

Reading and Interpreting S-Series System Log Files

This document describes the S-series server log files and how to read and interpret them. See [Change History](#) for a list of changes made to this document.

The subsystems log messages to the following files (for more information about a file, click the file name):

EMS Event Log Files

[\\$SYSTEM.ZLOGnn.ZZEVnnnn](#)

Description

The operator log file (\$0) used for some server subsystem and application EMS event messages. Used by OSM and TSM.

[\\$SYSTEM.ZLOGnn.ZZEVCONF](#)

The configuration file for the operator log (\$0) ZLOGnn subvols. Used by OSM and TSM.

[\\$SYSTEM.ZSERVICE.ZZSVnnnn](#)

Service (\$ZLOG) EMS event logs. Used by OSM and TSM.

[\\$SYSTEM.ZSERVICE.ZZSKnnnn](#)

Alternate key files for the ZZSVnnnn files. Used by OSM and TSM.

[\\$SYSTEM.ZSERVICE.ZZSVCONF](#)

The service EMS event log configuration file. Used by OSM and TSM.

Other System Log Files

[\\$SYSTEM.ZSERVICE.CPUHIST3](#)

A processor status log. Used by TSM.

[\\$SYSTEM.ZSERVICE.TSMERROR](#)

The TSM system resource model (SRM) error event log.

[\\$SYSTEM.ZSERVICE.ZZUSERS](#) and
[ZZUSERS2](#)

The current and previous TSM user log files.

[OSM\bin\startsys.log](#) and
[TSM\bin\startsys.log](#)

The low-level system startup messages log.

[Windows Event Viewer Application Log](#)

Application log for the Windows operating system. Used by OSM and TSM.

Other Related Files

[\\$SYSTEM.ZSERVICE.IAREPO](#)

A database file containing alarm history for alarms created by OSM.

[\\$SYSTEM.ZSERVICE.OSMCONF](#)

A text file containing configurable parameters for all OSM server processes.

[\\$SYSTEM.ZSERVICE.PERSIST](#)

A database of all current detailed TSM alarm objects, containing the level of detail seen in ZZAL* files, as well as pending incident report (IR) objects.

[\\$SYSTEM.ZSERVICE.PERSSUPP](#)

A database containing current TSM configuration information.

[\\$SYSTEM.ZSERVICE.SUPPREPO](#)

A database file containing dialout configuration information. Used by OSM.

[\\$SYSTEM.ZSERVICE.ZCT08153](#)

A catalog containing a table used by the TSM client software for converting alarm and IR binary values into text strings.

[\\$SYSTEM.ZSERVICE.ZCT08458](#)

A catalog used by the resource access layer (RAL) of TSM when reporting errors. It contains a table for converting binary values into text strings.

[\\$SYSTEM.ZSERVICE.ZZAAnnnn](#)

OSM alarm files.

[\\$SYSTEM.ZSERVICE.ZZALnnnn](#)

TSM server alarm files.

[\\$SYSTEM.ZSERVICE.ZZDCnnnn](#)

TSM inventory (snapshot) files.

[\\$SYSTEM.ZSERVICE.ZZPSnnnn](#)

Files containing processor scan strings. Used by OSM.

[\\$SYSTEM.ZSERVICE.ZZSNnnnn](#)

A text file containing a snapshot of the system at a particular time. Used by OSM.

[\\$SYSTEM.ZSERVICE.ZZSSnnnn](#)

Files containing processor scan strings. Used by TSM.

[\\$SYSTEM.ZSERVICE.ZTRC*](#)

Text files containing user trace logs. Used by OSM.

[\\$SYSTEM.ZSERVICE.ZTRC](#)

File containing a pointer to the current user trace log. Used by OSM.

EMS Event Logs

\$SYSTEM.ZLOGnn.ZZEVnnnn (\$0)

Customer applications and some NonStop S-series server subsystems write EMS event messages to the EMS collector process \$0 (the operator log). The \$0 log is normally located on the \$system.zlognn subvolume, where nn corresponds to the currently running SYSnn.

Notes:

- Operators can alter the volume used for log files.
- If you suspect that an operator has been switching between log file subvolumes, use the OSM or TSM Event Viewer Application to look for EMS file-switch events. You can use these events to trace your way back through all subvolumes.

These files are used by customers, field service engineers, and the Global Customer Support Center (GCSC) to diagnose problems.

