



IBM Multi-site Workload Lifeline V1.1 User's Guide

Version 1 Release 1

Note:

Before using this information and the product it supports, be sure to read the general information under “Notices” on page 145.

Second Edition (December 2011)

This edition applies to Version 1 Release 1 of IBM Multi-site Workload Lifeline (5655-U24).

IBM welcomes your comments. You may send your comments to the following address.

International Business Machines Corporation
Attn: z/OS Communications Server Information Development
Department AKCA, Building 501
P.O. Box 12195, 3039 Cornwallis Road
Research Triangle Park, North Carolina 27709-2195

You can send us comments electronically by using one of the following methods:

Fax (USA and Canada):

1+919-254-1258

Send the fax to “Attn: z/OS Communications Server Information Development”

Internet email:

comsvrcf@us.ibm.com

World Wide Web:

<http://www.ibm.com/systems/z/os/zos/webqs.html>

If you would like a reply, be sure to include your name, address, telephone number, or FAX number. Make sure to include the following in your comment or note:

- Title and order number of this document
- Page number or topic related to your comment

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright IBM Corporation 2011.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures	vii
Tables	ix
About this document	xi
Who should read this document	xi
How this document is organized	xi
How to use this document	xi
Determining whether a publication is current	xii
How to contact IBM service	xii
Conventions and terminology that are used in this document	xii
How to read a syntax diagram.	xiii
How to send your comments	xvi
Summary of changes	xvii
Chapter 1. Overview of Multi-site Workload Lifeline	1
Lifeline Advisors	3
Lifeline Agents	4
External load balancers	4
Internal load balancers	6
Chapter 2. Preparing to use Multi-site Workload Lifeline	7
Granting users explicit authority to control the Lifeline Advisor and Agent	7
Authorizing the Lifeline Advisors to use BCPii	8
Authorizing the Lifeline Agents to use WLM services.	9
Authorizing the Lifeline Agents to reset active connections	9
Chapter 3. Configuring Multi-site Workload Lifeline	11
Lifeline Advisor configuration file	11
Lifeline Agent configuration file	11
Configuring one Lifeline Advisor as the primary Advisor, and optionally one as the secondary Advisor	12
Configuring a Lifeline Agent	14
WLM recommendations	15
Configuring Lifeline Advisors to automatically restart	15
Recovering from a planned outage of the TCP/IP stack	16
Recovering from an unplanned outage of the TCP/IP stack	17
Configuring Lifeline Agents to automatically restart	17
Using the Base Control Program Internal Interface	18
Configuring and starting syslogd	18
Customizing the TCP/IP profiles of the TCP/IP stacks	19
CINET considerations	20
Configuring external load balancers	20
Configuring first-tier external load balancers	20
Configuring second-tier external load balancers	21
Configuring second-tier internal load balancers	23
Chapter 4. Starting the Lifeline Advisors and Agents	25
Chapter 5. Diagnosing problems in Multi-site Workload Lifeline	27
Debug levels	27
Diagnostic data	28
Verifying that the Lifeline Advisor and Agent systems are functioning correctly	29

Diagnosing problems when a workload is not distributed	30
Diagnosing workload distribution problems	32
Diagnosing problems when the Lifeline Advisor or Agent appears hung	33
Diagnosing problems when the group names are not readable	33
Diagnosing problems when load balancer connection terminates	34
Diagnosing problems when the Lifeline Agent connection terminates	34
Diagnosing problems when the Lifeline Advisor to Advisor connection terminates	35
Diagnosing failures of registering with ARM	35

Chapter 6. Multi-site Workload Lifeline configuration statements 37

Lifeline Advisor configuration statements	37
advisor_connection_port	38
advisor_id_list	38
advisor_takeover_policy	39
advisor_timeout	39
agent_connection_port	40
agent_id_list	40
cross_sysplex_list	41
debug_level	42
failure_detection_interval	43
lb_connection_v4	43
lb_connection_v6	44
lb_id_list	45
peer_advisor_id	45
update_interval	46
workload_switch_policy	47
Lifeline Agent configuration statements	48
advisor_id	48
advisor_id_list	49
debug_level	49
host_connection	50

Chapter 7. Lifeline Advisor commands 53

MODIFY <i>advisor_proc</i> ,DISPlay command: Display Lifeline Advisor information	53
MODIFY <i>advisor_proc</i> ,ACTivate command: Activate workloads	66
MODIFY <i>advisor_proc</i> ,DEACTivate command: Deactivate workloads	67
MODIFY <i>advisor_proc</i> ,DEBUg command: Change the debug level	68
MODIFY <i>advisor_proc</i> ,QUIESCE command: Quiesce workloads	69
MODIFY <i>advisor_proc</i> ,REFRESH command: Update configuration	70
MODIFY <i>advisor_proc</i> ,TAKEOVER command: Take over primary Advisor responsibilities	70

Chapter 8. Lifeline Agent commands 73

MODIFY <i>agent_proc</i> ,DISPlay command: Display Lifeline Agent information	73
MODIFY <i>agent_proc</i> ,ENABLe command: Enable server applications	78
MODIFY <i>agent_proc</i> ,QUIESCE command: Quiesce server applications	80
MODIFY <i>agent_proc</i> ,DEBUg command: Change the debug level	83

Chapter 9. Network management interface for Multi-site Workload Lifeline 85

NMI message format	87
------------------------------	----

Chapter 10. Multi-site Workload Lifeline messages 91

Appendix A. A sample started procedure for Lifeline Advisors 133

Appendix B. A sample started procedure for Lifeline Agents 135

Appendix C. Sample configuration statements 137

Appendix D. Accessibility 143

Notices	145
Policy for unsupported hardware.	147
Trademarks	147
Index	149
Communicating your comments to IBM	153

Figures

1.	Relationships between external load balancers, Lifeline Advisors, and Lifeline Agents	2
2.	Flow between the Lifeline NMI and the network management application	85
3.	Layout of the data response message	86
4.	Sample started procedure AQSADV	133
5.	Sample started procedure AQSAGE	135
6.	Multi-site Workload Lifeline configuration example	137
7.	Sample configuration statements for the Lifeline Advisor	139
8.	Sample configuration statements for the Lifeline Agent	140

Tables

1.	Lifeline Advisor Configuration Statements	37
2.	Lifeline Agent Configuration Statements	48

About this document

This document describes how to use IBM® Multi-site Workload Lifeline to load balance TCP/IP workload requests across two sites at unlimited distances when both sites run the same server applications and have the same data sources.

Who should read this document

This document is written for system administrators who need to understand how to load balance TCP/IP workload requests.

How this document is organized

This document contains the following information:

- "Chapter 1. Overview of Multi-site Workload Lifeline" introduces the concept of Lifeline Advisors, Lifeline Agents, external load balancers, and internal load balancers.
- "Chapter 2. Preparing to use Multi-site Workload Lifeline" contains the information about the tasks that you need to perform before you can configure Multi-site Workload Lifeline.
- "Chapter 3. Configuring Multi-site Workload Lifeline" contains the information about the tasks to configure Multi-site Workload Lifeline.
- "Chapter 4. Starting the Lifeline Advisors and Agents" contains the information about how to start the Lifeline Advisors and Agents that make up Multi-site Workload Lifeline.
- "Chapter 5. Diagnosing problems in Multi-site Workload Lifeline" contains the information that you need to diagnose problems.
- "Chapter 6. Multi-site Workload Lifeline configuration statements" describes the configuration statements of the Lifeline Advisors and Agents.
- "Chapter 7. Lifeline Advisor commands" describes the commands that you can use to display Lifeline Advisor information and modify Lifeline Advisor state information.
- "Chapter 8. Lifeline Agent commands" describes the commands that you can use to display Lifeline Agent information and modify Lifeline Advisor state information.
- "Chapter 9. Network management interface for Multi-site Workload Lifeline" describes the network management interface (NMI) that you can use to monitor Lifeline metrics and statistics.
- "Chapter 10. Multi-site Workload Lifeline messages" contains the Multi-site Workload Lifeline messages.
- "Accessibility" describes accessibility features to help users with physical disabilities.
- "Notices" contains notices and trademarks used in this document.

How to use this document

To use this document, you should be familiar with z/OS® TCP/IP Services and the TCP/IP suite of protocols.

Determining whether a publication is current

As needed, IBM updates its publications with new and changed information. For a given publication, updates to the hardcopy and associated BookManager® softcopy are usually available at the same time. Sometimes, however, the updates to hardcopy and softcopy are available at different times. The following information describes how to determine if you are looking at the most current copy of a publication:

- At the end of a publication's order number there is a dash followed by two digits, often referred to as the dash level. A publication with a higher dash level is more current than one with a lower dash level. For example, in the publication order number GC28-1747-07, the dash level 07 means that the publication is more current than previous levels, such as 05 or 04.
- If a hardcopy publication and a softcopy publication have the same dash level, it is possible that the softcopy publication is more current than the hardcopy publication. Check the dates shown in the Summary of Changes. The softcopy publication might have a more recently dated Summary of Changes than the hardcopy publication.
- To compare softcopy publications, you can check the last two characters of the publication's file name (also called the book name). The higher the number, the more recent the publication. Also, next to the publication titles in the CD-ROM booklet and the readme files, there is an asterisk (*) that indicates whether a publication is new or changed.

How to contact IBM service

For immediate assistance, visit this Web site: http://www.ibm.com/support/entry/portal/Overview/Software/Other_Software/z~OS_Communications_Server/

Most problems can be resolved at this Web site, where you can submit questions and problem reports electronically, as well as access a variety of diagnosis information.

For telephone assistance in problem diagnosis and resolution (in the United States or Puerto Rico), call the IBM Software Support Center anytime (1-800-IBM-SERV). You will receive a return call within 8 business hours (Monday – Friday, 8:00 a.m. – 5:00 p.m., local customer time).

Outside the United States or Puerto Rico, contact your local IBM representative or your authorized IBM supplier.

If you would like to provide feedback on this publication, see “Communicating your comments to IBM” on page 153.

Conventions and terminology that are used in this document

Samples used in this book might not be updated for each release. Evaluate a sample carefully before applying it to your system.

For definitions of the terms and abbreviations that are used in this document, you can view the latest IBM terminology at the IBM Terminology Web site.

Clarification of notes

Information traditionally qualified as **Notes** is further qualified as follows:

Note Supplemental detail

Tip Offers shortcuts or alternative ways of performing an action; a hint

Guideline

Customary way to perform a procedure

Rule Something you must do; limitations on your actions

Restriction

Indicates certain conditions are not supported; limitations on a product or facility

Requirement

Dependencies, prerequisites

Result Indicates the outcome

How to read a syntax diagram

This syntax information applies to all commands and statements that do not have their own syntax described elsewhere.

The syntax diagram shows you how to specify a command so that the operating system can correctly interpret what you type. Read the syntax diagram from left to right and from top to bottom, following the horizontal line (the main path).

Symbols and punctuation

The following symbols are used in syntax diagrams:

Symbol

Description

- ▶▶ Marks the beginning of the command syntax.
- ▶ Indicates that the command syntax is continued.
- | Marks the beginning and end of a fragment or part of the command syntax.
- ◀◀ Marks the end of the command syntax.

You must include all punctuation such as colons, semicolons, commas, quotation marks, and minus signs that are shown in the syntax diagram.

Parameters

The following types of parameters are used in syntax diagrams.

Required

Required parameters are displayed on the main path.

Optional

Optional parameters are displayed below the main path.

Default

Default parameters are displayed above the main path.

Parameters are classified as keywords or variables. For MVS™ console commands, the keywords are not case sensitive. You can code them in uppercase or lowercase. If the keyword appears in the syntax diagram in both uppercase and lowercase, the uppercase portion is the abbreviation for the keyword (for example, OPERand).

For the z/OS UNIX commands, the keywords must be entered in the case indicated in the syntax diagram.

Variables are italicized, appear in lowercase letters, and represent names or values you supply. For example, a data set is a variable.

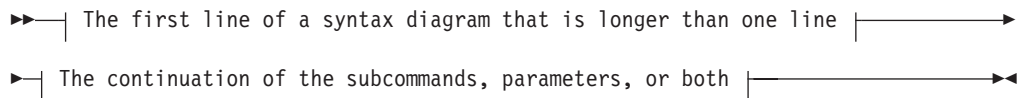
Syntax examples

In the following example, the USER command is a keyword. The required variable parameter is *user_id*, and the optional variable parameter is *password*. Replace the variable parameters with your own values.



Longer than one line

If a diagram is longer than one line, the first line ends with a single arrowhead and the second line begins with a single arrowhead.



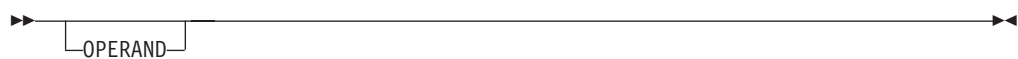
Required operands

Required operands and values appear on the main path line. You must code required operands and values.



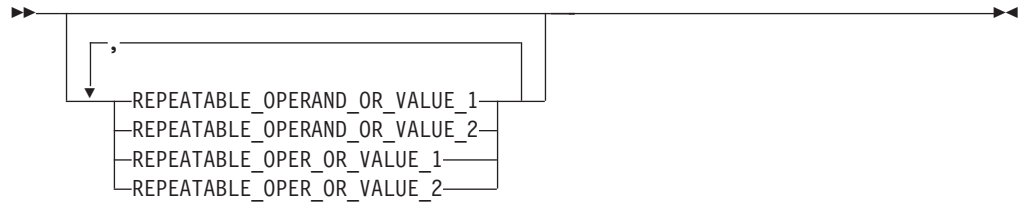
Optional values

Optional operands and values appear below the main path line. You do not have to code optional operands and values.



Selecting more than one operand

An arrow returning to the left above a group of operands or values means more than one can be selected, or a single one can be repeated.



Nonalphanumeric characters

If a diagram shows a character that is not alphanumeric (such as parentheses, periods, commas, and equal signs), you must code the character as part of the syntax. In this example, you must code OPERAND=(001,0.001).



Blank spaces in syntax diagrams

If a diagram shows a blank space, you must code the blank space as part of the syntax. In this example, you must code OPERAND=(001 FIXED).



Default operands

Default operands and values appear above the main path line. Multi-site Workload Lifeline uses the default if you omit the operand entirely.



Variables

A word in all lowercase italics is a *variable*. Where you see a variable in the syntax, you must replace it with one of its allowable names or values, as defined in the text.



Syntax fragments

Some diagrams contain syntax fragments, which serve to break up diagrams that are too long, too complex, or too repetitious. Syntax fragment names are in mixed case and are shown in the diagram and in the heading of the fragment. The fragment is placed below the main diagram.



Syntax fragment:

|—1ST_OPERAND—,—2ND_OPERAND—,—3RD_OPERAND—|

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. If you have any comments about this document or any other z/OS Communications Server documentation, do one of the following:

- Go to the z/OS contact page at <http://www.ibm.com/systems/z/os/zos/webqs.html>. You can enter and submit your comments in the form provided at this Web site.
- Send your comments by e-mail to comsvrcf@us.ibm.com. Be sure to include the name of the document, the part number of the document, the version of z/OS Communications Server, and, if applicable, the specific location of the text that you are commenting on (for example, a section number, a page number or a table number).

Summary of changes

Changes made in IBM Multi-site Workload Lifeline Version 1 Release 1

This document contains information previously presented in SC23-8600-00, which supports IBM Multi-site Workload Lifeline Version 1 Release 1. This document contains minor maintenance updates.

New Information

- Lifeline Advisor configuration statement “peer_advisor_id” on page 45 has been added.
- Lifeline Advisor Configuration statement “advisor_id_list” on page 49 has been added.
- Message AQS0190I
- Message AQS0191I

Changed information

- “External load balancers” on page 4 has been updated.
- “Granting users explicit authority to control the Lifeline Advisor and Agent” on page 7 has been updated.
- “Configuring Lifeline Agents to automatically restart” on page 17 has been updated.
- “cross_sysplex_list” on page 41 has been updated.
- “advisor_id” on page 48 has been updated.
- Message AQS0006I
- Message AQS0116I
- Message AQS0125I
- Message AQS0147I
- Message AQS0168I

Chapter 1. Overview of Multi-site Workload Lifeline

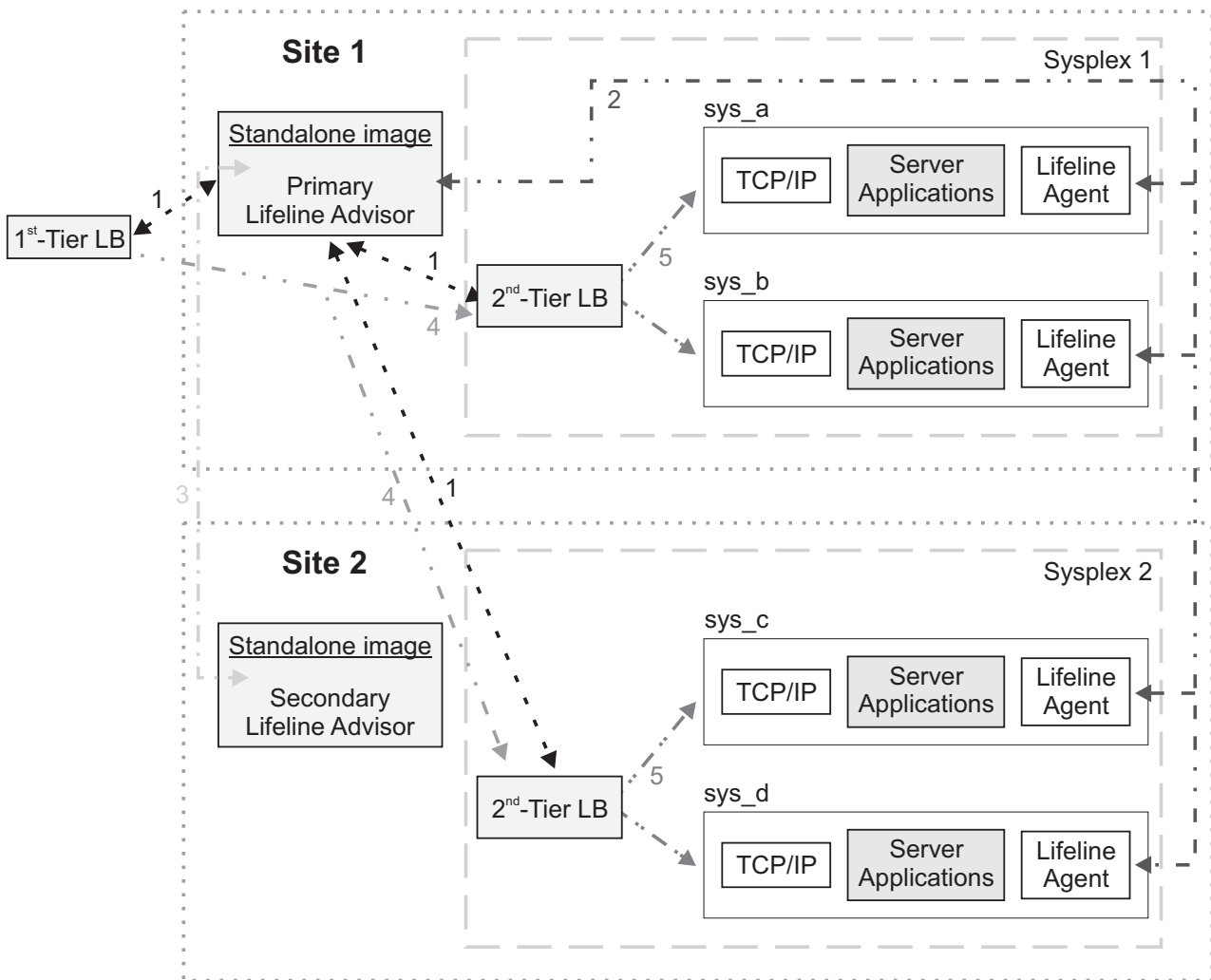
Multi-site Workload Lifeline provides the ability to load balance TCP/IP workload requests across two sites at unlimited distances, when both sites are running the same server applications and have the same data sources. Multi-site Workload Lifeline defines two tiers of load balancing. The first-tier load balancer determines which site to route a new workload request to and forwards the request to a second-tier load balancer. The second-tier load balancer determines which server application within the site to route the workload request to and forwards it to the z/OS system where the server application is running. Multi-site Workload Lifeline provides the different tiers with routing recommendations based on the availability and health of the server applications and the z/OS systems within the site.

Multi-site Workload Lifeline consists of Lifeline Advisors and Lifeline Agents. The primary Lifeline Advisor communicates with external load balancers by using the Server/Application State Protocol (SASP), one or more Lifeline Agents, and possibly a secondary Lifeline Advisor.

Rule: In this information, the word *site* is interchangeable with *sysplex*. All z/OS target systems in a particular site must belong to the same sysplex.

Figure 1 on page 2 illustrates the relationships between the external load balancers, Lifeline Advisors, and Lifeline Agents.

Multi-Site Workload Lifeline



- | | |
|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| 1. Lifeline Advisor 1 st and 2 nd tier load balancers SASP flows | 4. 1 st to 2 nd tier connection load balancing |
| 2. Lifeline Advisor to Lifeline Agents communication | 5. 2 nd -tier to server instance connection load balancing |
| 3. Primary to Secondary Lifeline Advisor state exchange | |

Figure 1. Relationships between external load balancers, Lifeline Advisors, and Lifeline Agents

In Figure 1, the Lifeline Agents running on each z/OS system in the two sites, Sysplex1 and Sysplex2, monitor the health of the server applications and the system where the Agent is active. The Lifeline Agents periodically send this information to the primary Lifeline Advisor, indicated by the network flows labeled **2**. The primary Lifeline Advisor uses this information to calculate routing recommendations for the workloads that use these server applications. The Lifeline Advisor periodically sends recommendations to first-tier load balancers about which site to route workload requests to and recommendations to second-tier load balancers about which server application within a site to route the workload requests to, indicated by the network flows labeled **1**.

The primary Lifeline Advisor also periodically notifies the secondary Lifeline Advisor about any changes in the workload states, indicated by the network flows labeled **3**, so that the secondary Advisor can take over primary Advisor responsibilities if the current primary Advisor becomes not-operational.

When workload requests are handled by the first-tier load balancers, based on routing recommendations from the Lifeline Advisor, the load balancer selects a site and forwards the request to the second-tier load balancer in that site, indicated by the network flows labeled **4**. When workload requests are handled by the second-tier load balancers, based on routing recommendations from the Lifeline Advisor, the load balancer selects a server application in the site and forwards it to the TCP/IP stack running on the z/OS system, indicated by the network flows labeled **5**.

Lifeline Advisors

The primary Lifeline Advisor provides recommendations that are used by a first-tier external load balancer to determine how to route new requests to a second-tier load balancer to select a target site. The second-tier load balancer then routes each request to a target z/OS system in the site to select a target application.

Rule: In this information, whenever the term Lifeline Advisor or Advisor is mentioned, it is referring to the primary Lifeline Advisor. Any references to the secondary Lifeline Advisor is indicated by the terminology secondary Lifeline Advisor or secondary Advisor.

The second-tier load balancer can be either another external load balancer or a z/OS sysplex distributor on a specific z/OS system in the site. If the second-tier load balancer is an external load balancer, it also uses the Lifeline Advisor recommendations to determine how to route these new requests to the target applications in the z/OS site. If the second-tier load balancer is a z/OS sysplex distributor, it creates its own recommendations that are similar to the ones that the Lifeline Advisor creates to determine how to route these new requests to the target applications in the z/OS site.

The Lifeline Advisor maintains at least two, and up to four, listening sockets or ports; one is for the Lifeline Agents to connect to, up to two are for the external load balancers to connect to, and optionally one is for the secondary Lifeline Advisor to connect to. There are separate IPv4 and IPv6 listening sockets for external load balancers. If your TCP/IP stack is not IPv6 enabled, you will not be able to use the IPv6 listening socket.

The Lifeline Advisor maintains an access control list that allows external load balancers, the secondary Lifeline Advisor, and the Lifeline Agents to connect to it. The access control list specifies the remote IP address of the connecting external load balancers, the remote IP address and port of the secondary Lifeline Advisor, and the Lifeline Agents that are allowed to connect to the Lifeline Advisor.

Recommendations provided by the Lifeline Advisor

The recommendations provided by the Lifeline Advisor are dynamic, and can change as the conditions of the target sites, systems, and server applications change. The recommendations include the following information:

- An indication of whether the target server application, the target system, or the target site is currently active. The Advisor uses this information to exclude systems or sites that are not active or do not have the required server applications running.
- z/OS Workload Management (WLM) server-specific recommendations. WLM recommendations provide a relative measure of the ability of a target system to handle new workload, as compared to other target systems across both sites. They also provide a measure of the performance of individual server applications, as compared to the WLM policy goals specified for that workload. The WLM recommendations are derived from the following metrics that are based on the importance of the workload, as defined by the WLM policy:
 - Displaceable general CPU capacity of each system
 - System z[®] Application Assist Processor (zAAP) capacity
 - System z Integrated Information Processor (zIIP) capacity
 - The proportion of each type of CPU that the server application is using
- An indication of server application health from a TCP/IP perspective. TCP/IP statistics for target applications are monitored to determine whether specific server applications are encountering problems that prevent the applications from keeping up with the current workload. For example, is a target TCP server application keeping up with TCP connection requests? Are requests being rejected because the backlog queue is full? In such scenarios, the recommendations passed back to the external load balancers are adjusted appropriately, so that the load balancer can direct fewer connections to any server application that is experiencing these problems. These recommendations are provided for TCP server applications and are referred to as Communications Server weights in this information.

Lifeline Agents

The Lifeline Agent receives from the Lifeline Advisor a list of server applications that are configured to receive workload requests from registered external load balancers. The Lifeline Agent gathers data about these server applications and returns the information to the Advisor.

The Lifeline Agent maintains a single connection to the Lifeline Advisor to communicate status information. This can be either an IPv4 or IPv6 connection. If the TCP/IP stack where the Agent resides is not IPv6-enabled, you will not be able to create the IPv6 connection.

See the Recommendations provided by the Lifeline Advisor section in “Lifeline Advisors” on page 3 for the set of metrics gather by the Agents about the server applications and z/OS system being monitored.

External load balancers

External load balancers use Server/Application State Protocol (SASP) to obtain recommendations and topology information related to server applications and systems in a clustered environment.

Rule: First-tier load balancers must be external load balancers that are SASP-enabled.

A second-tier load balancer can be an external load balancer that is SASP-enabled or a z/OS sysplex distributor on a z/OS system in the site.

External load balancers can obtain detailed information regarding the state of target z/OS applications and systems by communicating with the Lifeline Advisor using the SASP protocol. External load balancers use SASP to do the following things:

- Obtain detailed recommendations about how to distribute workload requests between the two sites, based on the current configuration and workload conditions.
- Obtain detailed recommendations about how to distribute workload requests in the site, based on the current configuration and workload conditions.
- Perform workload load balancing that is optimized for your two sites.

In some configurations, multiple server applications may be listening on the same port. When the TCP connection requests reach a target TCP/IP stack for these server applications sharing the same port, the connections are load balanced by TCP/IP across the multiple server application instances. How this load balancing is performed depends on whether the SHAREPORT or SHAREPORTWLM parameter is specified on the PORT statement. For more details about the PORT statement, see *z/OS Communications Server: IP Configuration Reference*. When you use Multi-site Workload Lifeline, all instances of this server application that share the same port on a target system are reported to external load balancers through a single member entry.

You might be able to customize the features of the way that the external load balancer communicates with the Lifeline Advisor. The SASP protocol defines two features of the external load balancer implementation that you might be able to configure:

- Whether the external load balancer polls the Lifeline Advisor for updated data or whether the updated data is pushed to the external load balancer.
- Whether only members that have updated data should be sent to the external load balancer or whether all members should be sent to the load balancer, regardless of whether their data has changed.

If you configure the external load balancer to request that the Lifeline Advisor push the updated information to the load balancer, the Lifeline Advisor updates the load balancer at least once every update interval. If you configure the external load balancer to poll the Lifeline Advisor for updated information, the Lifeline Advisor passes a recommended polling interval to the load balancer. However, you can configure the external load balancer to disregard this guideline.

External load balancers typically use a cluster IP address to represent the server applications that are being load balanced. Client applications use this cluster IP address as the destination IP address for their requests.

In addition, some external load balancers might be able to use either directed or dispatch mode when they forward packets to their destinations.

Directed mode

When an external load balancer uses directed mode to forward packets to their destinations, it can use NAT to convert the destination IP address (the cluster IP address) to an IP address owned by the target z/OS system. When IP packets for these connections are sent back to clients, the external load balancer converts the source IP address (the IP address of the target z/OS system) back to the cluster IP address that the application used on its request. The load balancer either modifies the destination IP address (server NAT) in the packet itself or modifies both the

destination and source IP addresses (server NAT and client NAT) in the packet. The packet must return through the same external load balancer, which recognizes the changes and does the reverse mapping. Then a packet can flow from the original destination to the original source.

Rule: Always configure first-tier load balancers to use directed mode. These load balancers route requests only to second-tier load balancers.

Guideline: You can configure external second-tier load balancers to use either directed or dispatch mode, although directed mode is recommended to avoid having to make server application changes.

Dispatch mode

When an external load balancer uses dispatch mode to forward packets to their destinations, the destination IP addresses for incoming IP packets are not changed. Instead, the external load balancer forwards the packet to a target z/OS system by using the MAC address of a network adapter on that system. The receiving z/OS system inspects the destination IP address of the packet, and accepts the packet if the IP address matches one of the IP addresses in its HOME list. As a result, with dispatch mode, all target z/OS systems must have the external load balancer's cluster IP address defined in their HOME list. However, these addresses must not be advertised externally through dynamic routing protocols. To prevent the addresses from being advertised externally through dynamic routing protocols, define these IP addresses as loopback addresses on z/OS.

Dispatch mode eliminates the need to perform network address translation (NAT). Dispatch mode has the following restrictions, which ensure that the second-tier external load balancer functions correctly:

Restrictions:

- An OSA device can be shared among logical partitions (LPARs) only if virtual MAC (VMAC) addressing is configured for each TCP/IP target stack that shares the OSA device.
- All target applications must bind to the IP address specified by INADDR_ANY or IN6ADDR_ANY, and the cluster IP address of the 2nd-tier load balancer must be defined to the stack. To ensure that this cluster IP address is not advertised, define it as a loopback address.
- First-tier load balancers cannot be configured in dispatch mode.

If you do not meet the previous restrictions, load balancing will not be optimal because work will not be routed to some servers.

Internal load balancers

An internal load balancer, also known as z/OS sysplex distributor, resides on a z/OS system in the site. It uses z/OS Communications Server functions to obtain recommendations and topology information related to server applications in a sysplex environment.

For more information about z/OS sysplex distributor, see *z/OS Communications Server: IP Configuration Guide*.

Tip: You can use z/OS sysplex distributor to perform the second-tier load balancing function.

Chapter 2. Preparing to use Multi-site Workload Lifeline

You need to evaluate TCP/IP workloads and grant users authority before you can configure Multi-site Workload Lifeline to balance TCP/IP workloads between the two z/OS sites.

Before you begin

You must meet the following requirements:

- All z/OS systems must be at least at the V1R11 level.
- You must have at least one first-tier external load balancer that supports the Server/Application State Protocol (SASP). The load balancer must have IP connectivity to each second-tier load balancer. The second-tier load balancer is either another external load balancer that supports SASP or a z/OS sysplex distributor running on a target system in the site.
- The TCP/IP applications that are identified to be load balanced must be able to run on target systems that are in different sites, and must be able to access data sources that are synchronized across the sites.

Granting users explicit authority to control the Lifeline Advisor and Agent

| Grant explicit authority to all users that can start, stop, or modify the Lifeline
| Advisor and Agent, to prevent unauthorized users from controlling it. If you do
| not grant explicit authority, any user that is able to issue the START, STOP, or
| MODIFY command can control the Lifeline Advisor and Agent.

About this task

| **Restriction:** The only commands that you can issue against the Lifeline Advisor
| and Agent are MODIFY commands, with the exception of the START
| command that you use to start the Lifeline Advisor or Agent or the
| STOP command that you use to stop the Lifeline Advisor or Agent.
| Limit which users are able to issue the START, STOP, and MODIFY
| commands for these two servers.

To grant users explicit authority to start, stop, or modify the Lifeline Advisor and Agent, perform the following steps:

Procedure

1. Issue the following two commands to ensure that the OPERCMDS class is active and that RACLIST processing is enabled:

```
SETROPTS CLASSACT(OPERCMDS)  
SETROPTS RACLIST (OPERCMDS)
```
2. Define the following OPERCMDS class profile using a security product like RACF® for the Lifeline Advisor:

```
RDEFINE OPERCMDS (MVS.SERVMGR.LLADVSR) UACC(NONE)
```
3. Define the following OPERCMDS class profile using a security product like RACF for the Lifeline Agent:

```
RDEFINE OPERCMDS (MVS.SERVMGR.LLAGENT) UACC(NONE)
```

4. Permit the Lifeline Advisor to the OPERCMDS class profile:

```
PERMIT MVS.SERVMGR.LLADVSR CLASS(OPERCMDS) ACCESS(CONTROL) ID(userid)
```
5. Permit the Lifeline Agent to the OPERCMDS class profile:

```
PERMIT MVS.SERVMGR.LLAGENT CLASS(OPERCMDS) ACCESS(CONTROL) ID(userid)
```
6. Issue the following command to refresh the OPERCMDS class profile:

```
SETROPTS RACLIST(OPERCMDS) REFRESH
```

Authorizing the Lifeline Advisors to use BCPii

You need to grant Lifeline Advisors general authority to use the Base Control Program Internal Interface (BCPii), including authority to specific resources such as the interconnected Central Processor Complexes (CPCs) and images on those CPCs.

About this task

To allow a Lifeline Advisor to query CPC and image information, perform the following steps. See “Using the Base Control Program Internal Interface” on page 18 for more information.

Procedure

1. Issue the following two commands to ensure that the FACILITY class is active and that RACLIST processing is enabled:

```
SETROPTS CLASSACT(FACILITY)
SETROPTS RACLIST (FACILITY)
```
2. Define the following FACILITY class profile for authority to use BCPii:

```
RDEFINE FACILITY HWI.APPLNAME.HWISERV UACC(NONE)
```
3. Permit the Lifeline Advisor to the FACILITY class:

```
PERMIT HWI.APPLNAME.HWISERV CLASS(FACILITY) ACCESS(READ) ID(userid)
```
4. Define the following FACILITY class profile (one for each CPC) for authority to query the CPC.

```
RDEFINE FACILITY HWI.TARGET.netid.nau UACC(NONE) APPLDATA(community-name)
```

Where:

- *netid.nau* represents the 3 to 17 character SNA name of the particular CPC.
- *community-name* is the SNMP community name that was defined on the Support Element for that CPC.

5. Permit the Lifeline Advisor to each of the FACILITY class profiles:

```
PERMIT HWI.TARGET.netid.nau CLASS(FACILITY) ACCESS(READ) ID(userid)
```
6. Define the following FACILITY class profile (one for each CPC) for authority to query each image of the CPC.

```
RDEFINE FACILITY HWI.TARGET.netid.nau.* UACC(NONE)
```

Where:

- *netid.nau* represents the 3 to 17 character SNA name of the particular CPC.

7. Permit the Lifeline Advisor to each of these FACILITY class profiles:

```
PERMIT HWI.TARGET.netid.nau.* CLASS(FACILITY) ACCESS(READ) ID(userid)
```
8. Issue the following command to refresh the FACILITY class profile:

```
SETROPTS RACLIST(FACILITY) REFRESH
```

Authorizing the Lifeline Agents to use WLM services

You need to grant Lifeline Agents access to the BPX.WLMSERVER resource only if you have already defined the resource profile.

About this task

If you are using RACF and have already defined the resource profile and enabled the FACILITY class, grant Lifeline Agents access to that resource.

