'OK', 'Apply', 'Cancel', and 'Help' buttons.

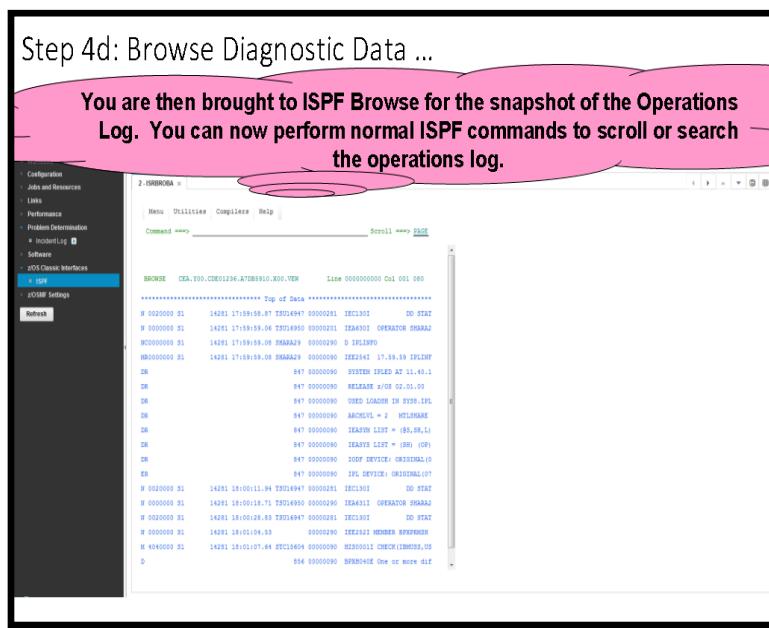
If you are the first person to use this ID to enter ISPF, then you will see the z/OSMF ISPF User Setup panel with default values. Please ensure that the logon procedure is set to SHARE and the Account number is set to SHR.

Optionally check box on top that will not open settings panel every time. If changes need to be made at a later time, you can click on 'Settings' on top right.

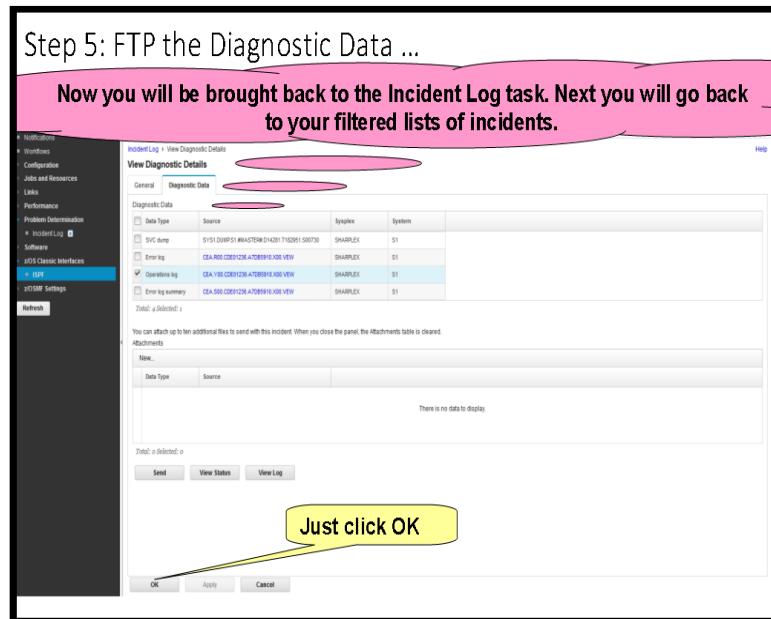
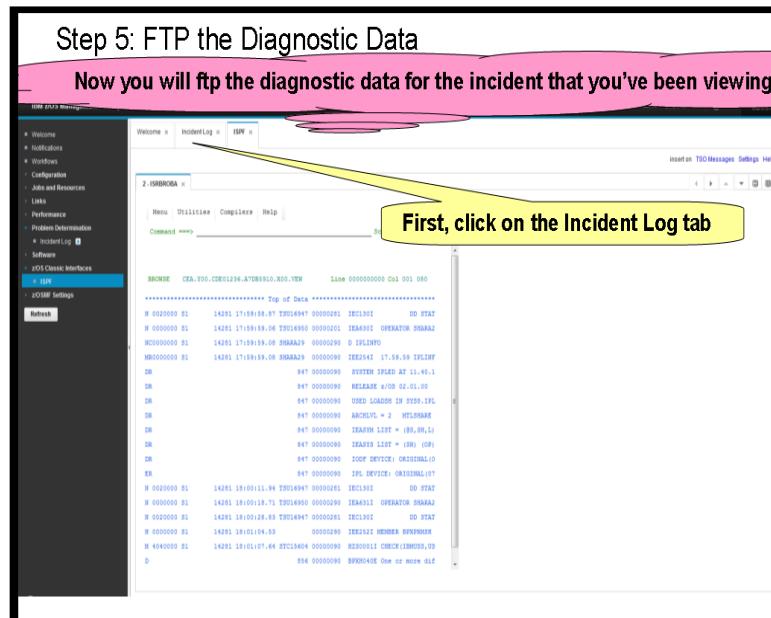
Click OK after entering the new values.