To view messages in operator log (\$0), use the EMS event viewer of your choice:

- EMSA
- EMSDIST
- OSM or TSM Event Viewer. See [Viewing the Windows Event Viewer Application Log Using OSM or TSM](#)
- ViewPoint

Use the EMSCINFO collector information utility to display the current location

and status of the operator log (\$0) files. In the output, look for the Current Log File field to determine where events are currently being logged.

```
>EMSINFO $0, [DETAIL]
```

i **Note:** The DETAIL parameter option can be used to display additional information.

For more information about an event viewer, see the appropriate manual or online help. For more information about operator messages, refer to the Operator Messages Manual.

[Top](#)

\$SYSTEM.ZLOGnn.ZZEVCONF

ZZEVCONF files are configuration files that contain operator log (\$0) file tracking information. These files are defined by EMS collectors.

System operators and field service engineers use this information to monitor the \$0 log file status.

For more information about the Event Management System (EMS), see the EMS Manual.

[Top](#)

\$SYSTEM.ZSERVICE.ZZSVnnnn (\$ZLOG)

Most of the NonStop S-series server subsystems related to hardware log EMS event messages to this log. In some cases, messages are also sent to the \$0 operator log. Customers, service providers, and the GCSC use this log to help diagnose problems with the server hardware.

To view messages in \$ZLOG, use the EMS event viewer of your choice:

- EMSA
- EMSDIST
- OSM or TSM Event Viewer
- ViewPoint

i **Notes:**

- Operators can alter the volume used for log files.
- If you suspect an operator has been switching between log file volumes, use the OSM or TSM Event Viewer to look for EMS File-Switch events. You can use these events to trace your way back through all of the volumes.
- When printing from a \$ZLOG file, some events might be missing printing templates. Sometimes events contain additional information not visible in the template-printed form. You can use the DUMP ON option of EMSDIST (undocumented) to list all the tokens in an event.
- For more information about using the event viewers, see the appropriate manual or to the online help (if available).
- For information about how to interpret events, see the Operator

[Top](#)

\$SYSTEM.ZSERVICE.ZZSVCONF

ZZEVCONF files are configuration files that contain service log (\$ZLOG) file tracking information. These files are defined by EMS collectors.

System operators and service providers use this information to monitor the service log (\$ZLOG) file status.

For more information about the Event Management System (EMS), refer to the EMS Manual.

[Top](#)

\$SYSTEM.ZSERVICE.ZZSKnnnn


ZZSKnnnn files are alternate key files for the SSZV* files.

[Top](#)

Other System Log Files

\$SYSTEM.ZSERVICE.CPUHIST3

CPUHIST3 is a small binary file used by the TSM server process (\$ZTSM). If the processor running \$ZTSM fails or is halted, when \$ZTSM restarts, CPUHIST3 is used to keep track of which processors have been analyzed by TSM.

 **Note:** CPUHIST3 is only used when \$ZTSM goes offline and restarts. \$ZTSM is not a mirrored process.

[Top](#)

\$SYSTEM.ZSERVICE.TSMERROR

TSM system resource model (SRM) error messages are logged to the TSMERROR file. TSMERROR is a code 180 file that is opened automatically when the SRM is started. If the file is not present when SRM starts, then SRM creates the file.

The SRM is a collection of C++ objects that model the diagnostic and serviceability state behavior of the managed system resources.

TSMERROR is used by the GCSC and Development for debugging problems.

Use the CTOEDIT utility to copy the contents of this file to an EDIT (type 101) file, and then use TEDIT to open and read the EDIT file.

```
TA CL2>VOLUME $SYSTEM.ZSERVICE
TA CL3>CTOEDIT TSMERROR, TSMTRACE
TA CL4>TEDIT TSMTRACE
```

[Top](#)


\$SYSTEM.ZSERVICE.ZZUSERS and ZZUSERS2

The two TSM service application connection audit files in the \$SYSTEM.ZSERVICE subvolume are ZZUSERS and ZZUSERS2. ZZUSERS is always the active audit file. When the maximum number of records for the ZZUSERS file is reached, the ZZUSERS file is copied over to the ZZUSERS2 file, a new ZZUSERS file is opened, and logging activity is resumed.