If you are using a security product other than RACF that by default denies access to the resource, grant the Lifeline Agents access to the resource.

If you are using RACF, perform the following steps to define the resource profile if you have not defined it, and grant Lifeline Agents access to the resource:

Procedure

1. Issue the following two commands to ensure that the FACILITY class is active and that RACLIST processing is enabled:

```
SETROPTS CLASSACT(FACILITY)
SETROPTS RACLIST (FACILITY)
```

2. Define the following FACILITY class profile:

```
RDEFINE FACILITY (BPX.WLMSERVER) UACC(NONE)
```

3. Grant the Lifeline Agent READ access to the FACILITY class profile:

```
PERMIT BPX.WLMSERVER CLASS(FACILITY) ACCESS(READ) ID(userid)
```

4. Issue the following command to refresh the FACILITY class profile:

```
SETROPTS RACLIST(FACILITY) REFRESH
```

Authorizing the Lifeline Agents to reset active connections

You need to grant Lifeline Agents access to the MVS.VARY.TCPIP.DROP resource.

About this task

To process a Lifeline Advisor DEACTIVATE command, the Lifeline Agents must be able to reset active connections that have been identified by the Advisor. See “MODIFY *advisor_proc*,DEACTivate command: Deactivate workloads” on page 67 for more information.

To grant Agents explicit authority to reset active connections, perform the following steps:

Procedure

1. Issue the following two commands to ensure that the OPERCMDS class is active and that RACLIST processing is enabled:

```
SETROPTS CLASSACT(OPERCMDS)
SETROPTS RACLIST (OPERCMDS)
```

2. Define the following OPERCMDS class profile:

```
RDEFINE OPERCMDS (MVS.VARY.TCPIP.DROP) UACC(NONE)
```

3. Permit the Lifeline Agent to the OPERCMDS class profile:

```
PERMIT MVS.VARY.TCPIP.DROP CLASS(OPERCMDS) ACCESS(CONTROL) ID(userid)
```

4. Issue the following command to refresh the OPERCMDS class profile:

```
SETROPTS RACLIST(OPERCMDS) REFRESH
```

Chapter 3. Configuring Multi-site Workload Lifeline

You need to configure Multi-site Workload Lifeline before you can use it to balance TCP/IP workloads among different z/OS sites.

Before you begin

Complete the tasks in Chapter 2, “Preparing to use Multi-site Workload Lifeline,” on page 7.

Lifeline Advisor configuration file

You specify the Lifeline Advisor configuration file on the CONFIG DD statement in the Lifeline Advisor started procedure to configure both the primary and secondary Lifeline Advisors.

The Lifeline Advisor configuration file serves three basic purposes:

- Defines the listening sockets for the external load balancers, the secondary Lifeline Advisor, and Lifeline Agents
- Provides an access control list for specifying which external load balancers, Lifeline Advisor, and Lifeline Agents can connect to the primary Lifeline Advisor
- Customizes optional parameters

The Lifeline Advisor reads configuration data from one file, which can be a z/OS UNIX file, a PDS or PDSE member, or a sequential data set.

See Appendix A, “A sample started procedure for Lifeline Advisors,” on page 133 for a sample Advisor start procedure.

Lifeline Agent configuration file

You specify the Lifeline Agent configuration file on the CONFIG DD statement in the Lifeline Agent start procedure.

The Lifeline Agent configuration file serves three basic purposes:

- Defines the IP address and port that the Lifeline Agent binds to for communication with the Lifeline Advisor
- Identifies the IP address and port of the Lifeline Advisor
- Customizes optional parameters

The Lifeline Agent configuration file can be a z/OS UNIX file, a PDS or PDSE member, or a sequential data set.

See Appendix B, “A sample started procedure for Lifeline Agents,” on page 135 for a sample Agent start procedure.

Configuring one Lifeline Advisor as the primary Advisor, and optionally one as the secondary Advisor

Use the Lifeline Advisor configuration file to configure one Lifeline Advisor as the primary Advisor. You can also use this file to configure an optional secondary Lifeline Advisor.

About this task

Only one Lifeline Advisor can serve as a primary Advisor at any given time. To start a secondary Lifeline Advisor to take over primary Advisor responsibilities in the case of a failure of the primary Advisor, specify identical statements in the Lifeline Advisor configuration file for both the primary and secondary Lifeline Advisors.

Perform the following steps to configure Lifeline Advisors:

Procedure

1. Define listening sockets, ports, or both.
 - a. Specify the local IPv4 address and port that the Lifeline Advisor listens on for IPv4 load balancer connections on the `lb_connection_v4` configuration statement. The default port for communications with external load balancers is 3860. You can also specify the local IPv6 address and port that the Lifeline Advisor listens on for IPv6 load balancer connections on the `lb_connection_v6` configuration statement.

Guideline: To enable the movement of the primary Lifeline Advisor to another system when the Lifeline Advisor or its underlying system fails, specify a dynamic VIPA (DVIPA) on the `lb_connection_v4` and `lb_connection_v6` statements. Furthermore, make this DVIPA a unique application-instance DVIPA (defined through `VIPARANGE`) rather than a multiple application-instance DVIPA (defined through `VIPADefine`). For more information about configuring DVIPAs, see *z/OS Communications Server: IP Configuration Reference*.

Rules:

- Run the Lifeline Advisor on an INET system. If you run the Lifeline Advisor on a CINET system, the address or addresses that you specify on the `lb_connection_v4` or `lb_connection_v6` statement tie the Lifeline Advisor to the stack owning those addresses. Consequently, the termination of that stack results in the termination of the Lifeline Advisor.
 - If the primary Lifeline Advisor is using IPv6 for the external load balancer connections, or if any Lifeline Agents are using IPv6 to connect to the Lifeline Advisor, you must configure the system in which the secondary Lifeline Advisor resides to be enabled for IPv6.
- b. Specify the local port that the Lifeline Advisor listens on for Lifeline Agent connections on the `agent_connection_port` statement. If the TCP/IP stack of the Lifeline Advisor is enabled for IPv6, the Lifeline Advisor opens a listening socket for Lifeline Agents on the IPv6 unspecified address (::) on the port specified by this statement. This enables Lifeline Agents to connect to the Lifeline Advisor using either the IPv4 address specified on the

lb_connection_v4 statement or the IPv6 address specified on the lb_connection_v6 statement. If the TCP/IP stack is not enabled for IPv6, the Lifeline Advisor opens a listening socket on the IPv4 unspecified address, 0.0.0.0. This enables Lifeline Agents to connect to the Lifeline Advisor using only the IPv4 address specified on the lb_connection_v4 statement.

- c. Specify the local port that the Lifeline Advisor listens on for a connection from the secondary Lifeline Advisor on the advisor_connection_port statement. The same information specified in the previous step about the use of the lb_connection_v4 and lb_connection_v6 statements applies in this step.
2. Define the access control list.

Rule: Specify only complete IP addresses in access control lists; subnetworks, IP prefixes, or other types of wildcards are not allowed.

- a. Specify the list of external load balancers that are allowed to connect to the Lifeline Advisor on the lb_id_list statement. There is a maximum limit of 100 external load balancers that can be connected to a Lifeline Advisor at any given time.
 - b. Specify the list of secondary Lifeline Advisors that are allowed to connect to the primary Lifeline Advisor on the advisor_id_list statement. Only a single secondary Lifeline Advisor can be connected to the primary Lifeline Advisor at any given time.
 - c. Specify the list of Lifeline Agents that are allowed to connect to the primary Lifeline Advisor on the agent_id_list statement.
3. Update the TCP/IP profiles on the systems where the primary and secondary Advisors reside to add the VIPARANGE definition that configures the IP address used in the lb_connection_v4 and lb_connection_v6 Advisor configuration statements.
 4. Define an OMVS segment for the Lifeline Advisor. The Lifeline Advisor accesses files in the UNIX System Services shell, so the Lifeline Advisor needs to have an OMVS segment defined for it. You can use the following JCL snippet to define the OMVS segment:

```
//EZARACF JOB MSGLEVEL=(1,1),MSGCLASS=A,CLASS=A
//DAEMONS EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
ADDUSER userid DFLTGRP(OMVSGRP) OMVS(UID(0) HOME('/'))
RDEFINE STARTED userid.* STDATA(USER(userid))
SETROPTS RACLIST(STARTED) REFRESH
/*
```

5. Optional: Customize optional statements, including the update_interval and debug_level statements.

Guideline: In most cases, do not customize the debug_level statement, unless you are directed to do so by an IBM service representative. Adding additional types of trace data can cause the amount of captured data to become voluminous. Reducing the amount of trace data from the default might make diagnosing a problem more difficult.

6. Optional: Change the location of the Multi-site Workload Lifeline message catalog. The Lifeline Advisor uses a standard message catalog. The message catalog must be in the z/OS UNIX file system. The default location of the message catalog is /usr/lib/nls/msg/C/aqs11msg.cat. If you want to store the message catalog in another location, you need to change the NLSPATH or the LANG environment variables. To change the two environment variables, you can update the started procedure of the Lifeline Advisor to pass the ENVAR

option to set NLSPATH. If aqslmsg.cat does not exist, the Lifeline Advisor by default uses the messages hardcoded in the software. These messages duplicate the English message catalog that is shipped with the Multi-site Workload Lifeline product.

Configuring a Lifeline Agent

Use the Lifeline Agent configuration file to configure one Lifeline Agent per z/OS target system across both sites.

About this task

Only one Lifeline Agent can be active per z/OS system at any time. Perform the following steps to configure Lifeline Agents:

Procedure

1. Specify the local IP address and port that the Lifeline Agent binds to for communicating with the Lifeline Advisor on the `host_connection` statement. This step is used as part of the Lifeline Advisor's access control enforcement.

Guideline: For high availability, use a static VIPA as the local IP address to tolerate individual link outages on the z/OS system. For more information about configuring static VIPAs, see *z/OS Communications Server: IP Configuration Reference*.

2. Specify the IP address and port of the Lifeline Advisor on the `advisor_id` statement.
3. Update the TCP/IP profiles on the systems where the Agents reside to add the static VIPA definition that configures the IP address used in the `host_connection` Agent configuration statement.
4. Define an OMVS segment for the Lifeline Agent. The Lifeline Agent accesses files in the UNIX System Services shell, so you need to define an OMVS segment for the Lifeline Agent. You can use the following JCL snippet to define the OMVS segment:

```
//EZARACF JOB MSGLEVEL=(1,1),MSGCLASS=A,CLASS=A
//DAEMONS EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
ADDUSER userid DFLTGRP(OMVSGRP) OMVS(UID(0) HOME('/'))
RDEFINE STARTED userid.* STDATA(USER(userid))
SETROPTS RACLIST(STARTED) REFRESH
/*
```

5. Optional: Use the `debug_level` statement to specify how much trace data is captured in the log file of the Lifeline Agent.

Rule: In most cases, you should not customize this statement, unless you are directed to do so by an IBM service representative. Adding additional types of trace data can cause the amount of data captured to become voluminous. Reducing the amount of trace data from the default might make diagnosing a problem more difficult.

6. Optional: Change the location of the Multi-site Workload Lifeline message catalog. The Lifeline Agent uses a standard message catalog. The message catalog must be in the z/OS UNIX file system. The default location of the message catalog is `/usr/lib/nls/msg/C/aqslmsg.cat`. If you want to store the message catalog in another location, you need to change the NLSPATH or the LANG environment variables. To change the two environment variables, you

can update the started procedure of the Lifeline Agent to pass the ENVAR option to set NLSPATH. If aqslmsg.cat does not exist, the Lifeline Agent by default uses the messages hardcoded in the software . These messages duplicate the English message catalog that is shipped with the Multi-site Workload Lifeline product.

WLM recommendations

The Lifeline Agents use a WLM recommendation that is referred to as server-specific WLM. Server-specific WLM provides a relative measure of the ability of a target system to handle additional workload requests, as compared to other systems across both sites. It also indicates how well individual server applications are doing compared to the WLM policy goals that have been specified for that workload.

Server-specific WLM recommendations are composed of two key elements:

- The amount of displaceable capacity (general, zAAP, and zIIP) available on the target system, based on the importance level of the server application, and the proportion of general, zAAP, and zIIP CPU that is currently being consumed by the workload of the application. For example, if the application is using only general and zAAP CPU, the displaceable zIIP capacity is not considered.
- The performance of the application compared to the WLM goals for that application workload.

WLM provides an interface that enables server applications to report the following additional information:

- The abnormal transaction completion rate, or the rate of abnormal completions per 1000 total transactions
- Application health, which is a value in the range 0 - 100% (100% is optimal), representing the overall health of the server application

Configuring Lifeline Advisors to automatically restart

You can use automation software or define an automatic restart manager (ARM) policy to automatically restart the Lifeline Advisor in case the Advisor or system fails. Although this task is optional, you should restart the Lifeline Advisor as soon as possible after it fails.

About this task

The restart capability covers scenarios where the Lifeline Advisor itself fails; in scenarios where the system the Lifeline Advisor is running on fails, you can configure a secondary Lifeline Advisor to automatically take over primary Advisor responsibilities.

If the Lifeline Advisor or its underlying system fails, and no secondary Lifeline Advisor is configured to automatically take over primary Advisor responsibilities, an external load balancer might do one of the following things:

- Continue to distribute workload requests according to the last set of information received from the Lifeline Advisor
- Resort to pre-configured weights
- Stop distributing new workload requests to second-tier load balancers or server applications

The actual behavior depends on the load balancer implementation. Consult the load balancer documentation for your specific external load balancer for details.

You need to restart the Lifeline Advisor as soon as possible when the Lifeline Advisor itself fails, or configure a secondary Lifeline Advisor to automatically take over primary Advisor responsibilities when the system on which the Lifeline Advisor is running fails.

For more information about defining ARM policies, see *z/OS MVS Setting Up a Sysplex*.

The Lifeline Advisor registers with ARM using the following values:

- ELEMTYPE=SYSLVL1
- ELEMNAME=AQSSLADVSR
- TERMTYPE=ELEMTERM

These values indicate that if the Lifeline Advisor fails on this system, the Lifeline Advisor needs to be restarted only on this system.

To configure Lifeline Advisors to automatically restart using ARM, perform the following step:

Procedure

Update the IXCARM resource. The Lifeline Advisors do not run using a system key. If you are using ARM registration, the started task IDs must be permitted with UPDATE authority to the IXCARM.SYSLVL1.AQSSLADVSR resource profile in the FACILITY class using the SAF product on your system. To enable the Advisor to register with ARM, use the following RACF commands to define the profiles and grant update access:

```
RDEFINE FACILITY IXCARM.SYSLVL1.AQSSLADVSR UACC(NONE)
PERMIT IXCARM.SYSLVL1.AQSSLADVSR CLASS(FACILITY) ID(userid) ACCESS(UPDATE)
SETROPTS RACLIST(FACILITY) REFRESH
```

Recovering from a planned outage of the TCP/IP stack

If you use automatic restart manager (ARM) and the TCP/IP stack address space terminates, you need to be sure that the system can recover from a planned outage of the TCP/IP stack.

About this task

When the TCP/IP stack becomes unavailable, the Lifeline Advisor also terminates, because the Advisor can no longer establish any TCP/IP communications. An ARM restart of the Lifeline Advisor will likely fail if the TCP/IP stack is not available when the restart occurs. Perform the following steps to recover from a planned outage of the TCP/IP stack:

Procedure

1. Ensure that a secondary Lifeline Advisor has been started on another system.
2. Configure the secondary Lifeline Advisor to automatically take over primary Advisor responsibilities as soon as the primary Lifeline Advisor terminates on the system where TCP/IP is stopped.

Recovering from an unplanned outage of the TCP/IP stack

If you are using automatic restart manager (ARM) and the TCP/IP stack address space terminates, you need to be sure that the system can recover from an unplanned outage of the TCP/IP stack.

About this task

When the TCP/IP stack becomes unavailable, the Lifeline Advisor also terminates, because the Advisor can no longer establish any TCP/IP communications. An ARM restart of the Lifeline Advisor will likely fail if the TCP/IP stack is not available when the restart occurs. Perform the following steps to recover from an unplanned outage of the TCP/IP stack:

Procedure

1. Ensure that an ARM policy or other automation is in place to quickly restart the TCP/IP stack on the same system.
2. Quickly restart the Lifeline Advisor on the same system. You can restart the Lifeline Advisor by using an automation software package, or by using the TCP/IP profile AUTOLOG statement. For more information about the AUTOLOG statement, see *z/OS Communications Server: Configuration Reference*.

Configuring Lifeline Agents to automatically restart

You can use automation software or define an automatic restart manager (ARM) policy to automatically restart the Lifeline Agent in case the Agent or system fails. Although this task is optional, you can perform it to provide high availability to your target applications.

About this task

When a Lifeline Agent fails, the Lifeline Advisor indicates that it has no information for any server applications running on that system. As a result, if the second-tier load balancer responsible for distributing workload requests for this site is an external load balancer, target applications on the failing system will no longer receive new workload requests until the Lifeline Agent is restarted. Automatically restarting the Lifeline Agent on the same system minimizes this perceived outage. For more information about defining ARM policies, see *z/OS MVS Setting Up a Sysplex*.

Tip: If the second-tier load balancer is z/OS sysplex distributor, target applications on the failing system might continue to receive new workload requests, as z/OS sysplex distributor does not rely on the Lifeline Agent to retrieve information about these target applications.

The Lifeline Agent registers with ARM using the following values:

- ELEMTYPE=SYSLVL1
- ELEMNAME=AQSLLAGENT
- TERMTYPE=ELEMTERM

These values indicate that if the Lifeline Agent fails on this system, the Lifeline Agent needs to be restarted only on this system.

To configure Lifeline Agents to automatically restart using ARM, perform the following step:

Procedure

Update the IXCARM resource. The Lifeline Agents do not run using a system key. If you are using ARM registration, the started task IDs must be permitted with UPDATE authority to the IXCARM.SYSLVL1.AQSLLAGENT resource profile in the FACILITY class using the SAF product on your system. To enable the Agent to register with ARM, use the following RACF commands to define the profiles and grant update access:

```
RDEFINE FACILITY IXCARM.SYSLVL1.AQSLLAGENT UACC(NONE)
PERMIT IXCARM.SYSLVL1.AQSLLAGENT CLASS(FACILITY) ID(userid) ACCESS(UPDATE)
SETROPTS RACLIST(FACILITY) REFRESH
```

Using the Base Control Program Internal Interface

The Lifeline Advisor uses Base Control Program Internal Interface (BCPii) services to periodically query all interconnected Central Processor Complexes (CPCs) and the images (LPARs) on these CPCs.

About this task

The Hardware Management Console (HMC) and Support Elements on each CPC typically communicate over a network that is separate from the network used for TCP/IP communications. The Advisor queries the images in a site over this network to determine whether the images are available or whether a site failure has occurred.

For these queries to succeed, perform the following steps:

Procedure

1. Configure the Support Elements to support BCPii. You need to define an SNMP community name, and be sure that the BCPii address space is active. See the information about BCPii in *z/OS MVS Programming: Callable Services for High-Level Languages* for more information.
2. Authorize the Lifeline Advisor to use the BCPii services. See “Authorizing the Lifeline Advisors to use BCPii” on page 8 for more information.

Configuring and starting syslogd

For the Lifeline Advisors and Agents to be able to write their log messages and trace data to the syslog daemon (syslogd), you must configure and start syslogd before you start the Advisor and Agent.

About this task

The Lifeline Advisor and Agent write most log messages and trace data to the syslog daemon (syslogd). A limited number of messages are written to the MVS console, but these are unaffected by syslogd configuration.

As more data is logged by the Lifeline Advisor and Agent, performance of the Lifeline Advisor and Agent can be adversely affected. The amount of data that is logged by the Lifeline Advisor and Agent is determined by the debug_level statement. If you back up the syslogd output file with a zFS file system instead of a z/OS UNIX file system, you can minimize performance impacts caused by logging.

Tip: Logging to syslog occurs at a default level until the configuration file has been read in.

For more information about configuring syslogd, see *z/OS Communications Server: IP Configuration Guide*.

Customizing the TCP/IP profiles of the TCP/IP stacks

To accommodate the Lifeline Advisors and Agents, you need to customize the TCP/IP profiles of the TCP/IP stacks that the Lifeline Advisors and Agents will run on.

About this task

Perform the following steps to customize the TCP/IP profiles of the TCP/IP stacks:

Procedure

1. Reserve the ports that the Lifeline Advisor and Agents will use in their respective TCP/IP profiles. All ports for the Lifeline Advisor and Agent use the TCP protocol; reserve all the ports for TCP. The Lifeline Advisor has at least two ports, and potentially four ports, to reserve, including the ports specified on the following statements:

- lb_connection_v4
- lb_connection_v6
- agent_connection_port
- advisor_connection_port

The Lifeline Agent has one port to reserve, which you specify on the following statement:

- host_connection
2. Configure VIPARANGE with the IP addresses specified on the Lifeline Advisor lb_connection_v4 and lb_connection_v6 statements on the TCP/IP stacks of the systems that the Lifeline Advisor can run on, and configure static VIPAs with the IP address specified on the Lifeline Agent host_connection statement on the TCP/IP stack of the system that the corresponding Lifeline Agent can run on.
 3. Optional: If you use the SHAREPORT or SHAREPORTWLM parameters on the TCP/IP profile PORT statement to enable multiple TCP server applications to share the same port, some additional considerations might apply to your configuration. For example, if the TCP server applications sharing the same port are also members of groups that are reported to external second-tier load balancers with SASP, ensure that consistent criteria are used by the various load balancing components. When using the Multi-site Workload Lifeline, all instances of a TCP server application that share the same port on a target system are reported to external second-tier load balancers using a single member entry, and therefore, a single recommendation. This recommendation reflects the average net weight calculated for all the server applications sharing the same port on a target system. When the TCP connection requests reach a target TCP/IP stack and multiple server applications are sharing the same port, the connections are then load balanced by TCP/IP across the multiple server application instances.

How this load balancing process is performed depends on whether you specify the SHAREPORT or SHAREPORTWLM parameter on the PORT statement. For more details about the PORT statement, see *z/OS Communications Server: IP Configuration Reference*.

CINET considerations

Although it is not recommended, the Lifeline Advisor can use multiple TCP/IP stacks in a Common INET (CINET) environment.

To simplify your configuration and to make Lifeline Advisor outages that are the result of a TCP/IP stack failure or termination more predictable and recoverable, configure all incoming connections to the Lifeline Advisor to use a single TCP/IP stack. The addresses that you specify in the `lb_connection_v4` and `lb_connection_v6` statements must belong to the same TCP/IP stack.

Use a `VIPARANGE` statement to define these dynamic VIPAs in the TCP/IP profiles of all the stacks in the CINET environment.

If the Lifeline Advisor is restarted as a result of failure in a given TCP/IP stack, the dynamic VIPAs are then activated on another TCP/IP stack in that system. If you decide to use the IPv4 or IPv6 unspecified addresses for the `lb_connection_v4` and `lb_connection_v6` statements, use the `BIND` parameter on the `PORT` reservation statement to bind these sockets to the dynamic VIPAs on the one TCP/IP stack that you have decided to use.

Configuring external load balancers

Configure external load balancers with the IP address and port of the Lifeline Advisor.

About this task

Guideline: If the Lifeline Advisor uses IPv6 for the external load balancer connections or if any Lifeline Agents use IPv6 to connect to the Lifeline Advisor, start the secondary Lifeline Advisor only on a system that supports IPv6.

For maximum availability, define the IP address of the Lifeline Advisor as a `VIPARANGE DVIPA`.

There is a maximum limit of 100 external load balancers that can be connected to a Lifeline Advisor at any given time.

Perform the following tasks to configure external load balancers:

Procedure

1. Configure the first-tier external load balancers.
2. Configure the second-tier load balancers. You can have either an external load balancer or a z/OS sysplex distributor on one z/OS target server in each site.

Configuring first-tier external load balancers

Configure the first-tier external load balancers with the IP address and port of the Lifeline Advisor.

About this task

Perform the following steps to configure the first-tier external load balancers:

Procedure

1. Customize features of the communication of the external load balancer with the Lifeline Advisor. For more information about the features, see “External load balancers” on page 4.
2. Optional: Configure redundant external load balancers for availability reasons. The unique load balancer identifier (LB UID), sometimes referred to as the UID or UUID, of the external load balancer identifies a load balancer. Duplicate LB UIDs are not allowed and connection attempts to the Lifeline Advisor from an external load balancer using the same LB UID as an existing connection force the existing connection to be broken and replaced by the new connection.

Requirements:

- If you want the redundant load balancers to serve as hot standbys that are connected simultaneously with the load balancer that they are backing up, you must specify unique LB UIDs.
 - If you configure the redundant load balancers with the same LB UID, the redundant load balancers must remain unconnected from the Lifeline Advisor until the original load balancer fails.
3. Configure external first-tier load balancers to use directed mode. For more information about directed mode, see “External load balancers” on page 4.

Rule: Always configure first-tier load balancers to use directed mode. These load balancers route workload requests only to second-tier load balancers.

4. Configure each first-tier external load balancer with the members that represent the second-tier load balancers.
 - a. Define members that can share the same type of workload under the same group. For example, define a TN3270E Telnet workload under one group and a HTTP workload under another.
 - b. Specify valid and reachable IP addresses, a nonzero port, and a nonzero protocol. The IP addresses of the members must represent the IP address of an external second-tier load balancer or the DVIPA of a z/OS sysplex distributor. The port number of the group represents the port number used by the server applications for the workloads. The protocol that is defined can be specified as either tcp or udp.

Rule: All members must be application members; a nonzero port number must be specified.

Configuring second-tier external load balancers

Configure the second-tier external load balancers with the IP address and port of the Lifeline Advisor.

About this task

Perform the following steps to configure the second-tier external load balancers:

Procedure

1. Customize features of the communication of the external load balancer with the Lifeline Advisor. For more information about the features, see “External load balancers” on page 4.

2. Optional: Configure redundant external load balancers for availability reasons. The unique load balancer identifier (LB UID), sometimes referred to as the UID or UUID, of the external load balancer identifies a load balancer. Duplicate LB UIDs are not allowed and connection attempts to the Lifeline Advisor from an external load balancer using the same LB UID as an existing connection force the existing connection to be broken and replaced by the new connection.

Requirements:

- If you want the redundant load balancers to serve as hot standbys that are connected simultaneously with the load balancer that they are backing up, you must specify unique LB UIDs.
 - If you configure the redundant load balancers with the same LB UID, the redundant load balancers must remain unconnected from the Lifeline Advisor until the original load balancer fails.
3. Configure external second-tier load balancers to use directed mode. For more information about directed mode, see “External load balancers” on page 4.

Guideline: You can configure external second-tier load balancers to use either directed or dispatch mode.

4. Configure each external load balancer with the members that represent the individual target application instances.
 - a. Define members that can share the same type of workload under the same group. For example, define TN3270E Telnet servers under one group and HTTP servers under another.
 - b. Specify an IP address, a nonzero port, and a nonzero protocol to define application members. The IP addresses of the members must represent valid and reachable addresses in each site where the server applications reside. The port number of the group represents the port number used by the server applications and must match the port number specified in the first-tier load balancer for this workload. The protocol that is defined can be specified as either tcp or udp and must match the protocol specified in the first-tier load balancer for this workload.

Rules:

- All IP addresses configured in members belonging to the same group must exist on all second-tier external load balancers.
- All members must be application members; a nonzero port number must be specified.
- Certain classes of IP addresses must not be coded for members in the external load balancer. This includes the following classes of addresses:
 - Deprecated IPv6 addresses. These are flagged as such in a NETSTAT HOME display. It is probably safest not to code any auto-configured IPv6 addresses within members.
 - Addresses that are not reachable from the load balancer, including loopback addresses.
 - Unavailable IPv6 addresses. These addresses might be marked as unavailable if duplicate address detection is in progress, has failed, or the interface ID is unknown. These addresses are displayed in a NETSTAT HOME display, along with the reason that they are marked as unavailable.

Configuring second-tier internal load balancers

Configure the second-tier internal load balancers, that is, the z/OS sysplex distributor, with the IP address and port number configured in the first-tier load balancer group that represents the DVIPA being distributed.

About this task

For information about configuring z/OS sysplex distributors, see *z/OS Communications Server: IP Configuration Reference*.

Chapter 4. Starting the Lifeline Advisors and Agents

To balance TCP/IP workloads between the two z/OS sites, you need to start the Lifeline Advisors and Agents that make up Multi-site Workload Lifeline.

Before you begin

You need to first complete the tasks in Chapter 2, “Preparing to use Multi-site Workload Lifeline,” on page 7 and Chapter 3, “Configuring Multi-site Workload Lifeline,” on page 11.

About this task

You can start the Lifeline Agents before the Lifeline Advisors, or start the Lifeline Advisors before the Lifeline Agents. If you start the Lifeline Advisor after you start the Lifeline Agents, the Lifeline Agents periodically attempt to connect to the Lifeline Advisor.

Procedure

1. Start the TCP/IP stacks that the Lifeline Advisors and the Agents will use.

Requirement: You must start the TCP/IP stacks that the Lifeline Advisors will use before you start the Lifeline Advisors. You can start a Lifeline Agent before the start of the TCP/IP stack that the Lifeline Agent uses. If the TCP/IP stack that the Lifeline Agent uses stops, the Lifeline Agent remains active and reestablishes communication with the TCP/IP stack when the TCP/IP stack is restarted.

2. Start the server applications that will be the target of load balancing. You do not need to modify these server applications, their configurations, or started procedures, unless the second-tier external load balancer is using dispatch mode for packet forwarding. For more information about dispatch mode, see “External load balancers” on page 4.
3. Optional: Customize WLM policies for the Lifeline Advisors and Agents, and assign the Lifeline Advisors and Agents to the WLM SYSSTC service class to receive the proper dispatching priority. For more information about categorizing work into service classes, see *z/OS MVS Planning: Workload Management*.

Rule: Ensure that the Lifeline Advisors and Agents receive an adequate amount of system resources to properly balance workloads.

4. Start the primary Lifeline Advisor from a started procedure as a started program (EXEC PGM=). See Appendix A, “A sample started procedure for Lifeline Advisors,” on page 133 for a sample Advisor start procedure. Verify that each Lifeline Agent that you expect to connect to the Lifeline Advisor has connected. You can also use the NETSTAT CONN command on the Lifeline Advisor's TCP/IP stack to see which Lifeline Agents are currently connected. As Lifeline Agents connect to the Lifeline Advisor, messages appear on the MVS consoles where the Advisor and Agents are active.

Restriction: You cannot start the Lifeline Advisor under BPXBATCH.

5. Start one Lifeline Agent from a started procedure as a started program (EXEC PGM=) on each z/OS target system that you want to participate in this method of workload balancing. See Appendix B, "A sample started procedure for Lifeline Agents," on page 135 for a sample Agent start procedure.
 - a. Optional: Update the SCHEDxx member to add an entry to the program properties table to make the Lifeline Advisors and Agents run non-swappable.

Restriction:

- You can start only one Lifeline Agent per z/OS system.
 - You must not start the Lifeline Agent under BPXBATCH.
6. Optional: Start the secondary Lifeline Advisor. When the secondary Advisor connects to the primary Advisor, messages are issued on the MVS consoles where each Lifeline Advisor is running.
 7. Start the first-tier and second-tier load balancers. When an external load balancer has connected, a message is issued on the MVS console where the Lifeline Advisor is running.

Chapter 5. Diagnosing problems in Multi-site Workload Lifeline

You can verify the performance and availability of the system and diagnose problems when you use Multi-site Workload Lifeline.

Debug levels

You can update the debug level to change the level of debug messages to be logged.

The following list describes available debug levels and the associated syslogd priority levels:

Debug level

syslogd priority level

- | | |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0 | NONE. No messages of any kind are sent to the syslog file after initialization is complete. |
| 1 | ERROR. Error messages indicate something that requires attention. Messages at this level could be fatal (terminating) or could indicate that an integral part of the workload advising system is not working properly. This information is logged at the syslogd ERROR priority level. |
| 2 | WARNING. Warning messages indicate that an error has occurred, but it is not severe enough to warrant an ERROR. Corrective actions might be necessary because the Advisor or Agent might not be behaving as intended. This information is logged at the syslogd WARNING priority level. |
| 4 | EVENT. Event messages are logged for events that occur periodically, like operator commands, UNIX signals, timer pops, and receipt of a network message. This information is logged at the syslogd NOTICE priority level. |
| 8 | INFO. Informational messages are sent to the syslog file. These messages do not require corrective actions. This information is logged at the syslogd INFO priority level. |
| 16 | MESSAGE. Message messages log the contents of message packets that are sent between the Advisor and the Load Balancer, the Advisor and peer Advisor, or between the Advisor and Agent. You can use these messages to assist debugging Advisor-to-load balancer, Advisor-to-Advisor, and Advisor-to-Agent communications. This information is logged at the syslogd DEBUG priority level. This level is intended only for IBM service use. |
| 32 | COLLECTION. Collection messages log the details of collecting and manipulating the data that forms the basis of weight calculations. This information is logged at the syslogd DEBUG priority level. COLLECTION is only used by the Agent. This level is intended only for IBM service use. |
| 64 | DEBUG. The intention of this level of message is to provide information that is useful in debugging code, logic, or timing errors. This information is logged at the syslogd DEBUG priority level. This level is intended for IBM service use only. |

- 128 TRACE. Trace messages are intended for development or service to track code processing (footprints). This information is logged at the syslogd DEBUG priority level. This level is intended for IBM service use only.
-

Diagnostic data

You can collect multiple pieces of diagnostic data to diagnose problems.

The following diagnostic data is helpful:

- Console messages for the Lifeline Advisors and Agents
- Output from the MODIFY command for the Lifeline Advisors and Agents
- syslogd log messages for Lifeline Advisors and Agents
- Lifeline Advisor and Agent address space dumps and snap output
- TCP/IP packet traces of communication with the primary Lifeline Advisor

Guidelines:

- You do not have to run syslogd before running the Lifeline Advisors or Agents; however, syslogd is the only logging facility that either the Advisors or Agents are able to use.
- Useful diagnostic information might be lost if syslogd is not running before the Advisor or Agents are started.

The Lifeline Advisor and Agent trigger address space dumps when they encounter certain unexpected error conditions. Both a CEEDUMP and address space snap output are produced and written to the data sets or files that are specified by the started procedure CEEDUMP and CEESNAP DD statements, respectively.

If the Lifeline Advisor or Agent abnormally stops (for example, an 0C4abend occurs), an unformatted SYSMDUMP is produced and written to the data set that is specified by the started procedure SYSMDUMP DD statement. If you override the Language Environment® run-time option TERMTHDACT during the installation or started procedure, the SYSMDUMP might not be produced, or a CEEDUMP might be produced instead. Therefore, do not override the TERMTHDACT run-time option. See *z/OS Language Environment Programming Guide* for more information about run-time options.

In other situations, the z/OS operator needs to dump the address space manually.

You can collect the TCP/IP packet trace data of communication with the primary Lifeline Advisor. For example, you might need to capture the following communication flows:

- Server/Application State Protocol (SASP) protocol messages sent between the primary Advisor and external LBs
- Messages sent between the primary Advisor and Agents
- Messages sent between the primary and secondary Advisors

For details about how to use the TCP/IP packet trace facility, see *z/OS Communications Server: IP Diagnosis Guide*.

Verifying that the Lifeline Advisor and Agent systems are functioning correctly

View the MVS console and the syslogd files of the Lifeline Advisor and Agent systems to verify that the Lifeline Advisor and Agents are started and running.

About this task

View the MVS console of the Lifeline Advisor and Agent systems after they are started to verify that the applications are started and running. View the syslogd files of the Lifeline Advisor and Agent systems to determine whether any error or warning messages were issued.

If there are any failure messages, see Chapter 10, “Multi-site Workload Lifeline messages,” on page 91 for the corrective actions that you need to take.

