Lab Exercise: z/OSMF Incident Log

Session ID: Part of 17422 and 17909

Estimated Lab Time: 15-20 minutes

Abstract:

The z/OS Management Facility (z/OSMF) provides a web-based graphical interface for system programmers on z/OS. This hands-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 6 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

Optional tasks if you have time and interest

7. View FTP destinations
8. 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.
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 (SHARxnn) 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
1. Logon to zOSMF

Step 1: Log in to z/OSMF

- Launch the Mozilla Firefox browser
  - Note: If browser asks to add exception for certificate, do so
- Point Browser to z/OSMF – enter the following url
  - https://mvs1.centers.ihost.com/zosmf/
  - Note: Ignore and close the warning message
    - IZUG809W Unsupported Web browser version or level
      found: "3.8.13 (.NET CLR 3.5.30729)". Some z/OSMF
      functions might not be available if you continue.
- Login with SHARE userid/pw as provided by the lab instructor
  - Each workstation has been assigned a unique z/OS User ID
    - SHARxnn (where x is either A, B, or C; and nn is 01 - 30)
    - Password: to be provided
  - Each User ID has been authorized to all the z/OSMF applications
    (Plug-ins)

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.
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!
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 **1000 days**.
Step 3a: Change the Date Filter …

Change Amount to 1000

Then click OK

Step 3a: Change the Date Filter …

Now the list of 42 incidents are displayed on a table
**Step 3b: Sort the Columns**

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

![Step 3b: Sort the Columns](image)
### Step 3b: Sort the Columns...

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

Now the columns have a primary sort criteria (1) based on 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.
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.

![Image of Step 3c: Configure Columns]

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

Click Actions, then Configure Columns

Click “Sysplex”, then “< Remove”
Step 3c: Configure Columns ...

Now click “System”, then “< Remove”

Now you configure the order in which columns are displayed

Click “Component Name” then use the “Up” button to position it after Date and Time
Step 3c: Configure Columns …

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.
### 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

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, "**MFUSR30 – TEST DUMP FOR USE WITH INCIDENT LOG IVP**" if your User ID is SHARC30).
Step 4b: View Diagnostic Details of the 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; or click on the selection box and then select Actions, View Diagnostic Details; or right click on User Initiated and select View Diagnostic Details.

We'll start with the easiest option, so click on “User Initiated”
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 Data;
- or
- Right click on “User Initiated” in the Incident Type column to view a context sensitive list of Actions, then select View Diagnostic Data.

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.
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.

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, let's move on to the other tab - General.
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.

- Enter “12345,123,123” for problem number
- Optionally check to identify the number as an IBM PMR
- Then Enter “TRKabc” for the Tracking ID
- Optionally, enter any text for notes
- When you are done, click OK

You now see the additional information in the table display.
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 4d: Browse Diagnostic Data**

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

This time you will select Actions, then View Diagnostic Details.

**Step 4d: Browse Diagnostic Data ...**

You are then brought to ISPF Browse for the snapshot of the Operations Log. You can now perform normal ISPF commands to scroll or search the operations log.
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.
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 and ISPF tab if you didn't already have one open, and invoke browse in context for you.

**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.

Note: If you do not already have a z/OSMF ISPF session running, you will get prompted for the TSO Sign-on parameters.
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.
Step 4d: Browse Diagnostic Data ...

You are then brought to ISPF Browse for the snapshot of the Operations Log. You can now perform normal ISPF commands to scroll or search the operations log.
You will ultimately find yourself using ISPF Browse on the diagnostic data element that you had clicked on from the Incident Log!!

**Step 5: FTP the Diagnostic Data**

Now you will ftp the diagnostic data for the incident that you've been viewing.

First, click on the Incident Log tab
5. FTP the diagnostic data captured for an incident to your service provider

Step 5: FTP the Diagnostic Data...

Now you will be brought back to the Incident Log task. Next you will go back to your filtered lists of incidents.

Step 5a: Select an Incident

Now you will be brought back to the filtered list of incidents. Ensure that the user initiated incident that you’ve been viewing is selected in the table.
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.

**Step 5b: Send Diagnostic Data for the Incident**

Now you are presented a wizard to guide you through the process of sending diagnostic data.

After reviewing, click Next.
Step 5c: Select the FTP Server

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

Note: Next is not enabled until an FTP server is selected.
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 …**

Select the IBM_securl_mvs FTP Server

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

Then click Next
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.

**Step 5d: Specify Security Settings**

The next step is to specify the security settings. For this server you can use an anonymous user id, which is the default.

Just click Next

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.

**Step 5e: Select FTP Profile**

The next step is to select an FTP Profile. Here you could specify a Proxy. For this server you can specify No Firewall or Proxy, which is the default.

Just click 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.

**Step 5f: Define Job Setting**

The next step is to specify a JCL Job card. For this lab, you can just use what has been previously defined.

![Diagram showing the process of defining job settings for the FTP Job.](image)
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.

**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.

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

**Step 5g: Review the FTP Information**

After reviewing each tab, click Close.
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.

**Step 5g: Review the FTP Information ...**

The last step is to click Finish which will submit the ftp jobs.

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

**Step 5g: Review the FTP Information ...**

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.
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.
Optional Exercises

__ 7. View FTP Destinations
__ 8. 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

Expand z/OSMF Settings
Step 7: View FTP Servers ...

Select FTP Servers

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.
Step 7: View FTP Servers ...

First select the IBM-eurep-rws FTP Server

Then, click Actions, followed by View

The properties of the FTP Server are displayed.

After reviewing, click Close
Step 8: View FTP Profiles

Click Actions, then FTP Profiles

Click on No Firewall or Proxy in the Name column
Step 8: View FTP Profiles …

The properties of the FTP Profile is displayed.

After reviewing, click Close.

Finish the Lab

The Incident Log Exercises are complete

If you plan on trying other z/OSMF functions in this session, close the open tabs by clicking the “X” in each tab for:
- Incident Log
- ISPF
- FTP Servers
Otherwise, click “Log Out”

End of exercise
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

Thank You
Additional Information

Additional information

- z/OS Management Facility website
- IBM z/OS Management Facility Browser Compatibility
  - [http://www-03.ibm.com/systems/z/os/zos/features/zosmf/browser_notes.html](http://www-03.ibm.com/systems/z/os/zos/features/zosmf/browser_notes.html)
- z/OS Management Facility Publications
    - Program Directory for z/OS Management Facility (GH1-9847)
    - IBM z/OS Management Facility Configuration Guide (SA38-0557)
    - IBM z/OS Management Facility Programming (SA32-1066)
- z/OS Management Facility Resource Requirements
- z/OS Management Facility Downloads

Complete your session evaluations online at www.SHARE.org/Orlando-Eval

Continue growing your IBM skills

ibm.com/training provides a comprehensive portfolio of skills and career accelerators that are designed to meet all your training needs.

- Training in cities local to you - where and when you need it, and in the format you want
  - Use IBM Training Search to locate public training classes near you with our five Global Training Providers
  - Private training is also available with our Global Training Providers
- Demanding a high standard of quality - view the paths to success
  - Browse Training Paths and Certifications to find the course that is right for you
- If you can't find the training that is right for you with our Global Training Providers, we can help.
  - Contact IBM Training at dmnc@us.ibm.com

Complete your session evaluations online at www.SHARE.org/Orlando-Eval