These files are used by customers, service providers, the GCSC, or Development to determine:

- In RVUs prior to G06.02 without SPR T7945AAE:
 - User name
 - IP address
 - Date and time
- In G06.02 and later or if SPR T7945AAE is installed:
 - User name
 - IP address
 - Date and time
 - Action name
 - Action object
 - Object ID
 - Object type

Prior to G06.02 without SPR T7945AAE, you cannot view the ZZUSERS audit file while it is open. You must first stop the \$ZTSM process, create an edit file, copy ZZUSERS to the edit file, and then view the edit file using the editor or the FUP copy command, with no [out-filename] specified. The default [out-filename] displays the output on your screen. You can also specify a spooler as an output device and print the file or view it by using PERUSE.

 **Note:** While the temporary file does not have to be an edit file, an edit file is recommended. FUP can then copy ZZUSERS to the temporary file in a structured edit format ready for viewing. If the destination file is not an edit file, ZZUSERS is copied in an unstructured format without line breaks.

Example:

1. Use SCF to stop the \$ZTSM process.
2. Create a temporary edit file and copy ZZUSERS to the file:

```
>Edit TEMP; EXIT
>FUP COPY $SYSTEM.ZSERVICE.ZZUSERS, TEMP
```

3. Use SCF to start the \$ZTSM process.
4. View the temporary file (TEMP) using the editor or the FUP copy command:

```
>FUP COPY TEMP
```

You can use the FUP COPY command to view the ZZUSERS2 file.

If the system is running G06.02 RVU or later, or if SPR T7945AAE is installed, you do not have to stop the \$ZTSM process. You can copy the ZZUSERS file by using the SHARE option of the FUP COPY command:

```
>FUP/OUT TEMP/COPY $SYSTEM.ZSERVICE.ZZUSERS, , SHARE
>FUP COPY TEMP
```


[Top](#)

OSM\bin\startsys.log and TSM\bin\startsys.log

Detailed low-level system startup status messages are generated from the time you open the System Startup dialog box and appear in the Start System Status window. The log file is overwritten when a new startup session is initiated. This log file is useful for troubleshooting system startup problems.

For OSM, these messages are logged to the file C:\OSM\bin\startsys.log.

For TSM, these messages are logged to the file C:\TSM\bin\startsys.log.

 **Note:** If you experience problems during the system startup process, you should create a copy of the startsys.log file before initiating another system startup.

[Top](#)

Windows Event Viewer Application Log

The Windows event viewer has 3 logs: an Application log, a Security log, and a System log. You can view and manage all three logs.

OSM and TSM send error, information, and warning messages to the event logs. Each message contains:

Type	Type of message (error, warning, or information)
Date	The date the event message was created
Time	The time the event message was created
Source	The software that logged the event
Category	The classification of the event, as defined by the source
Event	A number that identifies the specific event
User	Text that matches what is entered in the user name field
Computer	The name of the computer where the logged event occurred

To view the Event Viewer Application Log:

For Windows XP Professional:

- On the taskbar, select **Start > Control Panel**, double-click **Performance and Maintenance**, double-click **Administrative Tools**, and then double-click **Event Viewer**. In the control tree pane, click the log you want to view.

For Windows 2000:

- On the taskbar, select **Start> Settings> Control Panel**, and double-click **Administrative Tools** and **Event Viewer**. In the control tree pane, click the log you want to view.

For Windows NT:

- On the taskbar, select **Start> Programs> Administrative Tools (Common)> Event Viewer**. In the control tree pane, click the log you want to view.

You can also view the Windows Event Viewer Application Log using the TSM service application or the OSM or TSM Low-Level Link Application. See [Viewing the Windows Event Viewer Application Log Using OSM or TSM](#).

Notes:

- Do not confuse the Windows Event Viewer Application Log with the OSM or TSM Event Log. The OSM and TSM Event Logs contain EMS event messages.
- From the Windows event viewer, you can peruse the event logs on other Windows workstations. See [Selecting Another Computer](#). See also the event viewer application online help. Start the event viewer and select **Actions>Help**.

Related topics:

- [Managing the Windows NT Event Viewer Application Log](#)
- [Managing the Windows Event Viewer Application Log](#)

[Top](#)

Other Related Files

\$SYSTEM.ZSERVICE.IAREPO

IAREPO is a database file containing alarm history for alarms created by the OSM incident analysis provider (IAPRVD).

[Top](#)

\$SYSTEM.ZSERVICE.OSMCONF

OSMCONF is a text file containing configurable parameters for all OSM server processes.

[Top](#)

\$SYSTEM.ZSERVICE.PERSIST

PERSIST is a database of all current detailed TSM alarm objects, containing the level of detail seen in ZZAL* files, and pending incident report (IR) objects.