Perform the following steps to verify that the Lifeline Advisors and Lifeline Agents are functioning correctly:

Procedure

1. Determine whether the Lifeline Advisor is started and connected to the expected external load balancers by issuing the following command on the Lifeline Advisor:

```
MODIFY procname,DISPLAY,LB
```

Verify that each external load balancer is displayed.

2. Determine whether each external load balancer configured and registered the proper groups and members with the Lifeline Advisor.

Tip: The Lifeline Advisor does not check for improperly configured members.

- a. After the entire Multi-site Workload Lifeline system is started and running, display all members registered by each external load balancer by issuing the following command:

```
MODIFY procname,DISPLAY,LB,DETAIL
```

This command displays all groups and members that are defined to each of the load balancers.

- b. Verify that each member that you expect to be available is flagged as available.
 - c. Screen unavailable members for coding errors, such as incorrect IP addresses, ports, or protocols.
3. Determine whether each Lifeline Agent has started correctly and is communicating with the Lifeline Advisor by issuing the following command on each Lifeline Agent:

```
MODIFY procname,DISPLAY,MEMBERS
```

Each registered member that has an IP address owned by the TCP/IP stack where the Lifeline Agent is active will appear in the display output.

4. Determine whether the target server applications that you want to load balance are available for load balancing. On the Lifeline Advisor, issue the following command:

```
MODIFY procname,DISPLAY,LB,DETAIL
```

- a. In the display output, check the AVAIL flag for each member. The flag is either YES, meaning that the member is available for load balancing, or NO, meaning that it is not available for load balancing.
- b. For first-tier external load balancers, to make the member available for load balancing, ensure that either of the following condition is true:
 - The external second-tier load balancers must be started and connected to the Lifeline Advisor.
 - The z/OS Sysplex Distributor acting as a second-tier load balancer must be configured on a z/OS image within the site, and the Lifeline Agent on that z/OS image must be active and communicating with the Lifeline Advisor.

If both of the conditions are false, correct the situation and repeat the display command until you are satisfied that all members that you intend to make available for load balancing are displayed as being available.

- c. For second-tier external load balancers, to make the member available for load balancing, ensure that all of the following conditions are true:
 - The Lifeline Agent must be active on the TCP/IP stack owning the IP address of the member and be communicating with the Lifeline Advisor.
 - The server application must be active.
 - The member must not be quiesced by the Lifeline Agent operator or the external load balancer. The Lifeline Agent is able to quiesce any member that is owned by the TCP/IP stack where the Agent is active. Depending on the external load balancer implementation, the load balancer administrator might quiesce individual members.

If one of the conditions is false, correct the situation and repeat the display command until you are satisfied that all members that you intend to make available for load balancing are displayed as being available.

Diagnosing problems when a workload is not distributed

When a workload is not being distributed to a server application, you can use the information in this topic to diagnose problems.

About this task

To determine why a workload is not being distributed to a server application, perform the following steps:

Procedure

1. Determine whether the Advisor is running and that an Agent is running on the MVS system that contains the server application. If they are not running, start the Advisor or Agent.
2. To determine whether any external load balancers have registered the server application, issue the following command on the Lifeline Advisor:
`MODIFY procname,DISPLAY,LB`

Verify that at least one first-tier load balancer is connected to the Advisor.

3. Determine whether the lb_id_list statement of the Advisor includes the IP address of the load balancer in question.
4. For external first-tier load balancers, determine whether the IP address of the member defined on the load balancer matches the IP address of a second-tier

load balancer responsible for load balancing to the server application. If not, correct the definition at the first-tier load balancer.

5. For external second-tier load balancers, determine whether the IP address, port number, and protocol of the member defined on the load balancer match the IP address, port number, and protocol of the server application. If not, correct the definition at the second-tier load balancer.

6. To check the member information on the Lifeline Advisor, issue the following command:

```
MODIFY procname,DISPLAY,LB,DETAIL
```

If the DISTDVIPA flag is displayed for the server application, verify that z/OS sysplex distributor is distributing workload requests to the server application. See *z/OS Communications Server: IP Diagnosis* for more information about diagnosing dynamic VIPA and sysplex problems.

7. Determine whether the agent_id_list statement of the Advisor contains the IP address and port that the Agent is bound to on the system where the server application exists. If not, correct the agent_id_list statement in the Advisor configuration or the host_connection statement in the Agent configuration.
8. To check the member information on the Agent, issue the following command:

```
MODIFY procname,DISPLAY,MEMBERS
```

If the protocol is UDP and the IP address of the server application is a distributed DVIPA address, no workload requests will be distributed for this server application on target TCP/IP stacks. Only the z/OS Sysplex Distributor TCP/IP stack advertises the DVIPA address, so only server applications running on this TCP/IP stack that binds to the DVIPA for UDP have workload requests distributed to it. Server applications that bind to the distributed DVIPA for protocol UDP on other TCP/IP stacks do not have workload requests distributed to them.

9. Determine whether network connectivity exists between the Advisor and the Agent in question. Unexpected loss of network connectivity between the Advisor and the Agent results in MVS console messages and related messages in the Agent and Advisor logs. To determine which Agents have connected to the Advisor, and by omission, which have not, issue the following Advisor command:

```
MODIFY procname,DISPLAY,ADVISOR
```

10. To determine whether the server application is available and enabled (not quiesced), issue the following Advisor command:

```
MODIFY procname,DISPLAY,LB,DETAIL
```

- a. If the server application is unavailable, start the server application.
- b. If the server application is quiesced, enable the server application by using either of the following commands:
 - If the second-tier load balancer is an external load balancer, issue the `MODIFY procname,ENABLE` command on the system where the Agent is active.
 - If the second-tier load balancer is z/OS sysplex distributor, issue the `VARY TCPIP,,SYSPLEX,RESUME` command on the system where the server application is active.
11. Check the syslog file for ERROR or WARNING messages and take the appropriate corrective actions. The syslogd identifier is `lladvsr` for the Advisor and `llagent` for the Agent. If ERROR and WARNING level log messages are not enabled, enable them and recheck the syslog file later.

12. Determine whether the first-tier load balancer has connectivity to the second-tier load balancer, and the second-tier load balancer has connectivity to the TCP/IP stack owning the IP address of the server application in question.
13. Issue the following Advisor command to determine whether the workload has been activated to one of the sites:
`MODIFY procname,DISPLAY,WORKLOAD`

If not, activate the workload by issuing the `MODIFY procname,ACTIVATE` command.

Diagnosing workload distribution problems

When workload distribution problems occur, you can use the information in this topic to diagnose problems.

About this task

To diagnose workload distribution problems, perform the following steps:

Procedure

1. To determine whether a first-tier load balancer has connected to the Lifeline Advisor, issue the following command:

```
MODIFY procname,DISPLAY,LB,DETAIL
```

Ensure that there are groups in the display with the `CROSS_SYSPLEX` group flag set, and that the IP addresses listed in those groups are the IP addresses of the second-tier load balancers.

2. Determine whether the update interval value of the Advisor is not abnormally large. The Advisor must wait at least two update intervals before beginning to receive enough data to properly calculate weights when a server application becomes available or when an Agent is started.
 - a. Allow at least three update intervals to expire after a server application is started before re-examining the distribution of workload.
 - b. If the workload is occasionally being sent to overloaded server applications, adjust the `update_interval` downward so workload distribution can react more quickly to the pace of new workload requests.
3. To check routing recommendations, periodically issue the following Advisor command to check the weights of members within the group in question.

```
MODIFY procname,DISPLAY,LB,DETAIL
```

Determine whether the weights are consistent with the expected behavior. If not, see “`MODIFY advisor_proc,DISplay` command: Display Lifeline Advisor information” on page 53 for more information about how to analyze the server application weights.

4. Determine whether the `agent_id_list` value of the Advisor contains the IP addresses and ports that each Agent is bound to on the MVS systems where the server application exists. If not, correct the `agent_id_list` statement in the Advisor configuration or the `host_connection` statement in the Agent configuration.
5. Determine whether members of the group in question are not unexpectedly quiesced or unexpectedly unavailable by issuing the following Advisor command:

```
MODIFY procname,DISPLAY,LB,DETAIL
```

- If AVAIL status is NO, correct the issue with the server application.
6. Check the syslog file for ERROR or WARNING messages and take the appropriate corrective actions. The syslogd identifier is lladvsr for the Advisor and llagent for the Agent. If ERROR and WARNING level log messages are not enabled, enable them and check the syslog file again later.

Diagnosing problems when the Lifeline Advisor or Agent appears hung

When the Lifeline Advisor or Agent appears hung, you can use the information in this topic to diagnose problems.

About this task

To diagnose problems when the Lifeline Advisor or Agent appears hung, perform the following steps:

Procedure

1. To determine whether the Lifeline Advisor or Agent is hung, issue the following command on the system where the Advisor or Agent is running:
`MODIFY procname,DISPLAY,DEBUG`

If you do not receive a response, attempt to stop the Advisor or Agent instead of cancelling the Advisor or Agent. If the Advisor or Agent does not terminate, it might be hung.
2. If the hang occurred when the DEBUG-level Advisor or Agent trace was in effect, collect the problem documentation by taking the following sub-steps and call IBM Service.
 - a. Take an SVC dump of the Agent or Advisor address space (depending on which is hung) and of the OMVS address space including its data spaces.
 - b. Capture the MVS console messages.
 - c. Capture the Advisor or Agent messages written to syslogd. The syslogd identifier is lladvsr for the Advisor and llagent for the Agent.
3. If DEBUG-level trace was not in effect at the time, turn on DEBUG-level Advisor or Agent trace, reproduce the problem, collect the problem documentation, and call IBM Service.

Diagnosing problems when the group names are not readable

When the group names are not readable, you can use the information in this topic to diagnose problems.

About this task

To diagnose problems when the group names are not readable, perform the following steps:

Procedure

1. Determine whether the group names defined in the load balancers use characters limited to the ASCII character set. When the load balancers define group names, the names are coded in UTF-8 format. This character set is a superset of the EBCDIC character set; not all characters are translatable to EBCDIC.

2. To make the group names readable, rename the group names in the load balancers to use characters limited to the ASCII character set.

Diagnosing problems when load balancer connection terminates

When the external load balancer connection to the Advisor terminates, you can use the information in this topic to diagnose problems.

About this task

Guideline: The Lifeline Advisor has an internal maximum message size of 128K bytes. If this limit is exceeded, the connection with the external load balancer is closed and an error message is logged stating that the message is too large and was not received.

To diagnose problems when the load balancer connection to the Lifeline Advisor terminates unexpectedly, perform the following steps:

Procedure

1. Determine whether the network administrator has shut down the external load balancer.
2. Determine whether TCP/IP connectivity still exists between the load balancer and the Advisor. For example, from the Advisor system, ping the IP address used by the load balancer.
3. Check the syslog file of the Advisor for ERROR or WARNING messages and take the appropriate corrective action. The syslogd identifier is `lladvsr` for the Advisor.
 - a. If an ERROR message indicating a `send()` operation failed with `errno = EDC8102I Operation would block` is issued, you might have registered too many groups or members from the load balancer. Increase the `TCPCONFIG TCPSENDBFRSIZE` statement in the TCP/IP profile where the Advisor is active, or register fewer groups and members from the load balancer, and then try restarting the external load balancer. For details about the `TCPCONFIG` statement, see *z/OS Communications Server: IP Configuration Reference*.
 - b. If ERROR and WARNING level log messages are not enabled, enable them, repeat the operation, and recheck the syslog file again.
4. Check the load balancer for errors.

Diagnosing problems when the Lifeline Agent connection terminates

When the Agent connection to the Advisor terminates, you can use the information in this topic to diagnose problems.

About this task

Guideline: The Advisor and Agent have an internal maximum message size of 128KB. If this limit is exceeded, the connection is closed and an error message is logged stating that the message is too large and was not received.

If the connection between a Lifeline Agent and Advisor terminates unexpectedly, perform the following steps to diagnose problems:

Procedure

1. Determine whether the MVS operator has shut down this Agent.
2. Determine whether TCP/IP connectivity still exists between the Agent and the Advisor. For example, from the Advisor system, ping the IP address used by the Agent.
3. Check the syslog file of the Advisor for ERROR or WARNING messages and take the appropriate corrective action. The syslogd identifier is `lladvsr` for the Advisor.
 - a. If an ERROR message indicating a `send()` operation failed with `errno = EDC8102I Operation would block` is issued, you might have registered too many groups or members that belong to the same Agent. Increase the `TCPCONFIG TCPSENDBFRSIZE` statement in the TCP/IP profile where the Advisor is active, or register fewer groups and members belonging to the Agent, and then try restarting the Agent. For details about the `TCPCONFIG` statement, see *z/OS Communications Server: IP Configuration Reference*.
 - b. If ERROR and WARNING level log messages are not enabled, enable them, repeat the operation, and recheck the log file again.

Diagnosing problems when the Lifeline Advisor to Advisor connection terminates

When the connection between the peer Lifeline Advisor and this Advisor terminates unexpectedly, you can use the information in this topic to diagnose problems.

About this task

To diagnose problems when the Advisor to Advisor connection terminates, perform the following steps:

Procedure

1. Determine whether the MVS operator has shut down the peer Advisor.
2. Determine whether TCP/IP connectivity still exists between the peer Advisor and the Advisor. For example, from the Advisor system, ping the IP address used by the peer Advisor.
3. Check the syslog file of the Advisor for ERROR or WARNING messages and take the appropriate corrective actions. The syslogd identifier is `lladvsr` for the Advisor.
4. Check the syslog file of the peer Advisor for ERROR or WARNING messages and take the appropriate corrective actions.

Diagnosing failures of registering with ARM

When the Lifeline Advisor or Agent fails to register with the Automatic Restart manager (ARM), you can use the information in this topic to diagnose problems.

About this task

To diagnose problems when the Lifeline Advisor or Agent fails to register with ARM, perform the following step:

Procedure

Check the warning-level message written to the syslog file. This log message is issued when the IXARM call fails with the return code and the reason code indicated in the log message. See *z/OS MVS Programming: Sysplex Services Reference* for information about interpreting the IXARM return code and reason code. One of the common causes of failure is the lack of a security profile. See Chapter 3, “Configuring Multi-site Workload Lifeline,” on page 11 for information about how to add an ARM security profile for the Advisor or Agent.

Chapter 6. Multi-site Workload Lifeline configuration statements

Multi-site Workload Lifeline configuration statements define the information needed to establish communication with an Advisor and external load balancers, an Advisor and Agents, and between peer Advisors.

Two types of Multi-site Workload Lifeline configuration statements are: Lifeline Advisor configuration statements and Lifeline Agent configuration statements.

Lifeline Advisor configuration statements

Use the following configuration statements to configure Lifeline Advisors.

Table 1. Lifeline Advisor Configuration Statements

Configuration statement	Allowed values	Default value	Required or optional	Purpose
advisor_connection_port	1 - 65535	None	Required	Specifies the port on which the primary Advisor listens for connections from a secondary Advisor.
advisor_id_list		None	Required	Specifies which secondary Advisors are allowed to connect to the primary Advisor.
advisor_takeover_policy	automatic manual	manual	Optional	Specifies the action that a secondary Advisor should take when it determines that a primary Advisor has stopped.
advisor_timeout	10 - 600 (in seconds)	10	Optional	Specifies how often the Advisor checks the availability of the peer Advisor.
agent_connection_port	1 - 65535	None	Required	Specifies the port on which the primary Advisor listens for connections from Agents.
agent_id_list		None	Required	Specifies which Agents are allowed to connect to the primary Advisor.
cross_sysplex_list		None	Required	Specifies the mapping of second-tier load balancers and their site name for a specific workload.
debug_level	0 - 255	7	Optional	Specifies the level of debug information that is logged.
failure_detection_interval	10 - 600 (in seconds)	60	Optional	Specifies the interval that the primary Advisor waits before determining a workload or site failure.
lb_connection_v4		None	Required (if lb_connection_v6 is not specified)	Specifies the IPv4 address and port on which the primary Advisor listens for connections from external load balancers.
lb_connection_v6		None	Required (if lb_connection_v4 is not specified)	Specifies the IPv6 address and port on which the primary Advisor listens for connections from external load balancers.
lb_id_list		None	Required	Specifies which external load balancers are allowed to connect to the primary Advisor.
peer_advisor_id		The IPv4 address on the lb_connection_v4 statement or, if not specified, the IPv6 address on the lb_connection_v6 statement	Optional	Specifies the IP address on the primary Advisor that the secondary Advisor uses to connect to.

Table 1. Lifeline Advisor Configuration Statements (continued)

Configuration statement	Allowed values	Default value	Required or optional	Purpose
update_interval	10 - 600 (in seconds)	10	Optional	Specifies how frequently the Agents update the primary Advisor with new information.
workload_switch_policy	automatic manual	manual	Optional	Specifies the action that the primary Advisor should take when it determines either the workload is unavailable on the active site or the active site for a workload is unavailable.

advisor_connection_port

Use the `advisor_connection_port` statement to specify the port that the primary Advisor should listen on for connections from a secondary Advisor.

Syntax

```
▶▶—advisor_connection_port—host_port—————▶▶
```

Parameters

host_port

Specifies which port the primary Advisor listens on for connections from a secondary Advisor. The valid range of port values is 1- 65535.

Requirement: This port number must match the port number specified in the `advisor_connection_port` configuration statement for the secondary Advisor.

Restriction: Do not specify the same port that is on the `agent_connection_port`, `lb_connection_v4`, or `lb_connection_v6` configuration statements; otherwise, the secondary Advisor will connect to the primary Advisor's socket that is used for processing Agent connections or load balancer connections.

advisor_id_list

Use the `advisor_id_list` statement to specify which secondary Advisors are allowed to connect to the primary Advisor. This list is also used by the secondary Advisor to select a source IP address when it is connecting to the primary Advisor.

Syntax

```
▶▶—advisor_id_list—{—advisor_ipaddr—}—————▶▶
```

Parameters

advisor_ipaddr

Specifies a list of secondary Advisors that are allowed to connect to the primary Advisor. The list consists of one or more blank-delimited IP address entries, each specified on a separate line and enclosed in braces. Each of these entries represents the IP address of a given secondary Advisor.

Requirement: Only complete IPv4 or IPv6 addresses are accepted. Host names, prefixes, or subnets are not allowed. The IPv4 INADDR_ANY address (0.0.0.0) and the IPv6 unspecified address (::) are not allowed. Each `advisor_ipaddr` entry must be specified on one line. The `advisor_ipaddr` cannot be continued to a subsequent line.

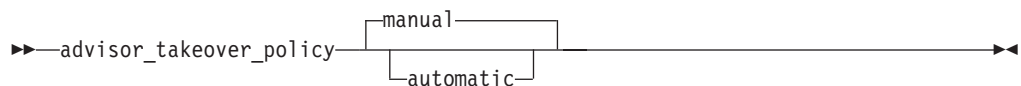
Guideline: You can dynamically update this statement by using the `MODIFY procname, REFRESH` command.

Requirement: You must also configure a local IP address for the primary Advisor in this list because it is used during initialization by the primary Advisor to determine whether another primary Advisor is currently active.

advisor_takeover_policy

Use the `advisor_takeover_policy` statement to specify the action that the secondary Advisor should take when it determines that the primary Advisor has stopped.

Syntax



Parameters

manual

Configures the secondary Advisor to wait for a `MODIFY procname, TAKEOVER` command before taking over as the primary Advisor. The default value is `manual`.

automatic

Configures the secondary Advisor to perform a takeover to become the primary Advisor.

Guideline: If automation is already in place to detect a primary Advisor failure, specifying `manual` will allow automation procedures to handle the takeover of the primary Advisor.

advisor_timeout

Use the `advisor_timeout` statement to specify how often the Advisor checks the availability of the peer Advisor.

Syntax



Parameters

interval

Specifies how frequently, in seconds, the Advisor checks the availability of the peer Advisor.

The valid range is 10 – 600 (in seconds). The default value is 10 seconds.

The configuration statement is used by the primary Advisor for the following reasons:

- During initialization to determine how long it waits before concluding that another primary Advisor is not active before becoming the primary Advisor.
- To determine how long to wait for the secondary Advisor to signal that it is available before declaring that the secondary Advisor is no longer active.

The configuration statement is used by the secondary Advisor for the following reason:

- To determine how long to wait for the primary Advisor to signal that it is available before declaring that the primary Advisor is no longer active.

agent_connection_port

Use the `agent_connection_port` statement to specify the port on which the primary Advisor should listen for connections from Agents.

Syntax

►►—agent_connection_port—host_port—————►►

Parameters

host_port

Specifies the port on which the primary Advisor listens for connections from Agents. The valid range of port values is 1- 65535.

Requirement: This port number must match the port number specified in the `advisor_id` configuration statement for the Agents.

Restriction: Do not specify the same port that is on the `advisor_connection_port`, `lb_connection_v4`, or `lb_connection_v6` configuration statement; otherwise, the Agent will connect to the primary Advisor's socket that is used for processing secondary Advisor connections or load balancer connections.

agent_id_list

Use the `agent_id_list` statement to specify which Agents are allowed to connect to the primary Advisor.

Syntax

►►—agent_id_list—{—agent_ipaddr..agent_port—}—————►►

Parameters

agent_ipaddr..agent_port

Specifies a list of Agents that are allowed to connect to the primary Advisor. The list consists of one or more blank-delimited IP address and port pairs, each

specified on a separate line and enclosed in braces. Each of these pairs represents the IP address and port of a given Agent. The valid range of port values is 1- 65535.

Rule: Do not put any spaces between the IP address, the two periods (.), and the port.

Requirement: Only complete IPv4 or IPv6 addresses are accepted. Host names, prefixes, or subnets are not allowed. The IPv4 INADDR_ANY address (0.0.0.0) and the IPv6 unspecified address (::) are not allowed. Each agent_ipaddr.agent_port pair must be specified on one line; it cannot be continued to a subsequent line.

Guideline: You can dynamically update this statement by using the MODIFY procname,REFRESH command.

If an Agent attempts to connect to the Advisor and the Agent's source IP address and port are not represented in this list, the connection is refused.

cross_sysplex_list

Use the cross_sysplex_list statement to specify the IP address and site name of each second-tier load balancer, the port of the application group used by the workload, and the workload name.

Syntax



Parameters

lb_ipaddr..appl_port,site,workload

Specifies a list of second-tier load balancers, the site the load balancer resides on, and the workload the load balancer is responsible for. The list consists of one or more blank-delimited IP address, port, site name, and workload name 4-tuples, each specified on a separate line and enclosed in braces. Each of these four-tuples represents the second-tier load balancer and the mapping of the site name and workload name for that workload. The valid range of port values is 1- 65535.

Rules:

- Do not put any spaces between the IP address, the two periods (.), the port, the comma (,), the site name, the comma (,), and the workload name.
- The site name corresponds to the MVS sysplex name for that site.

Requirements:

- Only complete IPv4 or IPv6 addresses are accepted. Host names, prefixes, or subnets are not allowed. The IPv4 INADDR_ANY address (0.0.0.0) and the IPv6 unspecified address (::) are not allowed.

- The workload name can consist of alphanumeric characters as well as the @, #, \$, -, and _ characters. The first character must be an alphabet character. The length of the workload name cannot exceed 64 characters.
- Each *lb_ipaddr.appl_port.site,workload* 4-tuple must be specified on one line; it cannot be continued to a subsequent line.

Restriction: You can specify only two unique site names in this list.

Guidelines:

- You can dynamically update this statement by using the *MODIFY procname,REFRESH* command.
- The second-tier load balancer IP address can be either the IP address of the external load balancer residing in the site, or the dynamic virtual IP address (VIPA) that is distributed by the z/OS sysplex distributor residing on a system image in the site.
- If a workload consists of multiple application groups, each application group must be specified with its own 4-tuple entry, and must be unique with other 4-tuple entries that are defined for the workload by specifying a different second-tier load balancer IP address or a different port.

If a first-tier load balancer attempts to connect to the primary Advisor and register second-tier load balancers that are not represented in this list, the connection is refused.

debug_level

Use the *debug_level* statement to specify the level of debug information that is logged.

Syntax



Parameters

level

Specifies the debug level. All log messages are written to syslogd. The level value represents a particular debug level or combination of debug levels. See “Debug levels” on page 27 for the possible values. The default level is 7, which means that all error, warning, and event messages are captured.

The valid range is 0 – 255.

Guidelines:

- You can dynamically update this statement by using the *MODIFY procname,DEBUG* command.
- To log a combination of debug levels, add the debug level numbers.

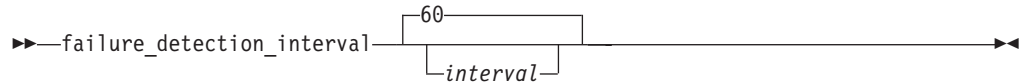
Restriction: Do not customize this statement unless you are directed to do so by an IBM Service representative. Adding additional types of trace data

can cause the amount of data captured to become voluminous. Reducing the amount of trace data from the default might make diagnosing a problem more difficult.

failure_detection_interval

Use the `failure_detection_interval` statement to specify how long the primary Advisor waits for determining that a workload is no longer available on a site or that a site is no longer available.

Syntax



Parameters

interval

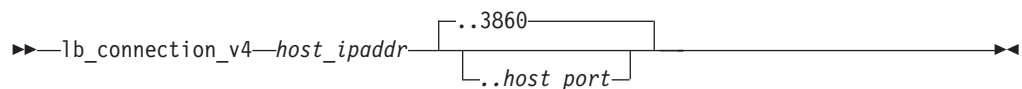
Specifies how long the primary Advisor waits for an indication that a workload or site is available. The valid range is 10 – 600 in seconds. The default interval is 60 seconds.

Requirement: The *interval* value cannot be less than the value specified on the `update_interval` statement.

lb_connection_v4

Use the `lb_connection_v4` statement to specify the IPv4 address and port that the primary Advisor should listen on for connections from external load balancers.

Syntax



Parameters

host_ipaddr..host_port

Specifies which IPv4 address, and optionally, the port, on which the primary Advisor listens for IPv4 connections from an external load balancer. This IP address and port must be coordinated on any load balancers that will connect to this Advisor. The port is optional. The default value is 3860.

The valid range of port values is 1- 65535.

Rule: If you specify the port, do not use spaces between the IP address, the two periods (..), and the port.

Requirement: Only a complete IPv4 address is accepted. Host names, prefixes, or subnets are not allowed. The IPv4 INADDR_ANY address (0.0.0.0) is not allowed.

This statement is optional. However, if neither a `lb_connection_v4` nor `lb_connection_v6` statement is present in the configuration file, a terminating error

occurs. If you specify this statement, you must specify at least one IPv4 address in the `lb_id_list` statement or a terminating error occurs.

Guideline: Define the IPv4 address as a VIPARANGE dynamic VIPA. This allows external load balancers and Agents to reconnect to this IP address when the secondary Advisor takes over as the primary Advisor and moves the dynamic VIPA to the host on which the secondary Advisor is active.

Restriction: Do not specify the same port that is on the `advisor_connection_port` or `agent_connection_port` configuration statements; otherwise, the Agents and secondary Advisor will connect to the primary Advisor's socket that is used for processing load balancer connections.

lb_connection_v6

Use the `lb_connection_v6` statement to specify the IPv6 address and port that the primary Advisor should listen on for connections from external load balancers.

Syntax

```
▶▶ lb_connection_v6 host_ipaddr [..3860] [..host_port] ▶▶
```

Parameters

host_ipaddr..host_port

Specifies which IPv6 address, and optionally the port, that the primary Advisor listens on for IPv6 connections from an external load balancer. This IP address and port must be coordinated on any load balancers that will connect to this Advisor. The port is optional. The valid range of port values is 1- 65535. The default value is 3860.

Rule: If you specify the port, do not use spaces between the IP address, the two periods (..), and the port.

Requirement: Only a complete IPv6 address is accepted. Host names, prefixes, or subnets are not allowed. The IPv6 unspecified address (::) is not allowed.

This statement is optional. However, if neither a `lb_connection_v4` nor `lb_connection_v6` statement is present in the configuration file, a terminating error occurs. If this statement is specified, you must specify at least one IPv6 address in the `lb_id_list` statement or a terminating error occurs.

Guideline: Define the IPv6 address as a VIPARANGE dynamic VIPA. This allows external load balancers and Agents to reconnect to this IP address when the secondary Advisor takes over as the primary Advisor and moves the dynamic VIPA to the host on which the secondary Advisor is active.

Restriction: Do not specify the same port that is on the `advisor_connection_port` or `agent_connection_port` configuration statements; otherwise, the Agents and secondary Advisor will connect to the primary Advisor's socket that is used for processing load balancer connections.

lb_id_list

Use the `lb_id_list` statement to specify which external load balancers are allowed to connect to the primary Advisor.

Syntax

```
▶▶ lb_id_list { lb_ipaddr } ▶▶
```

Parameters

lb_ipaddr

Specifies a list of external load balancers that are allowed to connect to the primary Advisor. The list consists of one or more blank-delimited IP address entries, each specified on a separate line and enclosed in braces. Each of these entries represents the IP address of a given secondary Advisor.

Requirement: Only complete IPv4 or IPv6 addresses are accepted. Host names, prefixes, or subnets are not allowed. The IPv4 INADDR_ANY address (0.0.0.0) and the IPv6 unspecified address (::) are not allowed. You must specify each `lb_ipaddr` entry on one line; it cannot be continued to a subsequent line.

If an external load balancer attempts to connect to the primary Advisor and the load balancer's source IP address is not represented in this list, the connection is refused.

Guidelines:

- You can dynamically update this statement by using the `MODIFY procname, REFRESH` command.
- You must configure all external load balancers, both first-tier and second-tier, in this list. If a z/OS sysplex distributor is acting as a second-tier load balancer, do not configure it in this list.

Rule: If you specify an IPv4 address, you must specify the `lb_connection_v4` statement or a terminating error occurs. Similarly, if you specify an IPv6 address, you must specify the `lb_connection_v6` statement or a terminating error occurs.

peer_advisor_id

Use the `peer_advisor_id` statement to specify the IP address of the primary Advisor that this secondary Advisor communicates with.

Syntax

```
▶▶ peer_advisor_id advisor_ipaddr ▶▶
```

Parameters

advisor_ipaddr

Specifies the IPv4 or IPv6 address which the Advisor, when acting as the secondary Advisor, uses as the destination IP address to connect to the primary Advisor.

Requirements:

- Only a complete IPv4 or IPv6 address is accepted. Hostnames, prefixes, or subnets are not allowed. The IPv4 INADDR_ANY address (0.0.0.0) and the IPv6 unspecified address (::) are not allowed.
- The IP address must match either the IPv4 address specified on the `lb_connection_v4` configuration statement or the IPv6 address specified on the `lb_connection_v6` configuration statement for the primary Advisor.

This statement is optional. If you do not specify the statement, it defaults to either the IPv4 address specified on the `lb_connection_v4` statement, if configured, or the IPv6 address specified on the `lb_connection_v6` statement.

update_interval

Use the `update_interval` statement to specify how often Agents update the primary Advisor with new information. You can also use this statement to determine how often the Advisor queries the status of each of the systems in both sites using BCPii communication.

Syntax



Parameters

interval

Specifies how frequently Agents update the primary Advisor with new information. At each interval, all Agents update the primary Advisor with the following status information for each registered member, which is the application server that the Agent is responsible for:

- Whether the target server application is active or inactive
- Whether the operator quiesced the target server application
- Various metrics that measure the target system
- The ability of the target server application to handle additional workload requests

The valid range is 10 – 600 in seconds. The default interval is 10 seconds.

Requirement: The *interval* value cannot be greater than the value specified on the `failure_detection_interval` statement.

The lower the update interval is, the more up-to-date the recommendations provided to the external load balancer will be with respect to the target's availability and capability to handle additional workload requests. However, the lower the update interval is, the higher the network traffic and CPU overhead are.

Depending on how the external load balancers are configured and implemented, the `update_interval` statement might also determine how often the external load balancer is updated with data from the primary Advisor. If the external load balancer supports the SASP push flag, and if the flag is set in the load balancer, the primary Advisor sends recommendations to the load balancer at least every update interval. Regardless of what value is set for the update interval, if the push flag is supported and configured in the load balancer, the Advisor might update the load balancer with recommendations before the update interval expires. Events that can trigger an earlier update include starting or stopping a target server application, or the addition or deletion of a member's IP address on the Agent host.

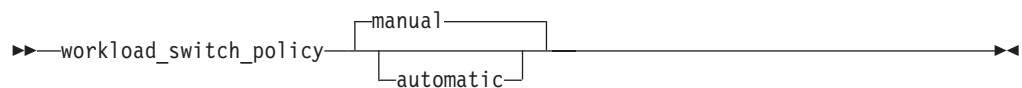
The update interval is a key factor in determining the latency period between when changes occur on the target system and when the load balancer is informed of them. Each Agent updates the primary Advisor with new information every update interval. The Advisor, in turn, updates the load balancer with changes in recommendations every update interval, if the load balancer supports the push flag. If the push flag is supported and configured in the load balancer, the Advisor updates the load balancer with any changes in the availability status of the target system and server application when it discovers such a change from the Agent, instead of waiting for the update interval to expire.

When the external load balancer supports and is configured for the push flag, the maximum amount of latency expected between a change in the member's recommendation and when the load balancer is informed of it, is twice the value of the update interval: one update interval for the Agent to report it to the primary Advisor, and one update interval for the Advisor to report it to the load balancer. However, on average, it takes about one update interval for a change in the target server application's recommendation to reach the load balancer.

workload_switch_policy

Use the `workload_switch_policy` statement to specify the action that the primary Advisor should take when it determines either that a workload is no longer available on the active site or the active site for a workload is unavailable.

Syntax



Parameters

manual

Configures the primary Advisor to wait for a `MODIFY procname,ACTIVATE` command before redistributing the workload to the alternate site. The default policy is manual.

automatic

Configures the primary Advisor to activate the redistribution of the workload to the alternate site.

Guidelines: If automation is already in place to detect a workload or site failure, specifying manual will allow automation procedures to handle the redistribution of the workload to the alternate site.

Lifeline Agent configuration statements

Use the following configuration statements to configure Lifeline Agents.

Table 2. Lifeline Agent Configuration Statements

Configuration Statement	Allowed values	Default Value	Required/Optional	Purpose
advisor_id		None	Required, if advisor_id_list is not specified	Specifies the IP address and port on the primary Advisor that the Agent connects to.
advisor_id_list		None	Required, if advisor_id is not specified	Specifies the list of IP address and port pairs on the primary Advisor that the Agent connects to.
debug_level	0 - 255	7	Optional	Specifies the level of debug information that is logged.
host_connection		None	Required	Specifies the local IP address and port the Agent binds to before connecting to the primary Advisor.

advisor_id

Use the `advisor_id` statement to specify the IP address and port of the primary Advisor that this Agent communicates with.

Syntax

►►—`advisor_id`—`advisor_ipaddr..advisor_port`—►►

Parameters

`advisor_ipaddr..advisor_port`

Specifies the IP address and port of the primary Advisor that this Agent communicates with. The valid range of port values is 1- 65535.

Rule: Do not use spaces between the IP address, the two periods (.), and the port.

Requirements:

- This port number must match the port number specified in the `agent_connection_port` configuration statement for the Advisor.
- Only a complete IPv4 or IPv6 address is accepted. Host names, prefixes, or subnets are not allowed. The IPv4 `INADDR_ANY` address (0.0.0.0) and the IPv6 unspecified address (::) are not allowed. The IP address must match either the `lb_connection_v4` or `lb_connection_v6` IP address.

Rule: If you specify an IPv4 address on this statement, you must also specify an IPv4 address on the `host_connection` statement. Similarly, if you specify an IPv6 address on this statement, you must also specify an IPv6 address on the `host_connection` statement.