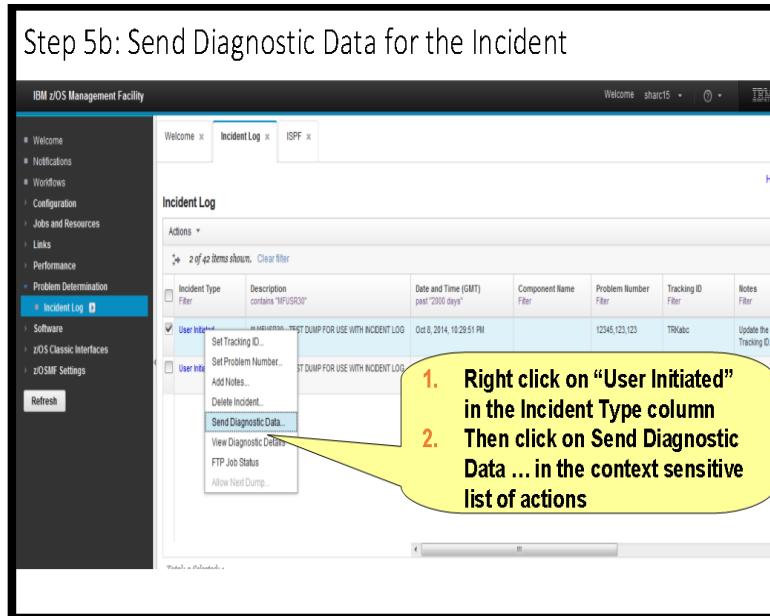


You will ultimately find yourself using ISPF Browse on the diagnostic data element that you had clicked on from the Incident Log!!



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





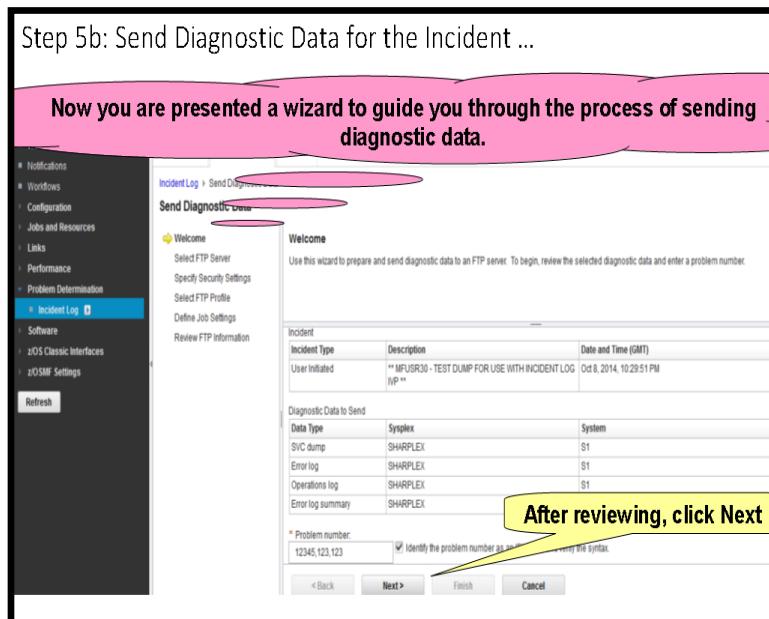
You will now be able to work with a wizard that will guide you through the steps to FTP the diagnostic data for that incident.

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.

Click on Next once you are done.



The next page in the wizard allows you to select where you want to send these files/datasets. For this exercise, select the first one in the list and click on Next.

Step 5c: Select the FTP Server

The first “real” step in the wizard is to select the FTP server.

Name	Activity	Host	Path Name	Port Number	Description
IBM-ap-mvs	ftp.ap.ecurep.ibm.com	ibmMVS			FTP
IBM-ap-lvol	ftp.ap.ecurep.ibm.com	ibmLVOL			FTP
IBM-ecurep-mvs	ftp.ecurep.ibm.com	ibmMVS			FTP
IBM-ecurep-mvs-ftp	ftp.ecurep.ibm.com	ibmMVS			FTP
IBM-ecurep-lvol	ftp.ecurep.ibm.com	ibmLVOL			FTP
IBM-ecurep-lvol-ftp	ftp.ecurep.ibm.com	ibmLVOL			FTP
IBM-hdcase-mvs	testcase.boulder.ibm.com	ibmMVS			FTP
IBM-hdcase-mvs-ftp	testcase.boulder.ibm.com	ibmMVS			FTP
IBM-hdcase-lvol	testcase.boulder.ibm.com	ibmLVOL			FTP
IBM-hdcase-lvol-ftp	testcase.boulder.ibm.com	ibmLVOL			FTP
z900FT-1chland.ibm.com	z900FT-1chland.ibm.com	/			test server

Total: 11 Selected: 1

Refresh Last refresh: Feb 24, 2016, 10:08:37 AM local time (Feb 24, 2016, 2:08:37 AM GMT)

< Back Next > Finish Cancel

Note: Next is not enabled until an FTP server is selected

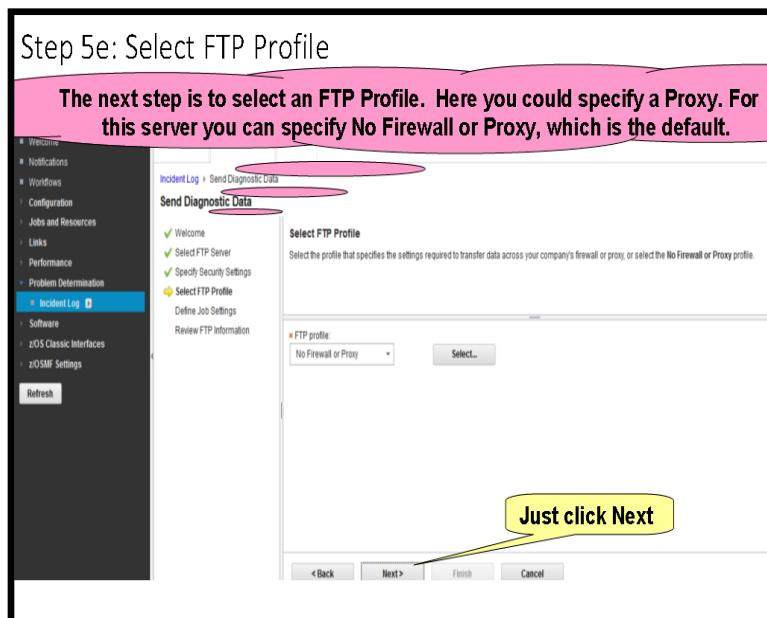
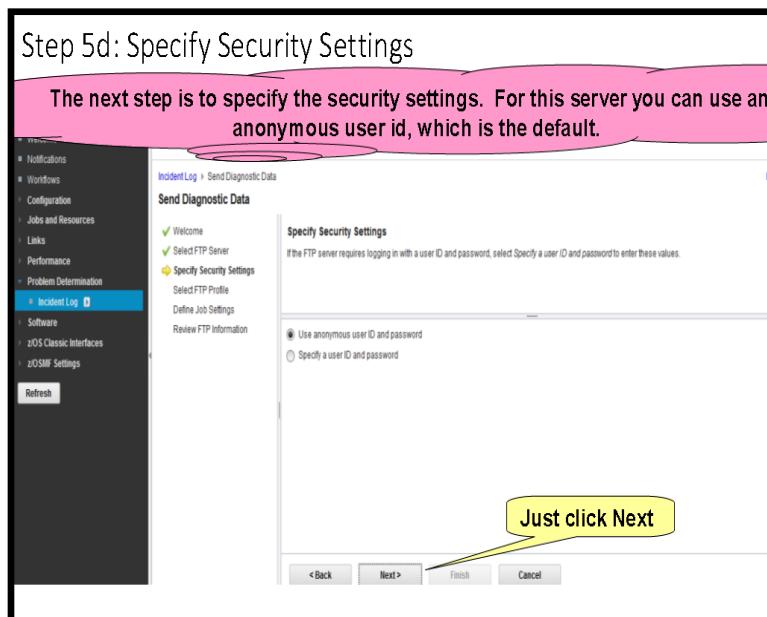
Step 5c: Select the FTP Server ...