In TSM application RVUs prior to G06.00, this file can become too large, due to old alarms that should have been deleted from the database. This problem can interfere with system discovery.

If this problem occurs, do the following:

1. Use the file utility program (FUP) to rename PERSIST to PERSOLD.
2. Stop \$ZTSM. Note that \$ZTSM restarts automatically and creates a new PERSIST file.

 **Note:** Undelivered IRs in PERSOLD will not be delivered.

[Top](#)

\$SYSTEM.ZSERVICE.PERSSUPP

PERSSUPP is a database that contains the current TSM software configuration information.

For G06.04 and later RVUs, PERSSUPP is created by the TSM Notification Director Application. For G06.03 and earlier RVUs, PERSSUPP is created by the TSM Configuration Application.

Development can use the information to assist with problem analysis related to the TSM software.

[Top](#)

\$SYSTEM.ZSERVICE.SUPPREPO

SUPPREPO is a database file containing dialout configuration information. This file is created and maintained by the OSM incident analysis provider (IAPRVD).

[Top](#)

\$SYSTEM.ZSERVICE.ZCT08153

This file is a catalog containing a table used by the TSM client for converting alarm and incident report (IR) binary values into text strings.

[Top](#)

\$SYSTEM.ZSERVICE.ZCT08458

This file is a catalog used by the TSM resource access layer (RAL) when reporting errors. It contains a table for converting binary values into text strings.

The RAL provides service clients with access to system resources in a system-independent manner.

[Top](#)

\$SYSTEM.ZSERVICE.ZZAAnnnn

ZZAAnnnn files are attachment files created for each OSM alarm. These files are created by the OSM incident analysis provider (IAPRVD).

The ZSERVICE.ZZAAnnnn files are generated when OSM incident analysis (IA) detects and generates alarms. Each ZZAAnnnn file contains one alarm. ZZAAnnnn files are text files with code 101, where nnnn is 0000 through 9999. The following information is logged: Resource Name, Description, Alert Type, Perceived Severity, Probable Cause, Creation Time and Repair Actions.

To view alarm messages:

1. Log on to the server using the OSM Service Connection.
2. On the toolbar select **Summary>Alarm**.

The Alarm Summary dialog box appears and displays a list of the current alarms.

3. For detailed information about an alarm message, select the message, and then click **Detail**. The Alarm Detail dialog box appears and displays:
 - Name of the resource associated with the alarm.
 - Whether the alarm dials out or not.
 - Time and date the alarm occurred.
 - Alarm type.
 - Description, severity and probable cause of the alarm.
 - Repair actions.

To clear an alarm:

On the Alarm Summary dialog box, select the alarm to be cleared, and then click **Delete**.

Notes:


- When a detected problem has been repaired, the alarm reporting that problem is cleared.
- In some cases, it is not possible to detect when an alarm condition has been repaired. After two weeks, these alarms are automatically cleared.

[Top](#)

\$SYSTEM.ZSERVICE.ZZALnnnn

The ZSERVICE.ZZALnnnn files are generated when analysis scripts in TSM detect and generate alarms. Each ZZALnnnn file contains one or more alarms. ZZALnnnn files are binary, type 180 files, where nnnn is 0000 through 9999. The following information is logged: resource name, event type, probable cause, specific problem, perceived severity, and problem detection time. Alarms can be augmented with the following information: additional text, analysis summary, correlated notifications, monitored attributes, repair actions, and ISO state.

To view alarm messages:

1. Log on to the server using the TSM Service Application.
2. On the toolbar, do one of the following:
 - Click **Alarms** or **Alarm Summary**  (depending on the TSM client version).
 - Select **Summary> Alarms**.

The Alarm Summary dialog box appears and displays a list of the

current alarms.

3. For detailed information about an alarm message, select the message, and then click **Show detail** or **Detail** (depending on the TSM client version). The Alarm Detail dialog box appears and displays:
 - Name of the resource associated with the alarm.
 - Time and date the alarm occurred.
 - Event type.
 - Description of the alarm, including perceived severity, probable cause, and specific problem of the alarm.
 - State information, including the state of the resource before and after the alarm, the current severity trend, and the name of the backup resource.
 - Repair action, which lists in priority order the steps to follow to correct the problem. For TSM client Version 7.0 and later, you must click the **Repair Actions** or **Repair Steps** button to view repair actions (depending on your client software version). This button is available only if value-added diagnostics are enabled for the system object.