This statement is optional. However, if neither an `advisor_id_list` nor `advisor_id` statement is present in the configuration file, a terminating error occurs. If this statement is specified, the `advisor_id_list` statement cannot be specified, or a terminating error occurs.

advisor_id_list

Use the `advisor_id_list` statement to specify the IP address and port pairs of the primary Advisors that this Agent communicates with.

Syntax

The diagram shows the syntax for the `advisor_id_list` statement. It starts with a right-pointing arrow followed by the text `advisor_id_list`. This is followed by a curly brace containing the text `advisor_ipaddr..advisor_port`. A bracket above the curly brace indicates that the content inside is repeated. The diagram ends with a right-pointing arrow.

Parameters

advisor_ipaddr..advisor_port

Specifies the IPv4 or IPv6 addresses and port of the primary Advisors that this Agent communicates with. The valid range of port values is 1- 65535. The Agent loops through all IP addresses until it successfully connects to the primary Advisor using one of these IP addresses. Each IP address must match either the `lb_connection_v4` or `lb_connection_v6` IP address of an Advisor.

Requirements:

- Only complete IPv4 or IPv6 addresses are accepted. Host names, prefixes, or subnets are not allowed. The IPv4 INADDR_ANY address (0.0.0.0) and the IPv6 unspecified address (::) are not allowed.
- Each `advisor_ipaddr..advisor_port` 2-tuple must be specified on one line; it cannot be continued to a subsequent line.

Rules:

- Do not put any spaces between the IP address, the two periods (.), and the port.
- The IP addresses specified must be either all IPv4 addresses or all IPv6 addresses. Do not mix IPv4 and IPv6 addresses in the list.
- If you specify IPv4 addresses on this statement, you must also specify an IPv4 address on the `host_connection` statement. Similarly, if you specify IPv6 addresses on this statement, you must also specify an IPv6 address on the `host_connection` statement.

This statement is optional. However, if neither an `advisor_id` nor `advisor_id_list` statement is present in the configuration file, a terminating error occurs. If this statement is specified, the `advisor_id` statement cannot be specified, or a terminating error occurs.

debug_level

Use the `debug_level` statement to specify the level of debug information that is logged.

Syntax

The diagram shows the syntax for the `debug_level` statement. It starts with a right-pointing arrow followed by the text `debug_level`. This is followed by a bracket containing the text `interval`. A small '7' is positioned above the bracket, indicating a range of values. The diagram ends with a right-pointing arrow.

Parameters

level

Specifies the debug level. All log messages are written to syslogd. The level value represents a particular debug level or combination of debug levels. See “Debug levels” on page 27 for the possible values. The default level is 7, which means that all error, warning, and event messages are captured.

The valid range is 0 – 255.

Guidelines:

- You can dynamically update this statement by using the `MODIFY procname,DEBUG` command.
- To log a combination of debug levels, add the debug level numbers.

Restriction: Do not customize this statement unless you are directed to do so by an IBM Service representative. Adding additional types of trace data can cause the amount of data captured to become voluminous. Reducing the amount of trace data from the default might make diagnosing a problem more difficult.

host_connection

Use the `host_connection` statement to specify the local IP address and port that the Agent binds to for communicating with the primary Advisor.

Syntax

►►—`host_connection—host_ipaddr..host_port`—————►►

Parameters

host_ipaddr..*host_port*

Use `host_ipaddr..host_port` to specify the IP address and port that this Agent binds to.

The valid range of port values is 1- 65535.

Requirement: Only a complete IPv4 or IPv6 address is accepted. Host names, prefixes, or subnets are not allowed. The IPv4 INADDR_ANY address (0.0.0.0) and the IPv6 unspecified address (::) are not allowed. The IP address and port must match one of the IP address and port pairs specified in the `agent_id_list` configuration statement for the Advisor.

Rule: If you specify an IPv4 address on the `host_connection` statement, you must specify an IPv4 address on the `advisor_id` statement. Similarly, if you specify an IPv6 address on the `host_connection` statement, you must specify an IPv6 address on the `advisor_id` statement.

Guidelines:

- To ensure high availability, specify the IP addresses in the `agent_id_list` statement for the Advisor and the `host_connection` statement for each Agent as static VIPAs, so that individual link outages on the hosts are tolerated.

- To ensure simplicity and consistency, specify the same port for this statement for each Agent, and reserve this port on each TCP/IP stack where an Agent will be active.
- You can specify an IPv6 address on this statement if the host where the Agent resides is an IPv6-enabled TCP/IP stack, and the Advisor resides on an IPv6-enabled TCP/IP stack.

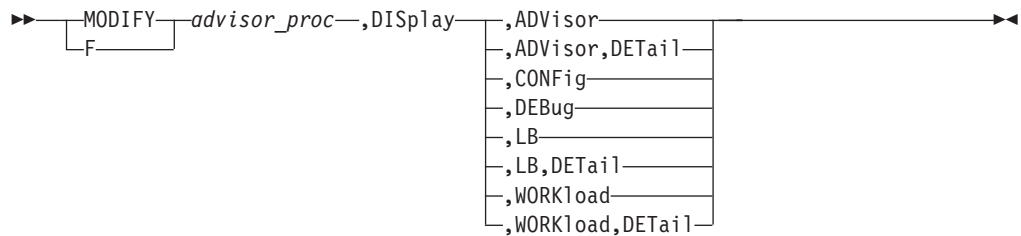
Chapter 7. Lifeline Advisor commands

Use the Life Advisor commands to display Lifeline Advisor information and modify Lifeline Advisor state information.

MODIFY *advisor_proc*,DISplay command: Display Lifeline Advisor information

The MODIFY *advisor_proc*,DISplay command displays the information related to the Lifeline Advisor.

Format



Parameters

advisor_proc

Indicates the member name of the cataloged procedure used to start the Advisor.

DISplay,ADVisor

Displays information about the external load balancers, Agents, and peer Advisor that are connected to this Advisor. When you issue this command on the secondary Advisor with this parameter, only the peer Advisor information is displayed.

DISplay,ADVisor,DETAil

Displays additional information, including the system name and site name where each Agent is and the system name where the peer Advisor is. When you issue this command on the secondary Advisor with this parameter, only the peer Advisor information is displayed.

DISplay,CONFig

Displays the active configuration for this Advisor.

DISplay,DEBUg

Displays the debug level in effect for this Advisor.

The debug level displayed is the sum of one or more levels of debug messages being logged. See “Debug levels” on page 27 for more information about the debug levels.

DISplay,LB

Displays information about the load balancers that are connected to the primary Advisor. You can specify this parameter only on the primary Advisor.

DISplay, LB, DETail

Displays additional information, including the register groups and member data for each load balancer. You can specify this parameter only on the primary Advisor.

DISplay, WORKload

Displays information about the workloads and their current state. You can specify this parameter only from the primary Advisor.

DISplay, WORKload, DETail

Displays additional information, including the server applications that make up each workload. You can specify this parameter only from the primary Advisor.

Examples

The following example shows a sample display when you issue F AQSADV, DISPLAY, ADVISOR on the primary Advisor.

```
F AQSADV, DISPLAY, ADVISOR
AQS0141I ADVISOR SUMMARY
ADVISOR ROLE   : PRIMARY
IPADDR        : 192.10.1.1
LOAD BALANCERS:
  IPADDR      : 192.10.1.32
  TIER        : 1
  IPADDR      : 192.10.1.64
  TIER        : 2
AGENTS        :
  IPADDR      : 192.10.110.1
  IPADDR      : 192.10.110.2
  IPADDR      : 192.20.110.1
  IPADDR      : 192.20.110.2
PEER ADVISOR  :
IPADDR        : 192.20.1.1
```

The following example shows a sample display when you issue F AQSADV, DISPLAY, ADVISOR on the secondary Advisor.

```
F AQSADV, DISPLAY, ADVISOR
AQS0141I ADVISOR SUMMARY
ADVISOR ROLE   : SECONDARY
IPADDR        : 192.20.1.1
PEER ADVISOR  :
IPADDR        : 192.10.1.1
```

The following information describes the fields in the previous sample display.

Field name**Descriptions****ADVISOR ROLE**

The current role and IP address for this Advisor. The IP address can be an IPv4 or an IPv6 address. The Advisor role has the following values:

PRIMARY

Indicates that this Lifeline Advisor is responsible for the following tasks:

- Communicating with the Agents to retrieve information about the systems and server applications that are being monitored
- Communicating with external load balancers to provide routing recommendations for incoming requests for the configured workloads

- Communicating with the secondary Advisor to provide state information for the configured workloads

SECONDARY

Indicates that this Lifeline Advisor is responsible for communicating with the primary Advisor to monitor whether this Advisor needs to take over the primary Advisor responsibilities.

LOAD BALANCERS

The list of external load balancers connected to this Advisor, the IP address of each load balancer, and the tier level of each load balancer. The IP address can be an IPv4 or an IPv6 address. The LOAD BALANCERS field is displayed only when you issue the command on the primary Advisor and at least one load balancer is connected. The tier can be one of the following values:

- 1 Indicates that this load balancer is a first-tier load balancer. The load balancer is responsible for selecting the site that an inbound workload request is routed to.
- 2 Indicates that this load balancer is a second-tier load balancer. The load balancer is responsible for selecting the server application instance in a site that an inbound workload request is routed to.

AGENTS

The list of Lifeline Agents connected to this Advisor and the IP address of the Agent. The IP address can be an IPv4 or an IPv6 address. The AGENTS field is displayed only when you issue the command on the primary Advisor and at least one Agent is connected.

PEER ADVISOR

The IP address of the peer Advisor that is connected to this Advisor. The IP address can be an IPv4 or an IPv6 address. If no peer Advisor is connected, the IP address is displayed as NONE.

The following example shows a sample display when you issue F AQSADV,DISPLAY,ADVISOR,DETAIL on the primary Advisor.

```
F AQSADV,DISPLAY,ADVISOR,DETAIL
AQS0142I ADVISOR DETAILS
ADVISOR ROLE   : PRIMARY
IPADDR        : 192.10.1.1
LOAD BALANCERS:
IPADDR   : 192.10.1.32
TIER     : 1
IPADDR   : 192.10.1.64
TIER     : 2
AGENTS   :
IPADDR   : 192.10.110.1
SYSTEM NAME : SYS1A      SITE : PLEX1
IPADDR   : 192.10.110.2
SYSTEM NAME : SYS1B      SITE : PLEX1
IPADDR   : 192.20.110.1
SYSTEM NAME : SYS2A      SITE : PLEX2
IPADDR   : 192.20.110.2
SYSTEM NAME : SYS2B      SITE : PLEX2
PEER ADVISOR :
IPADDR      : 192.20.1.1
SYSTEM NAME : CNTL2
```

The following example shows a sample display when you issue F AQSADV,DISPLAY,ADVISOR,DETAIL on the secondary Advisor.

```

F AQSADV,DISPLAY,ADVISOR,DETAIL
AQS0142I ADVISOR DETAILS
ADVISOR ROLE   : SECONDARY
IPADDR        : 192.20.1.1
PEER ADVISOR  :
IPADDR        : 192.10.1.1
SYSTEM NAME   : CNTL1

```

The following information describes the fields in the previous sample display.

Field name

Descriptions

ADVISOR ROLE

The current role and IP address for this Advisor. The IP address can be an IPv4 or an IPv6 address. The role has the following values:

PRIMARY

Indicates that this Advisor is responsible for the following tasks:

- Communicating with the Agents to retrieve information about the systems and server applications that are being monitored
- Communicating with external load balancers to provide routing recommendations for incoming requests for the configured workloads
- Communicating with the secondary Advisor to provide state information for the configured workloads

SECONDARY

Indicates that this Advisor is responsible for communicating with the primary Advisor to monitor whether this Advisor needs to take over the primary Advisor responsibilities.

LOAD BALANCERS

The list of external load balancers connected to this Advisor, the IP address of the load balancer, and the tier level of the load balancer. The IP address can be an IPv4 or an IPv6 address. The LOAD BALANCERS field is only displayed when you issue the command on the primary Advisor and at least one load balancer is connected. The tier has the following values:

- 1 Indicates that this load balancer is a first-tier load balancer. The load balancer is responsible for selecting the site that an inbound workload request will be routed to.
- 2 Indicates that this load balancer is a second-tier load balancer. The load balancer is responsible for selecting the server application instance within a site that an inbound workload request will be routed to.

AGENTS

The list of Lifeline Agents connected to this Advisor and the IP address of the Agent. The IP address can be an IPv4 or an IPv6 address. The AGENTS field is only displayed when you issue the command on the primary Advisor and at least one Agent is connected.

SYSTEM NAME

The MVS system name where the connected Agent or peer Advisor is active. If no peer Advisor is connected, this field is not displayed in the PEER ADVISOR section.

SITE The MVS sysplex name of the system where the connected Agent exists.

PEER ADVISOR

The IP address of the peer Advisor that is connected to this Advisor. The IP address can be an IPv4 or an IPv6 address. If no peer Advisor is connected, the IP address is displayed as NONE.

The following example shows a sample display when you issue F AQSADV,DISPLAY,CONFIG.

```
F AQSADV,DISPLAY,CONFIG
AQS0143I ADVISOR CONFIGURATION
CONFIG FILENAME   : USER.PROFILES(LBADVCNF)
DEBUG LEVEL      : 7
ADVISOR CONN PORT : 8200
ADVISOR ID LIST   :
  IPADDR : 192.10.1.1
  IPADDR : 192.20.1.1
ADVISOR TIMEOUT   : 10
ADVISOR TAKEOVER POLICY : MANUAL
AGENT CONN PORT   : 8181
AGENT ID LIST     :
  IPADDR..PORT : 192.10.110.1..4000
  IPADDR..PORT : 192.10.110.2..4000
  IPADDR..PORT : 192.20.110.1..4000
  IPADDR..PORT : 192.20.110.2..4000
UPDATE INTERVAL  : 10
FAILURE DETECTION INTERVAL : 60
LB CONNECTION V4 : 192.10.1.1..3860
LB CONNECTION V6 : 192::10:1:1..3860
LB ID LIST       :
  IPADDR : 192.10.1.32
  IPADDR : 192.10.1.64
WORKLOAD SWITCH POLICY : MANUAL
CROSS SYSPLEX LIST :
  IPADDR..PORT : 192.10.1.64..5001
  SITE        : PLEX1
  WORKLOAD    : WORKLOAD1
  IPADDR..PORT : 10.20.1.1..5001
  SITE        : PLEX2
  WORKLOAD    : WORKLOAD1
  IPADDR..PORT : 192.10.1.64..6001
  SITE        : PLEX1
  WORKLOAD    : WORKLOAD1
  IPADDR..PORT : 10.20.1.1..6001
  SITE        : PLEX2
  WORKLOAD    : WORKLOAD1
  IPADDR..PORT : 10.10.1.1..8020
  SITE        : PLEX1
  WORKLOAD    : WORKLOAD2
  IPADDR..PORT : 10.20.1.1..8020
  SITE        : PLEX2
  WORKLOAD    : WORKLOAD2
  IPADDR..PORT : 10.10.1.1..8021
  SITE        : PLEX1
  WORKLOAD    : WORKLOAD2
  IPADDR..PORT : 10.20.1.1..8021
  SITE        : PLEX2
  WORKLOAD    : WORKLOAD2
```

The following information describes the fields in the previous sample display.

Field name

Descriptions

CONFIG FILENAME

The configuration file used by this Advisor when the Advisor was initially started.

DEBUG LEVEL

The debug level currently in effect for this Advisor.

ADVISOR CONN PORT

The port number that the primary Advisor listens on for connections from a peer Advisor.

ADVISOR ID LIST

The list of the IP addresses of secondary Advisors that are permitted to connect to the primary Advisor. The IP address can be an IPv4 or an IPv6 address.

ADVISOR TIMEOUT

The interval (in seconds) that the primary Advisor uses to determine whether another primary Advisor is active. The interval used by the secondary Advisor to determine whether the primary Advisor is down.

ADVISOR TAKEOVER POLICY

The action that a secondary Advisor takes when it determines that the primary Advisor is down. The takeover policy allows the following values:

AUTOMATIC

Indicates that the secondary Advisor automatically takes over the primary Advisor responsibilities.

MANUAL

Indicates that the secondary Advisor waits until a `MODIFY AQSADV, TAKEOVER` command is issued before the secondary Advisor takes over the primary Advisor responsibilities.

AGENT CONN PORT

The port number that the primary Advisor listens on for connections from Agents.

AGENT ID LIST

The list of IP addresses of Agents that are permitted to connect to the primary Advisor. The IP address can be an IPv4 or an IPv6 address.

UPDATE INTERVAL

The interval (in seconds) that an Agent uses to update the primary Advisor with information about the system and server applications being monitored. Depending on how the external load balancer is configured, the `update_interval` statement might also determine how often the load balancer is updated with data from the Lifeline Advisor.

FAILURE DETECTION INTERVAL

The interval (in seconds) that a primary Advisor uses to detect a workload failure or site failure.

LB CONNECTION V4

The IPv4 address and port number that the primary Advisor listens on for connections from external load balancers.

LB CONNECTION V6

The IPv6 address and port number the primary Advisor listens on for connections from external load balancers.

LB ID LIST

The list of the IP addresses of external load balancers that are permitted to connect to the primary Advisor. The IP address can be an IPv4 or an IPv6 address.

WORKLOAD SWITCH POLICY

The action that a primary Advisor takes when it determines that a workload is no longer active. The switch policy allows the following values:

AUTOMATIC

Indicates that the primary Advisor automatically reroutes a failing workload to the alternate site.

MANUAL

Indicates that the primary Advisor waits until a MODIFY AQSADV,ACTIVATE command is issued before the primary Advisor reroutes a failing workload to the alternate site.

CROSS SYSPLEX LIST

The list of both the external and internal second-tier load balancers IP addresses, the site name (that is, sysplex name) that identifies each second-tier load balancer, the port number of the server application used for a specific workload, and the workload name. The IP address can be an IPv4 or an IPv6 address.

The following example shows a sample display when you issue F AQSADV,DISPLAY,DEBUG.

```
F AQSADV,DISPLAY,DEBUG
AQS0111I LLADVSR DEBUG LEVEL 7
```

The following example shows a sample display when you issue F AQSADV,DISPLAY,LB.

```
F AQSADV,DISPLAY,LB
AQS0112I LOAD BALANCER SUMMARY
LB INDEX      : 00          UUID      : F956AE65
IPADDR..PORT  : 192.10.1.64..55764
HEALTH        : 7E          FLAGS     : NOCHANGE PUSH
LB INDEX      : 01          UUID      : 9A78BE9E
IPADDR..PORT  : 192.10.1.32..40366
HEALTH        : 7E          FLAGS     : NOCHANGE PUSH
2 OF 2 RECORDS DISPLAYED
```

The following information describes the fields in the previous sample display.

Field name

Descriptions

LB INDEX

The reference number used to identify the load balancer. The same reference number is used for a load balancer as long as it remains connected.

UUID A hexadecimal value of the universally unique identifier assigned by the load balancer. This byte array can be up to 64 bytes in length. Only one load balancer with the same UUID can be connected to the primary Advisor at the same time.

IPADDR..PORT

The IP address and port number used by the load balancer to connect to the primary Advisor. The IP address can be an IPv4 or an IPv6 address.

HEALTH

A hexadecimal value supplied by the load balancer that indicates the general health of the load balancer. Valid values are in the range from 0 to X'7F'.

FLAGS

Indicators set by the load balancer. The flag values are shown as follows:

NOCHANGE

Indicates that the primary Advisor sends only weights that have changed since the last update interval to the load balancer.

PUSH Indicates that the primary Advisor sends weights to external load balancers when the update_interval has expired. If this flag is not present, the load balancer retrieves weights from the primary Advisor.

TRUST

Indicates that the load balancer trusts member applications to register themselves. This flag is ignored by the primary Advisor.

The following example shows a sample display when you issue F AQSADV,DISPLAY,LB,DETAIL.

```
F AQSADV,DISPLAY,LB,DETAIL
AQS01131 LOAD BALANCER DETAILS
LB INDEX      : 00          UUID      : F956AE65
IPADDR..PORT  : 192.10.1.64..55764
HEALTH        : 7E          FLAGS     : NOCHANGE PUSH
GROUP NAME    : WKLD2_GROUP1
WORKLOAD      : WORKLOAD2
GROUP FLAGS   : CROSS_SYSPLEX
IPADDR..PORT  : 10.10.1.1..8020
SYSPLEX      : PLEX1
SYSTEM NAME   : N/A          PROTOCOL : TCP  AVAIL    : YES
WLM WEIGHT    : N/A          CS WEIGHT : N/A  NET WEIGHT: 00001
FLAGS        : DISTDVIPA
IPADDR..PORT  : 10.20.1.1..8020
SYSPLEX      : PLEX2
SYSTEM NAME   : N/A          PROTOCOL : TCP  AVAIL    : YES
WLM WEIGHT    : N/A          CS WEIGHT : N/A  NET WEIGHT: 00000
FLAGS        : CMQ  DISTDVIPA
GROUP NAME    : WKLD2_GROUP2
WORKLOAD      : WORKLOAD2
GROUP FLAGS   : CROSS_SYSPLEX
IPADDR..PORT  : 10.10.1.1..8021
SYSPLEX      : PLEX1
SYSTEM NAME   : N/A          PROTOCOL : TCP  AVAIL    : YES
WLM WEIGHT    : N/A          CS WEIGHT : N/A  NET WEIGHT: 00001
FLAGS        : DISTDVIPA
IPADDR..PORT  : 10.20.1.1..8021
SYSPLEX      : PLEX2
SYSTEM NAME   : N/A          PROTOCOL : TCP  AVAIL    : YES
WLM WEIGHT    : N/A          CS WEIGHT : N/A  NET WEIGHT: 00000
FLAGS        : CMQ  DISTDVIPA
GROUP NAME    : WKLD1_GROUP1
WORKLOAD      : WORKLOAD1
GROUP FLAGS   : CROSS_SYSPLEX
IPADDR..PORT  : 192.10.1.32..5001
SYSPLEX      : PLEX1
SYSTEM NAME   : N/A          PROTOCOL : TCP  AVAIL    : NO
WLM WEIGHT    : N/A          CS WEIGHT : N/A  NET WEIGHT: 00000
FLAGS        : CMQ
IPADDR..PORT  : 10.20.1.1..5001
SYSPLEX      : PLEX2
SYSTEM NAME   : N/A          PROTOCOL : TCP  AVAIL    : YES
WLM WEIGHT    : N/A          CS WEIGHT : N/A  NET WEIGHT: 00001
FLAGS        : DISTDVIPA
GROUP NAME    : WKLD1_GROUP2
WORKLOAD      : WORKLOAD1
GROUP FLAGS   : CROSS_SYSPLEX
```

```

IPADDR..PORT: 192.10.1.32..6001
SYSPLEX : PLEX1
SYSTEM NAME: N/A      PROTOCOL : TCP  AVAIL    : NO
WLM WEIGHT : N/A      CS WEIGHT : N/A  NET WEIGHT: 00000
FLAGS      : CMQ
IPADDR..PORT: 10.20.1.1..6001
SSYSPLEX : PLEX2
SYSTEM NAME: N/A      PROTOCOL : TCP  AVAIL    : YES
WLM WEIGHT : N/A      CS WEIGHT : N/A  NET WEIGHT: 00001
FLAGS      : DISTDVIPA
LB INDEX   : 01      UUID      : 9A78BE9E
IPADDR..PORT: 192.10.1.32..40366
HEALTH    : 7E      FLAGS     : NOCHANGE PUSH
GROUP NAME : TIER2_GROUP1
WORKLOAD   : WORKLOAD1
GROUP FLAGS :
IPADDR..PORT: 192.10.110.1..5001
SSYSPLEX : PLEX1
SYSTEM NAME: SYS1A    PROTOCOL : TCP  AVAIL    : YES
WLM WEIGHT : 00058    CS WEIGHT : 100  NET WEIGHT: 00001
RAW        CP: 58    ZAAP: 00  ZIIP: 00
PROPORTIONAL CP: 58  ZAAP: 00  ZIIP: 00
ABNORM     : 00000    HEALTH    : 100
FLAGS      :
IPADDR..PORT: 192.10.110.2..5001
SYSPLEX : PLEX1
SYSTEM NAME: SYS1B    PROTOCOL : TCP  AVAIL    : YES
WLM WEIGHT : 00059    CS WEIGHT : 100  NET WEIGHT: 00001
RAW        CP: 59    ZAAP: 00  ZIIP: 00
PROPORTIONAL CP: 58  ZAAP: 00  ZIIP: 00
ABNORM     : 00000    HEALTH    : 100
FLAGS      :
GROUP NAME : TIER2_GROUP2
WORKLOAD   : WORKLOAD2
GROUP FLAGS :
IPADDR..PORT: 192.10.110.1..6001
SYSPLEX : PLEX1
SYSTEM NAME: SYS1A    PROTOCOL : TCP  AVAIL    : YES
WLM WEIGHT : 00058    CS WEIGHT : 100  NET WEIGHT: 00001
RAW        CP: 58    ZAAP: 00  ZIIP: 00
PROPORTIONAL CP: 58  ZAAP: 00  ZIIP: 00
ABNORM     : 00000    HEALTH    : 100
FLAGS      :
IPADDR..PORT: 192.10.110.2..6001
SYSPLEX : PLEX1
SYSTEM NAME: SYS1B    PROTOCOL : TCP  AVAIL    : YES
WLM WEIGHT : 00059    CS WEIGHT : 100  NET WEIGHT: 00001
RAW        CP: 59    ZAAP: 00  ZIIP: 00
PROPORTIONAL CP: 58  ZAAP: 00  ZIIP: 00
ABNORM     : 00000    HEALTH    : 100
FLAGS      :
2 OF 2 RECORDS DISPLAYED

```

The following information describes the fields in the previous sample display.

Field name

Descriptions

LB INDEX

A reference number used to identify the load balancer. The same reference number is used for a load balancer as long as it remains connected.

UUID

A hexadecimal value of the universally unique identifier assigned by the load balancer. This byte array can be up to 64 bytes in length. Only one load balancer with the same UUID can be connected to the primary Advisor at the same time.

IPADDR..PORT

- The instance listed under the LB INDEX field represents the IP address and port number used by the load balancer to connect to the primary Advisor. The IP address can be an IPv4 or an IPv6 address.
- The instances listed within the GROUP NAME block for first-tier load balancers represent the IP address and port number of a second-tier load balancers that the first-tier load balancer balances workload requests.
- The instances listed within the GROUP NAME block for second-tier load balancers represent the IP address and port number of a target server application that the second-tier load balancer balances workload requests.

HEALTH

A hexadecimal value supplied by the load balancer that indicates the general health of the load balancer. Valid values are in the range from 0 to X'7F'.

FLAGS

Indicators set by the load balancer. The flag values are shown as follows:

NOCHANGE

Indicates that the primary Advisor sends only weights that have changed since the last update interval to the load balancer.

PUSH Indicates that the primary Advisor sends weights to external load balancers when the update_interval has expired. If this flag is not present, the load balancer retrieves weights from the primary Advisor.

TRUST

Indicates that the load balancer trusts member applications to register themselves. This flag is ignored by the primary Advisor.

GROUP

The name of a registered group of related target server applications. The group name is a UTF-8 string displayed in EBCDIC on the MVS console. Any non-displayable character is displayed as a question mark (?).

GROUP FLAGS

The flags currently applicable to the group. Group flags are only valid for first-tier load balancers; for second-tier load balancers, this field is left blank. Here is the flag value:

CROSS_SYSPLEX

The group is a cross-sysplex group. This group is used to balance the workload across multiple sysplexes. The IP addresses specified in each cross-sysplex group identify the second-tier load balancers that the first-tier load balancer will balance across.

SYSPLEX

For a first-tier load balancer group, the value of SYSPLEX indicates the MVS sysplex name where the specified second-tier load balancer will load balance to.

For a second-tier load balancer group, the value of SYSPLEX indicates the MVS sysplex name of the system where the server application being load balanced exists.

SYSTEM NAME

For a first-tier load balancer group, the system name is N/A, as the

registered members are second-tier load balancers. For a second-tier load balancer group, the MVS system name of the system where the server application exists.

PROTOCOL

The protocol used by the second-tier load balancer for first-tier load balancer groups or server application for second-tier load balancer groups. Protocol value is either TCP or UDP.

AVAIL

Indicates whether the second-tier load balancer for a first-tier load balancer group or the server application for a second-tier load balancer group is available for workload distribution. The value YES indicates that the second-tier load balancer or the server application is available for load balancing. The value NO indicates that the second-tier load balancer or the server application is not recommended for load balancing.

WLM WEIGHT

The server-specific Workload Manager (WLM) weight value of the server application. For a first-tier load balancer group, the WLM weight is N/A, as the registered members are second-tier load balancers. For a second-tier load balancer group, the value is a composite weight, in the range of 0-64, indicating the sum of the proportional CP, zAAP, and zIIP weights for this server application.

CP Indicates that the RAW value is the WLM server-specific general CP recommendation. This is the amount of displaceable general CPU capacity based on the importance, which is defined by the WLM policy, of the server application as compared to the other target systems within the same MVS sysplex. The PROPORTIONAL value is the RAW value modified by the proportion of general CP capacity that is currently being consumed by the workload of the server application as compared with the other processors (zAAP and zIIP).

zAAP Indicates that the RAW value is the WLM server-specific zAAP recommendation. This is the amount of displaceable zAAP capacity based on the importance, which is defined by the WLM policy, of the server application as compared to the other target systems within the same MVS sysplex. The PROPORTIONAL value is the RAW value modified by the proportion of zAAP capacity that is currently being consumed by the workload of the server application as compared with the other processors (general CPU and zIIP).

zIIP Indicates that the RAW value is the WLM server-specific zIIP recommendation. This is the amount of displaceable zIIP capacity based on the importance, which is defined by the WLM policy, of the server application as compared with the other target systems within the same MVS sysplex. The PROPORTIONAL value is the RAW value modified by the proportion of zIIP capacity that is currently being consumed by the workload of the server application as compared with the other processors (general CPU and zAAP).

ABNORM

Indicates the rate of abnormal transaction completions per 1000 total transaction completions. The value is nonzero if the server application is experiencing conditions in which transactions are not

completed. It is applicable to server applications that report transaction status using Workload Management Services. Under normal conditions or if the server application is not providing this information to WLM, the value of ABNORM is 0. WLM uses abnormal transaction completion rate information to reduce the WLM weight reported for the server application.

HEALTH

The general health of the server application. Values less than 100 indicate that the server application is experiencing conditions that are not enabling it to process new workload requests successfully. It is applicable to server applications that report their health using Workload Management Services. Under normal circumstances or if the server application is not providing this information to WLM, the value of HEALTH is 100. WLM uses health information to reduce the WLM weight reported for the server application.

CS WEIGHT

The Communications Server (CS) weight value recommended by the Lifeline Agent. For a first-tier load balancer group, the CS weight is N/A, as the registered members are second-tier load balancers. For a second-tier load balancer group, the CS weight value range is 0-100. A higher weight indicates that the server application is able to handle more workload requests than a server application in the same group with a lower weight.

NET WEIGHT

For a first-tier load balancer group, NET WEIGHT indicates the relative weight of this second-tier load balancer compared to other second-tier load balancers for this workload. The net weight is either 0 or 1, with a value of 0 indicating that no workload requests are being distributed to this second-tier load balancer, while a value of 1 indicating that workload requests can be distributed to this second-tier load balancer.

For a second-tier load balancer group, NET WEIGHT indicates the relative weight of this server application compared with other server applications within the same site for this workload. The net weight value range is 0-64. A higher weight indicates that a server application can handle more workload requests than a lower weight server application in the same group. This weight is based upon the WLM weight, the CS weight, and other factors. Compare net weights for server applications only with other server applications within the same group. Weights within a group are normalized to yield the net weight. Normalization involves reducing the weight values while preserving the ratios between the weights.

The following example shows a sample display when you issue F AQSADV,DISPLAY,WORKLOAD.

```
F AQSADV,DISPLAY,WORKLOAD
AQS0145I WORKLOAD SUMMARY
WORKLOAD NAME   : WORKLOAD1
STATE  : ACTIVE   SITE  : PLEX2
WORKLOAD NAME   : WORKLOAD2
STATE  : QUIESCED SITE  : N/A
2 OF 2 RECORDS DISPLAYED
```

The following information describes the fields in the previous sample display.

Field name	Descriptions
------------	--------------

WORKLOAD

The name of the workload as defined in the cross_sysplex_list Advisor configuration statement.

STATE

The state of the workload. State values are shown as follows:

ACTIVE

Indicates that the workload has been activated to the specified site. The Advisor notifies first-tier load balancers to route all inbound requests for this workload to the specified site.

QUIESCED

Indicates that the workload has been quiesced to all sites. The Advisor notifies first-tier load balancers to not route any inbound requests for this workload.

SITE The MVS sysplex name where the workload is active. If the state of the workload is `QUIESCED`, the `SITE` value is set to `N/A`.

The following example shows a sample display when you issue `F AQSADV,DISPLAY,WORKLOAD,DETAIL`.

```
F AQSADV,DISPLAY,WORKLOAD,DETAIL
AQS0146I WORKLOAD DETAILS
WORKLOAD NAME   : WORKLOAD1
STATE   : ACTIVE   SITE   : PLEX2
SERVERS:
IPADDR..PORT : 192.10.110.1..5001
SYSTEM NAME : SYS1A   SYSPLEX : PLEX1   STATUS : AVAIL
IPADDR..PORT : 10.20.1.1..5001
SYSTEM NAME : SYS2A   SYSPLEX : PLEX2   STATUS : AVAIL
IPADDR..PORT : 192.10.110.2..5001
SYSTEM NAME : SYS1B   SYSPLEX : PLEX1   STATUS : AVAIL
IPADDR..PORT : 10.20.1.1..5001
SYSTEM NAME : SYS2B   SYSPLEX : PLEX2   STATUS : UNAVAIL
IPADDR..PORT : 192.10.110.1..6001
SYSTEM NAME : SYS1A   SYSPLEX : PLEX1   STATUS : AVAIL
IPADDR..PORT : 10.20.1.1..6001
SYSTEM NAME : SYS2A   SYSPLEX : PLEX2   STATUS : AVAIL
IPADDR..PORT : 192.10.110.2..6001
SYSTEM NAME : SYS1A   SYSPLEX : PLEX1   STATUS : AVAIL
IPADDR..PORT : 10.20.1.1..6001
SYSTEM NAME : SYS2B   SYSPLEX : PLEX2   STATUS : AVAIL
WORKLOAD NAME   : WORKLOAD2
STATE   : ACTIVE   SITE   : PLEX1
SERVERS:
IPADDR..PORT : 10.10.1.1..8020
SYSTEM NAME : SYS1A   SYSPLEX : PLEX1   STATUS : AVAIL
IPADDR..PORT : 10.10.1.1..8020
SYSTEM NAME : SYS1B   SYSPLEX : PLEX1   STATUS : AVAIL
IPADDR..PORT : 10.20.1.1..8020
SYSTEM NAME : SYS2A   SYSPLEX : PLEX2   STATUS : AVAIL
IPADDR..PORT : 10.20.1.1..8020
SYSTEM NAME : SYS2B   SYSPLEX : PLEX2   STATUS : AVAIL
IPADDR..PORT : 10.10.1.1..8021
SYSTEM NAME : SYS1A   SYSPLEX : PLEX1   STATUS : UNAVAIL
IPADDR..PORT : 10.10.1.1..8021
SYSTEM NAME : SYS1B   SYSPLEX : PLEX1   STATUS : AVAIL
IPADDR..PORT : 10.20.1.1..8021
SYSTEM NAME : SYS2A   SYSPLEX : PLEX2   STATUS : AVAIL
IPADDR..PORT : 10.20.1.1..8021
SYSTEM NAME : SYS2B   SYSPLEX : PLEX2   STATUS : AVAIL
2 OF 2 RECORDS DISPLAYED
```

The following information describes the fields in the previous sample display.