Select the IBM-ecurep-mvs FTP Server

Then click Next

Note: Once an FTP server is selected, Next is enabled

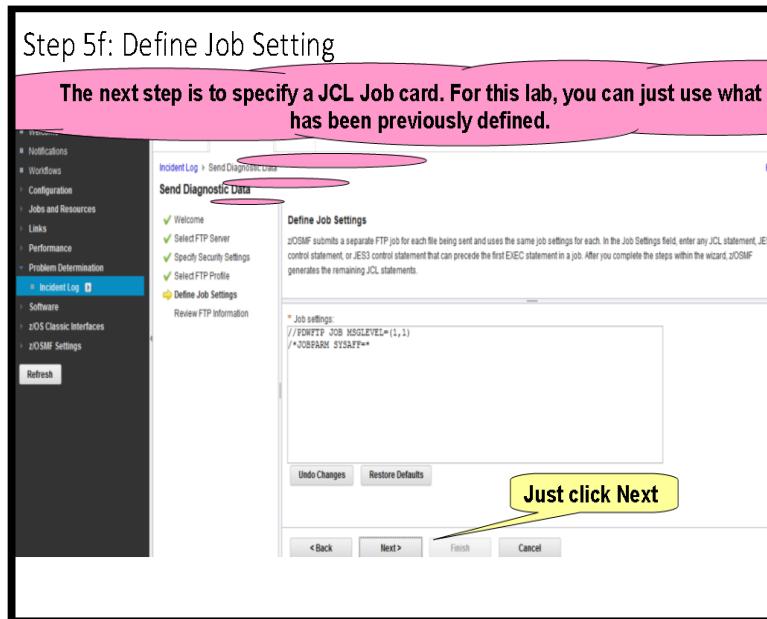
This is where you can enter the userid/password needed to access the FTP Destination server you selected in the previous step. In this exercise, we will use the anonymous sign on. Click on Next to move on.



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.

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.

Optionally, you can view or edit the JCL. We do not recommend changing the JCL.

Step 5g: Review the FTP Information

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

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.

FTP server: Name: IBM-europe-mvs
Host: ftp.europe.ibm.com
Path name: /ibmnames
Port number:

Transfer method: FTP

Security settings: User ID: anonymous
Password: *****

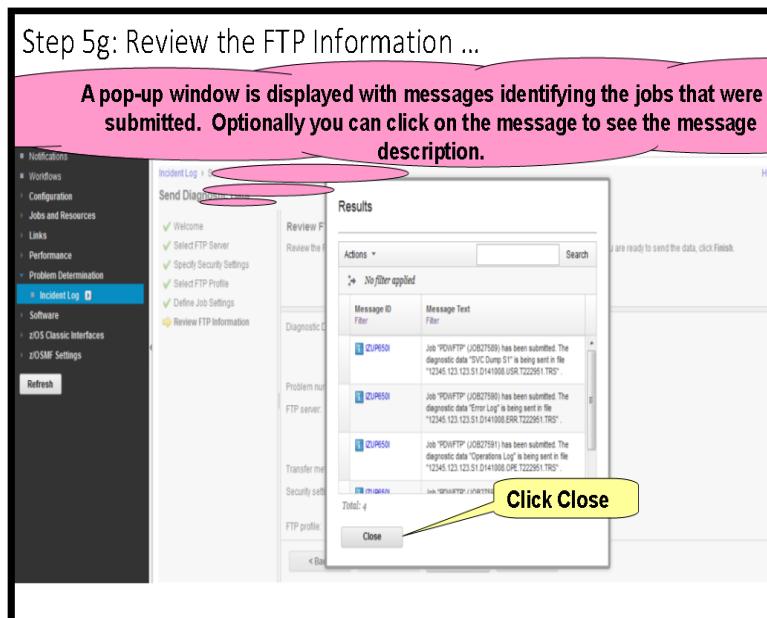
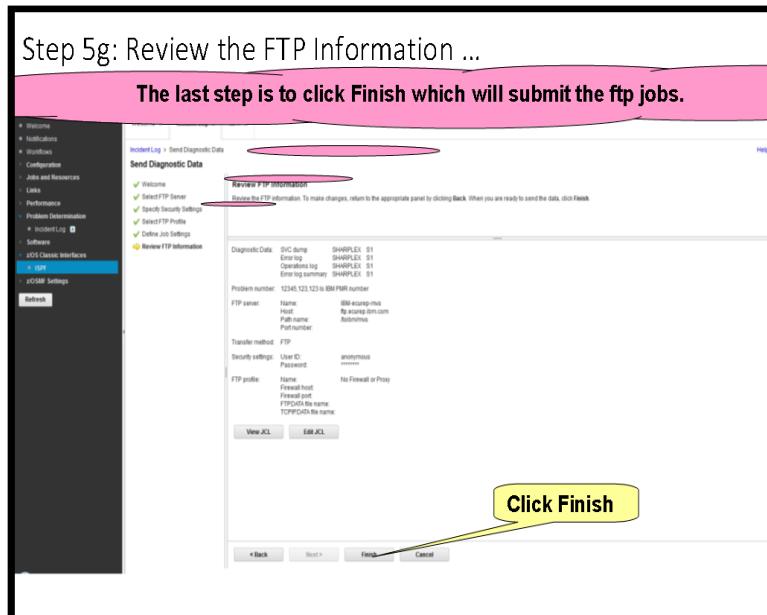
FTP profile: Name: No Firewall or Proxy
Firewall host:
Firewall port:
FTP/DATA file name:
TCP/IP/DATA file name:

View JCL Edit JCL

< Back Next Finish Cancel

Optionally you can view the JCL

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.



Once you click on the Finish button in the above step, z/OSMF will submit the jobs. You will get a confirmation window.

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

Step 6a: FTP Job Status

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

Step 6a: FTP Job Status ...

The job status is displayed.

After reviewing, click Close

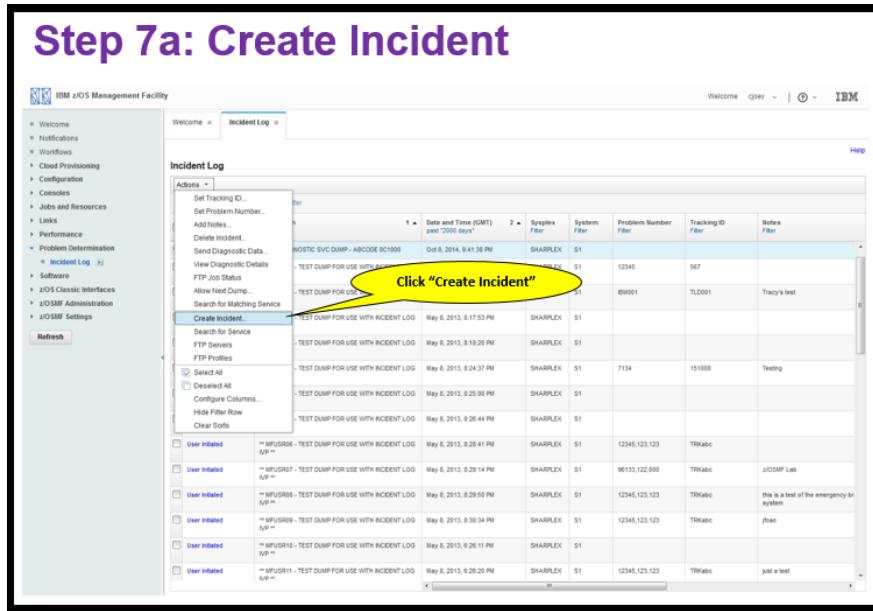
Note: The jobs during the lab will fail, on your system they should complete successfully.

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

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 SHARPLEX.S1 as System name, enter 2/5/2018 1:00 am as Date and Time, select V2R3 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;

Step 7a: Create Incident

The screenshot shows the 'Create Incident' form. The 'Description' field contains 'Manually created incident test'. A yellow callout bubble points to this field with the text 'Description is required'. The 'Create' button at the bottom is highlighted.

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”.

Step 7b: Click on Create Incident

The screenshot shows the 'Incident Log' main panel. A callout bubble points to the table header with the text 'There will be new record In the main panel of the Incident Log , Incident Type is Manual'. The table lists various incidents, including one with 'Incident Type: Manual Created' and 'Description: Manually created incident test'.

Actions	Incident Type	Description	Date and Time (GMT) past '2000 days'	Sysplex Filter	System Filter	Problem Number Filter	Tracking ID Filter	Notes Filter
<input type="checkbox"/> 44 of 44 items shown. Clear filter	<input type="checkbox"/> Incident Type Filter	<input type="checkbox"/> Description Filter						
	<input type="checkbox"/> Manual Created	Manually created incident test	Feb 5, 2018, 1:00:00 AM	SHARPLEX	S1		111	NOTES NOTES
	<input type="checkbox"/> User Initiated	SLIP DUMP E=0001	Jan 12, 2018, 9:13:39 PM	SHARPLEX	S1			
	<input type="checkbox"/> User Initiated	2P5 Abend - ABEND 50102 - Dec 22 18:14:54 in module OESCM at offset 0000000000000000	Dec 22, 2017, 6:14:57 PM	SHARPLEX	S1			
	<input type="checkbox"/> ABEND 50106	ABEND=50106 RC=0000F COMPON=62DF-ESTAE,COMPID=665-205,ISSUE=RH-STATE,SDSF-ABEND-ROUTINE	Nov 25, 2014, 2:26:34 PM	SHARPLEX	S1	1234_123		
	<input type="checkbox"/> ABEND 50100	COMPON=CEA,COMPID=SCCEA,ISSUE=CEA,REC,MODU	Oct 9, 2014, 9:05:52 PM	SHARPLEX	S1	12335_035_000	12345_000	Maria testing this.
	<input type="checkbox"/> User Initiated	** MFUR30 - TEST DUMP FOR USE WITH INCIDENT LOG	Oct 8, 2014, 9:29:51 PM	SHARPLEX	S1	12345_123_123	TRKabc	Update the problem n. O. ok
	<input type="checkbox"/> ABEND 5001	(EYES) DIAGNOSTIC SVC DUMP - ABCODE 0C1000	Oct 8, 2014, 9:41:38 PM	SHARPLEX	S1			
	<input type="checkbox"/> User Initiated	** MFUR30 - TEST DUMP FOR USE WITH INCIDENT LOG	Oct 8, 2014, 9:36:59 PM	SHARPLEX	S1	12345_123_123	R512345	Test incident.
	<input type="checkbox"/> User Initiated	** MFUR30 - TEST DUMP FOR USE WITH INCIDENT LOG	Oct 8, 2014, 9:36:19 PM	SHARPLEX	S1			
	<input type="checkbox"/> User Initiated	** MFUR30 - TEST DUMP FOR USE WITH INCIDENT LOG	Oct 8, 2014, 9:35:57 PM	SHARPLEX	S1			
	<input type="checkbox"/> User Initiated	** MFUR30 - TEST DUMP FOR USE WITH INCIDENT LOG	Oct 8, 2014, 9:35:33 PM	SHARPLEX	S1			
	<input type="checkbox"/> User Initiated	** MFUR30 - TEST DUMP FOR USE WITH INCIDENT LOG	Oct 8, 2014, 9:35:02 PM	SHARPLEX	S1			
	<input type="checkbox"/> User Initiated	** MFUR30 - TEST DUMP FOR USE WITH INCIDENT LOG	Oct 8, 2014, 9:34:38 PM	SHARPLEX	S1			
	<input type="checkbox"/> User Initiated	** MFUR301 - TRK RT DUMP FOR USE WITH INCIDENT LOG	Oct 8, 2014, 9:34:21 PM	SHARPLEX	S1	12345_123_123	TRKabc	Handle PAUSE