To clear an alarm:

In the **Alarm Summary** dialog box, select the alarm to be cleared, and click **Delete**.

Notes:

- When a detected problem has been repaired, an alarm with a cleared perceived severity is generated to clear the alarm from the outstanding list of alarms.
- In some cases, it is not possible to detect when an alarm condition has been repaired. After two weeks, these alarms are automatically cleared.

[Top](#)

\$SYSTEM.ZSERVICE.ZZDCnnnn

ZSERVICE.ZZDCnnnn (dynamic configuration file (DCF)) files contain snapshots of a NonStop S-series server's resources and configuration, such as disk logical names, firmware revision levels, and so on, at the time the snapshot was made. TSM snapshot files are located in the \$SYSTEM.ZSERVICE subvolume.

A DCF file is a binary type 180 file, where nnnn is a sequential number from 0000 through 9999. Each time a problem incident report (IR) is generated, a DCF file is created and sent as an attachment along with the IR to the GCSC.

The GCSC can use this file to help identify the source of the problem that caused the IR to be generated.

The GCSC uses the TSM Service Application to view DCF files. You can also use the TSM Low-Level Link Application to view DCF files.

To load a snapshot:

1. Open the TSM Service Application or TSM Low-Level Link Application, but do not log on to the server.
2. Select **File> Load snapshot**. If you are logged on to a server, a dialog box will appear asking if you want to terminate that connection. To continue, click **Yes**. The Load Snapshot dialog box appears.
3. From the **Snapshot File** list, select the system name. If the system you want to load does not appear in the Snapshot File list, a snapshot has never been created for that server.
4. Click **Load**. The snapshot is loaded and this dialog box is closed. (You can also double-click the system name to load a snapshot.)

Notes:

- You must use FTP to transfer the DCF file to the TSM workstation before it can be viewed.
- After you load a snapshot, the only way to close or unload it is to load a new snapshot or log on to a NonStop S-series server.
- You cannot be logged on to a server and have a snapshot loaded at the same time.
- You cannot have two snapshots loaded at the same time. If you already have a snapshot loaded, it closes when you load a new snapshot.
- The DCF file is sent automatically, using file transfer protocol (FTP), to the GCSC each time a problem IR is sent out.

[Top](#)

\$SYSTEM.ZSERVICE.ZZPSnnnn

ZZPSnnnn files contain processor scan strings binary files created by the OSM resource access layer provider (RALPRVD). When a hardware error freeze (HEF) is detected or a hung processor is forced to freeze, CPU incident analyzer (CPUIA) collects the scan strings on mips interface to equalizer ASICs (MITEs), the online access port (OLAP) history register, revisions of boards, and scan string information (similar to the CPUMON7 process on K-series servers). These files are sent to the GCSC along with problem incident reports (IRs).

GCSC and Development use the in-house Beguile tool to view the contents of these files for further analysis.

[Top](#)

\$SYSTEM.ZSERVICE.ZZSNnnnn

ZZSNnnnn files are text files containing snapshots of the system at particular times. These files are created by the OSM incident analysis provider (IAPRVD).

A ZZSNnnnn file is created when:

- The CIMOM process is started or restarted.

- A problem IR is created and another ZZSNnnnn file has not been created in the last 24 hours.
- When a periodic IR is created (every 14 days).
- When periodic IR is generated because of a user request from the Notification Director.

The GCSC can use this file to help identify the source of the problem that caused the IR to be generated.

To load a snapshot:

1. FTP the ZZSNnnnn file from the server to your workstation.
2. Start a new browser session.
3. In the address bar, enter the URL of an OSM service connection, followed by "snapshot/index.html." For example:
http://mysystem.lab.corp.net:9990/snapshot/index.html. This URL can be any valid service connection. It does not have to be the same system as the snapshot file you want to load. The Load Snapshot dialog box appears.
4. Navigate to the snapshot file you want to open and click **Open**.

Notes:

- You must use FTP to transfer the snapshot file to your workstation before it can be viewed.
- You can not use the same browser window to load a new snapshot or to start a new service connection.
- To close the snapshot or service connection, you must close the browser window.
- You cannot be logged on to a server and have a snapshot loaded at the same time in the same window. However, you can be logged on to a server and view a snapshot by opening two separate browser windows.