Field name

Descriptions

WORKLOAD

The name of the workload as defined in the `cross_sysplex_list` Advisor configuration statement.

STATE

The state of the workload. State values are shown as follows:

ACTIVE

Indicates that the workload has been activated to the specified site. The Advisor notifies first-tier load balancers to route all inbound requests for this workload to the specified site.

QUIESCED

Indicates that the workload has been quiesced to all sites. The Advisor notifies first-tier load balancers to not route any inbound requests for this workload.

SITE The MVS sysplex name where the workload is active. If the state of the workload is `QUIESCED`, the `SITE` value is set to `N/A`.

IPADDR..PORT

The IP address and port number that the server application is listening on. The IP address can be an IPv4 or an IPv6 address.

SYSTEM NAME

The MVS system name of the system where the server application exists.

SYSPLEX

The MVS sysplex name of the system where the server application exists.

STATUS

The status of the server application. Status values are shown as follows:

AVAIL

Indicates that the server application is available on the specified system and is able to process workload requests.

UNAVAIL

Indicates that the server application is not available on the specified system and is not able to process workload requests. Possible reasons for the server application being unavailable include not being active on the specified system or quiesced by the MVS operator.

MODIFY *advisor_proc*,ACTivate command: Activate workloads

Use the `MODIFY advisor_proc,ACTivate` command to force the Lifeline Advisor to signal first-tier load balancers that new connections for the specified workload or for all the workloads can be routed to the requested site.

Rule: You can issue this command only from the primary Advisor.

Format



►,ACTivate,WORKload=*workloadname*,Site=*sitename* →
 └─,WORKload=**ALL**,Site=*sitename* ─┘

Parameters

advisor_proc

Indicates the member name of the cataloged procedure used to start the Advisor.

ACTivate

Signals the first-tier load balancers that a workload can be distributed to a site.

WORKload=

workloadname

Specifies the name of the workload to be activated. The name must match one of the workload names specified in the `cross_sysplex_list` Advisor configuration statement. The *workloadname* value must not exceed 64 characters in length.

Rule: You must quiesce the specified workload before you issue the command to activate it.

ALL

Indicates that all the workloads specified in the `cross_sysplex_list` Advisor configuration statement are to be activated.

Rule: You must quiesce all the workloads before you issue the command to activate them.

Site=*sitename*

Specifies the name of the site where the workload is to be distributed. The name must match one of the site names specified in the `cross_sysplex_list` Advisor configuration statement. The *sitename* value must not exceed 8 characters in length.

Examples

The following example shows a sample display when you issue `F AQSADV,ACTIVATE,WORKLOAD=WORKLOAD1,SITE=PLEX1` on the primary Advisor.

```
F AQSADV,ACTIVATE,WORKLOAD=WORKLOAD1,SITE=PLEX1
AQS0153I WORKLOAD WORKLOAD1 ACTIVATED ON SITE PLEX1
```

The following example shows a sample display when you issue `F AQSADV,ACTIVATE,WORKLOAD=*ALL*,SITE=PLEX1` on the primary advisor.

```
F AQSADV,ACTIVATE,WORKLOAD=*ALL*,SITE=PLEX1
AQS0152I ALL WORKLOADS ACTIVATED ON SITE PLEX1
```

MODIFY *advisor_proc*,DEACTivate command: Deactivate workloads

Use the `MODIFY advisor_proc,DEACTivate` command to force the Lifeline Advisor to reset all the existing connections for the specified workload or for all workloads.

Rule: You can issue this command only from the primary Advisor.

Format

►► `MODIFY` *advisor_proc* `,DEACTivate` `,WORKload=workloadname` `,WORKload=*ALL*` ◀◀

Parameters

advisor_proc

Indicates the member name of the cataloged procedure used to start the Advisor.

DEACTivate

Signals the Advisor that a workload needs to be deactivated.

WORKload=

workloadname

Specifies the name of the workload to be deactivated. The name must match one of the workload names specified in the `cross_sysplex_list` Advisor configuration statement. The *workloadname* value must not exceed 64 characters in length.

Rule: You must quiesce the specified workload before you issue the command to deactivate it.

ALL

Indicates that all the workloads specified in the `cross_sysplex_list` Advisor configuration statement are to be deactivated.

Rule: You must quiesce all the workloads before you issue the command to deactivate them.

Examples

The following example shows a sample display when you issue `F AQSADV,DISPLAY,ADVISOR` on the primary Advisor.

```
F AQSADV,DEACTIVATE,WORKLOAD=WORKLOAD1
AQS0155I WORKLOAD WORKLOAD1 DEACTIVATED
```

The following example shows a sample display when you issue `F AQSADV,DEACTIVATE,WORKLOAD=*ALL*` on the primary Advisor.

```
F AQSADV,DEACTIVATE,WORKLOAD=*ALL*
AQS0154I ALL WORKLOADS DEACTIVATED
```

MODIFY *advisor_proc*,DEBUG command: Change the debug level

Use the `MODIFY advisor_proc,DEBUG` command to change the debug level that is in effect for the Lifeline Advisor.

Format

►► `MODIFY` *advisor_proc* `,DEBUG` `,Level=debuglevel` ◀◀

Parameters

advisor_proc

Indicates the member name of the cataloged procedure used to start the Advisor.

DEBug, Level=*debuglevel*

Changes the debug level in effect for this Advisor. The debug level that you can set is the sum of one or more levels of the debug messages to be logged. See “Debug levels” on page 27 for information about debug level values.

Example

The following example shows a sample display when you issue F AQSADV,DEBUG,LEVEL=127 on the Advisor.

```
F AQSADV,DEBUG,LEVEL=127
AQS0138I LLADVSR DEBUG LEVEL UPDATED
```

MODIFY *advisor_proc*,QUIESCE command: Quiesce workloads

Use the MODIFY *advisor_proc*,QUIESCE command to force the Lifeline Advisor to signal the first-tier load balancers that no new connections are to be routed for the specified workload or for all workloads.

Note: Existing connections for this workload will continue to be routed.

Rule: You can issue this command only from the primary Advisor.

Format

►► — [MODIFY] — *advisor_proc* — ,QUIESCE — [,WORKload=*workloadname*] — [,WORKload=*ALL*] — ►►

Parameters

advisor_proc

Indicates the member name of the cataloged procedure used to start the Advisor.

QUIESCE

Signals the first-tier load balancers that a workload can no longer be distributed to a site.

WORKload=

workloadname

Specifies the name of the workload to be quiesced. The name must match one of the workload names specified in the cross_sysplex_list Advisor configuration statement. The *workloadname* value must be less than or equal to 64 characters in length.

ALL

Indicates that all the workloads specified in the cross_sysplex_list Advisor configuration statement are to be quiesced.

Examples

The following example shows a sample display when you issue F AQSADV, QUIESCE, WORKLOAD=WORKLOAD1 on the primary Advisor.

```
F AQSADV, QUIESCE, WORKLOAD=WORKLOAD1
AQS0155I WORKLOAD WORKLOAD1 QUIESCED
```

The following example shows a sample display when you issue F AQSADV, QUIESCE, WORKLOAD=*ALL* on the primary Advisor.

```
F AQSADV, QUIESCE, WORKLOAD=*ALL*
AQS0154I ALL WORKLOADS QUIESCED
```

MODIFY *advisor_proc*, REFRESH command: Update configuration

Use the MODIFY *advisor_proc*, REFRESH command to force the Lifeline Advisor to read the configuration file again and apply any changes to its active configuration.

See “Lifeline Advisor configuration statements” on page 37 for the configuration statements that are refreshable.

Format

```
➤—[MODIFY]—advisor_proc—, REFRESH—➤
   [F]—
```

Parameters

advisor_proc

Indicates the member name of the cataloged procedure used to start the Advisor.

REFRESH

Forces this Advisor to read the configuration file again and apply any changes to its active configuration.

Example

The following example shows a sample display when you issue F AQSADV, REFRESH.

```
F AQSADV, REFRESH
AQS0181I LLADVSR CONFIGURATION UPDATED
```

MODIFY *advisor_proc*, TAKEOVER command: Take over primary Advisor responsibilities

Use the MODIFY *advisor_proc*, TAKEOVER command to force the Lifeline Advisor to take over primary Advisor responsibilities.

Rule: You can issue this command only from the secondary Advisor.

Format

```
➤—[MODIFY]—advisor_proc—, TAKEOVER—➤
   [F]—
```


Parameters

advisor_proc

Indicates the member name of the cataloged procedure used to start the Advisor.

TAKEOVER

Forces this Advisor to takeover primary Advisor responsibilities.

Example

The following example shows a sample display when you issue F AQSADV,TAKEOVER on the secondary Advisor.

```
F AQSADV,TAKEOVER
AQS0169I ADVISOR TAKEOVER SCHEDULED
AQS0166I ADVISOR IS NOW IN PRIMARY ROLE
```

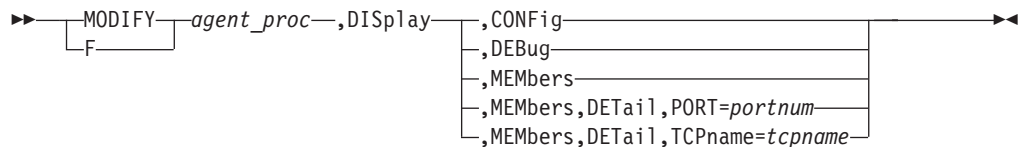
Chapter 8. Lifeline Agent commands

Use the Lifeline Agent commands to display Lifeline Agent information and modify Lifeline Agent state information.

MODIFY *agent_proc*,DISplay command: Display Lifeline Agent information

Use the MODIFY *agent_proc*,DISplay command to display Lifeline Agent information.

Format



Parameters

agent_proc

Indicates the member name of the cataloged procedure used to start the Agent.

DISplay,CONFig

Displays the active configuration for this Agent.

DISplay,DEBUg

Displays the debug level in effect for this Agent.

The debug level displayed is the sum of one or more levels of debug messages being logged. See “Debug levels” on page 27 for more information about the debug levels.

DISplay,MEMbers

Displays information about registered local server applications.

DISplay,MEMbers,DETAil

Displays detailed information about registered local server applications, including the job name and ASID of the server application.

DISplay,MEMbers,DETAil,PORT=portnum

Displays detailed information about registered local server applications that are bound to the specified port number. The port number value range is 0 - 65535.

DISplay,MEMbers,DETAil,TCPname=tcpname

Displays detailed information about registered local server applications that are associated with the specified TCP/IP stack. The *tcpname* value must be less than or equal to 8 characters in length.

Examples

The following example shows a sample display when you issue F AQSAGE,DISPLAY,CONFIG.

```

F AQSAGE,DISPLAY,CONFIG
AQS0144I AGENT CONFIGURATION
CONFIG FILENAME : USER.PROFILES(LBAGECNF)
DEBUG LEVEL : 7
ADVISOR ID : 192.10.1.1..8181
HOST CONNECTION : 192.10.110.1..4000

```

The following information describes the fields in the previous sample display.

Field name

Descriptions

CONFIG FILENAME

The configuration file used by this Agent when the Agent was initially started.

DEBUG LEVEL

The debug level currently in effect for this Agent.

ADVISOR ID

The IP address and port number that the primary Advisor listens on for connections from this Agent. The IP address can be an IPv4 or an IPv6 address.

HOST CONNECTION

The source IP address and port number that this Agent uses to connect to the primary Advisor. The IP address can be an IPv4 or an IPv6 address.

The following example shows a sample display when you issue F AQSAGE,DISPLAY,DEBUG.

```

F AQSAGE,DISPLAY,DEBUG
AQS0111I LLAGENT DEBUG LEVEL 7

```

The following example shows a sample display when you issue F AQSAGE,DISPLAY,MEMBERS.

```

F AQSAGE,DISPLAY,MEMBERS
AQS0114I MEMBER SUMMARY
LB INDEX : 00 UID : A67B6699
GROUP NAME : WKLD2_GROUP1
IPADDR..PORT: 10.10.1.1..8020
MATCHES : 001 PROTOCOL : TCP
FLAGS : ANY DISTDVIPA
GROUP NAME : WKLD2_GROUP2
IPADDR..PORT: 10.10.1.1..8021
MATCHES : 000 PROTOCOL : TCP
FLAGS : DISTDVIPA
LB INDEX : 01 UID : 9A78BE9E
GROUP NAME : TIER2_GROUP1
IPADDR..PORT: 192.10.110.1..5001
MATCHES : 001 PROTOCOL : TCP
FLAGS :
GROUP NAME : TIER2_GROUP2
IPADDR..PORT: 192.10.110.1..6001
MATCHES : 001 PROTOCOL : TCP
FLAGS :
4 OF 4 RECORDS DISPLAYED

```

The following information describes the fields in the previous sample display.

Field name

Descriptions

LB INDEX

The reference number used to identify the load balancer. The same reference number is used for a load balancer as long as the load balancer remains connected.

UUID A hexadecimal value of the universally unique identifier assigned by the load balancer. This byte array can be up to 64 bytes in length. Only one load balancer with the same UUID can be connected to the primary Advisor at the same time.

GROUP NAME

The name of a group of related target server applications registered on the external load balancer.

IPADDR..PORT

The IP address and port number of a member defined in the registered group. The IP address can be an IPv4 or an IPv6 address.

MATCHES

The number of server applications that match the IP address and port number. For the server applications sharing a port, this value can be more than 1. If the value of matches is 0, the Agent finds the IP address of the member reported on an active TCP/IP stack, but does not find a server application listening on that IP address or port number.

PROTOCOL

The protocol that the member is using. The protocol value is TCP or UDP.

FLAGS

Indicators for the member. The flag values are shown as follows:

ANY Indicates that the server application is bound to INADDR_ANY or the unspecified IPv6 address.

DISTDVIPA

Indicates that the IP address of the member is a distributable DVIPA. The IP address can be an IPv4 or an IPv6 address.

NODATA

Indicates that the Agent is reporting a temporary value for the Communications Server weight. Two update intervals are needed before the Agent can calculate a proper value for the Communications Server weight.

SYSQ, TCPQ, or APPQ

Indicates that the operator has requested that no more work be routed to the quiesced server application. The different flags reflect the highest level of the quiesce command that applies, and indicates the type of the enable command that must be used to enable the server application.

SYSQ Indicates that the server application was quiesced with the F agent_proc,QUIESCE,SYSTEM command, and that you must use the F agent_proc,ENABLE,SYSTEM command to enable the server application.

TCPQ Indicates that the server application was quiesced with the F agent_proc,QUIESCE,TCPNAME=tcpname command, and that you must use the F agent_proc,ENABLE,TCPNAME=tcpname command to enable the server application.

APPQ Indicates that the server application was quiesced with the F agent_proc,QUIESCE,PORT=port command, and that you must use the F agent_proc,ENABLE,PORT=port command to enable the server application.

V6 Indicates that the server application has specified the IPv6_V6ONLY socket option. Only workload requests from IPv6-enabled clients are able to communicate with the server application.

The following example shows a sample display when you issue F AQSAGE,DISPLAY,MEMBERS,DETAIL.

```
F AQSAGE,DISPLAY,MEMBERS,DETAIL
AQS0115I MEMBER DETAILS
LB INDEX      : 00          UUID      : A67B6699
GROUP NAME    : WKLD2_GROUP1
IPADDR..PORT : 10.10.1.1..8020
MATCHES      : 001          PROTOCOL   : TCP
FLAGS        : ANY DISTDVIPA
TCPNAME      : TCPIP
JOBNAME      : JOB1          ASID       : 0034 RESOURCE : 0000096B
GROUP NAME    : WKLD2_GROUP2
IPADDR..PORT : 10.10.1.1..8021
MATCHES      : 000          PROTOCOL   : TCP
FLAGS        : DISTDVIPA
TCPNAME      : TCPIP
JOBNAME      : N/A          ASID       : N/A RESOURCE : N/A
LB INDEX      : 01          UUID      : 9A78BE9E
GROUP NAME    : TIER2_GROUP1
IPADDR..PORT : 192.10.110.1..5001
MATCHES      : 001          PROTOCOL   : TCP
FLAGS        :
TCPNAME      : TCPIP
JOBNAME      : JOB3          ASID       : 0036 RESOURCE : 0000096D
GROUP NAME    : TIER2_GROUP2
IPADDR..PORT : 192.10.110.1..6001
MATCHES      : 001          PROTOCOL   : TCP
FLAGS        :
TCPNAME      : TCPIP
JOBNAME      : JOB4          ASID       : 0037 RESOURCE : 0000096E
4 OF 4 RECORDS DISPLAYED
```

The following information describes the fields in the previous sample display.

Field name

Descriptions

LB INDEX

Reference number used to identify the load balancer. The same reference number is used for a load balancer as long as the load balancer remains connected.

UUID A hexadecimal value of the universally unique identifier assigned by the load balancer. This byte array can be up to 64 bytes in length. Only one load balancer with the same UUID can be connected to the primary Advisor at the same time.

GROUP NAME

The name of a group of related target server applications registered on the external load balancer.

IPADDR..PORT

The IP address and port number of a member defined in the registered group. The IP address can be an IPv4 or an IPv6 address.

MATCHES

The number of server applications that match the IP address and port number. For server applications sharing a port, this value can be more than 1. If the value of matches is 0, the Agent found the IP address of the member reported on an active TCP/IP stack, but did not find a server application listening on that IP address or port number.

PROTOCOL

The protocol that the member is using. The protocol value will be TCP or UDP.

FLAGS

Indicators for the member. The flag values are shown as follows:

ANY Indicates that the server application is bound to INADDR_ANY or the unspecified IPv6 address.

DISTDVIPA

Indicates that the IP address of the member is a distributable DVIPA. The IP address can be an IPv4 or an IPv6 address.

NODATA

Indicates that the Agent is reporting a temporary value for the Communications Server weight. Two update intervals are needed before the Agent can calculate a proper value for the Communications Server weight.

SYSQ, TCPQ, or APPQ

Indicates that the operator has requested that no more work be routed to the quiesced server application. The different flags reflect the highest level of the quiesce command that applies, and indicates the type of the enable command that must be used to enable the server application.

SYSQ Indicates that the server application was quiesced with the F agent_proc,QUIESCE,SYSTEM command, and that you must use the F agent_proc,ENABLE,SYSTEM command to enable the server application.

TCPQ Indicates that the server application was quiesced with the F agent_proc,QUIESCE,TCPNAME=tcpname command, and that you must use the F agent_proc,ENABLE,TCPNAME=tcpname command to enable the server application.

APPQ Indicates that the server application was quiesced with the F agent_proc,QUIESCE,PORT=port command, and that you must use the F agent_proc,ENABLE,PORT=port command to enable the server application.

V6 Indicates that the server application has specified the IPv6_V6ONLY socket option. Only workload requests from IPv6-enabled clients are able to communicate with the server application.

TCPNAME

The name of the TCP/IP Server stack that owns the IP address for the member.

JOBNAME

The MVS job name of the server application. If there are no server applications matching this member, N/A is displayed.

ASID The MVS address space identifier of the server application. If there are no server applications matching this member, N/A is displayed.

RESOURCE

The identifier used by the TCP/IP stack that uniquely identifies one instance of the server application. The resource identifier is also displayed by the NETSTAT CONN command. If there are no server applications matching this member, N/A is displayed.

The following example shows a sample display when you issue F AQSAGE,DISPLAY,MEMBERS,DETAIL,PORT=5001.

```
F AQSAGE,DISPLAY,MEMBERS,DETAIL,PORT=5001
AQS0115I MEMBER DETAILS
LB INDEX      : 01          UUID       : 9A78BE9E
GROUP NAME    : TIER2_GROUP1
IPADDR..PORT: 192.10.110.1..5001
MATCHES      : 001        PROTOCOL    : TCP
FLAGS        :
TCPNAME      : TCPIP
JOBNAME      : JOB3       ASID        : 0036 RESOURCE : 0000096D
1 OF 1 RECORDS DISPLAYED
```

The following example shows a sample display when you issue F AQSAGE,DISPLAY,MEMBERS,DETAIL,TCPIPCNAME=TCPIP.

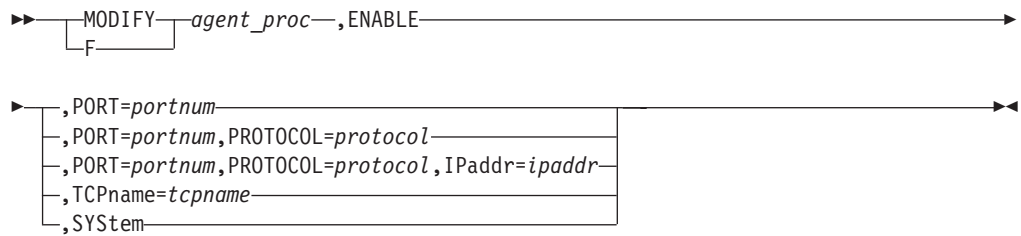
```
F AQSAGE,DISPLAY,MEMBERS,DETAIL,TCPIPCNAME=TCPIP
AQS0115I MEMBER DETAILS
LB INDEX      : 00          UUID       : A67B6699
GROUP NAME    : WKLD2_GROUP1
IPADDR..PORT: 10.10.1.1..8020
MATCHES      : 001        PROTOCOL    : TCP
FLAGS        : ANY DISTDVIPA
TCPNAME      : TCPIP
JOBNAME      : JOB1       ASID        : 0034 RESOURCE : 0000096B
GROUP NAME    : WKLD2_GROUP2
IPADDR..PORT: 10.10.1.1..8021
MATCHES      : 000        PROTOCOL    : TCP
FLAGS        : DISTDVIPA
TCPNAME      : TCPIP
JOBNAME      : N/A       ASID        : N/A RESOURCE : N/A
LB INDEX      : 01          UUID       : 9A78BE9E
GROUP NAME    : TIER2_GROUP1
IPADDR..PORT: 192.10.110.1..5001
MATCHES      : 001        PROTOCOL    : TCP
FLAGS        :
TCPNAME      : TCPIP
JOBNAME      : JOB3       ASID        : 0036 RESOURCE : 0000096D
GROUP NAME    : TIER2_GROUP2
IPADDR..PORT: 192.10.110.1..6001
MATCHES      : 001        PROTOCOL    : TCP
FLAGS        :
TCPNAME      : TCPIP
JOBNAME      : JOB4       ASID        : 0037 RESOURCE : 0000096E
4 OF 4 RECORDS DISPLAYED
```

MODIFY *agent_proc*,ENABLE command: Enable server applications

Use the MODIFY *agent_proc*,ENABLE command to mark the server applications as enabled. The Lifeline Agent will notify the Advisor to recommend this server application for new workload requests.

Tip: If more than one server application is sharing a port, all of the server applications are enabled.

Format



Parameters

agent_proc

Indicates the member name of the cataloged procedure used to start the Agent.

ENABLE,PORT=portnum

Marks the server applications bound to the specified port number as enabled. The range of the port number value is 0 - 65535.

Rule: If the IP address of the member is a distributable DVIPA when you specify this parameter, you can enable the server applications only by the VARY TCPIP,,SYSPLEX,RESUME,PORT=portnum command.

ENABLE,PORT=portnum,PROTOcol=protocol

Marks the server applications that are bound to the specified port number and use the specified protocol as enabled. The range of the port number value is 0 - 65535. The protocol value is TCP or UDP.

Rule: If the IP address of the member is a distributable DVIPA when you specify this parameter, you can enable the server applications only by the VARY TCPIP,,SYSPLEX,RESUME,PORT=portnum command.

ENABLE,PORT=portnum,PROTOcol=protocol,IPAddr=ipaddr

Marks the server applications that are bound to the specified port number and use the specified protocol and the specified IP address as enabled. The range of the port number value is 0 - 65535. The protocol value is TCP or UDP. The IP address can be an IPv4 or an IPv6 address.

Rule: If the IP address of the member is a distributable DVIPA when you specify this parameter, you can enable the server applications only by the VARY TCPIP,,SYSPLEX,RESUME,JOBNAME=jobname command.

ENABLE,TCPname=tcpname

Marks the server applications associated with the specified TCP/IP stack as enabled. The *tcpname* value must be less than or equal to 8 characters in length.

Rule: If the IP address of the member is a distributable DVIPA when you specify this parameter, you can enable the server applications only by the TCPIP,,SYSPLEX,RESUME,TARGET command.

ENABLE,SYStem

Marks the server applications on this system as enabled.

Rule: If the IP address of the member is a distributable DVIPA when you specify this parameter, you can enable the server applications only by the VARY TCPIP, ,SYSPLEX,RESUME,TARGET command.

Examples

The following example shows a sample display when you issue F AQSAGE,ENABLE,PORT=5001.

```
F AQSAGE,ENABLE,PORT=5001
AQS0139I ALL MATCHING REGISTERED APPLICATIONS ARE ENABLED
```

The following example shows a sample display when you issue F AQSAGE,ENABLE,PORT=8021.

```
F AQSAGE,ENABLE,PORT=8021
AQS0140I 0 OF 1 MATCHING REGISTERED APPLICATIONS ARE EsNABLED -
DISTRIBUTED DVIPA MEMBERS ARE IGNORED
```

The following example shows a sample display when you issue F AQSAGE,ENABLE,PORT=5001,PROTOCOL=TCP.

```
F AQSAGE,ENABLE,PORT=5001,PROTOCOL=TCP
AQS0139I ALL MATCHING REGISTERED APPLICATIONS ARE ENABLED
```

The following example shows a sample display when you issue F AQSAGE,ENABLE,PORT=8021,PROTOCOL=TCP.

```
F AQSAGE,ENABLE,PORT=8021,PROTOCOL=TCP
AQS0140I 0 OF 1 MATCHING REGISTERED APPLICATIONS ARE ENABLED -
DISTRIBUTED DVIPA MEMBERS ARE IGNORED
```

The following example shows a sample display when you issue F AQSAGE,ENABLE,PORT=5001,PROTOCOL=UDP.

```
F AQSAGE,ENABLE,PORT=5001,PROTOCOL=UDP
AQS0122I NO MEMBERS MATCH SELECTION CRITERIA
AQS0123I ENABLE APPLICATION COMMAND REJECTED
```

The following example shows a sample display when you issue F AQSAGE,ENABLE,PORT=5001,PROTOCOL=TCP,IPADDR=192.10.110.1.

```
F AQSAGE,ENABLE,PORT=5001,PROTOCOL=TCP,IPADDR=192.10.110.1
AQS0139I ALL MATCHING REGISTERED APPLICATIONS ARE ENABLED
```

The following example shows a sample display when you issue F AQSAGE,ENABLE,PORT=8021,PROTOCOL=TCP,IPADDR=10.10.1.1.

```
F AQSAGE,ENABLE,PORT=8021,PROTOCOL=TCP,IPADDR=10.10.1.1
AQS0140I 0 OF 1 MATCHING REGISTERED APPLICATIONS ARE ENABLED -
DISTRIBUTED DVIPA MEMBERS ARE IGNORED
```

The following example shows a sample display when you issue F AQSAGE,ENABLE,PORT=5001,PROTOCOL=TCP,IPADDR=10.10.1.2.

```
F AQSAGE,ENABLE,PORT=5001,PROTOCOL=TCP,IPADDR=10.10.1.2
AQS0122I NO MEMBERS MATCH SELECTION CRITERIA
AQS0123I ENABLE APPLICATION COMMAND REJECTED
```

MODIFY *agent_proc*, QUIESCE command: Quiesce server applications

Use the MODIFY *agent_proc*, QUIESCE command to mark the server applications as quiesced. The Lifeline Agent will notify the Advisor to not recommend this server application for new workload requests.

Rule: If the IP address of the member is a distributable DVIPA when you specify this parameter, you can quiesce the server applications only by the VARY TCPIP, ,SYSPLEX,QUIESCE,TARGET command.

Examples

The following example shows a sample display when you issue F AQSAGE,QUIESCE,PORT=5001.

```
F AQSAGE,QUIESCE,PORT=5001
AQS0139I ALL MATCHING REGISTERED APPLICATIONS ARE QUIESCED
```

The following example shows a sample display when you issue F AQSAGE,QUIESCE,PORT=8021.

```
F AQSAGE,QUIESCE,PORT=8021
AQS0140I 0 OF 1 MATCHING REGISTERED APPLICATIONS ARE QUIESCED -
DISTRIBUTED DVIPA MEMBERS ARE IGNORED
```

The following example shows a sample display when you issue F AQSAGE,QUIESCE,PORT=5001,PROTOCOL=TCP.

```
F AQSAGE,QUIESCE,PORT=5001,PROTOCOL=TCP
AQS0139I ALL MATCHING REGISTERED APPLICATIONS ARE QUIESCED
```

The following example shows a sample display when you issue F AQSAGE,QUIESCE,PORT=8021,PROTOCOL=TCP.

```
F AQSAGE,QUIESCE,PORT=8021,PROTOCOL=TCP
AQS0140I 0 OF 1 MATCHING REGISTERED APPLICATIONS ARE QUIESCED -
DISTRIBUTED DVIPA MEMBERS ARE IGNORED
```

The following example shows a sample display when you issue F AQSAGE,QUIESCE,PORT=5001,PROTOCOL=UDP.

```
F AQSAGE,QUIESCE,PORT=5001,PROTOCOL=UDP
AQS0122I NO MEMBERS MATCH SELECTION CRITERIA
AQS0123I QUIESCE APPLICATION COMMAND REJECTED
```

The following example shows a sample display when you issue F AQSAGE,QUIESCE,PORT=5001,PROTOCOL=TCP,IPADDR=192.10.110.1.

```
F AQSAGE,QUIESCE,PORT=5001,PROTOCOL=TCP,IPADDR=192.10.110.1
AQS0139I ALL MATCHING REGISTERED APPLICATIONS ARE QUIESCED
```

The following example shows a sample display when you issue F AQSAGE,QUIESCE,PORT=8021,PROTOCOL=TCP,IPADDR=10.10.1.1.

```
F AQSAGE,QUIESCE,PORT=8021,PROTOCOL=TCP,IPADDR=10.10.1.1
AQS0140I 0 OF 1 MATCHING REGISTERED APPLICATIONS ARE QUIESCED -
DISTRIBUTED DVIPA MEMBERS ARE IGNORED
```

The following example shows a sample display when you issue F AQSAGE,QUIESCE,PORT=5001,PROTOCOL=TCP,IPADDR=10.10.1.2.

```
F AQSAGE,QUIESCE,PORT=5001,PROTOCOL=TCP,IPADDR=10.10.1.2
AQS0122I NO MEMBERS MATCH SELECTION CRITERIA
AQS0123I QUIESCE APPLICATION COMMAND REJECTED
```

The following example shows a sample display when you issue F AQSAGE,QUIESCE,TCPNAME=TCPIP.

```
F AQSAGE,QUIESCE,TCPNAME=TCPIP
AQS0140I 2 OF 4 MATCHING REGISTERED APPLICATIONS ARE QUIESCED -
DISTRIBUTED DVIPA MEMBERS ARE IGNORED
```

The following example shows a sample display when you issue F AQSAGE,QUIESCE,SYSTEM.

```
F AQSAGE,QUIESCE,SYSTEM
AQS0140I 2 OF 4 MATCHING REGISTERED APPLICATIONS ARE QUIESCED -
DISTRIBUTED DVIPA MEMBERS ARE IGNORED
```

MODIFY *agent_proc*,DEBbug command: Change the debug level

Use the MODIFY *agent_proc*,DEBbug command to change the debug level that is in effect for the Lifeline Agent.

Format

```
►► [MODIFY] agent_proc [,DEBbug [Level=debuglevel]] ►►
```

Parameters

agent_proc

Indicates the member name of the cataloged procedure used to start the Agent.

DEBbug,Level=*debuglevel*

Changes the debug level in effect for this Agent. The debug level that you can set is the sum of one or more levels of the debug messages to be logged. See “Debug levels” on page 27 for debug level values.

Example

The following example shows a sample display when you issue F AQSAGE,DEBbug,LEVEL=127.

```
F AQSAGE,DEBbug,LEVEL=127
AQS0138I LLAGENT DEBbug LEVEL UPDATED
```


Chapter 9. Network management interface for Multi-site Workload Lifeline

Multi-site Workload Lifeline provides a network management interface (NMI) that you can use to monitor Lifeline metrics and statistics. Network management applications can communicate with the Lifeline NMI through an AF_UNIX socket using a series of messages.

The flow between the Lifeline NMI and the network management application is described in Figure 2.

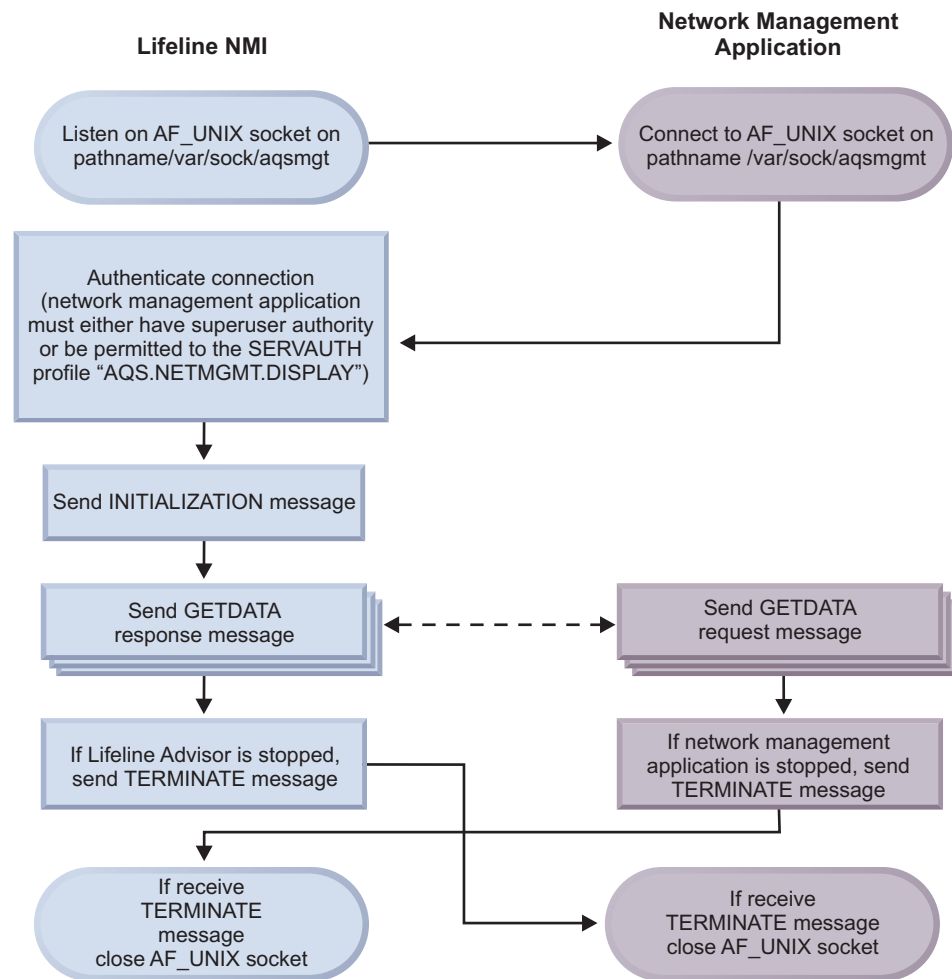


Figure 2. Flow between the Lifeline NMI and the network management application

There are three possible message types: an initialization message, a data message, and a termination message. The initialization, termination, and data request messages contain only a message header.

The data response message contains the following headers and section descriptors:

1. A message header.
2. A record header for the overall response.

3. A section descriptor for Lifeline Advisors, which maps one section for the primary Advisor, and optionally, one section for the secondary Advisor.
4. A section descriptor for workloads, which maps sections for each of the defined workloads.
5. A section descriptor for sites, which maps sections for each of the defined sites.
6. A section descriptor for Lifeline Agents, which maps each of the Agents that connect to the primary Advisor.
7. A section descriptor load balancers, which maps each of the load balancers (either external or sysplex distributor) that connect to the primary Advisor.
8. A section descriptor for load balancer groups, which maps the groups that are defined to external load balancers.
9. A section descriptor for load balancer group IP addresses, which maps the IP addresses that are configured for a specific load balancer group.
10. A section descriptor for servers, which maps all the servers that make up each of the defined workloads.