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.

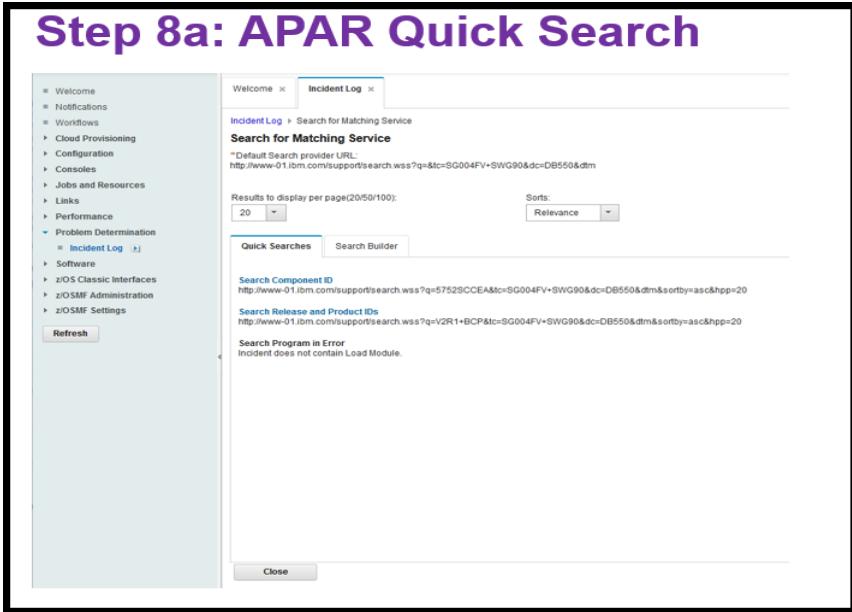
Step 8a: APAR Quick Search

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

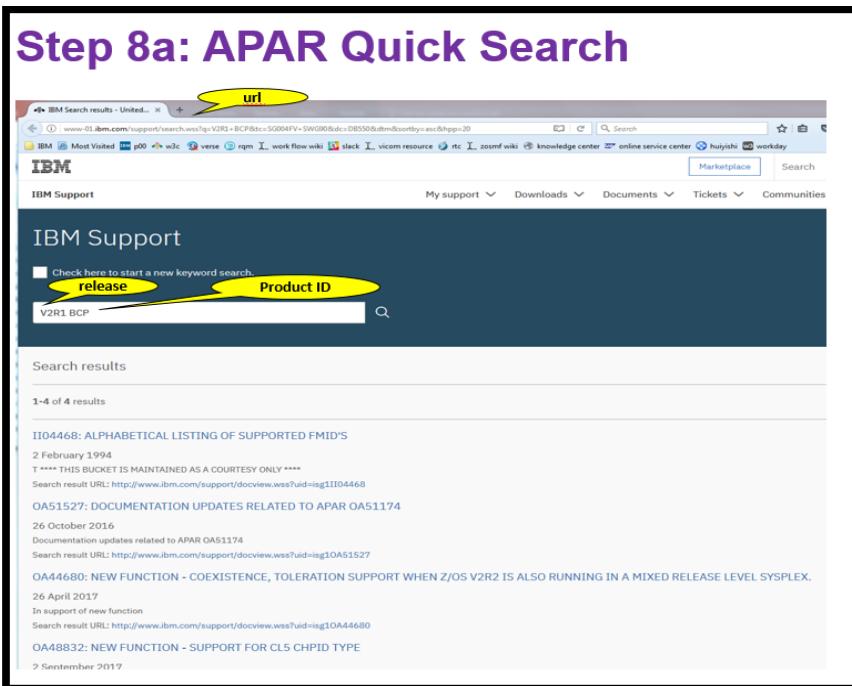
The screenshot shows the 'Incident Log' page with a sidebar containing navigation links like Welcome, Notifications, Workflows, Cloud Provisioning, Configuration, Consoles, Jobs and Resources, Links, Performance, Problem Determination (selected), Incident Log (selected), Software, z/OS Classic Interfaces, z/OSMF Administration, and z/OSMF Settings. The main area has tabs for 'Quick Searches' and 'Search Builder'. A callout bubble points to the 'Search for Matching Service' option in the 'Actions' dropdown menu, which is highlighted with a yellow oval. The table below lists several incidents, with one row selected and highlighted in blue. A yellow arrow points from the 'Search for Matching Service' label to the 'Selected' checkbox in the table row. A pink cloud-shaped callout bubble above the table says: 'To use "Search for Matching Service", you need select an incident with dump'.