To save a snapshot:

1. Select **Tools>Save Snapshot**.
2. In the Save Snapshot dialog box, click **Save**.

This action saves the snapshot file on the workstation in the folder C:\ZSupport\OSM. The name of the snapshot file is based on the name of the server and the date and time the snapshot was taken. Optionally, in the Save Snapshot dialog box, you can change both the file name and the destination folder for the snapshot.

[Top](#)

\$SYSTEM.ZSERVICE.ZZSSnnnn

ZZSSnnnn files are processor scan string binary files created by TSM. When a hardware error freeze (HEF) is detected or a hung processor is forced to freeze, CPU incident analyzer (CPUIA) collects the scan strings on mips interface to equalizer ASICs (MITEs), the online access port (OLAP) history

register, revisions of boards, and scan string information (similar to the CPUMON7 process on K-series servers). These files are sent to the GCSC along with problem incident reports (IRs).

GCSC and Development use the in-house Beguile tool to view the contents of these files for further analysis.

[Top](#)

\$SYSTEM.ZSERVICE.ZTRC*

ZTRC* files are text files containing user trace logs. These files are created and maintained by the main server process for OSM: the common information model object manager (CIMOM).

[Top](#)

\$SYSTEM.ZSERVICE.ZTRC

The ZTRC file contains a pointer to the current user trace log. This file is created and maintained by the OSM CIMOM.

[Top](#)

\$SYSTEM.ZOSM.ADDTCPIP

ADDTCPIP is an SCF command file that configures \$ZTCP0 and \$ZTCP1 as persistent processes.

[Top](#)

\$SYSTEM.ZOSM.ADDTOSCF

ADDTOSCF is an SCF command file that configures all OSM server processes as persistent processes.

[Top](#)

\$SYSTEM.ZOSM.ALTERIP

ALTERIP is an SCF command file that restarts the \$ZTCP0 and \$ZTCP1 processes such that they are configured using CTCPIP0 and CTCPIP1 instead of INIT0 and INIT1.

[Top](#)

\$SYSTEM.ZOSM.CTCPIP0/1

CTCPIP0 and CTCPIP1 are SCF command files that configure the \$ZTCP0 and \$ZTCP1 processes to use IP addresses other than the default IP addresses.

[Top](#)

\$SYSTEM.ZOSM.INIT0/1

INIT0 and INIT1 are SCF command files that start the \$ZTCP0 and \$ZTCP1 processes using the factory-default IP addresses.

[Top](#)

\$SYSTEM.ZOSM.LOGSCF

LOGTSCF is a trace log created when the the ALTERIP command file is executed.

[Top](#)

\$SYSTEM.ZOSM.LOGTCP0/1

LOGTCP0 is a trace log created when the the CTCPIP0 or INIT0 command file is executed.

LOGTCP1 is a trace logs created when the CTCPIP1 or INIT1 command file is executed.

[Top](#)

\$SYSTEM.ZOSM.LOGTCPIP

LOGTCPIP is a trace log created when the ADDTCPIP command file is executed.

[Top](#)

\$SYSTEM.SYSnn.CIMREPO

CIMREPO is a database file that contains the Document Management Task Force Common Information Model (DMTF CIM) class information for all the classes used by OSM. Used by CIMOM and the OSM service connection client software.

[Top](#)

\$SYSTEM.SYSnn.RAREPO

RAREPO is a database file that contains the OSM repair actions in XML format. This file is used by RALPRVD.

[Top](#)

\$SYSTEM.SYSnn.APPFLMAP


APPFLMAP is a text file that contains a mapping of client file names to operating system files. This file is used by the OSM applet provider (APPRVD).

Related Topic: [Gathering, Packaging, and Sending Files to the GCSC for Analysis](#)

Viewing the Windows Event Viewer Application Log Using OSM or TSM

Using the TSM Service Application or the OSM or TSM Low-Level Link:

- Select **Summary>Status Log**, or
- After system discovery is complete, on the toolbar,

- In OSM, click 

- In TSM, depending on the TSM client version, click **Status Log** or 


For detailed information about an event message, double-click on an event. The Event Detail dialog box appears and displays detailed information.

Notes:

- There is no link to the Windows Event Viewer application log from the OSM Service Connection.
- Do not confuse the Windows Event Viewer Application Log with the OSM or TSM Event Log. The OSM and TSM Event Logs contain EMS event messages and can be accessed using the OSM or TSM Event Viewer.
- From the Windows Event Viewer, you can peruse the event logs on other Windows workstations. See [Selecting Another Computer](#). See also the Windows Event Viewer application online help. Start the viewer and select **Actions>Help**.