Figure 3 describes the layout of the data response message.

Message Header
Record Header for Response
Section Descriptor for Lifeline Advisors
Section Descriptor for Workloads
Section Descriptor for Sites
Section Descriptor for Agents
Section Descriptor for Load Balancers
Section Descriptor for Load Balancer Groups
Section Descriptor for Load Balancer Group IP Addresses
Section Descriptor for Servers
Lifeline Advisor Sections (one for primary Advisor, and one for secondary Advisor – if active)
Zero or more Workload Sections
Zero or more Sites Sections
Zero or more Lifeline Agent Sections
Zero or more Load Balancer Sections (both external and Sysplex Distributor load balancers)
Zero or more Load Balancer Group Sections
Zero or more Load Balancer Group IP Address Sections
Zero or more Server Sections

Figure 3. Layout of the data response message

Use the record header descriptor in the message header to locate the response record header. You can locate the offset of the first section descriptor through the

header. All eight section descriptors are contiguous. You can locate the data for each of the sections through the respective section descriptor. See “NMI message format” for more details about the layout of the NMI messages.

NMI message format

The following information shows the format of an NMI message.

```

/*
** Message Header
*/
typedef struct _AQSMMessageHdr {
    char        MsgHdrID[4];           /* Identifier for Message Header      */
#define AQSMMessageHdrID "AQSM"
    unsigned int MsgHdrLength;        /* Length of message header          */
    unsigned short MsgHdrVersion;    /* Interface version                 */
#define AQSVersion 1
    unsigned short MsgHdrType;       /* Message type                      */
#define AQSSInitType 1
#define AQSSTermType 2
#define AQSSGetDataType 3
    char        MsgHdrRsvd1[4];       /* Reserved – set to 0               */
    char        MsgHdrCorrelator[16]; /* User-defined correlator           */
    unsigned int MsgHdrRc;           /* Return code                       */
#define AQSSRcOK 0
#define AQSSRcError 8
    unsigned int MsgHdrRsn;          /* Reason code                       */
#define AQSSBadID 1
#define AQSSBadVersion 2
#define AQSSBadType 3
#define AQSSBadSize 4
#define AQSSBadFields 5
#define AQSSConnsExceeded 6
#define AQSSInternalError 7
#define AQSSNotAuth 8
    unsigned int MsgHdrMsgLength;    /* Message length (including header) */
    unsigned int MsgHdrTime;         /* Timestamp when message was created */
    char        MsgHdrRsvd2[16];     /* Reserved – set to 0               */
    AQSSRecordDesc MsgHdrRecDesc;    /* Record Descriptor – only
                                     meaningful for GETDATA responses */
} AQSMMessageHdr;
/*
** Section Correlator
*/
typedef struct _AQSCorrelator {
    char        SecID[4];            /* Identifier for the section         */
    unsigned int SecInstance;        /* Instance count of this section    */
} AQSCorrelator;

#define AQSSAdvisorID "AQSA"        /* Identifier for Advisor section    */
#define AQSSWorkloadID "AQSW"       /* Identifier for Workload section   */
#define AQSSSiteID "AQSI"          /* Identifier for Site section       */
#define AQSSAgentID "AQSC"         /* Identifier for Agent section      */
#define AQSSLoadBalancerID "AQSL"  /* Identifier for Load Balancer section */
#define AQSSGroupID "AQSG"        /* Identifier for Group section      */
#define AQSSGrpIPID "AQSP"        /* Identifier for Group IP Address section */
#define AQSSServerID "AQSS"       /* Identifier for Servers section    */
/*
** Message Section for Lifeline Advisors (1st section)
*/
typedef struct _AQSSAdvisorSec {
    AQSCorrelator AdvCorr;          /* Advisor correlator                */
    struct in_addr AdvIpAddr4;      /* Advisor's IPv4 Address            */
    struct in6_addr AdvIpAddr6;    /* Advisor's IPv6 Address           */
    char        AdvSysName[8];      /* System Name where Advisor resides */
    unsigned char AdvRole;          /* Advisor role                      */
#define AQSSAdvisorPrimary 1
#define AQSSAdvisorSecondary 2
    char        AdvRsvd[3];         /* Reserved – set to 0               */
} AQSSAdvisorSec;
/*
** Message Section for Workloads (2nd section)
*/
typedef struct _AQSSWorkloadSec {
    AQSCorrelator WkldCorr;         /* Workload correlator               */
    char        WkldWorkloadName[64]; /* Name of workload                 */
}

```

```

    unsigned char    WkldStatus;          /* Routing status of workload          */
#define AQSWorkloadOk    1              /* Site and servers for workload      */
                                        /* are available                        */
#define AQSWorkloadNotOk 2             /* Site or servers for workload       */
                                        /* are not available                   */
    char            WkldRsvd[3];        /* Reserved – set to 0                 */
} AQSWorkloadSec;
/*
** Message Section for Sites (3rd section)
*/
AQSCorrelator    SiteIdCorr;           /* Site correlator*/
AQSCorrelator    SiteWkldCorr;        /* Correlator for workload this       */
                                        /* Site section maps to               */
union {
    struct in_addr in;                 /* Site's IPv4 address                */
    struct in6_addr in6;              /* Site's IPv6 address                */
} SiteIpAddr;
char            SiteName[8];          /* Name of site (i.e. sysplex name)   */
unsigned char    SiteWorkloadState;   /* Routing state of workload          */
#define AQSSiteWorkloadActive    1     /* Workload is active on this site    */
#define AQSSiteWorkloadQuiesce  2     /* Workload is quiesced on this site  */
char            SiteRsvd[3];         /* Reserved – set to 0                 */
unsigned short   SiteWeight;         /* Routing weight for the             */
                                        /* workload on this site              */
unsigned short   SiteFlags;          /* Site-wide flags                    */
#define AQSSiteIPv4            1      /* SiteIpAddr is IPv4 address         */
} AQSSiteSec;

/*
** Message Section for Lifeline Agents (4th section)
*/
typedef struct _AQSAgentSec {
    AQSCorrelator    AgntCorr;          /* Correlator for Agent               */
    union {
        struct in_addr in;             /* Agent's IPv4 address               */
        struct in6_addr in6;          /* Agent's IPv6 address               */
    } AgntIpAddr;
    char            AgntSysName[8];     /* System name where Agent resides    */
    char            AgntSiteName[8];   /* Name of site (i.e. sysplex name    */
                                        /* where Agent resides                */
    unsigned char    AgntState;        /* State of Agent                     */
#define AQSAgentActive    1           /* Agent is active                    */
#define AQSAgentInactive 2           /* Agent is inactive                  */
    char            AgntRsvd[1];       /* Reserved – set to zero              */
    unsigned short   AgntFlags;        /* Agent flags                         */
#define AQSAgentIPv4    1             /* AgntIpAddr is IPv4 address         */
} AQSAgentSec;

/*
** Message Section for Load Balancers (5th section)
*/
typedef struct _AQSLoadBalancerSec {
    AQSCorrelator    LBCorr;           /* Correlator for Load Balancer       */
    union {
        struct in_addr in;             /* Load Balancer's IPv4 address       */
        struct in6_addr in6;          /* Load Balancer's IPv6 address       */
    } LBIPAddr;
    unsigned char    LBTier;           /* Load Balancer Tier                 */
#define AQSLoadBalancerTier1    1     /* first-tier Load Balancer           */
#define AQSLoadBalancerTier2    2     /* second-tier Load Balancer          */
#define AQSLoadBalancerTierUnk  3     /* Unknown tier                        */
    unsigned char    LBState;         /* State of load balancer              */
#define AQSLoadBalancerActive    1     /* Load balancer is active            */
#define AQSLoadBalancerInactive 2     /* Load balancer is not active        */
    unsigned short   LBFlags;         /* Load balancer flags                */
#define AQSLoadBalancerInt    1       /* Internal load balancer (i.e.       */
                                        /* Sysplex Distributor)               */
#define AQSLoadBalancerIPv4    2      /* LBIPAddr is IPv4 address           */
    char            LBRsvd[8];        /* Reserved – set to zero              */
} AQSLoadBalancerSec;

/*
** Message Section for Groups (6th section)
*/
typedef struct _AQSGroupSec {
    AQSCorrelator    GrpCorr;          /* Correlator for Group               */
    AQSCorrelator    GrpLBCorr;       /* Correlator for Load Balancer       */
                                        /* this group is defined to           */
    AQSCorrelator    GrpWkldCorr;     /* Correlator for Workload this      */
                                        /* group belongs to                   */
    unsigned short   GrpPortNum;      /* Port number for the servers        */
                                        /* configured for this group          */
}

```

```

char      GrpName[255];      /* Group name */
unsigned short GrpFlags;    /* Group flags */
#define AQSGroupInt 1      /* Simulated group for internal load balancers (i.e. Sysplex Distributor) - there is not a corresponding GroupIP section for this group */
char GrpRsvd[1];          /* Reserved - set to zero */
} AQSGroupSec;
/*
** Message Section for Group IP Addresses (7th section)
*/
typedef struct _AQSGrpIpSec {
    AQSCorrelator GrpIpCorr; /* Correlator for GrpIp */
    AQSCorrelator GrpIpGrpCorr; /* Correlator for Load Balancer Group this IP Address is defined to */
    union {
        struct in_addr in; /* IPv4 address for a server configured for this group */
        struct in6_addr in6; /* IPv6 address for a server configured for this group */
    } GrpIpAddr;
    unsigned short GrpIpFlags; /* Group IP flags */
#define AQSGrpIpIPv4 1 /* GrpIpAddr is IPv4 address */
    char GrpIpRsvd[2]; /* Reserved - set to zero */
} AQSGrpIpSec;
/*
** Message Section for Servers (8th section)
*/
typedef struct _AQSServerSec {
    AQSCorrelator SrvrCorr; /* Correlator for Server */
    AQSCorrelator SrvrLBCorr; /* Correlator for Load Balancer this server is defined to */
    AQSCorrelator SrvrWkldCorr; /* Correlator for Workload this server belongs to */
    union {
        struct in_addr in; /* Server's IPv4 address */
        struct in6_addr in6; /* Server's IPv6 address */
    } SrvrIpAddr;
    char SrvrJobName[8]; /* The MVS jobname of server */
    char SrvrSysName[8]; /* System name where server resides */
    char SrvrSiteName[8]; /* Name of site (i.e. sysplex where server resides */
    unsigned int SrvrNormWeight; /* Net weight for this server relative to other servers on this site - calculated by applying CS health as percentage of WLM weight for this server */
    unsigned int SrvrWlmWeight; /* ServerWLM weight for this server - measure of how well server is meeting its WLM policies and represents the displaceable processor capacity based on server's importance relative to other servers on this site */
    unsigned int SrvrAbTerms; /* Server abnormal terminations - number of abnormal transaction completions per 1000 transactions */
    unsigned int SrvrHealth; /* Health indicator for server - used to adjust the reported ServerWLM weight */
    unsigned int SrvrCPUWeight; /* CPU factor in WLM weight - amount of displaceable general CPU capacity based on server's importance relative to other servers on this site and modified by proportion of general CPU capacity being consumed compared to zAAP and zIIP processors */
    unsigned int SrvrzAAPWeight; /* zAAP factor in WLM weight - amount of displaceable zAAP capacity based on server's importance relative to other servers on this site and modified by proportion of zAAP capacity being consumed compared to general CPU and zIIP */
}

```

```

        processors
        /* zIIP factor in WLM weight – amount of displaceable zIIP capacity based on server's importance relative to other servers on this site and modified by proportion of zIIP capacity being consumed compared to general CPU and zAAP processors */
unsigned int    SrvrZIIPWeight;

        /* Health of server from a Communications Server perspective – calculated based on how well server is keeping up with connections in backlog, how well it is establishing new connections, and whether the server is dropping connections */
unsigned int    SrvrCSHealth;

        /* Port number where server is listening */
unsigned short  SrvrPortNum;

        /* Server flags */
unsigned short  SrvrFlags;
#define AQSServerIPv4    1
        /* SrvrIPAddr is Ipv4 address */
unsigned char   SrvrState;
#define AQSServerUp      1
        /* State of server */
#define AQSServerDown    2
        /* Server is up */
        /* Server is down */
char            SrvrRsvd[3];
        /* Reserved – set to zero */
} AQSServerSec;

```

Chapter 10. Multi-site Workload Lifeline messages

AQS0001I MULTI-SITE WORKLOAD LIFELINE REQUIRES THE TCP/IP BASE FEATURE OF z/OS

Explanation: The Multi-site Workload Lifeline function is disabled because the TCP/IP base feature of z/OS is not enabled.

System action: Processing ends.

Operator response: Contact the system programmer.

System programmer response: The IFAPRDxx parmlib member specifies whether or not the TCP/IP base feature is enabled. Correct the IFAPRDxx parmlib member if it is in error. IBM has defined the appropriate product enablement settings in the IFAPRD00 member of SYS1.IBM.PARMLIB.

If TCP/IP_BASE is not part of your system, no action is required; the Multi-site Workload Lifeline function cannot be used.

Module: AQSUTUTI

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

AQS0004I *applname* IS NOT SUPPORTED IN THIS ENVIRONMENT

Explanation: The Multi-site Workload Lifeline application was started in an unsupported environment. It is supported only in the z/OS UNIX shell or batch environments.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

System action: Processing ends.

Operator response: Start the Multi-site Workload Lifeline Advisor or Agent in a supported environment.

System programmer response: None.

Module: AQSUTUTI

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0004I LLADVSR IS NOT SUPPORTED IN THIS ENVIRONMENT

AQS0005I *applname* MUST BE APF-AUTHORIZED

Explanation: The Multi-site Workload Lifeline application requires APF authorization to function correctly, but the application was not running as APF authorized.

In the message text:

AQS0006I • AQS0101I

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

System action: Processing ends.

Operator response: Contact the system programmer to ensure that the Advisor or Agent was installed correctly.

System programmer response: Ensure that the Advisor or Agent was installed correctly. If the Advisor or Agent executable application resides in the z/OS UNIX file system, ensure that the APF-authorized attribute is on. If the Advisor or Agent resides in a load module, ensure that the library that contains it is APF authorized.

Module: AQSUTUTI

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0005I LLADVSR MUST BE APF-AUTHORIZED

AQS0006I MESSAGE CATALOG *filename* COULD NOT BE OPENED – DEFAULT MESSAGES WILL BE USED

Explanation: The Multi-site Workload Lifeline message catalog file could not be opened. The command will use the default message strings instead of the message strings in the message catalog file.

In the message text:

filename

The name of the message catalog that could not be opened.

System action: Processing continues.

Operator response: Contact the system programmer.

| **System programmer response:** Ensure that the message catalog was installed properly. If the message catalog is
| installed in a location other than the default, verify the NLSPATH and LANG environment variables are correctly
| defined in your Lifeline Advisor and Lifeline Agent started procedures.

Module: AQSUTUTI

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0006I MESSAGE CATALOG aqs11msg.cat COULD NOT BE OPENED
– DEFAULT MESSAGES WILL BE USED

AQS0101I *applname* STARTING

Explanation: The Multi-site Workload Lifeline application is starting.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

System action: Processing continues.**Operator response:** None.**System programmer response:** None.**Module:** LAMAIN, LMMAIN**Routing code:** 8, 10**Descriptor code:** 12**Automation:** Not applicable for automation.**Example:**

AQS0101I LLADVSR STARTING

AQS0102I *applname* **INITIALIZATION COMPLETE****Explanation:** The Multi-site Workload Lifeline application completed initialization.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

System action: Processing continues.**Operator response:** None.**System programmer response:** None.**Module:** LAMAIN, LMMAIN**Routing code:** 8, 10**Descriptor code:** 12**Automation:** Not applicable for automation.**Example:**

AQS0102I LLADVSR INITIALIZATION COMPLETE

AQS0103I *applname* **SHUTDOWN IN PROGRESS****Explanation:** The Multi-site Workload Lifeline application is shutting down in response to a STOP command.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

System action: Processing continues.**Operator response:** None.**System programmer response:** None.

AQS0104I • AQS0105I

Module: LAMAIN, LMMAIN

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0103I LLADVSR SHUTDOWN IN PROGRESS

AQS0104I *applname* SHUTDOWN COMPLETE

Explanation: The Multi-site Workload Lifeline application ended in response to a STOP command.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

System action: Processing ends.

Operator response: None.

System programmer response: None.

Module: LAMAIN, LMMAIN

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0104I LLADVSR SHUTDOWN COMPLETE

AQS0105I *applname* CONFIGURATION ERRORS DETECTED

Explanation: The configuration file for the Multi-site Workload Lifeline application cannot be opened, or contains one or more errors.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

System action: Processing ends.

Operator response: Contact the system programmer.

System programmer response: Examine the syslogd file for configuration error messages. The syslogd identifier is lladvsr for the Advisor and llagent for the Agent. Correct the configuration file errors and restart the application. See Chapter 6, "Multi-site Workload Lifeline configuration statements," on page 37 for more information about configuration statements and parameters.

Module: LACONFIG, LMCMD, LMCONFIG

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0105I LLADVSR CONFIGURATION ERRORS DETECTED

AQS0107I *applname* **MODIFY COMMAND SYNTAX ERROR AT** *location*

Explanation: The Multi-site Workload Lifeline application detected a syntax error on a MODIFY command.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

location

The portion of the MODIFY command that is not syntactically valid.

System action: The MODIFY command is rejected.

Operator response: Examine the syslogd file to determine why the MODIFY command failed. The syslogd identifier is lladvr for the Advisor and llagent for the Agent. Re-enter the MODIFY command using the valid syntax. See Chapter 7, "Lifeline Advisor commands," on page 53 and Chapter 8, "Lifeline Agent commands," on page 73 for more information.

System programmer response: None.

Module: LACMD, LCCMD, LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0107I LLADVSR MODIFY COMMAND SYNTAX ERROR AT 'BAD'

AQS0108I *applname* **MODIFY COMMAND PARAMETER** *parm* **INCORRECT VALUE** *value*

Explanation: The Multi-site Workload Lifeline application detected an incorrect value for a parameter on a MODIFY command.

In the message text:

applname

The application name. Possible values:

LLADVSR

For the Multi-site Workload Lifeline Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

parm

The name of the MODIFY command parameter that is in error.

value

The incorrect value entered on the MODIFY command.

System action: The MODIFY command is rejected.

Operator response: Re-enter the MODIFY command with a valid value for the indicated parameter. See Chapter 7,

AQS0109I • AQS0110I

“Lifeline Advisor commands,” on page 53 and Chapter 8, “Lifeline Agent commands,” on page 73 for more information.

System programmer response: None.

Module: LCCMD, LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0108I LLADVSR MODIFY COMMAND PARAMETER LEVEL
INCORRECT VALUE 2000
```

AQS0109I *syscall* **CALL FAILED** *errno/errnojr* **FOR PORT** *port*

Explanation: The Multi-site Workload Lifeline Advisor or Agent application was unable to initialize a listening socket.

In the message text:

syscall

The type of call that failed. For example, the system call might be a SOCKET, SETSOCKOPT, or BIND call.

errno

The UNIX System Services return code. See *return codes (errno)* in *z/OS UNIX System Services Messages and Codes* for more information about these return codes.

errnojr

The hexadecimal UNIX System Services reason code. See *return codes (errno)* in *z/OS UNIX System Services Messages and Codes* for more information about the format of the 4-byte reason code.

port

The port number on which the call failed.

System action: Processing ends.

Operator response: Determine whether TCP/IP is available and restart if necessary. Restart the application. If TCP/IP is available when the application issues this message, save the syslogd file and contact the system programmer.

System programmer response: If TCP/IP is available when the application issues this message, examine the syslogd file and correct the error. The syslogd identifier is lladvr for the Advisor and llagent for the Agent.

Module: LMLISTEN

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0109I BIND CALL FAILED 6F/744C7246 FOR PORT 3860
```

AQS0110I **UNABLE TO ESTABLISH** *endpoint* **LISTENING SOCKET**

Explanation: The Multi-site Workload Lifeline Advisor was unable to initialize because it could not create a listening socket.

In the message text:

endpoint

The listening socket that could not be created. Possible values are LOAD BALANCER, ADVISOR, or AGENT.

System action: Processing ends.

Operator response: Determine whether TCP/IP is available and restart if necessary. Restart the application. If

TCP/IP is available when the application issues this message, save the syslogd file and contact the system programmer.

System programmer response: If TCP/IP is available when the Advisor issues this message, see message AQS0109I that might precede this message, or examine the syslogd file and correct the error. The syslogd identifier is 11advr for the Advisor.

Module: LMLISTEN

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0110I UNABLE TO ESTABLISH LOAD BALANCER LISTENING SOCKET

AQS0111I *applname* **DEBUG LEVEL** *level*

Explanation: This message is issued in response to a MODIFY *procname*,DISPLAY,DEBUG command.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

level

The current debug level in effect. Valid debug level values are:

- 1 Errors are logged.
- 2 Warnings are logged.
- 4 Significant events are logged.
- 8 Informational messages are logged.
- 16 Debug data messages are logged. This level is for IBM service use only. If the *applname* value is LLADVSR, messages related to TCP/IP messages sent between the Advisor and load balancers, between the primary and secondary Advisors, and between the Advisor and Agent are logged.
- 32 Debug data messages are logged. This level is for IBM service use only. If the *applname* value is LLAGENT, messages related to data collection and manipulation that support weight calculations are logged.
- 64 Internal debug data is logged. This level is for IBM service use only.
- 128 Function entry and exit tracing are logged. This level is for IBM service use only.

Individual values can be added together. For example, if the debug level displayed is 7, all error, warning, and significant event messages are logged. These messages are logged to the syslogd file.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LACMD, LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

AQS0112I • AQS0114I

Example:

AQS0111I LLADVSR DEBUG LEVEL 7

AQS0112I LOAD BALANCER SUMMARY

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,DISPLAY,LB command. This message is followed by summary information about connected load balancers. See "MODIFY *advisor_proc*,DISplay command: Display Lifeline Advisor information" on page 53 for the explanation of the display output.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 5, 8, 9

Automation: Not applicable for automation.

AQS0113I LOAD BALANCER DETAILS

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,DISPLAY,LB,DETAIL command. This message is followed by detailed information about connected load balancers. See "MODIFY *advisor_proc*,DISplay command: Display Lifeline Advisor information" on page 53 for the explanation of the display output.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 5, 8, 9

Automation: Not applicable for automation.

AQS0114I MEMBER SUMMARY

Explanation: The Multi-site Workload Lifeline Agent issues this message in response to a MODIFY *procname*,DISPLAY,MEMBERS command. This message is followed by summary information about members (applications being load balanced) that one or more load balancers registered with the Multi-site Workload Lifeline Advisor. See "MODIFY *agent_proc*,DISplay command: Display Lifeline Agent information" on page 73 for the explanation of the display output.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LACMD

Routing code: 8, 10

Descriptor code: 5, 8, 9

Automation: Not applicable for automation.

AQS0115I MEMBER DETAILS

Explanation: The Multi-site Workload Lifeline Agent issues this message in response to a MODIFY *procname*,DISPLAY,MEMBERS,DETAIL command. This message is followed by detailed information about members (applications being load balanced) that one or more load balancers registered with the Multi-site Workload Lifeline Advisor. See “MODIFY *agent_proc*,DISPlay command: Display Lifeline Agent information” on page 73 for the explanation of the display output.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LACMD

Routing code: 8, 10

Descriptor code: 5, 8, 9

Automation: Not applicable for automation.

AQS0116I *applname* INITIALIZATION ERROR - REASON CODE *reason*

Explanation: The Multi-site Workload Lifeline application could not initialize because it detected an error.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

reason

The code for the error encountered. Possible values for the reason code are:

- 1 Another copy of the application is already active. Only one copy of the Advisor or Agent can be active on an MVS system.
- 2 The Advisor or Agent application cannot open the configuration file, or found an error in the configuration file. Message AQS0105I might precede this message.
- 3 An internal error was encountered in the application.
- 4 The Advisor or Agent application found an error in a start option parameter in the started procedure.
- 5 The user ID associated with the started task is not authorized, or the application was not started as a started procedure.
- 6 A required resource is not available. For example, the TCP/IP stack is not started, or a configured IP address is not defined or available on the TCP/IP stack.
- 7 The Advisor or Agent application was started on an unsupported z/OS release.

System action: Processing ends.

Operator response:

- If the *reason* value is 1, verify that the instance of the active application is the one that you want. If a previous instance of the application is stopped but has not ended, issue a CANCEL command to cancel the previous instance before you start the new instance.
- If the *reason* value is 6, start the TCP/IP stack if it is not already started.
- If the reason value is 7, verify that the application is being started on a supported z/OS release. Multi-site Workload Lifeline is supported on z/OS V1R11 and higher releases.
- If the stack is already started, and for all other reason values, save the syslogd file and contact the system programmer.

AQS0117I

System programmer response: Ensure that there is sufficient information to debug this problem. Configure the application to use a debug level of 127. See “Debug levels” on page 27 for information about how to configure the debug level for the specified application. Take the appropriate action, based on the *reason* value:

- If the *reason* value is 2, examine the application syslogd file for errors. Correct the configuration file as needed. See Chapter 3, “Configuring Multi-site Workload Lifeline,” on page 11 for information about configuring the Advisor and Agent.
- If the *reason* value is 3, contact the IBM software support center. The application syslogd file is the minimum diagnostic data that must be provided. See “Diagnostic data” on page 28 for more information about collecting diagnostic data.
- If the *reason* value is 4, examine the application syslogd file for errors. Correct the started procedure as needed.
- If the *reason* value is 5, examine the security product profiles that have been established for the Advisor and Agent. Ensure that the application is started from a started procedure and that the user ID in the started procedure is permitted to the appropriate profiles if they are defined. See “Authorizing the Lifeline Agents to use WLM services” on page 9 for more information about setting up the authorization profiles for the security product.
- If the *reason* value is 6 and the TCP/IP stack is already started, examine the syslogd file for errors. The syslogd identifier is 11advr for the Advisor and 11agent for the Agent. Verify that the correct IP addresses are configured in the configuration file. Correct the configuration file as needed. See Chapter 3, “Configuring Multi-site Workload Lifeline,” on page 11 for more information about configuring the Advisor and Agent.

Module: LAMAIN, LMADV, LMMAIN

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0116I LLADVSR INITIALIZATION ERROR - REASON CODE 6
```

AQS0117I *applname* CONFIGURATION WARNINGS DETECTED

Explanation: The Multi-site Workload Lifeline application configuration file contains one or more statements that resulted in warning messages being logged. These warnings do not cause the application to end, but might indicate conditions that affect the normal operation of the application.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

System action: Processing continues.

Operator response: Save the syslogd file and contact the system programmer.

System programmer response: Examine the syslogd file for the application configuration warning messages. The syslogd identifier is 11advr for the Advisor and 11agent for the Agent. Correct the configuration file definitions that generated the warning messages and either restart the application or, if the *applname* value is LLADVSR and the corrections are for modifiable configuration definitions, and issue the MODIFY *procname*,REFRESH command. See Chapter 3, “Configuring Multi-site Workload Lifeline,” on page 11 for more information about configuring the Advisor and Agent.

Module: LACONFIG, LMADV, LMCMD, LMCONFIG

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0117I LLADVSR CONFIGURATION WARNINGS DETECTED

AQS0118I ALL APPLICATIONS ARE QUIESCED BY OPERATOR

Explanation: The Multi-site Workload Lifeline Agent issues this message in response to a request to quiesce or enable a subset of the target applications. A `MODIFY procname,QUIESCE` or `MODIFY procname,ENABLE` command was issued. A previous `MODIFY procname,QUIESCE,SYSTEM` command was issued to quiesce all applications for this Agent. The Agent enforces a hierarchy so that a previous `SYSTEM` action cannot be overridden by a `TCPNAME` or `PORT` request.

System action: The `MODIFY` command is rejected because all applications have been quiesced by the `MODIFY procname,QUIESCE,SYSTEM` command.

Operator response: Issue the `MODIFY procname,DISPLAY,MEMBERS` command to list the registered members and the status flags for each member. The operator quiesce flag (`SYSQ`) indicates that an MVS operator quiesced all members. If you do not want some of the members to be quiesced, issue the `MODIFY procname,ENABLE,SYSTEM` command to re-enable all members, and the `MODIFY procname,QUIESCE,TCPNAME=stackname` command or the `MODIFY procname,QUIESCE,PORT=portnum` command to quiesce a subset of the members. See Chapter 8, "Lifeline Agent commands," on page 73 for more information.

System programmer response: None.

Module: LACMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

AQS0120I ALL APPLICATIONS FOR *stackname* ARE QUIESCED BY OPERATOR

Explanation: The Multi-site Workload Lifeline Agent issues this message in response to a request to quiesce or enable a specific target application. A `MODIFY procname,QUIESCE` or `MODIFY procname,ENABLE` command was issued. A previous `MODIFY procname,QUIESCE,TCPNAME=stackname` command was issued to quiesce all applications for the TCP/IP stack. The Agent enforces a hierarchy so that a previous `TCPNAME` action cannot be overridden by a `PORT` request.

In the message text:

stackname

The name of the TCP/IP stack.

System action: The `MODIFY` command is rejected because all applications for this TCP/IP stack have been quiesced by the `MODIFY procname,QUIESCE,TCPNAME=stackname` command.

Operator response: Issue the `MODIFY procname,DISPLAY,MEMBERS` command to list the registered members and the status flags for each member. The operator quiesce flag (`TCPQ`) indicates that an MVS operator quiesced all members for the TCP/IP stack. If you do not want some of the members to be quiesced, issue the `MODIFY procname,ENABLE,TCPNAME=stackname` command to re-enable all members for this TCP/IP stack, and the `MODIFY procname,QUIESCE,PORT=portnum` command to quiesce a subset of the members. See Chapter 8, "Lifeline Agent commands," on page 73 for more information.

System programmer response: None.

Module: LACMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0120I ALL APPLICATIONS FOR TCPIP ARE QUIESCED BY OPERATOR

AQS0121I NETWORK ACCESS TO PEER ADVISOR ON *sysname* HAS RECOVERED

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it detects that it has reestablished network communication with its peer Advisor.

In the message text:

sysname

The MVS system name where the peer Advisor is active.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LMADV

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0121I NETWORK ACCESS TO PEER ADVISOR ON CNTL2 HAS RECOVERED

AQS0122I NO MEMBERS MATCH SELECTION CRITERIA

Explanation: The Multi-site Workload Lifeline Agent issues this message in response to a MODIFY *procname*,QUIESCE or a MODIFY *procname*,ENABLE command. The MODIFY command is rejected because no active registered target applications match the criteria specified in the MODIFY command.

This message is also issued in response to a MODIFY *procname*,QUIESCE,TCP=*stackname* or MODIFY *procname*,ENABLE,TCP=*stackname* command when the *stackname* value does not match a TCP/IP stack that is active on the Agent system.

System action: The MODIFY command is ignored. Processing continues.

Operator response: Issue the MODIFY *procname*,DISPLAY,MEMBERS command to list the registered members on the local MVS system and the status flags for each member. The operator quiesce flag (SYSQ, TCPQ, or APPQ) indicates that an MVS operator quiesced the member. The absence of this flag indicates that the member is enabled from an MVS operator perspective. If the flag value is not the value that you want, issue a MODIFY *procname*,QUIESCE or a MODIFY *procname*,ENABLE command to change the flag value. See Chapter 8, "Lifeline Agent commands," on page 73 for more information.

System programmer response: None.

Module: LACMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

AQS0123I *cmd* COMMAND REJECTED

Explanation: The Multi-site Workload Lifeline Agent issues this message in response to a MODIFY *procname*,QUIESCE or a MODIFY *procname*,ENABLE command. The MODIFY command is rejected. A more specific error message precedes this message and explains the reason for the command rejection.

In the message text:

cmd

The command that was rejected. Possible values are:

- QUIESCE TCPNAME
- ENABLE TCPNAME
- QUIESCE APPLICATION

- ENABLE APPLICATION

System action: The MODIFY command is ignored. Processing continues.

Operator response: Look for a previous message that provides more specific information about why the MODIFY command was rejected. Issue the MODIFY *procname*,DISPLAY,MEMBERS command to list the registered members on the local MVS system and the status flags for each member. The operator quiesce flag (SYSQ, TCPQ, or APPQ) indicates that an MVS operator quiesced the member. The absence of this flag indicates that the member is enabled from an MVS operator perspective. If the flag value is not the value that you want, issue a MODIFY *procname*,QUIESCE or a MODIFY *procname*,ENABLE command to change the flag value. See Chapter 8, “Lifeline Agent commands,” on page 73 for more information.

System programmer response: None.

Module: LACMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0123I QUIESCE APPLICATION COMMAND REJECTED
```

AQS0124I NETWORK ACCESS TO PEER ADVISOR ON *sysname* NOT AVAILABLE

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it detects that it can no longer communicate with its peer Advisor over the network. If the Lifeline Advisor that issues this message is the secondary Advisor, AQS0164W was issued before this message.

In the message text:

sysname

The MVS system name where the peer Advisor was last active.

System action: Processing continues.

Operator response: Contact the system programmer.

System programmer response: Verify the network connectivity between this Advisor and the peer Advisor. Ensure that the Advisor configuration files are identical between this Advisor and the peer Advisor. See *z/OS Communications Server: IP Diagnosis Guide* for more information about diagnosing connectivity problems.

Module: LMBCPII

Routing code: 8, 10

Descriptor code: 12

Automation: This message is a possible candidate for automation if you want to use the MODIFY *procname*,TAKEOVER command to have this Advisor assume the role of primary Advisor.

Example:

```
AQS0124I NETWORK ACCESS TO PEER ADVISOR ON CNTL2 NOT AVAILABLE
```

AQS0125I BCPII ACCESS TO PEER ADVISOR ON *sysname* NOT AVAILABLE

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it detects that it can no longer communicate with the image (LPAR) where the peer Advisor was active by using the z/OS Base Control Program Internal Interface (BCPii) service.

In the message text:

sysname

The MVS system name where the peer Advisor was last active.

System action: Processing continues.

Operator response: Contact the system programmer.

AQS0126I • AQS0127W

| **System programmer response:** Verify that z/OS is operational on the peer Advisor's image. Verify the connectivity
| used by BCPII to communicate with the peer Advisor's image. See *z/OS MVS Programming: Callable Services for*
| *High-Level Languages* for information about diagnosing BCPII issues.

Module: LMBCPII

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0125I BCPII ACCESS TO PEER ADVISOR ON CNTL2 NOT AVAILABLE

AQS0126I BCPII ACCESS TO PEER ADVISOR ON *sysname* HAS RECOVERED

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it detects that it has reestablished communication with the image (LPAR) where the peer Advisor was active by using the z/OS Base Control Program Internal Interface (BCPII) service.

In the message text:

sysname

The MVS system name where the peer Advisor is active.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LMBCPII

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0126I BCPII ACCESS TO PEER ADVISOR ON CNTL2 HAS RECOVERED

AQS0127W *applname* CONNECTION TO ADVISOR AT *ipaddress* CLOSED DUE TO PROTOCOL ERROR

Explanation: The Multi-site Workload Lifeline Advisor that was started as the secondary Advisor or Agent issues this message when it closes its connection to the primary Advisor. An internal protocol error generates this message. This message will be deleted when the secondary Advisor or Agent reconnects to the primary Advisor.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline secondary Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

ipaddress

The IP address of the primary Advisor.

System action: The secondary Advisor or Agent takes a CEEDUMP, writes messages to the syslogd file, and attempts to reconnect to the primary Advisor. The secondary Advisor or Agent attempts to reconnect to the primary Advisor.