User Initiated	Abend S008	CICS DUMP SYSTEM=SHRMAS1 CODE=KENDUMP D=090000	Date and Time (GMT)	Sysplex Filter	System Filter	Problem Number Filter	Tracking ID Filter	Notes Filter
<input type="checkbox"/>	<input checked="" type="checkbox"/>	** MFUSR2 - TEST DUMP FOR USE WITH INCIDENT LOG MP=	Oct 8, 2014, 8:35:57 PM	SHARPLEX	S1			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	** MFUSR21 - TEST DUMP FOR USE WITH INCIDENT LOG MP=	Oct 8, 2014, 8:35:33 PM	SHARPLEX	S1	12345,123,123	TRKabc	PWR
<input type="checkbox"/>	<input checked="" type="checkbox"/>	** MFUSR20 - TEST DUMP FOR USE WITH INCIDENT LOG	Oct 8, 2014, 8:35:02 PM	SHARPLEX	S1			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	** MFUSR20 - TEST DUMP FOR USE WITH INCIDENT LOG	Oct 8, 2014, 8:34:38 PM	SHARPLEX	S1			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	** MFUSR20 - TEST DUMP FOR USE WITH INCIDENT LOG	Oct 8, 2014, 8:34:21 PM	SHARPLEX	S1	12345,123,123	TRKabc	PWR PWR
<input type="checkbox"/>	<input checked="" type="checkbox"/>	** MFUSR20 - TEST DUMP FOR USE WITH INCIDENT LOG MP=	Oct 8, 2014, 8:34:01 PM	SHARPLEX	S1			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	** MFUSR21 - TEST DUMP FOR USE WITH INCIDENT LOG MP=	Oct 8, 2014, 8:33:04 PM	SHARPLEX	S1	12345,123,123	TRKabc	PWR
<input type="checkbox"/>	<input checked="" type="checkbox"/>	** MFUSR20 - TEST DUMP FOR USE WITH INCIDENT LOG	Sep 30, 2014, 7:36:07 PM	SHARPLEX	S1	12345,123,123	TRKabc	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	CICS DUMP SYSTEM=SHRMAS1 CODE=KENDUMP D=090000	Jul 25, 2013, 10:40:26 PM	SHARPLEX	S1			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	** MFUSR20 - TEST DUMP FOR USE WITH INCIDENT LOG MP=	Jun 19, 2013, 2:55:18 PM	SHARPLEX	S1	12345	567	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	COMPN=CEA,COMP0=DCCEA,ISSUER=CEAMREC,MODU	May 9, 2013, 4:41:10 PM	SHARPLEX	S1			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	** MFUSR20 - TEST DUMP FOR USE WITH INCIDENT LOG MP=	May 8, 2013, 9:29:19 PM	SHARPLEX	S1	12345,123,123	TRKabc	Update the problem no and track

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.

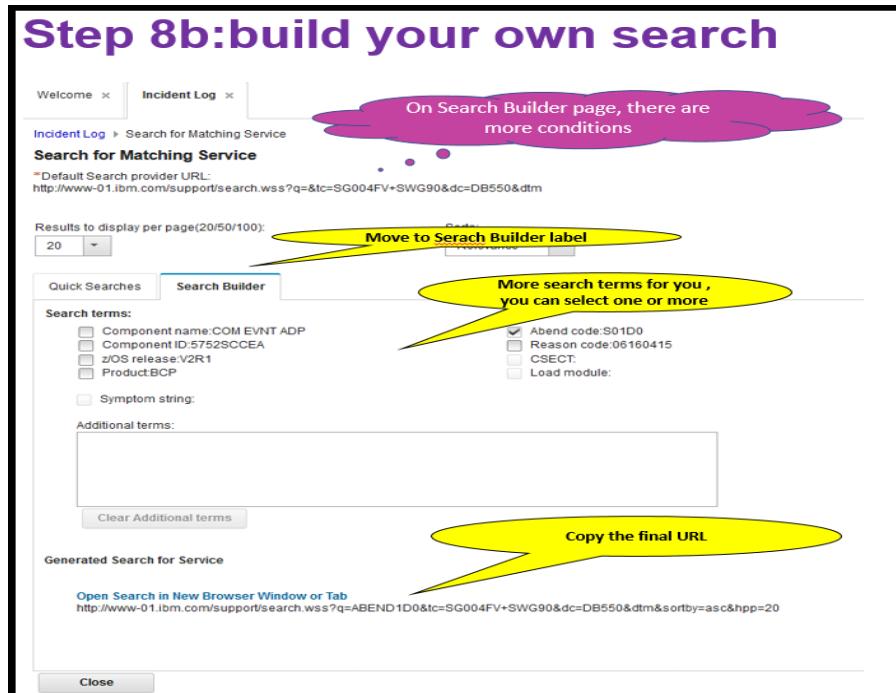


You can click the links to directly open search result. You can also copy the URL and open it with Browser to get corresponding APAR search results.