Selecting Another Computer

- 1 Select **Start>Run**, type **mmc**, and click **OK**.
- 2 Select **Console>Add/Remove Snap-in**. The Add/Remove Snap-in window appears.
- 3 On the Standalone tab, click **Add**. The Add Standalone Snap-in window appears.
- 4 Select **Event Viewer** and click **Add**. The Select Computer dialog box appears.
- 5 Click **Another Computer**, and then enter the path and name of the computer, for example, \\domain name\computer name.
- 6 Click **Finish**, click **Close**, and then click **OK**.

-  **Notes:**
- If Step 1 does not open a Microsoft Management Console (MMC) window, MMC might not be available on your computer. If an MMC window opens, but the console menu or the Add/Remove Snap-in command is not available, MMC is running in user mode, and snap-ins cannot be added or removed. For more information, see related topics in the Event Viewer online help or contact your network administrator.
 - The other computer can be a workstation running Windows XP Professional, Windows 2000 Professional, or Windows NT workstation; a server or domain controller running Windows XP, Windows 2000, or Windows NT server; or a LAN Manager 2.x server.
 - If the new computer requires a low-speed connection, right-click the log you want to view, and then click **Properties**. On the **General** tab, click **Low Speed Connection**.

Related Topics:

In Event Viewer online help:


- Add another view of an event log
- Event Viewer overview
- Research an event log
- Search for specific types of events
- View more details about an event log

Select **Start> Settings> Control Panel> Administrative Tools> Event Viewer> Action> Help** and search for topic.

Gathering, Packaging, and Sending Files to the GCSC For Analysis

When reporting problems, package and send the appropriate information to the Global Customer Support Center (GCSC) for analysis. The information you collect will be based on the problem being reported. Following are examples of the types of information you will need to collect.

1. Create a readme file that describes what you were doing at the time the error occurred and just prior to that time. Include the following information (as appropriate):
 - VPROC information for related object files
 - Current version of the operating system, service processor (SP) firmware, and related applications
 - SCF INFO for \$SYSTEM.ZSYSCONF.CONFIG and CONFSAVE
 - Any other information required by the GCSC or Development for analysis
2. If any files are to be collected from the system console, such as trace files, copy the files to a temporary directory on the workstation.
3. Use the NonStop systems FTP client, called FTPC32, to copy the temporary directory from the workstation to a temporary subvolume on the S-series server. (See Using FTP to Move Structured Files Without Causing Corruption.)
4. On the S-series server, assemble copies of all requested server files into the temporary subvolume.
5. Use the TN SCPAK utility to create a backup of these files that can be transferred, using e-mail, FTP, and other binary methods, to the GCSC. See Support Note 98052A for more information about obtaining and using the TN SCPAK utility.
 - If the TN SCPAK file is less than 2 megabytes, you can e-mail it to the GCSC analyst.
 - If the TN SCPAK file is larger than 2 megabytes, you can use FTP to send it to the GCSC's anonymous FTP site:
FTP.AUSTX.TANDEM.COM/pub/in.coming/<special-name> (Use the following naming conventions to determine <special-name>.)

 **Note:** It is possible to save only the relevant portion of an event log to a file for transmittal to the GCSC. Before doing this, check with the GCSC.

Naming convention for TN SCPAK and anonymous FTP pub/in.coming files:

Use the two letter mnemonic for the month, plus the last 6 digits of the Genesis case number:

Month mnemonics are: JA FE MR AP MY JU JY AG SE OC NO DE

Example: Case 10-970321-1243 would have the directory name:

MR211243 (If self-extracting, use extension .100. If non-self-extracting, use extension .1729.)

Mailing address for Federal Express tape delivery is:

HP Computers, Incorporated

Attn: Operations (Case #:10-nnnnnn-nn)

14231 Tandem Boulevard

Austin, TX 78728-6699

Related topic: Product Specific Information Gathering for Analysis

Change History for Reading and Interpreting S-Series System Log Files

September 24, 2003

Added information about OSM server files.

May 21, 2003

Updated instructions for using FUP copy to create an edit file and view the ZZUSERS file on systems prior to G06.02 without SPR T7945AAE.

February 7, 2003

Updated topic for Windows NT and Windows 2000 Professional.