Operator response: Save the dump, syslogd file, and packet trace if it is active. The dump data set is specified in the CEEDUMP DD statement in the Advisor's or Agent's started procedure. Contact the system programmer.

System programmer response: Examine the syslogd files for the Advisor and Agent. The syslogd identifier is

lladvsr for the Advisor and llagent for the Agent. If the debug level includes messages at the message level, the syslogd file will show the data that each application sent or received. If the data that was sent by one application was the same data received by the corresponding application, contact IBM software support services. If the data that was sent was not the same data that was received, this might indicate that the network integrity has been compromised. If the packet trace is active, examine the trace for the data that was sent and received. If the packet trace is not active, try to recreate the problem with active packet trace. See *z/OS Communications Server: IP Diagnosis Guide* for information about the packet trace.

Module: LMAARP

Routing code: 1, 8

Descriptor code: 2, 7

Automation: This message is a possible candidate for automation if you want to create snapshots of the Advisor and Agent syslogd files for later problem determination.

Example:

AQS0127W LLADVSR CONNECTION TO ADVISOR AT 10.10.10.1 CLOSED DUE TO PROTOCOL ERROR

AQS0128I *peername* CONNECTION FROM *ipaddress* CLOSED DUE TO INACTIVITY

Explanation: The Multi-site Workload Lifeline Advisor issues this message when the Advisor closes its connection to the Multi-site Workload Lifeline Agent or peer Advisor application because this Advisor did not receive a message from the application within the expected time.

In the message text:

peername

The application name. Possible values are:

ADVISOR

ADVISOR for the Multi-site Workload Lifeline Advisor

AGENT

AGENT for the Multi-site Workload Lifeline Agent

ipaddress

The IP address of the peer Advisor or Agent

System action: The Advisor closes the connection with the application. The peer Advisor or Agent attempts to reconnect to the Advisor until it is successful or is stopped. If the situation is temporary, the peer Advisor or Agent will successfully reconnect to the Advisor.

Operator response: If the peer Advisor or Agent is not active, start it. If the error persists, contact the system programmer.

System programmer response: Network connectivity problems, routing problems, slow system performance on the peer Advisor or Agent system, and low MVS dispatching priority for the application might cause this problem. If the error persists, increase the value of the `advisor_timeout` or `updated_interval` statement in the Advisor configuration file and restart the Advisor. See Chapter 6, "Multi-site Workload Lifeline configuration statements," on page 37 for more information about configuration statements. See *z/OS Communications Server: IP Diagnosis Guide* for information about diagnosing network connectivity problems.

Module: LMADV, LMAGNT

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0128I ADVISOR CONNECTION FROM 10.10.10.1 CLOSED DUE TO INACTIVITY

AQS0129I *applname* CONNECTED TO ADVISOR AT *ipaddress*

Explanation: The Multi-site Workload Lifeline secondary Advisor or Agent issues this message when it is connected to the Multi-site Workload Lifeline primary Advisor.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline secondary Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

ipaddress

The IP address of the primary Advisor

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LAADV, LMADV

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0129I LLADVSR CONNECTED TO ADVISOR AT 10.10.10.1

AQS0130I *applname* CONNECTION TO ADVISOR AT *ipaddress* IS NO LONGER ACTIVE

Explanation: The Multi-site Workload Lifeline Advisor or Agent issues this message when it has lost its connection to the peer Multi-site Workload Lifeline Advisor.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline primary or secondary Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

ipaddress

The IP address of the primary or secondary Advisor

System action: The Advisor or Agent attempts to reconnect to the other Advisor. If the situation is temporary, the Advisor or Agent will successfully reconnect to the other Advisor.

Operator response: If the other Advisor is not active, start it. If the Advisor is active, save the syslogd file and contact the system programmer.

System programmer response: Examine the syslogd file for Advisor or Agent error or warning messages. The syslogd identifier is lladvr for the Advisor and llagent for the Agent. Correct any errors and restart the application that is in error.

Module: LAMAIN, LMADV

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0130I LLADVSR CONNECTION TO ADVISOR AT 10.10.10.1 IS NO LONGER ACTIVE

AQS0131I AGENT CONNECTED FROM *ipaddress*

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it detects that it is connected to a Multi-site Workload Lifeline Agent.

In the message text:

ipaddress

The IP address of the Agent.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LMAGNT

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0131I AGENT CONNECTED FROM 10.10.10.1

AQS0132I AGENT CONNECTION FROM *ipaddress* IS NO LONGER ACTIVE

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it detects that it lost its connection to the Multi-site Workload Lifeline Agent. This message usually indicates that the Agent has been stopped.

In the message text:

ipaddress

The IP address of the previously connected Agent.

System action: Processing continues. If the Agent is not stopped, the Agent attempts to reconnect to the Advisor. If the situation is temporary, the Agent will reconnect to the Advisor.

Operator response: Determine whether the Agent has ended. Restart the Agent if necessary. If the Agent cannot reconnect to the Advisor, save the syslogd file and contact the system programmer.

System programmer response: No action is required if the Agent was intentionally stopped; otherwise, examine the syslogd file for Advisor or Agent errors, or warning messages. The syslogd identifier is 11advsr for the Advisor and 11agent for the Agent. Correct any errors and restart the application that is in error.

Module: LMAGNT

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0132I AGENT CONNECTION FROM 10.10.10.1 IS NO LONGER ACTIVE

AQS0133I LOAD BALANCER CONNECTED FROM *ipaddress*

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it detects that it is connected to a load balancer.

In the message text:

AQS0134I • AQS0135I

ipaddress

The IP address of the load balancer.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LMLB

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0133I LOAD BALANCER CONNECTED FROM 10.10.10.1
```

AQS0134I LOAD BALANCER CONNECTION FROM *ipaddress* IS NO LONGER ACTIVE

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it detects that it lost its connection with a load balancer. This message usually indicates that the load balancer has been stopped or the load balancer was incorrectly configured.

In the message text:

ipaddress

The IP address of the previously connected load balancer.

System action: Processing continues. If the load balancer is still active, it might attempt to reconnect to the Advisor.

Operator response: Determine whether the load balancer is active. Restart the load balancer, if necessary. If the load balancer is active, contact the system programmer.

System programmer response: Check the load balancer and correct any configuration or connectivity problems. Restart the load balancer, if necessary. See *z/OS Communications Server: IP Diagnosis Guide* for information about diagnosing network connectivity problems.

Module: LMLB

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0134I LOAD BALANCER CONNECTION FROM 10.10.10.1 IS NO  
LONGER ACTIVE
```

AQS0135I ADVISOR CONNECTION FROM *ipaddress* CLOSED DUE TO PROTOCOL ERROR

Explanation: The Multi-site Workload Lifeline Advisor that was started as the primary Advisor issues this message when it closes its connection to the secondary Advisor because of an internal protocol error.

In the message text:

ipaddress

The IP address of the secondary Advisor.

System action: The primary Advisor takes a CEEDUMP, writes messages to the syslogd file, and attempts to accept a reconnect from the secondary Advisor.

Operator response: Save the dump, syslogd file, and packet trace if it is active. The dump data set is specified in the CEEDUMP DD statement in the Advisor's started procedure. Contact the system programmer.

System programmer response: Examine the syslogd files for the Advisor. The syslogd identifier is 11advsr for the Advisor. If the debug level includes messages at the message level, the syslogd file will show the data that each application sent or received. If the data that was sent by one application was the same data received by the

corresponding application, contact IBM software support services. If the data that was sent was not the same data that was received, this might indicate that the network integrity has been compromised. If the packet trace is active, examine the trace for the data that was sent and received. If the packet trace is not active, try to recreate the problem with active packet trace. See *z/OS Communications Server: IP Diagnosis Guide* for information about the packet trace.

Module: LMAARP

Routing code: 8, 10

Descriptor code: 12

Automation: This message is a possible candidate for automation if you want to create snapshots of the Advisor and peer Advisor syslogd files for later problem determination.

Example:

```
AQS0135I ADVISOR CONNECTION FROM 10.10.10.1 CLOSED DUE TO
PROTOCOL ERROR
```

AQS0136W AGENT CONNECTION FROM *ipaddress* CLOSED DUE TO PROTOCOL ERROR

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it closes its connection to the Multi-site Workload Lifeline Agent because of an internal protocol error. This message will be deleted when the Agent reconnects to the Advisor.

In the message text:

ipaddress

The IP address of the previously connected Agent.

System action: The Advisor takes a CEEDUMP and writes messages to the syslogd file. If the Agent is still active, it attempts to reconnect to the Advisor until the Agent connects with the Advisor or the Agent is stopped. If the situation is temporary, the Agent will reconnect to the Advisor.

Operator response: Save the dump, syslogd file, and packet trace if it is active. The dump data set is specified in the CEEDUMP DD statement in the Advisor's started procedure. Contact the system programmer.

System programmer response: Examine the syslogd files for the Advisor and Agent. The syslogd identifier is 11advsr for the Advisor and 11agent for the Agent. If the debug level includes messages at the message level, the syslogd file will show the data that each application sent or received. If the data that was sent by one application was the same data received by the corresponding application, contact IBM software support services. If the data that was sent was not the same data that was received, this might indicate that the network integrity has been compromised. If the packet trace is active, examine the trace for the data that was sent and received. If the packet trace is not active, try to recreate the problem with active packet trace. See *z/OS Communications Server: IP Diagnosis Guide* for information about the packet trace.

Module: LCZAP, LMAGNT

Routing code: 1, 8

Descriptor code: 2, 7

Automation: This message is a possible candidate for automation if you want to create snapshots of the Advisor and Agent syslogd files for later problem determination.

Example:

```
AQS0136W AGENT CONNECTION FROM 10.10.10.1 CLOSED DUE TO
PROTOCOL ERROR
```

AQS0137I *applname* ENDED ABNORMALLY

Explanation: The Multi-site Workload Lifeline application ended in response to an unexpected error.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline Advisor

AQS0138I • AQS0139I

LLAGENT

For the Multi-site Workload Lifeline Agent

System action: Processing ends.

Operator response: Save the CEEDUMP, snap output, and syslogd file. Contact the system programmer.

System programmer response: Contact IBM software support services.

Module: LCASSERT, LCERROR

Routing code: 8, 10

Descriptor code: 12

Automation: This message is a possible candidate for automation if you want to create a snapshot of the Advisor or Agent syslogd file for later problem determination.

Example:

AQS0137I LLADVSR ENDED ABNORMALLY

AQS0138I *applname* DEBUG LEVEL UPDATED

Explanation: The Multi-site Workload Lifeline application issues this message in response to a MODIFY *procname*,DEBUG,LEVEL= command.

In the message text:

applname

The application name. Possible values are:

LLADVSR

For the Multi-site Workload Lifeline Advisor

LLAGENT

For the Multi-site Workload Lifeline Agent

System action: The MODIFY command is accepted. Processing continues.

Operator response: None.

System programmer response: None.

Module: LACMD, LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0138I LLADVSR DEBUG LEVEL UPDATED

AQS0139I ALL REGISTERED APPLICATIONS ARE NOW *state*

Explanation: The Multi-site Workload Lifeline Agent issues this message in response to a MODIFY *procname*,ENABLE|QUIESCE,SYSTEM command.

In the message text:

state

The state of the registered applications on the system where the command was issued. Possible values are:

- ENABLED
- QUIESCED

System action: The MODIFY command is accepted. Processing continues.

Operator response: None.

System programmer response: None.

Module: LACMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0139I ALL REGISTERED APPLICATIONS ARE NOW QUIESCED

AQS0140I *subtotal* OF total MATCHING REGISTERED APPLICATIONS ARE *state* – DISTRIBUTED DVIPA MEMBERS ARE IGNORED

Explanation: The Multi-site Workload Lifeline Agent issues this message in response to a MODIFY *procname*,ENABLE|QUIESCE,PORT|TCPNAME command.

In the message text:

subtotal

The count of matching applications that can be quiesced or enabled by the Agent.

total

The number of matching applications. This count includes the applications that can be quiesced or enabled by the Agent, and the applications that can only be quiesced or enabled by the VARY TCPIP,,SYSPLEX,QUIESCE|RESUME command.

state

The state of the registered applications on the system where the command was issued. Possible values are:

- ENABLED
- QUIESCED

System action: The MODIFY command is accepted. Processing continues.

Operator response: If the *subtotal* value does not equal the *total* value, the remaining matching applications can be quiesced or enabled by TCPIP using only the VARY TCPIP,,SYSPLEX,QUIESCE|RESUME command.

System programmer response: None.

Module: LACMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0140I 4 OF 5 MATCHING REGISTERED APPLICATIONS ARE
 QUIESCED – DISTRIBUTED DVIPA MEMBERS ARE IGNORED

AQS0141I ADVISOR SUMMARY

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,DISPLAY,ADVISOR command. This message is followed by summary information about this Advisor. See “MODIFY *advisor_proc*,DISPlay command: Display Lifeline Advisor information” on page 53 for the explanation of the display output.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 5, 8, 9

AQS0142I • AQS0144I

Automation: Not applicable for automation.

AQS0142I ADVISOR DETAILS

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,DISPLAY,ADVISOR,DETAIL command. This message is followed by detailed information about this Advisor. See "MODIFY *advisor_proc*,DISplay command: Display Lifeline Advisor information" on page 53 for the explanation of the display output.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 5, 8, 9

Automation: Not applicable for automation.

AQS0143I ADVISOR CONFIGURATION

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,DISPLAY,CONFIG command. This message is followed by the active configuration for this Advisor. See "MODIFY *advisor_proc*,DISplay command: Display Lifeline Advisor information" on page 53 for the explanation of the display output.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 5, 8, 9

Automation: Not applicable for automation.

AQS0144I AGENT CONFIGURATION

Explanation: The Multi-site Workload Lifeline Agent issues this message in response to a MODIFY *procname*,DISPLAY,CONFIG command. This message is followed by the active configuration for this Agent. See "MODIFY *agent_proc*,DISplay command: Display Lifeline Agent information" on page 73 for the explanation of the display output.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LACMD

Routing code: 8, 10

Descriptor code: 5, 8, 9

Automation: Not applicable for automation.

AQS0145I WORKLOAD SUMMARY

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,DISPLAY,WORKLOAD command. This message is followed by summary information about the workloads defined to this Advisor. See “MODIFY *advisor_proc*,DISPlay command: Display Lifeline Advisor information” on page 53 for the explanation of the display output.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 5, 8, 9

Automation: Not applicable for automation.

AQS0146I WORKLOAD DETAILS

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,DISPLAY,WORKLOAD,DETAIL command. This message is followed by detailed information about the workloads defined to this Advisor. See “MODIFY *advisor_proc*,DISPlay command: Display Lifeline Advisor information” on page 53 for the explanation of the display output.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 5, 8, 9

Automation: Not applicable for automation.

AQS0147I BCPII ACCESS TO SITE *sitename* NOT AVAILABLE

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it detects that it can no longer communicate with any of the images (LPARs) in the site specified by the *sitename* value by using the z/OS Base Control Program Internal Interface (BCPii) service.

In the message text:

sitename

The sysplex name of the site to which BCPii access is not available.

System action: Processing continues.

Operator response: Contact the system programmer.

| **System programmer response:** Verify that z/OS is operational on at least one of the site’s images. Verify the
| connectivity used by BCPii to communicate with each of the site’s images. See *z/OS MVS Programming: Callable
| Services for High-Level Languages* for information about diagnosing BCPii issues.

Module: LMBCPii

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0147I BCPII ACCESS TO SITE SITE02 NOT AVAILABLE

AQS0148I BCPII ACCESS TO SITE *sitename* HAS RECOVERED

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it detects that it has reestablished communication with at least one image (LPAR) in the site specified by the *sitename* value by using the z/OS Base Control Program Internal Interface (BCPii) service.

In the message text:

sitename

The sysplex name of the site to which BCPii access has recovered.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LMBCPII

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0148I BCPII ACCESS TO SITE SITE02 HAS RECOVERED

AQS0152I ALL WORKLOADS ACTIVATED ON SITE *sitename*

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,ACTIVATE,WORKLOAD=*ALL*,SITE=*sitename* command.

In the message text:

sitename

The sysplex name of the site.

System action: The Advisor notifies load balancers that new connection requests to server applications for all workloads must be routed to the site specified by the *sitename* value.

Operator response: None.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0152I ALL WORKLOADS ACTIVATED ON SITE SITE01

AQS0153I WORKLOAD *workloadname* ACTIVATED ON SITE *sitename*

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,ACTIVATE,WORKLOAD=*workloadname*,SITE=*sitename* command.

In the message text:

workloadname

The name of the workload defined in the Advisor configuration file.

sitename

The sysplex name of the site.

System action: The Advisor notifies load balancers that new connection requests to server applications defined for the workload specified by the *workloadname* value must be routed to the site specified by the *sitename* value.

Operator response: None.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0153I WORKLOAD WORK01 ACTIVATED ON SITE SITE01

AQS0154I ALL WORKLOADS *state*

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*, QUIESCE | DEACTIVATE, WORKLOAD=*ALL* command. This message is also issued when the Advisor is initially started and all workloads are automatically quiesced.

In the message text:

state

The state of the workloads. Possible values are:

- QUIESCED
- DEACTIVATED

System action: When the *state* value is QUIESCED, the Advisor notifies load balancers that new connection requests to server applications for all workloads must not be routed to any site. Connection timeouts or resets might occur on the client applications that initiate the requests while the workloads are in a quiesced state. All workloads are in a quiesced state when the Advisor is initially started. When the *state* value is DEACTIVATED, any active connections to servers that are defined in the workload definitions are terminated.

Operator response: If the message is issued in response to starting the Advisor, issue a MODIFY *procname*, ACTIVATE command to direct load balancers to begin routing connections to the specified site for the requested workloads. See Chapter 7, "Lifeline Advisor commands," on page 53 for more information.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0154I ALL WORKLOADS QUIESCED

AQS0155I WORKLOAD *workloadname state*

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*, QUIESCE | DEACTIVATE, WORKLOAD=*workloadname* command.

In the message text:

workloadname

The name of the workload defined in the Advisor configuration file.

state

The state of the specified workload. Possible values are:

- QUIESCED
- DEACTIVATED

System action: When the *state* value is QUIESCED, the Advisor notifies load balancers that new connection requests to server applications for the workload specified by the *workloadname* value must not be routed to any site.

AQS0156I • AQS0157I

Connection timeouts or resets might occur on the client applications that initiated the requests while the workload is in a quiesced state. When the *state* value is DEACTIVATED, any active connections to servers that are defined in the workload are terminated.

Operator response: None.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0155I WORKLOAD WORK01 QUIESCED
```

AQS0156I WORKLOAD *workloadname* IS NOT DEFINED TO SITE *sitename*

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,ACTIVATE command. The Advisor configuration file contains a cross_sysplex_list definition for the workload specified by the *workloadname* value, but there is no definition of this workload for the site specified by the *sitename* value.

In the message text:

workloadname

The name of the workload in the Advisor configuration file.

sitename

The sysplex name of the site for which the workload is to be activated.

System action: The MODIFY command is ignored. Processing continues.

Operator response: Save the syslogd file and contact the system programmer.

System programmer response: Examine the syslogd file for the Advisor configuration warning messages that were generated while the cross_sysplex_list definitions were being processed. The syslogd identifier is 11advr for the Advisor. Correct the configuration file warnings and either restart the Advisor or issue the MODIFY *procname*,REFRESH command. See Chapter 3, "Configuring Multi-site Workload Lifeline," on page 11 for more information about configuring the Advisor.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0156I WORKLOAD WORK01 IS NOT DEFINED TO SITE SITE01
```

AQS0157I NETWORK ACCESS TO SITE *sitename* NOT AVAILABLE

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it can no longer communicate over the network with any Multi-site Workload Lifeline Agents in the site specified by the *sitename* value.

In the message text:

sitename

The sysplex name of the site to which network access is not available.

System action: Processing continues. If the site specified by the *sitename* value represents the active site for some workloads, the Advisor continues to direct load balancers to route new connection requests to server applications for these workloads to this site.

Operator response: Contact the system programmer.

System programmer response: Verify network connectivity between the Advisor and the site specified by the *sitename* value. Verify that Agents are running on each LPAR in the site where a server application for the workloads resides. See *z/OS Communications Server: IP Diagnosis Guide* for information about diagnosing network connectivity problems.

Module: LMLB

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0157I NETWORK ACCESS TO SITE SITE01 NOT AVAILABLE

AQS0158I STANDBY SITE *sitename* HAS RECOVERED FOR WORKLOAD *workloadname*

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it determines that there is at least one server application available in the specified standby site for each of the load balancer groups defined in the specified workload.

In the message text:

sitename

The sysplex name of the standby site.

workloadname

The name of the workload defined in the Advisor configuration file.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LMLB

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0158I STANDBY SITE SITE02 HAS RECOVERED FOR WORKLOAD WORK01

AQS0159I STANDBY SITE *sitename* HAS UNAVAILABLE SERVERS FOR WORKLOAD *workloadname*

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it determines there are no server applications available in the specified standby site for at least one load balancer group defined in the specified workload.

In the message text:

sitename

The sysplex name of the standby site.

workloadname

The name of the workload defined in the Advisor configuration file.

System action: The site is no longer a usable target for the workload specified by the *workloadname* value.

Operator response: Notify the system programmer.

System programmer response: Ensure that server applications for the workload are active on the standby site specified by the *sitename* value.

Module: LMLB

Routing code: 8, 10

AQS0160I • AQS0162I

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0159I STANDBY SITE SITE02 HAS UNAVAILABLE SERVERS FOR WORKLOAD WORK01

AQS0160I NETWORK ACCESS TO SITE *sitename* HAS RECOVERED

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it reestablishes a connection with at least one Multi-site Workload Lifeline Agent in the site specified by the *sitename* value.

In the message text:

sitename

The sysplex name of the site to which network access has recovered.

System action: Processing continues.

Operator response: None.

System programmer response: None.

Module: LMAGNT, LMLB

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0160I NETWORK ACCESS TO SITE SITE01 HAS RECOVERED

AQS0161I UNABLE TO CONNECT TO PEER ADVISOR AFTER *time* SECONDS

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it is started as the primary Advisor and it does not detect another Advisor acting as the primary. When a configured primary Advisor is started, it always verifies that there is no other primary Advisor active before becoming the primary Advisor.

In the message text:

time

The number of seconds the Advisor waited trying to connect to the peer Advisor.

System action: The Advisor assumes the role of primary Advisor.

Operator response: None.

System programmer response: None.

Module: LMADV

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0161I UNABLE TO CONNECT TO PEER ADVISOR AFTER 10 SECONDS

AQS0162I MODIFY *cmd* COMMAND QUEUED - *reason*

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*, DEACTIVATE | QUIESCE | ACTIVATE command. Processing of the command is delayed until the specified reason has been resolved.

In the message text:

cmd

The MODIFY command. Possible values are DEACTIVATE, QUIESCE, or ACTIVATE.

reason

The explanation of why the command was not immediately processed. Possible reasons are:

- NO FIRST-TIER LOAD BALANCER IS REGISTERED
- DEACTIVATE COMMAND IN PROGRESS

System action: Processing continues. The command is not processed until either a first-tier load balancer registers or a prior DEACTIVATE command completes.

Operator response: Contact the system programmer.

System programmer response: If you are waiting for a first-tier load balancer, verify the network connectivity between the Advisor and first-tier load balancer. Check the load balancer and correct any configuration or connectivity problems. Restart the load balancer if necessary. See *z/OS Communications Server: IP Diagnosis Guide* for more information about diagnosing network connectivity problems.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0162I MODIFY QUIESCE COMMAND QUEUED – DEACTIVATE
COMMAND IN PROGRESS
```

AQS0163W WAITING FOR FIRST-TIER LOAD BALANCER REGISTRATION

Explanation: The Multi-site Workload Lifeline Advisor issues this message when no first-tier load balancers are connected and registered to it. This message will be deleted after the first first-tier load balancer connects and registers with the Advisor.

System action: Processing continues.

Operator response: Contact the system programmer.

System programmer response: Verify network connectivity between the Advisor and first-tier load balancer. Check the load balancer and correct any configuration or connectivity problems. Restart the load balancer if necessary. See *z/OS Communications Server: IP Diagnosis Guide* for more information about diagnosing network connectivity problems.

Module: LMMAIN

Routing code: 1, 8

Descriptor code: 2, 7

Automation: Not applicable for automation.

AQS0164W UNABLE TO CONNECT TO PEER ADVISOR AFTER *time* SECONDS

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it is started as the secondary Advisor and is unable to connect to another Advisor acting as the primary Advisor. The message is deleted when either the peer Advisor is contacted or this Advisor assumes the role of primary Advisor.

In the message text:

time

The number of seconds the Advisor waited to try to connect to the peer Advisor.

System action: If the Advisor `advisor_takeover_policy` configuration statement is configured as manual, the Advisor remains in the secondary role. If `advisor_takeover_policy` is configured as automatic, the Advisor assumes the role of primary Advisor.

Operator response: If `advisor_takeover_policy` is configured as manual, issue the `MODIFY procname,TAKEOVER`

AQS0165I • AQS0166I

command to have this Advisor assume the role of primary Advisor; otherwise, contact the system programmer.

System programmer response: Ensure that the Advisor started procedure is configured correctly (started in primary or secondary role). Verify the network connectivity between this Advisor and the peer Advisor. Ensure that the Advisor configuration files are identical between this Advisor and the peer Advisor. See Chapter 6, "Multi-site Workload Lifeline configuration statements," on page 37 for more information about configuration statements and parameters. See *z/OS Communications Server: IP Diagnosis Guide* for more information about diagnosing network connectivity problems.

Module: LMADV

Routing code: 1, 8

Descriptor code: 2, 7

Automation: This message is a possible candidate for automation if you want to use the `MODIFY procname,TAKEOVER` command to have this Advisor assume the role of primary Advisor.

Example:

```
AQS0164W UNABLE TO CONNECT TO PEER ADVISOR AFTER 10
SECONDS
```

AQS0165I PEER ADVISOR CONNECTED FROM *ipaddress*

Explanation: The Multi-site Workload Lifeline Advisor issues this message when a peer Advisor has established a connection with it.

In the message text:

ipaddress

The IP address of the peer Advisor.

System action: Processing continues if the peer Advisor is configured as the secondary Advisor. If the peer Advisor is configured as the primary Advisor, this Advisor will assume the role of secondary Advisor.

Operator response: None.

System programmer response: None.

Module: LMADV

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0165I PEER ADVISOR CONNECTED FROM 10.10.10.1
```

AQS0166I ADVISOR IS NOW IN PRIMARY ROLE

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it assumes the role of primary Advisor. The Advisor assumes the role of primary Advisor when one of the following has occurred; the Advisor procedure was configured to start the Advisor as the primary Advisor, and communication was lost with the peer Advisor acting as the primary Advisor, or a `MODIFY procname,TAKEOVER` command was issued.

System action: The Advisor assumes the role of primary Advisor and is able to accept connections from load balancers and Multi-site Workload Agents.

Operator response: None.

System programmer response: None.

Module: LMADV

Routing code: 8, 10

Descriptor code: 12

Automation: This message is a possible candidate for automation if you want to determine when to use MODIFY commands that are valid only for the primary Advisor.

AQS0167I CONNECTION FROM *ipaddress* REJECTED – *reason*

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it receives a connection request from a peer Advisor and it is not accepted.

In the message text:

ipaddress

The IP address of the peer Advisor.

reason

The reason the connection was rejected. Possible values are:

UNAUTHORIZED ADVISOR

The IP address of the peer Advisor is not included in the Advisor `advisor_id_list` configuration statement, or the IP address used to connect to this Advisor does not match the IP address in the Advisor `lb_connection_v4` or `lb_connection_v6` configuration statement.

SECONDARY ADVISOR ALREADY REGISTERED

This Advisor is already communicating with another peer Advisor, and only one peer connection is allowed.

System action: The connection from the peer Advisor is reset.

Operator response: Contact the system programmer.

System programmer response: Take the appropriate action, based on the *reason* value:

UNAUTHORIZED ADVISOR

Ensure that the IP address specified by the *ipaddress* value is included in the Advisor `advisor_id_list` configuration statement. Ensure that the IP address being used by the peer Advisor to connect to this Advisor matches the IP address in the Advisor `lb_connect_v4` or `lb_connection_v6` configuration statement. See Chapter 6, “Multi-site Workload Lifeline configuration statements,” on page 37 for more information about configuration statements and parameters.

SECONDARY ADVISOR ALREADY REGISTERED

Ensure that the peer Advisor currently connected to this Advisor is the correct one.

Module: LMADV

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0167I CONNECTION FROM 10.10.10.1 REJECTED –
UNAUTHORIZED ADVISOR
```

AQS0168I CONNECTION FROM *ipaddress* REJECTED – *reason*

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it receives a connection request from a load balancer or Agent and it is not accepted.

In the message text:

ipaddress

The IP address of the load balancer or Agent.

reason

The reason the connection was rejected. Possible values are:

AQS0168I

UNAUTHORIZED AGENT

The IP address of the Agent is not included in the Advisor `agent_id_list` configuration statement, or the IP address used to connect to this Advisor does not match the IP address in the Advisor `lb_connection_v4` or `lb_connection_v6` configuration statement.

UNAUTHORIZED LB

The IP address of the load balancer is not included in the Advisor `lb_id_list` configuration statement.

UNAUTHORIZED SITE

The sysplex name of the site where the Agent resides is not defined in the Advisor `cross_sysplex_list` configuration statement.

INCORRECT LB REGISTRATION

One of the following events occurred:

- A first-tier load balancer attempted to register a group with an IP address or port that is not included in the Advisor `cross_sysplex_list` configuration statement.
- A second-tier load balancer attempted to register before a first-tier load balancer has registered.
- A second-tier load balancer attempted to register a group name that does not match any group name registered by a first-tier load balancer.
- A load balancer attempted to register a group with no associated port.

System action: The connection from the load balancer or Agent is reset.

Operator response: Contact the system programmer.

System programmer response: Take the appropriate action, based on the *reason* values:

UNAUTHORIZED AGENT

Ensure that *ipaddress* is included in the Advisor `agent_id_list` configuration statement. Ensure that the IP address being used by the Agent to connect to this Advisor matches the IP address in the Advisor `lb_connection_v4` or `lb_connection_v6` configuration statement.

UNAUTHORIZED LB

Ensure that *ipaddress* is included in the Advisor `lb_id_list` configuration statement.

UNAUTHORIZED SITE

Ensure that the sysplex name where the Agent resides is included in the Advisor `cross_sysplex_list` configuration statement.

INCORRECT LB REGISTRATION

- Examine the `syslogd` file to determine which group is being registered incorrectly, and modify the first-tier load balancer to remove the group or ensure that the group is included in the Advisor `cross_sysplex_list` configuration statement.
- Ensure that a first-tier load balancer is configured to connect to the Advisor.
- Examine the `syslogd` file to determine which first-tier load balancer groups are registered, and modify the second-tier load balancer configuration to ensure that its groups match the registered first-tier load balancer groups.
- Examine the `syslogd` file to determine which group is being registered without a port and modify the load balancer configuration to specify a port for that group.

See Chapter 6, “Multi-site Workload Lifeline configuration statements,” on page 37 for more information about configuration statements and parameters.

Module: LMAGNT, LMMAIN

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0168I CONNECTION FROM 10.10.10.1 REJECTED –  
UNAUTHORIZED AGENT
```

AQS0169I PRIMARY ADVISOR TAKEOVER SCHEDULED

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,TAKEOVER command.

System action: The Advisor attempts to communicate with the peer Advisor to ensure that this Advisor will be the only one to assume the role of primary Advisor. Message AQS0166I will be issued when the takeover has completed.

Operator response: None.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

AQS0170I MODIFY TAKEOVER IGNORED – *reason*

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,TAKEOVER command.

In the message text:

reason

The reason the MODIFY TAKEOVER was ignored. Possible values are:

ALREADY PRIMARY

The Advisor is already the primary Advisor.

ALREADY SCHEDULED

A previous MODIFY *procname*,TAKEOVER command was issued and has not yet completed.

System action: The MODIFY command is ignored.

Operator response: None.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0170I MODIFY TAKEOVER IGNORED – ALREADY PRIMARY

AQS0172I TAKEOVER PROCESSING INCOMPLETE - UNRESPONSIVE PEER AT *ipaddress*

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,TAKEOVER command. The Advisor attempted to notify the peer Advisor that this Advisor will become the primary Advisor. The connection was lost before the notification completed.

In the message text:

ipaddress

The last known IP address of the peer Advisor.

System action: The Advisor assumes the role of primary Advisor, but the role of the peer Advisor is unknown. Message AQS0166I will be issued when the takeover has completed.

Operator response: Contact the system programmer.

System programmer response: Verify the network connectivity between this Advisor and the peer Advisor. If the peer Advisor is not active, restart it. If the peer Advisor is active, verify that it is running as the secondary Advisor.

AQS0173I • AQS0174I

See *z/OS Communications Server: IP Diagnosis Guide* for more information about diagnosing network connectivity problems.

Module: LMADV

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0172I TAKEOVER PROCESSING INCOMPLETE - UNRESPONSIVE  
PEER AT 10.10.10.1
```

AQS0173I ADVISOR IS NOW IN SECONDARY ROLE

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it assumes the role of secondary Advisor. The Advisor assumes the role of secondary Advisor when one of the following has occurred; the Advisor procedure was configured to start the Advisor as the secondary Advisor or a `MODIFY procname,TAKEOVER` command was issued on the peer Advisor.

System action: The Advisor assumes the role of secondary Advisor and attempts to connect to the peer Advisor.

Operator response: None.

System programmer response: None.

Module: LMADV

Routing code: 8, 10

Descriptor code: 12

Automation: This message is a possible candidate for automation if you want to determine when to use `MODIFY` commands that are valid only for the secondary Advisor.

AQS0174I TAKEOVER FAILED – ERROR ON PRIMARY ADVISOR AT *ipaddress*

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a `MODIFY procname,TAKEOVER` command. While attempting to communicate with the peer Advisor to ensure that this Advisor will be the only one to assume the role of primary Advisor, the peer Advisor did not relinquish its role as primary Advisor.

In the message text:

ipaddress

The IP address of the peer Advisor.

System action: This Advisor remains in the role of secondary Advisor and the peer Advisor is in an unknown role.

Operator response: Contact the system programmer.

System programmer response: Check for console messages or examine the `syslogd` file on the peer Advisor's system. The `syslogd` identifier is `11advr` for the Advisor. If the peer Advisor is not active, restart it in the role of primary Advisor. If the peer Advisor is active, verify that it is running as the primary Advisor.

Module: LMADV

Routing code: 8, 10

Descriptor code: 12

Automation: This message is a possible candidate for automation if you want to ensure the peer Advisor is stopped and this Advisor is restarted as the primary Advisor.

Example:

```
AQS0174I TAKEOVER FAILED – ERROR ON PRIMARY ADVISOR AT  
10.10.10.1
```

AQS0175I TAKEOVER FAILED – ERROR ESTABLISHING LISTENING SOCKETS

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,TAKEOVER command. While attempting to become the primary Advisor, this Advisor was unable to establish listening sockets to allow for load balancers, Multi-site Workload Lifeline Agents, or a peer Advisor to connect to it.

System action: The Advisor remains in the role of secondary Advisor.

Operator response: Determine whether TCP/IP is available and restart if necessary. Reissue the MODIFY *procname*,TAKEOVER command. If TCP/IP is available when this message is issued, save the syslogd file and contact the system programmer.

System programmer response: If TCP/IP is available when the Advisor issues this message, examine the syslogd file to determine which listening sockets cannot be established and correct the error. The syslogd identifier is 11advr for the Advisor.

Module: LMADV

Routing code: 8, 10

Descriptor code: 12

Automation: This message is a possible candidate for automation if you want to ensure the peer Advisor is started as the primary Advisor.

AQS0176I WORKLOAD STATE NOT REPLICATED TO SECONDARY ADVISOR

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it is unable to send updated workload state information, indicating whether the workload was rerouted or quiesced, to the secondary Advisor.

System action: Processing continues, but the primary and secondary Advisors are no longer in sync.

Operator response: Contact the system programmer.

System programmer response: Verify the network connectivity between this Advisor and the secondary Advisor. Examine the syslogd file to determine the cause of the communication failure. The syslogd identifier is 11advr for the Advisor. Restart the secondary Advisor to enable the two Advisors to resync. See *z/OS Communications Server: IP Diagnosis Guide* for information about diagnosing network connectivity problems.

Module: LMADV

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

AQS0177I ADVISOR STOPPING – *reason*

Explanation: The Multi-site Workload Lifeline Advisor issues this message during initialization when the peer Advisor resets the connection with this Advisor.

In the message text:

reason

The reason the Advisor is stopping. Possible values are:

NOT AUTHORIZED TO PRIMARY ADVISOR

The IP address of this Advisor is not included in the peer Advisor *advisor_id_list* configuration statement, or the IP address specified in the Advisor *lb_connection_v4* or *lb_connection_v6* configuration statement does not match what is defined in the peer Advisor's configuration.

PRIMARY ADVISOR ALREADY HAS A SECONDARY REGISTERED

The peer Advisor is already communicating with another peer Advisor; only one peer connection is allowed.

System action: Processing ends. The connection with the peer Advisor is reset.

Operator response: Contact the system programmer.

AQS0178I • AQS0179I

System programmer response: Take the appropriate action, based on the *reason* value:

NOT AUTHORIZED TO PRIMARY ADVISOR

Ensure that the Advisor's IP address is included in the peer Advisor's *advisor_id_list* configuration statement. Ensure that the Advisor's *lb_connection_v4* and *connection_v6* configuration statements match the peer Advisor's configuration statements. See Chapter 6, "Multi-site Workload Lifeline configuration statements," on page 37 for more information about configuration statements and parameters.

PRIMARY ADVISOR ALREADY HAS A SECONDARY REGISTERED

Ensure that the secondary Advisor connected to the peer Advisor is the correct one.

Module: LMADV

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0177I ADVISOR STOPPING – NOT AUTHORIZED TO PRIMARY  
ADVISOR
```

AQS0178I WORKLOAD *workloadname* MUST BE QUIESCED BEFORE ISSUING A *cmd* COMMAND

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a `MODIFY procname,DEACTIVATE|ACTIVATE` command. The workload must be quiesced before you can deactivate it or reroute it to an alternate standby site.