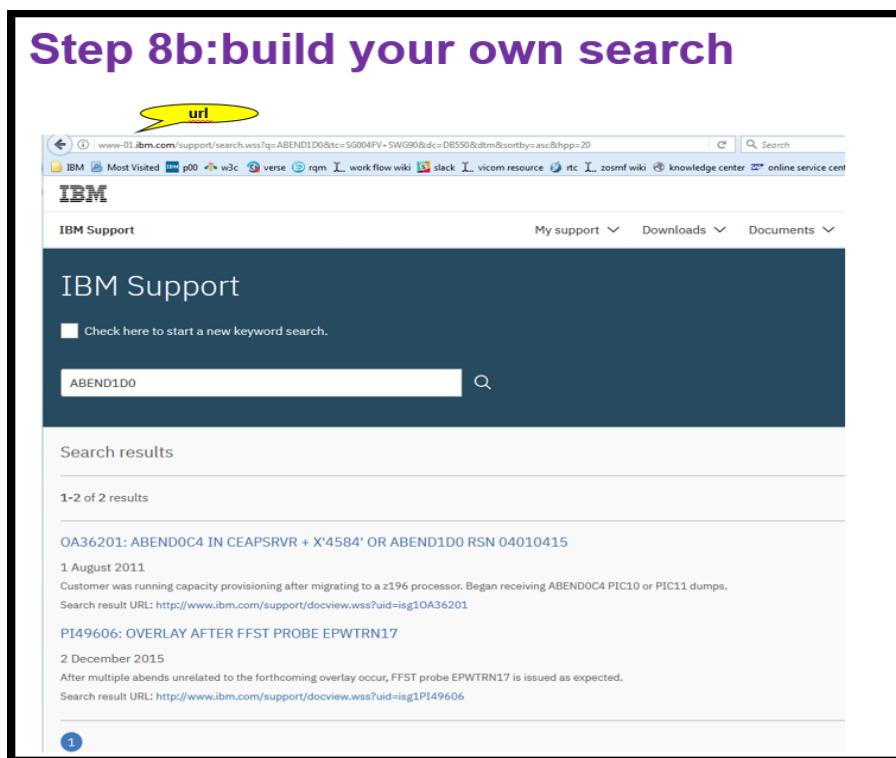


Step 8b: Build your own search

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.



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

Step 7: View FTP Servers

To get started, click on the Welcome tab

IBM z/OS Management Facility

Welcome x Incident Log x

Incident Log > FTP Job Status

FTP Job Status

Incident

Incident Type	Description	Date and Time (GMT)
User Initiated	** MFUSR30 - TEST DUMP FOR USE WITH INCIDENT LOG IPV **	Oct 8, 2014, 10:29:51 PM

Actions *

No filter applied

Data Type Filter	Source Filter	Status Filter	FTP Server Host Filter	FTP Server Path Filter
Error log summary	CEA.S00.CDE01236.A70B8910.X00 VEW	Failed. An error occurred with the FTP client.	ftp.ecupr.ibm.com	z0bmims
Operations log	CEA.Y00.CDE01236.A70B8910.X00 VEW	Failed. An error occurred with the FTP client.	ftp.ecupr.ibm.com	z0bmims
Error log	CEA.R00.CDE01236.A70B8910.X00 VEW	Failed. The diagnostic data was not gathered.	ftp.ecupr.ibm.com	z0bmims

Total: 16 Selected: 0

Refresh Last refresh: Feb 7, 2016, 10:34:02 AM local time (Feb 7, 2016, 2:34:02 AM GMT)

Step 7: View FTP Servers ...

Expand z/OSMF Settings

IBM z/OS Management Facility

Welcome to the z/OS Management Facility

The z/OS Management Facility (z/OSMF) provides a framework for managing various aspects of a z/OS system through a Web browser interface. By streamlining some traditional tasks and providing new management features, z/OSMF can help to simplify some areas of z/OS system management.

To learn more about z/OSMF, visit the links in the Learn More section.

To start managing your z/OS systems, select a task from the navigation area.

Learn More:

- What's New
- z/OSMF tasks at a glance
- Getting started with z/OSMF

Step 7: View FTP Servers ...

The screenshot shows the zOSMF interface with the 'Incident Log' option selected in the navigation menu. A yellow callout points to the 'Select FTP Servers' link in the main content area.

Step 7: View FTP Servers ...

A list of defined FTP servers is displayed. The zOSMF 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 in the zOSMF interface. The list includes the following entries:

Name	Activity	Rest	Path Name	Port Number	Description
BLI-ap-mvs	ftp.ap.ecurep.ibm.com	101m1mvs			
BLI-ap-bvol	ftp.ap.ecurep.ibm.com	101m1bvol			
BLI-ecurep-mvs	ftp.ecurep.ibm.com	101m1mvs			
BLI-ecurep-mvs-4tp	sftp.ecurep.ibm.com	101m1mvs			
BLI-ecurep-bvol-4tp	sftp.ecurep.ibm.com	101m1bvol			
BLI-testcase-mvs	testcase.boulder.ibm.com	101m1mvs			
BLI-testcase-mvs-4tp	testcase.boulder.ibm.com	101m1mvs			
BLI-testarea.html	testarea.boulder.ibm.com	101m1bvol			

Step 7: View FTP Servers ...

IBM z/OS Management Facility

Welcome sharc15 | Help

FTP Servers

Actions ▾

- Modify
- View
- Copy...
- Remove...
- Associate FTP Profile...
- Add...
- FTP Profiles
- Select All
- Deselected All
- Configure Columns...
- Hide Filter Row
- Clear Sorts
- Clear Cache
- IBM-testcase-mvs-ftp
- IBM-testcase-func

Activity Filter	Host Filter	Path Name Filter	Port Number Filter	Description Filter
	fp.ap.ecurep.ibm.com	/ibminvsi		
	fp.ap.ecurep.ibm.com	/ibminvsi		
	fp.ecurep.ibm.com	/ibminvsi		
	sftp.ecurep.ibm.com	/ibminvsi		
	fp.ecurep.ibm.com	/ibminvsi		
	sftp.ecurep.ibm.com	/ibminvsi		
	testcase.boulder.ibm.com	/ibminvsi		
	sftp.ecurep.ibm.com	/ibminvsi		
	testcase.boulder.ibm.com	/ibminvsi		
	testcase.boulder.ibm.com	/ibminvsi		

Total: 11 Selected: 1

Step 7: View FTP Servers ...

The properties of the FTP Server are displayed.