In the message text:

cmd

The `MODIFY` command that was issued. Possible values are `DEACTIVATE` and `ACTIVATE`.

workloadname

The name of the workload defined in the Advisor configuration file.

System action: The `MODIFY` command is ignored.

Operator response: Issue a `MODIFY procname,QUIESCE,WORKLOAD=workloadname` to quiesce the workload, and then reissue the `MODIFY procname,DEACTIVATE|ACTIVATE` command.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0178I WORKLOAD WORK01 MUST BE QUIESCED BEFORE  
ISSUING A DEACTIVATE COMMAND
```

AQS0179I MODIFY *cmd* COMMAND IGNORED – *reason*

Explanation: The Multi-site Workload Lifeline Advisor issues this message when a `MODIFY procname` command is ignored.

In the message text:

cmd

The `MODIFY` command that was issued.

reason

The reason that the `MODIFY` command was ignored. Possible values are:

ADVISOR MUST BE PRIMARY

The `MODIFY` command was issued on the Advisor that was acting as the secondary Advisor.

NO AGENT IS REGISTERED

The MODIFY *procname*,DEACTIVATE command was issued, but no Multi-site Workload Lifeline Agents are available to reset active connections on their systems.

SITE HAS NO ACTIVE AGENT

The MODIFY *procname*,ACTIVATE command was issued, but no Multi-site Workload Lifeline Agents are available in the site where the workload is being rerouted.

System action: The MODIFY command is ignored.

Operator response: Take the following actions based on the *reason* value:

ADVISOR MUST BE PRIMARY

Reissue the MODIFY command on the system where the primary Advisor is running.

NO AGENT IS REGISTERED

Contact the system programmer.

SITE HAS NO ACTIVE AGENTS

Contact the system programmer.

System programmer response: Verify whether the Agents on the site are active and restart, if necessary. Verify network connectivity between the Advisor and the Agents. See *z/OS Communications Server: IP Diagnosis Guide* for information about diagnosing network connectivity problems.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0179I MODIFY QUIESCE COMMAND IGNORED – ADVISOR MUST
BE PRIMARY
```

AQS0180W WORKLOAD *workloadname* HAS UNAVAILABLE SERVERS ON SITE *sitename*

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it determines there are no servers available in the site specified by the *sitename* value for at least one load balancer group defined in the workload specified by the *workloadname* value. This message will be deleted when at least one server in each load balancer group is active or the workload is rerouted to the alternate standby site.

In the message text:

workloadname

The name of the workload defined in the Advisor configuration file.

sitename

The sysplex name of the active site.

System action: The site is no longer a usable target for the workload specified by the *workloadname* value. If the Advisor *workload_switch_policy* configuration statement is configured as automatic, the Advisor will automatically notify load balancers that new connection requests to server applications for the specified workload that are currently being routed to the specified site must be routed to the alternate standby site. If the *workload_switch_policy* configuration statement is configured as manual, the Advisor continues to notify load balancers to route new connection requests to server applications for the workload specified by the *workloadname* value to the site specified by the *sitename* value.

Operator response: If the *workload_switch_policy* configuration statement is configured as manual, issue the MODIFY *procname*,ACTIVATE command for the workload specified by the *workloadname* value currently being routed to the site specified by the *sitename* value to notify the load balancers that new connection requests must be routed to the specified site. See Chapter 7, “Lifeline Advisor commands,” on page 53 for more information. Contact the system programmer.

System programmer response: Ensure that server applications for the workload are active on the active site specified by the *sitename* value.

AQS0181I • AQS0184W

Module: LMLB

Routing code: 1, 8

Descriptor code: 2, 7

Automation: This message is a possible candidate for automation if you want to use the MODIFY *procname*,ACTIVATE command to have the workload routed to the alternate site.

Example:

```
AQS0180W WORKLOAD WORK01 HAS UNAVAILABLE SERVERS ON
SITE SITE01
```

AQS0181I ADVISOR CONFIGURATION UPDATED

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,REFRESH command.

System action: The Advisor configuration is updated.

Operator response: None.

System programmer response: None.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

AQS0182I ADVISOR CONFIGURATION NOT UPDATED

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,REFRESH command. The Advisor configuration file cannot be opened, or contains one or more errors.

System action: The MODIFY command is ignored.

Operator response: Contact the system programmer.

System programmer response: Examine the syslogd file for configuration error messages. The syslogd identifier is 11advsr for the Advisor. Correct the configuration file errors and reissue the MODIFY *procname*,REFRESH command. See Chapter 6, "Multi-site Workload Lifeline configuration statements," on page 37 for more information about configuration statements and parameters.

Module: LMCMD

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

AQS0184W PRIMARY AND SECONDARY ADVISOR CONFIGURATION NOT IN SYNC

Explanation: The Multi-site Workload Lifeline Advisor issues this message in response to a MODIFY *procname*,REFRESH command issued from the peer Advisor when the active configuration for the two Advisors is no longer the same. This message will be deleted when the active configuration of both Advisors are back in sync.

System action: Processing continues.

Operator response: Ensure that the Advisor configuration file is updated to match the peer Advisor and issue the MODIFY *procname*,REFRESH command from this Advisor.

System programmer response: None.

Module: LMADV

Routing code: 1, 8

Descriptor code: 2, 7

Automation: Not applicable for automation.

AQS0185I AGENT CONNECTION TO ADVISOR AT *ipaddress* REJECTED – *reason*

Explanation: The Multi-site Workload Lifeline Agent issues this message during initialization when the Multi-site Workload Lifeline Advisor resets the connection with this Agent.

In the message text:

ipaddress

The IP address of the primary Advisor.

reason

The reason the Agent connection was rejected. Possible values are:

SITE NOT DEFINED TO ADVISOR

The site where this Agent resides is not included in the Advisor `cross_sysplex_list` configuration statement.

NOT AUTHORIZED TO ADVISOR

The IP address defined in the Agent `host_connection` configuration statement is not included in the Advisor `agent_id_list` configuration statement, or the IP address defined in the Agent `advisor_id` configuration statement does not match the Advisor `lb_connection_v4` or `lb_connection_v6` configuration statement.

System action: Processing ends. The connection with the primary Advisor is reset.

Operator response: Contact the system programmer.

System programmer response: Take the appropriate action, based on the *reason* value:

SITE NOT DEFINED TO ADVISOR

Ensure that the Agent's site is included in the Advisor's `cross_sysplex_list` configuration statement. See Chapter 6, "Multi-site Workload Lifeline configuration statements," on page 37 for more information about configuration statements and parameters.

NOT AUTHORIZED TO ADVISOR

Ensure that the Agent's IP address defined in the `host_connection` configuration statement is included in the Advisor's `agent_id_list` configuration statement. Ensure that the Agent's IP address defined in the `advisor_id` configuration statement matches the Advisor's `lb_connection_v4` or `lb_connection_v6` configuration statement. See Chapter 6, "Multi-site Workload Lifeline configuration statements," on page 37 for more information about configuration statements and parameters.

Module: LAADV

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

```
AQS0185I AGENT CONNECTION TO ADVISOR AT 10.10.10.1
REJECTED – NOT AUTHORIZED TO ADVISOR
```

AQS0186I ADVISOR NMI IS NO LONGER AVAILABLE

Explanation: The Multi-site Workload Lifeline Advisor issues this message when the Network Management Interface (NMI) is stopped.

System action: Processing continues. The NMI connections with network management agents are reset.

Operator response: Contact the system programmer.

System programmer response: Examine the `syslogd` file for NMI error messages and correct the error. The `syslogd` identifier is `11advr` for the Advisor. Recycle the Advisor to restart the NMI.

Module: LMNMI

AQS0187I • AQS0188W

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

AQS0187I BCPII MONITORING IS NOT AVAILABLE

Explanation: The Multi-site Workload Lifeline Advisor issues this message when it is unable to use the Base Control Program Internal Interface (BCPii) service.

System action: Processing continues.

Operator response: Save the syslogd file and contact the system programmer.

System programmer response: Verify that the BCPii address space was successfully started. Ensure that the Lifeline Advisor is authorized to use BCPii services. Examine the syslogd file to determine the cause of the BCPii failure. The syslogd identifier is lladvsr for the Advisor. Correct the problem, and then stop and restart the Lifeline Advisor. See *z/OS MVS Programming: Callable Services for High-Level Languages* for information about diagnosing BCPii issues.

Module: LMBCPII

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

AQS0188W SITE *sitename* IS NOT AVAILABLE

Explanation: The Multi-site Workload Lifeline Advisor issues this message when both of the following conditions occurs:

- The Advisor can no longer communicate over the network with any Multi-site Workload Lifeline Agents in the specified site.
- The Advisor can no longer communicate with any of the images (LPARs) in the specified site by using the Base Control Program Internal Interface (BCPii) service.

This message will be deleted when at least one Agent from this site reconnects to the Advisor or communication is reestablished with at least one image from this site by using BCPii services.

In the message text:

sitename

The sysplex name of the unresponsive site.

System action: The site is no longer considered responsive and is no longer a usable target for any defined workloads. If the Advisor workload_switch_policy configuration statement is configured with a value of automatic, the Advisor will automatically direct load balancers that new connection requests to server applications for workloads currently being routed to the site specified by the *sitename* value should be routed to the alternate, standby site. If workload_switch_policy is configured with a value of manual, the Advisor continues to direct load balancers to route new connection requests to server applications for these workloads to the site specified by the *sitename* value.

Operator response: If workload_switch_policy is configured with a value of manual, issue the MODIFY *procname*,ACTIVATE command for each workload currently being routed to the site specified by the *sitename* value. This will direct the load balancers that new connection requests should be routed to the alternate, standby site. See Chapter 7, "Lifeline Advisor commands," on page 53 for more information.

System programmer response: Ensure that the site specified by the *sitename* value is available. If the site is available, verify network connectivity between the Advisor and the site. Verify that Agents are running on each LPAR in the site where a server application for the workloads resides. Verify the connectivity used by BCPii to communicate with each of the site's images. See *z/OS Communications Server: IP Diagnosis Guide* for information about diagnosing network connectivity problems. See *z/OS MVS Programming: Callable Services for High-Level Languages* for information about diagnosing BCPii issues.

Module: LMBCPII, LMLB

Routing code: 1, 8

Descriptor code: 2, 7

Automation: This message is a possible candidate for automation if you want to use the MODIFY *procname*,ACTIVATE command to have workloads routed to the alternate site.

Example:

AQS0188W SITE SITE01 IS NOT AVAILABLE

AQS0189W PEER ADVISOR IS NOT AVAILABLE

Explanation: The Multi-site Workload Lifeline Advisor issues this message when both of the following conditions occurs:

- The Advisor can no longer communicate over the network with the peer Advisor.
- The Advisor can no longer communicate with the image (LPAR) where the peer Advisor was active by using the Base Control Program Internal Interface (BCPii) service.

This message will be deleted when the peer Advisor reconnects to this Advisor or communication is reestablished with the image where the peer Advisor was active by using BCPii services.

System action: Processing continues. The peer Advisor site is no longer considered responsive.

Operator response: If this Advisor is the secondary Advisor and *advisor_takeover_policy* is configured with a value of *manual*, issue the MODIFY *procname*,TAKEOVER command to make this Advisor assume the role of primary Advisor; otherwise, contact the system programmer.

System programmer response: Ensure that the peer Advisor is available. Check for prior AQS0124I and AQS0125I messages to determine the system name where the peer Advisor was active. If the peer Advisor is available, verify network connectivity between the Advisor and its peer Advisor. Verify the connectivity used by BCPii to communicate with each of the site's images. See *z/OS Communications Server: IP Diagnosis Guide* for information about diagnosing network connectivity problems. See *z/OS MVS Programming: Callable Services for High-Level Languages* for information about diagnosing BCPii issues.

Module: LMBCPii

Routing code: 1, 8

Descriptor code: 2, 7

Automation: This message is a possible candidate for automation if you want to use the MODIFY *procname*,TAKEOVER command to have this Advisor assume the role of primary Advisor.

AQS0190I MULTIPLE CONNECTION ATTEMPTS FROM *ipaddress* REJECTED

Explanation: The Multi-site Workload Lifeline Advisor issues this message when a load balancer repeatedly tries to connect. This usually indicates that the load balancer was configured incorrectly and the Advisor does not permit any of the connection attempts.

In the message text:

ipaddress

The IP address of the load balancer.

System action: Processing continues. If the load balancer is still active, it might continue to attempt to reconnect to the Advisor.

Operator response: Locate the prior AQS0168I message that precedes this message and contact the system programmer. Message AQS0168I describes the reason that the load balancer connection was rejected.

System programmer response: Refer to message AQS0168I for steps to correct the problem.

Module: LMLB

Routing code: 8, 10

Descriptor code: 12

Automation: Not applicable for automation.

Example:

AQS0191I

| AQS0190I MULTIPLE CONNECTION ATTEMPTS FROM 10.10.10.1 REJECTED

| **AQS0191I** **MODIFY ACTIVATE COMMAND IGNORED - WORKLOAD** *workloadname* **HAS CONNECTIONS**
| **ON SITE** *sitename*

| **Explanation:** The Multi-site Workload Lifeline Advisor issues this message when a **MODIFY** *procname*,**ACTIVATE**
| command is issued but active connections for the workload exist on the alternate site *sitename*.

| In the message text:

| *workloadname*

| The name of the workload defined in the Advisor configuration file.

| *sitename*

| The sysplex name of the alternate site.

| **System action:** The **MODIFY** command is ignored.

| **Operator response:** Issue the **MODIFY** *procname*,**DEACTIVATE**,**WORKLOAD**=*workloadname* command to reset any
| remaining active connections. Then reissue the **MODIFY** *procname*,**ACTIVATE** command.

| **System programmer response:** None

| **Module:** LMCMD

| **Routing code:** 8, 10

| **Descriptor code:** 12

| **Automation:** Not applicable for automation.

| **Example:**

| AQS0191I MODIFY ACTIVATE COMMAND IGNORED - WORKLOAD WORK01 HAS CONNECTIONS ON SITE SITE01

Appendix A. A sample started procedure for Lifeline Advisors

You can use the sample started procedure to understand how to set up the environment for the Lifeline Advisor.

```
//AQSADV PROC ROLE=S
//*
//*****
//* Function: Sample procedure for running the Multi-site
//* Workload Lifeline Advisor
//*
//* Parameters: [ROLE={S | P}]
//* S ==> Secondary Advisor (Default Role)
//* P ==> Primary Advisor
//*****
//AQSADV EXEC PGM=AQSLBADV,REGION=0K,TIME=NOLIMIT,
// PARM='/ -R &ROLE'
//*****
//* The STEPLIB card below points to the PDS/E where the Lifeline
//* load modules are kept.
//*****
//STEPLIB DD DSN=USER.LOADLIB,DISP=SHR
//*****
//* The CONFIG card below points to the member where the Lifeline
//* Advisor configuration file is located
//*****
//CONFIG DD DSN=USER.PROFILES(ADVCONF),DISP=SHR
//STDENV DD DUMMY
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=F,LRECL=80,BLKSIZE=80)
//SYSIN DD DUMMY
//SYSERR DD SYSOUT=*
//SYSOUT DD SYSOUT=*,DCB=(RECFM=F,LRECL=80,BLKSIZE=80)
//CEEDUMP DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
//SYSDUMP DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
//*****
//* The SYSTCPD card below points to the member where the TCPIP.DATA
//* file is located
//*****
//SYSTCPD DD DSN=USER.PROFILES(TCPDATA),DISP=SHR
```

Figure 4. Sample started procedure AQSADV

Appendix B. A sample started procedure for Lifeline Agents

You can use the sample started procedure to understand how to set up the environment for the Lifeline Agent.

```
//AQSAGE      PROC
//*
//*****
//*
//* Function: Sample procedure for running the Multi-site
//* Workload Lifeline Agent
//*
//*****
//AQSAGE EXEC PGM=AQSLBAGE,REGION=0K,TIME=NOLIMIT,
//  PARM='POSIX(ON) ALL31(ON)/'
//*****
//* The STEPLIB card below points to the PDS/E where the Lifeline
//* load modules are kept.
//*****
//STEPLIB DD DSN=USER.LOADLIB,DISP=SHR
//*****
//* The CONFIG card below points to the member where the Lifeline
//* Agent configuration file is located
//*****
//CONFIG DD DSN=USER.PROFILES(AGECONF),DISP=SHR
//STDENV DD DUMMY
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=F,LRECL=80,BLKSIZE=80)
//SYSIN DD DUMMY
//SYSERR DD SYSOUT=A
//SYSOUT DD SYSOUT=A
//CEEDUMP DD SYSOUT=A
//SYSDUMP DD SYSOUT=A
//*****
//* The SYSTCPD card below points to the member where the TCPIP.DATA
//* file is located
//*****
//SYSTCPD DD DSN=USER.PROFILES(TCPDATA),DISP=SHR
```

Figure 5. Sample started procedure AQSAGE

Appendix C. Sample configuration statements

You can use the following sample configuration statements to understand how to configure the Lifeline Advisor and the Lifeline Agent.

Multi-site Workload Lifeline configuration example

The following figure shows an example of a configuration of Multi-site Workload Lifeline and how to configure the Lifeline Advisors and Lifeline Agents to work in such an environment.

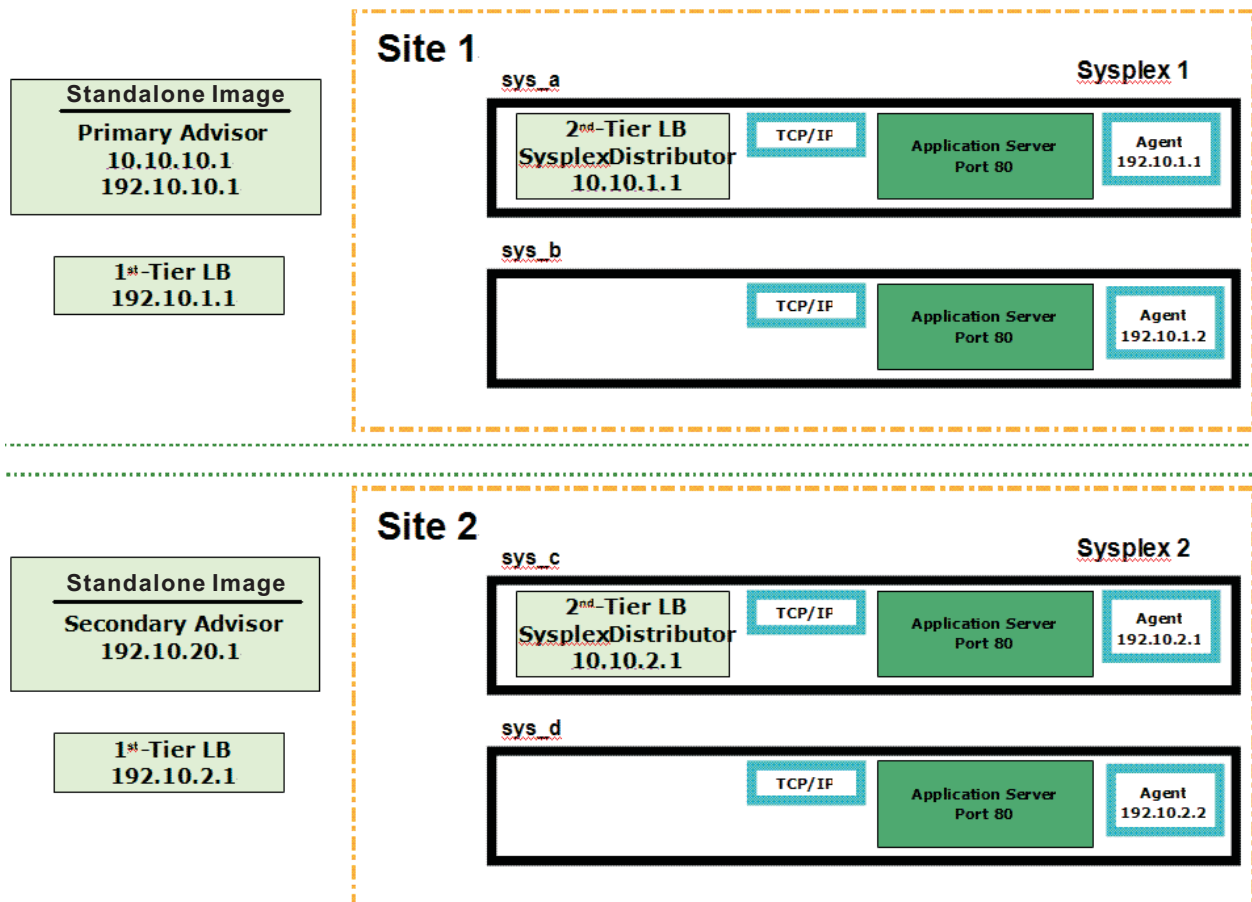


Figure 6. Multi-site Workload Lifeline configuration example

To configure the previous sample environment shown in Figure 6, perform the following tasks:

1. Configure and start the Lifeline Advisor on the primary controller in the primary role. The primary Advisor listens on dynamic VIPA (DVIPA) address 10.10.10.1, which is defined in the VIPARANGE statement.
2. Configure and start the Lifeline Advisor on the secondary controller, in the secondary role. The secondary Advisor uses static VIPA address 192.10.20.1 to communicate with the primary Advisor.

3. Define distributable DVIPA 10.10.1.1 on system sys_a in sysplex Site1, and allow both sys_a and sys_b to be targets of this DVIPA.
4. Define distributable DVIPA 10.10.2.1 on system sys_c in sysplex Site2, and allow both sys_c and sys_d to be targets of this DVIPA.
5. Configure and start Lifeline Agents on each of the images in Site 1 and Site 2, using the static VIPA that is defined in that image (192.10.1.1 on sys_a, 192.10.1.2 on sys_b, 192.10.2.1 on sys_c, and 192_10.2.2 on sys_d).

Sample configuration statements for the Lifeline Advisor

You can use the following sample configuration file to configure the Lifeline Advisor in the sample environment set in Appendix A, "A sample started procedure for Lifeline Advisors," on page 133. Use this configuration for the Advisors on both the primary and secondary controllers.

```

#=====
#
# This file contains sample configuration statements for the Lifeline
# Advisor - using default settings in most cases.
#
#=====

# Following specifies the port which the primary advisor will listen
# on for connections from agents.
agent_connection_port      8181

# Following specifies which agents are allowed to connect to the
# primary advisor.
agent_id_list
{
    192.10.1.1..4000      # IP address and port for sys_a
    192.10.1.2..4000      # IP address and port for sys_b
    192.10.2.1..4000      # IP address and port for sys_c
    192.10.2.2..4000      # IP address and port for sys_d
}

# Following specifies the port which the primary advisor will listen
# on for connections from a secondary advisor.
advisor_connection_port    8000

# Following specifies which secondary advisors are allowed to connect
# to the primary advisor (should contain at least IP address of this
# host)
advisor_id_list
{
    192.10.10.1          # IP address for Advisor on primary controller
    192.10.20.1          # IP address for Advisor on secondary controller
}

# Following specifies the IPv4 address and port the primary advisor
# listens on for connections from load balancers.
lb_connection_v4          10.10.10.1..3860

# Following specifies which load balancers are allowed to connect to
# the primary advisor.
lb_id_list
{
    192.10.1.1          # IP address of LB in Site1
    192.10.2.1          # IP address of LB in Site2
}

# Following specifies the IP address and site name (i.e. sysplex name)
# that identifies each second-tier load balancer, the port number of the
# application server used for a specific workload, and the workload name.
cross_sysplex_list
{
    10.10.1.1..80,SITE1,WORKLOAD1      # HTTP Server on Site1
    10.10.2.1..80,SITE2,WORKLOAD1      # HTTP Server on Site2
}

```

Figure 7. Sample configuration statements for the Lifeline Advisor

The Lifeline Advisor accesses files within the Unix System Services shell, so the Lifeline Advisor needs to have an OMVS segment defined for it. Assuming that the Lifeline Advisor is started using a procedure called AQSADV, use the following JCL snippet to define the OMVS segment:

```
//EZARACF JOB MSGLEVEL=(1,1),MSGCLASS=A,CLASS=A
//DAEMONS EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
    ADDUSER AQSADV DFLTGRP(OMVSGRP) OMVS(UID(0) HOME('/'))
    RDEFINE STARTED AQSADV.* STDATA(USER(AQSADV))
    SETROPTS RACLIST(STARTED) REFRESH
//*
```

According to previous samples, you need to update the TCPIP profile on both the primary and secondary controllers to contain the following information:

```
VIPADYNAMIC
VIPARANGE DEFINE 255.255.255.255 10.10.10.1
ENDVIPADYNAMIC
```

Sample configuration statements for the Lifeline Agent

You can use the following sample configuration file to configure the Lifeline Agent in the sample environment set in Appendix B, “A sample started procedure for Lifeline Agents,” on page 135.

```
#####
#
# This file contains sample configuration statements for the Lifeline
# Agent - most defaults are selected.
#
#####

# Following specifies the IP address and port of the primary advisor
# that this agent connects to.
advisor_id          10.10.10.1..8181

# Specifies the local IP address and port this agent binds to before
# connecting to the primary advisor. Uncomment the statement that
# applies to the image that the Agent is running on.
#host_connection    192.10.1.1..4000 # sys_a
#host_connection    192.10.1.2..4000 # sys_b
#host_connection    192.10.2.1..4000 # sys_c
#host_connection    192.10.2.2..4000 # sys_cd
```

Figure 8. Sample configuration statements for the Lifeline Agent

The Lifeline Advisor accesses files within the UNIX System Services shell, so you need to define an OMVS segment for the Lifeline Advisor. Assuming that the Lifeline Advisor is started using a procedure called AQSAGE, you can use the following JCL snippet to define the OMVS segment:

```
//EZARACF JOB MSGLEVEL=(1,1),MSGCLASS=A,CLASS=A
//DAEMONS EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
    ADDUSER AQSAGE DFLTGRP(OMVSGRP) OMVS(UID(0) HOME('/'))
    RDEFINE STARTED AQSAGE.* STDATA(USER(AQSAGE))
    SETROPTS RACLIST(STARTED) REFRESH
//*
```

According to previous samples, you need to update the TCPIP profile on the image owning the distributable dynamic VIPA in the following way:

```
VIPADYNAMIC
; Uncomment statement that applies to the image where the Sysplex Distributor
; is being started
;
; Site1 definitions
; VIPARANGE DEFINE 255.255.255.255 10.10.1.1
; VIPADIST DISTMETHOD SERVERWLM 10.10.1.1 PORT 80 DESTIP ALL
;
; Site2 definitions
; VIPARANGE DEFINE 255.255.255.255 10.10.2.1
; VIPADIST DISTMETHOD SERVERWLM 10.10.2.1 PORT 80 DESTIP ALL
ENDVIPADYNAMIC
```

Appendix D. Accessibility

Publications for this product are offered in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience problems, send an e-mail to mhvrcfs@us.ibm.com or write to:

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Mail Station P181
2455 South Road
Poughkeepsie, NY 12601-5400
U.S.A.

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:

- Use assistive technologies such as screen readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using such products to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to *z/OS TSO/E Primer*, *z/OS TSO/E User's Guide*, and *z/OS ISPF User's Guide Vol I* for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Mail Station P300
2455 South Road
Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of 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.

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

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Policy for unsupported hardware

Various z/OS elements, such as DFSMS, HCD, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Adobe and PostScript are registered trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Intel is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

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

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of IBM or other companies.

Index

Numerics

1st-tier load balancers 4

A

accessibility 143
activating workloads 66
advisor_connection_port 38
advisor_id 48
advisor_id_list 38, 49
advisor_takeover_policy 39
advisor_timeout 39
agent_connection_port 40
agent_id_list 40

B

BCPii 8

C

changing the debug level 68, 83
CINET Considerations 20
configuration statements 37
 Lifeline Advisor 37
 Lifeline Agent 48
configuring
 external load balancers 20
 first-tier external load balancers 20
 Lifeline Advisor 12, 15, 17
 Lifeline Agent 14
 Lifeline Agents
 WLM recommendations 15
 primary Advisor 12
 restart 15, 17
 second-tier external load balancers 31
 second-tier internal load balancers 23
 secondary Advisor 12
 syslogd 18
Configuring 11
 Base Control Program Internal Interface 18
 BCPii 18
cross_sysplex_list 41
customizing
 TCP/IP profiles 19, 20
 TCP/IP stacks 19

D

deactivating workloads 67
debug levels 27
debug_level 42, 49
diagnosing
 debug levels 27
 diagnostic data 28
 failure of registering with ARM 35
 Lifeline Advisor connection termination 35
 Lifeline Advisor hung 33
 Lifeline Agent hung 33

diagnosing (*continued*)
 Lifeline Agent termination 34
 load balancer connection termination 34
 Multi-site Workload Lifeline 27
 unreadable group names 33
 workload distribution problems 32
 workload not distributed 30
diagnostic data 28
directed mode 4
disability 143
dispatch mode 4
display command
 Lifeline Advisor
 configuration information 53
 debug level 53
 external load balancers 53
 Lifeline Agents 53
 peer Advisor 53
 work load 53
 Lifeline Agent
 configuration 73
 debug levels 73
 server applications 73

E

enabling server applications 79
external load balancers
 configuring 20
External load balancers
 directed mode 4
 dispatch mode 4

F

failure of registering with ARM 35
failure_detection_interval 43
first-tier external load balancers
 configuring 20

I

IBM Software Support Center, contacting xii
Internal load balancers 6

L

lb_connection_v4 43
lb_connection_v6 44
lb_id_list 45
Lifeline Advisor
 activating workloads 66
 changing the debug level 68
 deactivating workloads 67
 display command 53
 quiescing workloads 69
 sample configuration statements 137
 taking over primary Advisor responsibilities 70
 updating configuration 70

- Lifeline Advisor commands 53
- Lifeline Advisor configuration file 11
- Lifeline Advisor configuration statements 37
 - advisor_connection_port 38
 - advisor_id_list 38
 - advisor_takeover_policy 39
 - advisor_timeout 39
 - agent_connection_port 40
 - agent_id_list 40
 - cross_sysplex_list 41
 - debug_level 42
 - failure_detection_interval 43
 - lb_connection_v4 43
 - lb_connection_v6 44
 - lb_id_list 45
 - peer_advisor_id 45
 - update_interval 46
 - workload_switch_policy 47
- Lifeline Advisor connection termination 35
- Lifeline Advisor hung 33
- Lifeline Advisors 3
 - sample started procedure 133
 - starting 25
 - verifying 29
- Lifeline Agent
 - changing the debug level 83
 - display command 73
 - enabling server applications 79
 - quiescing server applications 81
 - sample configuration statements 137
- Lifeline Agent commands 73
- Lifeline Agent configuration file 11
- Lifeline Agent configuration statements 48
 - advisor_id 48
 - advisor_id_list 49
 - debug_level 49
- Lifeline Agent hung 33
- Lifeline Agents 4
 - sample started procedure 135
 - starting 25
 - verifying 29
- load balancer connection termination 34

M

- messages 91
- modify command
 - Lifeline Advisor
 - activating workloads 66
 - changing the debug level 68
 - deactivating workloads 67
 - quiescing workloads 69
 - taking over primary Advisor responsibilities 70
 - updating configuration 70
 - Lifeline Agent
 - changing the debug level 83
 - enabling server applications 79
 - quiescing server applications 81
- Multi-site Workload Lifeline 85
 - configuration example 137
 - configuration statements 37
 - configuring 11
 - diagnosing 27
 - messages 91
 - overview 1
 - preparing 7

N

- network management interface 85
 - message format 87

O

- overview
 - Multi-site Workload Lifeline 1

P

- peer_advisor_id 45
- preparing
 - active connections 9
 - authorizing the Lifeline Advisors 8
 - authorizing the Lifeline Agents 9
 - BCPii 8
 - granting users explicit authority 7
 - prerequisites 7
 - WLM services 9
- prerequisites 11

Q

- quiescing server applications 81
- quiescing workloads 69

R

- RACF 7, 9
- recommendations 3
- recovering
 - planned outage 16
 - TCP/IP stack 16, 17
 - unplanned outage 17

S

- sample configuration statements 137
- sample started procedure
 - Lifeline Advisors 133
 - Lifeline Agents 135
- second-tier external load balancers
 - configuring 21
- second-tier internal load balancers
 - configuring 23
- second-tier load balancers 4
- starting
 - Lifeline Advisors 25
 - Lifeline Agents 25
 - syslogd 18
- syntax diagram, how to read xiii
- syslogd 18
- syslogd priority level 27

T

- taking over primary Advisor responsibilities 70
- trademark information 147

U

unreadable group names 33
update_interval 46
updating configuration 70
users explicit authority 7

V

verifying
 Lifeline Advisors 29
 Lifeline Agents 29

W

WLM recommendations 15
WLM services 9
workload distribution problems 32
workload not distributed 30
workload_switch_policy 47

Z

z/OS sysplex distributor 6

Communicating your comments to IBM

If you especially like or dislike anything about this document, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this document. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Please send your comments to us in either of the following ways:

- If you prefer to send comments by FAX, use this number: 1+919-254-1258
- If you prefer to send comments electronically, use this address:
 - comsvrcf@us.ibm.com
- If you prefer to send comments by post, use this address:

International Business Machines Corporation
Attn: z/OS Communications Server Information Development
P.O. Box 12195, 3039 Cornwallis Road
Department AKCA, Building 501
Research Triangle Park, North Carolina 27709-2195

Make sure to include the following in your note:

- Title and publication number of this document
- Page number or topic to which your comment applies.



Printed in USA

SC23-8600-01