Welcome to Incident Log > Incident Log > View

View IBM-ecurep-mvs

FTP server name: IBM-ecurep-mvs

Transfer method:

- FTP
- SFTP (secure file based secure FTP)
- zOS Problem Documentation Upload Utility (Parallel FTP with optional encryption)

Host: fp.ecurep.ibm.com

Path name: /ibminvsi

Port number (must be between 1-65535):

FTP profile:

- Use the default profile. Currently the default FTP profile is No Firewall or Proxy
- Use the selected profile

Use anonymous user ID and password

Description:

Close

After reviewing, click Close

Step 8: View FTP Profiles

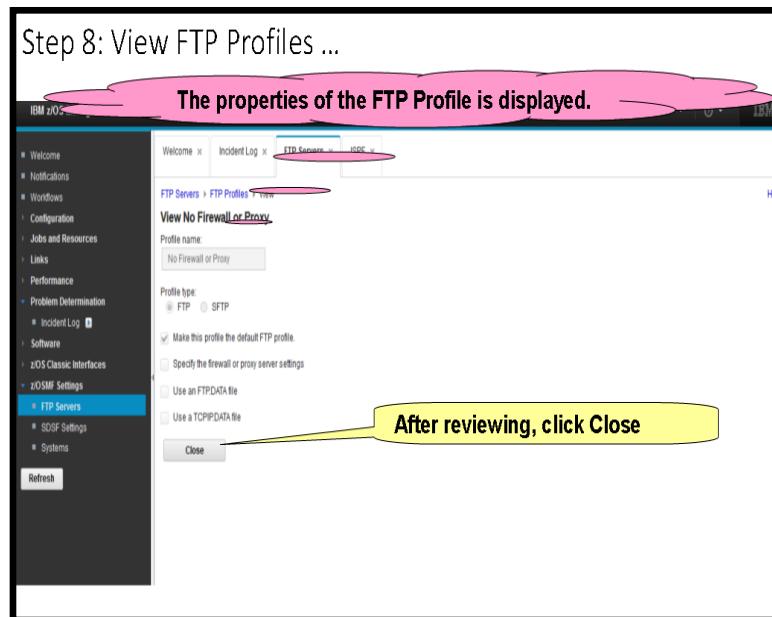
The screenshot shows the 'IBM z/OS Management Facility' interface. On the left, a navigation tree includes 'Welcome', 'Notifications', 'Workflows', 'Configuration', 'Jobs and Resources', 'Links', 'Performance', 'Problem Determination' (with 'Incident Log'), 'Software', 'z/OS Classic Interfaces', 'z/OSMF Settings', 'FTP Servers' (which is selected), 'SDSF Settings', and 'Systems'. A 'Refresh' button is at the bottom. In the center, a table titled 'FTP Servers' lists several entries. A yellow callout points to the 'Actions' dropdown menu for the first row, which contains options like 'Modify', 'View', 'Copy...', 'Remove...', 'Associate FTP Profile...', 'Add...', and 'FTP Profiles'. The 'FTP Profiles' option is highlighted. The table columns are 'Host', 'Path Name', 'Port Number', and 'Description'. The host column values are 'ftp.ecurep.ibm.com', 'sftp.ecurep.ibm.com', 'testcase.boulder.ibm.com', 'testcase.boulder.ibm.com', and 'nearNFS7.visiont.ibm.com'. The path name column values are 'hbmivs', 'hbmivs', 'hbmivs', 'hbmivs', and 'nearNFS7.visiont.ibm.com'. The port number column values are '21', '22', '21', '21', and '21'. The description column values are empty. At the bottom of the table, there is a note: 'Total: 11 Selected: 0'.

Click Actions, then FTP Profiles

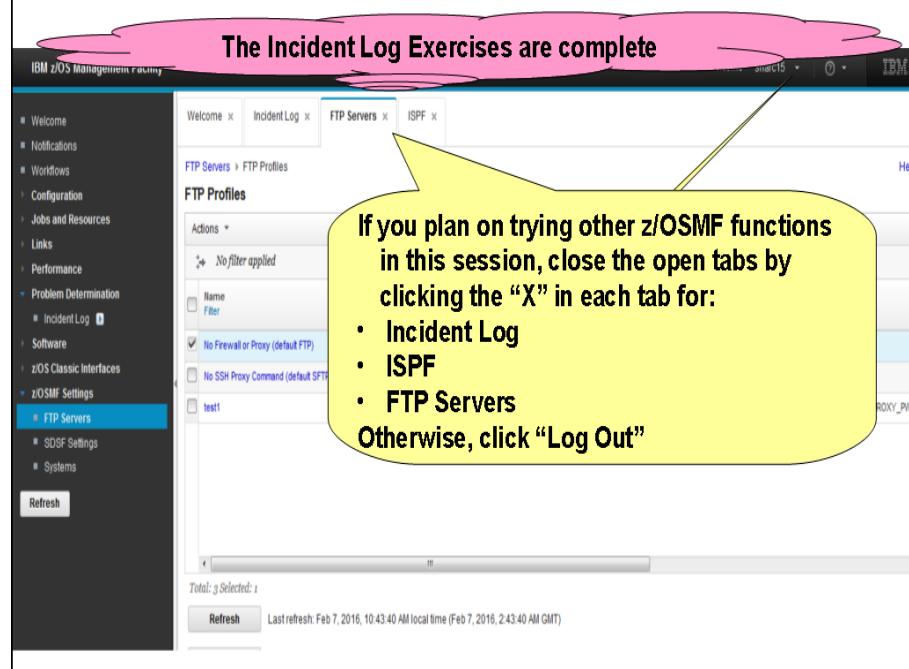
Step 8: View FTP Profiles ...

The screenshot shows the 'IBM z/OS Management Facility' interface. The navigation tree on the left is identical to the previous screenshot. In the center, a table titled 'FTP Profiles' lists three entries. A yellow callout points to the 'Name' column of the first row, which contains the value 'No Firewall or Proxy (default FTP)'. The table has columns for 'Name', 'Type', 'Activity', 'Firewall Host', 'Firewall User ID', 'Firewall Port', and 'Firewall Commands'. The 'Name' column values are 'No Firewall or Proxy (default FTP)', 'No SSH Proxy Command (default SFTP)', and 'test1'. The 'Type' column values are 'FTP', 'SFTP', and 'FTP'. The 'Activity' column values are empty. The 'Firewall Host' column values are 'aaa.bbb.com', 'zzzzzzzz', and 'aaa.bbb.com'. The 'Firewall User ID' column values are 'zzzzzzzz', '12345', and 'AUSER@AHOST'. The 'Firewall Port' column values are '21', '22', and '21'. The 'Firewall Commands' column values are empty. At the bottom of the table, there is a note: 'Total: 3 Selected: 0'.

Click on No Firewall or Proxy in the Name column



Finish the Lab



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 all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Microsoft 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